Initial Trust Establishment for Personal Space IoT Systems

A thesis submitted in fulfilment of the requirements for
the degree of Doctor of Philosophy
in the Faculty of Engineering and Information Technology
at the University of Technology Sydney

by

Thi Tham Nguyen

Supervised by

Professor Doan B. Hoang

2019

Certificate of original authorship

I, Thi Tham Nguyen declare that this thesis, is submitted in fulfilment of the requirements for the award of the degree of Doctor of Philosophy, in the Faculty of Engineering and Information Technology at the University of Technology Sydney.

This thesis is wholly my own work unless otherwise reference or acknowledged. In addition, I certify that all information sources and literature used are indicated in the thesis.

This document has not been submitted for qualifications at any other academic institution.

Signature: Production Note: Signature removed prior to publication. Thi Tham Nguyen

Date: 03, January 2019

Dedication

To my parents, my sisters and my brothers

Thank you for your love and support

Acknowledgments

I wish to express my profound gratitude and sincere thanks to my principal supervisor, Professor Doan B. Hoang for leading me along the way to this point and educating me on both academic research and life lessons. He has taught me how to look at problems from different perspectives, how to always come up with the best possible solutions, and how to deliver research results to different audiences effectively. He has been outstanding in providing insightful feedback and creating the balance between working and living. I am grateful to him for his constant advice on various aspects of a Ph.D. student's life, both inside and outside academia. He has not only advised me on technical issues but also given me many lessons in dealing with problems in life. Without his critical comments, suggestions and encouragement, none of my work would have been possible.

My special thanks to Data61-CSIRO for offering me the Ph.D. and Top-up Scholarships, to the University of Technology Sydney (UTS) for offering me the International Research Scholarship (IRS). I am also grateful to Professor Aruna Seneviratne in Data61-CSIRO for his support during my Ph.D. He has always been very encouraging and a continuous source of support and encouragement. I am grateful for his constant guidance and invaluable intellectual insight, and thankful to him for introducing me to great researchers and colleagues at Data61. I wish to thank the School of Electrical and Data Engineering, the Vice-Chancellor's Postgraduate Research Students Conference Fund at UTS and the Networks Research Group at Data61-CSIRO for providing me funding for attending international conferences.

I would also like to thank Dr. Diep Nguyen for his valuable feedback, discussions, and comments on my work on "Binary Initial Trust Establishment Model for Personal Space IoT systems," which is part of this thesis.

I wish to thank my colleagues and friends, who have influenced my views and efforts during my time here at UTS and Data61, including Chau Nguyen, Sara Farahmandian, Ngoc Le, Kathick Thiyagarajan, Ashish Nanda, Prashanthi Jayawardhane, Suranga

Seneviratne, Mosarrat Jahan, Harini Kolamunna, Rahat Masood, and Sara Khalifa. I would also like to thank all my wonderful friends inside and outside UTS and Data61 for bringing happiness and wisdom to my life.

Finally, I would like to thank my parents, my sisters and my brothers for their love and support during these years. My parents have made many sacrifices for me and have provided me with steady guidance and encouragement. This dissertation is dedicated to them.

Sydney, January 2019.

The Author's Publications

International Conference Publications and Proceedings:

- **Tham Nguyen**, Doan Hoang, Aruna Seneviratne, "Challenge-Response Trust Assessment Model for Personal Space IoT," in Proc. of *the 2016 IEEE International Conference on Pervasive Computing and Communications Workshops* (PerCom 2016), Sydney, Australia, 2016, pp. 1-6.
- **Tham Nguyen**, Doan Hoang, Diep Nguyen, Aruna Seneviratne, "Initial Trust Establishment for Personal Space IoT Systems," in Proc. of *the 2017 IEEE International Conference on Computer Communications Workshops* (INFOCOM 2017), Atlanta, USA, 2017, pp. 846-851.
- **Tham Nguyen**, Doan Hoang, Aruna Seneviratne, "Dirichlet-based Initial Trust Establishment for Personal Space IoT Systems," in Proc. of the *2018 IEEE International Conference on Communications* (ICC 2018), Kansas City, MO, USA, 2018, pp. 1-6. ERA: B
- **Tham Nguyen**, Doan Hoang, Aruna Seneviratne, "Exploring Challenge-Response Mechanism Designs for IoT Initial Trust Establishment," in Proc. of *the 2018 IEEE International Conference on Communications Workshops* (ICC 2018), Kansas City, MO, USA, 2018, pp. 1-6. ERA: B

Journal papers:

- **Tham Nguyen**, Doan Hoang, Aruna Seneviratne, "Information Design for Challenge-Response-based Initial Trust Establishment for Personal Space IoT Systems," submitted to *IEEE Transactions on Information Forensics and Security*. (Under Review) IF: 4.332 (2016)
- **Tham Nguyen**, Doan Hoang, Aruna Seneviratne, "Initial Trust-aware BLE Protocol for Personal Space IoT Systems," submitted to *IEEE Transactions on Mobile Computing*. (Under Review) IF: 3.822 (2016)

- Suranga Seneviratne, Yining Hu, **Tham Nguyen**, Guohao Lan, Sara Khalifa, Kanchana Thilakarathna, Mahbub Hassan, Aruna Seneviratne, "A Survey of Wearable Devices and Challenges," *IEEE Communications Surveys & Tutorials,* vol. 19, pp. 2573-2620, 2017. IF: 20.230 (2017)

Table of Contents

List of Figures

List of Tables

List of Abbreviations and Acronyms

6LoWPAN	Internet Protocol v6 & Low-power Wireless Personal Area Network
BLE	Bluetooth Low Energy
CA	Certificate Authority
CIA	Confidentiality, Integrity, Availability
CPU	Central Processing Unit
CRC	Cyclic Redundancy Check
CSRK	Connection Signature Resolving Key
DDoS	Distributed Denial of Service
ECG	Electrocardiography
EEG	Electroencephalography
EPC	Electronic Product Code
EV	Electric Vehicle
FPGA	Field-Programmable Gate Array
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IFS	Interframe Space
IoT	Internet of Things
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
IRK	Identity Resolving Key
ITU	International Telecommunication Union
LL	Link Layer
LTK	Long Term Key
MAC	Media Access Control
MANET	Mobile Adhoc Network
MIC	Message Integrity Check
MIT	Massachusetts Institute of Technology

NFC	Near-field communication
NIST	National Institute of Standards and Technology
OMNet++	Objective Modular Network Testbed in C++
OS	Operating System
P&G	Procter & Gamble
P2P	Peer-to-Peer
PDF	Probability Density Function
PDU	Protocol Data Unit
PKI	Public Key Infrastructure
QoS	Quality of Service
RFID	Radio Frequency Identification
SoA	Service-oriented Architecture
SoC	System on Chip
STK	Short Term Key
TK	Temporary Key
UML	Unified Modelling Language
UPC	Universal Product Code
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
UUID	Universally Unique Identifier
UWB	Ultra-wideband
VANET	Vehicular Adhoc Networks

Abstract

Internet of Things (IoT) is becoming a reality with innovative applications, and IoT platforms have been developed to transfer technologies from research to business solutions. With IoT applications, we have greater control over personal devices and achieve more insights into the resource consumption habits; business processes can be streamlined; people are also better connected to each other. Despite the benefits derived from the IoT systems, users are concerned about the trustworthiness of their collected data and offered services. Security controls can prevent user's data from being compromised during transmission, storage or unauthorized access, but do not provide a guarantee against the misbehaved devices that report incorrect information and poor services or avoid conducting a common task. Establishing trust relationship among devices and continuously monitoring their trust is the key to guarantee a reliable IoT system and hence mitigate user's concerns.

In this dissertation, we propose and investigate a novel initial trust establishment architecture for personal space IoT systems. In the initial trust establishment architecture, we propose a *trust evidence generation module* based on a challenge-response mechanism to generate the trust evidence relying on the device's responses to the challenges, a *trust knowledge assessment module* to obtain the knowledge about the device from the generated trust evidence, and a *trust evaluation scheme* to quantify the initial trust level of the devices. We design and investigate a *challenge-response information design* to determine feasible designs of the challenge-response mechanism that ensure meaningful and related trust knowledge about the device's trustworthiness captured from the challenge-response operations. A *new trust-aware communication protocol* is designed and implemented by incorporating the proposed initial trust establishment architecture into existing Bluetooth Low Energy (BLE) protocol to demonstrate the feasibility and efficiency of the proposed initial trust establishment architecture in practice.

In this work, we first study building blocks and possible architectures of the IoT and analyze key requirements of an IoT system. Based on the analysis, we identify the critical role of the initial trust establishment model and the challenges of establishing initial trust in IoT systems due to the lack of knowledge for the trust assessment to work. To address

the challenges, we propose a novel initial trust establishment architecture that can generate trust evidence for assessing the initial trust level of new devices by conducting challenge-response operations within a limited time window before they are admitted to the system.

We propose three new initial trust establishment models based on the proposed architecture. An implicit relationship between the responses and the challenges is assumed for the system to judge the initial trustworthiness of the devices. The first model assesses the initial trust value based on a probability associated with the device's behavior captured from the challenge-response process. The second model investigates the initial trust value based on a binary outcome set, and the third model quantifies the initial trust level based on a multiple-component outcome set from the challenge-response process.

Subsequently, we propose the challenge-response information design where the challenge-response process is investigated and designed to determine the information space of the challenger's view on its environment so that the challenge can invite relevant responses from the target environment. Based on the design of the challenge-response mechanism, the system can capture meaningful trust knowledge about the devices from challenge-response operations at their admission phase. We finally design and implement the initial trust-aware BLE protocol which incorporates the proposed initial trust establishment architecture into the existing BLE protocol. The simulation results show the efficiency, feasibility, and dependability of using initial trust-aware BLE protocol for building a trustworthy personal space IoT systems.

The novelty of this research lies in assessing the devices' initial trust level within a limited time window, before their admission to the personal space IoT system, without requiring prior experience or recommendations. The major contribution of this thesis is that it helps the IoT business solution providers to build secure and trustworthy IoT systems by admitting dependable devices, monitoring the trust of admitted devices, detecting maligned devices, and building long-term trust among. As a result, it mitigates the user's concerns about the trustworthiness of IoT systems and encourages broader adoption of IoT applications.

Chapter 1
Introduction

Internet of Things (IoT) is becoming a reality with innovative applications, and IoT platforms have been developed to transfer technologies from research to business solutions. The IoT brings automation and network-connected features to all facilities in our daily lives from smart appliances to smart healthcare systems, smart energy systems to smart transportation, smart cities, for example. IoT devices can sense, process and communicate sensing information and take actions and make decisions on behalf of the user over the operations of the IoT systems. In an IoT system, there is much heterogeneity among devices. Moreover, many of them have limited computational capacity and hence do not support complex security and trust control methods. Therefore, those devices are vulnerable to various attacks that open the door to many breaches of the whole system. Specifically, the IoT devices might be compromised to provide fake data that leads to inaccurate or even dangerous actions or be misbehaved by cooperating with others to provide poor and unreliable services.

It is noted that security control approaches can prevent the data from being modified, intercepted or unauthorizedly accessed. However, they do not provide a mechanism to monitor devices' behavior and detect the misbehaved, compromised and untrustworthy devices. Thus, IoT systems can be protected from some security attacks, but their collected data and provided services still cannot be trusted. Our critical infrastructures can also be damaged due to the intimate integration of untrustworthy and invaded IoT devices.

The trustworthiness of IoT devices is the basis of the cooperation and collaboration among them in the IoT systems which directly provide the reliability of their collected data and offered services. Without the devices' trustworthiness, their collected data might

not be trusted, and their provided IoT applications and services might not be reliably created. Therefore, an IoT system must verify the trust of its devices and continuously monitor every device from the time it is admitted into the system until the end of its lifecycle to ensure the trustworthiness of the device and its data and offered services. Importantly, an initial trust assessment that is conducted at the device admission phase could allow the IoT systems to admit trustworthy devices into the system while reducing the risks of attacks performed by misbehaved or compromised devices. Hence, initial trust establishment plays a crucial role in ensuring a reliable IoT system.

A number of studies have attempted to formalize the role of trust and propose trust management models for IoT. The existing proposed trust management models for IoT primarily provide approaches to observe the devices' trustworthiness and detect maligned devices once they have joined the IoT systems. In addition, these existing models require prior trust information such as historical experience or third-party recommendations as the basis for the trust assessment. For the initial trust establishment, the required prior trust resources for current trust management models are not available when the devices encounter the system for the first time, or the previous trust assessment might be no longer valid when the devices wish to rejoin the system after some absence periods. Moreover, the initial trust establishment is required to be conducted within a limited time window so that it does not significantly impact on the delay in the device admission of the IoT systems. Due to the lack of prior trust resources and the limited time window for the device admission phase, the existing trust management models are not applicable to the initial trust establishment.

In summary, it is challenging to quantify the initial trust level of devices and establish the trust relationship between the IoT system and the devices for admitting potential devices into the system under the time limitation. To our best knowledge, no previous work proposes an initial trust establishment model for an IoT system. In this thesis, we focus on proposing approaches to quantify the initial trust level of devices that are joining the IoT system and establish the initial trust relationship between the system and the devices before they are admitted to the systems to ensure the trustworthiness of admitted devices and hence guarantee their provided data and services worthiness.

This chapter is organized as follows. Section 1.1 briefly defines the critical role of trust in the Internet of Things. Section 1.2 outlines the research problem addressed by this thesis. Section 1.3 states the research motivation. Section 1.4 presents the research aim and objectives. Section 1.5 summaries the main contributions of the research in this thesis. Section 1.6 illustrates the research model and methodology. Finally, section 1.7 provides the structure of this thesis.

1.1 Defining Trust in the Internet of Things

As the research focuses on the initial trust establishment in IoT systems, in this section we provide the definition of trust, its properties and its role in the IoT.

- **Trust definition**

Trust is an essential attribute in building a relationship between entities. Generally, trust refers to a relationship in which an entity, often called the *trustor*, relies on someone or something, called the *trustee*, based on a *given criterion* [1]. It is perceived as the basis for decision making in many contexts and the motivation for maintaining long-term relationships based on cooperation and collaboration [1].

Trust has been studied for a long time by scientists in different disciplines from sociology, economics, psychology, automation to computing and networking [2]. However, the notion of trust has not been formally defined [3]. To human-beings, trust is a means for people to deal with the uncertainty about their partners' behavior and interactions. In computer science, the trust concept has been related to various areas such as security and access control in computer networks, reliability in distributed systems, game theory and agent systems, and policies for decision making under uncertainty.

Trust definition in different communities varies in how it is represented, computed and used [4, 5]. According to [4], trust is defined as the extent to which one party is willing to participate in a given action with a given partner, considering the risks and incentives involved. Understanding the notion of trust and its properties are the key to model trust properly in a specific discipline.

- **Properties of trust**

Subjective: it is the inherent nature of trust since evidence for the trust assessment may be uncertain, incomplete, and conflicting. It refers to the trust estimated based on local, uncertain, and incomplete evidence [1].

Dynamic: the trust of an agent on another agent can change dynamically. Trust evolves based on the types of experiences or the number of interactions, decays over time and is updated upon the arrival of new evidence [6-8].

Asymmetric: for two agents involved in a relationship, trust is not necessarily identical in both directions. This property can be affected by the difference in the agent's knowledge bases, experiences, and history [9].

Incomplete transitive: trust is not perfectly transitive in the mathematical sense [10] Moreover, trust is weakened or diluted by transitivity [11]. Although trust cannot be completely transitive, it can be easily transferred from one context to another context. For example, trust in personal relationships can be transferred to business relationships [1].

Context-dependent: it is a critical factor to estimate trust in a given context. For example, Alice trusts Bob to repair her car, but she does not trust Bob to revise her research article.

It can be seen that trust is a very complicated concept that is influenced by many measurable and non-measurable properties. It refers to the confidence, belief, and expectation on the reliability, integrity, security, dependability, and the ability of an entity [12]. It highly relates to security since ensuring system security and user safety is a necessity to build a trustworthy system. It concerns not only security but also many other factors, such as goodness, strength, reliability, availability, and ability [12]. Thus, it is complicated and challenging to establish, assess, and manage the trust.

- **Trust in the Internet of Things**

The Internet of Things (IoT) is a collection of billions of physical objects or "things" embedded with electronics, software, sensors, and connectivity to enable objects to collect and exchange data based on a variety of communication infrastructures. An IoT device is a connectivity-enabled and smart unit that is designed to do a task automatically and intelligently. It can be a very tiny and simple device or a big and complicated device that can be used in a small or an extensive system. With its ability to sense and control

objects, IoT creates opportunities for more direct integration between the physical world and computer-based systems. IoT brings potentially tremendous benefits to our life in many application sectors such as home automation, environmental monitoring, health and lifestyle, smart cities [13]. Today, we are witnessing the value and potential impact of the IoT on our daily lives. Within a few years, we expect a huge transition to the IoT. By 2020, industry estimates that almost 30 billion devices will be interconnected to improve the quality of life [14].

Despite the benefits of innovative IoT applications, its continuous and pervasive data acquisition and control capabilities, the IoT systems raise many concerns about security, trust and privacy [15, 16]. Importantly, trust management plays a vital role in IoT for reliable data fusion and mining, high-quality services with context-awareness, and preserving information security. Based on trust, users can overcome the perceptions of uncertainty and risk when using IoT services and applications [12]. While a considerable volume of research related to security and privacy in IoT has been investigated [17, 18], research on trust in the IoT is still in its early stages. Recently, attempts on addressing trust issues in IoT have been increased [12, 19].

In a trustworthy IoT system, the devices must cooperate with others so that the operations of the system are smooth and conducted adequately. In this thesis, we accept the definition of trust in the IoT as the confidence of the system on the devices from their admission to the system until they cease working in the system to ensure the trustworthiness of devices and their provided data and services.

1.2 Research Problem

Together with the fast growing of IoT applications in various domains, attacks that target resource-constrained IoT devices have multiplied over the last years [20]. For example, in November 2016, cybercriminals disabled the heating of two buildings in a city in Finland where temperatures at that time of year are below freezing. This was a Distributed Denial of Service (DDoS) attack where the attack managed to cause the heating controllers to continually reboot the heating systems until they eventually stopped functioning altogether [21]. In smart transportation systems which rely on sensor readings

to continuously provide transportation-assistant information, a known death caused by a self-driving car was disclosed by Tesla Motors [22]. The reason is that a car's sensor failed to distinguish a large white 18-wheel truck and trailer crossing the highway. It can see from these two recent issues that the information that sensors provided to a self-driving car's transport-assistant system and the commands to take actions of the heating controller were inaccurate and that brought danger to life.

The question is on what basis that we can rely the data and services provided by IoT devices and let them take actions automatically on our behalf. Security controls cannot guarantee the trustworthiness of the data and services provided by the IoT systems. Therefore, besides security, there is growing concerns about the trust in IoT. In fact, the IoT systems rely on cooperation and collaboration among devices to provide the desired services to the user. Trust has increasingly been recognized as a crucial factor in enhancing the security of IoT systems and guaranteeing the reliability of innovative IoT services and applications [15, 16, 23]. Without a trust management model in the system, security alone cannot guarantee the provided data and services worthiness in IoT systems.

To ensure a trustworthy IoT system, the devices' behavior must be assessed to monitor their trustworthiness and cooperativeness throughout the system's lifecycle. Importantly, the initial trust establishment plays a crucial role to build a trustworthy IoT system by assessing the devices' trustworthiness before they are admitted to the system. Currently, most proposed trust management models [24-26] monitor the integrity of entities by reactively detecting the misbehaved and maligned entities that have been admitted to the system. In addition, the proposed trust assessment methods primarily rely on information recorded through historical observations or trusted recommendations.

In real situations when the devices encounter the system for the first time, there is no historical observation available that the system can rely on to assess the initial trust level on the devices. In many situations especially in the less secure wireless environment, there is a lack of trusted recommendations that the system can utilize. In equally realistic conditions when a device had left the system for some periods due to some interruptions, the historical experience about the device is less reliable or no longer valid on its return. Thus, the IoT system cannot rely on those trust information resources to evaluate the

initial trust. As a result, it is crucial that the IoT system must be able to generate the trust information to establish the initial trust level of a device at its admission to the system.

The problem addressed in this thesis can be stated as follows.

"On what basis and how can an IoT system quantify the initial trust it places on its potential members when they encounter the system for the first time or rejoin the system after an absent period to ensure the trustworthiness of the system's components, data, and services?"

To address the stated problem, we investigate the following issues.

- **On what basis should an IoT system rely to make an initial judgment on the trustworthiness of the devices that want to join the system?**

An initial trust establishment model allows the IoT systems to judge the trustworthiness of the devices before admitting them into the system. However, in the initial trust assessment, the prior trust resources such as historical experience and recommendations are usually not available. Thus, the system must be able to generate the trust knowledge for the initial trust establishment model to work. As the basis for the system to rely on to judge its initial trustworthiness, the generated trust knowledge should capture and reflect the device's behavior accurately during the first encounter between the device and the system.

- **How can the trust knowledge for the initial trust establishment model be generated?**

The IoT system can conduct a challenge-response process during the first encounter between the device and the system to generate the trust knowledge by capturing the device's behavior from its response to the challenges. A trust knowledge assessment module is needed to assess the trust evidence generated from the challenge-response process to gain such trust knowledge about the device.

- **How can we design an information relationship between the system and the devices and build it into the challenge-response process so that meaningful knowledge about the devices' trustworthiness can be generated?**

The goal of creating the trust knowledge about the potential devices is to provide relevant and meaningful information for the initial trust establishment model to work. Specifically, the challenges must be carefully designed in such a way that they are related

to the environment and invite relevant responses from the devices. Moreover, there must be shared information between the challenges and the devices' responses for the trust assessment to judge the device's trustworthiness. Without such information sharing, very little knowledge about each other's trustworthiness can be gained from the challenge-response operations. Therefore, an information design of the challenge-response process is crucial for the initial trust establishment model to work.

- **How can the initial trust level be evaluated based on the generated initial trust knowledge?**

Clearly, current trust evaluation schemes cannot be directly applied to the initial trust establishment models as the required trust resources such as long-term experience and reliable recommendations are not available when the devices encounter the system for the first time or the devices reenter the environment after an absence period. Therefore, a novel trust evaluation scheme that can assess and obtain the meaningful initial trust knowledge based on the captured device's behavior during the challenge-response process to quantify the initial trust level is needed.

- **Can we design an effective protocol for realizing the initial trust establishment model in practice?**

The proposed initial trust establishment model relies on the trust knowledge gained from the challenge-response process between the system and the devices. The challenge-response process requires a mechanism to carry the challenge and response information. It can be done by utilizing possible interactions between two devices when they encounter each other. The communication protocol used by IoT devices usually provides several interactions for exchanging information to establish a connection. Therefore, conducting the challenge-response process over these interactions is practical. Designing and implementing a new protocol that incorporates our proposed model into an existing communication protocol and evaluating its performance are needed to demonstrate the feasibility and efficiency of the proposed solution in practice.

1.3 Research Motivation

The IoT affects many areas of our lives from personal services such as health-care, wearables to industry domains such as building and home automation, smart cities, smart manufacturing, automotive and precision agriculture. As IoT devices closely connect us to our personal and physical world by providing sensing information as well as taking actions on our behalf, their trustworthiness is of paramount importance in the IoT system. As a result, the trustworthiness of their collected data and provided services are becoming significant concerns when developing IoT business solutions.

The IoT systems rely solely on the cooperation of "things" to provide a service or complete a common task. The failure of one "thing" in the system due to its misbehavior or being compromised leads to a broken system. In a compromised IoT system, the collected data is inaccurate, and hence the provided services cannot be reliably created and that might tear down the system. In addition, sensitive data is easily accessed by unauthorized parties if "things" are compromised. Therefore, assessing and monitoring the trustworthiness of a "thing" from its admission phase over its lifecycle is crucial in the IoT systems. To do that, a robust and effective trust management model in the IoT system must assess the trustworthiness of devices right from its device admission phase over its operation to ensure the trustworthy IoT system and its reliable data and services.

Existing trust management models fail to assess the initial trust level of a device from its admission to the system because 1) prior trust resources are not available, 2) device is unknown to the system, and 3) device rejoins the system, and the prior trust assessment is no longer valid. We believe that to ensure the reliability of IoT services and the trustworthy collected data and prevent the systems from attacks deployed by misbehaving or compromised devices, a new initial trust establishment model is crucial in IoT. The initial trust establishment model could allow the IoT systems to establish the initial trust level on the potential devices before they can be admitted to the system. By doing so, the IoT system can reduce the risk of admitting maligned and misbehaved devices as they are judged by the system before being authenticated and granted permissions in the system.

In summary, an IoT system requires a trust management model to ensure the cooperation among devices for providing promised IoT applications. Importantly, the

initial trust establishment to assess and quantify the initial trust level of devices prior to their admission to the IoT systems is critical but has not been comprehensively investigated. This motivates us to conduct this research. Our research proposes an initial trust establishment architecture that allows the IoT systems to admit reliable and trustworthy devices into the system and hence provide trustworthy data and IoT services. The proposed initial trust establishment architecture can also be used as a new option for conventional trust management models to generate trust information during the trust observational phase where the previous trust resource is no longer valid.

1.4 Research Aim and Objectives

The primary focus of this thesis is to provide solutions to build trustworthy IoT systems so that they provide trusted data and offer reliable services and applications. We aim to create a secure and trustworthy IoT system by seeking an initial trust establishment architecture that allows the system to assess and quantify the initial trust level of devices before admitting or readmitting them to the system.

To achieve the research aim, the objectives of the thesis can be stated as follows.

1. Exploring issues and approaches related to the initial trust establishment in IoT and related areas.
2. Proposing a novel initial trust establishment architecture for the IoT systems and designing components of the proposed architecture.
3. Developing initial trust establishment models based on the proposed architecture that utilize different mathematical foundations to obtain the trust knowledge.
4. Designing the challenge-response mechanism to ensure that there always exists shared information between the system and the device in challenge-response operations that merit meaningful trust knowledge for the initial trust establishment models to assess the initial trust of the device.
5. Evaluating the feasibility and efficiency performance of the proposed initial trust establishment architecture.

The research focuses on the personal environment where the IoT systems are deployed in a personal space to provide services and applications to the user, i.e., the

owner of IoT devices or the person who wishes to use IoT devices that are available in his/her space. The personal space IoT environment will be defined in chapter 3.

1.5 Research Contribution

The study focuses on the initial trust establishment in personal space IoT systems. The wide usage of IoT technologies in all aspects of our daily lives has raised more concern on the trustworthy of IoT systems. Despite the critical contribution of the trust management model in the success of developing and deploying IoT systems, research on the trust management in IoT is relatively limited and in its early stage. This thesis conducts the research on the initial trust establishment model for the personal space IoT systems and makes a number of significant contributions:

1. A novel initial trust establishment architecture is proposed. The proposed initial trust establishment architecture allows the IoT systems to evaluate the trustworthiness of new devices or re-evaluate the trustworthiness of devices that wish to rejoin the system after interruptions before their admission to the system. The novelty of this initial trust establishment architecture is that it does not require historical interactions or recommendations for the trust assessment to work that are usually demanded by existing trust management models and are not available at the first encounter between the device and the system or no longer valid as the device has been absent from the system.
2. For the initial trust establishment architecture to work in the different environment and IoT settings, three new initial trust establishment models are introduced based on the proposed architecture. Each initial trust establishment model assesses the trust knowledge via information entropy and a mathematical foundation that cover different circumstances so that the IoT system can choose a suitable model for its application and preference.
3. An information design of the challenge-response process is proposed. The novelty of the design of the challenge-response process is that it investigates the information space of the challenger's view on its environment so that the challenge can invite relevant responses from the target environment. It can

engineer implicit shared information between the challenge and the device's response in any challenge-response operation, and thus provide meaningful trust knowledge for the initial trust establishment models to judge the device's trustworthiness.

4. The experimental results generated on extensive simulations demonstrate the feasibility of the proposed initial trust establishment models for the system not only to initially judge the trustworthiness of devices before they are admitted to the system but also to reevaluate the trust level of admitted devices and monitor their behavior throughout their lifecycle.
5. A new initial trust-aware BLE protocol is designed and implemented by incorporating the proposed initial trust establishment architecture and its challenge-response information design into the existing Bluetooth Low Energy (BLE) protocol demonstrating the practicability of the research outcomes presented in this thesis. The trust-aware feature provided by the initial trust-aware BLE protocol contributes to the development of the Bluetooth specification by enhancing its security and trust controls and expanding its usage in IoT systems.

In summary, this thesis contributes to the development of the trust management approaches in deploying trustworthy IoT systems. It provides new initial trust establishment models that allow the IoT systems to quantify the initial trust level of elements and admit trustworthy elements into the system without requiring prior knowledge such as historical experience or recommendations. The challenge-response process and its information design can also be used for conventional trust assessment models in the operational phase of IoT systems to observe their member's trustworthiness where the required trust resources have been invalid. The proposed initial trust establishment models can help the IoT solution providers to encourage the broader use of their solutions as they ensure the data and services worthiness provided by IoT systems.

1.6 Research Model and Methodology

Figure 1.1 illustrates the research model and methodology of this research. The research strategy consists of three main stages: problem definition, developing new

approaches and practical realization [27]. The thesis starts with defining the research problem. We determine research questions behind the described problem and hypotheses to answer the research questions. We then review current approaches related to the stated problems, analyze the proposed solutions to examine their feasibility to solve the issues stated. Based on the background and related work, we define the research scope, identify requirements that new approaches must meet to solve the research problem and determine objectives that the research has to achieve to address the problem. According to research objectives and defined requirements, we create a new proposal and design to satisfy the requirements and fulfill the research objectives. Specifically, we propose a new initial trust establishment architecture and design three different trust assessment models based on this architecture. We realize the proposed initial trust assessment models according to the proposal and evaluate their performance. We then validate the proposed initial trust establishment model by designing and implementing a new initial trust-aware BLE protocol that incorporates the proposed solutions into the existing BLE protocol. Finally, we evaluate the efficiency performance of the implemented initial trust-aware BLE protocol.

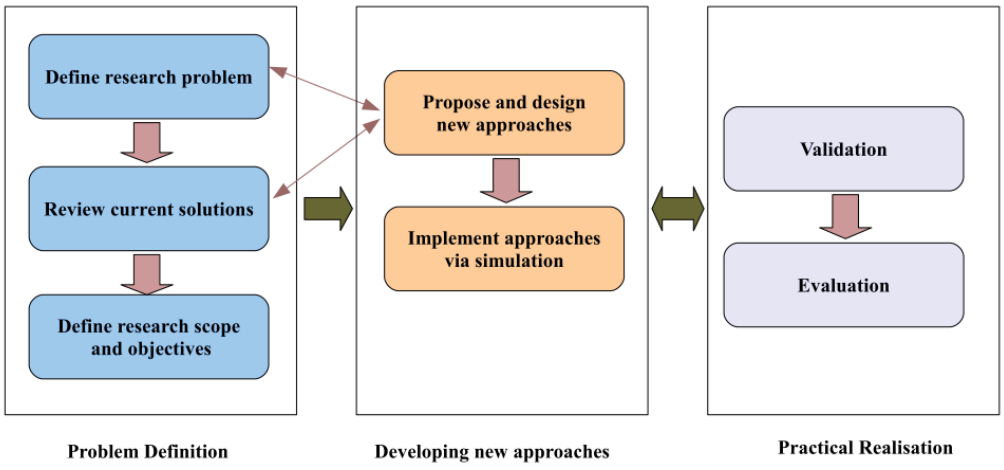


Figure 1.1 Research model and methodology

1.7 Structure of the Thesis

This research has produced four published international conference papers and two under-review journal papers. The thesis is organized into nine chapters as follows.

Chapter 1 is an introductory chapter that presents an overview of the study. It first provides the introduction of trust in the Internet of Things. It then states the research problem in establishing the initial trust in IoT systems which inspired our research motivation. The research aims and objectives, research contribution and research model and methodology are presented in the chapter.

Chapter 2 provides the background of the Internet of Things (IoT), trust management in IoT, and related work that has been investigated relative to the initial trust establishment in IoT. Then, the relevant parts of the existing Bluetooth Low Energy protocol in relation to the initial trust-aware BLE protocol proposed in the thesis are presented in this chapter. The related mathematical background is also provided to better understand the proposed initial trust establishment model in this thesis.

Chapter 3 introduces a new definition of an IoT environment – *the personal space IoT* and discusses the importance of establishing initial trust in a personal space IoT system. It then introduces a systematic overview of the proposed initial trust establishment architecture in the personal space IoT context. We present the overall architecture of our proposed initial trust establishment for the personal space IoT system and the functionality of each component. The realization of the proposed initial trust establishment model over the existing communication protocol for IoT system is discussed in the chapter.

Chapter 4 presents a new probability-based initial trust establishment model for personal space IoT systems where we assess the trust knowledge about the device based on a probability associated with the uncertainty that the system has about the device's behavior. This probability is estimated based on the evidence captured from the challenge-response process. This is the first initial trust establishment model based on our proposed initial trust establishment architecture for personal space IoT systems.

Chapter 5 introduces a binary initial trust establishment model that employs the advances of probability distribution and the Bayesian inference approach. This model focuses on the binary trust evidence generated by a challenge-response process during the first encounter between the device and the personal space IoT system.

Chapter 6 presents a multilevel initial trust establishment model for the personal space IoT systems which utilizes the Bayesian inference adopting Dirichlet distribution as the

mathematical foundation to assess the initial trust knowledge. This model investigates more realistic trust evidence where the satisfaction level that the device's responses are assigned by the system is considered. The initial trust evidence learned from the challenge-response process is based on a multiple-outcomes set.

Chapter 7 presents the information design of the challenge-response process for initial trust establishment in personal space IoT systems. This chapter investigates the feasible designs of the challenge-response process so that it ensures the initial trust establishment works appropriately. By carefully designing the information content of challenges and the underlying relationship between challenges and responses, our information designs of the challenge-response process provide effective means for the trust evidence generation to create meaningful and relevant evidence for the initial trust establishment.

Chapter 8 demonstrates the feasibility of our proposed initial trust establishment in practice. We design and implement a new initial trust-aware BLE protocol which incorporates the proposed initial trust establishment model into the existing Bluetooth Low Energy protocol. The chapter first describes the protocol design and implementation detail of the initial trust-aware BLE protocol. We then evaluate the performance of the initial trust-aware BLE protocol regarding the investigation of the initial trust value and the efficiency performance in protocol processing delay and communication overhead.

Chapter 9 summarizes the ideas presented in this thesis, the major contributions of this research, and future research work.

Chapter 2

Background and Related work

In this chapter, we first present the background of the Internet of Things (IoT) and the trust management in IoT. The background covers the architecture, building blocks, and the requirements of an IoT system. We then review existing initial trust establishment approaches. We explore existing trust computation methods that are related to our proposed approaches in this thesis. The initial trust establishment model proposed in this thesis will be realized and implemented over an existing communication protocol. Bluetooth Low Energy (BLE) protocol is used as a framework for realizing our proposed solutions. Therefore, we give a brief overview of the BLE protocol and its trust consideration feature. Finally, we provide the related mathematical foundation including information entropy, Bayesian inference, Beta distribution and Dirichlet distribution to quantify trust level in the proposed initial trust establishment model in this thesis.

The structure of this chapter is as follows. Sections 2.1 gives an overview of the Internet of Things which focuses on the definitions, architectures, building blocks, and requirements of the IoT systems. The section emphasizes the importance of trust management in IoT. Section 2.2 reviews the existing initial trust establishment approaches and points out their limitations. Section 2.3 explores existing trust computation schemes in IoT and other related areas. Section 2.4 briefly introduces portions of the BLE protocol that are relevant to the implementation of our proposed solutions. Section 2.5 provides the mathematical background for our proposed initial trust establishment model. Section 2.6 concludes the chapter.

2.1 Internet of Things

The chapter begins by providing the history of the Internet of Things concept. In 1999, Kevin Ashton, the co-founder and executive director of the Auto-ID Center at the Massachusetts Institute of Technology (MIT), coined the term 'the Internet of Things' as a title of his presentation made at Procter & Gamble (P&G) to promote the RFID technology. The Auto-ID center used the term "Internet of Things" in 2000 and promoted the concepts and ideas of a connected world with the Electronic Product Code (EPC) system as the basis of how things are connected to the Internet [28]. The phrase Internet of Things became popular in 2011. It appeared as a newly emerging phenomenon of Gartner's list – a market research company and became the theme of Europe's most significant and longest-running technology conference – Leweb. The IoT reached the mass market in early 2014.

During recent years, the Internet of Things (IoT) has attracted significant attention in both academia and industry, and a lot of progress has been made. However, there is a variety of IoT definitions provided by different organizations and individuals [13, 29, 30]. For example, the Institute of Electrical and Electronics Engineers (IEEE) IoT Initiative established a baseline definition of IoT in the context of various applications from small, localized systems to an extensive global system. IEEE described the Internet of Things as "*A network of items – each embedded with sensors – which are connected to the Internet.*"

A study group of International Telecommunication Union (ITU), ITU-T, has defined IoT as "*A global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies.*"

Internet Engineering Task Force (IETF) provides its own description of the Internet of Things as "*The basic idea is that IoT will connect objects around us (electronic, electrical, non-electrical) to provide seamless communication and contextual services provided by them. Development of RFID tags, sensors, actuators, mobile phones makes it possible to materialize IoT which interact and co-operate with each other to make the service better and accessible anytime, from anywhere*."

A crucial component of the IoT are objects that get connected to it, or simply "things." Generally, things in IoT can be anything that has connectivity capability such as simple RFIDs attached tags to smart thermostats installed in buildings, medical devices implanted on or carried by patients to auto devices with built-in sensors. IETF defined "things" in the IoT as "*In the vision of IoT, 'things' are very various such as computers, sensors, people, actuators, refrigerators, TVs, vehicles, mobile phones, clothes, food, medicines, books, etc. These things are classified into three scopes: people, machine (for example, sensor, actuator, etc.) and information (for example, clothes, food, medicine, books, etc.). These 'things' should be identified at least by one unique way of identification for the capability of addressing and communicating with each other and verifying their identities. In here, if the 'thing' is identified, we call it the 'object.*"

Although many definitions have been stated for the Internet of Things, they generally identify the following features of the IoT [28].

- **Interconnection of Things:** IoT is a system that deals with the interconnection of "Things."
- **The connection of Things to the Internet:** In an IoT system, "things" are connected to the Internet.
- **Uniquely identifiable Things:** An IoT system is composed of uniquely recognizable Things.
- **Ubiquity:** It is a major feature of an IoT system, indicating a network which is available anywhere and anytime.
- **Sensing/actuation capability:** The sensors/actuators are connected to the "Things" and perform the sensing/actuation.
- **Embedded intelligence:** Objects in IoT are smart and dynamic with emergent behavior, embedded intelligence, and knowledge functions.
- **Self-configurable:** Due to the heterogeneity of devices the natural direction for IoT devices is to manage themselves in terms of software/hardware configuration and resource utilization. Self-configuration primarily involves the actions of device and service discovery, network organization and resource provisioning.

- **Programmability:** The "things" in IoT are programmable objects. A programmable device can take on a variety of behaviors at a user's command without requiring physical changes.

2.1.1 Building Blocks of the Internet of Things

Understanding the building blocks of the IoT helps us to gain a better insight into the features and functionalities of each component in the IoT. Based on that knowledge we can identify the problems related to trust management in an IoT system [31]. In this section, we provide an overview of the IoT building blocks.

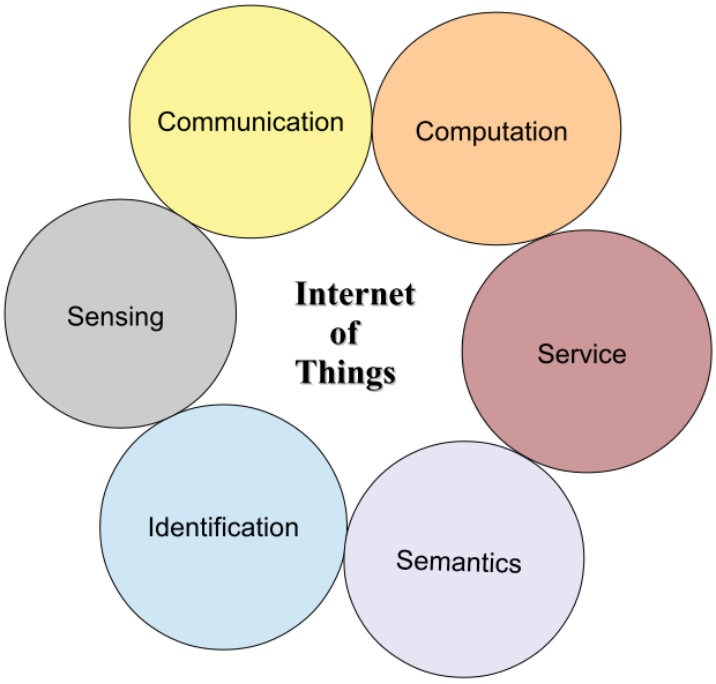


Figure 2.1 Building blocks of the Internet of Things

The work in [32] provided a comprehensive analysis of the building blocks of the IoT. The IoT should be capable of interconnecting billions of various objects and allowing them to collaborate with each other to provide emerging applications. In order to deliver the functionalities of an IoT system, there are six main blocks to build a comprehensive IoT system as illustrated in **Figure 2.1**. Following is the brief explanation of each building block of the IoT system [32].

- **Identification**

Identification techniques provide a means for the IoT to name and match services with their demand. They also enable the IoT objects to differentiate from other objects. There are three identification groups regarding which layer in the IoT architecture is considered [31]. First, object identifiers are used for uniquely identifying physical or virtual objects. Some examples of the object identifier are EPC, UPC, UUID, ubiquitous Code, MAC address. Second, communication identifiers are used to identify devices in communication range of others. IPv4, IPv6, 6LoWPAN [33] are some examples of communication identifiers. Third, application identifiers such as URIs, URL are used to identify uniquely applications and services used in the scope of IoT applications.

- **Sensing**

The sensing provides the capability to gather data within the network and send it back to the database of IoT objects such as sensors, actuators, and wearable sensing devices. IoT devices can sense/monitor the surrounding environment, gather data and make it ready for communicating within the IoT network or with the external network. Typically, these devices connect to a central management portal to provide requested data [32].

- **Communication**

The communication technologies in the IoT systems are responsible for connecting heterogeneous objects so that the systems can offer desired services. The communication technologies for the IoT can be from an ultra-short range communication protocol such as RFID, NFC, to a short-range communication protocol such as Bluetooth and UWB and to a long-range communication protocol such as WiFi, cellular. For example, RFID technology is usually used for shipping, supplying IoT related applications [34]. Bluetooth version 4.2 provides Bluetooth Low Energy (BLE), high-speed and IP connectivity to support IoT applications [35]. BLE has been demonstrated to be more efficient in terms of energy consumption compared to other short-range communication technologies such as Zigbee [36]. WiFi enables smart devices to communicate and exchange information in ad-hoc configurations. It has been used in many IoT systems such as a home security surveillance system which utilizes its advances in high data rate, supports long distance [37] or low-cost and in-home IoT appliances [38].

- **Computation**

The computation block acts as the *brain* of the IoT system. It is served by processing units such as microcontrollers, microprocessor, SoC, FPGA and software applications. Many hardware platforms have been developed to run the IoT applications such as Arduino, Intel Galileo, Raspberry PI, UDOO, Friendly ARM, Gadgeteer. A number of software platforms are utilized to provide IoT functionalities. The Contiki [39] real-time operating system with its simulator called Cooja has been used widely in IoT scenarios whereas TinyOS [40], and LiteOS [41] provide light-weight OS for IoT environments. Furthermore, cloud platforms play another crucial computational part of the IoT which allows the smart objects to send data to the cloud so the data processing is conducted in real-time.

- **Service**

There are four classes of IoT services: identity-related services, information aggregation services, collaborative-aware services and ubiquitous services. The identity-related services are essential services as they are utilized in other service types. The information aggregation services collect raw data, i.e., sensory measurements and report them to the IoT application. The collaborative-aware services utilize the obtained data from the information aggregation services for decision making and reacting corresponding to the data. The ubiquitous services provide facilities anytime and anywhere they are needed for anyone who needs them. Most of the existing IoT applications offer the identity-related services, the information aggregation services, and the collaborative-aware services [32].

The IoT brings a lot of innovative applications in many areas of our lives. Specifically, in the building and home automation sector a wide range of innovative IoT applications are developed for controlling smart homes such as connected appliances, light control, smart thermostat, wireless environmental sensor [42]. In the smart city sector, a variety of systems are interconnected to provide desired services such as health, utilities, transportation, government and buildings [32]. In the smart manufacturing sector [43], IoT products can be in robotics [44], CPU, industry 4.0 [45], a portable monitor. In the industrial automation sector [46], IoT can provide services in a modern automobile such as engine management, infotainment, EV charging stations. In the wearables sector [47], efficient ultra-low power solutions for the wearables become a reality such as

augmented reality and entertainment, location and tracking, wearable fitness. In the healthcare sector [48], IoT products and applications are provided to improve the quality and accessibility of digital products for health and fitness industries such as telehealth gateway and aggregation, wireless patient monitor, electroencephalography (EEG), electrocardiography (ECG)-based transceiver [49]. In the precision agriculture sector [50-53], IoT products can be a power converter and provider of charging for agricultural equipment, drones, and sensors for agricultural equipment [54].

- **Semantics**

Semantics in the IoT means the ability to extract knowledge by using different machines to provide the desired services. Extracting knowledge consists of resource discovery, resource utilization, and information modeling. Moreover, it also includes data recognition and data analysis data to provide the required services.

2.1.2 IoT Architectures

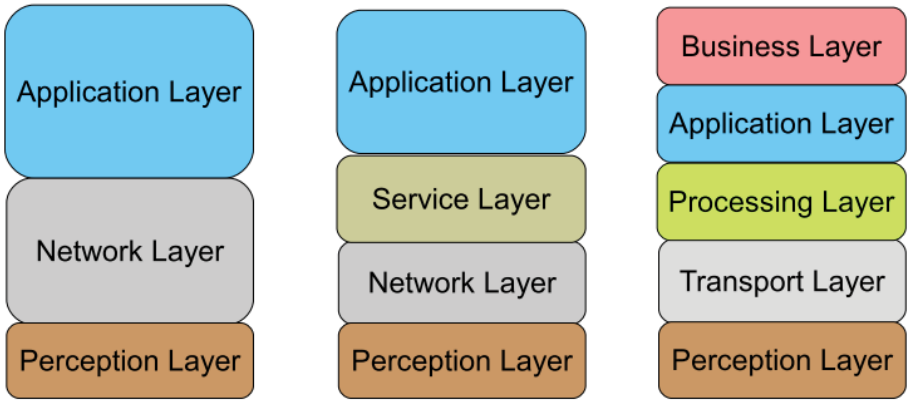
The definition of IoT implies the interconnection of billions of various objects through the Internet and the provision of promising applications. However, this entails strict requirements on the trust and the security of the infrastructure and its components.

There are a number of architectures proposed for IoT [55-57]. In the literature, the basic IoT architecture is a three-layer architecture that includes the Perception Layer, Network Layer and Application Layer [58, 59]. Some other proposed models add more abstraction to the IoT architecture such as middleware-based model, SOA-based model or five-layer model [58, 60, 61].

- **Three-layer architecture**

The three-layer architecture has been designed and realized in a number of IoT systems. Generally, the three-layer architecture of the IoT is illustrated in **Figure 2.2**a. Specifically, the perception layer is implemented at the bottom of the IoT architecture. It is responsible for sensing and collecting the data for the IoT objects and transmitting the collected data to the upper layer [57, 62]. The network layer is implemented in the middle of the IoT architecture [57] to receive the information provided by the perception layer and determine the paths for transmitting gathered data to an IoT gateway device. The

application layer is implemented at the top of the IoT architecture [32, 57] and acts as an interface between the IoT application and the end users.



(a) (b) (c)

Figure 2.2 IoT architecture (a) three-layer, (b) four-layer SOA-based, (c) five-layer

- **Four-layer SoA-based Architecture**

As suggested by [57], a service layer should be implemented to provide the data services in IoT. The service-oriented architecture (SoA) is a component-based model which uses interfaces and protocols to connect different functional units of an application [57, 63, 64]. It can be easily integrated into IoT architecture where the data services can be separated to form a new layer, called the service layer. The SoA-based architecture is composed of four layers: the perception layer, the network layer, the service layer and the application layer (see **Figure 2.2**b) [57]. The perception layer, network layer, and application layer have similar functionalities with these layers in the three-layer architecture. The service layer including service discovery, service composition, service management, and service interface is implemented between the network layer and the application layer to provide services to the application layer [32].

- **Five-Layer Architecture**

While the four-layer SoA-based architecture is the expanded version of the traditional three-layer architecture, the five-layer architecture (see **Figure 2.2**c) focuses on providing more facilities in the application layer [58, 62]. In this architecture, the perception layer represents the physical sensors and devices of the IoT. The transport layer relays the data provided by the perception layer to the processing layer. The processing layer includes a

database, intelligent processing, cloud computing, and ubiquitous computing units to deliver the required services to the upper layer based on received data from the lower layer. The application layer provides the required services to the users via diverse IoT applications such as smart home, smart building, healthcare, industrial automation. Finally, the business layer provides facilities to build a business model based on the received data and is responsible for designing, analyzing, implementing, evaluating, monitoring and developing the IoT system [62].

In summary, the three-layer architecture is the simplest architecture of IoT. However, the functions and operations in the network layer and the application layer are complicated because many facilities for data processing to various related services need to be implemented. The four-layer SoA-based architecture adds a service layer to separate the roles of data services but brings more challenges to resource-constrained devices. The five-layer architecture is the most complicated architecture, but it has been considered as the most applicable model for IoT applications. It provides the business layer to manage the overall IoT system's activities and services and to compare the output of each underlying layer with the expected output to enhance services' quality and maintain users' privacy [62].

Regardless of which architecture that an IoT system is designed in, gaining insights into its implemented architecture and the functionalities of each element in the architecture is a critical factor to comprehensively identify the challenges in developing secure and trust control approaches for the IoT system. For example, with the three-layer architecture, the primary purpose of the perception layer in IoT is to collect data. Thus, the challenges in this layer are how to ensure the reliability of the collected data and the trustworthiness of physical sensors or IoT sensing devices. The network layer is responsible for transmitting collected data. Hence, this layer must also focus on the impact of the availability of network resources and the reliability of communication links.

2.1.3 Requirements of an IoT System

An IoT system must be developed in a way that it fulfills the user's needs in both functional and non-functional requirements. The functional requirements of IoT systems

include diverse connectivity, ability to leverage a range of applications, the range of devices, generate a massive amount of data, and have potent data analytics. However, even if an IoT system is built with those functional requirements, there are still a lot of concerns about non-functional requirements including security, safety, resilience, reliability and privacy and trust [65]. In the following, we will look at these main non-functional requirements.

- **Security**

Security goal of an IoT system refers to whether an aspect of the system meets the standards of confidentiality, integrity, and availability (CIA) [5]. Confidentiality ensures that the data is available to authorized users only and will not be accessed by non-authorized users [47, 57]. In order to achieve the confidentiality in IoT, advanced techniques in access control (authorization), encryption and cryptography are required. Integrity is the ability to ensure that the improper information modification or destruction is guarded against [65]. To ensure the integrity requirement in IoT, key generation and exchange methods and authentication protocols should be applied [47]. Availability means that the data and devices are available for authorized users and services whenever they are requested. In IoT, services are usually required in real-time. Thus, they require that the requested data and devices are always available [57].

- **Privacy**

Privacy ensures that an individual or a group can control what information related to them may be collected, processed and stored and to whom that information may be disclosed [5]. An individual in the IoT system becomes a source of multiple data sets. For example, wearable devices in a healthcare system can collect a massive amount of personal data and the surrounding environment. Medical devices and fitness applications raise more privacy concerns in health-related data since the personal and sensitive data is easily exposed to unauthorized parties.

