Bayesian Methods for Modelling and Management of Trust in Wireless Sensor Networks

By

Mohammad Momani

Submitted in partial fulfilment of the requirements for the degree of the Doctor of Philosophy

Faculty of Engineering
UNIVERSITY OF TECHNOLOGY, SYDNEY
July, 2008

Certificate of Authorship/Originality

I certify that the work in this thesis has not previously been submitted for a degree nor has it been submitted as part of requirements for a degree except as fully acknowledged within the text. I also certify that the thesis has been written by me. Any help that I have received in my research work and the preparation of the thesis itself has been acknowledged. In addition, I certify that all information sources and literature used are indicated in the thesis.

Acknowledgements

I would like to express my gratitude to my supervisor, Prof. Subhash Challa, whose generosity and commitment are above and beyond the call of duty; words do not describe my gratitude. I appreciate his vast knowledge and skill in many areas and his assistance in completing this thesis. I would like also to thank my co-supervisor, Dr. Tim Aubrey for his assistance and support.

I must also acknowledge the following people from the University of Technology, Dr. Johnson Agbinya and Dr. Tracy Tung for their initial inputs and discussions on the research topic, Dr. Khalid Aboura for his assistance and advice in statistics, Dr. David Davis for his support and useful discussions, Dr. Rami Al-hmouz and Maen Takruri for their support and invaluable philosophical debates, exchanges of knowledge, skills, which helped enrich the experience. Thanks, also goes out to Dr. Rajib Chakravarty and Dr. Nickens Okello from the University of Melbourne for their advice in Bayesian networks.

I would also like to extend my gratitude to my family for the support they provided me through my entire life, without their love, patience and encouragements I would not have finished this thesis.

In conclusion, I recognize that this research would not have been possible without the financial assistance from the University of Technology through a postgraduate scholarship (UTSD) and the partial funding from Thales Australia through the ARC Linkage Grant LP0561200, and I express my gratitude to those agencies.

Contents

List of Figures

List of Tables

List of Abbreviations

BN: Bayesian Network

CONFIDANT: Cooperation of Nodes, Fairness In Dynamic Ad-hoc Networks

CORE: Collaborative Reputation Mechanism to enforce node cooperation in MANETs

CT: Communication Trust

DRBTS: Distributed Reputation-based Beacon Trust System

DT: Data Trust

FC: Fusion Centre

GTRSSN: Gaussian Trust and Reputation System

IDS: Intrusion Detection System

MANET: Mobile Ad-hoc Network

P2P: Peer to Peer

QoS: Quality of Services

RFSN: Reputation-based Framework for High Integrity sensor networks

SRP: Source Routing Protocol

WSN: Wireless Sensor Network

Abstract

Security and trust are two interdependent concepts and are often used interchangeably when defining a secure wireless sensor network (WSN) system. However, security is different from trust in that, it assumes no node is trustworthy and requires ongoing authentication using sophisticated protocols leading to high communication and computation overheads. This makes the traditional cryptographic security tools hard, if not impossible, to be used in wireless sensor networks that are severely resource constrained. Trust on the other hand is the exact opposite of security in that any node can interact with any other and requires no authentication and unwrapping of hidden keys to carry on with their business and hence carries zero overhead. However, this leads to the miss-use and abuse of networks causing loss and damage to the owners of the networks. This thesis focuses on developing novel methods for modelling and managing trust that enable WSN to be secure while significantly reducing computing and communication overheads.

Although researchers have been studying the problem of trust modelling and management in wireless sensor networks for over a decade, their focus was on the trust associated with routing messages between nodes (communication trust). However, wireless sensor networks are mainly deployed to sense the world and report data, both continuous and discrete. However, there are no methods in the literature that focus on the trust associated with misreporting data (data trust). In this thesis, we model the trust associated with the integrity of the data, and

propose methods to combine the data trust with the communication trust to infer the total trust.

Bayesian probabilistic approach is used to model and manage trust. A new risk assessment algorithm for establishing trust in wireless sensor networks based on the quality of services characteristics of sensor nodes, using the traditional weighting approach is introduced. Then a Beta distribution is used to model communication trust (due to its binary nature) and determine the weights in terms of the Beta distribution parameters to probabilistically combine direct and indirect trust.

The thesis extends the Bayesian probabilistic approach to model data trust for cases when the sensed data is continuous. It introduces the Gaussian trust and reputation system to that accounts for uncertain characteristics of sensor data. Finally we introduce a Bayesian fusion algorithm to combine the data trust and communication trust to infer the overall trust between nodes. Simulation results are presented to demonstrate how the models accurately classify different nodes as being trustworthy or not based on their reliability in sensor reporting and routing functions.

1. Introduction

Trust is an old but important issue in any networked environment and can solve some problems beyond the power of the traditional cryptographic security. Trust in general plays a major role in establishing a relationship between entities and has been studied for a long time, mainly by social scientists. Trust is something humans use every day to promote interactions and accept risk; exchanging information with others, buying and selling and all the other interactions with the environment involve some form of trust. Humans base their trust decisions on the situations in which they find themselves, which emphasises the fact that trust is a situational phenomenon [1]. Even though most of the trust decisions are made spontaneously, trust is dependent on time; it can increase or decrease with time based on the available evidence, direct interactions with the same entity or recommendations from other trusted entities.

A wireless sensor network (WSN) is a collection of self-organised sensor nodes, with limited computation and communication capabilities deployed by large numbers mainly in unattended areas (difficult or hostile environments), which makes them open to unique problems; physical capture, communication failure, etc. Neither centralised network administration nor pre-defined network infrastructure exist in such networks. Nodes in WSNs have a limited transmission range, so they employ a multi-hop strategy for communicating with other nodes in

the network and each node simultaneously acts as a router and as a host. Furthermore, sensor nodes have a limited power supply available, as power supplied by batteries is easily exhausted. Lastly, sensor nodes may join or leave a network at any given time, due to the growth of the network or the replacement of failing and unreliable nodes, which results in a highly dynamic network topology.

