A Comparative Analysis of Scalable and Context-Aware Trust Management Approaches for Internet of Things

Mohammad Dahman Alshehri[1,2], Farookh Khadeer Hussain[2]

[1] College of Computers and Information Technology, Taif University, Taif, Saudi Arabia
[2] School of Software, Centre for Quantum Computation and Intelligent Systems - QCIS, Decision Systems and e-Service Intelligence Laboratory - DeSI, University of Technology Sydney, Sydney, New South Wales, Australia
Mohammad.D.Alshehri@student.uts.edu.au, Farookh.Hussain@uts.edu.au

Abstract. The Internet of Things – IoT – is a new paradigm in technology that allows most physical 'things' to contact each other. Trust between IoT devices is a critical factor. Trust in the IoT environment can be modeled using various approaches, such as confidence level and reputation parameters. Furthermore, trust is an important element in engineering reliable and scalable networks. In this paper, we survey scalable and context-aware trust management for IoT from three perspectives. First, we present an overview of the IoT and the importance of trust in relation to it, and then we provide an in-depth trust/reliable management protocol for the IoT and evaluate comparable trust management protocols. We also investigate a scalable solution for trust management in the IoT and provide a comparative evaluation of existing trust solutions. We then present a context-aware assessment for the IoT and compare the different trust solutions. Lastly, we give a full comparative analysis of trust/reliability management in the IoT. Our results are drawn from this comparative analysis, and directions for future research are outlined.

Keywords: Internet of Things, Trust Management, Trust Protocol, IoT Scalable, Context-Aware Assessment.

1 Introduction

The Internet of Things (IoT) refers to a system of physical components or 'things' integrated with hardware, software, programming, sensors and a network to enable it to offer effective and efficient value in service through information sharing with manufacturers, users and/or connected devices [19]. Each component in the IoT can be uniquely identified but also has the capacity to inter-operate within the underlying internet infrastructure [16]. Scholars such as [15] use the expression 'Web of Things' to refer to the IoT. According to [14], the term was initially recorded in 1999 by Kevin Ashton, a British visionary. Typically, the IoT is relied upon to offer better integration and connectivity of devices, network infrastructures, systems, and services that span connectivity beyond machine-to-machine links, and it is spread across a mixed collection of conventions or protocols, applications, and domains. The interconnec-

tion between these embedded components, coupled with the growing addition of intelligence, or 'smartness' in devices, is expected to introduce automation in almost all areas, while at the same time facilitating better applications such as Smart Grid [7].

Since 2014, the development of the IoT has rapidly grown because of the convergence of a range of technological advances, including remote connectivity via fault-tolerant networks, wireless communication, embedded systems, and micro-electro-mechanical systems [20]. This implies that the conventional areas of automation, remote sensors, control systems, embedded systems, and augmented reality all contribute to empowering the IoT. The idea of a system of intelligent devices has been discussed since the 1980s, when a Coca-Cola (Coke) machine was developed at Carnegie Mellon University which reported on its stock and the state of coldness of recently stacked beverages [4]. Mark Weiser's fundamental 1991 paper about computing anywhere, anytime in 1991, titled, 'The Computer of the 21st Century', gave rise to the expression 'ubiquitous computing' and is another milestone in the IoT.

Scholarly venues, for example, UbiComp, PerCom and IEEE Spectrum, created the modern concept of the IoT [19]. This concept was further galvanized in 1994 with conceptualization of 'moving little data packets to a huge collection of hubs', in order to incorporate and computerize everything ranging from personal, home and business appliances to complete factory operations [13]. In the period 1993-1996, organizations like Novell proposed such solutions as the Novell Embedded Systems Technology (NEST). In 1999, the field started to gain momentum with MIT's Auto-ID Center and related corporate sector publications [6].

In the IoT, 'things' include, but are not limited to: wearable devices such as heart monitoring tools, biochip transponders implanted in animals, cars with in-built sensors, electric clams used in coastal water areas, field operation equipment for rescue purposes, radio-frequency identification (RFID) applications, and surveillance devices. [6] argues that these devices are used to gather valuable information with the assistance of different innovations. The devices stream the information across other devices in their individual autonomous capacity. Current commercial IoT applications include: intelligent indoor regulator systems, health-oriented wearable devices to screen body temperature, heart rate and other wellbeing issues, spying devices, and home appliances that use Wi-Fi for remote operation and monitoring.