- **Safety**

Safety is the condition of the IoT system operating without causing risk of physical injury or damage to people either directly or indirectly, as a result of damage to property or to the environment [65].

- **Resilience**

Resilience is an emergent property of an IoT system that behaves in a way to avoid, absorb and manage dynamic adversarial conditions while finishing the assigned missions, and reconstitute the tasks after interruptions [65]. Resilience is often achieved by designing the system so that failures are compartmentalized.

- **Reliability**

Reliability is the ability of a system or component to perform its required functions under stated conditions for a specified period. If a single function fails, there should be alternate ways to perform the failed function automatically, immediately and reliably [65]. In the IoT context, data reliability is also critical as it affects other actions which can be triggered by the actuators.

- **Trust**

Trust plays a crucial role in IoT for reliable data fusion and mining, qualified services with context-aware intelligence, and information security [12]. Security controls can prevent the data from modification and interception, but do not provide a mechanism to detect and isolate misbehaved or maligned devices. Although IoT systems can be secured by using security methods, their provided data and services might not be trusted completely. Therefore, besides security, trust is a critical requirement to ensure the data and services worthiness in the IoT systems. Moreover, trust has been recognized as an essential factor that ensures the effectiveness of security approaches. For example, trust is the basis of authentication. To authenticate an entity based on its certification issued by a certificate authority (CA), we have to trust the CA. In the key management and distribution process, the parties must establish a trust relationship to agree on a shared key for secure data transmission [66]. Trust is also the basis for cooperation and collaboration in the IoT.

A full life cycle of trust management is from the initialization of a trust relationship via an initial trust establishment to its usage in decision making and then to the updating of trust based on observations [4]. According to [67], the motivation of providing a trust management model for IoT systems is that there are misbehaved devices that may perform discriminatory attacks for their benefit. This requires a trust management model implemented in the IoT systems. In [68], the authors argue that the trust management model in IoT systems could establish a trust relationship between two entities, evaluate

the trustworthiness of an entity in the systems and provide solutions to use the trust value obtained from the trust evaluation to manage or improve the performance of the IoT systems. While many studies on security in IoT have been conducted, research on trust in IoT has not yet been comprehensively investigated.

2.2 Existing Initial Trust Establishment Approaches

The trust relationship among IoT devices is the basis of the cooperation and collaboration among them in the IoT systems. Without establishing the trust relationship among IoT devices and monitoring the device's trustworthiness, their collected data might not be trusted. Moreover, IoT applications and services offered by the IoT systems also cannot be reliably created. Therefore, IoT systems need a trust management element to establish initial trust level on devices before admitting them into the system and to continuously monitor the trust of every device from the time it is admitted into the systems until the end of its lifecycle to ensure the trustworthiness of the provided data and offered services.

Generally, initial trust is a critical factor that people rely on to start a collaboration, engage with others, admit something or someone into their's space or organization. Initial trust establishment in an IoT system is vital for the success of the system and the trustworthiness of its services and applications. Importantly, initial trust assessment at the device admission phase could allow the IoT systems to admit trustworthy devices into the system while reducing the risks of attacks performed by misbehaved or compromised devices. Moreover, it is challenging to establish the initial trust relationship between the IoT system and the devices for admitting potential devices into the system due to the time limitation and the lack of prior trust evidence. Therefore, research on initial trust establishment design and investigation for an IoT system is of critical importance. However, research on initial trust establishment in IoT has not yet been comprehensively investigated. In this thesis, we focus on the initial trust establishment in the IoT systems.

In general, there are very few research efforts concerning the initial trust value and initial trust establishment. We categorize and discuss the previous efforts in this section.

Assigning a default initial trust value: In a trust management model, newcomers become a problem since they usually come without prior knowledge. Generally, for the entirely unknown entity, assigning a default value for the initial trust level of newcomers is the most common solution [4, 69, 70]. However, the default value assigned by a system might not be feasible due to the lack of knowledge about entities at the onset of their joining the system. Moreover, there are situations where a known entity wishes to rejoin the system, but its prior trust assessment is no longer valid as the entity might have been infected while being absent from the system.

Relying on given credentials: A trust relationship can also be established via an authentication process which allows the system to determine an initial trust level of an entity through the proof of having membership/credentials in a group with a good reputation [4, 71]. This method is merely deciding how much one trusts given credentials rather than the trustworthiness of the entity.

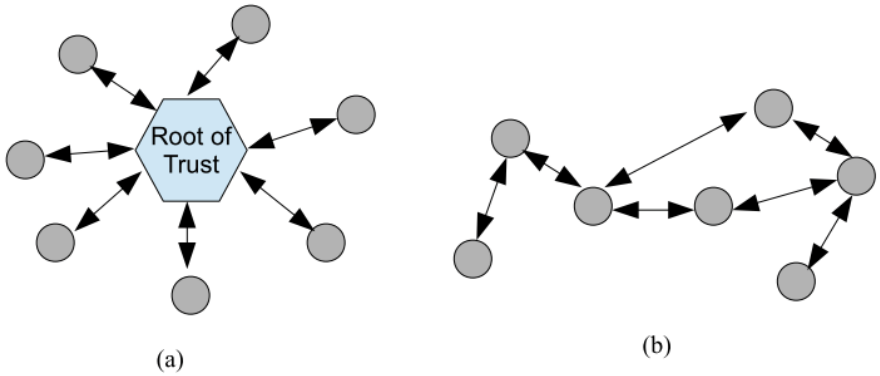


Figure 2.3 (a) Establishing centralized initial trust using a root of trust, (b) Establishing distributed initial trust [72]

Relying on a root of trust: Establishing initial trust relies on a *root of trust* that constructs an initial trust relationship between two entities [72]. With the root of trust, the trust relationship between two entities that maintain a common relation with the root can be achieved. Example of a root of trust can be a special hardware component such as a trusted platform module or the root certificate in public key infrastructure (PKI). The system can utilize the root of trust as a centralized authority to determine and store the initial trust of all entities in the network. Then, the trust among entities is derived from this root. Another way is that the system employs distributed entities that can monitor and

maintain a trust relationship with others and also support others in establishing initial trust with the entities that they know [72]. The illustration of establishing initial trust in the centralized and distributed ways are showed in **Figure 2.3**a and **Figure 2.3**b, respectively.

The root of trust is usually called a centralized authority. In the context of IoT, when the IoT system wants to evaluate initial trust of the entities before admitting them into the system, the trust relationship between a centralized authority in the system and the new entities has not yet been established. Therefore, using the root of trust is only feasible when all new entities have established their initial trust with the root, and the initial trust establishment among admitted entities is needed.

Similarly, in the existing distributed trust schemes the initial trust relationship among entities in the network is also based on the initial trust established between two participants beforehand. Other participants that have not established an initial trust relationship can rely on the distributed nodes in the system to build its initial trust with others. Again, the problem in these schemes is how to quantify the initial trust relationship between two entities so that later we can use this to derive trust relationship between two entities that do not maintain a relationship in the distributed network. In addition, once the initial trust between two entities is established, the further initial trust establishment based on the established trust might not be accurate when the distributed nodes are compromised or misbehaved for their benefit.

Relying on recommendations: The initial trust establishment can be determined by using the recommendations from other parties [4]. However, determining the initial trust value based on the experiences of third parties (recommendations) or authorized entities may be a poor estimate due to the difference in the view of authority entities or the colluded third parties. In addition, with the dynamic nature of the IoT system in a personal environment, there might be a lack of recommendations from the third parties.

Using a committee to judge the initial trust: A possible approach is to aggregate a committee to judge the trustworthiness of the device at the instance of its encounter with the system [73]. In the personal space IoT scenario, collective community judgment is not feasible and only a limited amount of time is available for establishing the initial trust.

It is noted that when the IoT systems admit a device the prior trust resources such as the historical experience or the recommendations from other entities are usually not

available or no longer valid as the device is either new or unknown to the system and its environment or is returning to the IoT system after an absence period. Therefore, it is challenging to quantify the initial trust on potential devices before admitting them into the system within a limited time window where prior knowledge is usually not available. Moreover, existing initial trust establishment approaches have limitations and are not applicable in personal space IoT systems.

In this thesis, we propose a novel initial trust establishment framework that allows the IoT system to generate meaningful initial trust evidence about a device so that the system can assess and quantify the device's initial trust level before deciding to admit the device into the system.

2.3 Existing Trust Computation Schemes

This section explores existing trust computation schemes which are used in related areas such as wireless sensor networks, multi-agent systems, social networks, and IoT. These approaches are different means to observe and compute the trust level of entities during the operational phase of the system where the knowledge for trust assessment is available in the form of direct observations or recommendations. Numerous methods have been proposed to calculate trust. However, we only review existing trust computation schemes that are related to our proposed solutions in this thesis.

2.3.1 Bayesian Inference-based Computation Schemes

In Bayesian inference-based trust computation schemes, trust is derived from a random variable following a probability distribution where its model parameters are being updated upon new observations. Bayesian-based trust computation schemes have been widely used in trust management models thanks to their simplicity and sound statistical basis [67].

Bayesian approaches have been widely used to compute trust whereby Beta distribution is adopted for the trust computation schemes. For instance, Chen et al., [24] proposed a trust management model for service-oriented application by taking Bayesian framework as the underlying model to evaluate the direct trust towards a service based

on user's satisfaction level. The trust value of a user on a service is a weighted combination of his satisfactory direct experience and recommendations from his friends. This model requires entities to keep track of their past observations of all other entities in the system.

The authors in [7] introduced a classical beta reputation-based framework for sensor networks where nodes use reputation to evaluate other's trustworthiness. In this work, a node estimates the reputation of another node based on their transactions with others over a period and reputation information recommended by its neighbors. By fitting the distribution of the node's reputation to beta distribution, the authors define the trust of a node as the statistical expectation value of the beta probability density function (pdf) associated with its reputation. The mapping of the statistical expectation value of the beta distribution to trust value is then utilized in a number of studies [24, 74-77].

Similarly, the authors in [75] adopted a Bayesian framework as an underlying model for evaluating direct trust from the records of successful and unsuccessful interactions maintained at each node. The beta distribution is used to represent the distribution of interactions among nodes. The direct trust of a node is then represented by the expectation value of the pdf of the beta distribution.

In [74], a probabilistic trust management model is proposed based on the experience of previous interactions and recommendations. The beta distribution is also used to represent the distribution of the probability of a satisfactory interaction when the number of previous satisfied and unsatisfied interactions from direct observations and recommendations are known. The trust value is influenced by the expected value of the pdf of the beta distribution. However, in this approach devices must keep lists of the history of interactions with others and requests for recommendations.

Dirichlet distribution is also commonly used as a prior distribution of a multi-component random variable where the initial belief of the random variable is updated with collected data and hence can be represented by a posterior distribution. This is utilized as the foundational mathematics of some trust computation schemes [6, 26, 78, 79]. For example, in [6], Josang et al., use the Dirichlet distribution as the basis for a multi-level reputation system for e-commerce where parties can rate each other with graded levels from a set of predefined values. The posterior Dirichlet model combines

the previous reputation score with a new rating to find the updated reputation score of an agent. This work mainly relies on the ratings that are recommended by other agents in the community. The drawback is that it requires large transactions and rating process to build an agent's reputation.

Fung et al., [26] adapted Dirichlet-based trust management to collaborate with host-based intrusion detection networks (HIDS) to detect intrusions and malicious nodes. This model determines the trustworthiness of a HIDS node by collecting both intrusion consultations and its feedbacks to some 'test' messages. It then computes the trust level of a HIDS node through the posterior Dirichlet distribution. This approach mainly focuses on reactively detecting the malicious nodes and intrusions once the HIDS is in operation stage and requires long-term collaboration leading to high overhead due to the 'test' messages.

In [78] the authors proposed Dirichlet-based trust management for an inter-provider cooperation network where the entities in different domains cooperate with each other using client-server interactions. This work relies on the interactions between entities in different domains where the server accepts the interactions and implicitly evaluates the trustworthiness of the requested client.

In summary, the Bayesian inference-based trust computation schemes update the prior trust knowledge with the available observations to achieve the posterior trust information. In the initial trust establishment, it is practical to rely on the noninformative prior knowledge and update it with new observations. Therefore, if we can create the initial trust knowledge to update the noninformative prior knowledge to a meaningful posterior knowledge, the Bayesian inference can be a possible basis to compute the initial trust level. Moreover, additional mechanisms need to be proposed to create meaningful information to update the prior belief.

2.3.2 Other Trust Computation Schemes

Dempster-Shafer theory-based trust computation: In [66], the authors utilized Dempster-Shafer theory [80] as the underlying trust computational model to compute the trust of agents in multi-agent systems. Each agent determines the trustworthiness of

another agent based on its prior interactions and the testimonies given by other trusted agents who have interacted with the under-evaluation agent. The trust value is computed based on combining belief function defined by Dempster-Shafer theory.

Li et al. [81] proposed an attack-resistant trust management scheme for vehicular ad hoc networks (VANETs) which can detect and cope with malicious attacks and evaluate trustworthiness mobile nodes and the data collected and transferred by these nodes in VANETs. Especially, the data trust is evaluated based on the data sensed and collected from multiple nodes. The trustworthiness of a node is assessed via the functional trust and recommendation trust. The functional trust verifies whether a node fulfills its functions whereas the recommendation trust verifies if the node can provide trustworthy recommendations to other nodes in the network. The Dempster–Shafer theory of evidence (DST) is utilized to combine the first-hand evidence collected by a mobile node itself and the second-hand evidence shared by other mobile nodes.

In [82], Li et al. also proposed a policy-based secure and trustworthy sensing for IoT in smart cities. The scheme evaluates the trustworthiness of the IoT devices and the data collected by the devices based on the reporting of other devices in the systems. The policies are used to identify malicious nodes that have been compromised by attackers using contextual information.

The Dempster–Shafer theory-based trust computation schemes combine the evidence from the trustor' own view and from the indirect view given by other nodes to learn the trustee's behavior. These schemes can only work at the operational phase of IoT systems where a lot of evidence can be collected from the node's activities and observations.

Fuzzy logic-based trust computation: Fuzzy logic has been used to manage uncertainty and to model trust in various network environments such as semantic web, peer-to-peer (P2P) networks, grid computing, mobile ad hoc networks, and e-commerce [67]. It is a form of many-valued logic in which the truth values of variables may be ranged from 0 to 1. For example, in [83], Chen et al. utilized a fuzzy membership function and collected information of the positive and negative experiences observed from the end-to-end packet forwarding ratio, packet delivery ratio, energy consumption, to compute trust in an IoT system. This requires a period of observation to work out positive or negative experiences.

In [84], a trust-based access control model is proposed where a fuzzy logic approach is utilized to deal with the linguistic information of devices in the IoT. The trust related semantic information is collected under the form of experience (EX), knowledge (KN) and recommendation (RC). The trust level is calculated based on received information, i.e., exact values of EX (bad, average, good), KN (insufficient, less, complete), RC (negative, neutral, high), and rules-based fuzzy model. Then, the fuzzy trust values are mapped to access permissions to achieve access control in the IoT system.

In [85], a fuzzy logic-based trust model is proposed to detect untrusted nodes in smart grid networks. The authors defined the linguistic inputs of the fuzzy logic trust model including the direct trust observed at the sensor node level, the indirect trust observed at the base station level, and the past trust referring the historical behavior of each node. The proposed model used triangular and trapezoidal membership functions to map input values to fuzzy sets. The trust values are calculated by passing the fuzzy sets through fuzzy inference rules under IF-THEN description.

The trust computation schemes based on fuzzy logic [83-85] require different opinions from various resources observed in long-term interactions. They can be applied to calculate the trust of entities during the operational phase of the system where historical experiences and recommendations are available.

Subjective logic-based computation: Subjective logic uses opinions to denote the representation of a subjective belief [86]. The basic idea of subjective logic-based trust computation schemes is to model trust by belief, disbelief, and uncertainty. For example, Josang et al. [87] described a node's opinion in another node by belief (b), disbelief (d), and uncertainty (u), with $b + d + u = 1$. The average trust value is given by the probability expectation value computed from the opinion as $b + au$, where a is the base rate probability in the absence of evidence. Subjective logic operators such as the discount and consensus operators are used to combine opinions (either self-observations or recommendations).

In [88], the authors proposed a subjective logic-based trust model in MANETs that enables mobile nodes to explicitly represent and manage ignorance as uncertainty during the establishment of trust relationships with other nodes. Accurately, in this model belief (b) and disbelief (d) are summarized from the evidence captured for benign and malicious

behaviors respectively, and uncertainty (u) represents the ignorance or level of confidence in a node's knowledge. Three kinds of opinion including direct operation observed opinion and recommended opinion are used to formulate the advice of a mobile node for other nodes based on the evidence collected from the benign and malicious behaviors of those nodes. The proposed model adds a fading operator to subjective logic to address the uncertainty introduced by recommended nodes. The consensus operator is used to combine defined opinions into a global opinion which is used to evaluate the nature of the trust relationship that a node holds for another node (i.e., trustworthy, untrustworthy and uncertainty).

In [89], Ri et al. proposed a solution to predict the trust relationship between users' social networks based on subjective logic. The proposed subjective logic-based trust prediction defined four different type of personal opinions based on the ratings of a user A to the activities of user B, ratings of B to the activities of A, and the common ratings of A and B to the activities of another user. The opinion of a user about another user is defined as the fusion of four defined subjective opinions. Then the trust relationship is computed from the average fusion opinion which can be 1 to represent the trust opinion and -1 to express the distrust opinion.

Thus, in order to form reliable opinions, the entities in the trust network have to be involved in observations/interactions for a long time. However, in the initial trust establishment, forming opinions and combining them to extract a trust value is not applicable as the time window is limited.

Uncertainty-based trust computation: Sun et al. [90] introduced the utilization of uncertainty as a measure of trust. Trust can be measured from the uncertainty level in the actions of an agent in the future. The uncertainty level is measured through concatenation and multipath propagation of recommendations when the direct observation is not available. Similar to other mentioned approaches, this approach is also not applicable to estimate the initial trust of the system on an unknown entity due to the lack of third parties' recommendations at its first encounter with the system.

Logistic regression-based trust computation: In [91], Wang et al. adopted logistic regression to dynamically learn the relation between cumulative evidence collected by one node about another node and the corresponding environmental context variables of

energy-sensitivity, capability-limitation, and cost-awareness. This relation is then used to predict if the given node can provide a good service when it is requested in a given environment setting that is characterized by a set of context variables. The analysis describes the trust evidence and explains the relationship between the trust evidence and the environmental context. It requires the nodes to collect the evidence for a long time before it is used for predicting a trust level considering the environment setting.

Similarity-based trust computation: Chen et al. [92] proposed a trust management model for social IoT systems that considers the dynamically changing social relationships among the owners. Each device evaluates the honesty, cooperativeness, and community-interest trust properties of others by combining direct observations and indirect recommendations. Chen et al. used similarity (derived from social trust) as the weight for indirect trust aggregation [24]. The similarity concerns the social relationships among owners of devices. It requires the owners to engage with each other before observing their trust.

Weighted combination-based trust computation: In [93], the authors proposed a distributed-based framework whereby the trust parameters are observed via the information transmission. A node can compute the trust level of its neighbors based on observation of their past behavior. The metrics such as number of data packets and control packets that are successfully transmitted or being modified are combined together with predefined weight values to determine a trust value. Similarly, Wang et al., [94] presented a trust evaluation model in P2P networks. The trust value that a peer places on another peer is determined based on the historical interactions between the under-evaluating peer and other peers in the network and its friend's recommendations. The trust value is the aggregated value of local values derived from historical interactions and from the trust values given by other peers. These methods require long-term interactions before the knowledge can be observed.

Graph theory-based trust computation: In [95], the authors proposed a trust evaluation model as a problem on a directed graph where nodes represent entities and edges represent trust relations. The indirect trust relationship between two users is established by using second-hand information from a third party. Thus, their trust model needs direct trust relations between the third entity and one of the two users. Also, there

is no mechanism to guarantee that the third party is a trusted recommender. This method requires the third party to maintain a direct graph with the trustees to observe the knowledge for making recommendations.

2.3.3 Discussion

The reviewing of existing trust computation methods provides possible ways to evaluate the trust level. Each scheme requires either the observations over a long time or third-party entities that can provide related recommendations or the combination of opinions from a community to calculate trust. These trust computation schemes cannot be applied directly to the initial trust establishment model due to the lack of required knowledge when the entities encounter each other for the first time. It is practical to propose an additional mechanism to generate the initial trust resource within a reasonable time. When the initial trust resources are available, any existing trust computation scheme can be used to quantify the initial trust level. However, it is challenging to generate the initial trust evidence and gain meaningful knowledge for the initial trust computation.

In order to generate trust evidence and gain essential trust resources for the initial trust computation for personal space IoT system, a novel mechanism is needed at the device admission phase of the system so that it can capture the device's behavior and gain the required resources. In this thesis, we proposed a challenge-response-based initial trust establishment model that uses challenge-response operations for generating trust evidence and the Bayesian inference for the mathematical foundation of its trust evaluation module. Specifically, we propose a challenge-response process to generate trust evidence at the device admission phase of the system within a short time window. In addition, we propose a design of the information space of the challenge-response process that can be tailored to the target environment and capture related evidence within a reasonable time window for the trust computation. Then, several Bayesian-based trust computation methods are proposed to quantify the initial trust level of the IoT device based on the trust evidence observed by the challenge-response process.

It is noted that when the devices are admitted into the system and participate in many operations in the system, there are more trust resources which can be gained from these

interactions. Thus, many trust computation schemes can be used to reevaluate the trust level of the admitted devices.

2.4 Bluetooth Low Energy and Its Trust Consideration

Bluetooth Low Energy can be used as a framework for realizing our proposed initial trust establishment model in practice. This section briefly introduces portions of Bluetooth Low Energy protocol that relates to the demonstration of the feasibility and efficiency of the proposed solutions.

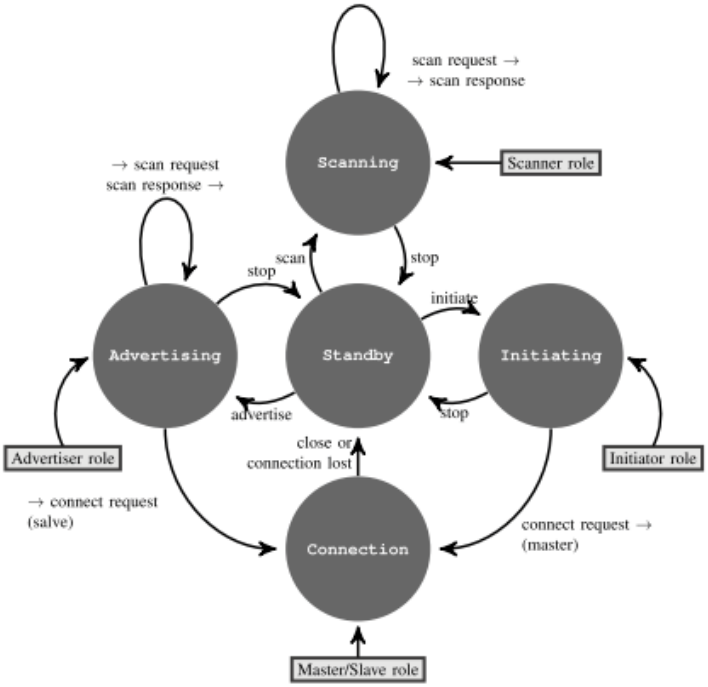


Figure 2.4 BLE finite state machine [96]

The BLE protocol specification establishes five states (see **Figure 2.4**): *standby, advertising, scanning, initiating* and *connection*. During the device discovery phase, using only three advertising channels (channels 37, 38, 39) devices transit through *standby, scanning* and *initiating* states for scanners, or through *standby* and *advertising* for advertisers. In the connected mode, when one of the devices initiates the connection request packet, devices transit through *connection* and *standby* state, and use 37 data channels (channel 1 to channel 36, and channel 40) for data exchanging.

Two BLE devices communicate with each other during their first encounter in the device discovery phase and the connection establishment duration. Several packets are exchanged on the advertising channels during the device discovery phase to transfer information between the devices before a connection establishment.

According to the Bluetooth specification version 4.2, there is only one packet format used for packet exchanging in the advertising channels as well as the data channels as shown in **Figure 2.5**. Each packet is composed of the preamble, the access address, the PDU and the CRC. The preamble for all packets exchanging on advertising channels is fixed at 10101010b and is either 10101010b or 01010101b for packets exchanging on data channels. While the access address for all advertising channel packets is 0x8E89BED6, it is different for each data channel packet depending on each connection. The PDU for advertising channel packets and data channel packets are different for each packet type. The CRC has 24-bit length and is calculated over PDU for packet error check purpose. The packet payload's PDU in the BLE protocol has the potential to carry optional information if needed. For example, the advertisement packet's and the scanning response packet's payload PDUs can include advertisement data that the two devices wish to send to each other.

Figure 2.5 BLE Packet Format

In BLE, once the two devices are connected (at the connected mode), if one of the devices wishes to exchange data securely they must perform a pairing process where they exchange necessary information to establish an encrypted connection. The method of pairing model is selected based on the I/O capabilities of each device. Pairing involves authenticating the identity of two devices to be paired through a process of sharing a secret, encrypting the link using a Short-Term Key (STK) shared by the two authenticated devices, and then distributing long-term keys via the link encrypted by the STK. A Long-Term Key (LTK) is used to encrypt subsequent reconnections without repairing between

devices. A Connection Signature Resolving Key is used for data signing, and an Identity Resolving Key (IRK) is used for private MAC address generation and lookup. The distribution of keys is to allow security to be restarted on a reconnection more quickly.

According to the "Guide to Bluetooth Security" of NIST special publication [97], Bluetooth pairing is a process of creating shared secret keys and storing these keys for subsequent connections. It can be expressed that in Bluetooth trust relationship is the consequence of a successful pairing process. According to [71], a trusted device is the one that has been authenticated, shared a link key, and is marked as "trusted" in the device database of the initiating device of the pairing process. It is noteworthy that the device's trust level was used to be considered in Bluetooth classic specification to guarantee secure access control. In contrast, this feature is not supported in BLE. The successful pairing in BLE only confirms that the two devices' identities are verified, but the device's behavior is not evaluated during the pairing procedure.

The possible interactions between two BLE devices when they first encounter each other can be utilized to conduct the challenge-response process to generate trust knowledge for our initial trust establishment architecture. Moreover, incorporating the trust-aware feature to the existing BLE protocol is critical to enhance the security and trust of IoT systems that use BLE as the underlying communication protocol among the devices in the system.

2.5 Mathematical Background

This section briefly describes the mathematical foundation required for our proposed initial trust establishment framework. We start by introducing the Shannon entropy which is considered as a natural measure of uncertainty [98]. We then describe the Bayesian inference which is a framework to analyze the model when more observation becomes available. Finally, the background of Beta distribution and Dirichlet distribution which are used as the foundations for our initial trust computation module in the initial trust establishment framework are described.

2.5.1 Shannon Entropy

The concept of entropy originated in the physical and engineering sciences but now plays a ubiquitous role in many disciplines [99]. According to Shannon's mathematical theory of communication, entropy could be used as a measure of information content and uncertainty. Specific information is the information conveyed by the occurrence of an event x_i with the probability of the event $p(x_i)$ and quantified as below.

$$I(x_i) = -\log_2 p(x_i) \tag{2.1}$$

Shannon's formula defines the entropy as the weighted average of the specific information for each event in the system of N possible events.

$$H(X) = -\sum_{i=1}^{N} p(x_i) \log_2 p(x_i) \tag{2.2}$$

If we consider a process of N possible outcomes and the probability distribution of the events is uniform, the maximum entropy value is $\log_2 N$. This refers to the highest uncertainty when one wishes to know the appearance of an outcome. On the other hand, the minimum entropy value occurs when one of the outcomes certainly happens with a probability of 1 and all other possible outcomes have a probability of zero. This refers to the lowest uncertainty, or equivalently, there is certainty about the occurrence of a given result.

In [99], the authors also suggested that the entropy is best interpreted as a measure of uncertainty. This idea has been applied to trust models which consider the uncertainty of the entities' behavior in the future. For example, authors in [100] adopted information theory with Shannon entropy to model a trust computation method for ad hoc networks. In our proposed initial trust establishment model, we applied the Shannon entropy as a measure of the uncertainty that the system has about a device when we learn the device's behavior and assess its trustworthiness at the initialization of the IoT system.

2.5.2 Bayesian Inference

Bayesian inference derives the posterior probability as a consequence of two antecedents: a prior probability and a "likelihood function" achieved from a statistical

model for the observed data. Bayesian inference computes the posterior probability according to Bayes' theorem

$$P(X \mid Y) = \frac{P(Y \mid X)P(X)}{P(Y)} \tag{2.3}$$

where X and Y are events, and P(Y) ≠ 0.

The terms used in the expression of Bayesian inference are explained as below.

- P(X): prior distribution which quantifies the a priori understanding of the unobservable quantities of interest. In general, prior distribution can be informative or non-informative.
- P(Y|X): likelihood or data distribution which is merely the distribution of the data, given the unobservable.
- $P(Y) = \int p(y \mid x)p(x)dx$: marginal likelihood which is also known as the prior predictive distribution or "normalizing constant" in Bayes' formula.
- P(X|Y): posterior distribution of the unobservable given the likelihood data is the primary interest for inference. The posterior is the update of the previous knowledge about unobservable quantities of interest (X) as summarized in $p(x)$ given the actual observations data (Y). In this sense, applying the Bayesian approach means that we have a prior belief about X, then we collect data, and update our knowledge on X given the new data Y becomes available (observation) [101].

The Bayesian approach has also been applied to the problem of trust evaluation in networked principles (see section 2.4.2.1). In this problem, observations about the behavior of an agent are gathered from its interaction with a subject. The subject learns the behavior of the agent via the accumulated evidence. Therefore, it assigns a probability distribution over possible hypotheses regarding future interactions with the agent. Regarding theory and observed data, the Bayesian inference can be expressed as follows.

$$P(hypothesis \mid data) \propto P(data \mid hypothesis) \times P(hypothesis) \tag{2.4}$$

2.5.3 Beta Distribution

The beta distribution is a continuous probability distribution which is defined on the interval [0, 1] and parametrized by two favorable shape parameters, denoted by α and β. These parameters appear as exponents of the random variable and control the shape of the distribution. It is usually used as the conjugate prior distribution for binomial proportions in Bayesian inference [102].

The probability density function (pdf) of a beta distribution with the parameters α and β, for a random variable x is in [0, 1] and $\alpha, \beta > 1$, is as follow.

$$f(x;\alpha,\beta) = \frac{x^{\alpha-1}(1-x)^{\beta-1}}{\int_0^1 x^{\alpha-1}(1-x)^{\beta-1}dx} = \frac{1}{B(\alpha,\beta)}x^{\alpha-1}(1-x)^{\beta-1}, \text{ where } 0 \le x \le 1 \tag{2.5}$$

The mean μ and variance σ^2 values of a random variable with Beta distribution are given by

$$\mu = \frac{\alpha}{\alpha+\beta} \tag{2.6}$$

and

$$\sigma^2 = \frac{\alpha\beta}{(\alpha+\beta)^2(\alpha+\beta+1)} \tag{2.7}.$$

The beta distribution has been adopted in numerous Bayesian inference-based trust models (see section 2.3.1) to evaluate the trust level of entities in a networked system where their behavior/interactions/provided services are observed to be either a positive experience or a negative experience. It is a mathematical foundation for the trust evaluation when there are two possible outcomes from the trust behavior observations. In the initial trust establishment, if there is an additional mechanism which is invested for observing the behavior of newcomers, it is possible to estimate the trust level under the assumption of beta distribution of the observed data. The beta distribution is employed as a mathematical foundation of an initial trust establishment model proposed in chapter 5.

2.5.4 Dirichlet Distribution

Dirichlet distribution is a family of continuous multivariate probability distributions [103] parameterized by a vector of positive real numbers, α. Dirichlet distributions are commonly used as a conjugate prior distribution of the categorical distribution and multinomial distribution in Bayesian inference [104].

The Dirichlet distribution of a multi-component random variable $X = (x_1,...,x_N)$ with N dimensions and parameter vector $(\alpha_1,...,\alpha_N)$ has probability density function (pdf) given by

$$f(x_1,...,x_N;\alpha_1,...,\alpha_N) = \frac{1}{B(\alpha)}\prod_{i=1}^{N} x_i^{\alpha_i - 1} \tag{2.8}$$

where $\sum_{i=1}^{N} x_i = 1;\ x_i \geq 0, \forall i \in [1,n]$ and $B(\alpha) = \frac{\prod_{i=1}^{N}\Gamma(\alpha_i)}{\Gamma(\sum_{i=1}^{N}\alpha_i)}$, $\alpha = (\alpha_1,...,\alpha_N)$.

The mean and variance corresponding to each component in the multi-component random variable X are given as below.

$$E[x_i] = \frac{\alpha_i}{\alpha_0} \tag{2.9}$$

$$Var[x_i] = \frac{\alpha_i(\alpha_o - \alpha_i)}{\alpha_0^2(\alpha_0 + 1)} \tag{2.10}$$

where $\alpha_0 = \sum_{i=1}^{N}\alpha_i$.

The Dirichlet distributions are commonly used in Bayesian inference to express the multivariate distribution where the interest is on a multi-component random variable. Rating process in reputation systems is a favorite example of a multi-component random variable. In literature, Dirichlet distributions have been used in trust models where the observations are interested in multiple possible outcomes [6]. In our proposed initial trust establishment framework, we adopt a Dirichlet distribution to build the initial trust evidence.

2.6 Summary

In this chapter, we presented a brief overview of the IoT architectures; its building blocks to the emerging applications of IoT are presented. We then provided the requirements of an IoT system and emphasized the crucial roles of trust requirement in IoT. Existing initial trust establishment approaches are reviewed. We then reviewed the existing trust computation schemes that are related to our proposed solutions. We presented a brief overview of portions of the existing BLE protocol which are used as the framework to realize our proposed solution. We also introduced the related mathematical background for a better understanding of our proposed approaches in this thesis.

Chapter 3

Initial Trust Establishment for Personal Space IoT Systems – Overall Architecture

3.1 Introduction

The Internet of Things system ranges from a small system which contains uniquely identifiable things and small sensors to a large system that interconnects billions of things to deliver complex services [28]. Proposing a single approach for building a trustworthy IoT system, in general, might not be realistic for all IoT systems. Defining the scope of an IoT system (or subsystem) to be protected is critical in terms of architectural organization, system modularization, separation of security concerns, and providing the foundation for building more secure and complex IoT systems. This motivates us to introduce and define a new IoT environment with a personal space scope – *the personal space IoT system*. The aim of the solutions proposed in this thesis is to establish an initial trust relationship between the controller and IoT devices within a personal space IoT system so that a secure and trustworthy personal environment can be established to provide reliable services to its user.

Since the devices in personal space IoT systems closely connect us to our personal and physical world by providing sensing information as well as taking actions on our behalf, their trustworthiness is of paramount importance for a secure personal space IoT.

In this chapter, we will discuss the importance of establishing initial trust in a personal space IoT system and emphasize the necessity of a framework to establish initial trust in the personal space IoT. We then present an overall architecture of our proposed initial trust establishment model for the personal space IoT system. In order to realize our model, we introduce a new initial trust-aware protocol over an existing communication protocol, in particular, the Bluetooth Low Energy protocol.

The remainder of this chapter is organized as follows. Section 3.2 provides our definition of the personal space IoT system. Section 3.3 discusses the importance of initial trust establishment for the personal space IoT systems and emphasizes the necessity of a framework to establish initial trust level. Section 3.4 presents the overall architecture of our proposed initial trust establishment model for the defined personal space IoT system where all modules are discussed accordingly. Section 3.5 discusses the possible realization of our proposed initial trust establishment over the existing Bluetooth LE protocol. Section 3.6 provides the roadmap of the work which will be presented in this thesis. Finally, section 3.7 summaries the chapter.

3.2 Definition of a Personal Space IoT System

The personal space IoT system is a group of connectivity-enabled devices working together within the space of a user. Each personal space IoT system consists of a group of user-implanted and wearable devices providing services to a user, and other devices that are within the wireless communication radius of the user's devices. In this system, a smartphone or a capability-comparable device acts as the centralized controller, managing the space including admitting devices to the system and monitoring their activities. The environment covers all devices that are present within the controller's radio range of the IoT system. It also includes external devices that can be placed in a fixed position or are movable with their owner. Those devices can cooperate with the devices in the IoT system to provide potential services and data to the user. However, the operations of external devices may also maliciously interfere with operations of the IoT system. Therefore, in order to admit a device into the IoT system, the system must assess whether it is trustworthy and able to provide trustworthy and desired data and services.

Figure 3.1 illustrates the personal space IoT environment where each circle represents a personal space IoT system. In the following, we describe the properties of entities in a personal space IoT system.

- *The centralized controller*

The main functions of the centralized controller in the IoT systems are to discover devices, verify their trustworthiness and admit trusted and suited devices into the system. It also monitors the interactions among admitted devices within the system and acts as a gateway to deliver collected data to a remote server. The centralized controller can be any device that is powerful enough to manage all mentioned functions such as a smartphone or a capability-comparable device. For example, a smartphone with fundamental capabilities of a mobile phone such as sending a text message, making a call, accessing to network, and extensive abilities such as device discovery, service discovery, data processing and transferring can be able to act as a gateway for the personal space IoT system.

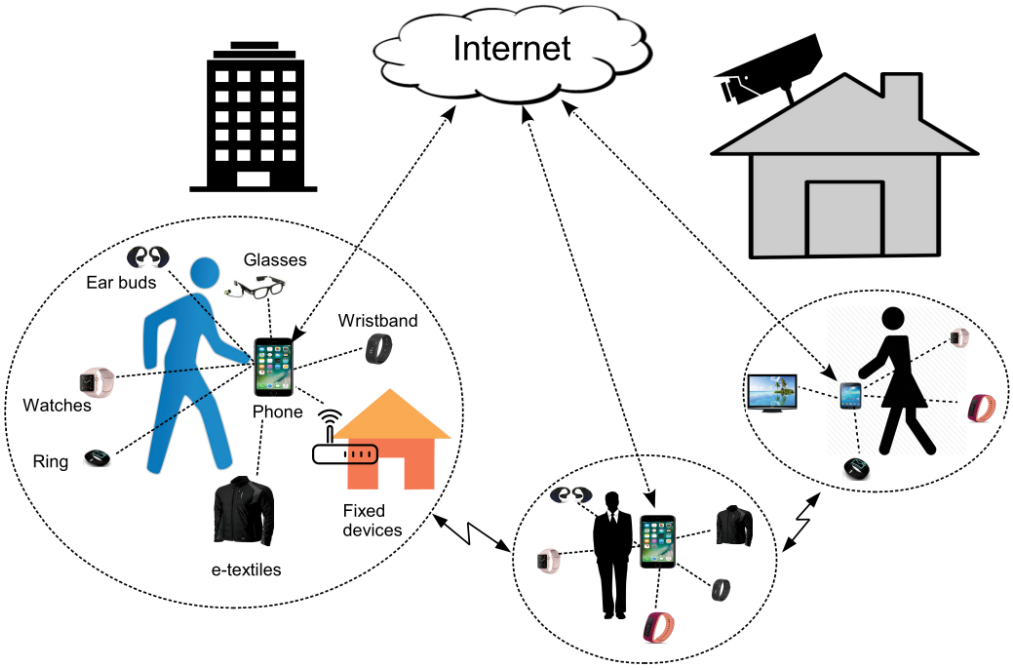


Figure 3.1 The personal space IoT environment

The built-in properties of a centralized controller include mechanisms to discover other devices, gather sensing data from personal devices, abilities to communicate with the remote server, locally store collected data, and process and transfer collected data. In addition, the controller must have capabilities of switching among various wireless communication protocols such as WiFi, Bluetooth, Zigbee, UWB, or cellular data network. The centralized controller must be able to implement new mechanisms such as relaying data to the remote server, selectively link with specific devices, and to discover the provided services of other devices. Moreover, it needs to be programmable to adapt and configure new applications and services.

In the personal space IoT system, the centralized controller represents all other admitted devices for communicating with the external environment. It is also responsible for discovering and establishing the connection with potential devices which can provide desired services or data. Moreover, it is required to be able to safeguard and protect the IoT system from being compromised for deploying attacks.

- *The user personal devices*

The user personal devices are implanted/carried by the user or operate within the radius range of the controller. Precisely, they belong to the user of the personal space IoT system. However, they still need to be verified by the controller before joining the personal space. These devices are admitted to the system after being verified during the initial trust establishment and being successfully authenticated by the controller. They are monitored by the controller and collaborate with each other to provide desired services to the user. The personal devices enable communication with each other that allows the user to access real-time data. Examples of personal devices include smartwatches, glasses, contact lenses, e-textiles and smart fabrics, headbands, beanies and caps, jewelry such as rings, bracelets, and hearing aid-like devices. The built-in properties of these devices include the ability to sense instant or variable data and transmit data to the controller in short-range connectivity. They can also communicate with each other in a peer-to-peer fashion and communicate with the controller in a client-server fashion to transmit data.

- *The external devices*

The external devices do not belong to the user of an IoT system. They might be personal devices of other IoT systems. They may be mobile or positioned at a fixed

position and can be used by any system where applicable. The external device might potentially provide useful services to a personal space IoT system. They can be admitted to a personal space IoT system to provide useful services to the user within some periods. Therefore, during the lifecycle of a personal space IoT system, the controller also discovers external devices and assesses them to decide whether to admit them into the system to make use of their potential services. It is noted that these devices can also be intruders whose interactions might harm the personal space IoT system.

3.3 Initial Trust Establishment in Personal Space IoT Systems

In the personal space IoT systems, as we add devices to our clothes, bodies, and proximity personal environment, more personal-related and sensitive information will be collected. Since those devices are capable of providing sensing as well as taking actions on our behalf, the devices' trustworthiness is of paramount importance. The major concerns in the personal space IoT system are about the integrity of the system, the provided data security and trustworthiness, the reliability of services and user's privacy. It is thus essential for the system to be confident about the integrity of its devices, the data and the quality of services they provide and be able to safeguard and manage the devices' behavior from their inception to the end of their lifecycle.

Recently, trust has been recognized as a crucial factor in enhancing the security of highly connected systems such as IoT systems [15, 70, 105]. It is noteworthy that the device's trust level used to be considered in Bluetooth classic specification to guarantee secure access control. Specifically, classic Bluetooth defines two different levels of device trust: a trusted device or untrusted device which is explicitly determined by a trust marking process. According to [71], a trusted device is the device that has been previously authenticated, knows a shared link key, and is marked as "trusted" in the initiating device's database. An untrusted device is the one that has also been previously authenticated, knows a shared link key, but is not marked as "trusted." According to [97], a trusted device has a fixed relationship with the initiating device and has full access to all services whereas an untrusted device receives restricted access to services. Thus, the

trustworthiness of the devices, their data, and offered services is a crucial concern in preserving the integrity of the system even when security control methods are implemented.

Consequently, to guarantee the integrity of the IoT system, the device's behavior must constantly be evaluated in the form of trust right from its admission to the system throughout its entire lifecycle. Preferably, the device should establish some level of initial trust before it is authenticated for admission to the system. Then, it also needs to maintain a certain trust level to the system to remain as a trustworthy member of the system.

The initial trust establishment is important in the personal space IoT system as admitted devices can access sensitive data and private services relative to the user. This requires admitted devices to be honest and cooperative with each other to provide accurate data, and high-quality and reliable services right from joining the system. A trust management model usually determines an initial trust level of an unknown device relying on some form of recommendations. It might also assign a default initial trust level on unknown devices [4]. However, based on recommendations to determine the initial trust level on a device is not always feasible for personal space IoT because of its dynamic nature where the device is unknown and encountered for the first time or its trustworthiness is no longer valid when it rejoins the space after an absence period. In addition, the default trust value assigned by a system might not be feasible due to the lack of knowledge about devices at the onset of their joining the system. Moreover, there are situations where a known device wishes to rejoin the system again, but its prior trust assessment is no longer valid as the device might have been infected while absent from the system [69]. This increases the risk of admitting malicious devices to the IoT system. Therefore, a mechanism that allows the personal space IoT system to intentionally investigate the initial trust level of devices to be admitted to the system is of paramount importance.

Existing proposed trust management models [24, 25, 106] primarily monitor the trustworthiness of entities in a system when the system is at the operational phase to detect misbehaving and malicious authenticated entities. Moreover, the proposed trust assessment methods rely on information recorded through historical experience or recommendations. These current trust assessment models are, however, not applicable

when a) such trust resources are not available, b) devices are unknown to the trust resources, and c) a known device wishes to rejoin the IoT system after an interruption, but its trust assessment is no longer valid as it may have been infected while absent from the system.

The question is that on what basis the system can rely to investigate the initial trust level of a new device if prior trust information resources are not available or no longer valid. In this thesis, to address this question, we propose a challenge-response-based initial trust establishment model that generates and gathers the trust information based on the device's responses to challenges and establishes initial trust between the controller of the personal space IoT system and new devices before they are admitted to the system.

A simple scenario about the initial trust establishment for a personal space IoT system can be a person with his/her devices forming a personal space IoT system enters a new building and wishes to use a printer to print out some documents. An initial trust establishment between the user's controller device, say a smartphone, and the printer is conducted using the challenge-response process to generate trust knowledge about the printer and assess its initial trust level. Hence, the user can decide whether to use the printer in this building. To conduct the challenge-response process to learn the printer's trustworthiness, the controller must set pre-conditions on the services it will use. The pre-conditions are used to judge the suitability and reliability of an entity to serve the controller's need. For example, the challenges are questions to check the knowledge of the printer about the controller, the conditions under that the printer serves others, and the knowledge about the service will be performed by the printer. If the printer's responses meet the pre-conditions of the controller, it will be admitted as the member of the personal space IoT system and serve the needs of the user.

In the next section, we present the overall architecture of our proposed initial trust establishment model.

3.4 Initial Trust Establishment – Overall Architecture

The goal of an initial trust establishment model is to provide mechanisms to investigate the initial trust level on devices, which have the potential to be admitted to the

personal space IoT system and provide services to the user, where prior information about those devices' trustworthiness is usually not available in the personal space environment.

This section presents the overall architecture of our proposed initial trust establishment model and provides details of each module. The proposed initial trust establishment architecture is composed of four modules. First, a *trust evidence generation module* conducts a challenge-response process at the first encounter of the device and the IoT system to generate the trust evidence for the initial trust establishment model. Second, a *trust knowledge assessment module* analyses the device's behavior throughout the challenge-response process to gain the knowledge about the trustworthiness of the device from the trust evidence generated in the previous module. Third, a *trust evaluation module* calculates the trust level that the system places on the device based on the knowledge obtained from the trust knowledge assessment module. The fourth module is a *challenge-response information design* to provide a mutual information shared between the challenge space and the response space in such a way that the challenge-response process captures relevant and meaningful trust evidence for the trust assessment process. **Figure 3.2** illustrates the overall architecture of our proposed initial trust establishment model.

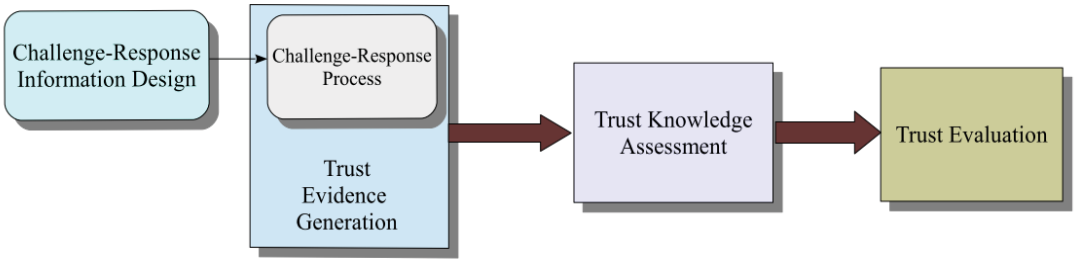


Figure 3.2 Overall architecture of the proposed initial trust establishment model

It is noteworthy that with the first three modules (trust evidence generation module, trust knowledge assessment module, and trust evaluation module), an initial trust establishment model can work under the assumption that there exists an implicit relationship between the challenges and the responses. In order to eliminate the assumption of the relationship between the challenges and the responses, the challenge-response information design module is implemented. In the challenge-response

information design, we aim to design the challenge and response information (or more precisely, the information contents of the challenge, the response and their correlation) in such the way that they fulfill the purpose of collecting meaningful knowledge for quantifying the initial trust (that is the right information about the device's behavior). If the information content of the challenges is not carefully designed from the challenger's perspective over its environment, these challenges might be entirely irrelevant to the devices in its environment.

By conducting a challenge-response process at the first encounter between the new device and the IoT system, our initial trust establishment model allows the system to generate trust evidence relative to the behavior and trustworthiness of the devices based on their responses to the challenges. The proposed initial trust establishment model does not require prior trust knowledge from historical interactions or recommendations that are usually not available at the device's first encounter with the personal space IoT system. It effectively prevents untrustworthy or maligned devices to be authenticated to the system as there is additional information of the established initial trust level to support the authentication process.

3.4.1 Trust Evidence Generation Module

This section presents the purpose and functionality of the trust evidence generation module. The core of this module is the operation of a challenge-response process. We first introduce the purpose of a challenge-response process and its operation in our proposed initial trust establishment architecture. We then review existing procedures that utilized the challenge-response concept. We also outline the differences and features of our challenge-response mechanism in the trust evidence generation module.

- **Our challenge-response process**

In our proposed architecture, we utilize the concept of challenge-response to develop a mechanism to generate trust evidence for the initial trust establishment. This section provides the design of our proposed challenge-response process. At the first encounter between a device and an IoT system, the essential information resources that existing trust assessment models rely on such as historical observations and recommendations are

usually not available. Therefore, the need of creating trust knowledge for IoT systems to assess and quantify the initial trust level of unknown devices becomes crucial. A challenge-response method has the potential for capturing the behavior of unknown devices at their first encounter with the system and hence creating the trust knowledge about these devices.

Our proposed challenge-response process consists of a sequence of challenge-response operations which are conducted within a narrow time window. In a challenge-response operation, the centralized controller (representing the system) throws out a 'challenge' requesting a 'response' from the device. The proposed challenge-response process is illustrated in **Figure 3.3**. Given the challenge-response process with a set of challenges, and a set of possible responses provided by a device, a trust assessment scheme determines the degree of trust that the system may place on the device based on information generated and gained from the challenge-response process. Various schemes for quantifying the initial trust value based on the challenge-response scheme can be applied to our proposed architecture.

Intuitively, the proposed challenge-response mechanism is a process of generating knowledge about the trustworthiness of a device by investigating its responses toward challenges. It is performed intentionally by the controller at the first encounter between a device and the IoT system. The process contains several challenges that the controller requests responses from a device before it is admitted to the system. A challenge can be a request for certain information about the personal environment. It can be an action that the device must perform to a certain satisfaction level of the system. The type of a challenge depends on the applications that the personal space supports or the operating environment of the IoT systems. Each challenge followed by response is defined as a challenge-response round. Once one round is completed, the obtained result will be combined with information from previous rounds to form the trust knowledge about the device.

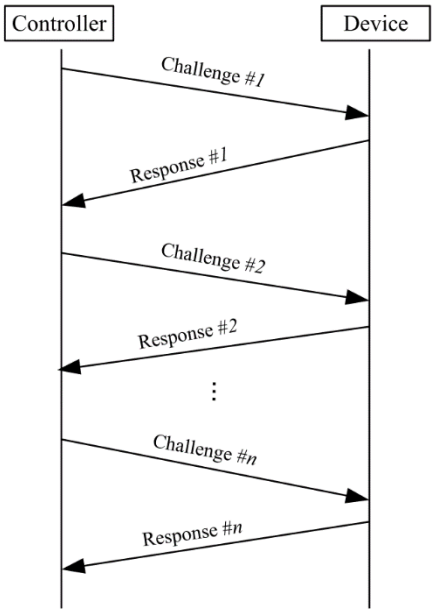


Figure 3.3 The challenge-response process in the trust evidence generation module

The challenge-response process exploits typical interactions between the controller and the devices when they encounter each other just before the conventional authentication process. For example, in a practical personal space IoT system, the controller discovers nearby devices and verifies the trustworthiness of a device that is suited to the system's requirements through possible interactions between them. The number of interactions between a device and the controller during their first encounter depends on the underlying communication technology used by the devices such as Bluetooth Low Energy protocol as indicated in [107].