While wireless communication already exists in all sectors of daily life, WSNs have yet to step beyond the experimental stage. There is a strong interest in the deployment of WSNs in many applications, and this forces the nodes to be of low cost, which prohibits the use of sophisticated measures to ensure data authentication and therefore results in less reliability. Some methods used, such as cryptographic, authentication and other mechanisms [2-7], do not solve the problem entirely and can result in the total breakdown of a network. Therefore new innovative methods to secure communication and to distinguish between good nodes and malicious nodes are needed.

Trust and trust establishment between nodes in WSNs are the starting point for constructing the network and making the addition and/or deletion of sensor nodes very smooth and transparent in such a dynamic and infrastructure-less network. WSNs closely resemble a human behaviour model, wherein a number of nodes that have just met are able to communicate with each other based on mutual trust levels developed over a period of time. In other words there is no a priori trusted subset of nodes to support the network functionality. Trust may only be developed over time, while trust relationships among nodes may also change. So the presence of some optimistic nodes willing to take risks is required in the case of

forming trust with new nodes when there is no evidence of past behaviour. The level of trust must be modified as additional evidence becomes available and that will change the risk assessment of the node. The creation, operation, management and survival of WSNs are dependent upon the cooperative and trusting nature of their nodes, therefore the trust establishment between nodes is a must. That is, for cooperation to happen between nodes, a trust between them must exist, which means that, cooperation influences trust and vice versa. Trust also improves network performances, because honest nodes can avoid working with less trustworthy nodes, as the main benefit of using trust is to accelerate the detection of misbehaving nodes.

Even though trust has been formalised as a computational model, it still means different things for different research communities. Even in the same research field, trust can be defined in different ways, depending on the applications and the methodologies used to calculate trust. We argue that defining trust in WSNs, which has not yet been properly achieved, is the key to understand the meaning of trust and to easily model trust. So we presented a definition of trust in WSNs and from that definition, the properties of trust has been extracted as can be seen in later chapters. Here, the sensed data has also been introduced for the first time as a trust component, so trust in WSNs needs to be redefined to reflect the newly introduced trust component. Based on that, it has been stated that, trust in WSNs will accommodate more than one definition, depend on the applications and/or the attributes involved in calculating trust and few definitions have been presented.

Most studies of trust in WSNs have focused on the trust associated with the routing and the successful performance of a sensor node in some predetermined

tasks. This resulted in examining binary events. However, WSNs have an additional function to the traditional functions of ad-hoc networks (routing), which consists of monitoring events and reporting data. This observed difference is the foundation of our new approach to model trust in WSNs, that is, the trustworthiness and reliability of nodes in WSNs when the sensing data is continuous have not been addressed yet. We look at the issue of security in WSNs using the trust concept, in the case of sensed data that are of a continuous nature.

The trust-modelling problem in WSNs is a decision problem under uncertainty, and the most coherent way to deal with uncertainty is through probability. There are several frameworks for reasoning under uncertainty, but it is well accepted that the probabilistic paradigm is the theoretically sound framework for solving decision problems under uncertainty. Some of the trust models introduced for sensor networks employ probabilistic solutions mixed with ad-hoc approaches. None of them produces a full probabilistic answer to the problem. The problem of assessing a reputation based on observed data is a statistical problem, so a statistical answer to problems where encryption and cryptography keys fail to provide a complete solution has been introduced in the notion of trust.

1.1. Problem scope and definition

Formally, the problem addressed in this thesis can be stated as: “Given a network of large number of sensor nodes deployed in some area distant from a fusion centre, as presented in Figure 1.1. Sensor nodes perform measurements and the fusion centre would like to query statistics of the measured values. However, sensor nodes, as mentioned before, cannot report the measurements directly to the fusion centre, due to their power and range capability, so they employ a multi-hop strategy for communicating with other nodes in the network to deliver the data to the fusion centre. That is, each node in the network acts as a host (senses events) and as a router (routes messages for other nodes) simultaneously. As there is no guarantee that all nodes in the discovered route are trusted nodes and will behave as expected, some malicious or selfish nodes might exist, and that can lead to network malfunctioning or even to a total breakdown of the network. So, how can we exclude the malicious sensor nodes that do not route messages and/or provide correct or reliable sensed data?”

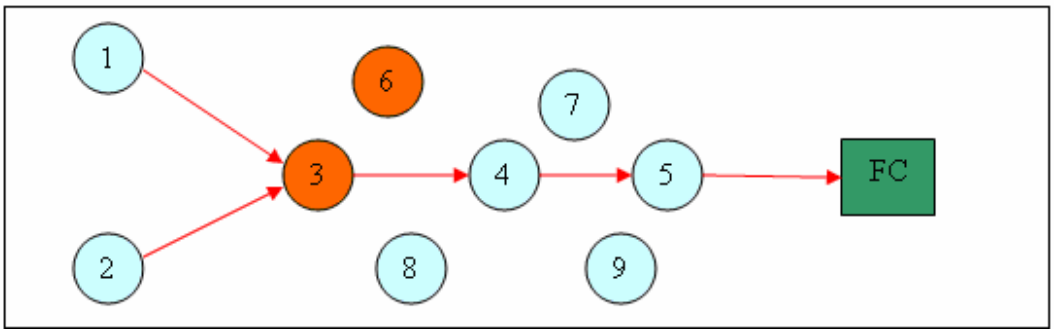

Figure 1.1. Wireless sensor network example

To further illustrate the problem, let us consider the following scenario for the network presented in Figure 1.1, which assumes that a WSN consists of several sensor nodes and a fusion centre (FC). Nodes are deployed to monitor an event and to report the sensed data to the FC. Nodes can communicate, send and receive messages, even if some of them are malicious, but for unseen reasons (being faulty or malicious), they do not report their own sensed data and, vice versa, nodes do report their sensed data but do not route messages for other nodes. In other words, node (3) in Figure 1.1, for example, is forwarding all messages from node (1) and node (2) to the FC using a multi-hop route through nodes (4) and (5), which means that node (3) is very trustworthy from the communication point of view. On the other hand, node (3) is not reporting its actual data to other nodes in the network. For example, if node (3) is a malicious (having been captured by an enemy) node and because the reported data will affect it somehow, imagine that the sensed data are pointing to intruder personnel from the same group as node (3) entering and leaving a battle-field: of course node (3) is not going to report it, so node (3) is untrustworthy from the data point of view. That is, node (3) is trustworthy from a communication point of view and can be untrustworthy from the data point of view. The same situation is valid when all three nodes are sending their sensed data, temperature, for example, but due to the high cost of communication in such networks and because of node (3) being selfish, it is not routing messages from nodes (1) and (2). In this situation, node (3) is trusted from the data point of view but not from the communication point of view. So a mechanism to judge and predict the behaviour of node (3) and to notify the other

nodes and/or the FC about node (3)'s trustworthiness is needed, in order for appropriate actions to be taken.