As with the plethora of new applications areas for internet-based automation to venture into, the IoT is likewise expected to create huge chunks of information that is rapidly amassed from disparate areas. As such, there is an increasing need to advance indexing, storage and processing capacity to derive value from the massively growing body of information [10]. [9] stated that the IoT has and will continue to expose people to privacy issues, especially with the 'big data' concept. As such, the IoT may erode the control we have over our own lives as corporations and governments try to amass huge volumes of data and endeavor to maximize financial advantage and control [11]. The importance of trust management in IoT will enable an IoT node to make reliable and context-aware assessments about its interacting partner.

In this paper we will focus on the existing work on trust management in the Internet of Things (IoT), with a view to identifying key shortcomings in this field. This will identify gaps in current state-of-the-art practice to facilitate the realization of a trustworthy IoT network. We use the following classification to categorize the existing approaches:

- Trust/Reliable management protocol for IoT
- Scalable Solution for trust management in IoT
- Context-aware trust assessment in IoT Networks

The paper is organized as follows: Section 2 outlines the trust/reliable management protocol for IoT, and Section 3 presents s scalable solution for trust management of the IoT. Context-aware trust assessment in IoT networks is discussed in Section 4, and Section 5 offers a comparative analysis of trust/reliability management approaches in IoT and discussions.

2 Trust/Reliable Management Protocol for IoT

An IoT network includes a huge number of day-to-day life devices operating in heterogeneous networks, which creates a serious problem with regard to reliability and security management, notwithstanding which, all the elements of an IoT system need to inter-operate agreeably [17]. Reliability can be compromised by the failure to uphold acceptable levels of security, which exposes the system to attacks. Devices in the IoT framework are regularly open to the public and communicate wirelessly, thus creating vulnerability to breaches of security. Conventional approaches to trust protocol, network, system and data security, information management, identity administration, and fault tolerance and governance cannot accommodate modern IoT constraints because of the scalability, data explosion and high diversity of identity types [5]. Therefore, the types of relationship between devices in IoT environments are more complicated than ever before.

A trust management protocol for IoT frameworks was proposed in [2] that has two main goals: to provide an exact and flexible trust evaluation of the trust levels of IoT components, and to use the proposed protocol in different IoT applications to optimize application performance. The trust management protocol models a community-oriented social IoT setting by working with many social relationships across device owners. [2] they claim that social trust is clearly expected in such an environment. The system does not have a specialized trusted authority, but instead spreads the role of trust evaluation to individual nodes.

The underlying principle of the protocol rests in managing nodes in the IoT system to prevent them from misbehaving and to prevent malicious nodes from breaking into its primary functionality to launch trust-related attacks such as bad-mouthing. It considers an IoT framework that is being implemented in an intelligent group where every node self-sufficiently performs trust assessment. The authors give a formal consideration of the convergence, versatility, and accuracy properties of their trust management protocol.

A fuzzy-oriented trust management protocol was proposed by [3] for use in the IoT system that consists of wireless sensors only. The protocol uses Quality of Service (QoS) trust parameters such as energy utilization and packet transfer to delivery ratio. Sensors may create direct communication links between themselves using the IPv6 over the Low the Power Wireless Personal Area Networks (6LoWPAN) protocol, a protocol used for IPv6 networking in devices with low data rates and low power radio

transmission. A reputation and trust framework is perceived to be a critical means of preventing malicious nodes from accessing vast sensor IoT networks, because trust creation instruments can empower a coordinated effort across distributed things, support the discovery of malicious components, and facilitate the decision making process.