- **Challenge-response process in related work**

It is worth noting that the challenge-response scheme has been widely used in various existing authentication approaches [108-112] where a party must provide a 'valid' response to a challenge from another party to be authenticated. For example, in computer security, the Salted Challenge Response Authentication Mechanism (SCRAM) is a set of password-based challenge-response authentication schemes to authenticate a user to an Internet service provider [113]. Challenge-response protocols are also used to verify things other than knowledge of a shared secret value. For example, CAPTCHAs (Completely Automated Public Turing test to tell Computers and Humans Apart) [114]

are methods to determine whether a web user is a real person. Specifically, the challenge sent to the user is a distorted image of some text, and the viewer must respond by typing the exact displayed text into the server to be authenticated as a human. In [115] a real-time captcha-based user authentication model is proposed where the user is required to provide an audible captcha response to the challenge. The audio captcha response is verified if it matches the sent captcha. The user's voice and face samples are captured and sent to the server for authentication. In addition, the delay until the user starts recording the audio response is verified as a criterion for the authentication. The limitation of this method is that it requires an audible response which could not be usable in some certain cases such as for disabled people.

In wireless networks, the authentication at the physical layer is usually based on a challenge-response mechanism. For example, in [112] a physical layer challenge-response authentication mechanism (PHY-CRAM) for single-hop communications is proposed. The basic idea of PHY-CRAM is to use a random number and channel fading to mask the authentication key and exploit channel reciprocity to cancel out the channel effect using inverse operations such that the verifier can decode the secret without knowing the channel state information.

In [108], an extension of PHY-CRAM, a physical layer challenge-response authentication mechanism with the relay is proposed for two-hop wireless networks involving a trusted relay. It fully utilizes the randomness, reciprocity, and location decorrelation features of the wireless fading channel to hide/encrypt the challenge and response messages at the physical layer and is immune to outside attacks with a trusted relay. The common feature of proposed challenge-response authentication methods in [108] and [112] is the need of a shared secret between the verifier and the prover. In contrast, our purpose of using a challenge-response mechanism is to learn the behavior of the entities towards challenges without requiring a known secret.

In [109], Gao et al. proposed an Obfuscated-Physical Unclonable Function (OB-PUF) in which the verifier sends a partial challenge to the OB-PUF (i.e., the prover). Subsequently, within an OB-PUF, a partial challenge is padded with a random pattern generated by a random number generator to make up a full-length challenge. However, this method is time-consuming as it must run the matching algorithm on the verifier side.

In summary, in existing challenge-response-based authentication schemes, the valid response can only be generated by using an algorithm or a secret shared between both parties. On the contrary, our challenge-response process aims at generating the trust knowledge about entities which encounter the system for the first time or attempt to rejoin the system after some interruptions. It does not require a shared secret or a known algorithm between the challenger and the responder for generating a response towards a challenge. Our challenge-response process accepts different responses and determines the relevance of a response to the expectation of the challenger. We investigate trust evidence as the number of times that the device satisfies a certain criterion set by the challenger. The output of this module is the trust evidence capturing the device's behavior. The trust knowledge about the responder will be assessed and obtained through the trust knowledge assessment module.

3.4.2 Trust Knowledge Assessment Module

The purpose of the trust knowledge assessment module is to assess the evidence obtained from the *trust evidence generation module* to gain the knowledge about the device's trustworthiness. The idea of this module is based on the fundamental understanding of trust – trust is a function of uncertainty. Specifically, when the system is totally uncertain about how the device will behave in the future, it has maximum uncertainty in the device's behavior. In this case, the system is not able to determine to trust or distrust the device. In other words, a neutral trust is given to the device. When the system is certain about how the device shall behave in the future, it has minimum uncertainty in the device's behavior. In this case, if the system is certain that the device will act as the system's expectation, a trust level should be given to that device. Otherwise, a distrust level should be given to devices that will not behave in the way that the system is expecting. Therefore, we obtain the trust knowledge from generated evidence by measuring the uncertainty that the system has about the device's behavior. **Figure 3.4** illustrates the inputs, outputs, and functionality of this module.

Information theory states that entropy is a natural measure of uncertainty. In our solution, we determine the uncertainty related to trust via entropy. The measure of entropy

is based on a probability. Therefore, to work out the uncertainty that the system has about a device, we estimate the probability that the device is willing to provide an expected response to the challenge in the future based on the trust evidence generated via the challenge-response process in the trust evidence generation module. This probability is associated with the uncertainty that the system has about a device's behavior. Thus, the main function of this module is to determine the probability associated with the uncertainty and calculate the uncertainty that the system has about the device's behavior based on this probability.

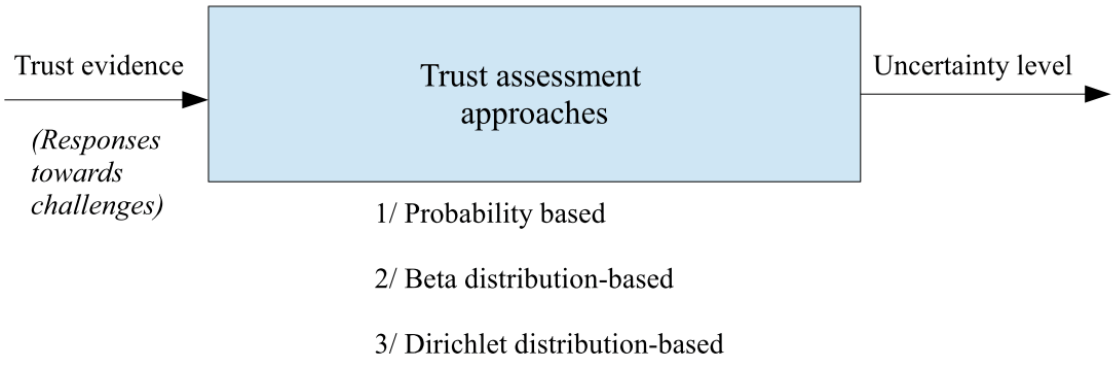


Figure 3.4 Trust knowledge assessment module

Several mathematical models can be used in this module to determine the probability associated with the uncertainty that the system has about the device's behavior. This thesis proposes three different mechanisms to assess the trust knowledge on the device based on the generated trust evidence. Each mechanism is integrated to an initial trust establishment model that will be presented in following chapters.

In the first model, the trust knowledge about a device is measured in the form of uncertainty (measured by the entropy). In order to measure how much uncertainty that the system has about the device's behavior, we estimate a probability associated with this uncertainty. The associated probability is modeled as a function of two probabilities: the probability that the expected response is returned by the device and the probability that the device is an intended device of the IoT system conditioned on its response. The detail of the probability-based initial trust establishment model will be presented in chapter 4.

In the second model, to improve the accuracy of estimating the uncertainty that the system has about the device's behavior, we came up with the idea of using the *probability distribution*. We adopt the Bayesian inference as for the mathematical foundation for assessing the trust knowledge about the devices based on the evidence generated from the challenge-response process. We consider the probability associated with the uncertainty that the system has about the device is a random variable. This model addresses the trust knowledge about a device obtained from a binary evidence set, i.e., the trust evidence is determined from a binary outcome set. The probability associated with the uncertainty that the system has about the device's behavior has a Beta distribution. As this is a probability random variable, the mean of its distribution is then used as the probability associated with the uncertainty that the system has about the device's behavior. The details of an initial trust establishment model that uses this mathematical model will be presented in chapter 5.

In the third model, we deal with the trust knowledge gained from a multi-component evidence set. We consider that the probability associated with the uncertainty that the system has about the device is a multi-component random variable has a Dirichlet distribution. The Bayesian inference adopts the Dirichlet distribution to assess the evidence and extract trust knowledge about the device. The mean of this distribution is then used as the probability associated with the uncertainty that the system has about the device's behavior. The details of an initial trust establishment model based on this mathematical model will be described in chapter 6.

3.4.3 Trust Evaluation Module

The purpose of the trust evaluation module is to calculate the trust level that the system places on a device based on the trust knowledge gained from the trust knowledge assessment module. It simply provides the means for interpreting the obtained knowledge to a trust level. In our initial trust establishment model, the scale of trust level is [-1, 1) where the value of 1 is exclusive since we accept the idea that an entity never places an absolute trust on another. **Figure 3.5** illustrates the inputs, outputs, and functionality of this module.

This module interprets the amount of uncertainty that the system has about a device into a trust level. A device might be considered as a completely distrusted device and unlikely to be involved in any further interactions when it is given an initial trust value of -1 by the system after the trust evaluation module. A device might be viewed as a more distrusted or less distrusted device when the system determines an initial trust value is within -1 or 0. In contrast, a device is supposed to be a more trusted or less trusted device if the system places an established initial trust value within the range of (0, 1) on the device. We define a neutral trust value in the trust scale to mean that the system is at the position of not trust or not distrust a device due to the lack of information that a decision on trust or distrust can be made.

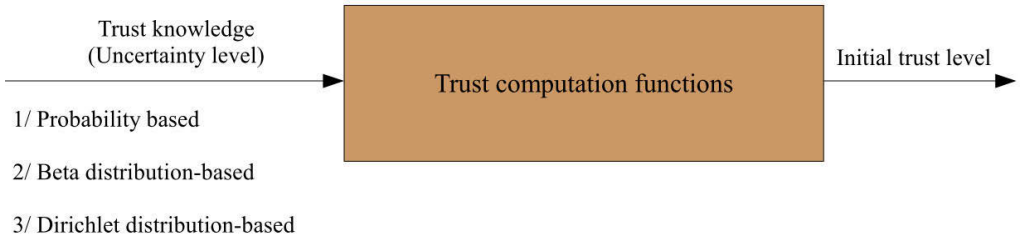


Figure 3.5 Trust evaluation module

Note that all modules in our architecture are conducted in parallel with the challenge-response process. Therefore, we define two metrics of trust during the initial trust establishment of the personal space IoT. One of the metrics is called "*instant trust*" which refers to the trust value learned from a single challenge-response round. At the end of each challenge-response round, the trust knowledge is updated, and then the trust evaluation module can determine the instant trust value. The other metric is the "*aggregated initial trust*" which is updated when more trust knowledge is available over the initial trust establishment. The initial trust value that the personal space IoT system places on a device after conducting the initial trust establishment model is the final aggregated initial trust value updated from the first to the final challenge-response round. For each method implemented in the trust knowledge assessment module, there is a method for interpreting the trust knowledge to a trust level accordingly.

3.4.4 Challenge-Response Information Design Module

Clearly, when two parties have no prior knowledge about each other, and no third party can make any recommendation, it is impossible to establish a trusted relationship between them under such circumstances. The challenge-response process proposed in this thesis aims to create a common pool of knowledge between the two parties. As such, the challenger and the responder must implicitly share some knowledge for the trust assessment process to work. Without such implicit information sharing, very little knowledge about each other's trustworthiness can be gained from the challenge-response operations.

The question is how to engineer the shared information between the challenger and the responder through the challenge-response operations. To address this question, we propose a challenge-response information design to provide an information space from the challenger's perspective over its environment that is used to conduct the challenge-response process to determine if there exists mutual information between itself and its responder as the basis for trust evaluation.

The proposed information design of the challenge-response process is inspired by the "mechanism design" in game theory where a designer designs a mechanism through which the gets the players play strategies that end up implementing exactly what he/she intended [116]. Precisely, each player plays its strategies to gain maximum reward. However, the strategies that the player chooses are in fact guided by the design of the game. In other words, the designer is interested in how to design the game using information contents to get what he/she wants rather than how best to play the game.

Intuitively, the challenge must be designed in such a way that it invites relevant responses that satisfy the aim of the challenge-response process to decide whether to trust the responder (the device). Therefore, there must exist an implicit underlying relationship/correlation between the information content of the challenge and the response. Our proposed challenge-response information design carefully determines feasible challenge and response distributions to achieve meaningful shared information as the basis for a consistent initial trust assessment.

The aim of the challenge-response process is to judge the trustworthiness of an IoT device that may become a member of a personal space IoT system. To achieve this aim, our challenge-response information design considers the intention of the challenges and the relationship between the information content of the challenges and potential responses. The designed challenges intend to invite responses from the responders in the target environment that fit into the challenger's environment and share mutual information with the challenge so that there exists the meaningful and relevant knowledge for the challenger to judge the responders' trustworthiness.

The proposed challenge-response information design ensures that the challenges are relevant to the target population so that the challenger receives related responses connecting to the challenger's environment. Thus, the design of the information content of the challenges is critical. Furthermore, the design of challenges must gain more insight into the respondents' trustworthiness based on the shared knowledge between the responder and the challenger. Therefore, the relation between the challenges and the responses need to be carefully designed. The details of the proposed information design for the challenge-response process in our initial trust establishment architecture will be presented in chapter 7.

3.5 Realization of the Proposed Initial Trust Establishment Model

The proposed initial trust establishment model conducts challenge-response operations for generating the knowledge related to the devices' initial trustworthiness within a limited time window during their first encounter. In practice, the proposed model requires a mechanism to carry the challenge and response information for the trust assessment process to work. Specifically, the proposed model has to be realized through interactions between devices when they encounter each other. There are two main questions to realize the feasibility and efficiency of the proposed initial trust establishment model. First, is it possible to generate trust evidence through the challenge-response process and how to achieve the challenge and response information? Second, if the challenge-response process can be performed by utilizing possible interactions

between devices at their first encounter, can it be done within a limited time window and with practical processing delay and communication overhead? Therefore, it is crucial to demonstrate the feasibility and efficiency of our proposed initial trust establishment model over an existing communication protocol.

Bluetooth Low Energy communication protocol has been widely used in IoT systems especially in a personal environment. BLE devices start their connections from the device discovery phase to a normal connection establishment and then to a secure connection establishment via a pairing process if needed. The communications between two devices when they encounter each other include several interactions that exchange information in plain text. We investigate the challenge-response operations through the typical interactions between BLE devices. We propose and demonstrate our solution by designing and implementing a new initial trust-aware protocol over the existing BLE protocol, the "initial trust-aware BLE protocol". The protocol design, the detailed implementation and performance evaluation of the initial trust-aware BLE protocol will be presented in chapter 8.

3.6 Roadmap

It is worth noting that this chapter provides the overall architecture of our novel initial trust establishment model proposed for personal space IoT system. In order to generate the evidence about the trustworthiness of new devices, our initial trust establishment model conducts a challenge-response process to collect device's responses to the challenges which capture the device behavior. This task is done in the first module of the architecture – *trust evidence generation module*.

For the second module – *trust knowledge assessment module*, various mathematical models can be used to investigate the trust knowledge from the evidence learned from the challenge-response process. In this thesis, we introduce three different trust assessment models to investigate the trust evidence based on three different settings of the knowledge related to the investigated evidence. For the third module – *trust evaluation module*, three different trust evaluation methods are introduced to interpret the trust knowledge to an initial trust level that the system places on the new device.

Three discussed modules provide the process to generate the trust evidence, assess the evidence to gain trust knowledge and calculate a trust level from the achieved knowledge. The outcomes from the challenge-response process for generating trust evidence are assumed to be meaningful for these three modules to work. However, the challenges need to be carefully designed in order to invite relevant responses from the possible respondents in the environment so that the proposed initial trust model can capture meaningful information to judge the device's trustworthiness. Therefore, the fourth module – *challenge-response information design*, is crucial for an initial trust establishment model to work in practice without requiring the assumption of the given outcomes from the challenge-response process.

The roadmap of the rest of this thesis is organized as below.

In chapters 4, 5 and 6, we describe the design and operation of three initial trust establishment models respectively to three different trust assessment approaches. These models work under the assumption that the relationship between the challenge and each possible response is given and challenges are relevant to the environment so that the device has some knowledge about the challenges. Therefore, the challenge-response information design will not be implemented in these models.

In chapter 7, we describe the challenge-response information design to determine the feasible design of the information content of the challenges and the design of the relationship between the possible responses and challenges so that the initial trust establishment model can work without requiring the assumption of a given relationship between the challenges and responses. The evaluation of the initial trust establishment deployed with the challenge-response information design is comprehensively discussed.

It is critical to demonstrate the feasibility and efficiency of the proposed initial trust establishment model in practice. Thus, in chapter 8, we present the protocol design and implementation of the initial trust-aware BLE protocol which is the practical implementation of the proposed initial trust establishment model over the existing BLE protocol. We demonstrate the feasibility and efficiency of the initial trust-aware BLE protocol for personal space IoT systems through extensive simulations.

3.7 Summary

This chapter provided the overall architecture of our new initial trust establishment model for personal space IoT systems and showed a roadmap of the thesis. We first presented our new definition of a personal space IoT environment and identified the necessity of an initial trust establishment model for building a trustworthy personal space IoT system. We then described the overall architecture of the proposed initial trust establishment model and explained the functionality and significance of each module in the overall architecture. We discussed the realization of the proposed initial trust establishment model and introduced the design and implementation of the new initial trust-aware BLE protocol for demonstrating the feasibility and efficiency of the proposed initial trust establishment model in practice. A roadmap of the thesis is included at the end of the chapter.

Chapter 4

Probability-based Initial Trust Establishment Model for Personal Space IoT systems

4.1 Introduction

The cooperation among devices in a personal space IoT environment often requires reliable and trusted participating members in order to provide useful services to the end user. Consequently, a personal space IoT system needs to evaluate the initial trust level of all devices before admitting them as members of the system. As discussed in chapter 2, existing trust assessment models are based on historical observations and recommendations to evaluate the trust level of a device during the operational phase of the system. However, at the device admission phase of an IoT system, the system has no experience on the new device since there are no interactions in the past; the third parties are not able to make a recommendation due to the lack of information about the device or dynamic changes in the environment. In such situations, the existing trust models fail to investigate an initial trust value of a device because of the lack of trust resources. Therefore, in order to establish an initial trust level between the IoT system and a device, a new initial trust establishment model is critical.

In chapter 3, the overall architecture of our proposed initial trust establishment model is presented. In this chapter, based on the overall architecture we will present a

probability-based initial trust establishment model. We assess the trust knowledge about the device based on a probability associated with the uncertainty that the system has about the device's behavior. This probability is estimated based on the evidence captured from the challenge-response process. The evidence is related to a probability that a certain response will be returned by the device and a probability value that expresses the belief of whether the device is an intended device to the system, i.e., a device that can cooperate with other devices to provide reliable data and high-quality services for the user of the IoT system. The proposed design and findings from this work have been published in [117].

The rest of this chapter is organized as follow. Section 4.2 presents the detail of each module in the probability-based initial trust establishment model based on the overall architecture presented in chapter 3. Section 4.3 gives the experimental evaluation of the proposed model and discusses the numerical results of the evaluation. Finally, section 4.4 concludes the chapter.

4.2 Probability-based Initial Trust Establishment Model

This section provides detail of our probability-based initial trust establishment model. The description of each module is presented according to the overall architecture of our proposed initial trust establishment model. We employ the one-to-one relationship between the probability associated with the uncertainty that the system has about the device's behavior and the trust level to investigate the initial trust level that the system places on a device.

4.2.1 Trust Evidence Generation Module

In this module, a challenge-response process is the means for generating the trust evidence about the trustworthiness of a device which potentially becomes a member of the personal space IoT system. The challenge-response process will be conducted at the device admission phase of the IoT system where the device encounters the controller and wants to join the system, and the system will decide if it admit the device as a member of the system.

Generally, a trust relationship between two entities can be expressed as [*Subject: Agent, Action*] whereby the subject is the entity that performs the trust evaluation, and the agent is the entity that trust is evaluated on its actions. In our initial trust establishment model, the controller plays the role of the *subject* while the device under the trust assessment is the *agent*. Particularly, the controller on behalf of the IoT system performs the initial trust evaluation on devices that want to join the system regarding how the devices react to the challenges initiated by the controller. The initial trust relationship between the personal space IoT system and a device is expressed as [*Controller: Device, Respond to the challenge*].

Any device will be verified by the controller with a number of challenges to learn the device's trustworthiness. The device is required to respond to the challenges in such a way that its responses satisfy the controller's expectation. Each challenge followed by a response is considered as a challenge-response round of the trust evidence generation module. In each round, the fact that the response returned by the device can be accepted by the controller or not depends on whether it satisfies the controller's expectation. The controller evaluates the device's response to determine whether it satisfies the challenge.

The output of this module is the trust evidence indicating how the device respond to the challenges. The evidence is then used as the input of the *trust knowledge assessment module*.

4.2.2 Probability-based Trust Knowledge Assessment Module

In this section, we present the operations of the trust knowledge assessment module in the probability-based initial trust establishment model. We describe the measurement of the uncertainty that the system has about the device's behavior based on the evidence that is captured from the trust evidence generation module.

During the challenge-response process in the trust evidence generation module, after each challenge-response round is completed, the controller can measure how much uncertainty that it has about the device's behavior. Over the trust evidence generation module, the controller gradually learns more about the device's behavior. Here, the trust

knowledge is how much uncertainty that the controller has about the device's behavior after evaluating its responses to the challenges.

In this approach, we define the probability associated with the uncertainty that the system has about the device's behavior as the probability that an intended device provides expected responses to the challenges. In fact, the controller may trust in the context of a given response to a certain degree. Meanwhile, the device which provided a given response may or may not be an intended device for the IoT system, i.e., a device that suits the system's needs and is likely to provide reliable and useful services.

Consequently, the probability associated with the uncertainty that the system has about the device's behavior is calculated from two parameters: the probability that the controller trusts a given response, and the probability that the device that provided the given response is an intended device for the IoT system. Specifically, the first parameter considers how much the controller trusts in the context of a given response. The second parameter considers the probability that the device is an intended device for the system given that it provided an expected response or an unexpected response. If the device's response is an expected response to the controller, it is more likely that the device is an intended device for the IoT system. Otherwise, if the device's response does not satisfy the expectation of the controller about a specific challenge, it is more likely that the device is not an intended device for the system.

Now we describe how the probability associated with the uncertainty that the controller has about a device is calculated. Let p_{CR_i} denote the probability that the controller trusts a given response R_i (the first defined parameter). As a device that returns a response (say R_i) can be an intended response to the IoT system or not, we learned the probability that a device is an intended one given that it returned R_i to the challenge i^{th}. Thus, we denote p_{DR_i} as the probability that the device is considered as an intended device for the system at the i^{th} response (the second defined parameter). In addition, we learn the device's behavior via the probability that it provides an expected response to the controller. Therefore, we also denote p_{R_i} as the probability that the device's response R_i is expected, $p_{D|R_i=1}$ as the probability that the device is an intended device given its

response is an expected response, and $p_{D|R_i=0}$ as the probability that the device is an intended device given its response is an unexpected response. Then, the probability associated with the uncertainty level that the controller has on a specific device's behavior p_{CD} can be determined as below

$$p_{CD} = p_{R_i} p_{D|R_i=1} + (1 - p_{R_i}) p_{D|R_i=0} \quad (4.1).$$

The principle of calculating p_{CD} can be explained as follow. When a device returns a response to a given challenge, there are a probability of p_{R_i} that the response is an expected response and a probability of $(1 - p_{R_i})$ that the response is an unexpected response. If the response is an expected one to the challenge, there is a conditional probability of $p_{D|R_i=1}$ that the device is considered as an intended device of the IoT system. Otherwise, when the response is an expected one, there is a conditional probability of $p_{D|R_i=0}$ that the device is still considered as an intended one of the IoT system. As the outcome of the response's evaluation performed by the controller is either an expected response or an unexpected response, it is reasonable to combine the two related outcomes into the calculation of p_{CD} . When one outcome happens, the other one will not happen. Therefore, the calculation of p_{CD} is based on the two defined probabilities.

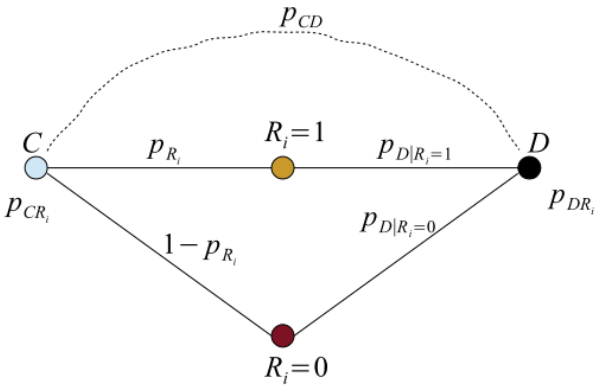


Figure 4.1 Calculation of the probability associated with the uncertainty

As the controller can evaluate the device's response, it is reasonable for the controller to assume that $p_{R_i} = p_{CR_i}$ and $p_{D|R_i=1} = p_{DR_i}$. In addition, if a device provides an unexpected response, there is a low probability that it is an intended device for the system. Thus, we can calculate $p_{D|R_i=0}$ by subtracting $p_{D|R_i=1}$ from 1. Consequently, (4.1) becomes

$$p_{CD} = p_{CR_i} p_{DR_i} + (1 - p_{CR_i})(1 - p_{DR_i}) \quad (4.2).$$

Figure 4.1 illustrates the relationship among probabilities in calculating the probability associated with the uncertainty that the controller has about the device, p_{CD}.

The probability p_{CD} is then used to measure the uncertainty that the system has about the device's behavior. We measure the uncertainty that the system has about the device's behavior by using the Shannon entropy [98] as below.

$$H(p_{CD}) = -p_{CD} \log_2 p_{CD} - (1 - p_{CD}) \log_2 (1 - p_{CD}) \quad (4.3)$$

By interpreting the uncertainty to the trust value through entropy, the controller will be able to decide to trust or distrust the device to a specific trust degree. We propose a trust evaluation method in the next section.

4.2.3 Initial Trust Evaluation Module

This module is responsible for interpreting the trust knowledge about the device into an initial trust level. Specifically, in the probability-based initial trust establishment model, we interpret the uncertainty that the controller has about the device's behavior as a trust level that the controller places on the device.

The idea behind the proposed initial trust establishment model is to reduce the uncertainty that the controller has about the device's behavior of which the controller has no prior knowledge at the beginning of the assessment. By conducting the trust knowledge assessment module, the controller learns more about the device's behavior

and trustworthiness and gradually updates its uncertainty level about the device's behavior. Thus, it is able to determine the initial trust value of the device by transferring the uncertainty level to a trust value. The uncertainty measured from the associated probability via entropy function will be then interpreted as the trust value in the trust evaluation module. The measurement and interpretation processes are performed at the end of each challenge-response round and continuously over the challenge-response process to determine the initial trust value of the device.

The mapping between the uncertainty and the trust value regarding the associated probability of the uncertainty is a one-to-one process. If there is a high probability that the device provides an expected response to the controller, a low uncertainty level is expected, and it is more likely that the device will be trusted. In contrast, when this probability is very low, a low uncertainty might be expected, but it is more likely that the device will be distrusted. The higher the probability, the more trust the controller places on the device.

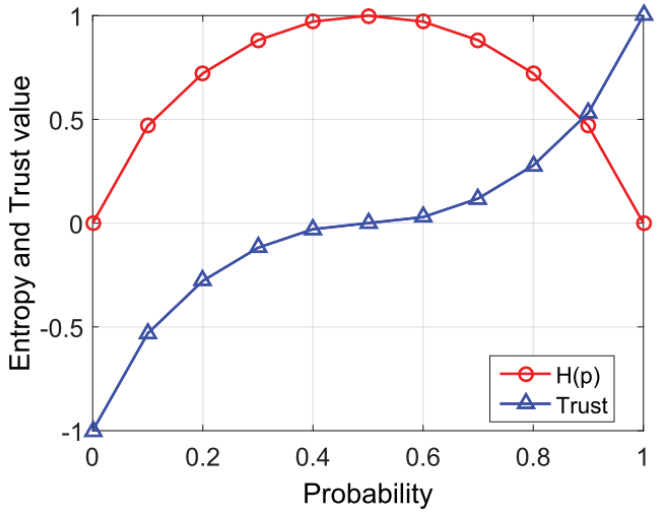


Figure 4.2 Mapping of entropy and trust level with the associated probability

The trust value is depicted as a real number in the [-1, 1) interval whereby it ranges from a complete distrust over neutral trust measure to a near full trust as shown in **Figure 4.2**. In fact, the trust is an increasing function of the probability. Specifically, the trust value is increased when the probability is increasing from 0 to 1. However, the entropy is a symmetric function of probability. It is a non-negative quantity, and it reaches a

maximum value at 1 when the probability is 0.5, minimum value at 0 when the probability is at 0 or 1.

Specifically, the maximum value of the entropy implies the highest uncertainty of the device so that the controller cannot decide to trust or distrust the device. Therefore, the trust value is a neutral trust measure and is interpreted to 0. On the side with probabilities lower than 0.5, the uncertainty of the device reduces with the lower probability. It reaches 0 at the probability of 0, and obviously, it is certain that the device will not provide an expected response. Thus, the trust value should be translated to -1 which refers to a complete distrust opinion of the controller. Likewise, on the opposite side, the uncertainty reduces when the probabilities are increasing from 0.5 to 1. It reaches 0 at the probability of 1. This implies that it is certain that the device will provide an expected response. Therefore, the trust value should be interpreted to near 1 which refers to a nearly full trust opinion of the controller on the device but not an absolute trust value. **Figure 4.2** shows the entropy and the trust value as functions of the probability.

In order to interpret the entropy value to the trust value, (4.4) is used since it satisfies all the requirements of the trust value translation.

$$\tau = \begin{cases} 1 - H(p_{CD}), if\ 0.5 \le p_{CD} \le 1 \\ H(p_{CD}) - 1, if\ 0 \le p_{CD} < 0.5 \end{cases} \tag{4.4}$$

During the initial trust establishment, an instant trust value is measured after each challenge-response round. The initial trust value is aggregated up to the last challenge-response round by combining the previous trust values with the latest trust value.

$$T^i = (1 - w_i)T^{i-1} + w_i\tau_i \tag{4.5}$$

where, T^i is the initial trust aggregating after *i* rounds and τ_i is the instant trust from the i^{th} round, respectively; w_i is the weight for the instant trust achieved from the current round (the i^{th} round).

The weights allow us to take into account various considerations such as the environment in which the personal space IoT system operates and the emphasis of different rounds of the challenge-response process. Intuitively, the weights w_i are used

to vary the contribution of the latest knowledge to the overall knowledge that the system learned about the device throughout the challenge-response process. In practice, the weights value can be determined based on the timeliness of the challenge-response rounds. For example, the instant trust value obtained from a single challenge-response round may weigh more than that from the previous challenge-response rounds to reflect the degree of knowledge gained through the assessment process.

In practice, the device which provides an expected response may not be an intended device. On the other hand, the device which provides an unexpected response may not be a malicious intruder as the device may make mistakes during the trust assessment procedure. Our initial trust establishment model offers chances for a device to recover and improve its initial trust value by challenging the devices in several challenge-response rounds. However, the initial trust establishment stops when a device continuously returns unexpected responses to the challenger as the initial trust level of the device is lower than a given distrust threshold or the allocated time is expired.

4.3 Experimental Evaluation

In this section, we present the experimental setup and discuss the obtained results with the proposed probability-based initial trust establishment model.

4.3.1 Simulation Setup

We conduct simulations to investigate how our initial trust establishment model works in a personal space IoT system. Initially, the controller on behalf of the system discovers devices within the space and performs the initial trust establishment with discovered devices which potentially provide desired services to the IoT system. Every new device is verified by the controller via challenge-response operations before being admitted to the system.

In a challenge-response operation, the controller decides if the device's response satisfies the expectation of the system based on a relationship between the challenge and the response. In this approach, the relationship between a challenge and a possible response has been assumed. Precisely, it is assumed that there is a relationship between a

received response and the corresponding challenge. This relationship refers to how much the response correlates to the challenge. With a given response, the assumed relationship is used to determine if the device's response satisfies the system's expectation.

We assume that a device is considered as an intended device to the system when it returns a response to the corresponding challenge with a probability value assigned by the controller. The probability that the device is considered as an intended device to the system will be assigned by the controller according to which device's response is provided. The device that provides an expected response is more likely to be trusted as an intended device to the system. In contrast, the device that returns an unexpected response is much less likely to be trusted as an intended device. Specifically, the assigned probability is increased when an expected response follows another expected response. It will be decreased if an unexpected response follows another unexpected response. Our experiments focus mainly on the feasibility and consistency of the proposed initial trust establishment scheme. Therefore, in the experiments, we assume 0.98 as the probability that the controller trusts the response, 0.9 or greater is the probability that a device is an intended device conditioned on an expected response. The weight assigned to the instant trust level obtained from the latest challenge-response round is 0.6. The distrust and trust thresholds with which the initial trust establishment stops are -0.8 and 0.8, respectively.

4.3.2 Numerical Results

- **Experiment 1:**

In the first experiment, we conduct an initial trust assessment between the personal space IoT system and a device within a 2-round challenge-response process. We simulate four different cases in this experiment in regard to four different device's behavior patterns. In the first simulation, a device under the trust assessment provides both expected responses (it is considered as a benign device) to the challenges. In the second simulation, a device provides an expected response at the first round and an unexpected response at the second round. The third simulation considers a device which provides an unexpected response at the first round and an expected response at the second round. In the last simulation, a device provides both unexpected responses to the challenges.

We investigate the uncertainty that the system has about the device's behavior measured from the trust knowledge assessment module, the instant trust value that the controller places on the device after each challenge-response round and the aggregated initial trust value from the initial trust establishment. The initial trust that the system places on a new device based on the trust knowledge assessment is the trust value aggregated from all the challenge-response rounds. The following figures show the entropy, the instant trust value computed after each challenge-response round, and the initial trust value which is aggregated from challenge-response rounds.

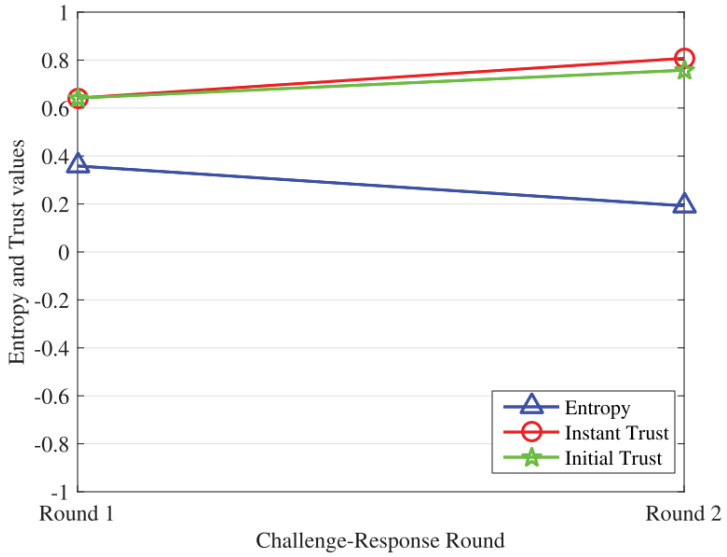


Figure 4.3 Experiment1: Entropy and Trust values from the initial trust establishment on a device provides two expected responses to the challenges

Figure 4.3 shows the investigated values from the initial trust establishment between the system and a device which provided expected responses in both rounds. We can see that the uncertainty level that the system has about the device (the entropy) decreases over the challenge-response process. Specifically, the entropy is about 0.37 after the first round. It then drops to 0.2 after the second round. Due to the decreasing in the entropy, i.e., the uncertainty that the system has about the device's behavior is reduced over the challenge-response process, the instant trust value computed after each challenge-response round increases from 0.64 to 0.80 accordingly. It is noted that in our approach, the device's response from the latest round is considered as more important than the one

from the previous rounds. The uncertainty measured from the latest round contributes more to the initial trust calculation. Therefore, the initial trust value aggregated from two rounds is 0.74.

Figure 4.4 presents the results from the second simulation where we simulated the initial trust establishment between the system and a device which provides an expected response to the first challenge-response round and unexpected response to the second round. The numerical results indicate that the uncertainty that the system has about the device's behavior (the entropy) decreases over the challenge-response process. It is expected that a more trust or a more distrust level should be interpreted from the reduction in the uncertainty level of the system about the device. In the first round, since the device provides the expected response to the challenge, the instant trust level interpreted from the uncertainty expresses a trust opinion. However, as the device provides an unexpected response to the second round, the instant trust value computed in this round expresses a distrust opinion. The aggregated initial trust value is degraded over the challenge-response process. It expresses a distrust opinion as the device provides an unexpected response to the second challenge which takes more weight than that of the first challenge. Specifically, the instant trust computed from the second round contributes more to the aggregated initial trust calculation. As a result, the system places a distrust amount of -0.2 on this device.

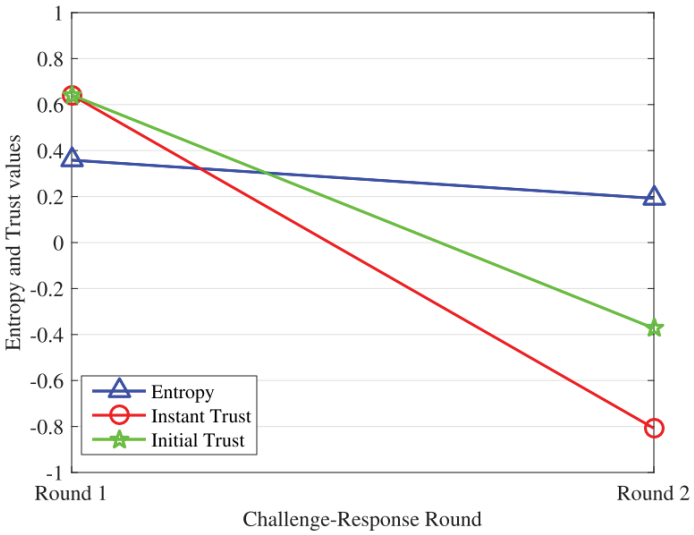


Figure 4.4 Experiment 1: Entropy and Trust values from the initial trust establishment on a device provides an expected response followed by an unexpected response

The results from the third simulation, where the device provided an unexpected response to the first challenge and an expected response to the second challenge, are indicated in **Figure 4.5**. As shown in the figure, the uncertainty that the system has about the device (the entropy) reduces over the challenge-response process as the system knows more about the device's behavior. The results indicate that the instant trust value calculated from the first round is a distrust value due to the unexpected response of the device to the first challenge. The system then places a trust value on the device according to its expected response to the second challenge. Accordingly, the aggregated initial trust value is recovered from a distrust to a trust opinion since the device provides an expected response at the second round. In summary, the initial trust value that the system places on the device is about 0.2 which expresses a trust opinion.

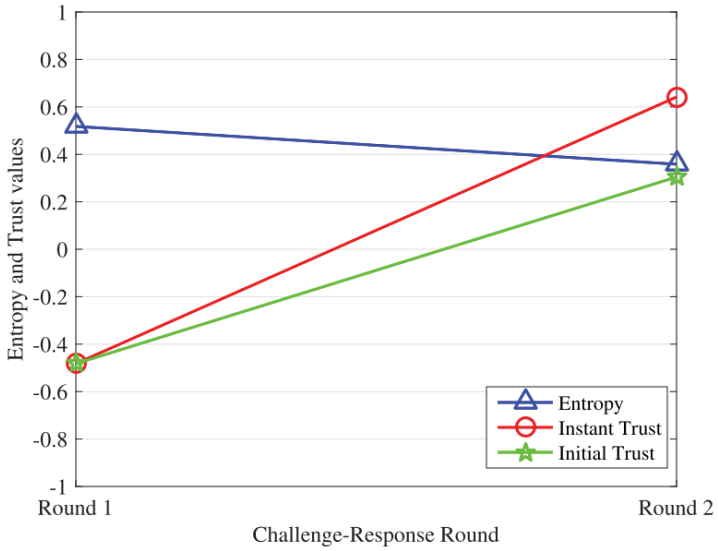


Figure 4.5 Experiment 1: Entropy and Trust values from the initial trust establishment on a device provides an unexpected response followed by an expected response

Figure 4.6 shows the numerical results from the last simulation, where an initial trust establishment between the IoT system and a device that provides unexpected responses to both challenge-response rounds is simulated. We can see that the entropy is reduced over the challenge-response process. Since the device provides unexpected responses to both challenge-response rounds, the uncertainty that the system has about the device's

trustworthiness reduces, and the probability that the device will return an expected response to the challenge is less than 0.5. Therefore, the instant trust calculated at each challenge-response round is a distrust amount accordingly. The system places a more instant distrust value on the device in the second round as the device is more likely to provide an unexpected response in the future. The initial trust value that the system places on the device in this simulation is around -0.7 that expresses a distrust opinion.

It is interesting to discuss the characteristics of the aggregated initial trust value. It is a weighted combination of instant trust values from all challenge-response rounds. Specifically, the aggregated initial trust value that the system places on a device is increased when the device consistently provides expected responses to the challenges. In contrast, it is reduced when the device continuously provides unexpected responses to the challenges.

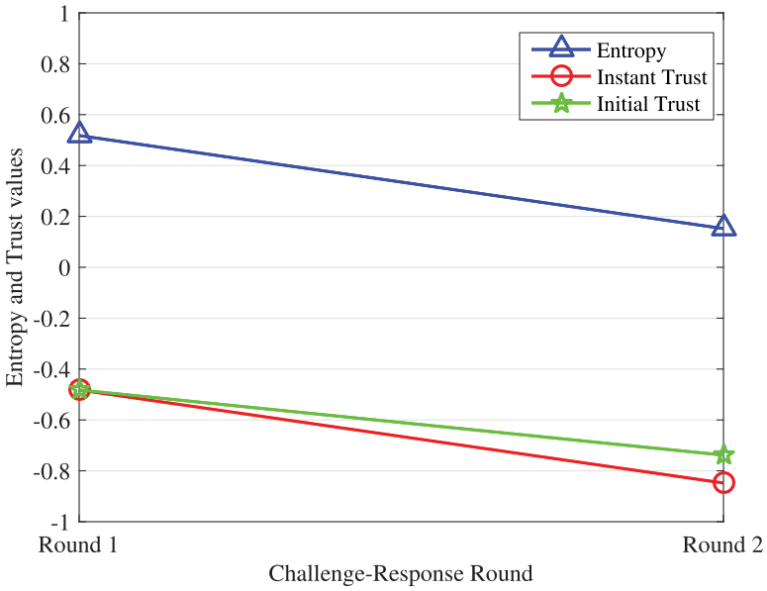


Figure 4.6 Experiment 1: Entropy and Trust values from the initial trust establishment on a device that provided two unexpected responses to the challenges

- **Experiment 2:**

In order to investigate the effect of trust thresholds in the initial trust establishment procedure, we conduct an initial trust assessment between the personal space IoT system and a device in a number of challenge-response rounds and determine when the initial

trust establishment procedure terminates. We simulate two different cases of the device's behavior. In the first simulation, the device consistently provides the expected responses to all challenges. The second case simulates a device that continuously provides unexpected responses to the challenges.

In the first simulation, since all the responses are expected to the challenges the probability that the device is an intended device to the system increases after each challenge. Accordingly, the probability associated with the uncertainty that the system has about the device (the entropy) is increased toward 1. Thus, the uncertainty is decreased after each challenge-response round. As shown in **Figure 4.7**, the entropy value is decreased with the increase of the associated probability. The instant trust value calculated at each round refers to a trust opinion. The aggregated initial trust value increases over the challenge-response process and reaches the trust threshold after *four* challenge-response rounds. The initial trust value that the system places on the device in this simulation is around 0.82 that expresses a trust opinion and meets the trust threshold. Therefore, the initial trust establishment process stops without performing further challenge-response operations.

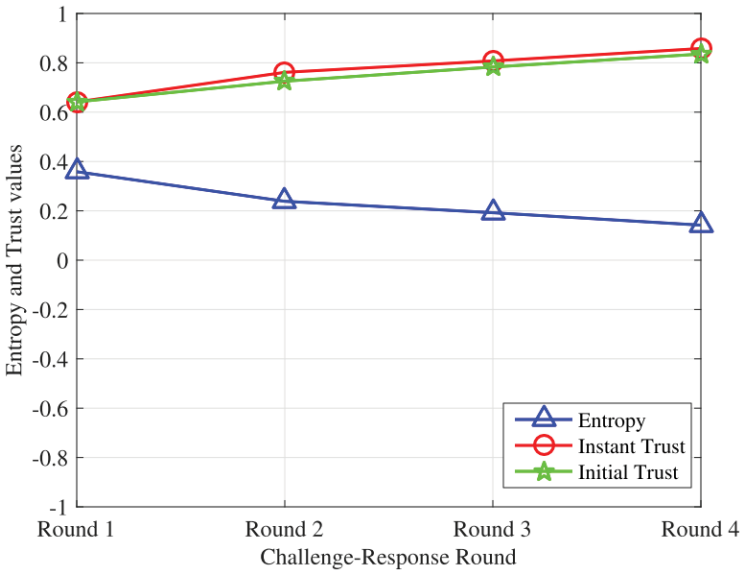


Figure 4.7 Experiment 2: Entropy and Trust values from the initial trust establishment on a device that provided all expected responses to all challenges

Figure 4.8 shows the numerical results from the second simulation of experiment 2. As the device continuously provides unexpected responses to all challenges, the uncertainty that the system has about the device reduces over the challenge-response process. In addition, the probability associated with this uncertainty is reduced to a value of less than 0.5. The one-to-one mapping between the trust and uncertainty indicates that the system is more certain about the device's behavior. Explicitly, the system knows that the probability that the device will provide an expected response to a challenge is very small, or equivalently the device is unlikely to provide an expected response to the challenge in the future. The aggregated initial trust value is degraded over the challenge-response process and meets the distrust threshold of -0.8 after the third challenge-response round. The simulation terminates after three challenge-response rounds as the aggregated initial trust value is under the distrust threshold at which the system considers that the device cannot recover its trustworthiness.

From the numerical results in this experiment, it is noted that the initial trust establishment terminates within a time window. The thresholds set for a trust opinion and a distrust opinion decides how long the initial trust establishment needs to investigate the trustworthiness of a device.

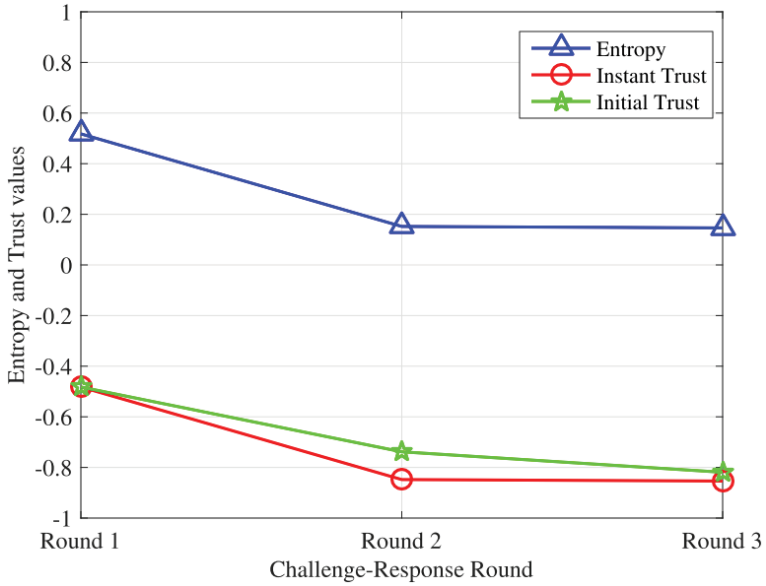


Figure 4.8 Experiment 2: Entropy and Trust values from the initial trust establishment on a device that provided unexpected responses to all challenges

The primary emphasis of the experimental evaluation is to demonstrate that our proposed probability-based initial trust establishment approach is feasible for initial trust evaluation as it consistently captures the device's behavior for the trust assessment. Clearly, without direct observations or the presence of a recommendation, our proposed scheme can initiate a challenge and then evaluate the device's response to obtaining an informed trust assessment as shown by the results. In the recommendation scheme, the trust value does not increase with the concatenation of recommendation. This is consistent and expected since the overall entropy of the system increases with the additional recommendation. For our proposed scheme, initial trust level increases with additional expected responses and decreases with unexpected responses. The consistency of the proposed initial trust evaluation scheme has been demonstrated.

4.4 Summary

This chapter presented our probability-based initial trust establishment model for personal space IoT systems. We explained the purpose and detailed the design of each module in our proposed initial trust establishment model. We finally presented the validation of the probability-based initial trust establishment model for personal space IoTs via extensive simulations. The experimental results demonstrate the consistency of the proposed approach in that the achieved initial trust value can be gained or degraded during the trust assessment depending on the device's behavior posed by its responses to the challenges. The challenge-response process allows the controller to capture the evidence and assess the uncertainty that the system has about the device's behavior and make an informed initial trust/distrust decision on the device.

Chapter 5

Binary Initial Trust Establishment Model for Personal Space IoT systems

5.1 Introduction

The probability-based initial trust establishment model that has been presented in chapter 4 relies on assumptions about the assigned parameters (probabilities) to estimate the uncertainty that the system has about the device's behavior. However, when the personal space IoT environment is dense and unfriendly, these assumptions might not reflect the actual device's trustworthiness. To cope with that problem, in this chapter we introduce a new method that employs the advances of *probability distribution* and *Bayesian inference* approach to estimate the uncertainty that the system has about the device without relying on the assigned probabilities. To establish the initial trust of devices to be admitted to a personal space IoT system, the Bayesian inference is utilized to assess the trust knowledge from the evidence captured in the trust evidence generation module. In particular, we consider the probability associated with the uncertainty that the system has about the device's behavior as a random variable and investigate its posterior probability distribution once new evidence is obtained from the trust evidence generation module. The expected value derived from the posterior probability distribution is then

used as the probability associated with the uncertainty that the system has about the device's behavior.

In addition, in this model, we consider the outcome of a challenge-response round is from a binary set. This means that there are two different outcomes from a challenge-response operation including the response that satisfies the system's expectation and the response that does not satisfy the system's expectation. The occurrence of a response to a challenge is the likelihood data in the Bayesian inference that updates the posterior distribution from the prior distribution and the likelihood. The proposed design and findings from this work have been published in [107].

The rest of this chapter is organized as follows. Section 5.2 presents the binary initial trust establishment model where each module is described in detail. Section 5.3 gives the experimental evaluation of the proposed binary initial trust establishment model. Finally, section 5.4 summarizes the chapter.

5.2 Binary Initial Trust Establishment Model

This section presents our proposed binary initial trust establishment model for personal space IoT systems. The details of each module of the proposed model will be described in detail.

5.2.1 Binary Trust Evidence Generation Module

This module is responsible for generating evidence for the binary initial trust establishment. The core of this module is the challenge-response process. The challenge-response process is performed intentionally by the controller at the first encounter between the system and an unknown device to investigate the device's behavior and then use this knowledge for the trust evaluation before deciding on whether to admit it into the system. It consists of several rounds. The binary result from each challenge-response round determines whether the device's response satisfies the controller's expectation. The outcome of a challenge-response round will be accumulated with outcomes from previous rounds for further assessment in the next module.

A challenge can be a request for the knowledge about the surrounding environment or a task that the device must perform successfully and honestly. It can be generated artificially by using a knowledge database built from surveys or the learning process. The semantics of the challenge varies depending on the type of the device, the population in the environment, and the knowledge of the population.

Now, the question is how to estimate the unknown probability associated with the uncertainty that the system has about the device's behavior, given the binary evidence from the conducted challenge-response rounds. Note that this probability value refers to how likely a device will behave as the system's expectation in the future if it is admitted to the system.