From the above discussion, I have highlighted that traditional security measurements cannot solve such problems, and there are different approaches targeting different domains to solve this problem, such as:

- Secure routing, to protect the integrity and authenticity of exchanged data, using a low-cost cryptography without placing any overhead at intermediate nodes [8].
- Providing economic incentives to nodes, so they comply with protocol rules.
- Trust-and reputation-modelling, to discover misbehaving nodes and report them, and to maintain a set of metrics, reflecting the past behaviours of other nodes in the network.

Secure routing and economic incentives solve part of the problem, but not all of it. The goal of a trust and reputation system is to enable nodes to make decisions about which nodes to cooperate with and/or to exclude from the network.

Based on the above illustration, the problem questions can be formulated as follows:

- How do sensor nodes trust each other?
- How do individual nodes establish trust among themselves? And, in the case of a node being captured by an enemy or in case of a node acting

maliciously, how can that node be discovered and excluded, and how to verify and notify the other nodes in the network?

- How much trust is enough? And what is the risk associated with each trust value?
- How do trust relationships evolve over time?

These questions are important, but difficult, if not impossible, to answer using the existing security mechanisms.

Initially, the primary focus of the research on trust in WSNs was on whether or not a node will detect appropriately, will report the detected event(s) and will route information. The uncertainty in these actions warranted the development of reputation systems and corresponding trust models. Trust-modelling represents the trustworthiness of each node in the opinion of another node, thus each node associates a trust value with every other node and, based on that trust value, the risk value associated with every task can be calculated.

In other words, trust-modelling is simply the mathematical representation of a node's opinion of another node in a network. That is, we need mathematical tools to represent trust and reputation, update these continuously based on new direct/indirect observations and finally make the decision about the trustworthiness of nodes in WSNs. Several probability distributions can be used to represent the trust and reputation of a node, such as Beta, Gaussian, Poisson, Binomial, etc., as they have a sound theoretical foundation and deal with uncertainty problems. The Beta distribution has been used to represent

communication trust, when the transactions are binary, and the Gaussian distribution has been used to represent data trust, as the sensed data is of a continuous nature. We use Beta distribution for the proper weighting of direct and indirect trust values in one of our algorithms to produce the total trust value and we use the Bayesian estimation to classify nodes as misbehaving or normal nodes.

Our research focuses on modelling and calculating trust between nodes in WSNs, based on sensed continuous data to address security issues and to deal with malicious and unreliable nodes. We propose a new trust model and a reputation system for WSNs. The trust model establishes the continuous version of the Beta reputation system applied to binary events and presents a new Gaussian Trust and Reputation System for Sensor Networks (GTRSSN). We introduce a theoretically sound Bayesian probabilistic approach for mixing second-hand information from neighbouring nodes with directly observed information to calculate trust between nodes in WSNs. We also propose a new Bayesian fusion algorithm to combine both data trust and communication trust to infer the overall trust in WSNs.

1.2. Thesis structure and contributions

The structure of the thesis is organised as follows:

Chapter 2 surveys trust and reputation in various domains. It begins with a brief introduction to the topic of security in sensor networks and the history of trust. It briefly surveys the trust models in social sciences and e-commerce, distributed and peer-to-peer networks, and covers the models in ad-hoc and sensor networks

in detail, as they are more closely related to the research topic. Towards the end, the chapter summarises the methodologies used to model trust in general and their references and also summarises the factors affecting trust updating. It also provides some examples of the systems in which these factors have been implemented.

Chapter 3 explains the trust properties: definitions, classifications, characteristics and values, as a prerequisite to understanding trust. It reviews most of the definitions of trust and presents more than one definition of trust in WSNs, based on the deployment scenario. It also presents the classification of trust in WSNs including trust types and trust constructs and produces the trust typology in WSNs. The chapter also introduces the characteristics of trust in WSNs and concludes with the possible values of trust, which can be assigned between nodes in a WSN.

The main contributions of Chapter 3 are:

1. Defining trust in WSNs, by providing more than one definition based on the applications and the deployed environments.
2. Classifying trust in WSNs, categorising trust types and trust constructs.
3. Building a new trust typology for WSNs, reflecting the trust types and constructs.
4. Characterising trust in WSNs for better understanding and easy modelling.
5. Explaining the possible trust values that can be assigned to nodes in WSNs.

Chapter 4 proposes a new risk assessment algorithm to calculate trust in WSNs, based on the trust properties discussed in Chapter 3. First it reviews the trust factors, which play a major role in building trust in WSNs, it also explains the dynamic aspects of trust and finally presents a new risk assessment algorithm to establish trust in WSNs. The most important part of the algorithm is the trust fusion part, which is a combination of direct and indirect trust to produce the total trust. Several ways of combining trust factors are discussed and a new weighting approach using the Beta probability distribution to weight the direct and indirect trust is proposed. The Beta distribution is being used due to its simplicity, flexibility and easy estimation.