An Energy-efficient Protocol of Reliable Trust-based Data Aggregation (ERTDA) protocol was proposed in [5]. The objective of this protocol is to reduce the nodes' energy consumption using an effective routing and recovery approach. Path selection is also used to realize security and reliability in data segregation. The protocol ensures that security is upheld in data capturing, processing and sharing, in addition to identifying mutual trust relationships between nodes and excluding compromised components from the IoT network. This is achieved in three steps as follows: In step 1, every group of aggregated nodes should have its security guaranteed, and have adequate energy to support aggregation and data sharing; In step 2, link availability is ascertained based on the energy in neighboring nodes; and in the final step the importance of the outcome of data aggregation to allow selection of multiple paths is highlighted.

Table 1. Overview and comparative evaluation of Trust/Reliability management protocol for the IoT

Trust management protocol for IoT approach	Description of the approach	Features of the approach	Issues/lacking of the approach
Trust management approach - Dynamic trust management Protocol (DTMP)	A distributed protocol based on a social IoT environment to model trust evaluation between nodes.	Trust is a factor of honesty, community-consciousness and cooperativeness; covers both encounter-based and activity-based incidents; trust evaluation is based on personal experience and recommendations from other common nodes.	A node can only manage its trust assessment to a limited collection of nodes, and thus cannot support trust management for large-scale IoT networks.
Trust, reputation and scalable management approach –(TRM-IoT)	A fuzzy-based trust and reputation management protocol for use in the IoT system consisting of strictly wireless sensors.	Considers a balance between battery drain and security guarantee; trust and reputation elements are derived from direct observation and recommendations; is meant for wireless sensor networks; trust metrics include: successful packet delivery and energy utilization.	Supports wireless sensor IoT networks only; devices with low data rates and/or low power radio transmissions may constrain coordination of trust evaluation across nodes.
Trust and reliability management approach – (ERTDA)	A trust and reliability evaluation protocol that relies on the observations of the cooperation between IoT nodes to enhance understanding of their behavior and detect incidents of compromised nodes.	Optimized routing to reduce energy consumption.	Computation complexity may arise in the course of election of parent node and intense routing.

The next section, we will focus on the scalable solution for trust management in IoT.

3 Scalable Solution for Trust Management in The IoT

As an IoT network connects a huge number of devices and applications, there is an increased challenge with respect to meeting the demands of scalability, dynamic adaptability and compatibility. [1] notes that the IoT assists applications such as continuous e-health and smart product management by capturing, processing and sharing data, which necessitates the use of effective trust management protocols to manage trust between different IoT entities. However, [11] argues that trust management is constrained by the vast quantity of IoT entities, which challenge scalability with respect to accommodating the growing number of computational and storage entities. In addition, IoT networks should evolve to adapt to nodes that are joining and leaving, while building up trust rapidly and accurately. This implies that trust management protocols for IoT networks should be highly resilient to trust-based attacks to endure security issues in hostile environments. According to [1], scalability should be a key consideration in the design of trust/reliable management protocols for IoT. In other works, the trust management protocols proposed by [2], [5], [8], [18], and [12] did not address scalability, undermining their applicability in large-scale IoT networks. Therefore, it is important to consider trust management protocols that have been designed to address the scalability challenge. We now outline and discuss the working of each of these methods.

Firstly, [1] proposed the Scalable, Adaptive and Survivable Trust Management for Community of Interest (CoI) based IoT, recognizing that nodes in IoT networks are owned by individuals and interconnected by social networks. To achieve scalability, they designed a protocol whereby each node can store the trust relationship data of a set of nodes within its CoI, thus enhancing convergence. Nodes can dynamically join or leave while rapidly building up trust towards others due to the increased convergence in the CoI framework and enhanced survivability. Storage is optimized to ensure there is effective utilization of the constrained storage space and make it suitable for large-scale application.

Secondly, [11] proposed an IoT protocol framework for RFID-based devices - the Scalable RFID Security Framework and Protocol Supporting IoT (SRSFPSI). They noted that RFID frameworks should be installed with a comprehensive security structure for a secure, yet scalable operation. The proposal entails an effective ID procedure founded on a hybrid framework (group-based and collaborative technique) and highly adaptive security monitoring handoff for RFID IoT networks. The protocol offers adaptability and scalability while upholding secure and adaptable RFID networks. Other than preventing the introduction of malicious nodes and facilitating scalability, the protocol is integrated with a malware recognition tool.