5.2.2 Binary Trust Knowledge Assessment Module

This section describes the design of the trust knowledge assessment module which estimates the uncertainty level that the system has about a device based on trust evidence generated from the trust evidence generation module. In this approach, the trust knowledge assessment module employs a Bayesian inference method that adopts Beta distribution as the mathematical foundation for the knowledge assessment. Intuitively, the purpose of this module is to assess the binary evidence from the challenge-response process to learn the uncertainty that the system has about the device's behavior.

Firstly, we explain the reason for choosing the Bayesian inference method as the mathematical foundation for the trust knowledge assessment module in this initial trust establishment approach.

- **Bayesian inference for initial trust assessment**

The Bayesian inference has been widely used in trust management models as it provides a means for updating belief of a subject on something when more evidence related to the belief becomes available through a posterior distribution model. In a system built with a trust management model, trust is dynamically changed over time as the system's entity behavior/activities are captured and monitored by the trust management model over its lifecycle. Therefore, a Bayesian-based mathematical model can nicely serve as a function updating belief over time in a trust management model.

In our initial trust establishment architecture, we conduct a challenge-response process for generating evidence about the trustworthiness of a device. As the evidence is captured continuously during the initial trust establishment, the knowledge/belief of the controller about the trustworthiness of a device will be changed over time. Note that we start the initial trust establishment without prior knowledge about the device. Therefore, the uncertainty that the system has about the device's behavior is generally unknown.

As uncertainty is a function of probability, in order to estimate that uncertainty, we assume that there is a probability value associated with the measure of the uncertainty. It is hard to estimate the probability associated with an unknown uncertainty when there is no prior information. Therefore, instead of determining the exact probability value, we came up with the idea of estimating its probability distribution and determining its expected value. Bayesian inference is a best-suited solution for estimating the probability distribution when more evidence about the observed event becomes available. Moreover, according to the related work survey in chapter 2, Bayesian-based trust evaluation method has been used in numerous trust management models. Therefore, using Bayesian inference to estimate an unknown probability associated with the uncertainty is practical.

In the binary initial trust establishment model, the probability associated with the uncertainty level in a device's behavior refers to the probability that the device's response shall satisfy the system, i.e., the device will behave as the system's expectation in the future. To estimate the probability associated with the uncertainty that the system has about the device's behavior, we consider this probability as a random variable with an unknown value from 0 to 1 and estimate its probability distribution over the challenge-response process. Precisely, we measure the uncertainty that the system has about a device's behavior based on Bayesian inference where the posterior model describes the distribution of the probability associated with the uncertainty conditioned on the binary evidence from challenge-response rounds.

As there is no experience or recommendation about the device's trustworthiness at the beginning of the initial trust establishment, prior to challenge-response rounds, the probability associated with the uncertainty that the system has about the device's behavior can be seen as a random variable which is uniformly distributed over [0, 1]. When the result from a challenge-response round occurs, this probability value could reasonably be

distributed over a smaller range since there is more evidence on how the device behaves to the challenge. The posterior distribution of this probability will be derived from the prior distribution and the results of the challenge-response process (likelihood) to reflect our additional information about the device's behavior.

Let θ denote the probability associated with the uncertainty that the system has about the device's behavior. To estimate the value of θ, we first assign a prior distribution to θ, $p(\theta)$, that is associated with the uncertainty that the system has about the device's behavior before any challenge-response rounds. Initially, θ is an unknown parameter and is uniformly distributed in the range of [0,1]. It is reasonable to choose $p(\theta)$ from the Beta family which is defined as follows [7, 24, 118], where α and β are parameters of the Beta distribution.

$$p(\theta) = \frac{1}{B(\alpha, \beta)} \theta^{\alpha-1}(1-\theta)^{\beta-1} \tag{5.1}$$

As probability distribution of θ is uniformly distributed over [0, 1], the prior distribution of θ is non-informative. To represent the non-informative prior distribution of θ before any challenge-response rounds, we can choose parameters of the Beta distribution at $\alpha = \beta = 1$.

In our binary initial trust assessment model, each challenge-response round is considered as a binary event with two possible outputs. Let R denote the output from one round. Output R can take a value of 1 or 0 that reflects the device's response satisfies the controller's expectation (R = 1) or the device's response does not satisfy the controller's expectation (R = 0), respectively. We design independent challenge-response rounds for estimating the value of probability θ. The probability that the outcome R will occur in each challenge-response round given the unknown probability θ can be calculated as follows.

$$p(R \mid \theta) = \theta^{R}(1-\theta)^{1-R} \tag{5.2}$$

Once a challenge-response round is completed, the posterior distribution of θ can be updated by applying Bayes' theorem.

$$p(\theta \mid R) = \frac{p(R \mid \theta) p(\theta)}{\int_0^1 p(R \mid \theta) p(\theta) d\theta} \tag{5.3}$$

Replacing (5.1) and (5.2) to (5.3), the expression of the posterior distribution of θ becomes

$$\begin{aligned} p(\theta \mid R) &= \frac{\theta^R (1-\theta)^{1-R} \frac{1}{B(\alpha,\beta)} \theta^{\alpha-1}(1-\theta)^{\beta-1}}{\int_0^1 \theta^R (1-\theta)^{1-R} \frac{1}{B(\alpha,\beta)} \theta^{\alpha-1}(1-\theta)^{\beta-1} d\theta} \\ &= \frac{\theta^{\alpha+R-1}(1-\theta)^{\beta+1-R-1}}{\int_0^1 \theta^{\alpha+R-1}(1-\theta)^{\beta+1-R-1} d\theta} \\ &= \frac{1}{B(\alpha+R, \beta+1-R)} \theta^{\alpha+R-1}(1-\theta)^{\beta+1-R-1} \end{aligned} \tag{5.4}.$$

The expression in (5.4) shows that the posterior distribution of θ has a Beta distribution with parameters $(\alpha + R)$ and $(\beta + 1 - R)$, where α and β are parameters of the prior distribution of θ before the current round takes place. It can be seen that, when the outcome from the first round occurs, the posterior distribution of θ has a Beta distribution with parameters $(1+R)$ and $(1+1-R)$ as its prior distribution is non-informative.

The estimation of θ with outcomes from subsequent challenge-response rounds will take the previous updated posterior distribution of θ as the prior distribution. Updating from the prior distribution and the outcomes of the challenge-response rounds by the same way, the posterior distribution of θ after *n* rounds $p(\theta \mid R_1, R_2, ..., R_n)$ is again a Beta distribution with parameters $(1 + n\bar{R})$ and $(1 + n - n\bar{R})$ where $\bar{R} = \frac{1}{n}\sum_{i=1}^{n} R_i$ and $R_i \in \{0,1\}$ representing the average number of rounds at which the binary outcome is an expected response to the challenge.

As θ is a probability random variable, for a given θ the posterior probability density $p(\theta \mid \bar{R})$ represents the probability that θ has a specific value (a probability value). Since

the random variable θ is continuous, the second-order probability $p(\theta \mid \bar{R})$ for any given value of θ in [0,1] is very small and therefore meaningless [118]. It is only meaningful to compute the posterior expected value of θ as in (5.5) and use it as the estimated value for the probability associated with the unknown uncertainty that the system has about the device's behavior, i.e., θ.

$$E[\theta \mid \bar{R}] = \frac{n\bar{R}+1}{n+2} = \frac{2}{n+2} \times \frac{1}{2} + (1 - \frac{2}{n+2}) \times \bar{R} \tag{5.5}$$

The form of the calculation of the posterior expected value of θ in (5.5) shows that when we conduct a large number of challenge-response rounds, i.e., *n* grows very large, the posterior expected value of θ mainly relies on the mean of the observed results $\bar{R}$.

It can be seen that by applying Bayesian inference that adopts Beta distribution as the prior distribution, we can gradually estimate the probability that is associated with the uncertainty that the system has about the device's behavior. With this approach, the expected value of θ achieved from the posterior distribution estimates the probability that a device will provide response that satisfies the controller's expectation. Thus, we can rely on this posterior expected value to learn the uncertainty that the system has about the device's behavior and then calculate the trustworthiness of the device at the initial phase of the IoT system.

Now, we measure the uncertainty that the system has about the device's behavior from the posterior expected value of θ by using the Shannon binary entropy [98].

$$H(x) = -x\log_2(x) - (1-x)\log_2(1-x) \tag{5.6}$$

where $x = E[\theta \mid \bar{R}]$ is the posterior expected value of θ that represents the probability associated with the uncertainty that the system has about the device's behavior after *n* challenge-response rounds.

5.2.3 Binary Initial Trust Evaluation Module

This section describes how the initial trust value is evaluated from the trust knowledge represented by binary entropy (uncertainty) gained from the trust evidence generation module and the trust knowledge assessment module.

Figure 5.1 shows the uncertainty that the system has about the device's behavior measured from the posterior expected value of probability θ, i.e., $E[\theta \mid \bar{R}]$, taking a value from [0, 1]. In fact, trust is an increasing function of the probability θ. Trust value should be increased when the probability that the device behaves as expected increases from 0 to 1. More specifically, the higher θ is, the more likely that the new device provides an expected response to the challenge is. As a result, the higher initial trust level that the system places on the new device is.

In our initial trust establishment model, the proportion of $(n\bar{R}+1)$ to (n + 2), as shown in (5.5), affects the uncertainty that the system has about the device's behavior as it determines the posterior expected value of the unknown probability θ. From (5.6), we can see that the maximum value of the uncertainty that the system has about the device's behavior is at 1 when $E[\theta \mid \bar{R}] = 0.5$. This case is when the number of device's responses satisfies the system is equal to the number of device's responses that do not satisfy the system, i.e., $\bar{R} = 0.5$. In this case, trust should be interpreted as a neutral value to indicate that there is no trust or distrust that the system can place on the device due to the lack of information.

In addition, the uncertainty level reduces from 1 to 0 when the associated probability value $E[\theta \mid \bar{R}]$ spreads far away from 0.5 towards 0 or 1. As the uncertainty is a symmetric function of the probability, it reaches nearly 0 when either $(n\bar{R}+1) << (n+2)$ or $(n\bar{R}+1) \approx (n+2)$. The corresponding trust value that the system places on the device should be interpreted to -1 to express a full distrust opinion on the device that does not satisfy the system's expectation in all challenge-response rounds. On the contrary, the trust value should be interpreted to 1 which indicates a nearly complete trust opinion on the device that satisfies the system's expectation in all challenge-response rounds. To interpret the uncertainty that the system has about the device's behavior to the initial trust value, similar to the trust interpretation method used in our proposed probability-based initial trust establishment scheme, in this approach we use (5.7) for the trust mapping from uncertainty where $x = E[\theta \mid \bar{R}]$.

$$T = \begin{cases} 1 - H(x), if\ 0.5 \le x < 1 \\ H(x) - 1, if\ 0 < x < 0.5 \end{cases} \tag{5.7}$$

The mapping in (5.7) satisfies the requirements for the initial trust metric as discussed above. **Figure 5.1** also illustrates our interpretation of the uncertainty that the system has about the device's behavior to the initial trust value with associated probabilities. In particular, the trust level depicts an amount from the range of [-1, 1) which can represent a full distrust, a less distrust, a neutral trust, a more trust opinion when the posterior expected value of probability θ increases from 0 to 1.

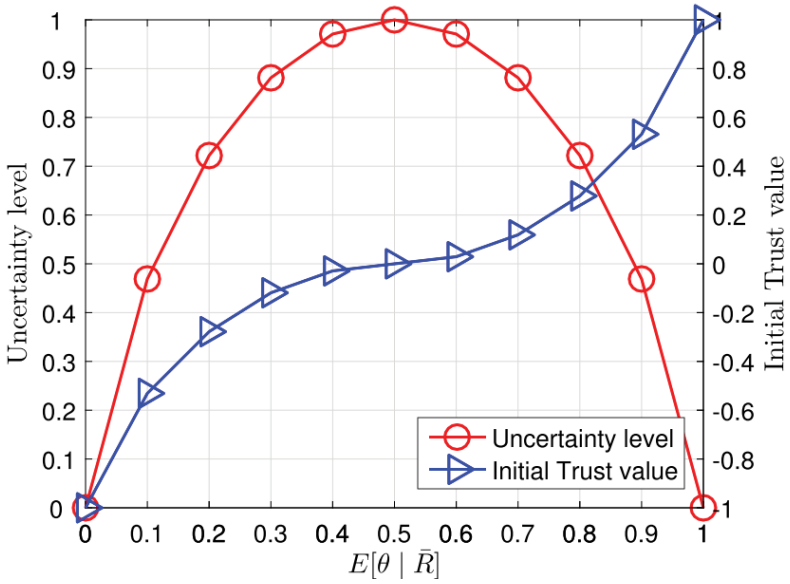


Figure 5.1 Mapping of uncertainty and initial trust value with the posterior expected value of probability θ

It is crucial to end the initial trust establishment within a reasonable time window for the creation phase of the personal space IoT system. We set thresholds to ensure that the initial trust assessment process ends upon the established initial trust value reaching a given threshold.

5.3 Experimental Evaluation

This section presents the evaluation of our proposed binary initial trust establishment model via simulation and discusses the obtained results. To thoroughly study the behavior of our proposed approach and the impact of salient parameters under various circumstances, we will not impose the time limit or the number of iterations in the challenge-response (C-R) process in our investigation below.

5.3.1 Simulation Setup

In the experiments, we conduct a challenge-response process for the trust evidence generation module with seven C-R rounds where each device will be verified with seven challenges by the controller. The optimal number of challenge-response rounds depends on the applications and the operating environment of the IoT system. Software objects are simulated as the controller role and the new device role to numerically investigate our proposed binary initial trust establishment. In a challenge-response round, an event of sending a challenge is first executed at the controller object. It is followed by an event of sending a response executed at the device object. The response evaluation process is conducted at the controller by a computation module. The binary outcomes of either "the device's response satisfies the controller" (R = 1) or "the device's response does not satisfy the controller" (R = 0) will be returned by this computation module. Another module at the controller object will accumulate the outcome R and pass it to the trust knowledge assessment module where a Bayesian analysis is executed to update the posterior distribution and compute the posterior expected value of the probability associated with the uncertainty that the controller has about the device's behavior.

The simulation of the challenge-response process is repeated until the last round is completed. The output of the initial trust establishment process is an initial trust level that the controller places on the device over the challenge-response process. This initial trust value is then involved in the decision making of the forthcoming authentication or other security methods before the device is granted permission to be a member of the personal space IoT system.

We investigate the change of the posterior probability density function (pdf), the posterior expected value of the random variable θ, the uncertainty level in the device's behavior measured from the posterior expected value of θ, and the initial trust value during the challenge-response process with various cases of device's responses.

5.3.2 Numerical Results

In the experiment, we simulate four different cases that represent four different device's response patterns to the challenges. Firstly, we conduct the initial trust establishment between the controller (on behalf of the personal space IoT system) and a new device whose responses satisfy the controller's expectation in all challenge-response rounds. **Figure 5.2** and **Figure 5.3** shows the numerical results of the investigated parameters from this simulation.

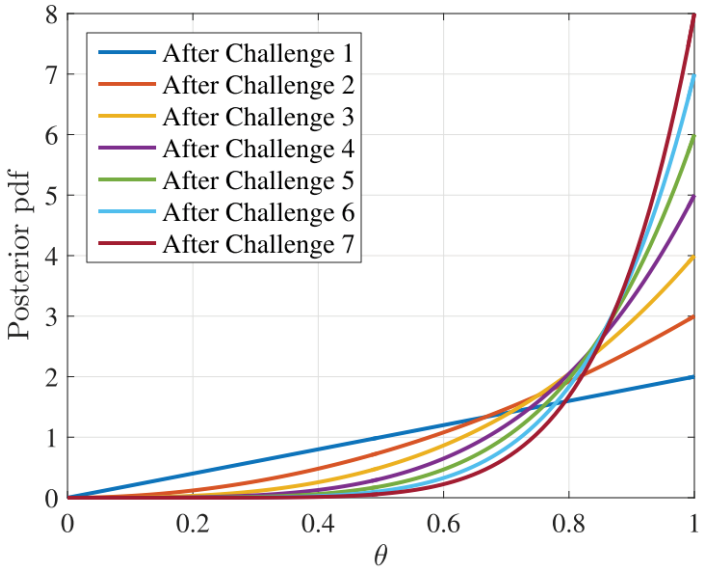


Figure 5.2 Posterior pdf of a random variable θ over 7 C-R rounds when a device whose responses satisfy the system in all rounds

Specifically, **Figure 5.2** shows the change of the posterior pdf shape over 7 challenge-response rounds when a device's responses satisfy the system in all rounds. The curve representing the posterior pdf has gradually shifted to the right side when more device's responses satisfy the system. This shifting indicates the predicted value of unknown probability θ over the period [0, 1]. It can be seen that the scope of the distribution of the

random variable probability θ is narrower. This means that the more evidence from the challenge-response process occurs, the more accurate in prediction of the probability value θ is. In this case, a high value of θ is expected as its probability distribution is getting closer to 1.

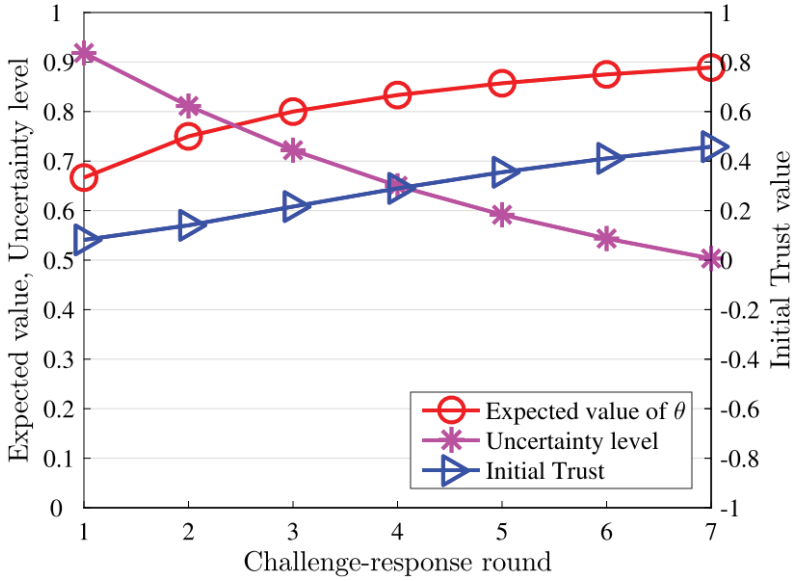


Figure 5.3 Posterior expected value of θ, uncertainty level and initial trust level over 7 C-R rounds with a device whose responses satisfy the system in all rounds

Figure 5.3 presents the change in the posterior expected value of θ, the uncertainty that the system has about the device's behavior, and the mapped initial trust value over seven challenge-response rounds with a device whose responses satisfy the system in all challenge-response rounds. According to the narrower shape and the shifting toward 1 of the posterior pdf as shown in **Figure 5.2**, the posterior expected value of θ increases from 0.68 to 0.88. This results in a reduction in the uncertainty level because the device consistently satisfies the system in challenge-response rounds. With the mapping from uncertainty to trust, the initial trust value increases from 0.1 to around 0.48 since the controller reduces its uncertainty about the device's behavior. The trust level refers to a trust opinion placed on the device because it is consistently well-behaved over the challenge-response process. Once the challenge-response process has ended, the controller gains more knowledge concerning the device and places an initial trust value of 0.48 on the device.

Secondly, we simulate a binary initial trust establishment between the controller and a new device whose responses do not satisfy the system in all challenge-response rounds. **Figure 5.4** and **Figure 5.5** present the numerical results of investigated parameters from this simulation.

Particularly, **Figure 5.4** shows how the posterior pdf shape changed over seven challenge-response rounds when a device does not satisfy the system in all challenge-response rounds. Since there is more evidence available during the challenge-response process, the shape of the posterior pdf is narrowed. This means the area under the curve of the posterior pdf of the unknown probability θ is smaller. As the device's response do not satisfy the system in all challenge-response rounds, the posterior pdf has gradually shifted to the left side indicating a low probability that the device will return an expected response to future challenges. Based on this, we can predict that the probability θ that the device provides an expected response to a challenge in the future is small and around some value that is close to 0.

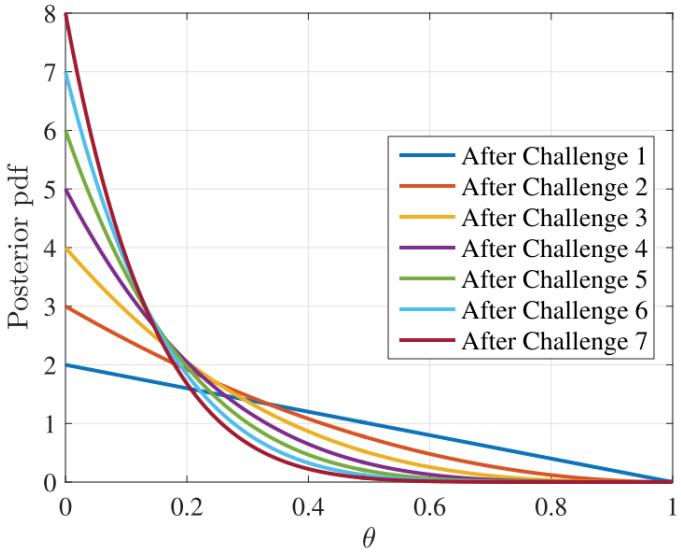


Figure 5.4 Posterior pdf of random variable θ over 7 C-R rounds with a device whose responses do not satisfy the system in all rounds

Figure 5.5 presents the posterior expected value of θ, the uncertainty level and initial trust value over seven challenge-response rounds when a device does not satisfy the system in all challenge-response rounds. In particular, the posterior expected value of θ continuously reduces from 0.34 to 0.11. This is accordingly consistent with the change in

the shape of its posterior pdf indicated in **Figure 5.4**. The corresponding measured uncertainty level reduces to around 0.5. Although the measured uncertainty level is similar to that in the first simulation, the initial trust value is interpreted to -0.48 which refers to a distrust opinion placed on the device because it continuously does not satisfy the system that implies a bad behavior.

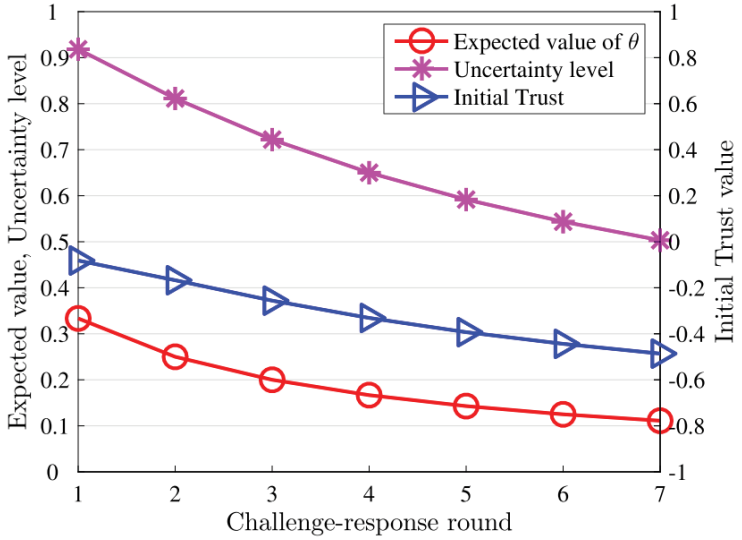


Figure 5.5 Posterior expected value of θ, uncertainty level and initial trust level over 7 C-R rounds with a device whose responses do not satisfy the system in all rounds

Thirdly, a binary initial trust establishment procedure between the controller and a new device is simulated. The device's responses satisfy the system in the first three rounds and do not satisfy the system in the last four rounds. **Figure 5.6** and **Figure 5.7** show the numerical results of investigated parameters from this simulation.

Specifically, **Figure 5.6** illustrates how the posterior pdf shape changed over the simulation when a device provided satisfied responses in the first three rounds and unsatisfied responses to the system in subsequent rounds. Different from the first two simulations, in this simulation, the posterior pdf has a bell shape and shifts to either the right or the left side depending on the accumulated number of expected responses. Over the first three challenge-response rounds, since the device's responses satisfy the system, the posterior pdf had a flat shape and shifted to the right side indicating a potential high probability of θ. However, the posterior pdf has the bell shape and also shifted to the left side because the device's responses do not satisfy the system in the last four challenges.

After seven challenge-response rounds, the area under the bell curve of the posterior pdf is shifted to the center of the range [0, 1] indicating that the probability θ is located somewhere around the center of [0, 1].

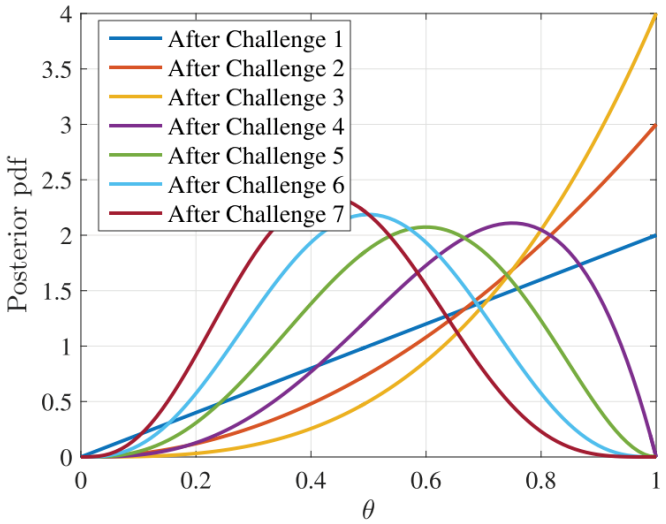


Figure 5.6 Posterior pdf of random variable θ over 7 C-R rounds with a device whose responses satisfy the system in the first 3 rounds and do not satisfy the system in the last 4 rounds

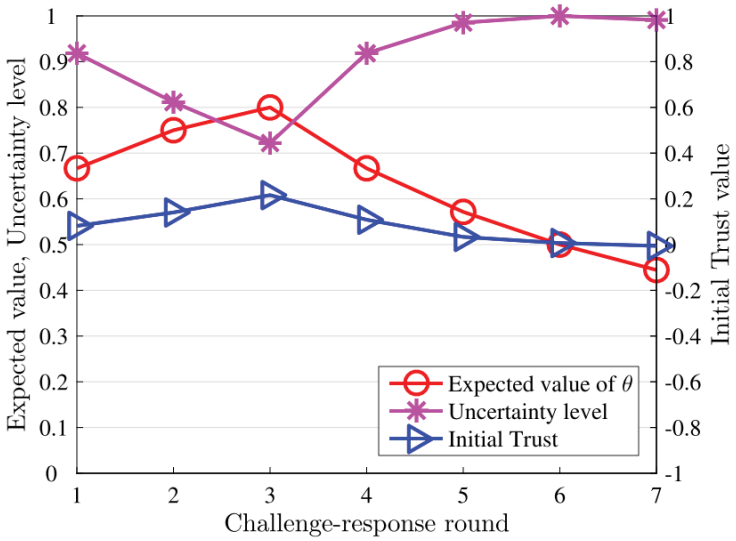


Figure 5.7 Posterior expected value of θ, uncertainty level and initial trust level over 7 C-R rounds with a device whose responses satisfy the system in the first 3 rounds and do not satisfy the system in the last 4 rounds

According to the change in the posterior pdf shape and position, **Figure 5.7** shows that the uncertainty level reduces over the first three rounds and increases again to a very

high value when the device's responses are unsatisfied by the system in the subsequent rounds. The corresponding initial trust value increases from a neutral value to 0.2 in the first three rounds and drops to a neutral value as the device does not provide good behavior consistently to the last four challenges. Based on the posterior expected value of θ the system can consistently capture the device's behavior and places a reasonable initial trust value on the device.

Lastly, we simulate a binary initial trust establishment procedure between the controller and a new device whose responses do not satisfy the system in the first two rounds and satisfy the system in all other challenge-response rounds. The numerical results of the investigated parameters are shown in **Figure 5.8** and **Figure 5.9**.

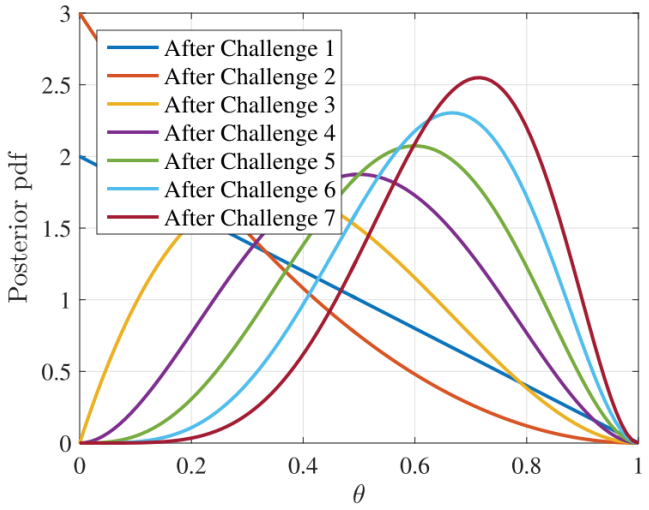


Figure 5.8 Posterior pdf of random variable θ over 7 C-R rounds with a device whose responses do not satisfy the system in the first 2 rounds and satisfy the system in the last 5 rounds

Figure 5.8 presents the changes of posterior pdf shape and position over this simulation. The curve of the posterior pdf is narrowed and shifted to the right side, and the posterior expected value reduces in the first two rounds and increases during the subsequent five rounds. Over the last five challenge-response rounds, the area under the bell curve of the posterior pdf has gradually shifted to the right side due to the more expected responses that the device provided. It implies that the probability value θ is located closely toward 1.

Figure 5.9 shows that the initial trust value drops to -0.5 which refers to a distrust opinion over the first two rounds as the device's response are satisfied by the system. Although the device's responses satisfy the system in the subsequent five challenges, the initial trust value increases to a small trust value at 0.07. This indicates that with this device's behavior the controller places a small initial trust level on this device.

It can be seen that using the Bayesian posterior distribution update model, the trust knowledge assessment model can consistently learn the device's behavior and predict the probability that a device will behave as expected in the future. For various device's behavior patterns, the trust knowledge assessment can accurately extract the knowledge based on posterior probability distribution updating throughout the challenge-response process.

In summary, the simulation results show that our binary initial trust establishment model based on the challenge-response mechanism allows the controller to place the trust levels on devices that behaved as expected consistently to the challenges and the distrust levels on ones that fail to fulfill the expectation of the system.

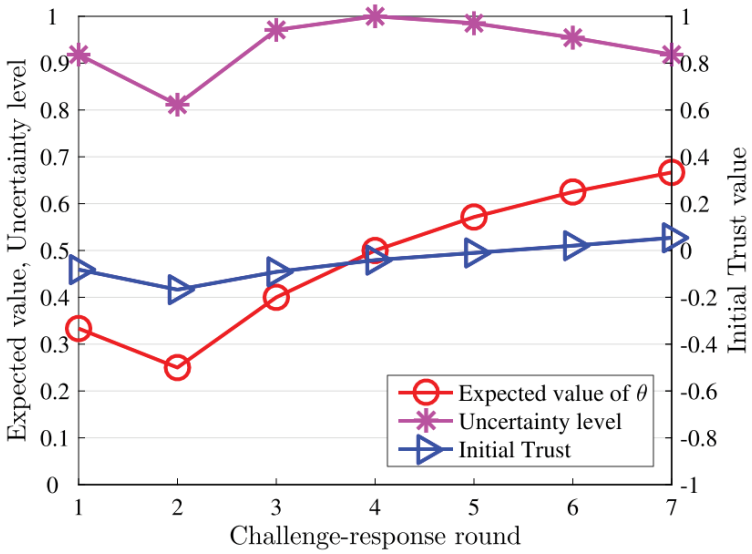


Figure 5.9 Posterior expected value of θ, uncertainty level and initial trust level over 7 C-R rounds with a device whose responses do not satisfy the system in the first 2 rounds and satisfy the system in the last 5 rounds

5.4 Summary

In this chapter, we described a binary initial trust establishment model for personal space IoT systems where the Bayesian approach adopting a Beta distribution is used as the mathematical foundation for the trust computation. We evaluated the performance of our proposed initial trust establishment with various device's response patterns. The numerical results showed that our proposed approach allows the IoT system to consistently capture the device's behavior and determine initial trust level on the device according to its behavior to the challenges. This model provides a new method to quantify the initial trust level of devices before they are admitted to the system where the device's behavior can be accessed via its response's satisfaction level to the challenges of the system.

Chapter 6

Multilevel Initial Trust Establishment Model for Personal Space IoT systems

6.1 Introduction

In chapter 5, we proposed a binary initial trust establishment for the personal space IoT system. The binary initial trust establishment approach relies on the binary outcomes from a challenge-response process (the device's response satisfies the system or the device's response does not satisfy the system). However, the satisfaction level of the challenger on a response are not often two values either satisfied or unsatisfied but multiple values that indicate various degrees of satisfaction [6]. It requires a more accurate trust knowledge assessment method to estimate the device's behavior according to the satisfaction level that the system experiences from the device's responses. This motivates us to propose a multilevel initial trust establishment model where the trust knowledge is extracted from a multiple outcome set of challenge-response operations.

In this chapter, we present a multilevel initial trust establishment model. The architecture of this model is based on the presented overall architecture where the challenge-response information design module is not included as we only investigate the outcomes of challenge-response operations and assume that they are relevant and meaningful for the trust assessment process. Our multilevel initial trust establishment model investigates the multi-valued satisfaction level that the system learns about the

device's responses. With this setting, in the trust evidence generation module the evaluation of a device's response leads to multiple outcomes, i.e., multiple levels associated with various degrees of satisfaction that the system has about that response. Similar to the proposed binary initial trust establishment model, this model aims to estimate the probability associated with the uncertainty that the system has about the device's behaviour by monitoring its posterior probability distribution. However, in the multilevel initial trust establishment model, we consider the unknown probability associated with the uncertainty that the system has about the device's behavior *as a multi-component random variable*. For the trust knowledge assessment module, we propose a Bayesian approach that adopts the Dirichlet distribution as the mathematical foundation for measuring the uncertainty that the system has about the device's behavior where the device satisfies the system to one of the multiple satisfaction levels. In the multilevel initial trust evaluation module, a trust interpretation method is proposed to interpret the uncertainty that the system has about the device's behavior to a trust level. The proposed design and findings from this work have been published in [119].

The rest of this chapter is organized as follows. Section 6.2 describes our proposed multilevel initial trust establishment model and explains the detail of each module. Section 6.3 gives the experimental evaluation and discusses the numerical results. Finally, section 6.4 summaries the chapter.

6.2 Multilevel Initial Trust Establishment Model

This section describes our proposed multilevel initial trust establishment model. It further describes individual components of the multilevel initial trust establishment model when the multilevel trust knowledge assessment is investigated.

6.2.1 Multilevel Trust Evidence Generation Module

This section describes how the trust evidence is generated in the multilevel initial trust establishment model. The core of the trust evidence generation module is the challenge-response process. In order to generate trust evidence for the initial trust establishment model when a device encounters the IoT system for the first time, the system requests

responses from the device for a number of challenges. The input of the trust evidence generation module is a set of challenges and the device's responses to the challenges. The output is the trust evidence based on the satisfaction level that the system has on the device's responses.

We define a multi-valued satisfaction set which will be used for the system to judge whether a device's response satisfies the system to a specific level. The multi-valued satisfaction level set can be set so that it reflects the user's preferences and depends on the application domain. For example, in a rating system for the customer's satisfaction on a service, the system categories satisfaction level into multiple degrees to describe the customer's feedback to a more accurate evaluation rather than providing them only two options to rate.

In the trust evidence generation module, several challenge-response rounds are conducted to learn how the new device responds to the challenges requested by the controller. The trust evidence generated from the challenge-response rounds is based on the observation that at each round at which level the device's response satisfies the system. To achieve this information at each challenge-response round, the controller evaluates the device's response and assigns one of the levels from a predefined multi-valued satisfaction set to the received response. The accumulated number of rounds that a specific satisfaction level is met by the device's response is collected and used as the inputs for the multilevel trust knowledge assessment module.

The predefined satisfaction level set includes multiple values from a lowest to a highest satisfaction level. The higher satisfaction level that the device's response is assigned by the controller, the more likely that the device is trusted by the system. The lower sataifaction level that the device's response is assigned by the controller, the more likely that the device is not trusted by the system.

6.2.2 Multilevel Trust Knowledge Assessment Module

In this section, we describe the multilevel trust knowledge assessment module in our proposed multiple initial trust establishment model. We first explain the reason for adopting the Dirichlet distribution in the Bayesian approach to estimating the multilevel

trust knowledge. We then present a mathematical analysis to show how the multilevel trust knowledge is updated based on the Bayesian inference with the Dirichlet distribution.

According to Bayesian statistics, the posterior distribution presents the updating in the prior distribution of an unknown event once the prior belief is updated with more evidence. One of the properties of trust is that it is dynamically changed over time due to the appearance of the new evidence achieved from on the new observations. The current belief should be updated with the new information and changed to a new belief status. Bayesian inference is best suited for the belief updating. Furthermore, in our multilevel initial trust knowledge assessment module, the evidence is evaluated and collected based on a multi-valued satisfaction level of the device's response to the system from the trust evidence generation module. In fact, the posterior Dirichlet distribution of a multi-component random variable is based on its prior distribution and the observations on the distribution of each component. Therefore, it is reasonable to use the Dirichlet distribution for the Bayesian analysis in our trust knowledge assessment to estimate the probability associated with the uncertainty in the device's behavior where the device's behavior is observed from the satisfaction level of its responses to the system.

Let X be a discrete random variable representing the discrete satisfaction level of a response to a challenge. The system defines k values for the satisfaction level to evaluate the response. Therefore, X can take on one of k values from $\{x_1, x_2, ..., x_k\}$, where x_i denotes one of the satisfaction levels. Each satisfaction level x_i is assigned a weight value w_i in a way that for $x_{i+1} > x_i$, $w_{i+1} > w_i$ & $\sum_{i=1}^{k} w_i = 1$.

Let Θ denote a random variable representing the probability that a device will return a response with a certain satisfaction level. Note that, Θ is a k-component random variable, i.e., $\Theta = \{\theta_1, \theta_2, ..., \theta_k\}$. Let θ_i denote the probability that a device will return a response with a satisfaction level x_i. In other words, for a device, the probability that X takes value x_i is θ_i.

$$\theta_i = P(X = x_i) \;\; s.t \;\; \sum_{i=1}^{k} \theta_i = 1 \tag{6.1}$$

For the initial trust establishment model conducted between the IoT system and new devices encountered for the first time, it is supposed that before the challenge-response process, the pre-knowledge on the probability distribution of Θ is usually not available. Thus, we consider that the prior distribution of Θ is uniform, i.e., the probability that the device will provide a response with each satisfaction level is equally likely. In fact, the uniform distribution captures initial ignorance and is a special case of the Dirichlet distribution. Therefore, it is reasonable to choose Dirichlet distribution as the prior distribution of Θ as in (6.2) where α_i denotes concentration parameter of positive real value.

$$p(\theta_1,...\theta_k;\alpha_1,...,\alpha_k) = \frac{\Gamma(\sum_{i=1}^{k}\alpha_i)}{\prod_{i=1}^{k}\Gamma(\alpha_i)} \prod_{i=1}^{k} \theta_i^{\alpha_i - 1} \tag{6.2}$$

As the prior distribution of Θ is uniform, we choose the parameters α_i in its Dirichlet distribution form as $\alpha_i = 1, \forall i = 1,...,k$ to represent the non-informative prior distribution.

The outcome from the evaluation of the device's response conducted after a single challenge-response round is one of the satisfaction levels assigned by the controller to the received response. Let Y^j denote the outcome vector from the j^{th} challenge-response round. Let y_i represent the i^{th} element in the vector $Y^j = \{y_1, y_2, ..., y_k\}$. Note that each y_i can take a value in $\{1,0\}$ which indicates whether the device's response satisfies level x_i or not, i.e., $y_i = 1$ means the device's response satisfies level x_i and $y_i = 0$ refers to the fact that it meets other satisfaction levels.

After each challenge-response round, we accumulate the number of rounds in which the device returns a response with a given satisfaction level. Let s_i denote the number of

rounds that the device's response satisfies level x_i after n challenge-response rounds where $\sum_{i=1}^{k} s_i = n$. We accumulate s_i as below.

$$s_i = \sum_{j=1}^{n} Y^j\{y_i\} \tag{6.3}$$

where $Y^j\{y_i\}$ is the i^{th} element in a vector Y^j which indicates whether the device's response satisfies level x_i at round j^{th}, and $Y^j(y_i) = 1$ or $Y^j(y_i) = 0$.

For vector $\Theta = \{\theta_1, \theta_2, ..., \theta_k\}$, we can treat each θ_i $(i = 1, ..., k)$ as an independent variable. The challenge-response observation conforms to a multinomial distribution as each round is independent and its outcome is one of k possible satisfaction levels. Each θ_i is converged on an unknown value $(0 < \theta_i < 1)$. Therefore, the probability that a device's response satisfies a satisfaction level x_i in s_i rounds given the unknown probabilities θ_i is given by

$$p(s_1, ..., s_k \mid \theta_1, ..., \theta_k) = \frac{n!}{\prod_{i=1}^{k} s_i!} \prod_{i=1}^{k} \theta_i^{s_i} \tag{6.4}.$$

Then, the posterior distribution of Θ can be updated from the prior Dirichlet distribution in (6.2) and the likelihood in (6.4) according to Bayes' formula as below.

$$\begin{aligned} p(\theta_1, ..., \theta_k \mid s_1, ..., s_k) &= \frac{\frac{n!}{\prod_{i=1}^{k} s_i!} \prod_{i=1}^{k} \theta_i^{s_i} \times \frac{\Gamma(\sum_{i=1}^{k} \alpha_i)}{\prod_{i=1}^{k} \Gamma(\alpha_i)} \prod_{i=1}^{k} \theta_i^{\alpha_i - 1}}{\prod_{i=1}^{k} \int_0^1 \frac{n!}{\prod_{i=1}^{k} s_i!} \theta_i^{s_i} \times \frac{\Gamma(\sum_{i=1}^{k} \alpha_i)}{\prod_{i=1}^{k} \Gamma(\alpha_i)} \theta_i^{\alpha_i - 1} d\theta_i} \\ &= \frac{1}{\prod_{i=1}^{k} \int_0^1 \theta_i^{s_i + \alpha_i - 1} d\theta_i} \prod_{i=1}^{k} \theta_i^{s_i + \alpha_i - 1} = \frac{1}{B(s_i + \alpha_i)} \prod_{i=1}^{k} \theta_i^{s_i + \alpha_i - 1} \end{aligned} \tag{6.5}$$

The expression in (6.5) shows that the posterior distribution of each θ_i has a Dirichlet distribution with parameters $(s_i + \alpha_i), \forall i = (1,...,k)$. It can be seen that, when the outcome from the first challenge-response round occurs, the posterior distribution of θ_i have a Dirichlet distribution with parameter $y_i + 1$ as its prior distribution is non-informative, i.e., $\forall \alpha_i = 1$, where y_i can take a value in {1, 0}. The estimation of θ_i in subsequent challenge-response rounds will use the previous posterior distribution of θ_i as the prior distribution. Updating from the prior distribution and the accumulated likelihood, the posterior distribution of θ_i after *n* rounds also has Dirichlet distribution with parameters $s_i + 1$ where s_i is given in (6.3).

In summary, the prior distribution of random variables θ_i has a Dirichlet distribution with parameters $\alpha_i = 1$, $\forall i = (1,...,k)$. The parameters $s_i + \alpha_i$ of the posterior Dirichlet distribution of θ_i is updated once a challenge-response round is completed by adding 1 to s_i if the device's response meets the corresponding satisfaction level x_i.

As each θ_i is a probability value, the posterior probability distribution density $p(\theta_i \mid s_i)$ represents the probability that θ_i has a specific value given the observation of s_i. Since the variable θ_i is continuous, the second order probability $p(\theta_i \mid s_i)$ for any given value of θ_i in [0, 1] is minuscule and hence meaningless [118]. It is only meaningful to compute the posterior expected value of θ_i from its Dirichlet posterior distribution as below.

$$E[\theta_i \mid s_1,...,s_k] = \frac{1 + s_i}{k + \sum_{i=1}^{k} s_i} \tag{6.6}$$

In our proposed multilevel trust knowledge assessment module, we derive the uncertainty that the system has about the device's behavior from the posterior distribution of the probability vector Θ for capturing the initial trustworthiness of the device. We measure the uncertainty level based on the posterior expected value of θ_i and the weight value of each satisfaction level by using Shannon entropy [98]. Note that the purpose of

using the weight value is to prioritize the responses with high satisfaction levels in measuring initial trust value. The weight values are chosen in such a way that the higher satisfaction level has a higher weight.

$$H = \sum_{i=1}^{k} -w_i E[\theta_i \mid s_1,...,s_k] \log_2(w_i E[\theta_i \mid s_1,...,s_k]) \tag{6.7}$$

The output of the trust knowledge assessment module is the uncertainty that the system has about the device's behavior that is learned from the evidence generated during the challenge-response process. In the next section, we describe how the uncertainty level is interpreted as the initial trust value.

6.2.3 Multilevel Initial Trust Evaluation Module

This section presents the initial trust computation module which evaluates an initial trust value on a device based on the knowledge learned from the previous modules.

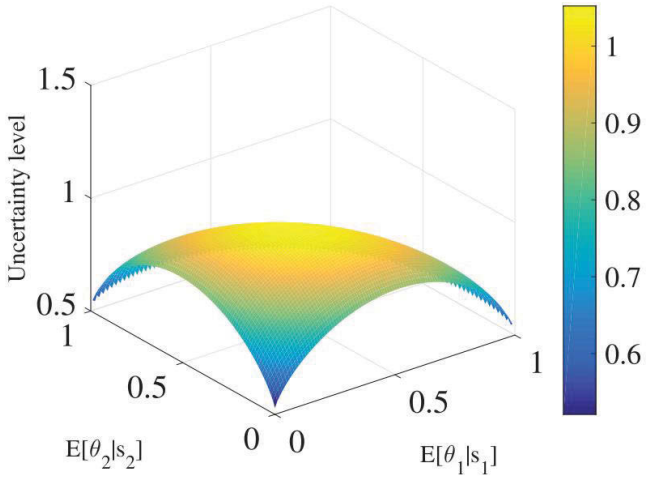
In order to determine whether the uncertainty that the system has about the device's behavior should be interpreted to a trust or a distrust value, we calculate the average value of the posterior expected values of elements in vector Θ, called $\bar{\theta}$, as given in (6.8). The purpose of using this average value is to deal with the fact that the uncertainty measured by information entropy is symmetric. Each point in the uncertainty curve can be a result of the combination of multiple sets of posterior expected values. Our defined average value is used as an indicator to determine the trend/direction of the uncertainty amount when it is mapped to the trust domain.

$$\bar{\theta} = \sum_{i=1}^{k} w_i E[\theta_i \mid s_1,...,s_k] \tag{6.8}$$

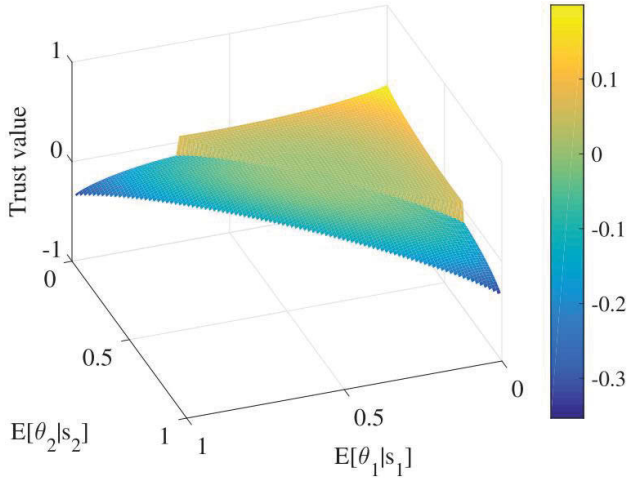
In order to determine the requirements that a trust interpretation method must guarantee to map the uncertainty that the system has about the device's behavior learned from the trust knowledge assessment module to a proper initial trust level, we analyze the possible uncertainty level in a device's behavior and its meaning in the trust domain. To visualize the shape of the uncertainty's curve, we choose a three-valued satisfaction level set for the initial trust establishment to analyze the uncertainty and its relation to trust. Note that any multiple-valued satisfaction level set can work in our trust knowledge

assessment, i.e., $(\forall k > 2)$. The analysis is based on an initial trust establishment in an IoT system which considers three-valued satisfaction level set.

Figure 6.1a shows the uncertainty level in the device's behavior in 3-dimensional space where the system defines three satisfaction levels with the weight values of 0.3, 0.3, and 0.4, respectively. It is worth noting that the optimal weight values vary with different purposes of various applications. Each point in the uncertainty curve is computed from three expected values of three probability components of the probability vector $\Theta = \{\theta_1, \theta_2, \theta_3\}$ according to (6.7).



(a)



(b)

Figure 6.1 a) Uncertainty level and (b) Trust value with the posterior expected values of θ_i in a system which uses three-valued satisfaction level set

In fact, the trust that the system places on a device is an increasing function of the probability that the device will always behave as expected to the system. For the multilevel initial trust establishment model, the trust value should be increased when the average value of the posterior expected values of elements in the vector Θ, $\bar{\theta}$, increases from 0 to 1. For all possible combinations of posterior expected values $E[\theta_i]$, the uncertainty level is spanned across 3-dimensional space with values from a minimum amount to a maximum amount computed depending on $E[\theta_i]$ and their related weight values. It can be seen that the system has maximum uncertainty (at the peak area of the uncertainty curve) in the device's behavior when the three posterior expected values of the probability components multiplied by their weight values are equally likely. In contrast, the system has minimum uncertainty in the device's behavior when one of the probability components in the probability vector $\Theta = \{\theta_1, \theta_2, \theta_3\}$ has a posterior expected value of 1. This implies that the device is most likely to provide a response that satisfies the system to a given level in the future.

We define the requirements for the initial trust interpretation method as follows. Firstly, at the maximum uncertainty point in the uncertainty curve, the trust value should be a neutral value indicating there is no trust or distrust that can be decided. At the minimum uncertainty point in the uncertainty curve (H = 0), the trust value should be translated to a lowest or highest value in the trust domain. At any other point in the uncertainty curve, depending on the average value $\bar{\theta}$, the trustworthiness of the device should be interpreted to some degree of trust or distrust considering the fact that trust is an increasing function of probability. When $\bar{\theta}$ is less than *1/k*, the uncertainty level is translated to a distrust value. Otherwise, it is interpreted as a trust value. Note that when $\bar{\theta} = 1/k$ the distribution of θ_i is uniform leading to a neutral belief on the trustworthiness.

As $\bar{\theta}$ value is derived from $E[\theta_i]$ values and it can be identical for many permutations of a set of $E[\theta_i]$, we embed $(1-\bar{\theta})$ and $\bar{\theta}$ into the trust interpretation function in order

to distinguish different response patterns. The purpose of using factors $(1-\bar{\theta})$ and $\bar{\theta}$ is to ensure the consistent mapping of the uncertainty value into the trust scale of $(-1,1)$.

We use (6.9) to interpret trust value from the uncertainty level, where H_{max} is the maximum uncertainty value considering the number of satisfaction levels and their weight values. For instance, in a trust assessment model with three satisfaction levels, the maximum value H_{max} is placed at the peak area of the uncertainty level visualized in **Figure 6.1a**. The mapping in (6.9) meets the defined requirements of a trust interpretation function.

$$T = \begin{cases} (1-\bar{\theta})(H - H_{\max})\dfrac{1}{H_{\max}}, & if\ 0 \le \bar{\theta} \le \dfrac{1}{k} \\ \bar{\theta}(H_{\max} - H)\dfrac{1}{H_{\max}}, & otherwise \end{cases} \tag{6.9}$$

Figure 6.1b illustrates the trust value in 3-dimensional space with a trust plane and a distrust plane. The trust level depicts a value representing a distrust value, a neutral value, or a trust value when the posterior expected values of probability components in vector Θ, $E[\theta_i \mid s_i]$, increase from 0 to 1. It should be noted that the trust values can be scaled up within a specific range by using a function of H_{max} value. In this approach, we scale up the initial trust value within the scope of $(-1,1)$. It is essential to set thresholds for the initial trust evaluation to ensure that the initial trust establishment ends when the established initial trust value reaches a given threshold.