The contributions of Chapter 4 include:

1. An explanation of the trust factors: direct trust, indirect trust, reputation and risk, which contribute to trust establishment between nodes in WSNs.
2. A review of the dynamic aspects of trust: trust formation, trust updating and trust deletion.
3. A new generic trust computational model is presented.
4. Proposal of a new risk assessment algorithm to calculate trust in WSNs based on different criteria. The algorithm combines the direct and indirect trust and eventually calculates the risk associated with every task.
5. A novel method to combine direct and indirect trust values using the Beta probability distributions is introduced. The newly created approach explains how to weight the different types of trust to infer the overall trust value, by treating the direct trust value as a prior in the Beta distribution.

Chapter 5 proposes a new Bayesian probabilistic approach to modelling trust in WSNs. It represents a breakthrough in the way trust is modelled in WSNs. It introduces the continuous sensed data as a core component when deciding to trust nodes in WSNs, as all the previous studies on trust were based on binary events. It also presents a new Gaussian trust and reputation model for sensor networks.

The contributions of Chapter 5 are:

1. Introduction of continuous sensor data as a core component of trust in WSNs.
2. A review of the node misbehaviour classification based on the sensed data.
3. Modification of the trust computational mode introduced in the previous chapter, to reflect the new changes.
4. Discussion of the Beta reputation system and the expert opinion theory and their usage of modelling trust in WSNs.
5. Introduction of a Bayesian probabilistic approach for incorporating the second-hand information from neighbouring nodes, with directly observed information, and showing that this leads to a highly reliable network with fast response to emerging attacks from malicious nodes.
6. Presentation of a new Gaussian trust and reputation system for sensor networks (GTRSSN).

Chapter 6 proposes a novel Bayesian fusion algorithm for inferring trust in WSNs. It argues that one trust component is not enough when deciding on whether or not to trust a specific node in a sensor network. It discusses and analyses the results from the communication trust component (binary) and the data trust component

(continuous) and demonstrate that either component, if considered by itself, can mislead the network or can even cause a total breakdown of the network. So, new methodologies are needed to combine more than one trust component to produce the overall trust. We strongly believe that Bayesian fusion algorithms are good candidates in this regard.

The contributions of Chapter 6 are:

1. A review of the trust components and extension of the trust computational model introduced in the previous chapter, to reflect the new changes.
2. A review of and analysis of the communication trust component.
3. A review of and analysis of the data trust component.
4. Analysis and comparison of the results from data trust and communication trust.
5. Presentation of a new Bayesian fusion algorithm to combine data trust and communication trust to infer the overall trust.

Finally, Chapter 7 concludes the thesis and presents the future research directions.

1.3. Publications arising from this thesis

Journal Papers

- M. Momani and S. Challa, "Bayesian Fusion Algorithm for Inferring Trust in Wireless Sensor Networks ", submitted to Journal of Advances in Information Fusion, July, 2008.

- M. Momani and S. Challa, "Modelling Trust in different domains: a Survey of Trust Models in Wireless Sensor Networks", submitted to International Journal of Distributed Sensor Networks, July, 2008
- M. Momani and S. Challa, “Probabilistic Modelling and Recursive Bayesian Estimation of Trust in Wireless Sensor Networks” submitted to Information Fusion, May, 2008.

Conference Papers

- M. Momani, S. Challa and R. Alhmouz, "BNWSN: Bayesian Network Trust Model for Wireless Sensor Networks", submitted to Mosharaka International Conference on Communications, Computers and Applications (MIC-CCA ’08), Amman, Jordan, 2008.
- M. Momani, S. Challa and R. Alhmouz, “Can we Trust Trusted Nodes in Wireless Sensor Networks?”, presented at The International Conference on Computer and Communication Engineering (ICCCE ’08), Kuala Lumpur, Malaysia, 2008.
- M. Momani, K. Aboura and S. Challa, “RBATMWSN: Recursive Bayesian Approach to Trust Management in Wireless Sensor Networks”, presented at The Third International Conference on Intelligent Sensors, Sensor Networks and Information Processing, Melbourne, Australia, 2007.
- M. Momani and S. Challa, “GTRSSN: Gaussian Trust and Reputation System for Sensor Networks”, presented at International Joint Conferences on Computer, Information, and Systems Sciences, and Engineering (CIS2E 07), University of Bridgeport, USA 2007.

- M. Momani, S. Challa and K. Aboura, “Modelling Trust in Wireless Sensor Networks from the Sensor Reliability Prospective”, in Innovative Algorithms and Techniques in Automation, Industrial Electronics and Telecommunications, Springer, Netherlands, 2006.
- M. Momani, J. Agbinya, R. Alhmouz, G. P. Navarrete and M. Akache, “A New Framework of Establishing Trust in Wireless Sensor Networks”, presented at the International Conference on Computer & Communication Engineering, (ICCCE '06). Kuala Lumpur, Malaysia, 2006.
- D. Umuhoza, M. Momani, J. Agbinya and C. Omlin, “On Trust Metric and Trust Modelling in Mobile Ad Hoc Networks”, presented at the ICTe Africa 2006, Nairobi, Kenya, 2006.
- M. Momani, J. Agbinya, G. P. Navarrete and M. Akache, “A New Algorithm of Trust Formation in Wireless Sensor Networks” presented in AusWireless’06. Sydney, Australia, 2006.
- M. Momani, J. Agbinya, G. P. Navarrete and M. Akache, “Trust Classification in wireless sensor networks”, presented in the 8th International Symposium on DSP and Communication Systems, DSPCS'2005. Noosa Heads, Queensland, Australia, 2005.

Workshop Papers

- M. Momani and S. Challa, “Trust Management in Wireless Sensor Networks”, presented at the SenSys2007 Doctoral Colloquium, Sydney, Australia, 2007.

- M. Momani, S. Challa and K. Aboura, "Security and Trust in Wireless Sensor Networks", presented at ISSNIP ECR Workshop on Sensor Networks (ATNAC2006), Melbourne, Australia, 2006.