Thirdly, [17] argued that trust management is a vital step in securing WSN and IoT environments characterized by frequent encounters with unknown agents. They proposed a scalable protocol for an IoT framework that is founded on existing IoT principles of trust management and reputation at semantic and data management levels. To establish tangible levels of scalability, there is no central database, which promotes global knowledge sharing as a means of evaluating earlier interactions. The approach scales well to meet the trust management demands of large sets of nodes, a feat achieved due to the implementation of completely IoT decentralized IoT systems.

Table 2. Overview and comparative evaluation of Scalable solution for trust management in the IoT

Scalable solution for trust management in IoT	Description of the approach	Features of the approach	Issues/lacking of the approach
Trust and adaptive scalable management approach - Scalable, Adaptive and Survivable Trust Management for Community of Interest (CoI) Based IoT.	A distributed, dynamic and scalable trust management IoT protocol based on CoI and storage management approach to extend the functionality of DTMP.	Distributed IoT protocol; trust relationships are evaluated on nodes within a CoI subset; uses a storage management approach to enhance scalability.	Recommendations may be biased if they are from nodes residing in different CoIs, especially in instances where minimal interactions have previously existed.
Trust and scalable management approach - SRSFPSI	A scalable trust framework for a highly mobile RFID-based IoT network.	Applicable in RFID IoT networks; incorporates malware detection capacity; ensures scalable implementation of RFID nodes for a distributed IoT.	Designed for RFID IoT networks only.

In the next section, we will investigate the context-aware assessment for IoT.

4 Context-Aware Trust Assessment in IoT Networks

In IoT networks, context awareness is the capacity to use environmental and situational data to predict instantaneous needs and offer relevant proactive responses [8]. IoT consists of the following technologies: embedded sensors, smart mobile devices, cloud computing, and big data analytics, which work collaboratively to collect, model and guide users. Modern computers, networks and, in this respect, the Internet, are completely dependent on people for data. The greater percentage of the approximately 50 Terabytes of information accessible on the Internet is a result of human effort such as typing, recording, taking digital pictures, or scanning [6]. The challenge lies in the fact that humans are constrained by time, accuracy, memory, and attention, implying that they are relatively poor at capturing information about real world things [2]. With a fully-functioning IoT, we would leverage information about all things, tracking and checking everything and significantly reducing waste and cost. In addition, it would be possible to identify things that require replacement, repair, review, or that are obsolete [12].

Trust management protocols were proposed by [17], [2], [1], and [5] that did not address the context awareness issue. [9] argues that stakeholders in the IoT area of mobile, wearable and ubiquitous computing have recognized the need to secede from the conventional desktop model as more and more devices become mobile. As such, all services should be extended and enhanced to adapt to constantly changing contexts, but this complicates the implementation of trust management protocols in the IoT. [12] claimed that developing context-aware enabling technologies requires a well-defined security framework for IoT networks, whereby nodes are secure despite cutting across different settings – transportation, home, office and others. According to [8], network reactions in relation to user mobility and settings should be adjusted to meet different needs though real-time learning and monitoring to bolster precision.

The Context Awareness for Internet of Things (CA4IOT) framework proposed by [8] is based on automated filtering, synthesis, saving and reasoning in the realm of sensor data collection and the creation of meaningful information from raw data. The framework understands and maintains context data about sensors (such as location, nearby sensor, battery life and sampling rate) using appropriate annotations for quick retrieval. Relationships within different domains are learned from knowledge bases that amass information. The CA4IOT framework follows a layered architecture consisting of: the user – the device owner, application or service, user management, processing, reasoning, context discovery, data acquisition, and sensing

In a work by [18], it is apparent that the future of wireless systems is expected to be highly context-aware, to boost user experiences through personalized services. However, the area of context awareness is constrained by trust and security issues. The Context Broker Architecture (CoBrA) is a framework that facilitates the identification, acquisition, reasoning and presentation of context information. Additionally, it consists of privacy protection mechanisms. The fundamental assumption in CoBrA is that all context-oriented information providers (sensors) have past knowledge (stored in the database) about the presence of context brokers.