6.3 Experimental Evaluation

This section presents the performance evaluation of our proposed multilevel initial trust establishment model. Various device's behavior patterns are investigated to show the consistency of our initial trust establishment model in a personal space IoT system.

6.3.1 Simulation Setup

The following experiments investigate various device's behavior of new devices which intend to join a personal space IoT system. A software object is created to represent the controller. Other software objects are also built to simulate several devices to be investigated by our proposed multilevel initial trust establishment model.

In each experiment, we define a set of satisfaction levels for the trust evidence generation module and thresholds for terminating the trust establishment process. The software object playing the controller's role will generate an event of sending a challenge and wait for the response event created by the software object performing the device's role. The response is made according to the device's behavior pattern. In the controller-role object, a computation module is responsible for evaluating the device's response and assigns a certain satisfaction level to the received response. The evidence generation and trust knowledge assessment modules are conducted by computation functions implemented in the software object playing the controller's role. This process is repeated for a number of rounds until the aggregated initial trust level meets a given threshold or the controller stops the initial trust establishment.

6.3.2 Numerical Results

This section discusses the numerical results from the experimental evaluation of our proposed multilevel initial trust establishment model.

- **Experiment 1**

In order to visualize the posterior Dirichlet pdf, we conduct an investigation that simulates an initial trust assessment process in eight challenge-response rounds (n = 8) where the system defines three satisfaction levels (k = 3). The three-valued satisfaction level set can be used to represent a set of unsatisfied (level 1), neutral (level 2) and satisfied (level 3) that the system assigns to a device's response. We show how the Dirichlet pdf refines the investigated probability distribution when more observed responses are available. We also investigate the changes in the average value of the posterior expected values, $\overline{\theta}$, the uncertainty level and the initial trust value during the challenge-response process. The weight values for satisfaction levels are set at 0.05, 0.2

and 0.75, respectively. This experiment simulates that the device's response satisfies the challenge to level 1 in the first two rounds, to level 2 in the subsequent two rounds and level 3 in the last four rounds.

Figure 6.2 illustrates the changing in the shape of the posterior pdf with the probability vector $\{\theta_1,...,\theta_k\}$ and the parameter vector $\{s_i,...,s_k\}$ updated over the challenge-response process. It also shows how the maximum point of the investigated Dirichlet pdf curve moves within the 3-dimensional space over eight challenge-response rounds. After the first two rounds, the shape of the posterior pdf in the 3-dimensional space is flat. It achieves the maximum value when θ_1 grows to 1 as the device provides a response with satisfaction level 1 in both rounds. The flat shape is narrowed and gets a higher maximum value after the second round due to the greater contribution of θ_1 to the probability density function. Then, after the third and fourth rounds, the curve representing the posterior pdf has a bell shape and moves towards the center of the space since θ_2 also contributes to the pdf and changes the parameter vector of the posterior Dirichlet distribution. When the device continuously provides responses that satisfy the system to the highest satisfaction level in the last four rounds, the posterior pdf curve is also narrowed due to the contribution of θ_3.

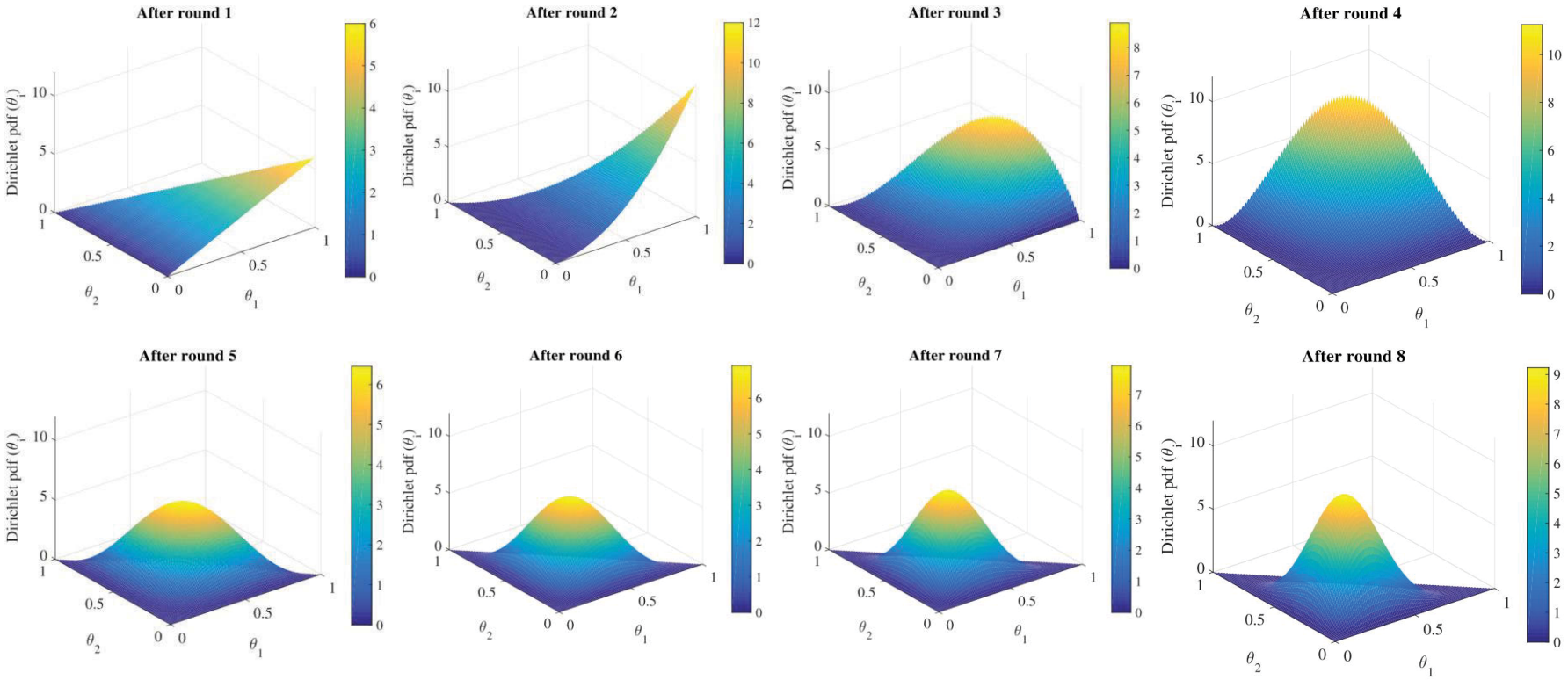


Figure 6.2 The posterior Dirichlet pdf over 8 C-R rounds with the device's response satisfying the system to levels 1, 1, 2, 2, 3, 3, 3, 3 respectively

Figure 6.3 shows the changing of investigated metrics over eight challenge-response rounds. The posterior pdf curve is narrower when more responses are obtained. The expected values $E[\theta_i]$ will be updated to a new value according to the moving of the peak area of the posterior pdf curve. According to predefined weight values, the expected value associated with the probability that a device's response is assigned with the satisfaction level 3 (i.e., $E[\theta_3]$) contributes the most to the average value $\bar{\theta}$. Note that when $\bar{\theta} = 1/3$ the probability distribution of values θ_i is uniform indicating a maximum uncertainty that the system has about the device's behavior. Over eight rounds, the average value $\bar{\theta}$ is lower than 1/3 in the first four rounds and then is higher than 1/3 in the last four rounds. The reason is that over the last four rounds there are contributions of the responses with satisfaction level 3 and its highest weight value to the computation of the average value $\bar{\theta}$.

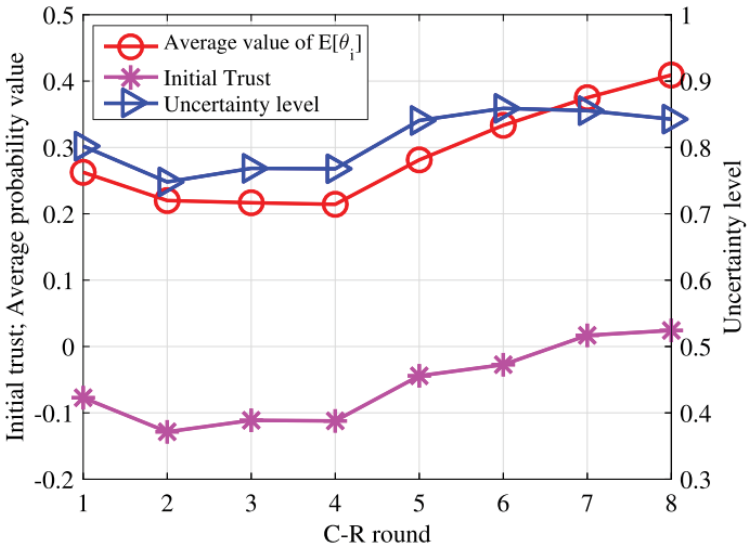


Figure 6.3 Investigated values over 8 challenge-response rounds in Experiment 1

According to the trust interpretation method that considers the average value $\bar{\theta}$, the trust value in the first four challenge-response rounds is interpreted to a distrust value due to the device responses satisfy the system to a low satisfaction level. This trend is kept over the 5th and 6th rounds even though the device satisfies the system to the highest level in these two rounds. The trust level is recovered and slowly gets to the trust plane with a

small value after the 7th round since the device's responses satisfy the system to the highest level over these four rounds leading to a reduction in uncertainty level. In particular, the trust value that the system places on the device is a distrust value at -0.09 and continuously decreases to -0.13 after the first two rounds as the responses satisfy the lowest satisfaction level. The device gradually recovers its trustworthiness since it provides more responses with the highest satisfaction level to the system. Finally, the device is given a small initial trust value of 0.04.

- **Experiment 2**

In this experiment, we simulate an initial trust establishment between an IoT system and a device in five challenge-response rounds where the system defines a five-valued satisfaction level set. In practice, those levels can be mapped to extremely unsatisfied (level 1), unsatisfied (level 2), neutral (level 3), satisfied (level 4) and extremely satisfied (level 5) [6]. The difference between satisfied and extremely satisfied is on the degree that a device's response matches the expectation of the controller. In practice, a device might return a response that satisfies the controller in an aspect but does not satisfy the controller in other aspects. On the other hand, in some cases, the device's response has completely matched the expectation of the controller. It is hard to visualize the posterior pdf shape of the Dirichlet distribution associated with the change of the pdf during the trust knowledge assessment when the five-valued satisfaction level set is used to investigate the device's behavior. Therefore, we only discuss how the uncertainty value, the average value $\bar{\theta}$ and the initial trust value change during the initial trust establishment process. We simulate several devices' behavior patterns to investigate the performance of our proposed approach. The weight values for five satisfaction levels are assigned at 0.03, 0.07, 0.15, 0.25 and 0.5, respectively.

Firstly, we simulate the initial trust establishment between the controller and a device in which the device's responses satisfy the system to the lowest satisfaction level (level 1) in all challenge-response rounds. **Figure 6.4** shows the simulation results from this experiment. The average value $\bar{\theta}$ continuously decreases and is less than 0.2 at which the system has maximum uncertainty in the device's behavior indicating a neutral belief. The uncertainty level is continuously decreased during the simulation. The trust value is

on the distrust plane and goes down from -0.14 to -0.32. This shows the consistency of our trust interpretation approach as it agrees with the trends of the changing of the uncertainty level and the average probability value over the trust evaluation process.

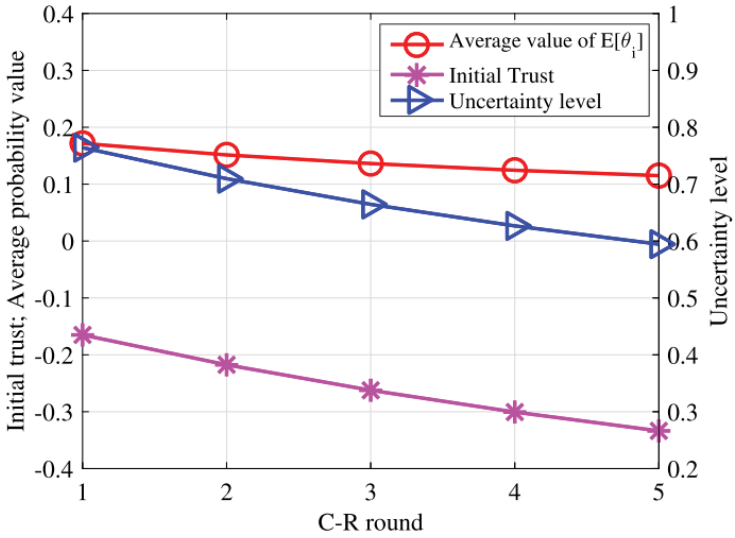


Figure 6.4 Investigated values over 5 C-R rounds with the device's response satisfying the system to level 1 in all rounds

Secondly, we simulate a multilevel initial trust establishment of a controller to a device in which its responses satisfy the system to the highest level (level 5) in all challenge-response rounds.

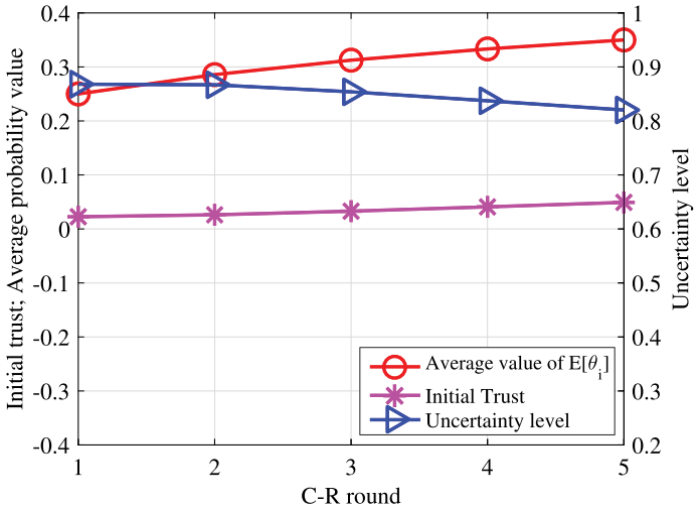


Figure 6.5 Investigated values over 5 C-R rounds with the device's response satisfying the system to level 5 in all rounds

Figure 6.5 presents the simulation results from this simulation. The uncertainty level reduces over five challenge-response rounds since more evidence on the device's behavior is observed from the challenge-response rounds and the device continuously satisfies the system to the highest level. Since the average probability value is greater than 0.2 indicating the trust metric should stay on the trust plane, the device is given a trust value ($T > 0$) over the simulation. However, the trust is slowly increased as we interpret trust in such a way that the speed of gaining trust is less than the rate of losing trust. The trust value is increased from a neutral value at the beginning of the simulation to a small amount of 0.05 indicating the system has a positive initial trust on this new device.

Next, we simulate another multilevel initial trust establishment of the controller of the personal space IoT on a new device in which its responses satisfy the system to a different level including very unsatisfied level, neutral level and very satisfied level. **Figure 6.6** shows the simulation results of this case where the device provides two very unsatisfied responses (level 1) in the first two rounds, followed by a neutral response (level 3) and two very satisfied responses (level 5) in the last two rounds. Firstly, the trust level is on the distrust plane as the device's response does not satisfy the system over the first three challenge-response rounds (two very unsatisfied responses and a neutral response). Then, the device recovers its trustworthiness to a small degree of trust (around 0.035) since its responses are assigned a highest satisfaction level in the last two rounds.

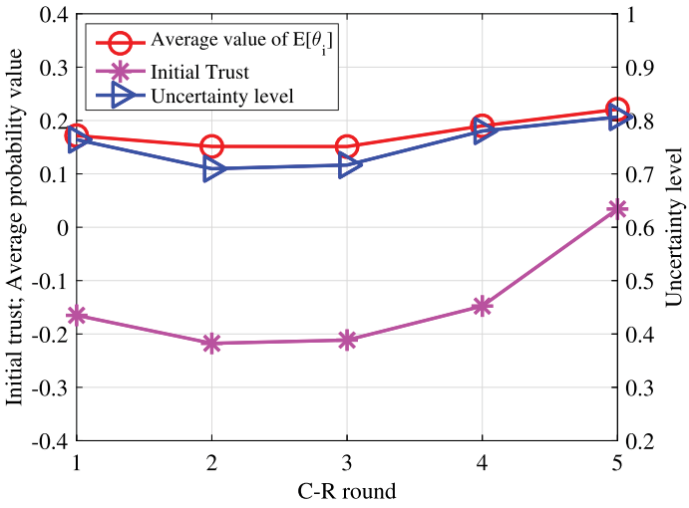


Figure 6.6 Investigated values over 5 C-R rounds with the device's response satisfying the system to levels 1, 1, 3, 5, 5 respectively

Lastly, we simulate a multilevel initial trust establishment between the personal space IoT system and a device in which its responses satisfy the system to level 4 for the first challenge-response round and lower satisfaction levels (level 2 and level 1) at the last four rounds. **Figure 6.7** shows the numerical results from this simulation. We can see that the average value $\bar{\theta}$ continuously decreases over the simulation. The uncertainty level is consistently reduced according to the average value $\bar{\theta}$ indicating the more knowledge that the system learns from the challenge-response process when the device consistently fails to satisfy the system. Explicitly, the device is given a distrust value of -0.2 after five challenge-response rounds due to its unsatisfactory behavior.

In summary, the multilevel trust value is aggregated over the challenge-response process. Our estimation of a device's trustworthiness based on monitoring its uncertainty level and a trust interpretation approach in a multi-valued satisfaction level setup allows the IoT system to consistently investigate the initial trust value of a new device by evaluating the satisfaction level of the device's response to the challenges.

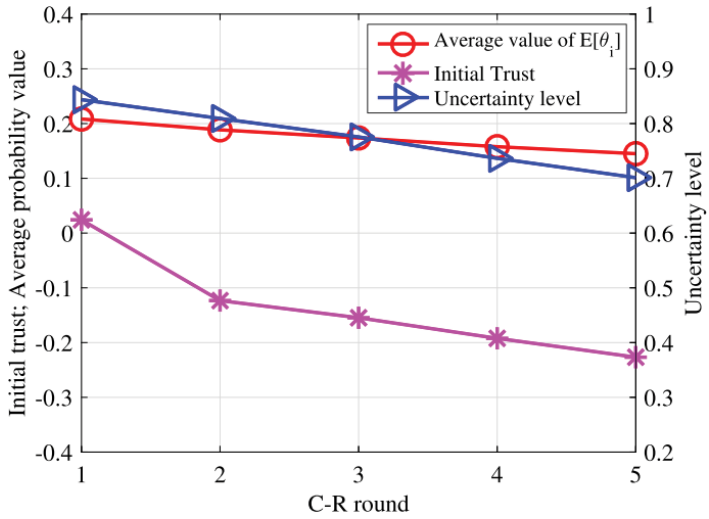


Figure 6.7 Investigated values over 5 C-R rounds with the device's response satisfying the system to levels 4, 2, 2, 1, 1 respectively

6.4 Summary

This chapter presented our proposed multilevel initial trust establishment model for personal space IoT systems. The system relies on the predefined multi-valued satisfaction level set to judge the device's responses via a challenge-response process for collecting the evidence for the trust evaluation. The posterior Dirichlet distribution is exploited as the mathematical foundation for measuring the uncertainty level that the system has about the device's behavior. Then, a trust interpretation approach is proposed to evaluate the initial trust value. The experimental results show that the proposed multilevel initial trust establishment model can consistently determine the initial trust degree of a device by observing its behavior in responding to challenges.

Chapter 7

Challenge-Response Information Design for Initial Trust Establishment

7.1 Introduction

The challenge-response process is the core of the trust evidence generation module in our proposed initial trust establishment architecture. The definition and operations of the challenge-response process are presented in chapter 3, section 3.4.1. The purpose of conducting the challenge-response process at the device admission phase of the IoT systems is to generate meaningful evidence about the trustworthiness of a device for the initial trust assessment. In the challenge-response-based initial trust establishment, the challenger and the responder must implicitly share some knowledge for the trust assessment process to work. Without such implicit information sharing, very little knowledge about each other's trustworthiness can be gained from the challenge-response operations.

In our proposed initial trust establishment models presented in previous chapters, the implicit shared information between the challenges and the responses is assumed and has never been investigated. Specifically, the previous proposed initial trust establishment models assumed that the outputs from the challenge-response operations are the shared knowledge between the challenger and the responder that can be used as the evidence for the trust assessment to work. However, if the information content of the challenges is not

carefully designed from the challenger's perspective over its environment, these challenges might be entirely irrelevant to the devices in its environment. In other words, the potential devices in the personal space IoT environment are ignorant of the challenges. Consequently, the assumption of the shared knowledge between the challenger and the responder is no longer realistic.

It is crucial to engineer the shared information between the challenger and the responder through the challenge-response operations. In particular, it is critical to design the challenge-response process so that the challenger (the controller of the IoT system) can capture related and meaningful knowledge about the trustworthiness of a device through challenge-response operations. Importantly, the information design of the challenge-response process needs to be carefully designed with guiding principles to invite responses from the responders that fit into the challenger's environment and share mutual information with the challenger so that there exists meaningful and relevant knowledge for the challenger to judge the responders' trustworthiness.

In this chapter, we present the *challenge-response information design* for the proposed initial trust establishment model. First, we describe the design settings of the challenge-response information design. We then explore the possible information designs of the challenge-response process and discuss the necessity of design principles. Next, we propose a search algorithm for determining the feasible challenge-response designs that ensure the shared information between the challenger and the responder for a consistent trust assessment. Finally, we conduct extensive simulations based on the feasible challenge-response designs to evaluate the performance of the proposed challenge-response information design and its practical realization and discuss several concerns about its attack defending ability and its delay cost. It is worth noting that this is the first time that the information design of the challenge-response process for the initial trust establishment in IoT systems has been considered. The proposed design and preliminary findings from this work have been published in [120].

The remainder of the chapter is organized as follows. Section 7.2 describes the information design settings. Section 7.3 explores the problems of arbitrary challenge-response information design and defines essential design principles for the challenge-response information design. Section 7.4 describes the search algorithm to seek feasible

challenge-response information designs. Section 7.5 gives the experimental evaluation and the numerical results for various evaluation cases. Finally, section 7.6 summaries the chapter.

7.2 Challenge-Response Information Design – Settings

To address the problem of obtaining irrelevant trust evidence from the challenge-response process, we propose the information design required by the challenge-response process to ensure that the initial trust establishment model works under the meaningful trust knowledge gained from its challenge-response operations.

- **Design settings**

In the information design of the challenge-response process, we consider a challenge as a random variable and design its information content. Here, we follow Shannon [98] in defining the information content of a random variable. According to Shannon, the information content of a challenge in our design does not depend upon the semantics of the challenge itself but relies on the probability of its occurrence. Therefore, we design the information contents of the challenges by designing their probability distribution, i.e., their probability of occurrence.

A challenge can expect many responses from the responders in the target environment. We consider a possible response to a challenge as another random variable. A response occurs conditionally on the occurrence of a given challenge. On the occurrence of a response, it is important to determine if there is shared information between the occurred response and the given challenge. Thus, we design the information content related to the shared information between a possible response and a given challenge by designing a probability of a response conditioned on the given challenge.

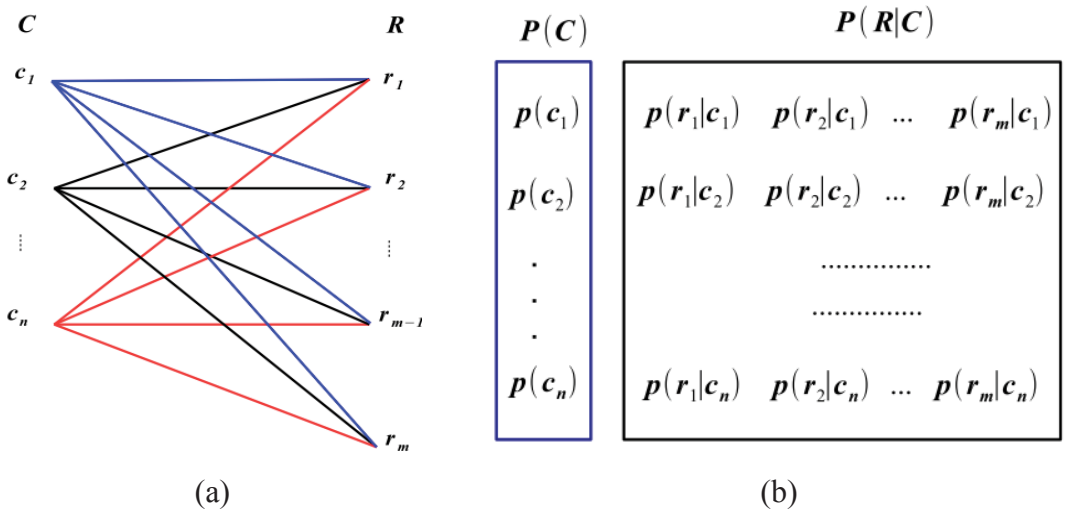
In summary, in our challenge-response information design, we seek to design the probability distribution of the challenges and the probability distributions of possible responses conditioned on the given challenges.

We define a set of events $C = \{c_i\}$ where each c_i represents a challenge and can take on a probability value $p(c_i)$ that refers to its unpredictability level. Then, we design a probability distribution of set C which is denoted by $P(C) = \{p(c_i)\}$.

We also define R as a set of events $R = \{r_j\}$ where each r_j refers to a possible response to a given challenge. To relate the shared information between a challenge in set C and a response in set R, we design a conditional probability distribution of set R given set C which is denoted by $P(R \mid C) = \{p(r_j \mid c_i)\}$ where each $p(r_j \mid c_i)$ represents the probability that response r_j is returned given that challenge is c_i.

In a challenge-response process, there are *n* possible challenges and *m* possible responses to each challenge. We design a set C of *n* events and a set R of *m* events for the design setting of the challenge-response information design as shown in **Figure 7.1**a. There are *m* possible events in set R that have a relation to each event in set C where event r_m represents all responses other than responses $r_1, r_2, ..., r_{m-1}$ so that the probability space of set R is complete.

Figure 7.1b illustrates the numerical presentation of the defined probability distributions (the probability distribution of the challenges and the conditional probability distribution of possible responses given a challenge) in the proposed challenge-response information design. Specifically, one space represents the probability distribution of events in set C that refers to the unpredictability level of challenges in the challenge-response information design, $p(c_i), \forall\, i = 1...n$. The other space represents the conditional probability distributions that are related to the shared information between possible responses in set R and the challenges in set C, $p(r_j \mid c_i), \forall\, i = 1...n; j = 1...m$.



(a) (b)

Figure 7.1 a) Overall setting of the challenge-response information design, b) The numerical presentation of the challenge-response information design

It is noted that for a given challenge, there is a conditional probability distribution of possible responses conditioned on the given challenge. The binding of the probability distribution of the challenge set, $P(C)=\{p(c_i)\}$, and the set of conditional probability distributions, $P(R\,|\,C)=\{p(r_j\,|\,c_i)\}$, are the building blocks of the proposed challenge-response information design.

- **Correlation definition**

Given a challenge and a response occurring in one challenge-response operation, to determine if there is shared information between the challenge and the response, we define a metric called the "correlation" between a challenge and a response. This correlation is the desired outcome of a challenge-response operation which is then used as the basis for the trust assessment. It is important that in any challenge-response operation, there must exist a correlation between the challenge and the response; if no such correlation exists the responder has nothing to do with the challenger. In the following, we describe the quantification of the correlation metric in our challenge-response information design.

In a single challenge-response operation, a challenge c_i is drawn from set C with a probability of $p(c_i)$. Depending on the conditional probability of set R given set C, a

response r_j is determined by the conditional probability, $p(r_j \mid c_i)$. We wish to know the amount of shared information between the response r_j and the challenge c_i. Therefore, we must quantify the correlation between the response r_j and the challenge c_i. We first determine the conditional probability that the challenge is c_i given that the received response is r_j, that is denoted by $p(c_i \mid r_j)$. According to Bayes' formula, $p(c_i \mid r_j)$ can be calculated by (7.1).

$$p(c_i \mid r_j) = \frac{p(r_j \mid c_i)p(c_i)}{p(r_j)} = \frac{p(r_j \mid c_i)p(c_i)}{\sum_{k=1}^{n} p(r_j \mid c_k)p(c_k)} \tag{7.1}$$

As the occurrence of the response r_j redefines the probability distribution of the challenge c_i, we define the correlation between the challenge c_i and the response r_j as the distance between $p(c_i \mid r_j)$ and $p(c_i)$ as shown in (7.2). Δ_{ij} denotes the correlation between the challenge c_i and the response r_j.

$$\Delta_{ij} = p(c_i \mid r_j) - p(c_i) \tag{7.2}$$

The correlation is then utilized as the basis for the trust assessment process. It can be seen in (7.2) that the defined correlation can be positive, negative or non-correlated. We analyze the meaning of each correlation case and discuss its interpretation in the trust domain as follows.

A positive correlation occurs when $p(c_i \mid r_j) > p(c_i)$. It indicates that the device's response and the given challenge are positively correlated. The device's response conveys the expected information to the system that leads to a reduction in the unpredictability of the challenge. In the trust domain, if the system finds a positive correlation from a challenge-response operation, it places a level of trust on the device. The higher the positive correlation is found, the more trust that the device can be given by the system.

A negative correlation is given when $p(c_i \mid r_j) < p(c_i)$. It indicates that the device's response and the given challenge are negatively correlated. This may be interpreted to mean that the response contains factors that interfere with the system's expectation and increase the unpredictability of the challenge. In the trust domain, if the system learns about a negative correlation from a challenge-response operation, it places a distrust level on the device.

A non-correlation happens when $p(c_i \mid r_j) = p(c_i)$. This value indicates that the response does not provide any additional knowledge, and this makes no change in the unpredictability of the challenge. Mapping to the trust domain, the system can only be in the neutral position as it cannot decide whether to trust the device or not.

- **Requirements for the consistent correlation**

As the correlation is the basis for the trust assessment, the information design of the challenge-response process must provide consistent correlations between the challenges and the responses so that a trust assessment scheme can consistently determine the trust level of the responder based on the challenge-response operations. Consistent correlations from the challenge-response information design mean that there is consistency in the *direction* and the *strength* of the relationship between the challenges and the responses in the design. Thus, there are two main requirements that a challenge-response information design must satisfy to provide consistent correlations.

- First, the *direction* of the relationship between a challenge and a response (determined by the sign of the correlation) must be consistent with the quality of the response (e.g., intended response or unintended response). Here, we define an intended response is the response that the system intends to get from a device when it designs a challenge.
- Second, the unpredictability level of a challenge is related to the significance of the information learned from the occurrence of an intended response towards this challenge. Information acquired from an intended response towards a more unpredictable challenge is expected to be more significant than that towards a less unpredictable challenge. Thus, the *strength* of the relationship between a challenge and its intended response (determined by the

size of a positive correlation) needs to consistently reflect the appropriate amount of information learned from the occurrence of the challenge and its intended response.

7.3 Principles for the Challenge-Response Information Design

In this section, we first explore the possible challenge-response process information designs by arbitrarily choosing the probability distribution arrangement and analyzing the problems of using the arbitrary challenge-response designs for the initial trust establishment. Then, we introduce the guiding principles for the challenge-response information design to determine the feasible information designs so that the initial trust establishment based on these feasible designs will work consistently.

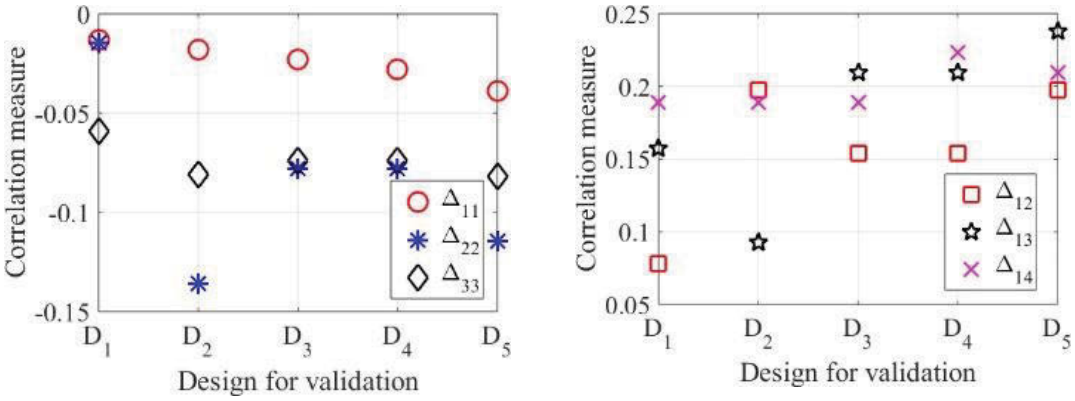
7.3.1 Problems of Challenge-Response Information Designs without Principles

Clearly, one may start with an arbitrary probability distribution for the challenge P(C). For a given probability distribution P(C), there is an infinite number of conditional probability distributions, P(R|C), that can be assigned. Each pairing of P(C) and P(R|C) is considered as an information design of the challenge-response process. Many pairings of P(C) and P(R|C) do not produce consistent correlations. In the following, we show some examples of the challenge-response information designs that do not provide consistent correlations.

For demonstration, we validate the information designs of a challenge-response process with the following settings: there are a set of three challenges (c_1, c_2, c_3) with probabilities $p(c_1), p(c_2), p(c_3)$ and a set of four responses (r_1, r_2, r_3, r_4). We choose to investigate designs of a given challenge space with the probability distribution of $P(C) = \{0.7, 0.2, 0.1\}$ and arbitrary configurations of P(R|C) without any guiding principles. It is worth noting that choosing an optimal configuration of P(C) for a

challenge-response process depends on the specific environment and the purpose of the challenger. We assess whether there are pairings of P(C) and P(R|C) designed without any guiding principles, that do not provide consistent correlations.

According to the requirement for a consistent correlation, the feasible information designs for the above challenge-response process's settings must satisfy the following conditions. First, when sending out the challenge c_i, the system expects to receive the intended response $r_i, \forall i = 1...3$. Referring to the correlation definition and quantification, for every challenge c_i, if the device's response is close enough to the intended response r_i, a positive correlation is reasonable and desired. Otherwise, a non-positive correlation is expected. Second, receiving an intended response towards a more unpredictable challenge c_3 with $p(c_3) = 0.1$ is more valuable in terms of gaining more information about the responder than that regarding a less unpredictable challenge c_1 with $p(c_1) = 0.7$. A consistent information design of this challenge-response process needs to satisfy those mentioned features.



(a) (b)

Figure 7.2 Example of arbitrary designs a) when a positive correlation is desired, b) when a negative correlation is desired

In many pairings of $p(c_i) = \{0.7, 0.2, 0.1\}$ and $p(r_j \mid c_i), (\forall i = 1...3; \forall j = 1...4)$, the conditional probabilities $p(r_j \mid c_i)$ are such that when r_i is received as the intended

response to the challenge $c_i, (\forall i = 1...3)$, the correlation is non-positive instead of a positive value as expected (this violates the first requirement of the consistent correlation). For example, **Figure 7.2**a shows the correlations from five information designs of a given $p(c_i) = \{0.7, 0.2, 0.1\}$ and various configurations of $p(r_j \mid c_i)$, (in designs D_1, …, D_5). As we can see, in all designs, a negative correlation between c_i and $r_i, (\forall i = 1...3)$ is achieved instead of a positive correlation. In contrast, **Figure 7.2**b indicates that in all five considered designs the correlations between challenge c_1 and its unintended responses, i.e., r_2, r_3, r_4 are positive while the non-positive correlations are intended (this also violates the first requirement of the consistent correlation). It can be seen that these designs (D_1, …, D_5) do not provide consistency in the *direction* of the relationship between the challenges and the responses (the sign of the correlations).

The reason for this violation can be explained as follows. As designed, a response r_i is related to all challenges with different conditional probabilities. Therefore, when r_i is designed as the intended response to a challenge c_i, the design of $p(r_i \mid c_i)$ and other $p(r_i \mid c_k)$ decides the direction of the correlation. When the relation of the response r_i with the challenge c_i is weaker than that of the response r_i with other challenges c_k, i.e., $p(r_i \mid c_i) < p(r_i \mid c_k), (\forall k \neq i)$, it will result in a negative correlation between the response r_i and the challenge c_i due to the strong interference of other unintended responses to the challenge c_i.

Many other designs provide correlations that are consistent in terms of the direction of the relationship (the sign of the correlation) but are inconsistent regarding the strength of the relationship (correlation's size) as they do not account for the unpredictability of the challenge. **Figure 7.3** shows the correlation between the challenge c_i and its intended response $r_i, (\forall i = 1...3)$, with the challenge-response information designs of the given configuration of $p(c_i) = \{0.7, 0.2, 0.1\}$ and various configurations of $p(r_j \mid c_i)$, (designs

D_6 – D_{10}). It is expected that the size of the correlation between challenge c_3 and its intended response r_3 is highest since c_3 is the most unpredictable challenge $(p(c_3) = 0.1)$. However, in all tested designs (D_6 – D_{10}), the correlation between the challenge c_3 and intended response r_3 is positive but less than that between the challenge c_2 and its intended response r_2, where the challenge c_2 is less unpredictable then challenge c_3. This indicates the inconsistent correlation in terms of correlation's size, i.e., it violates the second condition.

The reason for this violation is that the designs in **Figure 7.3** do not take into account the unpredictability level of the challenges when designing the conditional probability distribution P(C|R). Hence, the size of the correlations between each challenge and its intended response does not reflect the significance of the obtained information appropriately according to its unpredictability level. Specifically, each challenge is spread out to all possible responses with different conditional probabilities. The distribution of the conditional probabilities and the unpredictability of a challenge directly affect the size of the correlation. It implies that the designed correlation needs to be inversely proportional to the unpredictability of the challenge.

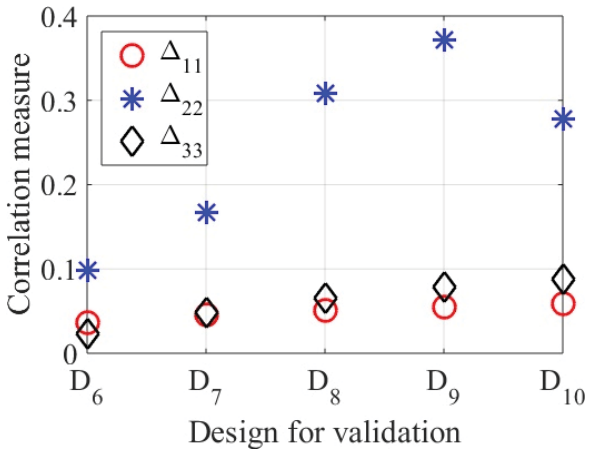


Figure 7.3 Example of arbitrary designs where the positive correlation is inconsistent with challenge's unpredictability level

7.3.2 Design Principles

Pairing the challenges and the responses in an arbitrary way does not always produce a consistent correlation as the responders may be ignorant of the challenges. Hence, they cannot provide shared information so that the challenger can assess the trustworthiness of the responders. Specifically, as a random variable can take on any probability distribution of its occurrence, there is an infinite number of configurations for the probability distribution of the challenge set, P(C). Similarly, there are many possible configurations for the conditional probability distribution of the responses given a challenge, P(R|C).

As pointed out in the earlier section, many challenge-response information designs based on the binding of arbitrary probability distributions P(C) and P(R|C) do not provide consistent correlations for a consistent trust assessment process. As a result, it is necessary to establish design principles in the challenge-response information design to provide feasible information designs that engineer consistent shared information between the challenges and the responses for the consistent trust assessment.

In the following, we establish essential principles and their entailed conditions to guide the information design of the challenge-response process so that the responder would yield responses consistently to the challenges in the design. Hence, the information design allows the challenger to gain meaningful trust evidence for the trust evaluation module to work.

- **Intended Response – Positive Correlation Consistency Principle**

According to section 7.3.1, not all possible pairings of the probability distributions P(C) and P(R|C) can produce consistent correlations between the challenges and the responses. For a given challenge, if the response is an intended response of the challenge, it is logical and desirable to expect that the correlation between the challenge and its intended response is positive. It is also expected that the direction of the correlation between the challenge and unintended responses must be distinguished from that between the challenge and the intended response. Consequently, we define the “intended response - positive correlation” consistency principle as follows.

"***The correlation between a challenge and its intended response has to be positive; and the correlation between a challenge and an unintended response is non-positive.***"

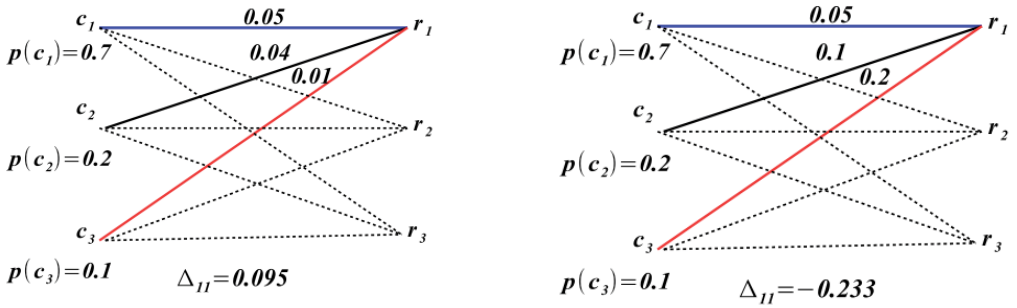
Specifically, an information design of the challenge-response process must arrange defined probability distributions so that for any challenge-response operation the system can work out from the correlation metric if the response is an intended one. The conditions behind this principle for the design of a challenge-response process with *n* challenges and *m* responses are formulated as below.

$$\begin{aligned} &\Delta_{ij} = p(c_i \mid r_j) - p(c_i) > 0 \\ &\Leftrightarrow \frac{p(r_j \mid c_i)p(c_i)}{p(r_j \mid c_i)p(c_i) + \sum_{k=1,k\neq i}^{n} p(r_j \mid c_k)p(c_k)} - p(c_i) > 0 \\ &\Leftrightarrow p(r_j \mid c_i)(1 - p(c_i)) > \sum_{k=1,k\neq i}^{n} p(r_j \mid c_k)p(c_k) \end{aligned} \tag{7.3}$$

Firstly, the condition for a positive correlation between a challenge c_i and a response r_j is given in (7.3). An intended response is distinguished from other responses by a positive correlation between it and the challenge. For this to be satisfied, the design of probability distributions related to the challenges and the responses must satisfy (7.3). In some cases, an intended response, say r_j, to the challenge c_i can take on a very small conditional probability value $p(r_j \mid c_i)$. It is crucial that the conditional probability of the challenge c_i given the occurrence of the response r_j, $p(c_i \mid r_j)$, must be positively correlated to the original probability of the challenge c_i, $p(c_i)$, to ensure a positive correlation between the challenge c_i and its intended response r_j.

Figure 7.4 shows the arrangement of the probability distributions of two information designs of the challenge-response process regarding a requirement of a positive correlation. Specifically, **Figure 7.4**a shows the arrangement of probability distributions of a design that satisfies the condition in (7.3) and provide a positive correlation between the challenge c_1 and its intended response r_1, $(\Delta_{11} = 0.095)$ even when $p(r_1 \mid c_1)$ is very small at 0.05. For the same value of $p(r_1 \mid c_1)$, the design described in **Figure 7.4**b does not satisfy

the condition in (7.3). It produces a negative correlation between the challenge c_1 and its intended response r_1 $(\Delta_{11} = -0.2333)$ partially caused by the undue influence of the challenge c_2 and c_3 through $p(r_1 | c_2)$ and $p(r_1 | c_3)$.



(a) (b)

Figure 7.4 a) A design provides a positive correlation as expected; b) A design provides a negative correlation instead of a positive correlation

Secondly, the condition for a non-positive correlation between a challenge c_i and a response r_j is given in (7.4).

$$\begin{aligned} &\Delta_{ij} = p(c_i \mid r_j) - p(c_i) \le 0 \\ &\Leftrightarrow p(r_j \mid c_i)(1 - p(c_i)) \le \sum_{k=1, k \ne i}^{n} p(r_j \mid c_k) p(c_k) \end{aligned} \tag{7.4}$$

The challenge-response information designs must also satisfy the condition in (7.4) to ensure that the correlation between a challenge c_i and its unintended responses, say r_j is non-positive. It is crucial that given the occurrence of the unintended response r_j the conditional probability of the challenge c_i, $p(c_i | r_j)$, must be negatively correlated or not be correlated to the original probability of the challenge c_i, $p(c_i)$, to ensure a non-positive correlation between the challenge c_i and its unintended responses.

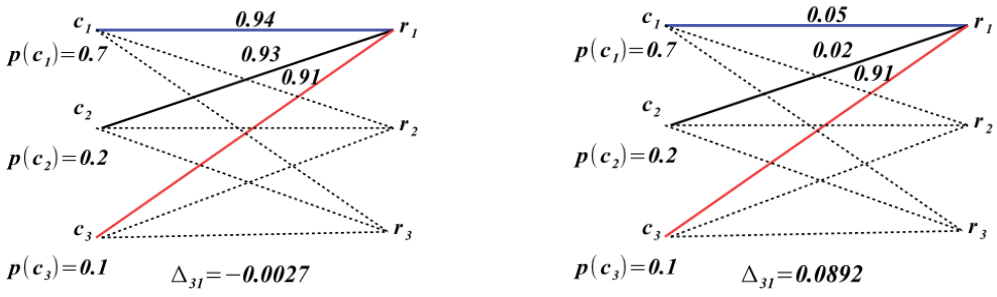


Figure 7.5 a) A design provides a negative correlation as desired, b) A design provides a positive correlation instead of a negative correlation

Figure 7.5 shows the arrangement of the probability distributions of two information designs of the challenge-response process regarding a requirement of a non-positive correlation. Specifically, **Figure 7.5**a shows the arrangement of the probability distributions of a design that satisfies the condition in (7.4). It provides a negative correlation between the challenge c_3 and its unintended response r_1, $(\Delta_{31} = -0.0027)$ even when $p(r_1 | c_3)$ is very large at 0.91. In contrast, for the same value of $p(r_1 | c_3)$, **Figure 7.5**b shows the arrangement of probability distributions of a design that does not satisfy the condition in (7.4) and produces a positive correlation $(\Delta_{31} = 0.0892)$ between the challenge c_3 and its unintended response r_1 instead of a non-positive correlation as desired.

The non-correlation occurs when the equality in (7.4) is satisfied. This case happens when the system receives a response r_j to the challenge c_i, but it does not learn any additional knowledge about the responder. Therefore, the design of probability distributions must satisfy the equality in (7.4) to indicate that a response has no relation to the challenge.

Consequently, to produce consistent correlations, firstly the information design of the challenge-response process must satisfy the conditions of the intended response–positive correlation consistency principle expressed in (7.3) and (7.4).

- **Information Entropy – Consistency Principle**

This principle relies on the fundamental idea of information theory and has regard to the consistency in the size of the correlation between a challenge and a response (the strength of the relationship between them) based on defined probability distributions.

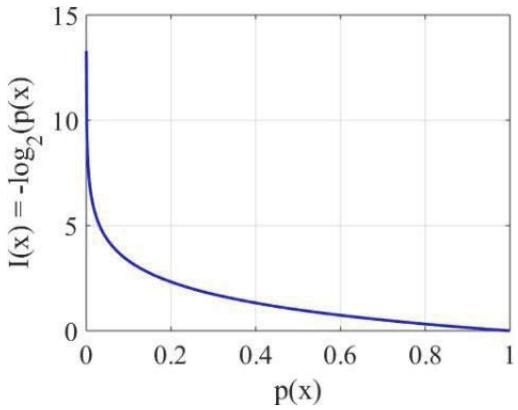


Figure 7.6 Information entropy of a random event [121]

According to information theory, the entropy of a message is inversely proportional to the message likelihood (the probability of occurrence of the message) [121]. This means that learning about an unlikely event that has occurred is more informative than learning of the appearance of a likely event. **Figure 7.6** shows the information measure (or the information entropy) from the occurrence of a random event '*x*' with the probability of occurrence value *p(x)*. It can be seen that the more likely an event '*x*' will occur, the less information one can learn when it occurs [98].

Similarly, in a challenge-response operation, the challenge which has a lower probability of occurrence (an unlikely event) can reveal more useful information than that of other challenges which have a higher probability of occurrence (more likely event), when intended responses are provided. For this to be guaranteed in the information design of a challenge-response process, we define the information entropy - consistency principle as follows.

"***The correlation between a challenge and its intended response is inversely proportional to the probability of its occurrence.***"

This principle states that the design of probability distributions for the challenge and the response must ensure that the size of the positive correlation between a challenge and its intended response is inversely proportional (non-linearly) to its probability of occurrence. More specifically, the size of a positive correlation between a highly unpredictable challenge and its intended response should be larger than that associated with a more likely challenge and its intended response.

The condition entailed in this principle is expressed as follows. For different challenges c_i and c_j with the unpredictability that $p(c_i) < p(c_j)$ and their intended responses, r_i and r_j, respectively, the correlations between these challenges and their intended responses are given as below.

$$\Delta_{ii} = p(c_i \mid r_i) - p(c_i) \tag{7.5}$$

$$\Delta_{jj} = p(c_j \mid r_j) - p(c_j) \tag{7.6}$$

To ensure the information entropy - consistency principle, the design of probability distributions must satisfy the following condition.

$$\Delta_{ii} > \Delta_{jj}, \quad for\ \forall i, j\ \&\ p(c_i) < p(c_j) \tag{7.7}$$

Figure 7.7 shows the arrangement of the probability distributions of two information designs of a challenge-response process which consists of three challenges and three responses. Assuming that r_1, r_2, r_3 are the intended responses of the challenges c_1, c_2, c_3, respectively. The probability distribution of the challenge set is given as $p(c_1) > p(c_2) > p(c_3)$. **Figure 7.7**a illustrates the probability distributions of a design that satisfies the conditions of both guiding principles: the intended response – positive correlation consistency principle and the information entropy consistency principle. In contrast, **Figure 7.7**b describes a design that does not meet the guiding principles.

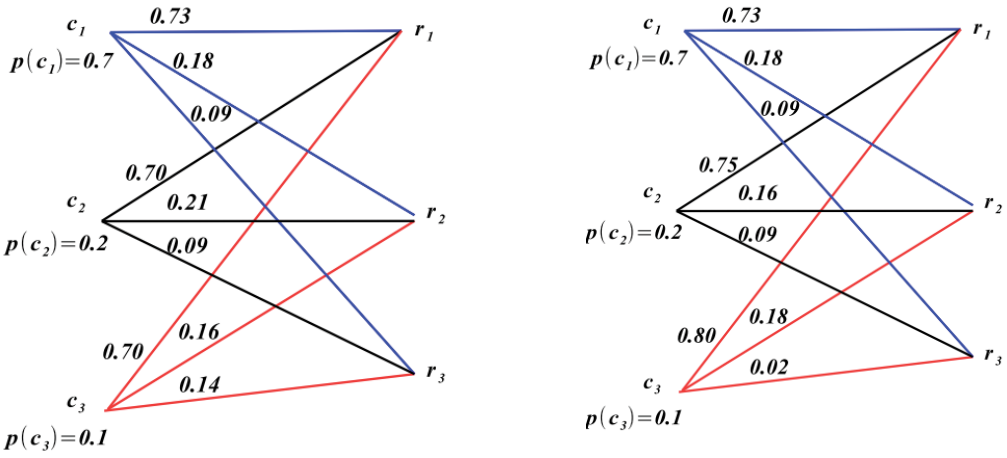


Figure 7.7 a) A design meets defined principles where $\Delta_{11} = 0.0087 < \Delta_{22} = 0.0283 < \Delta_{33} = 0.0474$ & others are negative, b) A design does not meet defined principles where $\Delta_{11} = -0.01$; $\Delta_{22} = -0.018$; $\Delta_{33} = -0.076$ & others are positive

By combining the two principles, we establish the entailed conditions for a feasible information design of a challenge-response process for the initial trust establishment as below.

$$\Delta_{ii} > \Delta_{jj} > 0, \quad \forall i, j, \, for \; p(c_i) < p(c_j) \tag{7.8}$$

$$\Delta_{ij} \leq 0, \text{ for } r_j \text{ are unintented response to } c_i, \forall i, j \tag{7.9}$$

In summary, by establishing two design principles and their entailed conditions, we arrive at feasible designs that can distinguish intended responses from others and prioritize the size of positive correlations based on the challenges' unpredictability by providing consistent correlations. Intuitively, the feasible information designs of the challenge-response process are designs that allow the system to achieve shared information between a challenge and a response in any challenge-response operation that is the basis for a consistent trust assessment.