2. Literature Review

This chapter introduces wireless sensor networks and their intended usage. It discusses the security and trust concepts and explains the difference between them, stating that even though both terms are used interchangeably when defining a secure system, they are not the same. The difference between reputation and trust is also explained, highlighting that reputation partially affects trust. A survey of trust and reputation systems in various domains is conducted, with more details given to models in ad-hoc and sensor networks as they are closely related to each other and to the research topic. The methodologies used to model trust and their references are presented and also the factors affecting trust updating are summarised and some examples of the systems in which these factors have been implemented are given. The survey concludes that, even though researchers have started to explore the issue of trust in wireless sensor networks, they are still examining the trust associated with routing messages between nodes (binary events). However, wireless sensor networks are mainly deployed to monitor events and report data, both continuous and discrete. This leads to the development of new trust models addressing the continuous data issue and also to combine the data trust and the communication trust to infer the total trust as discussed in later chapters.

2.1. Wireless Sensor Networks

Wireless sensor networks have an unprecedented ability to observe and manipulate the physical world, however, as with almost every technology, the benefits of WSNs are accompanied by a significant risk factors and potential for abuse. So, someone might ask, how can a user trust the information provided by the sensor network?

Sensor nodes are small in size and able to sense, process data, and communicate with each other to transfer information to the interested users. Figure 2.1, shows a typical sensor node (mote) developed by researchers at UC Berkeley called Mica2 as presented in [9]. Typically, a sensor node consists of four sub-systems [10, 11]:

- Computing sub-system (processor and memory): responsible for the control of the sensors and the execution of communication protocols.
- Communication sub-system (transceiver): used to communicate with neighbouring nodes and the outside world.
- Sensing sub-system (sensor): link the node to the outside world.
- Power supply sub-system (battery): supplies power to the node.

WSNs are a collection of self-organised sensor nodes that form a temporary network. Neither pre-defined network infrastructure nor centralised network administration exists. Wireless nodes communicate with each other via radio links and since they have a limited transmission range, nodes wishing to communicate with other nodes employ a multi-hop strategy for communicating and each node simultaneously acts as a router and as a host.

Figure 2.1. Sensor node example (mica2)

It should be noted that bandwidth available between communicating wireless nodes is restricted. This is because wireless networks, in general, have a significantly lower data transmission capacity compared to fixed-line data networks. Furthermore, wireless nodes only have a limited power supply available, as power supplied by batteries is easily exhausted. Lastly, wireless nodes may join or leave a network at any given time and frequently change their location in a network; this results in a highly dynamic network topology.

WSNs consist of sensor nodes with limited computation and communication capabilities deployed in large numbers, that is, tens of thousands as opposed to tens or hundreds of nodes. They present the same challenges that any other Mobile ad-hoc network (MANET) presents (absence of infrastructure, mobility, lack of guaranteed connectivity), but the computation constraint makes the design of solutions even harder. Also, WSNs have an additional function to the traditional functions of MANETs, which concerns monitoring events, collect and process data and transmit sensed information to interested users. This observed difference is the foundation of this new research to model trust in WSNs.

WSNs technology is a relatively new and emerging concept and has received increasing attention due to impressive technological innovations in electronics and communications in the last few years. In addition, the need to have very tiny and cheap nodes being deployed in large numbers and in difficult environments such as military zones led to increased focus by researchers on WSNs [12, 13]. While wireless communication is already used in all sectors of daily life, WSNs have yet to step beyond the experimental stage.

There is a strong interest in the deployment of WSNs in many applications and the research effort is significant. Such deployment can be in controlled environments, such as sensing the atmosphere in buildings and factories, where the mobility of the nodes is of interest. Or they can be spread in hazardous and hostile environments and left unattended. Originally motivated by surveillance in battlefields for the military, interest in WSNs spread over a wide range of applications, from scientific exploration and monitoring, for example, the deployment of a WSN on an active volcano [14, 15], to monitoring the microclimate throughout the volume of redwood trees [16], to building and bridge monitoring [17, 18], to health-care monitoring [19] and a number of other applications such as [11, 12, 20, 21] such as:

- **Industrial Control and Monitoring**: control of commercial lighting, detect the presence of dangerous materials, control of the heating, ventilating, and air conditioning of buildings.
- **Home Automation**: design of the universal remote control, that can control not only the television, DVD player, stereo, and other home

electronic equipment, but the lights, curtains, and locks. Personal computer peripherals control, such as wireless keyboards and mice. Remote keyless entry feature found on many automobiles.

- **Security and Military Sensing:** monitor the status and locations of troops, weapons, and supplies. Detect, locate or track enemy movements. Increase alertness to potential terrorist threats. Monitor and control civilian populations. Provide security in a shopping mall, parking garage or at some other facility.
- **Asset Tracking and Supply Chain Management:** tracking of goods and assets.
- **Intelligent Agriculture and Environmental Monitoring**: crop and livestock management, habitat monitoring and disaster detection.
- **Health Monitoring and Surgery:** physiological data such as body temperature, blood pressure, and pulse are sensed and automatically transmitted to a computer or physician.
- **Civil Engineering**: detect and warn of structural weakness (bridges), track groundwater patterns and how much carbon dioxide cities are expelling. Monitor traffic conditions and plan routes effectively. Determine which spots are occupied and which spots are free in car parks, etc.

2.2. Security in Wireless Sensor Networks

In general, the key security goals of any network are to protect the network against all sorts of attacks, such as eavesdropping, fabrication, injection and modification of packets, impersonation; node capturing and many others, and to address other issues, like privacy, availability, accountability, data authentication, data integrity and data freshness. All these issues apply to traditional and wireless networks, but can have different consequences in WSNs, due to the open transmission medium, the resource constraints and the mass unattended deployment, especially in difficult and dangerous environments.

Research continues to be conducted into the design and optimisation of WSNs, as the use of these networks is still in its infancy phase. The security issue has been raised by many researchers [8, 22-31], and, due to the deployment of WSNs nodes in hazardous and/or hostile areas in large numbers, such deployment forces the nodes to be of low cost and therefore less reliable or more prone to overtaking by an adversary force. Some methods used, such as cryptographic authentication and other mechanisms [2-7, 32, 33], do not entirely solve the problem. For example, adversarial nodes can have access to valid cryptographic keys to access other nodes in the network. The reliability issue is certainly not addressed when sensor nodes are subject to system faults. These two sources of problems, system faults and erroneous data or bad routing by malicious nodes, can result in the total breakdown of a network and cryptography by itself is insufficient to solve these

problems. So new tools from different domains – social sciences, statistics, e-commerce and others – should be integrated with cryptography to completely solve the unique security attacks in WSNs, such as node capturing, Sybil attacks, denial of service attacks, etc.