A context-aware trust management system was proposed by [12] for the IoT (CTMS4IOT) which adds an element of adaptability to meet the needs of today's dynamic IoT networks. The proposed model entails the following phases: information gathering, entity selection, transaction, reward and punish, and learning. For trust management, the approach uses past behavior and allows for fine-tuning to overcome challenges brought about by malicious nodes. It uses centralized trust management servers and prioritizes the context where evaluations are captured; therefore, appropriate trust management servers return context information with trustworthy values for each node.

Table 3. Overview and comparative evaluation of Context-aware trust assessments

Context-aware trust assessment in IoT approaches	Description of the approach	Features of the approach	Issues/lacking of the approach
Trust context-based – (CA4IOT)	A framework based on automated filtering, synthesis, saving and reasoning in sensor data collection and reasoning to derive valuable information.	Supports learning by understanding and maintaining context data in knowledge bases; uses appropriate annotations for quick retrieval; follows a layered architecture.	Relies on a dedicated server to facilitate knowledge sharing, thus is subject to a single point of failure which may challenge trust management; poor in scaling.
Ontology – (CoBrA)	A context-aware framework that relies heavily on a context broker to capture contextual information from disparate sources and integrate it into a unified model for sharing across computing devices in the IoT network.	The context broker is the fundamental component that maintains a context information sharing model for devices, agents, and services in the IoT; uses ontology to model contexts, and supports privacy protection	In a dynamic environment, the assumption that information about context brokers is well-known in advance can lead to poor implementations that are incapable of handling inconsistent contexts; poor in scaling.
Trust context-based – (CTMS4IOT)	A context-aware distributed trust management system designed to address trust issues based on contextual information and learning.	Its operation is divided into five phases. Allows for fine tuning to meet disparate contextual constraints; modeled on a centralized server setting; support for learning.	Use of centralized trust management servers constrains scalability.

The next section evaluates the comparative analysis of trust/reliability management for the Internet of Things.

5 Comparative Analysis of Trust/Reliability Management Approaches in The IoT and Discussions

Table 4 presents a comparative analysis of trust/reliability management protocols in the IoT to measure the extent to which each protocol meets scalability and context-aware needs. Validation for compliance with trust and reliability considers both scalability and context-awareness. In the table:

- ✗ Implies that a trust/reliability management protocol is neither scalable nor context-aware.
- ✓ Implies that a trust/reliability management protocol is both scalable and context-aware.
- ✓- Implies that a trust/reliability management protocol meets either the threshold for scalability or context-awareness, but not both.

Table 4. Comparative analysis of Trust/Reliability management in the IoT

Approach	Protocol/ Mechanism	Scalable	Context-Aware	Validation	Research Paper
Trust-based	DTMP	✗	✗	✗	[2]
Trust scalable and context-aware	TRM-IoT	✗	✗	✓	[3]
Trust-based	ERTDA	✗	✗	✗	[5]
Trust and scalable	Scalable, Adaptive and Survivable Trust Management for Community of Interest (CoI) Based IoT	✓	✗	✓-	[1]
Trust scalable and context-aware	SRSFPSI	✓	✗	✓	[11]
Trust and scalable	IoT trust framework	✓	✗	✓-	[17]
Trust and context-aware	CA4IOT	✗	✓	✓-	[8]
Ontology	CoBrA	✗	✓	✓-	[18]
Trust and context-aware	CTMS4IOT	✗	✓	✓-	[12]

It is clear from the above comparisons that none of the existing methods for trust modeling in IoT combine the features of scalability and context-aware trust assessment, and validate the working of the proposed approaches. Hence, we can argue that there is a need for research to develop trust management methods that can scale to accommodate billions of IoT nodes and enable trustworthy assessments of IoT nodes.

6 Conclusion

This paper evaluates the existing approaches to trust management in the Internet of Things based on three parameters. The first parameter focuses on trust management protocol in IoT, the second parameter concerns scalable solutions for trust management in IoT, and the third parameter addresses context-aware assessment in IoT. We have given a comparative evaluation of each existing approach for trust modeling in IoT, based on these parameters. Further research into trust management in IoT is required to develop scalable and context-aware trust solutions in IoT networks, actually in the future we plan to focus to tackle that in our works.