7.4 Search Algorithm for Feasible Challenge-Response Information Design

We propose a search algorithm for finding feasible information designs of the challenge-response process. The search algorithm is proposed to demonstrate that with a given environment configuration, there always exists feasible solutions for the information design of the challenge-response process. Specifically, a feasible information design of the challenge-response process provides P(C) and P(R|C) and ensures that the pairing of these probability distributions meet the design principles and provide consistent correlations between the challenges and the responses. Note that unfeasible designs are the ones that provide inconsistent correlations (as shown in section 7.3.1) and hence result in an inconsistent trust evaluation.

In the search algorithm, we find feasible designs that satisfy all the constraints generated from the defined guiding principles. We do not attempt to do an exhaustive search for all solutions. Instead, we focus on finding feasible designs that ensure all constraints to demonstrate the existence of feasible designs of the challenge-response process. Furthermore, an optimal design relies on other factors concerning the target environment and the specific goal of the challenges and is not within the scope of this thesis.

In general, it is possible that there is more than one intended response to a given challenge. For simplicity, we chose a corresponding response as the intended response where its information content ensures the closeness to the system's expectation. We assume that the corresponding response has an identical label with the challenge. Explicitly, for the challenge c_i, its intended response is $r_i, (\forall i = 1...n)$.

Algorithm 7.1 The Search Algorithm

Objective: Finding consistent and feasible information designs for the challenge-response process

Inputs:

n: number of challenges

m: number of possible responses to a given challenge, response m^{th} refers to all other responses that are not specified

$p(c_1), p(c_2), ..., p(c_n)$: assigned probability of challenges $c_1, c_2, ..., c_n$

Outputs:

The matrices of conditional probability distribution:

$[p(r_j|c_1); p(r_j|c_2); ...; p(r_j|c_n)], \forall j = \{1...m\}$ that satisfy the defined principles

Assumptions:

r_i is the intended response to challenge c_i, $\forall i = \{1..n\}$, other responses $r_j \neq r_i$, $\forall j = \{1..m\}$ are unintended

1: **for** each matrix $[p(r_j|c_i)]^{n \times m}$ where $p(r_j|c_i) \in [0.01 : 0.01 : 0.99]$, $\forall i = \{1..n\}, \forall j = \{1...m\}$ **do**
2: $p(c_i|r_j) = \frac{(p(r_j|c_i)p(c_i))}{\sum_{k=1}^{n} p(r_j|c_k)p(c_k)}, \forall i, j, k;$
3: $\Delta_{ij} = p(c_i|r_j) - p(c_i);$
4: $\Delta_{ii} = p(c_i|r_i) - p(c_i);$
5: $\Delta_{jj} = p(c_j|r_j) - p(c_j);$
6: //Verify the "intended response - positive correlation consistency principle"
7: **for** any $\Delta_{ii}, \forall i = \{1...n\}$ **do** ▷ With intended responses
8: **if** $\Delta_{ii} > 0$ **then**
9: *Continue*;
10: **else**
11: *Break*;
12: **end if**
13: **end for**

```
    for any Δ_ij, ∀i = {1...n}, ∀j = {1...m}, i ≠ j do        ▷ With other responses
        if Δ_ij ≤ 0 then
            Continue;
        else
            Break;
        end if
    end for
    //Verify the "information entropy - consistency principle"
    for any p(c_i) < p(c_j), ∀i ≠ j do
        if Δ_ii > Δ_jj then
            Continue;
        else
            Break;
        end if
    end for
    Record satisfied matrices
end for
return : Satisfied matrices[p(r_j|c_i)]^{n×m}, ∀i = {1...n}, ∀j = {1...m}
```

According to the intended response – positive correlation consistency principle, the design must select relevant probabilities so that the correlation between the challenge c_i and its intended response r_i is always positive. Also, the correlation between the challenge c_i and other responses (other than r_i) is non-positive. In addition, according to the information entropy - consistency principle, the size of the correlation is also affected by the probability of occurrence of the challenge. We design the relevant conditional probabilities of the responses considering the challenge's unpredictability level to make sure that the size of the desired correlation is inversely proportional to the challenge's unpredictability.

In the search algorithm, the probability for each challenge is randomly arranged so that a complete probability space is ensured. Then, the algorithm will search for feasible designs based on given probabilities of the challenges and the defined principles.

Specifically, the inputs of the algorithm include the number of challenges, the probabilities of all challenges, and the number of possible responses to each challenge. The outputs of the algorithm are matrices of conditional probabilities with a size of $(n \times m)$ where each row consists of *m* conditional probabilities of the responses given a challenge. The conditions entailed in the design principles are used to generate the constraints that are then verified with all possible probability arrangements to find feasible solutions. If these constraints are met using a matrix of $[p(r_j \mid c_i)]^{n \times m}, (\forall i = 1...n, \forall j = 1...m)$, the algorithm stores this matrix and checks other possible matrices. The pseudo-code of our proposed search algorithm is presented in **Algorithm 7.1**.

7.5 Experimental Evaluation

This section presents the experimental evaluation of the information design of the challenge-response process used in the initial trust establishment in a personal space IoT system. Various information designs found from the search algorithm are validated to demonstrate the consistency in the correlations provided by these designs.

As the correlation between a challenge and a response is the basis for the trust assessment, we define the trust level that the system places on a device after a single challenge-response round as a function of the correlation. Clearly, many functions relating the correlation to the trust level are possible depending on various evaluation criteria including priority, time, operating environment, and preferred interpretations. In this thesis, we use the correlation between the sent challenge and the received response in a challenge-response round directly as the instant trust level. Explicitly, the instant trust level τ is determined from the correlation between a challenge c_i and its response r_j as given in (7.10).

$$\tau = T[c_i, r_j] = \Delta_{ij} \tag{7.10}$$

The initial trust level that the challenger gives the device is obtained from a challenge-response process that consists of multiple challenge-response rounds. There are many ways to compute the initial trust from the instant trust values obtained at the end of each

challenge-response round. For example, initial trust value can be aggregated from all instant trust values obtained from each round. Another way can be averaging the instant trust values from challenge-response rounds with different weight values.

In this thesis, without loss of generality, we simply compute the initial trust value by aggregating the instant trust values from all rounds in the challenge-response process. The initial trust value that the system places on a device after an *N-round* challenge-response process is given in (7.11).

$$T = \sum_{k=1}^{N} \tau_k \tag{7.11}$$

We also define two thresholds for the initial trust assessment process. A value called the *trust threshold* is set to determine if a device gets an acceptable initial trust value for further interactions. The other value called *distrust threshold* is set to determine when a device is distrusted and cannot recover its trustworthiness. The challenge-response process will be terminated once the aggregated initial trust value is beyond any threshold.

7.5.1 Simulation Setup

The experiments simulate the initial trust establishment procedure in a personal space IoT that uses the challenge-response information designs found from the search algorithm for its challenge-response process. In each C-R round, the challenge and the response are generated according to their relevant probabilities specified in the information design. We select the challenge by executing a program that chooses a challenge based on its probability distribution. The response is selected from its conditional probability distribution related to the probability distribution of the selected challenge. As defined, we investigate the instant trust level obtained from each challenge-response operation and the initial trust level that the system places on the device according to its responses during the challenge-response process. The initial trust establishment completes after a predefined number of rounds, or one of the thresholds is met.

We use two information designs found from the proposed search algorithm. The designed probability distributions of these information designs are described in **Table 7.1**. Design 1 is the challenge-response information design for the settings of three

challenges and three responses towards each challenge. Design 2 is the challenge-response information design for the settings of three challenges and four responses towards each challenge.

Table 7.1 Information designs used in the experimental evaluation

Design 1		**Design 2**	
P(C)	P(R|C) (j = 1…3)	P(C)	P(R|C) (j = 1…4)
$p(c_1) = 0.7$	$p(r_j\|c_1) = 0.71; 0.18; 0.11$	$p(c_1) = 0.6$	$p(r_j\|c_1) = 0.51;0.34;0.02;0.13$
$p(c_2) = 0.2$	$p(r_j\|c_2) = 0.70; 0.25; 0.05$	$p(c_2) = 0.3$	$p(r_j\|c_2) = 0.50;0.36;0.01;0.13$
$p(c_3) = 0.1$	$p(r_j\|c_3) = 0.70; 0.06; 0.24$	$p(c_3) = 0.1$	$p(r_j\|c_3) = 0.50;0.31;0.06;0.13$

7.5.2 Numerical Results

- **Investigation of the instant trust value from a single challenge-response operation**

We interpret the correlation between a challenge and a response from a challenge-response operation into an instant trust value. In this section, we investigate the instant trust value that is obtained from a single challenge-response operation by conducting two experiments of a trust assessment with one-round challenge-response (C-R) process. The challenge-response information designs used in the simulations are described in **Table 7.1**. Note that the designs used in our experiments consider the corresponding response as the intended response to a challenge, i.e., when the system sends a challenge c_i, the intended response is r_i.

For each experiment, we generated 50 test cases for the one-round C-R process. In each test case, a correlation between the challenge and its response is produced. Then, the instant trust value from the one-round C-R process is determined based on this correlation.

- ***Experiment with Design 1:***

Figure 7.8 shows the investigation of the instant trust value from each simulation run (test case) using Design 1 with its designed probability distribution as is described in

Table 7.1. When a device provides an intended response to the selected challenge, it is given a positive instant trust level that is interpreted from the positive correlation between the device's response and the sent challenge. The degree of this instant trust is appropriate to the challenge's unpredictability. Precisely, the instant trust level that the system places on the device when it provides intended response to the challenge c_3 is highest (0.116) compared to that when it provides intended response to the challenge c_1 (0.003) and to the challenge c_2 (0.0747) as c_3 is the most unpredictable challenge. In contrast, when the device returns an unintended response to the challenge, it is given a negative trust level (distrust) that is interpreted from the negative correlation between the device's response and the sent challenge. The information design of the challenge-response process described in Design 1 provides consistent correlation for the initial trust establishment. Specifically, the challenge-response process using this design always produces consistency in the direction and the strength of the relationship between the challenges and the responses that are generated in all test cases.

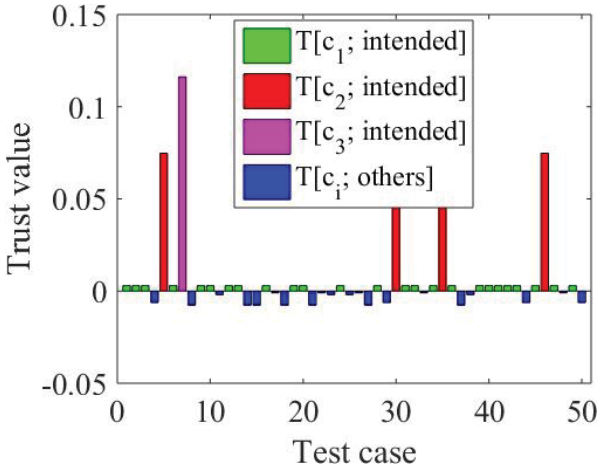


Figure 7.8 The instant trust value obtained from the one-round C-R process in test case 1st to test case 50th using Design 1

- ***Experiment with Design 2:***

Figure 7.9 shows the investigation of the instant trust value computed from each test case of a one-round challenge-response process that uses the challenge-response design as described in Design 2 in **Table 7.1**. The instant trust value that the system places on a

device when it provides an intended response to the challenge is positive. Otherwise, the system places a negative instant trust value (distrust) on the device. The level of the distrust depends on the size of the negative correlation. It can be seen that the challenge with high unpredictability is rarely chosen (here it is the challenge c_3). When it is selected, and the device provides an intended response, the device is given a positive trust value that is significantly higher than that when the device provides an intended response to other challenges. Particularly, when the challenge c_3 is selected, and the device's response is its intended response r_3, the instant trust value that the system places on this device is 0.185. This positive trust value is significantly higher than that when the device provides the intended response r_1 to the challenge c_1 (0.004) and r_2 to challenge c_2 (0.015), respectively. The information design for the challenge-response process described in Design 2 in **Table 7.1** also provides consistent correlation for the initial trust establishment where the consistency in the direction and the strength of the relationship between the challenge and the response generated in all test cases are ensured.

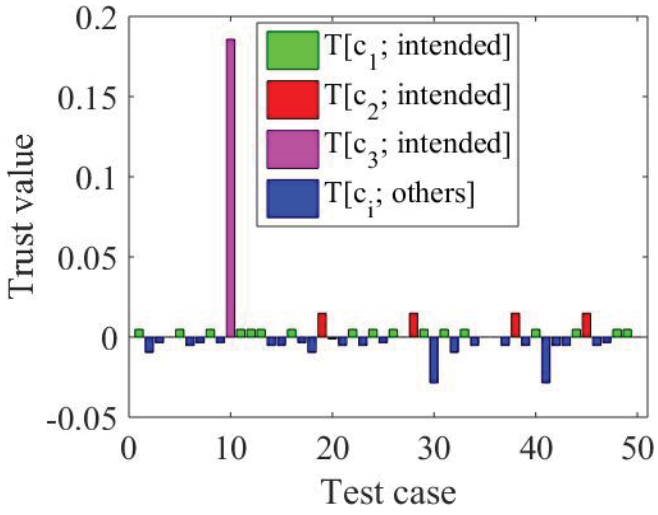


Figure 7.9 The trust value from the one-round C-R process in test 1st to test 50th using Design 2

In summary, the simulation results from the above experiments show that the information designs found from our search algorithm for the two challenge-response process settings provide consistency in the direction and strength of the correlation measure between a challenge and a response in any challenge-response round. This ensures the consistency in the instant trust calculation for a single challenge-response

process. In the next evaluation, we investigate whether these designs ensure that the initial trust value aggregated over the challenge-response process captures the device's behavior consistently and correctly.

- **Investigation of the initial trust value**

In this section, we investigate the initial trust value obtained from two experiments that conduct an initial trust establishment process based on a challenge-response process that uses the challenge-response information designs as described in **Table 7.1**. In the experiment that uses Design 1 for the required challenge-response information design, we conduct a three-round C-R process for the initial trust establishment process. In the experiment with Design 2, we conduct a five-round C-R process. Each experiment is repeated in 100 simulation runs to simulate different device's response patterns to various challenge's patterns from the system. It is noted that the number of rounds for the challenge-response process depends on the time window that is assigned for the system initialization and the requirements of trust thresholds. We choose a trust threshold at 0.35 and a distrust threshold at -0.3 [122] for simulations even though the optimal thresholds can be different depending on applications' demand or the operating environment of an IoT system.

As shown in the previous investigation, in the one-round C-R process the instant trust value computation from Design 1 and Design 2 is consistent with the defined principles. The simulation results from the experiments in this investigation show that the initial trust value aggregated from all rounds of the C-R process consistently reflects the device's behavior patterns. For different device's response patterns, the initial trust value is updated over the C-R process and aggregated to a reasonable initial trust degree.

- ***Experiment with Design 1:***

Figure 7.10 shows the initial trust value obtained from the challenge-response process in six selected simulations that use the Design 1 as described in **Table 7.1** for generating the challenge-response operations. The initial trust value is updated over three rounds. There are several trends in the aggregation of the initial trust level that the system places on the device. We choose to show the results from six simulations which indicate the typical trends.

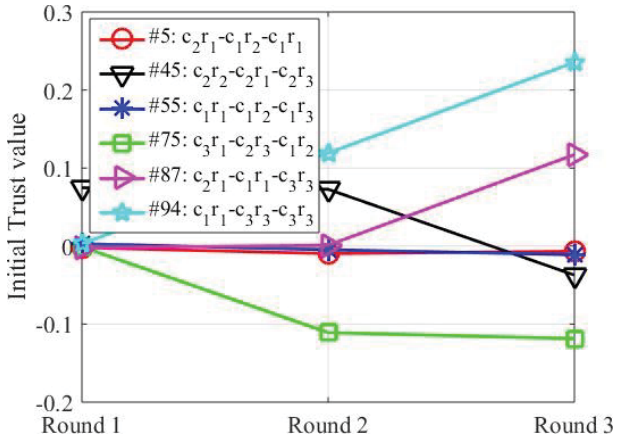


Figure 7.10 Initial trust value aggregated over the three-round C-R process in different simulations using Design 1

The first trend is that the initial trust value of a device is reinforced over three rounds where the device provides intended responses to all challenges. For example, in the 94th simulation, the initial trust value is increasing and reaches a value of 0.24. Similarly, when the device fails to provide an intended response to the first challenge, it first gets a distrust value. However, since the device provides the intended responses to subsequent challenges, its initial trust level is recovered and reinforced to a trust value. For instance, the initial trust trend from the 87th simulation represents this trend where it is labeled by a distrust of -0.002 after the first round and then achieves an initial trust value of 0.11 after the three-round C-R process.

The second trend indicates that the initial trust value is decreased over three rounds because the device fails to provide the intended response to the challenge in all rounds. For example, in the 75th simulation, the initial trust value is decreasing and reaches a value of -0.113 after three rounds. A similar trend can be observed when the device provides an intended response in the first round of the challenge-response process and then fails to do so in the rest of the process. For example, in the 45th simulation, the initial trust value that the system places on the device is at a trust value of 0.07 after the first round and then decrease to distrust value of -0.0425 after three rounds.

Another trend is that the initial trust value slightly fluctuates and almost keeps at the neutral position during the C-R process due to the device does not consistently providing

an intended response to the highly unpredictable challenges. For example, the initial trust values from the fifth and 55th simulations show this trend.

- ***Experiment with Design 2:***

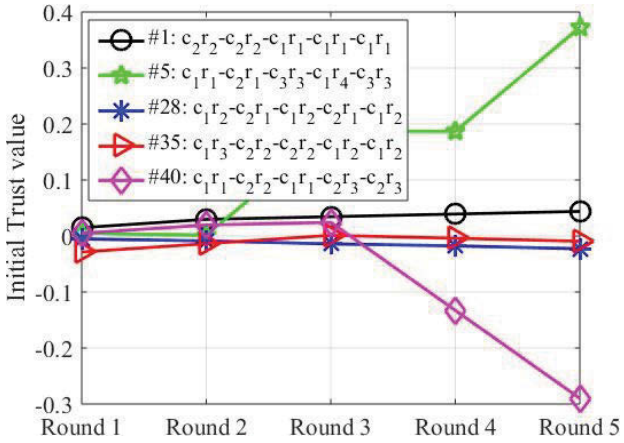


Figure 7.11 Initial trust value aggregated over the five-round C-R process in different simulations using Design 2

Figure 7.11 shows the initial trust value obtained from the challenge-response process in five selected simulations that uses Design 2 as described in **Table 7.1**. Several trends in the updating of the initial trust can be seen from the five-round C-R process in this experiment. Interestingly, in the fifth and 40th simulations, the initial trust values are beyond the thresholds after the C-R process. Particularly, the device with a behavior pattern in the fifth simulation will be admitted to the system for further interactions since its initial trust value reaches the trust threshold of 0.35. On the other hand, the device with a behavior pattern in the 40th simulation will not get more chance to recover its trustworthiness as its initial trust reaches the distrust threshold of -0.3.

In summary, as shown in the experimental results, our proposed challenge-response information design provides feasible information designs of the challenge-response process that produce consistent correlation for the consistent initial trust assessment. The challenges in the challenge-response process are generated based on the probability distribution of the challenge set. The conditional probability of a response given the selected challenge leads the device to behave consistently with the designed probability distributions. Thus, the challenge-response process can reveal the knowledge about the

initial trustworthiness of the device. Our proposed information design of the challenge-response process allows the system to explore the trustworthiness of a device according to the correlation between the challenges and the device's responses.

7.5.3 Discussion

The first concern about the performance of our proposed initial trust establishment model using the information design for its challenge-response process is whether it can cope with common trust attacks such as bad-mouth attack, ballot-stuffing attack, and on-off attack.

The challenge-response information design allows the trust evidence generation module in our proposed initial trust establishment model to capture shared information between the system's challenge and the device's response. The initial trust establishment model relies on this shared information learned through the challenge-response operations to assess the device's initial trust. It is noted that our proposed initial trust establishment does not rely on the recommendations of other devices about the under-tested device to assess the initial trust level of a device. All the information about the trustworthiness of a device is directly created through the challenge-response operations between the system and the device. Therefore, naturally, our proposed initial trust establishment is not affected by popular trust attacks such as the bad-mouth attack [90] or ballot-stuffing attack [92] that tries to disrupt the trust model via fake recommendations.

In the on-off attack [25], the attacker can occasionally alter their malicious behavior patterns so that it is difficult for the trust management model to detect them. One can argue that the on-off attacker can pretend to provide the intended responses to all the challenges. This can disrupt our proposed initial trust establishment model as the trust assessment will inaccurately capture the initial trust of the compromised device and admit it to the system. It is noted that with the proposed information design of the challenge-response process, we ensure that the challenges are randomly selected, and its intended responses are unpredictable. Therefore, it is hard for an on-and-off attacker to always provide intended response to different challenges if it does not fit the challenger's

environment to be aware of the intended responses to the challenges that occur with different probabilities.

The second concern about the performance of our proposed initial trust establishment model is the delay that it might add to the device admission phase in the personal space IoT system. It is worth noting that our initial trust establishment with its challenge-response information design will be conducted within a little time window at the device admission which will add negligible delay to the device admission. Moreover, the operations of the trust evidence generation and the trust computation are computed at the controller device that has powerful computation capacity and will not pose a problem with the delay of processing time. The trust thresholds and the maximum number of challenge-response rounds are also set to prevent the non-stop challenge-response process. The delay cost by our proposed initial trust establishment in the device admission phase of the system will be fully investigated in chapter 8 where our proposed model is incorporated into an existing communication protocol, and its efficiency is evaluated.

7.6 Summary

In this chapter, we presented the information design of the challenge-response process for the proposed initial trust establishment model in personal space IoT. The feasible designs of the challenge-response process are carefully determined by applying guiding principles to ensure that the initial trust establishment consistently works based on the meaningful trust knowledge provided by the challenge-response operations. Specifically, the information content of the challenges and the relationship between the challenges and the responses are designed in the form of probability distributions so that by conducting the challenge-response process the IoT system can achieve meaningful information for consistent initial trust assessment. We defined principles and their entailed conditions to guide the design of the challenge-response process towards feasible solutions which produce consistent correlations. A search algorithm is proposed to explore feasible information designs. Extensive simulations are conducted using the found information designs of the challenge-response process to demonstrate the consistency of our designs and its realistic realization.

Chapter 8

Initial Trust-aware BLE Protocol for Personal Space IoT Systems

8.1 Introduction

In this chapter, to demonstrate the feasibility of our proposed initial trust establishment architecture in a practical setting, we design and implement a new trust-aware communi-cation protocol, the initial trust-aware BLE protocol that incorporates our proposed initial trust establish-ment model into the existing Bluetooth Low Energy (BLE) protocol. The aim is to provide trust-aware features to personal space IoT systems that use BLE as the underlying communication protocol among their devices by introducing challenge-response-based trust establishment model to the existing BLE protocol. The initial trust-aware BLE protocol allows the personal space IoT system to generate trust knowledge about a BLE-enabled device via BLE communications between the controller and the device and quantify the initial trust value of the device before a decision is made on its admission to the system. It is noted that the initial trust-aware BLE protocol utilizes the limited time-window of the device discovery phase and the connection establishment phase of the BLE communication protocol when message exchanges are still in plain text to conduct the challenge-response process for generating trust knowledge. The focus of this chapter is to present the design and implementation of the initial trust-aware BLE protocol and evaluate its performance in personal space IoT

systems. It is also worth noting that our proposed initial trust establishment model can be similarly incorporated into other communication protocols.

The rest of this chapter is organized as follows. Section 8.2 introduces the overview of relevant parts of the BLE protocol that relate to the design and implementation of our initial trust-aware BLE protocol. Section 8.3 provides the realization of our proposed initial trust establishment over personal space IoT systems using BLE protocol for communication. Section 8.4 describes the design of our proposed initial trust-aware BLE protocol. Then, section 8.5 presents the detailed implementation of the initial trust-aware BLE protocol. Section 8.6 gives the experimental evaluation of the initial trust-aware BLE protocol. Section 8.7 discusses the simulation results. Finally, section 8.8 summaries the chapter.

8.2 BLE Protocol Overview

The incorporation of our solution into BLE protocol results in a new initial trust-aware BLE protocol that extends the existing BLE for supporting trust management and enhancing security for BLE communication. As our new initial trust-aware BLE protocol is based on BLE protocol and implements new features of initial trust establishment, in this section, we will briefly summarize portions of the BLE protocol that are relevant to the implementation of the initial trust-aware BLE protocol. Other features and operations of BLE protocol remain unchanged. We then discuss the necessity of initial trust establishment to improve the security feature of the IoT system using BLE communications.

8.2.1 BLE Communication

To provide background on the operations of the initial trust-aware BLE protocol, this section only focuses on the operations of BLE devices and packets exchanged during the device discovery phase (see **Figure 8.1**) and the connection phase (see **Figure 8.2**).

According to the Bluetooth specification version 4.2 [35], a BLE scanner periodically scans advertising channels 37, 38 and 39, to receive advertising information from other devices. The BLE advertiser sends *advertising packets* to the advertising channels to

indicate that it is discoverable or connectable or to broadcast data. Once a scanner receives the advertising packet in an advertising channel, it may send a *scan request packet* to get more information from the discovered advertiser. The advertiser responds to the scanner with a *scan response packet* including the information responding to the scan request packet. The operations of BLE devices during the device discovery phase is illustrated in **Figure 8.1**.

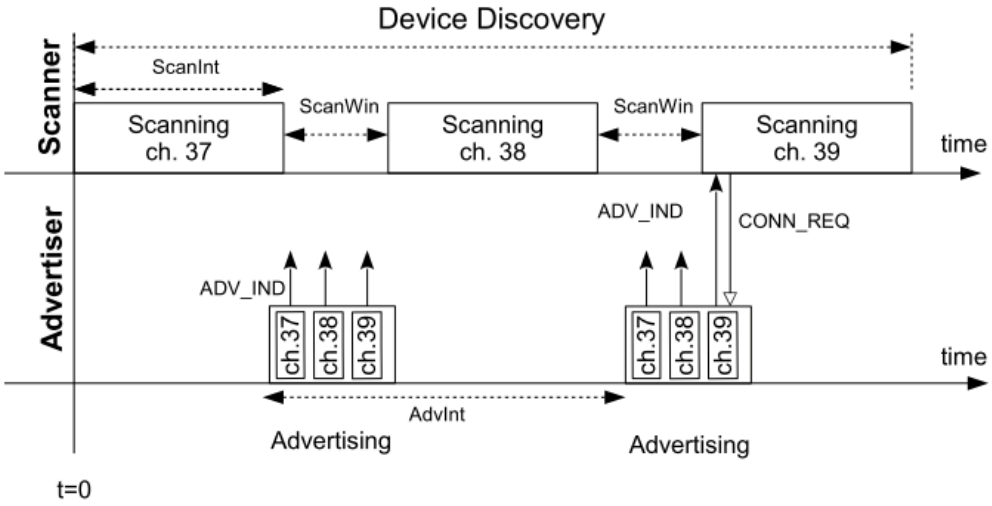


Figure 8.1 BLE device's operation at the device discovery

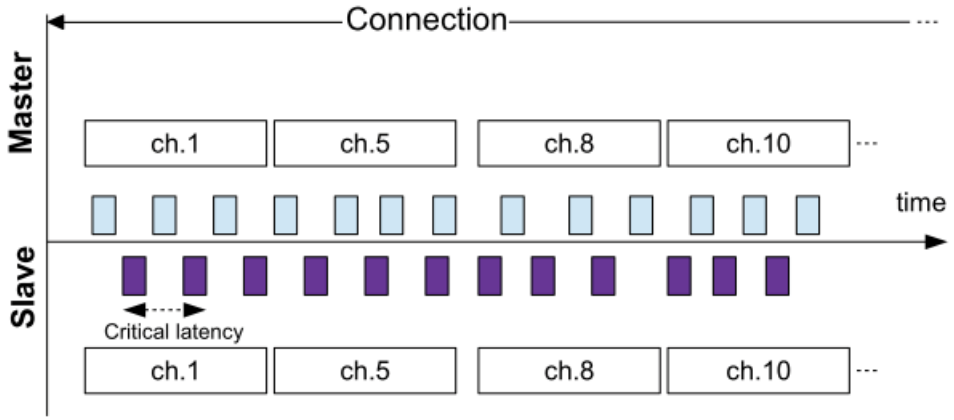


Figure 8.2 BLE device's operation at the connected mode

On receiving an advertising packet successfully, the device transits from a standby state to an initiating state and sends a *connection request packet* to the advertiser to set

the timing of the connection. The initiator becomes the master, and the advertiser becomes the slave of this connection. This connection starts without security consideration.

In the connected mode, BLE devices have to interact with each other regularly to guarantee a *critical latency* and correct synchronization. The critical latency is the maximum communication latency that ensures acceptable operation or user experience. The synchronization depends on the system constraints, mostly on the oscillator accuracy that has a direct impact on clock drift. **Figure 8.2** presents the operation of BLE devices at the connected mode.

In the following, we provide the format of the packet's PDUs in BLE. There are two classes of packet's PDU in BLE: PDUs exchanging on advertising channels called *advertising channel PDUs* and PDUs exchanging on data channels called *data channel PDUs*.

Advertising channel PDUs include three different types: advertising PDUs, scanning PDUs and initiating PDUs.

- Advertising PDUs are used by an advertiser to advertise that it is connectable and undirected to any scanner, is connectable and directed to a specific scanner, is unconnectable and undirected, or is scannable and undirected.
- Scanning PDUs are used by the scanner and the advertiser to exchange additional information when the scanner discovers the advertiser. Scanning PDUs include SCAN_REQ for scan request packet and SCAN_RSP for scan response packet. The SCAN_REQ PDU does not contain any data from the scanner. The SCAN_RSP PDU may contain up to 31 bytes of advertiser's data to provide additional information to the scanner. The size of the current SCAN_REQ PDU is only 12 bytes which is much less than 31 bytes recommended by BLE specification for advertising packets' payload. We will exploit this fact for our initial trust-aware BLE protocol.
- Initiating PDU includes only CONN_REQ PDU for the connection request packet. This payload is sent by the initiator and received by the advertiser once they are synchronized and have exchanged some advertising and scanning packets.

Data channel PDU has a 16-bit header, a variable size payload and may include a Message Integrity Check (MIC) field for security purposes. The payload field is up to 27 bytes in length.

8.2.2 Trust Consideration in Bluetooth and Bluetooth LE

BLE is becoming one of the most common wireless standards used for IoT devices and applications where sensitive information is being collected and transferred such as in a personal space IoT system. Consequently, security and trust consideration in the BLE has raised concerns to IoT product makers and the IoT research community.

As specified in the Core Specification v4.2, each BLE connection starts its lifetime in Security Mode 1, Level 1 (No authentication, no encryption). The initiator sends a connection request packet to the discovered advertiser to set the time and channel mapping for the connection with the advertiser. The two devices hold the connection based on time synchronization and channel hopping.

In BLE, once the two devices are connected, if one of the devices wishes to exchange data securely they must perform a pairing process where they exchange necessary information to establish an encrypted connection. The new security level of the connection is achieved according to the pairing method selected based on the I/O capabilities of each device.

According to the "Guide to Bluetooth Security" of NIST special publication [97], Bluetooth pairing is a process of creating one or more shared secret keys and the storing of these keys to use in subsequent connections to form a trusted device pair. A trust relationship is the consequence of a successful pairing process. In the following, we discuss the implication of trust in Bluetooth (classic) and point out the necessity of support trust quantification/establishment in Bluetooth Low Energy.

Bluetooth Classic allows two different levels of trust: trusted device or untrusted device. According to [71], a trusted device is the device that has been previously authenticated, a link key is stored, and the device is marked as "trusted" in the device database of the initiating device of the pairing process. An untrusted device is the one that has been previously authenticated, a link key is stored, but the device is not marked as

"trusted" in the device database. An unknown device where there is no security information available for this device is also an untrusted device. The trust marking is responsible for marking of a paired device as trusted or not. It can be done by the user, or automatically by the device (e.g., when in bondable mode) after a successful pairing [71]. However, Bluetooth classic specification versions do not provide a means to decide which device is to be marked as trusted after a successful pairing. In other words, no method has been provided in Bluetooth specification to quantify the device's trust level except for the two qualitative labels "trusted" and "untrusted" marked in the database of the initiating device.

According to [97], a trusted device has a fixed relationship with the initiating device and has full access to all services. An untrusted device does not have an established relationship with the initiating device and thus receives restricted access to services. It is noteworthy that the device's trust level used to be considered in Bluetooth classic specification for guarantee of secure access control. In contrast, this feature is not supported in BLE. The successful pairing in BLE confirms that the two devices' identities are verified as they have a shared key. However, the device's behavior is not evaluated during the pairing procedure.

It is possible that an authenticated BLE device might not cooperate with other paired devices, might provide fake information or poor services, or might be compromised. Thus, monitoring the devices' behavior and observing their trustworthiness will help the system to detect devices which know the shared key but are not willing to cooperate with others to provide high-quality service and accurate data. Moreover, estimating the initial trust level on a device and then conducting device authentication would enhance the security of BLE connections, and hence, protect the IoT system from possible attacks. Therefore, it motivates us to incorporate our proposed initial trust establishment model into BLE protocol to provide a means for quantifying the trust level of a device and supporting a stronger device authentication in BLE.

8.3 Realizable Solution of Initial Trust Establishment Model with BLE Protocol

This section demonstrates the feasibility of our proposed initial trust establishment model over the existing BLE communication protocol.

Our initial trust assessment model relies on the trust evidence generated from the challenge-response process where new devices encounter the personal space IoT system for the first time. The challenge-response process exploits possible interactions between a device and the controller during their first encounter. In the following, we analyze the device's interactions during the creation phase of a personal space IoT system where devices are communicating with one another via BLE, to provide a realizable solution for the implementation of our proposed protocol.

Generally, a BLE device discovers other devices presented in its communication radius range during the discovery phase and establishes a connection with them for data exchange. Furthermore, two connected devices will establish an encrypted connection through a pairing process. **Figure 8.3** illustrates typical interactions between a controller and a device via BLE protocol at their first encounter from the device discovery phase to the normal connection and then to the encrypted connection establishment. During the device discovery phase, there are several interactions between the two devices for exchanging their identities and additional information such as the device type, service, and manufacturer information through ADV_IND, SCAN_REQ and SCAN_RSP in advertising channels. In this phase, all packets are exchanged in plain text. Therefore, it is permissible to insert additional pieces of data into these packets to carry information about a challenge or a response.

When the controller retrieves information about the discovered device and wants to make a connection for further data exchanging, it initiates a CONN_REQ packet. The two devices are connected when the other device receives the CONN_REQ packet and switches to the data channel that is indicated in the channel mapping in this packet. At this time, the connection between them is unencrypted. Any data packet exchanging at this period is still in plain text. It is also permissible to implement some challenge-response rounds during this period.

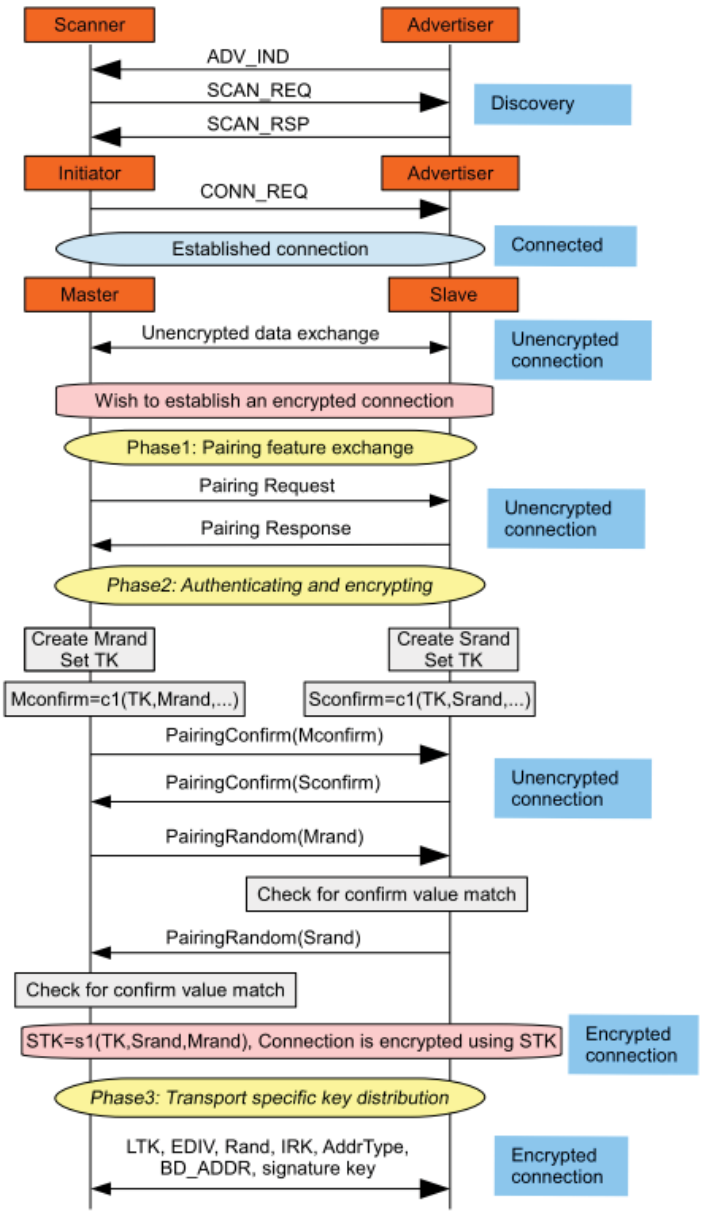


Figure 8.3 BLE device's interactions from the device discovery phase to the secure connection establishment

Once connected, the two devices participate in a pairing process if one device wishes to exchange data securely. During the pairing process, the two devices exchange information of their input/output capabilities, random numbers and confirmation values for the device authentication purpose. In **Figure 8.3**, the "LE secure connection" pairing model is illustrated. Some packets exchanging between two devices during their pairing

process are still in plain text such as the Pairing Request, Pairing Response, Pairing Confirm, and Pairing Random packets.

It is clear that our proposed initial trust establishment requires trust information through an exchange of unencrypted messages, within a limited time window, between devices when they first encounter each other. The challenge is how to design and implement our required challenge and response process within the existing BLE protocol as illustrated in **Figure 8.3**. We consider several alternatives for conducting the challenge-response process by inserting challenge and response information into the packets that carry plain text information exchanging between devices. The first alternative is to exploit scanning packets exchanged in the device discovery phase, and the unencrypted data packets exchanged in the connected mode between two devices to conduct our challenge-response process. The second alternative is utilizing scanning packets exchanged in the device discovery phase and packets that are exchanged in plain text during the pairing process. The third option is to exploit the scanning packets exchanged between two devices and the advertising packets in the device discovery phase for simple information broadcast (beacons) [123, 124] to conduct the challenge-response process.

Among these alternatives, the second option is not efficient as we can only conduct a few challenge-response rounds over a fixed number of pairing packets exchanged in plaintext. Furthermore, the controller must wait until the pairing process to conduct the challenge-response process that might result in an excessive delay in the device admission. In the third alternative, when a device broadcasts beacons to respond to the controller, it might need to broadcast several beacons until the controller successfully receives a response as its advertising and the controller's scanning operation are not always in the same channel. Thus, this option is also inefficient since it significantly increases communication overhead during the device discovery phase and hence drains IoT devices' power. With these considerations, we choose to conduct the challenge-response process within the device discovery phase exploiting the scanning packets exchanging and the connection phase utilizing unencrypted data packets exchanging. The design choice also allows us space to accommodate additional challenge-response rounds

when needed as this requires the exchange of additional scanning packets in the device discovery phase and additional data packets in the connection phase.

In summary, there are several interactions between two BLE devices during their first encounter that can be employed to perform the challenge-response process for generating trust evidence for our proposed initial trust establishment. We describe the proposed initial trust-aware BLE in the next section.

8.4 Initial Trust-aware BLE – Protocol Design

In this section, we introduce a new protocol called *initial trust-aware BLE* protocol which can be considered as an extension of BLE protocol for enhancing trust and security for BLE communication.

- **The overall architecture of initial trust-aware BLE:**

In the initial trust-aware BLE protocol, we implement our initial trust establishment into the operations of BLE devices during the discovery and connection phases. The initial trust establishment is conducted in parallel with the existing typical interactions between BLE devices. A trust calculation module is run at the initiating device to evaluate the initial trust level on a responding device. This initial trust level is then used as a reference for the decision making such as establishing a secure connection via a pairing process or evaluating connections in the future.

Specifically, for the *trust evidence generation module*, we establish the challenge-response process in parallel with the existing interactions during the device discovery phase and the connection establishment phase of BLE devices. The information for the challenge and the response will be carried by typical packets that are exchanged during the device discovery and by unencrypted data packets transferred between the two devices at their unencrypted connection. The interactions during device discovery and unencrypted connection mode allow the IoT system to investigate a device's behavior within a narrow time window.

The *trust knowledge assessment module* and *trust evaluation module* are implemented as computational functions in the computation module of the BLE device. Note that these

computational functions perform simple tasks and, hence, do not affect the BLE communication operations.

As discussed in section 8.2.2, in Bluetooth classic, the trust marking operation is responsible for labeling the trust attribute of a device. However, this feature is not supported in the current BLE protocol. We argue that this trust feature will become essential in future BLE versions as well as other communication protocols when trust is crucial for data trustworthiness and system security. Conducting the trust marking in the initial trust establishment can also help the system to record the trust attribute of other devices and use this information as the prior knowledge about the device when it rejoins the IoT system after some interruptions. In addition, the trust marking also provides information for a device to make a recommendation if requested. For these reasons, we implement a trust marking module in the initial trust-aware BLE protocol. The trust marking module takes the initial trust value aggregated from our initial trust evaluation and the authentication result from the BLE pairing process if available as the inputs. The output of this module is a trust marking for the responding device which is passed to the device's database. As a result, the responding device can be authenticated but not trusted or be authenticated and trusted at some levels as anticipated in the specification of the Bluetooth classic.

- **Operations related to the challenge-response process:**

The initial trust-aware BLE protocol remains the same core of BLE protocol. We only describe the changes that we make to implement our initial trust establishment into BLE protocol. All other operations and transitions that the BLE devices go through will also be implemented in our proposed initial trust-aware BLE protocol.

The operations of the device using the proposed initial trust-aware BLE protocol during the device discovery and connection before pairing process are described in **Figure 8.4**. For convenience, we named the scanning packet PDUs and data packet PDU that carrying our challenge and response information as *SCAN_REQ_wChallenge*, *SCAN_RSP_wResponse*, and *unencrypted_DATA_wChallengeResponse*. The PDU format of these packets is described in **Figure 8.4.**

In our initial trust-aware BLE protocol, the challenge and response for the trust evidence generation module are added to advertising channel packets including the

SCAN_REQ_wChallenge and *SCAN_RSP_wResponse* packets during the device discovery phase. The information for the challenge-response operation is also inserted into data exchanging packets called *unencrypted_DATA_wChallengeResponse* packet during the connection before a secure connection is established by the pairing process.

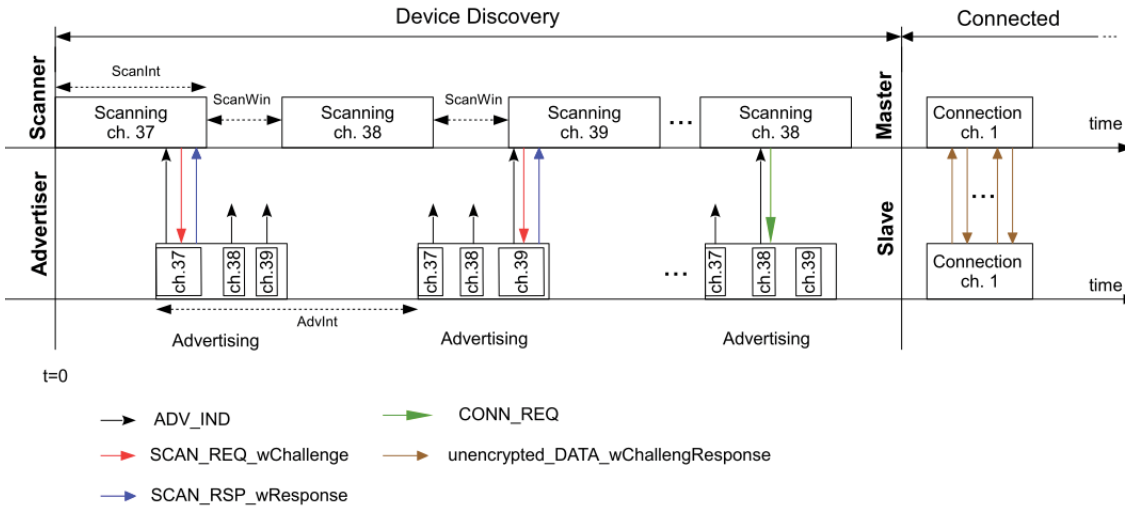


Figure 8.4 Operations of devices in *trust-aware BLE protocol* during the device discovery and the unencrypted connection

As shown in **Figure 8.4**, the initial trust-aware BLE protocol employs more than one pair of scanning packets exchanging for generating trust evidence via challenge-response operation carrying with the scanning packets and at the connected mode with data packets.

- **Packet format:**

As mentioned earlier, the size of the current SCAN_REQ packet is much less than the recommended packets' size exchanged in the advertising channels in the BLE specification. Therefore, it is practical to add another field to the current SCAN_REQ packet for a specific purpose. In our proposed initial trust-aware BLE protocol, we add a *ScnReqData* field into the *SCAN_REQ_wChallenge* payload to carry our challenge information. **Figure 8.5** illustrates the PDU formats of the *SCAN_REQ_wChallenge*, *SCAN_RSP_wResponse* and *unencrypted_DATA_wChallengeResponse* packets in the initial trust-aware BLE protocol. The *SCAN_RSP_wResponse* PDU and the

unencrypted_DATA_wChallengeResponse PDU have the same format with the scan response packet and data packet in the existing BLE protocol. Note that there is no change in the *advertising packet* PDU (ADV_IND) and the *connection request packet* PDU (CONN_REQ).

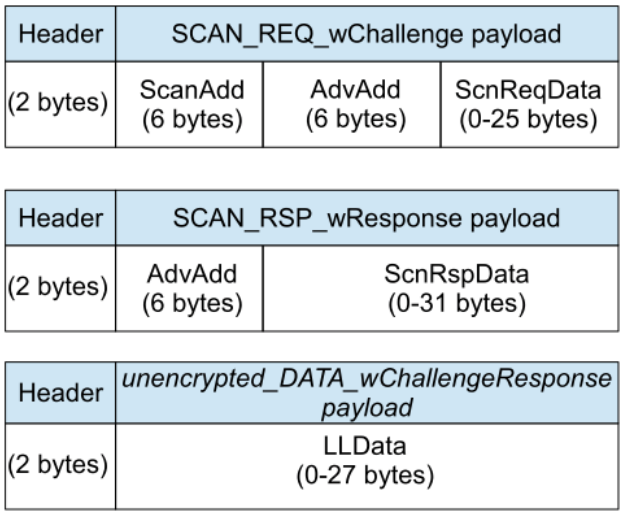


Figure 8.5 Packet PDU formats used for challenge-response operations in the initial trust-aware BLE protocol

In summary, the operations of the proposed initial trust-aware BLE protocol and its packet formats are slightly changed from the original BLE protocol. We highlight features of our proposed initial trust-aware BLE protocol compared to the original BLE protocol version 4.2 as below.

- We employ several scanning packets exchanging during the device discovery phase to serve the challenge-response process.
- We use the *SCAN_REQ_wChallenge* packet which is an extended version of the original SCAN_REQ packet where the *ScnReqData* field is added to carry challenge information.
- Once initial trust-aware BLE devices are at the connected mode, we utilize unencrypted data packets exchanging during this connection period for the challenge-response operations by adding challenge and response information to their payload.

8.5 Implementing the Initial Trust-aware BLE protocol

This section presents the implementation of our proposed initial trust-aware BLE protocol.

8.5.1 Implementation Details

This section presents the detail of our proposed initial trust-aware BLE protocol. The overview of functions implemented in a device with initial trust-aware BLE protocol is graphically illustrated in **Figure 8.6**. We then provide the UML class diagram of the implementation of our initial trust-aware BLE protocol. Finally, the pseudo code of primary computational functions implemented in the initial trust-aware BLE protocol is listed.

- **Functions implemented in the initial trust-aware BLE device**

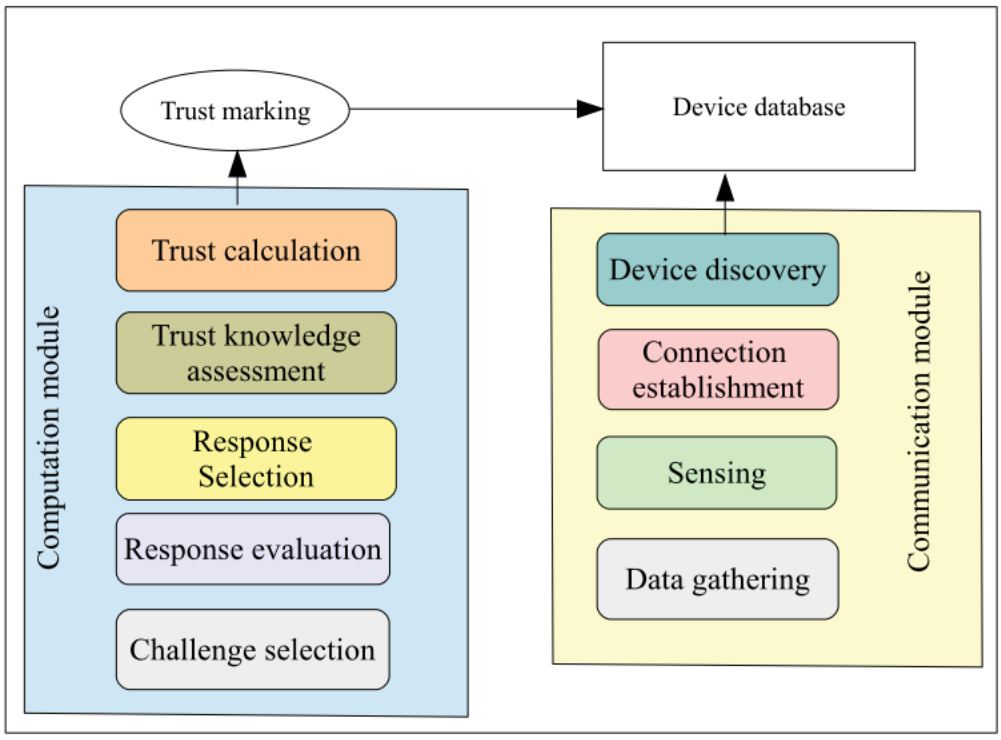


Figure 8.6 Overview of functions implemented in a device with initial trust-aware BLE protocol

In the initial trust-aware BLE protocol, device discovery, connection establishment and other device's capabilities such as sensing, data gathering are implemented in the

communication module. In addition, a computation module is implemented for challenge selection, response selection, response evaluation, trust knowledge assessment and trust calculation function. When the device acts as a controller for the personal space IoT system, the computation module activates challenge selection, response evaluation, trust knowledge assessment, trust calculation functions. When the device acts as a normal device that intends to join a personal space IoT system, the computation module runs the response selection function only. For both device roles, the communication module executes device discovery, connection establishment, sensing, and data gathering functions. The trust marking module is used for indicating the initial trust level of a discovered device and a label of a trust or distrust attribute. The device database stores the device address of discovered devices and their corresponding initial trust level.