To protect the network from the above-mentioned attacks, a secure routing protocol (SRP), which addresses the limitation of sensor networks, must be used to secure the communication channel between nodes [34]; since routing in WSNs is a cooperative process whereby route information is relayed between nodes. As there is no guarantee that all nodes in the discovered route will behave as expected to fulfil the promises made. Some malicious or selfish nodes may exist and can lead to a network malfunction or breakdown and will require the SRP to discover and isolate the problem nodes, as the survivability of a WSN requires robustness against rapidly changing topologies and malicious attacks. There are different approaches followed by researchers [8] targeting MANETs and WSNs to solve this problem:

- Maintaining a trust and reputation table for all nodes in a sub-network
- The use of a watchdog mechanism to monitor the behaviour of all the surrounding nodes
- Discover faulty and/or misbehaving nodes, report them and exclude them from the network
- Provide incentives to nodes, so they comply with protocol rules
- The use of low-cost cryptography to protect the integrity and authenticity of exchanged data, without placing any overhead at intermediate nodes

All these approaches will be discussed in detail later in this chapter.

2.3. Notion of Trust

Due to the nature of WSNs deployment being prone to the surrounding environment and suffering from other types of attacks in addition to the attacks found in traditional networks, other security measurements different from the traditional approaches must be in place to improve the security of the network. The trust establishment between nodes is a must to evaluate the trustworthiness of other nodes, as the survival of a WSN is dependent upon the cooperative and trusting nature of its nodes.

Security and trust are two tightly interdependent concepts and because of this interdependence, these terms are used interchangeably when defining a secure system [35]. However, security is different from trust and the key difference is that, it is more complex and the overhead is high. In other words, security means no one is trusted and requires authentication all the time and this leads to very high overhead, while, trust means everybody is trusted somehow and does not require authentication (less overhead).

Trust has been the focus of researchers for a long time [36], from the social sciences, where trust between humans has been studied to the effects of trust in economic transactions [37-39]. Although intuitively easy to comprehend, the notion of trust has not been formally defined. Unlike, for example, reliability, which was originally a measure of how long a machine can be trustworthy, and came to be rigorously defined as a probability, trust is yet to adopt a formal definition.

Along with the notion of trust, comes that of reputation [40], which is occasionally treated by some authors as trust. Reputation is not to be confused with trust: the former only partially affects the latter. Reputation is the opinion of one person about the other, of one internet buyer about an internet seller, and by construct, of one sensor node about another. Trust is a derivation of the reputation of an entity. Based on the reputation, a level of trust is bestowed upon an entity. The reputation itself has been built over time based on that entity's history of behaviour, and may be reflecting a positive or negative assessment. It is these quantities that researchers try to model and apply to security problems in WSNs.

Among the motivating fields for the development of trust models is e-commerce, which necessitated the notion of judging how trusted an internet seller can be [40, 41]. This was the case for peer-to-peer networks and other internet forums where users deal with each other in a decentralised fashion [42-46]. Recently, attention has been given to the concept of trust to increase security and reliability in ad-hoc [35, 47-54] and sensor networks [55-57]. WSNs are open to unique problems, due to their deployment and application nature. The low cost of the sensor nodes of a WSN prohibits sophisticated measures to ensure data authentication. Some methods used, such as cryptographic, authentication and other mechanisms [2-7], do not entirely solve the problem. In the following section a brief survey, introducing only the methodology used to formulate trust and how is it being updated, of existing research on trust from different disciplines is presented in order to easily understand the concept of trust. More attention will be given to research being conducted on trust in MANETs and WSNs, as this is the area of interest for this research.

2.4. Trust and Reputation in Different Domains

Understanding the notion of trust is the key to model trust properly in a specific discipline. Trust is an old but important issue in any networked environment; it has been there all of time and people have been using it in their daily life interactions without noticing, that is, buying and selling, communicating, cooperating, decision-making etc. involves some sort of trust without paying attention to it as a specific phenomenon.

2.4.1. Trust in Social Science and E-Commerce

Social science is concerned with the relationships between individuals in a society [58]. The concept of reputation in social networks is a natural one and people experience it in everyday life (buying, selling). Trust in general simplifies daily life by helping to solve some complex processes and by enabling the delegation of tasks and decisions to other trusted parties [59].

Reputation and trust systems in the context of e-commerce systems, such as eBay [40], Yahoo auctions [40], and internet-based systems such as Keynote [43, 45], use a centralised trust authority to maintain the reputation and trust values. Additionally, these systems use several debatable heuristics for the key steps of reputation updates and integration; due to the use of deterministic numbers for representing reputation [57].

Abdul-Rahman and Hailes in [60] proposed a model for supporting trust in virtual communities, based on direct experiences and reputation. Their model is based on

a word-of-mouth mechanism, which allows agents to decide which other agents' opinion they trust more. They use direct and indirect (recommendations) trust and they introduced the semantic distance of the ratings in their mode.

In [61] Josang and Ismail developed the beta reputation system for electronic markets, based on distribution by modelling reputation as posterior probability based on past experiences. They used the beta probability density functions to combine feedback and derive reputation ratings. The advantages of the beta reputation system are flexibility and simplicity, as well as its foundation on the theory of statistics. The certainty of the trust calculation is defined by mapping the beta distribution to an opinion, which describes beliefs about the truth of statements.

Sabater and Sierra proposed the reputation system ReGreT in [62], which uses direct experiences, witness reputation and analysis of the social network in which the subject is embedded, to calculate trust. Trust is calculated as a weighted average of these experiences and uses the same value range. In [63] and [64], trust is explicitly based on rating experiences and integrating the rating into the existing trust. In [65] and [66], the authors indicated that "trust is more than a subjective probability" and presented a model of trust based on fuzzy logic that took into account many different beliefs and personality factors. On the topic of reputation, the authors of [67] presented a model in which agents can revise their beliefs based on information gathered from other agents and use Bayesian belief networks to filter out information they regard as false.