References

1. Bao, F., Chen, I.-R., Guo, J.: Scalable, adaptive and survivable trust management for community of interest based Internet of Things systems. 2013 IEEE Eleventh International Symposium on Autonomous Decentralized Systems (ISADS), pp. 1–7 (2013).
2. Bao, F., Chen, I.-R.: Dynamic trust management for internet of things applications. Proceedings of the 2012 International Workshop on Self-aware Internet of Things, pp. 1–6 (2012).
3. Chen, D., Chang, G., Sun, D., Li, J., Jia, J., Wang, X.: TRM-IoT: A Trust Management Model Based on Fuzzy Reputation for Internet of Things. Computer Science and Information Systems, Vol. 8, No. 4, 1207-1228. (2011)
4. Hersent, O., Boswarthick, D. and Elloumi, O. (2011) Z-Wave, in The Internet of Things: Key Applications and Protocols, John Wiley & Sons, Ltd, Chichester, UK.
5. Ma, T., Liu, Y., Zhang, Z.: An energy-efficient reliable trust-based data aggregation protocol for wireless sensor networks. International Journal of Control and Automation, 8(3), 305–318 (2015).
6. Ning, H.: Unit and ubiquitous Internet of Things. CRC Press, Boca Raton FL (2013).
7. Nixon, P. a, Terzis, S.: Trust Management. Lecture Notes in Computer Science vol. 2692, Springer-Verlag, Berlin-Heidelberg (2003).
8. Perera, C., Zaslavsky, A., Christen, P., Georgakopoulos, D.: CA4IOT: Context awareness for Internet of Things. Proceedings of the 2012 IEEE International Conference on Green Computing and Communications, pp. 775–782 (2012).

9. Perera, C., Zaslavsky, A., Christen, P., Georgakopoulos, D.: Context aware computing for the internet of things: A survey. IEEE Communications Surveys & Tutorials. 16(1), 414–454 (2014).
10. Pfister, C.: Getting Started with the Internet of Things. O'Reilly Media, Sebastopol CA.
11. Ray, B.R., Abawajy, J., Chowdhury, M.: Scalable RFID security framework and protocol supporting Internet of Things. Computer Networks. 67, 89–103 (2014).
12. Ben Saied, Y., Olivereau, A., Zeghlache, D., Laurent, M.: Trust management system design for the Internet of Things: A context-aware and multi-service approach. Computers & Security 39, 351–365 (2013).
13. Sicari, S., Rizzardi, a., Grieco, L. a., Coen-Porisini, a.: Security, privacy and trust in Internet of Things: The road ahead. Computer Networks. 76, 146–164 (2015).
14. Singh, M.P.: The practical handbook of internet computing. CRC Press, Boca Raton FL (2004).
15. Tselentis, G., Domingue, J., Galis, A.: Towards the Future Internet: A European Research Perspective. IOS Press, Amsterdam, The Netherlands (2009).
16. Uckelmann, D., Harrison, M., Michahelles, F.: Architecting the Internet of Things. Springer Verlag, Berlin Heidelberg (2011).
17. Wang, J., Bin, S.: Distributed Trust Management Mechanism for the Internet of Things. Proceedings of the 2nd International Conference on Computer Science and Electronics Engineering (ICCSEE 2013), 2197–2200 (2013).
18. Wrona, K., Gomez, L.: Context-aware security and secure context-awareness in ubiquitous computing environments. Proceedings of the XXI Autumn Meeting of Polish Information Processing Society, 255–265 (2005).
19. Yan, Z., Zhang, P., Vasilakos, A. V.: A survey on trust management for Internet of Things. Journal of Network and Computer Applications, 42, 120–134 (2014).
20. Zanella, A., Bui, N., Castellani, A., Vangelista, L., Zorzi, M.: Internet of Things for Smart Cities. IEEE Internet of Things Journal 1(1) 21-32 (2014).