- **Operations in one challenge-response round during device discovery**

The controller first discovers the nearby devices. During the device discovery phase, on receiving an advertising packet (ADV_IND), it runs the challenge selection function to generate challenge information. It then initiates a *SCAN_REQ_wChallenge* packet including the challenge information and sends this packet to the discovered device in the same channel at which it received the advertising packet.

The discovered device (advertiser) receives the *SCAN_REQ_wChallenge* packet and generates the *SCAN_RSP_wResponse* packet including the response information. The response information is generated through the response selection function in the computation module. The advertiser then sends the *SCAN_RSP_wResponse* packet to the same channel expecting that the controller receives it.

A challenge-response round is completed when the controller and the advertiser exchange successfully a pair of *SCAN_REQ_wChallenge* and *SCAN_RSP_wResponse* packets. The controller then executes the response evaluation function to evaluate the response from the advertiser. This information is then transferred to the trust knowledge assessment and trust evaluation mechanisms in the computation module to estimate a trust level.

- **Operations in one challenge-response round during the connected mode**

When the two devices are connected, they can start exchanging unencrypted data packets. They listen to a channel that they agreed on according to the channel scheduled

in the connection request packet. First, the controller (now becomes the master of this connection) sends a data packet with challenge information after executing the challenge selection function. When the advertiser (now becomes the slave) receives this data packet from the master, it returns a data packet including the response to the challenge, which is generated by the response selection function, to the master. The master evaluates the received data packet from the slave to generate trust evidence and conduct the trust knowledge assessment and trust evaluation functions.

At the end of the challenge-response process, the trust evaluation mechanism in the computation module of the controller returns an initial trust level that it learned from all interactions with the discovered device. This information is then transferred to the trust marking module for further process. The output from the trust marking module will be stored in the device database of the controller.

- **UML class diagram of the implementation of the initial trust-aware BLE protocol**

Figure 8.7 shows the major classes of the initial trust-aware BLE protocol. All computational functions for initial trust establishment are implemented in the BLE MAC class. For example, the generation of the *SCAN_REQ_wChallenge* and the *SCAN_RSP_wResponse* packets are implemented as *generateScanRequest()* and *generateScan_Rsp()* operations in the BLE MAC class. The trust calculation function is implemented in the *updateStatusAdvertising()* and *updateStatusConnected()* operations in the BLE MAC class. It is noted that each class only displays the main operations and attributes. Many other attributes and operations are implemented in the class. The details of BLE MAC class (BLE MacV2), the BLE Advertising packet class (BLE_Adv_MacPkt), and the BLE Data packet class (BLE_Data_MacPkt) class are illustrated in **Figure 8.8**, **Figure 8.9** and **Figure 8.10**.

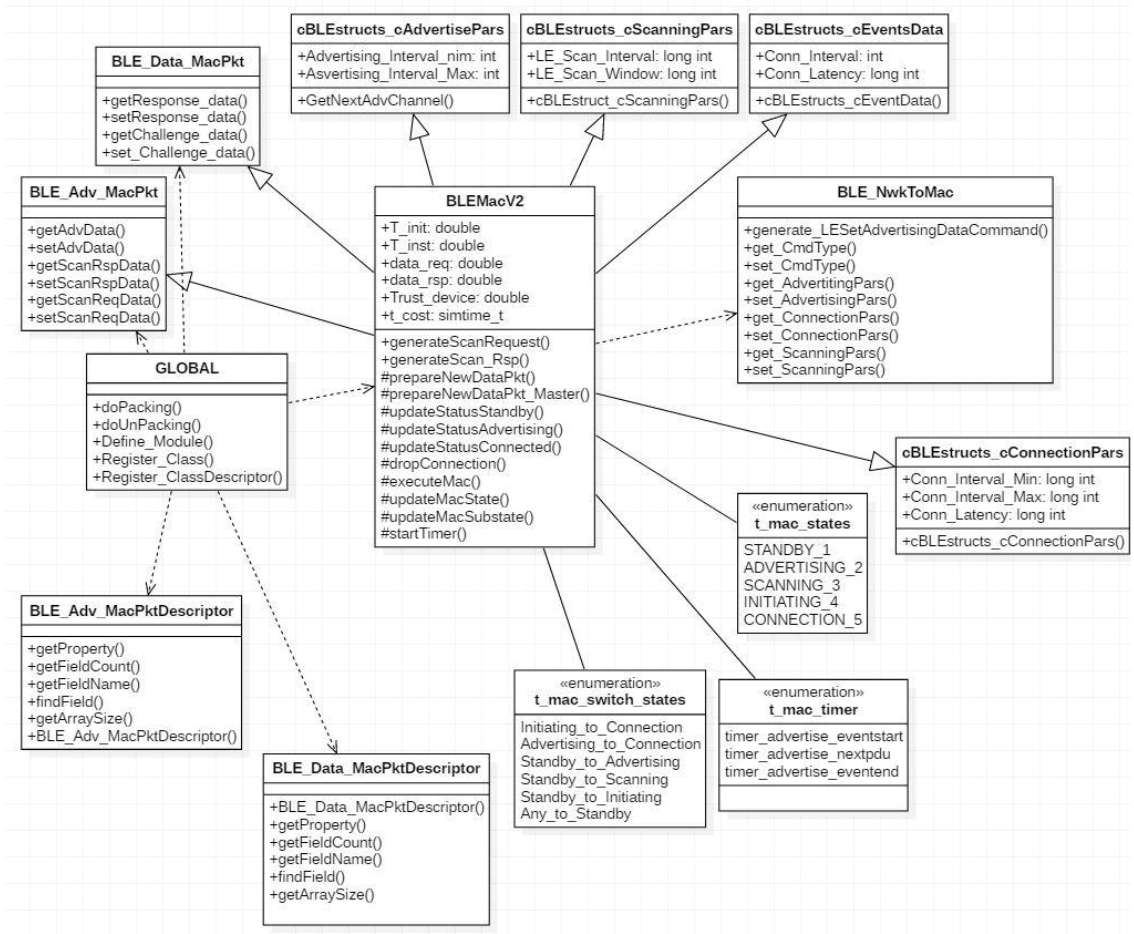


Figure 8.7 The UML of major classes of the initial trust-aware BLE protocol

The BLE MAC class that shows the attributes and operations of the main initial trust-aware BLE communication protocol as shown in **Figure 8.8**.

Figure 8.8 The BLE MAC class

The BLE ADV packet class and its interaction with the main BLE communication protocol are shown in **Figure 8.9**.

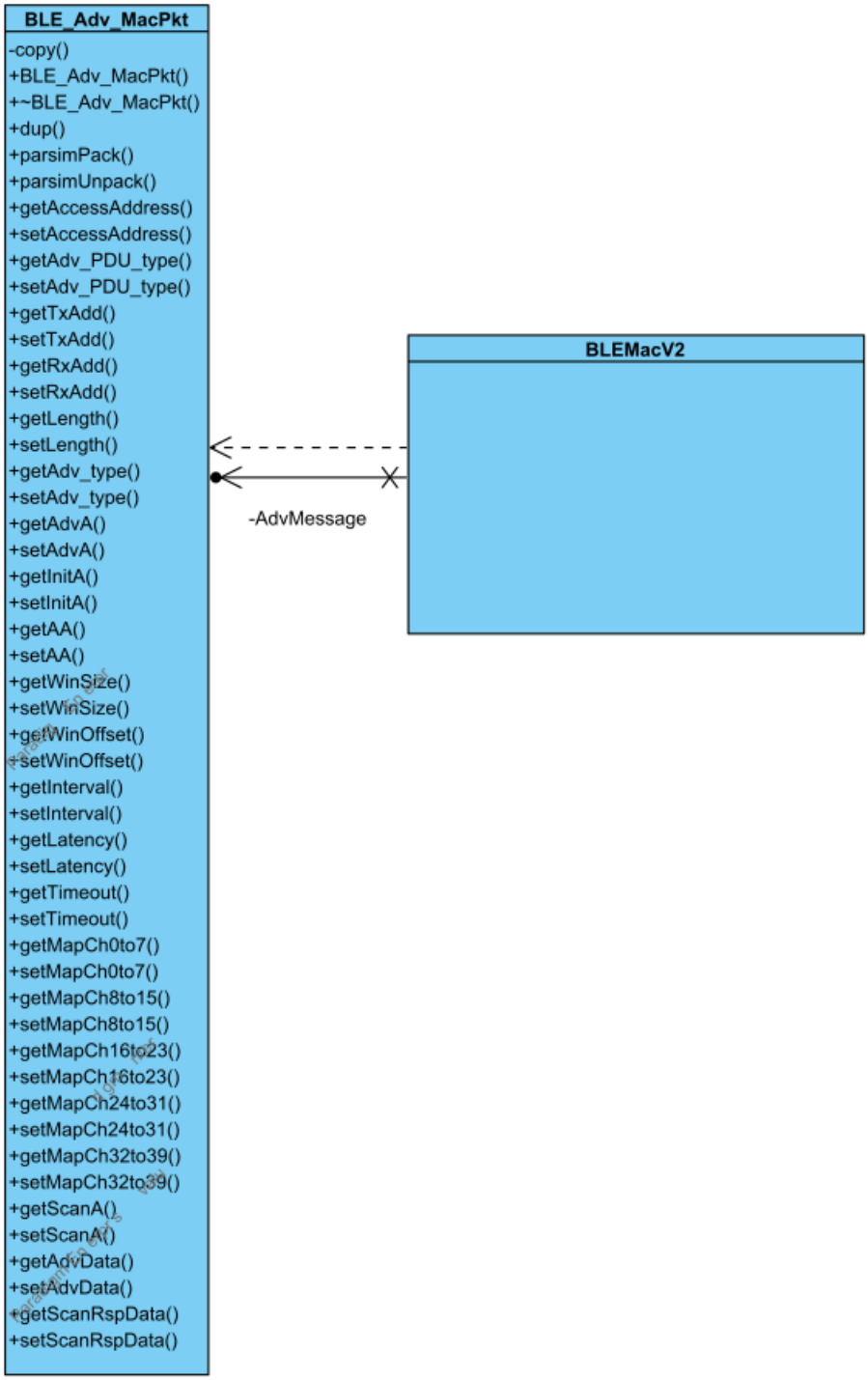


Figure 8.9 The BLE Advertising Packet class diagram

The BLE Data packet class diagram and its relationship with the BLE MAC communication protocol are shown in **Figure 8.10**.

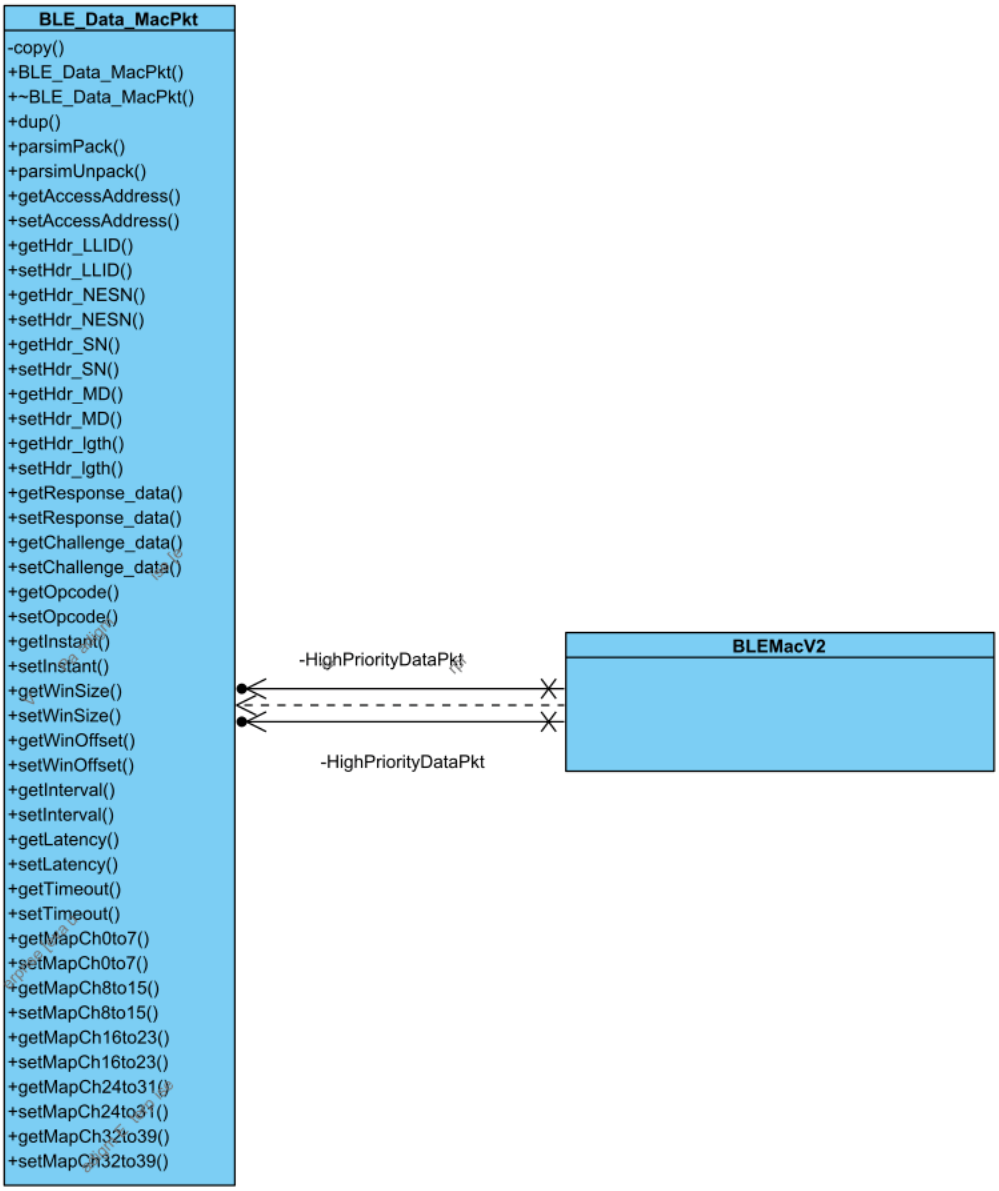


Figure 8.10 The BLE Data Packet class diagram

- **Pseudocode of the implementation**

In the following, we provide the pseudo code of each function that we implemented in our proposed initial trust-aware BLE protocol. We focus on providing our implementation of functions in the computation model. Functions in the communication module remain the same as in the original BLE protocol.

The pseudo code of the initial trust establishment implementation in BLE protocol is described as in **Algorithm 8.1**.

Algorithm 8.1 Initial trust establishment procedure

Inputs:

Information design of the challenge-response (C-R) process: $[p(c_i)], \forall i = 1 \ldots n$, and $[p(r_j|c_i)], \forall i = 1 \ldots n, \forall j = 1 \ldots m, (n, m > 1)$

$CR_{discover}$: number of C-R rounds in discovery phase

CR_{conn}: number of C-R rounds in unencrypted connection

$r_{discover} = 0$; $r_{conn} = 0$;

Outputs: Initial trust level on the new device

1: **in device discovery phase:**
2: **is the controller?**
3: event: receiving a packet
4: **switch** received packet **do**
5: **case** *Advertising packet*
6: challenge = generate *Scan_Request* packet;
7: send *Scan_Request* packet;
8: **case** *Scan_Response packet*
9: **if** $r_{discover} < CR_{discover}$ **then**
10: obtain the response;
11: execute *trust_knowledge_assessment*();
12: execute *execute trust_calculation*();
13: $r_{discover}++$;
14: generate & send *Scan_Request* packet;
15: **else**
16: execute *trust_knowledge_assessment*();
17: execute *trust_calculation*();
18: generate *Connection_Request* packet;
19: send *Connection_Request* packet;
20: **end if**

```
21: is a device?
22: send Advertising packet;
23: event: receiving a packet
24: switch received packet do
25:     case Scan_Response packet
26:         obtain the challenge;
27:         generate & send Scan_Response packet;
28:     case Connection_Request packet;
29:         obtain connection setting parameters;
30:         switch to the predefined channel;
31: in unencrypted connection:
32: is a master?
33: generate & send unencrypted packet with challenge;
34: event: receiving a data packet;
35: if r_conn < CR_conn then
36:     obtain the response;
37:     execute trust_knowledge_assessment();
38:     execute trust_calculation();
39:     r_conn + +;
40:     generate & send unencrypted packet with challenge;
41: else
42:     execute trust_knowledge_assessment();
43:     execute trust_calculation();
44: end if
45: is a slave?
46: event: receiving a data packet;
47: obtain the challenge from received data packet;
48: generate & send unencrypted data pkt with response;
```

The pseudocode for trust knowledge assessment and trust calculation functions at the controller are described in **Algorithm 8.2**. The trust knowledge assessment includes the response evaluation function.

Algorithm 8.2 *trust_knowledge_assessment()* and *trust_calculation()*

Inputs:

Information design of the C-R process: $[p(c_i)], \forall i = 1 \ldots n$,

and $[p(r_j|c_i)], \forall i = 1 \ldots n, \forall j = 1 \ldots m, (n, m > 1)$;

challenge from $SCAN\_REQ\_wChallenge$ packet: c_i;

$SCAN\_RSP\_wResponse$ packet;

current round index: k; weight value ω_k

Outputs:

Trust knowledge = correlation between a challenge and received response; Instant trust at current round;

Updated initial trust up to current round;

1: obtain response r_j from $SCAN\_RSP\_wResponse$;
2: map response information r_j to c_i;
3: derive $p(r_j|c_i)$ from r_j and c_i;
4: compute $p(c_i|r_j)$;
5: $correlation$: $\Delta_{ij} = p(c_i|r_j) - p(c_i)$;
6: update k;
7: $instant\ trust\ \tau_k = \mathbf{f}(\Delta_{ij})$;
8: retrieve initial trust value from previous rounds;
9: $initial\ trust = T^{(k)} = (1 - \omega_k)T^{(k-1)} + \omega_k \tau_k$;
10: **return** : k, τ_k, T^k

Packet generation modules are implemented as follows.

- **Advertising packet:** see **Appendix 1**.
- **Scanning packets:**

Pseudo code for the scan request packet generation function is illustrated in **Algorithm 8.3**.

Algorithm 8.3 Generating *SCAN_REQ_wChallenge* packet

Inputs:

challenge set: $C = c_1, c_2, \ldots, c_n$;

probability distribution: $P(C) = [p(c_i)]^n, \forall i = 1 \ldots n$;

AdvAdd: device's address; ScanAdd: controller's address;

Outputs: *SCAN_REQ_wChallenge* packet;

1: select challenge: c_i = **myRand**$(C, P(C), n)$;
2: encapsulate $SCAN\_REQ\_wChallenge = Header + ScanAddr + AdvAdd + c_i$;
3: record sent challenge: c_i;
4: **return** : *SCAN_REQ_wChallenge*

The pseudo code for the scan response packet generation function is described in **Algorithm 8.4**.

Algorithm 8.4 Generating *SCAN_RSP_wResponse* packet

Inputs:

response set: $R = r_1, r_2, \ldots, r_m$; probability distribution: $P(R|C) = [p(r_j|c_i)], \forall (i = 1 \ldots n, j = 1 \ldots m)$; *SCAN_REQ_wChallenge*; AdvAdd: device's address;

Outputs: *SCAN_RSP_wResponse*;

1: obtain challenge from *SCAN_REQ_wChallenge*: c_i;
2: select a response (r_j): r_j = **myRand**$(R, P(R|C), m, c_i)$;
3: encapsulate $SCAN\_RSP\_wResponse = Header + AdvAdd + r_j$;
4: **return** : *SCAN_RSP_wResponse*

- **Initiating packet (connection request packet):** see **Appendix 2.**
- **Unencrypted data packet:**

Pseudocode for the data packet for the controller (master), including the challenge section function is presented in **Algorithm 8.5**.

Algorithm 8.5 Data packet generation at the Master

Inputs:

Header: data type (control or data PDU), NESN (next expected sequence number), SN (sequence number), MD (more data), Length of payload;

Data to send: M_{data};

Challenge probability distribution: $P(C) = [p(c_i)]^n, \forall i = 1 \ldots n$;

Outputs: $Master\_unencrypted\_data\_packet$

1: achieve header information;
2: select challenge: c_i = **myRand**$(C, P(C), n)$;
3: encapsulate encapsulate data PDU = $Header + M_{data} + c_i$;
4: record sent challenge: c_i;
5: **return** : $Master\_unencrypted\_data\_packet$;

Pseudo code for the data packet for slave device, including the response selection is presented in **Algorithm 8.6**.

Algorithm 8.6 Data packet generation at the Slaver

Inputs:

Header: data type (control or data PDU), NESN (next expected sequence number), SN (sequence number), MD (more data), Length of payload;

Data to send: S_{data};

Challenge from received $Master\_unencrypted\_data\_packet$;

probability distribution: $P(R|C) = [p(r_j|c_i)], \forall (i = 1 \ldots n, j = 1 \ldots m)$;

Outputs: $Slave\_unencrypted\_data\_packet$

1: achieve header information;
2: obtain challenge from the received $Master\_unencrypted\_data\_packet$: c_i;
3: select a response (say r_j) from the response set corresponding to its probability and the corresponding challenge c_i;
4: r_j = **myRand**$(R, P(R|C), m, c_i)$;
5: encapsulate encapsulate data PDU = $Header + S_{data} + r_j$;
6: **return** : $Slave\_unencrypted\_data\_packet$;

8.5.2 Simulation Tool

Our implementation is based on an open source BLE simulation tool developed by Mikhaylov [125]. This tool uses the MiXiM framework (v2.2.1) [126] based on the popular OMNet++ engine (v.4.2.2) [127] to implement the BLE communication protocol. OMNet++ is a C++ based discrete event simulator for modeling communication networks, multiprocessors and other distributed or parallel systems. Instead of directly providing simulation components for each network, it provides the basic machinery and tools to create such simulations. MiXiM is a very powerful extension to simulate wireless and mobile networks using the discrete event simulator OMNeT++. It provides detailed models of radio wave propagation, interference estimation, radio transceiver power consumption and wireless MAC protocols.

In the BLE simulation tool in [125], the Link Layer (LL) model was implemented as a state machine with five states (i.e., Standby, Advertising, Scanning, Initiating and Connection) as described in the BLE specification v4.2. All the parameters of the BLE communication such as advertising and connection intervals, supervision timeout, frequency hop increment, the lists of data and advertisement channels are defined in the simulation initialization file.

It is noted that in the BLE simulation by Mikhaylov, the available simulated operations of BLE devices includes advertising in one or multiple advertising channels, scanning for the advertising packets, establishing a connection, connection upkeep and terminating. Specifically, only the directed advertising packet (ADV_DIRECT_IND), connection request packet (CONN_REQ) and data packet are implemented.

To implement our initial trust-aware BLE protocol, we employ the indirect advertising packet (ADV_IND) for a new device to broadcast its advertisement and the scanning packets including *SCAN_REQ_wChallenge* and *SCAN_RSP_wResponse* packets for carrying the challenge and response information. We also implement the unencrypted data packet generation (for master and slave) to insert the challenge and response information. The functions in the computation module such as trust knowledge assessment, trust calculation, challenge and response selection based on their probability

distributions, response evaluation are implemented in our proposed initial trust-aware BLE protocol.

8.6 Experimental Evaluation

This section provides the experimental setup and the performance evaluation of our proposed initial trust-aware BLE protocol. We show the simulation results on various evaluation parameters from the trust level updating over the experiment to the processing time and overhead cost of the proposed initial trust-aware BLE protocol and explain the implication of the obtained results.

8.6.1 Simulation Setup

For the experimental evaluation, we simulated a network consisting of two BLE nodes placed in an area of (10m x 10m) where one node is acting as the controller of the personal space IoT system and the other node is playing the role of a new device which wishes to join the personal space IoT system. The parameters of the BLE communication are defined in the simulation initialization file (*.ini* file) and remain constant during the simulation. The summary of the main parameters is described in **Table 8.1**.

Table 8.1 Parameters of initial trust-aware BLE communication

Parameter	Value
Advertising interval	25ms
Scanning interval	25ms
Scanning window	25ms
Connection interval	5ms
Supervision timeout	6.25ms
Interframe space (IFS)	0.15ms

Particularly, the controller node starts in an advertising channel to scan for advertising packets within a scanning interval of 25ms. The device node (advertiser) starts in an advertising channel and broadcasts ADV_IND packets within an advertising interval of 25ms. The data exchanging between the controller and the advertiser is conducted with a

connection interval of 5ms. During the experiment, two nodes use all three advertising channels and all 37 data channels. The Interframe Space period (IFS) is set at 0.15ms. As the challenge and response information expresses a probability value, the maximum length of *scanReqData* and *scanRspData* field in the scanning packets' payload is set at 8 bytes.

Table 8.2 Information design used for the experiment

P(C)	P(R|C) (j = 1…4)
$p(c_1) = 0.6$	$p(r_j\|c_1) = 0.51; 0.34; 0.02; 0.13$
$p(c_2) = 0.3$	$p(r_j\|c_2) = 0.50; 0.36; 0.01; 0.13$
$p(c_3) = 0.1$	$p(r_j\|c_3) = 0.50; 0.31; 0.06; 0.13$

The inputs for the challenge-response process are the probability distribution of the challenge space and the conditional probability distribution referring to the relationship between the challenges and the responses. The detail of the information design that we use in this experiment is presented in **Table 8.2**. The actual challenges and responses chosen during the challenge-response process are selected by executing the challenge selection and response selection functions that are provided by the computation module at the controller and the devices.

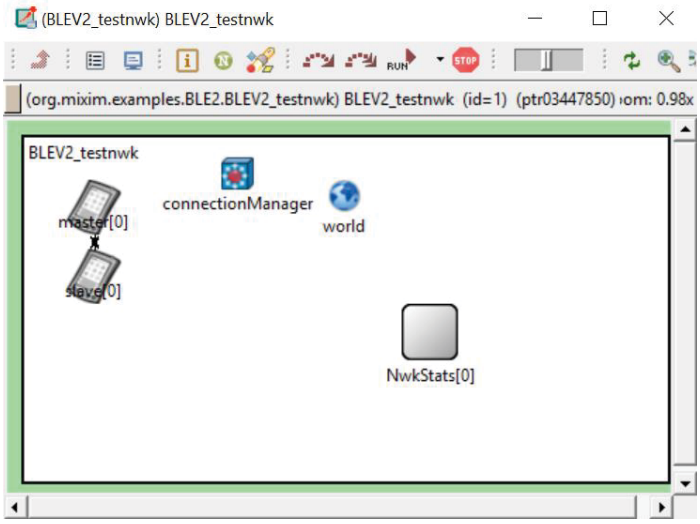


Figure 8.11 Network topology in the experiments

The screenshot of the network topology displayed by *Tkenv* user interface in OMNeT++ is shown in **Figure 8.11**. The user interface of the operations that happened during the experiments are presented in **Appendix 3**, **Appendix 4**, **Appendix 5** and **Appendix 6**.

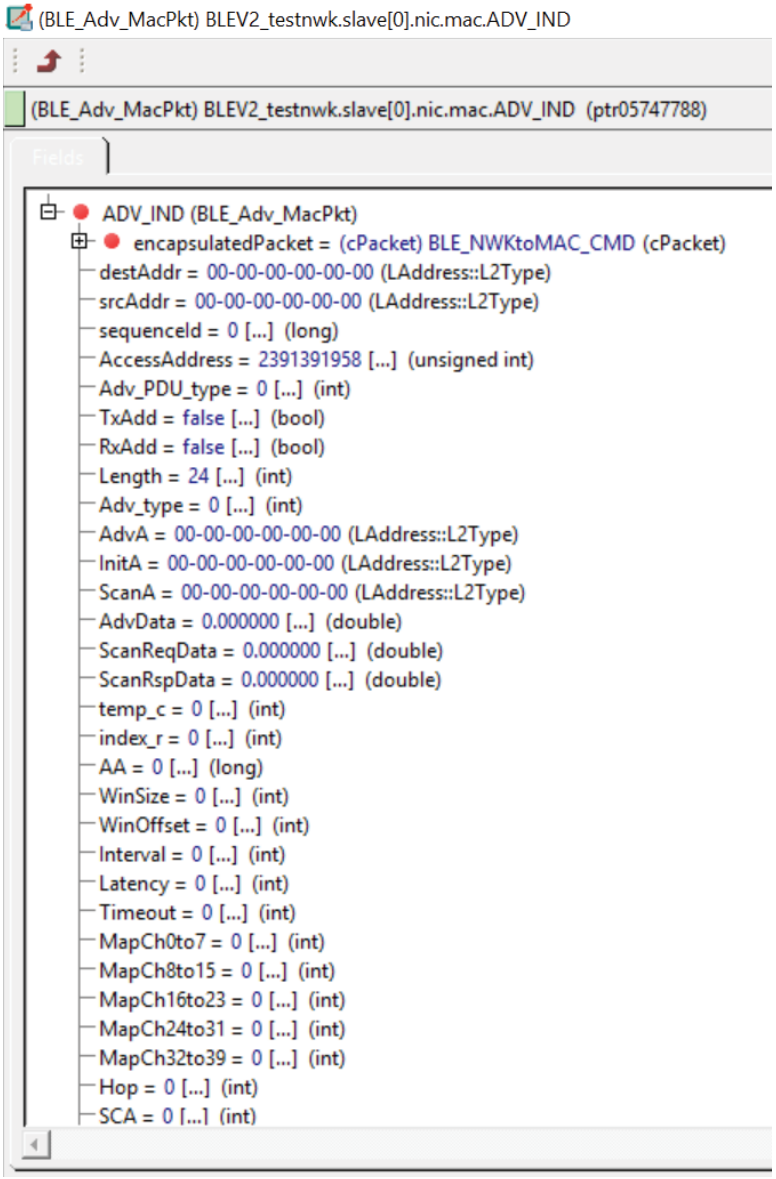


Figure 8.12 The advertisement packet sent by the advertiser node

8.6.2 Simulation Results

In this section, we first demonstrate the working of the proposed initial trust-aware BLE protocol with an emphasis on the challenge-response-based trust evidence generation module and then the working of the overall initial trust establishment model. Finally, we evaluate the efficiency performance of the trust-aware BLE in terms of communication overhead and protocol processing time.

- **Challenge-Response-based trust evidence generation module - Packets exchanged:**

We conduct an experiment that includes one round of challenge-response at the device discovery phase and one round of challenge-response at the connected mode between the controller node and a device node. The information design of the challenge-response process is shown in **Table 8.2**. The challenge and response information inserted in the related packet is shown in the *ScanReqData* and *ScanRspData* field in the corresponding packet. For example, the *SCAN_REQ_wChallenge* packet includes the challenge information in the *ScanReqData* field.

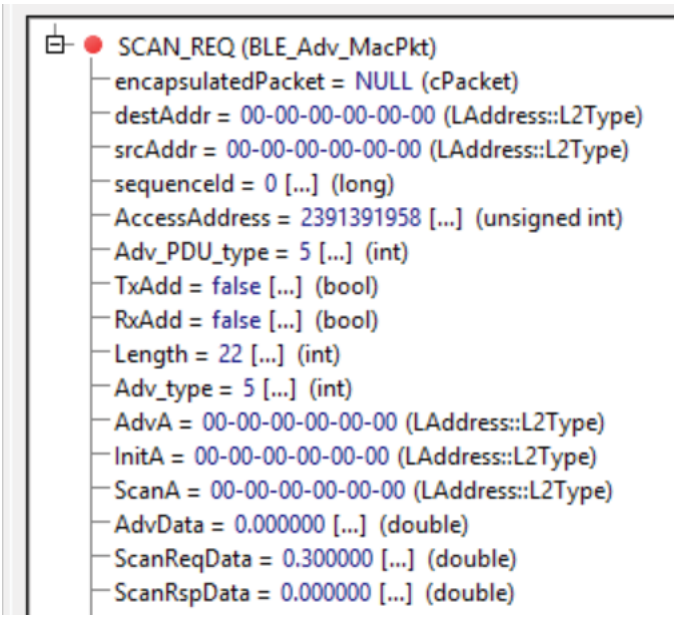


Figure 8.13 The scan request packet with a challenge sent by the controller node

Advertiser broadcasts an advertisement packet which has ADV_IND PDU. The inspection of the advertising packet in the simulation is given in **Figure 8.12**. The ADV_IND packet includes the access address displayed as 2391391958 (decimal value of 0x8E89BED6), ADV_PDU type indicating the indirect advertisement packet; no advertisement data is included.

Once the controller receives the ADV_IND packet, it sends a SCAN_REQ packet to the advertiser with a challenge in the *ScanReqData* field of the packet. **Figure 8.13** presents the inspection of this packet. This SCAN_REQ packet carries the challenge information of a probability of 0.3 in the *ScanReqData* field. Packet's length is 22 bytes. The scanner's address is included in the packet.

When the advertiser receives a scan request packet, it checks the AdvA and ScanA fields to see if the packet is for itself and where the packet is. The advertiser also looks for a challenge in the *ScanReqData* field. It then generates a scan response packet with its response to the challenge and sends the scan response with a response to the controller. The inspection of the scan response packet sent by the advertiser is shown in **Figure 8.14**. This SCAN_RSP packet carried a response of a probability value of 0.36 in the *ScanReqData* field.

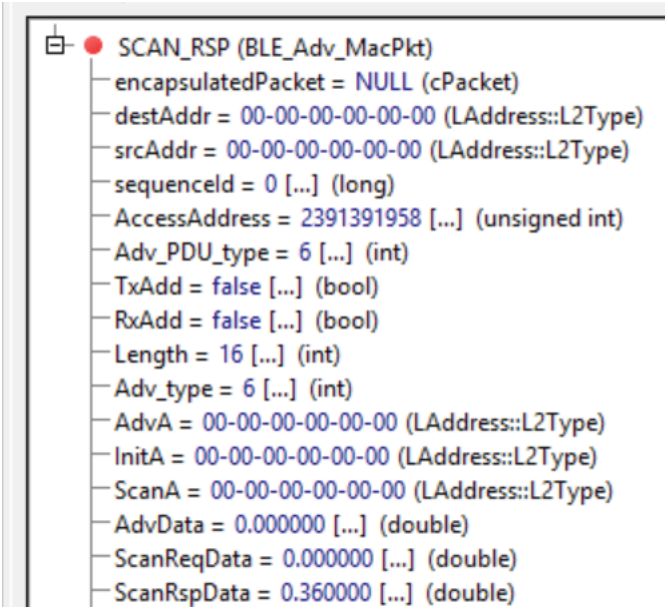


Figure 8.14 The scan response packet with a response sent by the advertiser node

The exchanging of scanning packets to perform some challenge-response rounds is repeated until the controller initiates a connection request packet and sends it to the advertiser node. The connection request packet sent in the simulation includes the channel access address for data exchanging at the connected mode (2337329927 – the decimal value of 0x8B50D307), a window size of 1, connection interval of 8*0.0625ms, and channel mapping indicating the data channel used for the connection, hop, latency. Inspection of this packet is provided in **Appendix 7**.

After being connected, the two nodes can exchange unencrypted data packets for some applications without security requirement. The initial trust-aware BLE protocol employs some exchanging rounds to generate the initial trust evidence. The data packet sent by the controller to challenge the advertiser includes a challenge in the packet payload. The inspection of an unencrypted data packet sent by the controller (now acting as master) is given in **Figure 8.15.** This packet carried a challenge of a probability value of 0.6 in the *challenge_data* field. The access address that is set in the connection request packet is used for this data packet.

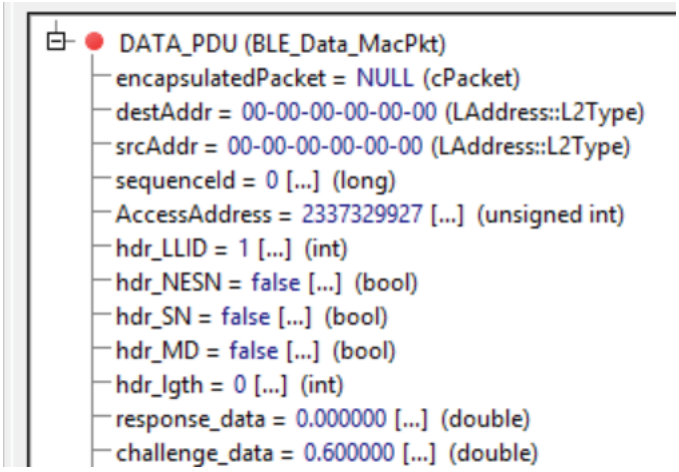


Figure 8.15 The data packet with the request information sent by the controller node (master)

When the advertiser (now acting as the slave) receives a data packet from the master, it looks for the challenge in the packet payload and generates a data packet with a response to return to the master. The inspection of a data packet with response data is provided in

Figure 8.16. This data packet carried a response of a probability value of 0.51 in the *response_data* field.

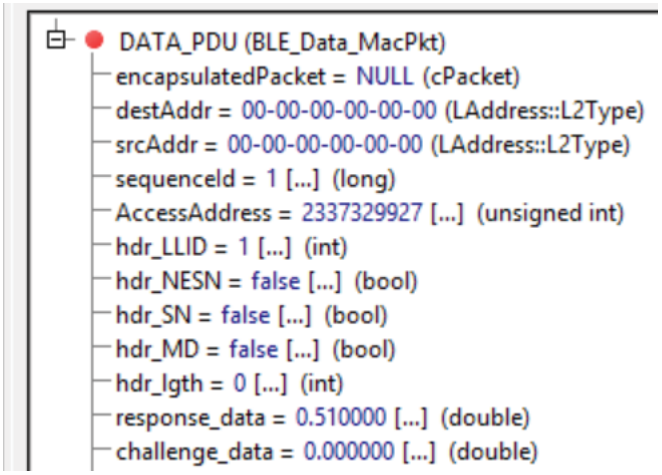


Figure 8.16 The data packet with a response sent by the advertiser node (slave)

- **Evaluation 1: Investigation of the overall initial trust establishment procedure**

The challenge-response rounds conducted during the device discovery phase and the unencrypted connection period are set at 3 and 2, respectively. This section shows the instant trust calculation from each challenge-response round and the aggregated initial trust value over five challenge-response rounds.

Four simulation instances are investigated where the controller generates different challenge sets, and the device node provides different response patterns. In the first instance, the challenges selected for the initial trust establishment were C_1, C_1, C_2, C_2, and C_1 according to the challenge distribution of 0.6, 0.3 and 0.1. The responses that the BLE node returns to the selected challenges are R_2, R_2, R_2, R_1, and R_1 respectively, according to the design described in **Table 8.2**.

Figure 8.17 shows the instant trust and updated initial trust over five challenge-response rounds based on the challenges sent by the controller and the response set returned by the device node. In the first two rounds, as the device node returned an unintended response to the controller, it is given a distrust value (negative value) after each round. In the third round, the device node returned an intended response to the

challenge, (response R_2 to challenge C_2), it is given a positive instant trust value after this round. Next, in the fourth and fifth round, when the device node provided an unintended response and an intended response to challenges, it is given a negative instant trust value after the fourth round and a positive instant trust value after the fifth round. The initial trust value is aggregated from instant trust values over the simulation. Finally, the controller node places an initial trust value of 0.0048 to the device node in this simulation.

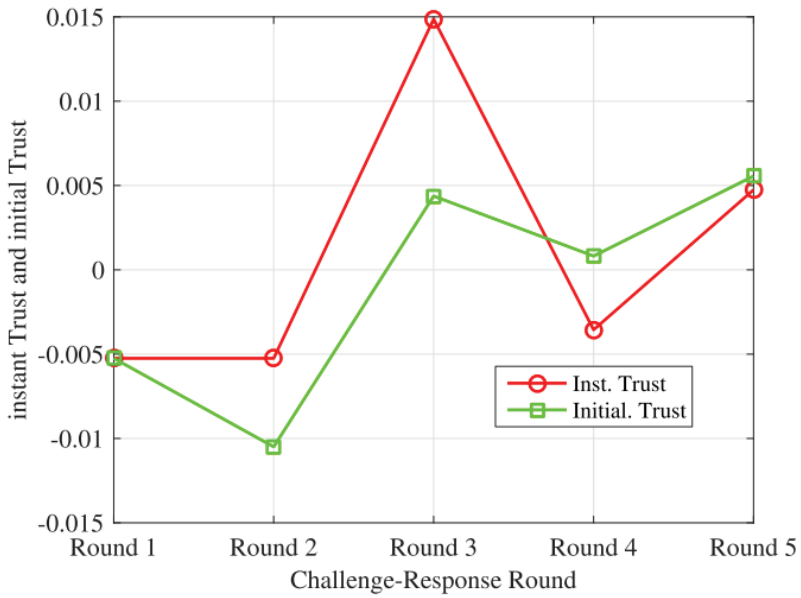


Figure 8.17 The instant trust value and aggregated initial trust value from the first simulation instance

In the second instance, the challenges selected for the initial trust establishment were C_3, C_1, C_1, C_3, and C_3 and the responses that the device node returns to the selected challenges are R_4, R_1, R_1, R_1, and R_3 respectively. **Figure 8.18** provides the investigated instant trust value and aggregated initial trust value from this simulation. In the first round, the device node provided an unintended response to challenge C_3, which is considered as a very rare challenge. Thus, it is given a negative instant trust value for its unintended response. In the next two rounds, as the device node provided two intended responses to the challenges C_1, the device places positive instant trust values to the device after these challenge-response round. In the last round, the device node provided an intended response to the highest unpredictable challenge C_3. Thus, the device node is given a high instant trust level in the last round. This instant trust value significantly

contributes to the initial trust aggregation. Consequently, with this response pattern the controller node establishes an initial trust value of 0.13 on the device node in this simulation.

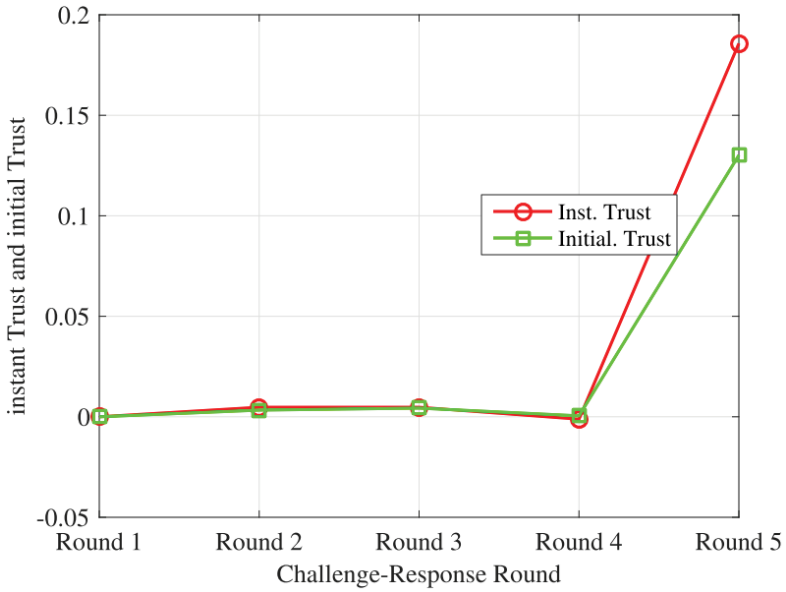


Figure 8.18 The instant trust value and aggregated initial trust value from the second simulation instance

In the third instance, the challenges selected for the initial trust establishment were C_1, C_1, C_1, C_3, and C_2 according and the device node returns responses R_1, R_1, R_2, R_1, and R_3 to the selected challenges, respectively. **Figure 8.19** illustrates the instant trust value and the initial trust aggregated that the controller node establishes on the device over the simulation. In the first two rounds, the selected challenges are C_1 which is less unpredictable compared to other challenges and the device node provided intended responses to both challenges. Thus, the device node is given positive instant trust values after each round. However, as the device node provided the unintended responses to the last three rounds, it is given negative instant trust value after each round. As the challenges in the last two rounds are more unpredictable, the corresponding instant trust values that the device node is given during these rounds contribute more in the initial trust aggregation. Therefore, the controller node places a negative initial trust value of -0.11 to the device node in this simulation.

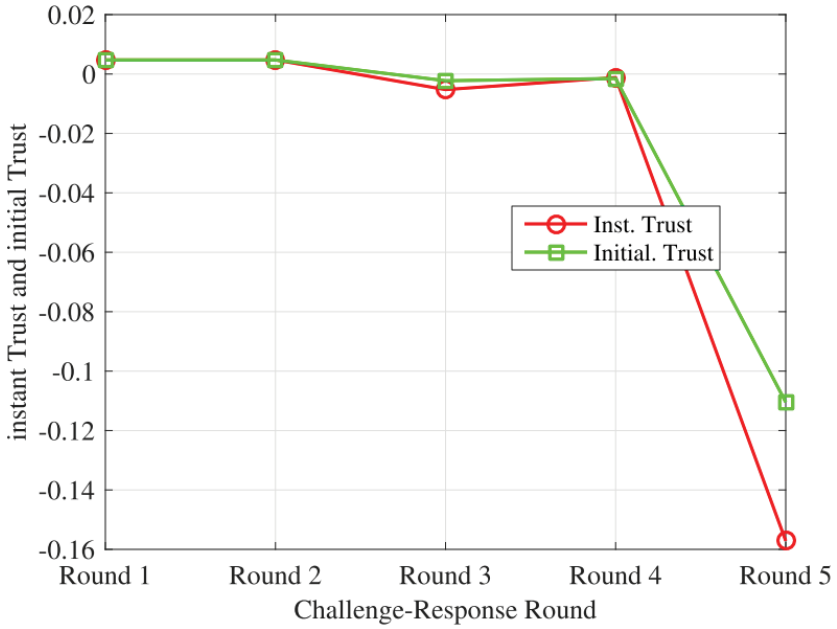


Figure 8.19 The instant trust value and aggregated initial trust value from the third simulation instance

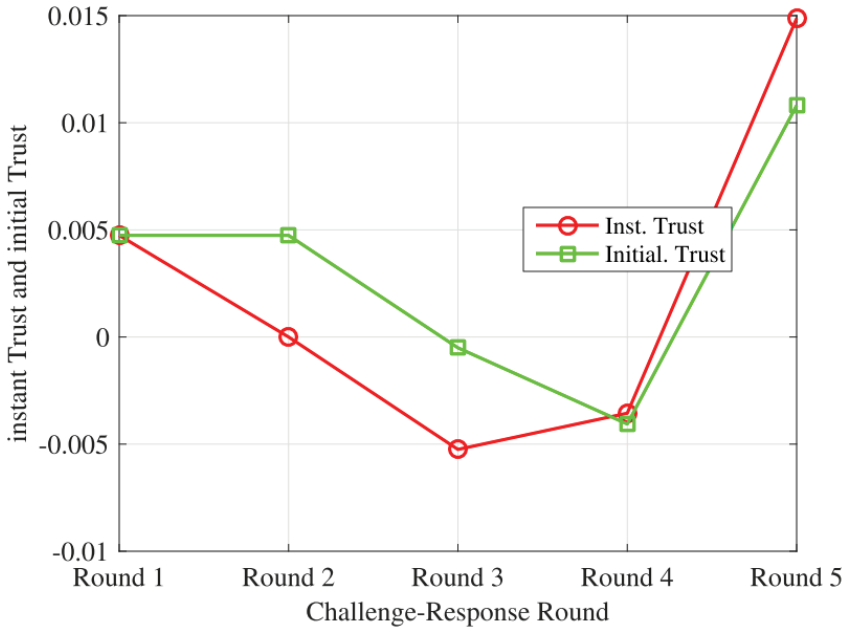


Figure 8.20 The instant trust value and aggregated initial trust value from the fourth simulation instance

In the last instance, the challenges selected for the initial trust establishment were C_1, C_1, C_1, C_2 and C_2 and the responses that the device node returns to the selected challenges are R_1, R_4, R_2, R_1, and R_2, respectively. **Figure 8.20** illustrates the instant trust value and the initial trust aggregated that are investigated over this simulation. In the first round,

the selected challenge is C_1, and the device node provided an intended response to this challenge. Thus, the controller places a positive instant trust value to the device after the first round. However, the device node provided unintended responses to challenges in the next three rounds. Therefore, the initial trust value is decreased to a distrust value of -0.0045. In the last round, as the device node provided an intended response to the challenge C_2, it recovers its initial trust from a negative value to a positive value. The reason for this recovering is because the device node provided an intended response to challenge C_2 which is considered as a rare challenge and the information that is learned from an intended response to the rare challenge (C_2) is more meaningful than others.

Using the scanning packets and unencrypted data packets to carry the information for the challenge-response process in the proposed initial trust establishment model is successfully incorporated into the existing BLE protocol. With these interactions, the controller of an IoT system can learn the device's behavior at their first encounter and determine the initial trust level of the device before deciding whether to admit the device to the system.

- **Evaluation 2: Efficiency of the initial trust-aware BLE protocol**

To investigate the efficiency of our proposed initial trust-aware BLE protocol, we perform five different experiments with different numbers of challenge-response rounds. Note that, the number of challenge-response rounds during the device discovery phase is set to 1, 2, 3, 4 and 5, respectively in five experiments (Exp. 2, …, Exp. 6). The number of challenge-response rounds during the unencrypted connection period in all experiments is set to 2 rounds. We investigate the processing time and overhead cost of the initial trust-aware BLE protocol.

We simulate the normal device discovery and connection establishment of a network of two devices using the existing BLE protocol (Exp. 1). We determine the processing time for the BLE device node to be discovered and to be connected and to exchange two data packets with the controller node. We also investigate the number of ADV_IND packets that the advertiser had to send until it is discovered by the controller.

The tables below show the comparison between the efficiency of a network, regarding the processing time and the communication overhead, using existing BLE protocol and using our proposed initial trust-aware BLE protocol.

- **Processing time**

We first investigate the processing time for the advertiser node to be discovered by the controller, be involved in the scanning packet exchanging to perform the challenge-response process until the controller initiates a connection request. This is called the processing time in device discovery. We also determine the processing time for the two devices to exchange some data packets after they entered the connected mode before the pairing establishment. This period is called processing time in connected mode. Then, we calculate the total processing time that each experiment takes for the challenge-response process so that an initial trust value is determined and stored in the controller's database.

Table 8.3 Processing time in different experiments

Processing Time (s)	Exp1: Existing BLE	Exp2: 3 Rounds	Exp3: 4 Rounds	Exp4: 5 Rounds	Exp5: 6 Rounds	Exp6: 7 Rounds
In Device Discovery(s)	0.0437	0.0536	0.090	0.1005	0.138	0.191
In Connected Mode (s)	0.022	0.022	0.022	0.022	0.022	0.022
Total (s)	0.0657	0.0756	0.112	0.1225	0.160	0.213

The processing time values calculated from these experiments are shown in **Table 8.3**. The processing time that the two devices using existing BLE protocol took in the device discovery phase is 0.0437s. Meanwhile, the processing time value that the two devices using initial trust-aware BLE protocol took to conduct one challenge-response round during the device discovery is only 0.01s longer than the normal device discovery. When the number of challenge-response rounds required in the device discovery phase is increased to 2 or 3 rounds, there is a little more time cost for conducting two rounds (0.046s longer) or 3 rounds (0.056s longer) of exchanging scanning packets. When the

number of challenge-response rounds increases to 4 or 5 rounds in the device discovery phase, the processing time is increased more quickly, i.e., 0.094s and 0.147s longer, respectively. The reason is that the two devices keep switching to different advertising channels according to the advertising interval and scanning interval for more scanning packets exchanging. As a result, the controller must listen to the next ADV_IND packet sent by the advertiser to initiate the next round of scanning packet exchanging. The more scanning packets are exchanging, the more process time costs for the controller to synchronize its radio to the same channel with the advertiser. However, the processing time in the device discovery phase is reasonable (less than 0.2s) even when seven challenge-response rounds are required.