2.4.2. Trust in Distributed and Peer-to-Peer Systems

Reputation and trust systems in the context of distributed and peer-to-peer (P2P) networks are distributed; there is no centralised entity to oversee the behaviour of nodes in a network, so users keep track of their peers' behaviour and exchange this information directly with others; and also maintain a statistical representation of the reputation by borrowing tools from the realms of game theory [44], Bayesian networks [68-70] and other domains. These systems try to counter selfish routing misbehaviour of nodes by enforcing nodes to cooperate with each other.

Aberer and Despotovic in [42] were one of the first researchers to propose a reputation-based management system for P2P systems. However, their trust metric simply summarises the complaints a peer receives and it is very sensitive to the misbehaviour of peers. The resurrecting duckling model in [23] and its descendants [71, 72] represent a peer-to-peer trust establishment framework in which principals authenticate their communication channel by first exchanging keying material via an out-of-band physical contact. The established trust is binary; the communication channel is either secure or not secure and the model is based upon a hierarchical graph of master-slave relationships and is most suitable for security in large-scale dumb sensor nodes where pre-configuration has to be avoided.

The SECURE project [73, 74] (Secure Environments for Collaboration among Ubiquitous Roaming Entities) attempts to combine all aspects of trust-modelling into a single framework, ranging from trust-modelling and risk analysis to entity

recognition and collaboration models [75]. The SECURE trust model extends the work of Weeks [76] in formalising trust management in security access control systems in terms of least fixed-point calculations, into evidence-based trust models. The model proposed allows each principal to express it's trust policy as a mathematical function which determines it's trust in everyone else, in terms of everyone else's trust assignments. These trust policies can then be combined to produce a consistent trust assignment for all participating principals.

The Distributed Trust Model proposed in [77] makes use of a protocol to exchange, revoke and refresh recommendations about other entities. By using a recommendation protocol, each entity maintains its own trust database. The proposed model is suitable for less formal, provisional and temporary trust relationships and adopts an averaging mechanism to yield a single recommendation value. The handling of false or malicious recommendations has to be supported via some out-of-band mechanism.

Wang and Vassileva in [68-70] modelled trust using Bayesian networks based on the quality of services provided by agents. An agent broadly builds two kinds of trust in another agent; one is the trust in another agent's competence to provide services and the other is the trust in another agent's reliability in providing recommendations about other agents. The systems use binary events – successful or unsuccessful transactions to model trust and weight the direct and indirect information differently. According to the authors, the node will discard the recommendations from the untrustworthy sources but will combine the

recommendations from the trustworthy and unknown sources. Here the reliability includes two aspects: whether the agent is truthful in telling its information and whether the agent is trustworthy or not. Although the models presented in [78] and [79] are based on the quality of services provided by the other peer, they model trust as a weighted vector of all services provided and each service is weighted differently based on its importance.

Kinateder et al., in [80] presented a good comparison between some trust update algorithms and proposed a generic trust model "UniTEC", which provides a common trust representation for trust update algorithms based on experiences. They used direct and indirect trust update separately, by giving more weight to the recent experience than to the old one. This calculates a new trust value based on the old trust value and the new rating. Ratings in the original UniTEC proposal are expressed as a binary metric of either bad or good experience. Azzedin and Maheswaran's trust model in [81] computed the eventual trust based on a combination of direct trust and reputation, by weighting the two components differently; giving more weight to the direct trust. The trust level is built on past experiences and is given for a specific context. Other authors, such as [82] and [83], proposed a neural network approach to model reputation in distributed systems.

BambooTrust, presented in [84], is a practical and high-performance distributed trust management system for global public computing platforms such as grid computing systems. It is based on the XenoTrust presented in [85] and the Bamboo hash table and is implemented to facilitate performance, scalability,

efficiency and load-balancing. BambooTrust is built as a peer-to-peer system in which nodes are identical in terms of what they do, and it also requires a public and a private key to be used. XenoTrust [85] uses the criteria of performance (reliability, honesty and throughput) to assess the others. It is an event-based distributed trust management used in the Xenoserver open platform. Most of the existing trust management systems depend on the traditional request/reply paradigm, which involves polling and causes communication overhead, while the event-based depends on whether a change has occurred or not.

Shand et al., in [86], presented a trust framework to facilitate secure collaboration in pervasive computer systems. Most trust models before this model used security policy, which permits or prohibits the actions and these policy-based models are not suitable for dynamic networks, with topology changing all the time. For each entity recommendation a policy function is formed and by combining these policy functions with other policy functions, the trust level is calculated. Daniele et al., who presented the B-trust model in [87], proposed a lightweight distributed trust framework for pervasive computing that evolves trust based on a Bayesian formalisation, and protects user anonymity, whilst being resistant to "Sybil attacks". They used the weighting approach to weight the direct and indirect (both good and bad) information.

2.4.3. Trust in Ad-hoc Networks

Ad-hoc networks are characterised by dynamically changing their structure; this means nodes join and leave networks very often. While in a roaming process

nodes are continuously confronted with other (unknown) nodes, which can be of a great help to them if they can collaborate with each other, collaboration between strange nodes is not fully utilised, due to the fear of not being trusted and the potential risk of such collaboration. Trust relationships in MANETs are established, evolved, propagated and expired on the fly (no infrastructure) and are very susceptible to attacks, as the whole environment is vulnerable due to the shared wireless medium. In other words, there is no a priori trusted subset of nodes to support the network functionality. Trust may only be developed over time, while trust relationships among nodes may also change [8].

Reputation and trust systems in the context of ad-hoc networks, CONFIDANT [51] and CORE [52], maintain a statistical representation of the reputation by borrowing tools from the realms of Bayesian estimation and game theory respectively. These systems try to counter selfish routing misbehaviour of nodes by enforcing nodes to cooperate with each other. Recently proposed reputation systems in the domain of ad-hoc networks formulate the problem in the realm of Bayesian analytics rather than game theory [88, 89].