We can see that when two devices are in the connected mode, the processing time for performing two rounds of data packet exchanging are the same for devices using our initial trust-aware BLE protocol and devices using existing BLE protocol. As a result, the total processing time is raised more quickly when more challenge-response rounds are conducted during the device discovery phase.

- **Communication Overhead**

In experiment 1, to establish a connection between two devices using existing BLE communication, the advertiser node had to send two ADV_IND packets to the advertising channel until it is discovered by the controller. It can be seen from the **Table 8.4** that the two devices using the initial trust-aware BLE protocol had to exchange more packets during the device discovery phase when the required number of challenge-response rounds is increased. **Table 8.4** presents investigated communication overhead in six experiments.

Table 8.4 Overhead in different experiments

Number of Packets	Exp1	Exp2	Exp3	Exp4	Exp5	Exp6
ADV_IND	2	3	7	8	12	17
SCAN_REQ_wChallenge	0	1	2	3	4	5
SCAN_RSP_wResponse	0	1	2	3	4	5
Unencrypted_DATA	4	4	4	4	4	4

It can be seen from the **Table 8.4** that the two devices using initial trust-aware BLE protocol had to exchange more packets during the device discovery phase when the required number of challenge-response rounds is increased. The number of *SCAN_REQ_wChallenge* packets and the number of *SCAN_RSP_wResponse* packets is equal to the number of required challenge-response rounds in the device discovery phase. The number of ADV_IND packets that the advertiser node had to send is increased when more challenge-response rounds are required in the device discovery phase. For example, in experiment 2, three challenge-response rounds are required for the initial trust establishment where one round was performed during the device discovery and two rounds were performed during the connected mode. The advertiser had to send the three ADV_IND packets until the controller receives an advertisement packet from the device node and starts exchanging scanning packets. The reason is that the advertiser sent the first two ADV_IND packets in channels that are different from the one that the controller is scanning. In experiment 6, seven challenge-response rounds are required for the initial trust establishment which includes five rounds performed in the device discovery phase and two rounds in the connection phase. The advertiser had to send 17 ADV_IND packets in the device discovery phase.

In summary, by introducing the challenge-response operations within the device discovery phase and the unencrypted connection phase of the existing BLE, our initial trust-aware BLE is feasible and practical. The delay added by the initial trust establishment to the device admission phase is only 0.03s to 0.11s longer than the existing device admission phase without the challenge-response procedure, where 3 to 6 challenge-response rounds are conducted respectively, that is acceptable for BLE protocol. Also, when more challenge-response rounds are needed for the trust evidence generation, one can employ unencrypted data packets exchanging in the connection phase for carrying the challenge-response operations to minimize the total processing time.

8.7 Discussion

The implementation of our initial trust-aware BLE protocol and its performance evaluation demonstrate the feasibility of the proposed initial trust establishment model

over an existing communication protocol. The initial trust-aware BLE protocol requires modifications in the format of scanning packets to insert the challenge and response information to establish initial trust level of new devices. The size of the new scanning packet's PDU for carrying the challenge and response information is tiny (22 and 16 bytes). The number of challenge-response rounds required for performing trust evidence generation does not significantly affect the device discovery phase of the initial trust-aware trust BLE protocol. The total processing time for the devices establishing a connection and conducting several rounds of challenge-response operation is not significantly higher than that with the existing BLE protocol.

In addition, the operations of computational functions such as challenge selection, response evaluation, trust knowledge assessment and trust calculation are implemented at the controller, a less power-constrained device, and hence they have minimum effect on power-constrained, non-controller IoT devices in the environment. Consequently, the initial trust-aware BLE protocol is feasible and practicable as an extension of the BLE protocol where the introduced features can be realistically implemented in a next version of the BLE protocol.

It is envisaged that the initial trust establishment model in the initial trust-aware BLE protocol can be deployed in several scenarios. A possible implementation is to conduct the initial trust establishment and the device authentication together. With this deployment, a device is judged based on both its initial trust value and its authentication results, resulting in a higher security level for the BLE communication since the connection is encrypted for data exchanged between authenticated and trusted devices only. Another deployment is for the controller to use the results of the initial trust establishment process to decide if the discovered device should be authenticated. This means the controller may not initiate the pairing process with a device that is marked "untrusted."

The initial trust establishment in the initial trust-aware BLE protocol can also be used throughout the lifecycle of a device. It can be used to investigate the initial trust of a new device when joining an IoT system. It can also be employed to reevaluate the trust level of already admitted entities by conducting a challenge-response process when needed during their tenure in the IoT system. The trust evidence from the challenge-response

process can also be combined with other trust evidence such as recommendations or historical knowledge about the devices to provide a more robust trust assessment on current devices within the system and its data and services worthiness.

8.8 Summary

In this chapter, we presented the design and practical implementation of our proposed initial trust establishment. We presented the implementation of the initial trust-aware BLE protocol and analyzed its performance evaluation to demonstrate its feasibility and efficiency. The implementation showed that the proposed initial trust establishment model could be well incorporated into the existing BLE protocol. The performance evaluation demonstrated the feasibility and efficiency of the initial trust-aware BLE protocol. The proposed initial trust-aware BLE protocol can be considered as a realistic extension of the existing BLE protocol for providing both trust and security of personal space IoT systems.

Chapter 9
Conclusion and Future Work

In this chapter, we first summarize the research and outline the main contributions of the thesis. We then suggest directions for future research.

9.1 Summary and contributions of the thesis

Internet of Things is becoming a reality that brings a lot of creative applications to all aspects of our modern life such as smart appliances, smart healthcare, wearables, smart cars, smart buildings. However, it also opens the door to many challenges in the security and trustworthy of IoT systems and applications. Despite the benefits derived from the Internet of Things (IoT) systems, users are concerned about the trustworthiness of their collected data and offered services. Security control approaches do not provide a mechanism to monitor devices' behavior and detect misbehaved and untrustworthy devices that provide fake data, poor services, or uncooperative. As a result, security controls might secure an IoT system, but its devices and their provided data and applications might not be trusted completely. Therefore, to guarantee the trusted data and reliable services provided by an IoT system and hence mitigate user's concerns when using IoT applications in the personal environment, the IoT system must verify the initial trust of the devices before admitting them to the system. It then must continuously monitor the trustworthiness of every admitted device throughout its lifecycle until it ceases working in the system.

Clearly, research on trust in the IoT becomes more crucial than ever to help IoT solution providers to design and build secure and trustworthy IoT systems and broader usage of IoT solutions. In fact, a full cycle of trust management for IoT has not been

comprehensively investigated. In particular, current trust management models proposed and studied trust evaluation schemes for updating trustworthiness of entities during the operational phase of a system. Initial trust establishment models have not yet investigated in current research efforts. Moreover, establishing an initial trust between two devices at their first encounter has been a challenge when little knowledge is available for the trust assessment. Consequently, it is crucial to investigate the initial trust establishment in IoT comprehensively to provide effective solutions that allow the IoT systems to admit trustworthy components and hence guarantee the trustworthiness of their provided data and services as well as improve the reliability of IoT solutions.

This thesis aims to create a secure and trustworthy IoT system in a personal space environment by seeking a new initial trust establishment architecture that allows the system to quantify and assess the initial trust level of devices before admitting or readmitting them into the system. The new initial trust establishment architecture includes a new scheme to generate trust knowledge for the initial trust assessment, new trust evaluation models that suit different generated trust knowledge and is feasible to be integrated into a trust-aware communication protocol.

As the research achievement, we first proposed an initial trust establishment architecture for personal space IoT systems. Based on the overall architecture, we designed and investigated three initial trust assessment models that allow the IoT systems to assess the initial trust of devices before they are admitted to the system without requiring historical observations or recommendations. We proposed a challenge-response information design that determines the feasible information designs needed for the challenge-response process to capture meaningful information about the devices' trustworthiness for the trust assessment. We designed and implemented a new initial trust-aware BLE protocol which incorporates the proposed initial trust establishment architecture into the existing BLE protocol. The performance evaluation of the new initial trust-aware BLE protocol demonstrates the feasibility and efficiency of our research outcomes in practice.

The novelty of this work lies in creating a reliable IoT system in a personal space environment where the trustworthiness of its components, collected data and provided services are guaranteed by an effective initial trust management model. By using our

proposed challenge-response-based initial trust establishment architecture and the information design of the challenge-response operations, the IoT system can assess and quantify the initial trust level of devices before admitting or readmitting them into the system within a short time window and without prior trust knowledge.

The research contributions of this thesis can be summarized as follows.

- We proposed a novel initial trust establishment architecture that allows the IoT systems to assess and trustworthiness of devices before admitting or readmitting them to the IoT systems. The proposed initial trust establishment procedure allows the IoT systems to admit trustworthy devices and reduce the risk of attacks deployed by misbehaved and compromised devices. The proposed initial trust establishment architecture provides an additional scheme for the current trust management models to reevaluate the trustworthiness of admitted members over their operations when historical interactions and recommendations become less reliable or are no longer valid.
- We introduced three new initial trust establishment models based on the proposed architecture to ensure the scalability of the proposed initial trust establishment architecture. These proposed models adequately quantify the device's trustworthiness at the device admission phase of the IoT systems and take into account different settings that affect the obtained trust evidence.
- We proposed a challenge-response information design which provides an information space from the challenger's view over its environment to invite relevant responses. The information design of the challenge-response process ensures that there exists shared information between the potential device and the system for the system to rely on to judge the devices' initial trust.
- We realized the proposed initial trust establishment models and evaluated their performance through extensive simulations. The simulation results demonstrate the feasibility and consistency of the proposed initial trust establishment models.
- We designed and implemented a new initial trust-aware BLE protocol by incorporating our proposed initial trust establishment model and its feasible challenge-response information design into the existing BLE protocol. The trust-aware feature in the new initial trust-aware BLE protocol can enhance the security

and trust controls in the existing Bluetooth protocol and expand its usage in IoT systems.

The initial trust establishment model plays a crucial role in building a secure and trustworthy IoT system. It allows the IoT system to verify devices which wish to join the system and ensure the trustworthiness of admitted devices in the IoT system. However, it is challenging in assessing the trust of devices at their first encounter with the system due to the lack of prior experience or recommendations. Moreover, very few research efforts have focused on this challenge. This thesis is the first attempt in proposing initial trust establishment in IoT and provides timely solutions to develop trustworthy IoT systems. The research outcomes from this thesis provide innovative schemes that allow the IoT system to generate meaningful trust knowledge within a limited time window and quantify the initial trust level of every device before admitting or readmitting it into the system. These research outcomes also help the IoT business solution providers to build secure and trustworthy IoT systems and to mitigate the users' concerns on the trustworthiness of the data and the services provided by IoT systems.

9.2 Future Work

It is crucial to build a secure and trustworthy IoT system that can provide trustworthy data and services to the users. By using our proposed initial trust establishment models, the IoT systems can judge the devices' behavior and quantify their trustworthiness before admitting them into the systems without requiring prior experience or recommendations. The system will be built with trustworthy components and hence provide trusted data and reliable services. Future research can be conducted in the following aspects.

The proposed trust assessment schemes can be used during the operational phase of the IoT systems to regularly reassess the trustworthiness of its components and to readmit components after an interrupting event that causes a loss of the communication/control between the controller and these components. In these situations, additional conditions may apply. In the future, we will investigate the performance of the proposed trust assessment schemes over the mentioned situations. We will also combine the proposed initial trust establishment architecture with existing trust management models to provide

a comprehensive and robust trust management model to enhance the security and trustworthiness of IoT systems.

The challenge-response process aims to accurately capture the trust knowledge about the responders through their responses to the challenges. Optimum information design that satisfies the challenge-response process's aim requires the knowledge of the ultimate aim of the process and the environment in which it seeks to apply. Therefore, we will investigate the information space of the challenge-response process to determine the optimum information design that allows the system to capture the relevant and accurate trust knowledge about the device through the challenge-response operations.

Mapping is required to map the information design to the parameters of the final intended purposes and target environment where physical factors such as population, the device's type, and the general knowledge of the population affect the operations of a challenge-response process. For future work, we intend to propose a mapping scheme to produce a specific challenge set and response set for an initial trust establishment in a specific personal space IoT environment.

The current work experimentally evaluated the performance of proposed initial trust establishment models based on simulated IoT devices. For future work, we will investigate their performance in real IoT environments by implementing them into real IoT devices.

The current initial trust-aware BLE protocol utilized the interactions between devices during the device discovery phase and the unencrypted connection establishment phase for conducting challenge-response operations in the trust assessment procedure. Various directions to the adoption of the next generation BLEs that includes the trust assessment can be investigated.

Appendices

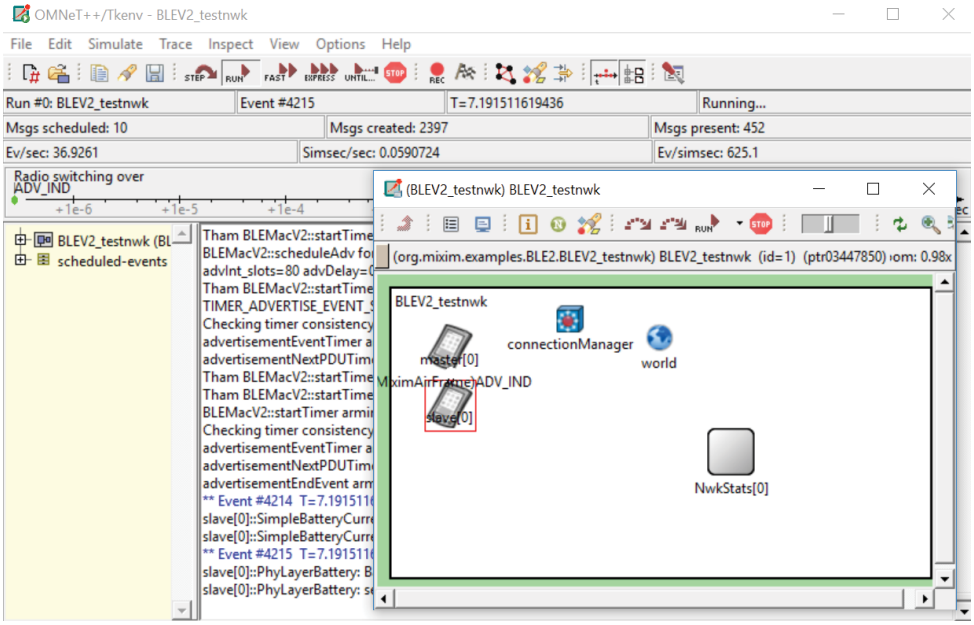
Appendix 1 Pseudocode for advertising packet generation

```
Inputs:

   - AdvAdd: Advertiser's Address
   - AdvData: data if the advertiser wants to broadcast

Outputs: Indirect advertising packet (ADV_IND PDU)

1: encapsulate advertising packet = AdvAdd + AdvData
```

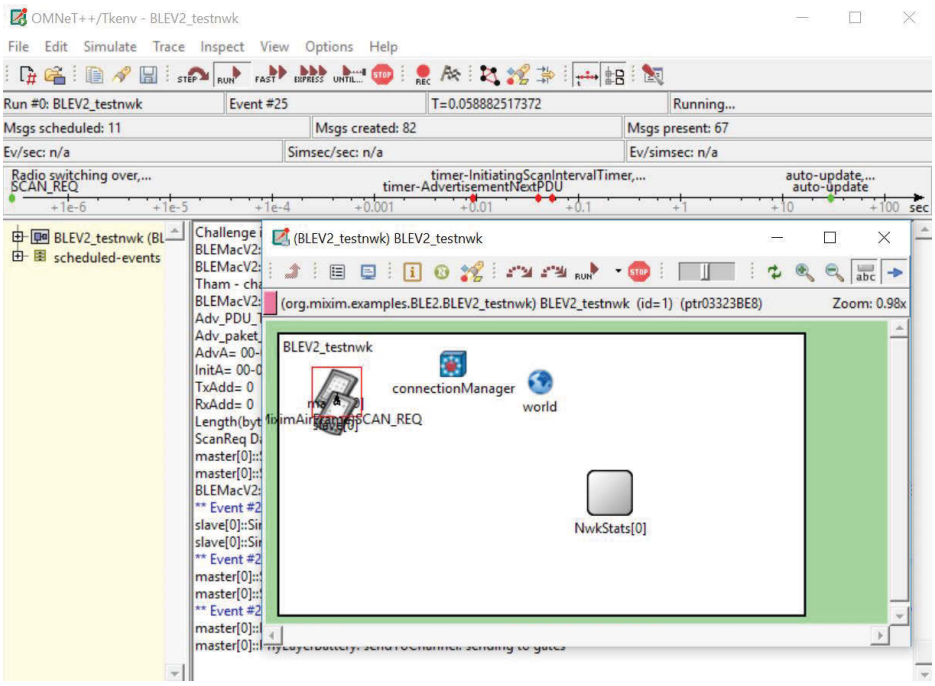
Appendix 2 Pseudocode for connection request packet generation

```
Inputs:

   - AdvAdd: Advertiser's Address
   - InitAdd: Controller's Address

Outputs: Connection_Request packet

1: obtain Access Address

2: set channel mapping

3: set transmission window size

4: set transmission window offset

5: set connection interval;

6: set timeout;

7: encapsulate Connection_Request packet PDU = Header +
InitAdd + AdvAdd + LLData (access add, channel mapping,
trans window size etc.)
```

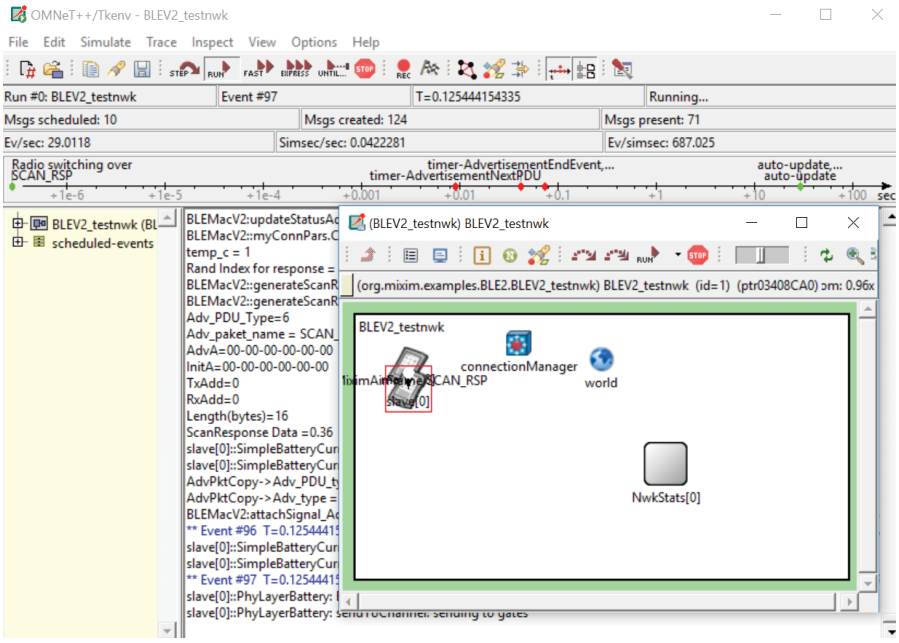
Appendix 3 User interface of initial trust-aware BLE communications when the advertiser sends an ADV_IND packet



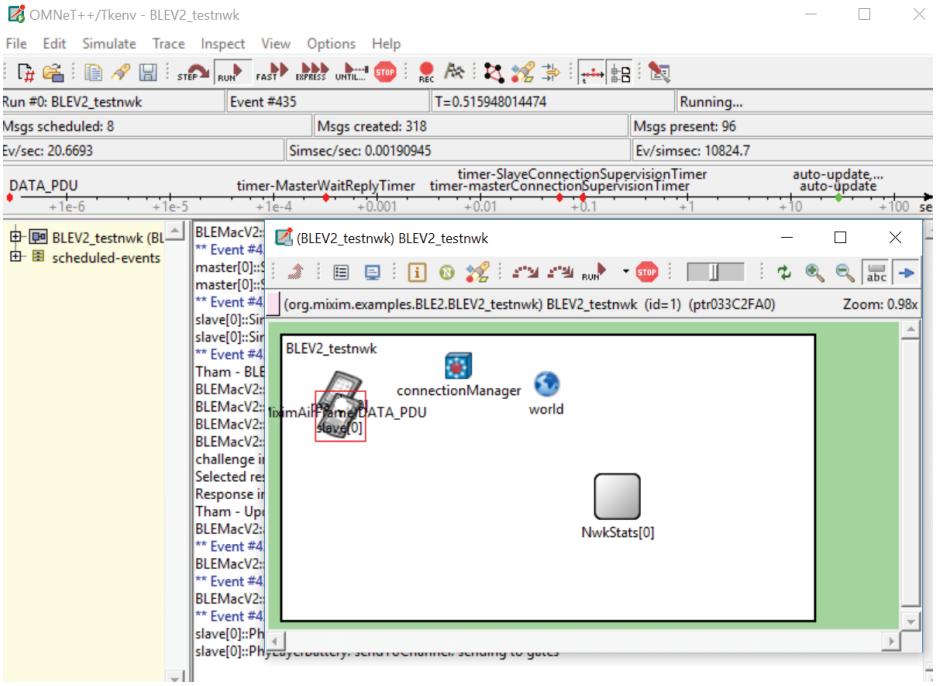
Appendix 4 Screenshot of the user interface of initial trust-aware BLE communications when a SCAN_REQ packet is sent from the controller to the node



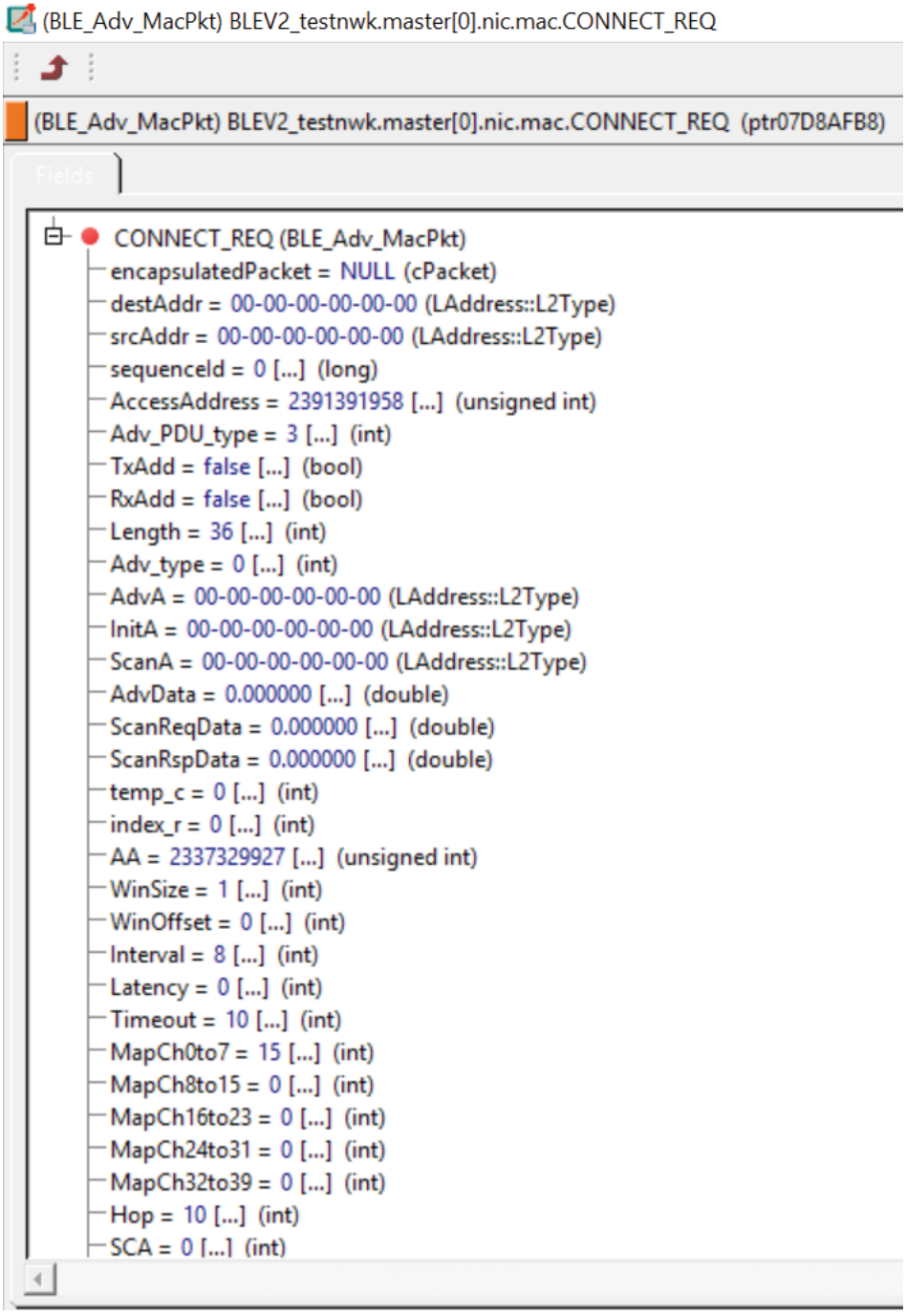
Appendix 5 Screenshot of the user interface of initial trust-aware BLE communications when a SCAN_RSP packet is sent from node to controller



Appendix 6 Screenshot of the user interface of initial trust-aware BLE communications when a DATA packet is sent from the controller to the node



Appendix 7 The connection request packet sent by the controller to the advertiser



Bibliography

[1] J.-H. Cho, K. Chan, and S. Adali, "A Survey on Trust Modeling," *ACM Comput. Surv.,* vol. 48, pp. 1-40, 2015.

[2] J. H. Cho, A. Swami, and I. R. Chen, "A Survey on Trust Management for Mobile Ad Hoc Networks," *IEEE Communications Surveys & Tutorials,* vol. 13, pp. 562-583, 2011.

[3] M. Momani and S. Challa, "Survey of trust models in different network domains," *CoRR,* vol. abs/1010.0168, / 2010.

[4] S. Ruohomaa and L. Kutvonen, "Trust management survey," presented at the Proceedings of the Third international conference on Trust Management, Paris, France, 2005.

[5] F. Gasteiger and E. Hunter, "Security versus Trust requirements: similarities and differences."

[6] A. Josang and J. Haller, "Dirichlet Reputation Systems," presented at the Proceedings of the The Second International Conference on Availability, Reliability and Security, 2007.

[7] S. Ganeriwal, L. K. Balzano, and M. B. Srivastava, "Reputation-based framework for high integrity sensor networks," *ACM Trans. Sen. Netw.,* vol. 4, pp. 1-37, 2008.

[8] F. Bao and I.-R. Chen, "Dynamic trust management for internet of things applications," presented at the Proceedings of the 2012 international workshop on Self-aware internet of things, San Jose, California, USA, 2012.

[9] J. Golbeck, "Computing with Trust: Definition, Properties, and Algorithms," in *2006 Securecomm and Workshops*, 2006, pp. 1-7.

[10] S. Marsh, "Formalising trust as a computational concept," // 1994.

[11] A. Jøsang and S. L. Presti, "Analysing the relationship between risk and trust," in *International Conference on Trust Management*, 2004, pp. 135-145.

[12] Z. Yan, P. Zhang, and A. V. Vasilakos, "A survey on trust management for Internet of Things," *Journal of Network and Computer Applications,* vol. 42, pp. 120-134, 6// 2014.

[13] H. Chaouchi, "Introduction to the Internet of Things," pp. 1-33, 2013.

[14] *IoT devices statistic*. Available: https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/

[15] J. A. Stankovic, "Research Directions for the Internet of Things," *IEEE Internet of Things Journal,* vol. 1, pp. 3-9, 2014.

[16] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "Security, privacy and trust in Internet of Things," *Comput. Netw.,* vol. 76, pp. 146-164, 2015.

[17] I. Andrea, C. Chrysostomou, and G. Hadjichristofi, "Internet of Things: Security vulnerabilities and challenges," in *2015 IEEE Symposium on Computers and Communication (ISCC)*, 2015, pp. 180-187.

[18] Y. Yang, L. Wu, G. Yin, L. Li, and H. Zhao, "A Survey on Security and Privacy Issues in Internet-of-Things," *IEEE Internet of Things Journal,* vol. 4, pp. 1250-1258, 2017.

[19] Y. Ruan, A. Durresi, and L. Alfantoukh, "Trust Management Framework for Internet of Things," in *2016 IEEE 30th International Conference on Advanced Information Networking and Applications (AINA)*, 2016, pp. 1013-1019.
[20] I. Stellios, P. Kotzanikolaou, M. Psarakis, C. Alcaraz, and J. Lopez, "A Survey of IoT-enabled Cyberattacks: Assessing Attack Paths to Critical Infrastructures and Services," *IEEE Communications Surveys & Tutorials,* pp. 1-1, 2018.
[21] R. Daws. (2016). *Another IoT-based DDoS attack leaves Finnish properties without heating*. Available: https://www.iottechnews.com/news/2016/nov/08/another-iot-based-ddos-attack-leaves-finnish-properties-without-heating/
[22] D. Yadron and D. Tynan, "Tesla driver dies in first fatal crash while using autopilot mode," ed, 2016.
[23] Y. Ben Saied, A. Olivereau, D. Zeghlache, and M. Laurent, "Trust management system design for the Internet of Things: A context-aware and multi-service approach," *Computers & Security,* vol. 39, pp. 351-365, 2013/11/01/ 2013.
[24] I. R. Chen, J. Guo, and F. Bao, "Trust Management for SOA-Based IoT and Its Application to Service Composition," *IEEE Transactions on Services Computing,* vol. 9, pp. 482-495, 2016.
[25] Y. Chae, L. C. DiPippo, and Y. L. Sun, "Trust Management for Defending On-Off Attacks," *IEEE Transactions on Parallel and Distributed Systems,* vol. 26, pp. 1178-1191, 2015.
[26] C. J. Fung, J. Zhang, I. Aib, and R. Boutaba, "Dirichlet-Based Trust Management for Effective Collaborative Intrusion Detection Networks," *IEEE Transactions on Network and Service Management,* vol. 8, pp. 79-91, 2011.
[27] D. V. Thiel, *Research Methods for Engineers*: Cambridge University Press, 2014.
[28] Minerva R., Biru A., and R. D. Torino, "Towards a Definition of the Internet of Things (IoT)," I. I. Initiative, Ed., ed. Italy, 2015.
[29] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions," *Future Generation Computer Systems,* vol. 29, pp. 1645-1660, 2013.
[30] C. Perera, A. Zaslavsky, P. Christen, and D. Georgakopoulos, "Context aware computing for the internet of things: A survey," *IEEE Communications Surveys and Tutorials,* vol. 16, pp. 414-454, 2014.
[31] A. Serbanati, C. M. Medaglia, and U. B. Ceipidor, *Building blocks of the internet of things: State of the art and beyond*: INTECH Open Access Publisher, 2011.
[32] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications," *IEEE Communications Surveys & Tutorials,* vol. 17, pp. 2347-2376, 2015.
[33] J. Tan and S. G. Koo, "A Survey of Technologies in Internet of Things," in *Distributed Computing in Sensor Systems (DCOSS), 2014 IEEE International Conference on*, 2014, pp. 269-274.
[34] L. Yan, Y. Zhang, L. T. Yang, and H. Ning, *The Internet of things: from RFID to the next-generation pervasive networked systems*: CRC Press, 2008.
[35] Bluetooth.org. *Core specification v4.2*. Available: https://www.bluetooth.com/specifications/adopted-specifications

[36] M. Siekkinen, M. Hiienkari, J. K. Nurminen, and J. Nieminen, "How low energy is bluetooth low energy? Comparative measurements with ZigBee/802.15.4," in *2012 IEEE Wireless Communications and Networking Conference Workshops (WCNCW)*, 2012, pp. 232-237.

[37] S. Sruthy and S. N. George, "WiFi enabled home security surveillance system using Raspberry Pi and IoT module," in *2017 IEEE International Conference on Signal Processing, Informatics, Communication and Energy Systems (SPICES)*, 2017, pp. 1-6.

[38] F. Montori, R. Contigiani, and L. Bedogni, "Is WiFi suitable for energy efficient IoT deployments? A performance study," in *2017 IEEE 3rd International Forum on Research and Technologies for Society and Industry (RTSI)*, 2017, pp. 1-5.

[39] A. Dunkels, B. Gronvall, and T. Voigt, "Contiki - a lightweight and flexible operating system for tiny networked sensors," in *29th Annual IEEE International Conference on Local Computer Networks*, 2004, pp. 455-462.

[40] P. Levis, S. Madden, J. Polastre, R. Szewczyk, K. Whitehouse, A. Woo*, et al.*, "TinyOS: An Operating System for Sensor Networks," in *Ambient Intelligence*, W. Weber, J. M. Rabaey, and E. Aarts, Eds., ed Berlin, Heidelberg: Springer Berlin Heidelberg, 2005, pp. 115-148.

[41] Q. Cao, T. Abdelzaher, J. Stankovic, and T. He, "The LiteOS Operating System: Towards Unix-Like Abstractions for Wireless Sensor Networks," in *2008 International Conference on Information Processing in Sensor Networks (ipsn 2008)*, 2008, pp. 233-244.

[42] D. J. Cook, A. S. Crandall, B. L. Thomas, and N. C. Krishnan, "CASAS: A Smart Home in a Box," *Computer,* vol. 46, pp. 62-69, 2013.

[43] I. Ungurean, N. C. Gaitan, and V. G. Gaitan, "An IoT architecture for things from industrial environment," in *2014 10th International Conference on Communications (COMM)*, 2014, pp. 1-4.

[44] M. Murar and S. Brad, "Monitoring and controlling of smart equipments using Android compatible devices towards IoT applications and services in manufacturing industry," in *2014 IEEE International Conference on Automation, Quality and Testing, Robotics*, 2014, pp. 1-5.

[45] J. Wan, B. Chen, M. Imran, F. Tao, D. Li, C. Liu*, et al.*, "Toward Dynamic Resources Management for IoT-Based Manufacturing," *IEEE Communications Magazine,* vol. 56, pp. 52-59, 2018.

[46] C. Wang, Z. Bi, and L. D. Xu, "IoT and Cloud Computing in Automation of Assembly Modeling Systems," *IEEE Transactions on Industrial Informatics,* vol. 10, pp. 1426-1434, 2014.

[47] S. Seneviratne, Y. Hu, T. Nguyen, G. Lan, S. Khalifa, K. Thilakarathna*, et al.*, "A Survey of Wearable Devices and Challenges," *IEEE Communications Surveys & Tutorials,* vol. 19, pp. 2573-2620, 2017.

[48] H. H. Nguyen, F. Mirza, M. A. Naeem, and M. Nguyen, "A review on IoT healthcare monitoring applications and a vision for transforming sensor data into real-time clinical feedback," in *2017 IEEE 21st International Conference on Computer Supported Cooperative Work in Design (CSCWD)*, 2017, pp. 257-262.

[49] A. A. Abdellatif, M. G. Khafagy, A. Mohamed, and C. F. Chiasserini, "EEG-based Transceiver Design with Data Decomposition for Healthcare IoT Applications," *IEEE Internet of Things Journal,* pp. 1-1, 2018.
[50] C. Brewster, I. Roussaki, N. Kalatzis, K. Doolin, and K. Ellis, "IoT in Agriculture: Designing a Europe-Wide Large-Scale Pilot," *IEEE Communications Magazine,* vol. 55, pp. 26-33, 2017.
[51] C. Cambra, S. Sendra, J. Lloret, and L. Garcia, "An IoT service-oriented system for agriculture monitoring," in *2017 IEEE International Conference on Communications (ICC)*, 2017, pp. 1-6.
[52] S. Heble, A. Kumar, K. V. V. D. Prasad, S. Samirana, P. Rajalakshmi, and U. B. Desai, "A low power IoT network for smart agriculture," in *2018 IEEE 4th World Forum on Internet of Things (WF-IoT)*, 2018, pp. 609-614.
[53] M. A. Uddin, A. Mansour, D. L. Jeune, and E. H. M. Aggoune, "Agriculture internet of things: AG-IoT," in *2017 27th International Telecommunication Networks and Applications Conference (ITNAC)*, 2017, pp. 1-6.
[54] *IoT applications*. Available: http://www.ti.com/ww/en/internet_of_things/iot-applications.html
[55] S. Krčo, B. Pokrić, and F. Carrez, "Designing IoT architecture(s): A European perspective," in *2014 IEEE World Forum on Internet of Things (WF-IoT)*, 2014, pp. 79-84.
[56] I. Yaqoob, E. Ahmed, I. A. T. Hashem, A. I. A. Ahmed, A. Gani, M. Imran*, et al.*, "Internet of Things Architecture: Recent Advances, Taxonomy, Requirements, and Open Challenges," *IEEE Wireless Communications,* vol. 24, pp. 10-16, 2017.
[57] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, "A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications," *IEEE Internet of Things Journal,* vol. 4, pp. 1125-1142, 2017.
[58] R. Khan, S. U. Khan, R. Zaheer, and S. Khan, "Future Internet: The Internet of Things Architecture, Possible Applications and Key Challenges," in *2012 10th International Conference on Frontiers of Information Technology*, 2012, pp. 257-260.
[59] S. A. Hinai and A. V. Singh, "Internet of things: Architecture, security challenges and solutions," in *2017 International Conference on Infocom Technologies and Unmanned Systems (Trends and Future Directions) (ICTUS)*, 2017, pp. 1-4.
[60] Y. Zhihong, Y. Yingzhao, Y. Yu, P. Yufeng, W. Xiaobo, and L. Wenji, "Study and application on the architecture and key technologies for IOT," in *2011 International Conference on Multimedia Technology*, 2011, pp. 747-751.
[61] M. A. Chaqfeh and N. Mohamed, "Challenges in middleware solutions for the internet of things," in *2012 International Conference on Collaboration Technologies and Systems (CTS)*, 2012, pp. 21-26.
[62] W. Miao, L. Ting-Jie, L. Fei-Yang, S. Jing, and D. Hui-Ying, "Research on the architecture of Internet of Things," in *2010 3rd International Conference on Advanced Computer Theory and Engineering(ICACTE)*, 2010, pp. V5-484-V5-487.
[63] L. D. Xu, W. He, and S. Li, "Internet of Things in Industries: A Survey," *IEEE Transactions on Industrial Informatics,* vol. 10, pp. 2233-2243, 2014.

[64] D. Miorandi, S. Sicari, F. D. Pellegrini, and I. Chlamtac, "Internet of things," *Ad Hoc Netw.,* vol. 10, pp. 1497-1516, 2012.
[65] I. I. Consortium, "Industrial Internet of Things Volume G4: Security Framework," *Ind. Internet Consort,* pp. 1-173, 2016.
[66] B. Yu and M. P. Singh, "An evidential model of distributed reputation management," presented at the Proceedings of the first international joint conference on Autonomous agents and multiagent systems: part 1, Bologna, Italy, 2002.
[67] J. Guo, I.-R. Chen, and J. J. P. Tsai, "A survey of trust computation models for service management in internet of things systems," *Computer Communications,* vol. 97, pp. 1-14, 2017/01/01/ 2017.
[68] S. Sen, "A comprehensive approach to trust management," presented at the Proceedings of the 2013 international conference on Autonomous agents and multi-agent systems, St. Paul, MN, USA, 2013.
[69] K. S. Barber, K. Fullam, and J. Kim, "Challenges for trust, fraud and deception research in multi-agent systems," presented at the Proceedings of the 2002 international conference on Trust, reputation, and security: theories and practice, Bologna, Italy, 2003.
[70] Y. B. Saied, A. Olivereau, D. Zeghlache, and M. Laurent, "Trust management system design for the Internet of Things: A context-aware and multi-service approach," *Comput. Secur.,* vol. 39, pp. 351-365, 2013.
[71] T. Müller, "Bluetooth Security Architecture Whitepaper v1.0," 1999.
[72] H. Kim and E. A. Lee, "Authentication and Authorization for the Internet of Things," *IT Professional,* vol. 19, pp. 27-33, 2017.
[73] W. Sherchan, S. Nepal, and C. Paris, "A survey of trust in social networks," *ACM Comput. Surv.,* vol. 45, pp. 1-33, 2013.
[74] M. K. Deno and T. Sun, "Probabilistic Trust Management in Pervasive Computing," presented at the Proceedings of the 2008 IEEE/IFIP International Conference on Embedded and Ubiquitous Computing - Volume 02, 2008.
[75] R. Feng, X. Han, Q. Liu, and N. Yu, "A Credible Bayesian-Based Trust Management Scheme for Wireless Sensor Networks," *International Journal of Distributed Sensor Networks,* vol. 11, November 1, 2015 2015.
[76] T. Qin, H. Yu, C. Leung, Z. Shen, and C. Miao, "Towards a trust aware cognitive radio architecture," *SIGMOBILE Mob. Comput. Commun. Rev.,* vol. 13, pp. 86-95, 2009.
[77] H. Chen, H. Wu, X. Zhou, and C. Gao, "Agent-based Trust Model in Wireless Sensor Networks," in *Eighth ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing (SNPD 2007)*, 2007, pp. 119-124.
[78] C. J. Fung, B. Martini, M. Gharbaoui, F. Paolucci, A. Giorgetti, and P. Castoldi, "Quality of interaction among path computation elements for trust-aware inter-provider cooperation," in *2014 IEEE International Conference on Communications (ICC)*, 2014, pp. 677-682.
[79] K. Thirunarayan, P. Anantharam, C. Henson, and A. Sheth, "Comparative trust management with applications: Bayesian approaches emphasis," *Future Generation Computer Systems,* vol. 31, pp. 182-199, 2// 2014.

[80] L. A. Zadeh, "A simple view of the Dempster-Shafer theory of evidence and its implication for the rule of combination," *AI Mag.,* vol. 7, pp. 85-90, 1986.
[81] W. Li and H. Song, "ART: An attack-resistant trust management scheme for securing vehicular ad hoc networks," *IEEE Transactions on Intelligent Transportation Systems,* vol. 17, pp. 960-969, 2016.
[82] W. Li, H. Song, and F. Zeng, "Policy-based secure and trustworthy sensing for internet of things in smart cities," *IEEE Internet of Things Journal,* vol. 5, pp. 716-723, 2018.
[83] D. Chen, G. Chang, D. Sun, J. Li, J. Jia, and X. Wang, "TRM-IoT: A Trust Management Model Based on Fuzzy Reputation for Internet of Things," *Computer Science and Information Systems,* pp. 1207-1228, 2011.
[84] P. N. Mahalle, P. A. Thakre, N. R. Prasad, and R. Prasad, "A fuzzy approach to trust based access control in internet of things," in *Wireless VITAE 2013*, 2013, pp. 1-5.
[85] A. Alnasser and H. Sun, "A Fuzzy Logic Trust Model for Secure Routing in Smart Grid Networks," *IEEE Access,* vol. 5, pp. 17896-17903, 2017.
[86] A. Josang, "A logic for uncertain probabilities," *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems,* vol. 09, pp. 279-311, 2001.
[87] A. Jøsang, R. Ismail, and C. Boyd, "A survey of trust and reputation systems for online service provision," *Decision Support Systems,* vol. 43, pp. 618-644, 2007/03/01/ 2007.
[88] V. Balakrishnan, V. Varadharajan, and U. Tupakula, "Subjective logic based trust model for mobile ad hoc networks," presented at the Proceedings of the 4th international conference on Security and privacy in communication netowrks, Istanbul, Turkey, 2008.
[89] J. Ri, H. Lu, Z. Gan, G. Choe, and S. Ri, "Prediction of trust relationship based on subjective logic," in *2015 IEEE International Conference on Cyber Technology in Automation, Control, and Intelligent Systems (CYBER)*, 2015, pp. 1006-1011.
[90] Y. L. Sun, Z. Han, W. Yu, and K. J. R. Liu, "A trust evaluation framework in distributed networks: Vulnerability analysis and defense against attacks," in *Proceedings IEEE INFOCOM 2006. 25TH IEEE International Conference on Computer Communications*, 2006, pp. 1-13.
[91] Y. Wang, Y.-C. Lu, I.-R. Chen, J.-H. Cho, A. Swami, and C.-T. Lu, "LogitTrust: A Logit Regression-based Trust Model for Mobile Ad Hoc Networks," in *Proceedings of the 6th ASE International Conference on Privacy, Security, Risk and Trust*, Boston, MA, USA, 2014.
[92] R. Chen, F. Bao, and J. Guo, "Trust-based service management for social internet of things systems," *IEEE transactions on dependable and secure computing,* vol. 13, pp. 684-696, 2016.
[93] G. V. Crosby, N. Pissinou, and J. Gadze, "A framework for trust-based cluster head election in wireless sensor networks," in *Second IEEE Workshop on Dependability and Security in Sensor Networks and Systems*, 2006, pp. 10 pp.-22.

[94] Y. Wang and V. Vijay, "Trust2: developing trust in peer-to-peer environments," in *2005 IEEE International Conference on Services Computing (SCC'05) Vol-1*, 2005, pp. 24-31 vol.1.
[95] G. Theodorakopoulos and J. S. Baras, "On trust models and trust evaluation metrics for ad hoc networks," *IEEE Journal on Selected Areas in Communications,* vol. 24, pp. 318-328, 2006.
[96] A. Liendo, D. Morche, R. Guizzetti, and F. Rousseau, "Efficient Bluetooth Low Energy Operation for Low Duty Cycle Applications," in *IEEE International Conference on Communications (ICC'2018)*, 2018.
[97] J. Padgette, "Guide to bluetooth security," *NIST Special Publication,* vol. 800, p. 121, 2017.
[98] C. E. Shannon, "A mathematical theory of communication," *SIGMOBILE Mob. Comput. Commun. Rev.,* vol. 5, pp. 3-55, 2001.
[99] D. Robinson, "Entropy and Uncertainty," *Entropy,* vol. 10, p. 493, 2008.
[100] S. Yan Lindsay, Y. Wei, H. Zhu, and K. J. R. Liu, "Information theoretic framework of trust modeling and evaluation for ad hoc networks," *IEEE Journal on Selected Areas in Communications,* vol. 24, pp. 305-317, 2006.
[101] C. K. Wikle and L. M. Berliner, "A Bayesian tutorial for data assimilation," *Physica D: Nonlinear Phenomena,* vol. 230, pp. 1-16, 2007/06/01/ 2007.
[102] M. Evans, N. Hastings, and B. Peacock, "Statistical distributions," ed: Wiley, 2000, p. 34.
[103] M. Sobel, V. R. R. Uppuluri, and K. Frankowski, *Dirichlet distribution, type 1*: American Mathematical Society, 1977.
[104] S. Kotz, N. Balakrishnan, and N. L. Johnson, "Continuous multivariate distributions, Volume 1: Models and applications," ed: John Wiley & Sons, 2004, p. 485.
[105] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "Security, privacy and trust in Internet of Things: The road ahead," *Computer Networks,* vol. 76, pp. 146-164, 1/15/ 2015.
[106] Y. Zhong, B. Bhargava, Y. Lu, and P. Angin, "A Computational Dynamic Trust Model for User Authorization," *IEEE Transactions on Dependable and Secure Computing,* vol. 12, pp. 1-15, 2015.
[107] T. Nguyen, D. Hoang, D. Nguyen, and A. Seneviratne, "Initial trust establishment for personal space IoT systems," in *2017 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, Atlanta, Georgia, USA, 2017, pp. 784-789.
[108] X. Du, D. Shan, K. Zeng, and L. Huie, "Physical layer challenge-response authentication in wireless networks with relay," in *IEEE INFOCOM 2014 - IEEE Conference on Computer Communications*, 2014, pp. 1276-1284.
[109] Y. Gao, G. Li, H. Ma, S. F. Al-Sarawi, O. Kavehei, D. Abbott*, et al.*, "Obfuscated challenge-response: A secure lightweight authentication mechanism for PUF-based pervasive devices," in *2016 IEEE International Conference on Pervasive Computing and Communication Workshops (PerCom Workshops)*, 2016, pp. 1-6.
[110] K. Rhee, J. Kwak, S. Kim, and D. Won, "Challenge-Response Based RFID Authentication Protocol for Distributed Database Environment," in *Security in*

Pervasive Computing: Second International Conference, SPC 2005, Boppard, Germany, April 6-8, 2005. Proceedings, ed, 2005, pp. 70-84.
[111] J. L. Hernández-Ramos, M. P. Pawlowski, A. J. Jara, A. F. Skarmeta, and L. Ladid, "Toward a Lightweight Authentication and Authorization Framework for Smart Objects," *IEEE Journal on Selected Areas in Communications,* vol. 33, pp. 690-702, 2015.
[112] D. Shan, K. Zeng, W. Xiang, P. Richardson, and Y. Dong, "PHY-CRAM: Physical Layer Challenge-Response Authentication Mechanism for Wireless Networks," *IEEE Journal on Selected Areas in Communications,* vol. 31, pp. 1817-1827, 2013.
[113] C. Newman, A. Menon-Sen, A. Melnikov, and N. Williams, "Salted challenge response authentication mechanism (SCRAM) SASL and GSS-API mechanisms," 2070-1721, 2010.
[114] L. Von Ahn, M. Blum, N. J. Hopper, and J. Langford, "CAPTCHA: Using hard AI problems for security," in *International Conference on the Theory and Applications of Cryptographic Techniques*, 2003, pp. 294-311.
[115] E. Uzun, S. P. H. Chung, I. Essa, and W. Lee, "rtCaptcha: A Real-Time CAPTCHA Based Liveness Detection System," in *NDSS Symposium*, San Diego, CA, USA, 2018.
[116] S. Tadelis, *Game Theory: An Introduction*: Princeton University Press, 2013.
[117] T. Nguyen, D. Hoang, and A. Seneviratne, "Challenge-response trust assessment model for personal space IoT," in *2016 IEEE International Conference on Pervasive Computing and Communication Workshops (PerCom Workshops)*, Sydney, Australia, 2016, pp. 1-6.
[118] A. Jøsang and R. Ismail, "The Beta Reputation System," in *15th Bled Electronic Commerce Conference*, 2002.
[119] T. Nguyen, D. Hoang, and A. Seneviratne, "Dirichlet-based Initial Trust Establishment for Personal Space IoT Systems," in *2018 IEEE Internation Conference on Communications (ICC 2018)*, Kansas City, MO, USA, 2018, pp. 1-6.
[120] T. Nguyen, D. Hoang, and A. Seneviratne, "Exploring Challenge-Response Mechanism Designs for IoT Initial Trust Establishment," in *2018 IEEE International Conference on Communications Workshops (ICC 2018)*, Kansas City, MO, USA, 2018, pp. 1-6.
[121] S. Keshav, *Mathematical Foundation of Computer Networking*: Pearson (Addison-Wesley), 2012.
[122] J.-H. Cho, I.-R. Chen, and K. S. Chan, "Trust threshold based public key management in mobile ad hoc networks," *Ad Hoc Networks,* vol. 44, pp. 58-75, 2016/07/01/ 2016.
[123] Apple-Inc. *iBeacon for Developers*. Available: https://developer.apple.com/ibeacon/
[124] Texas-Instruments-Incorporated. Bluetooth Low Energy Beacons [Online]. Available: www.ti.com/lit/pdf/swra475
[125] K. Mikhaylov, "Simulation of network-level performance for Bluetooth Low Energy," in *Personal, Indoor, and Mobile Radio Communication (PIMRC), 2014 IEEE 25th Annual International Symposium on*, 2014, pp. 1259-1263.

[126] MiXiM project [Online]. Available: http://mixim.sourceforge.net/index.html
[127] OMNet++ [Online]. Available: https://www.omnetpp.org/