Michiardi and Molva, in [52], proposed the CORE system (A Collaborative Reputation Mechanism to enforce node cooperation in MANETs), which uses game theoretic analysis to model reputation. Members that have a good reputation, because they helpfully contribute to the community life, can use the resources, while members with a bad reputation, because they refuse to cooperate, are gradually excluded from the community. In CORE [52], the term "subjective reputation" is used to represent the reputation calculated from direct observations'

using a weighted mean of the observations rating factors, giving more relevance to the past observations. The system uses only the positive value of the indirect reputation to prevent the badmouthing attacks, but does not address the issue of collusion to create false praise. The term "functional reputation" is introduced to allow the subjective and the indirect reputation to be calculated with regard to different functions and to combine them using different weights to obtain a global reputation value.

The CONFIDANT Protocol (Cooperation of Nodes, Fairness In Dynamic Ad-hoc Networks) proposed in [51] is based on direct observations and on second-hand information from other nodes and is updated according to a Bayesian estimation. The model shows that using second-hand information can significantly accelerate the detection and subsequent isolation of malicious nodes. The authors later improved CONFIDANT with an adaptive Bayesian reputation and trust system in [90] and [91]. CONFIDANT differs from CORE only in that it sends reputation values to other nodes in the network, which exposes the scheme to malicious spreading of false reputation values. If a node is observed to behave in a cooperative fashion, then positive reputation is assigned to it, otherwise a negative reputation is assigned to it.

Theodorakopoulos and Baras' model, in [92], presented an extension of their previous work in [93], using the theory of semirings to evaluate the process, which is modelled as a path problem on a directed graph, where nodes represent entities and edges represent trust relations. In their model, users can use the second-hand information from the intermediate nodes to form their opinion about

the others, which means they do not need to have a direct connection with the other nodes to deal with them. The second-hand information is not as valuable as the direct interactions. Also Baras et al., in [48], proposed a solution to the problem of establishing and maintaining trust in MANETs, which addresses the dynamism and the resource constraints of such a network. The network in [48] is modelled as an undirected graph (nodes and links), which is based on the Ising model in physics [94]; nodes interact only with their neighbours.

Buchegger and Boudec, in [90], proposed a system which is robust to false ratings: accusation or praise. Every node maintains a reputation rating and trust rating for other one, and the first-hand information is exchanged with others from time to time. Using a modified Bayesian approach, only the second-hand reputation information that is compatible with the current reputation information is accepted. Reputation rating is modified based on the accepted information and trust rating is updated based on reputation rating. They introduced the re-evaluation process and reputation fading to prevent the exploitation of good reputation built over time. In their model, only the first-hand information is published and, to allow for reputation fading, they weight the evidence by time, giving less weight to observations received in the past. This is different from the standard Bayesian, which gives the same weight for all observations regardless of their time of occurrence; that is why the system is a modified Bayesian approach. To accelerate the detection of misbehaving nodes, the authors used selected second-hand information, which comes from continuously trusted nodes, or passed the deviation test which evaluates compatibility with its own reputation ratings.

Pirzada and McDonald introduced the notion of belief in their communication trust-based model in [35], which provides a dynamic measure of reliability and trustworthiness suitable for applications in an ad-hoc network. The trust model in [35] is an adaptation of Marsh's [95] trust model, but they merged utility and importance in one variable called weight for simplicity. They categorised trust into different categories and calculated trust as a sum of all these weighted categories. Based on the protocol and on the scenario to which the trust model is applied, the total number of categories was defined. The main goal of their model was to build route trustworthiness in nodes by extending the dynamic source protocol to receive a complete list of all nodes through which a protocol has passed.

Trust as a measure of uncertainty was presented in [96] by Sun et al., and as such trust values can be measured by entropy. From this understanding of trust, a few techniques were developed to calculate trust values from observation. In addition, two models were designed: the entropy-based trust model and probability-based trust model to address the concatenation and multi-path trust propagation problems in ad-hoc networks. The proposed models investigate trust relationship associated with packet forwarding, as well as making recommendations.

Liu et al., model, proposed in [34], is used to determine and maintain dynamic trust relationships and then make routing decisions. The purpose of the model is to enhance the security of message routing in MANETs, via selecting the most secure route based on the determined and maintained trust values between nodes. It is based on the assumptions that every node deployed possesses an intrusion

detection system (IDS) that can detect and report the behaviour of malicious nodes, and that nodes are stimulated to cooperate adequately on the network. Each node in the network is initially authenticated by an authentication mechanism and is assigned with a trust value, which is updated automatically based on reports from the IDS.

Davis, in [50], presented a trust management scheme based on a structured hierarchical trust model, which addresses the explicit revocation of certificates and, as they claimed their scheme is robust against malicious accusation exploits (one node accuses the other as malicious, whereas it is not malicious). The model mainly uses digital certificates to establish trust and for a node to be trusted, it needs to present an active certificate which has never been revoked, which means every node is pre-deployed with a certificate. The model is based on assigning different weights to different accusations, and if the sum of all weighted accusations is greater than a pre-defined threshold, the certificate should be revoked.

Models in [97] and [98] propose probabilistic solutions based on a distributed trust model to establish trust relationships between nodes in an ad-hoc network, which does not rely on any previous assumptions. In [97], the authors used the idea of directed graph as their mathematical representations, while in [98], they are using the Beta distribution to calculate trust in MANETs. Jiang and Baras' trust model, presented in [99], consists of two components: a trust computational model (evaluation model) and a trust evidence distribution model (the input of the evaluation model). The model uses the swarm intelligence paradigm and ideas

from a P2P file-sharing system. The model mainly addresses the evidence distribution and retrieval system, using the public and private key concepts, and uses certificates to distribute the evidence.

2.4.4. Trust in Sensor Networks

Trust in WSN networks plays an important role in constructing the network and making the addition and/or deletion of sensor nodes from a network, due to the growth of the network, or the replacement of failing and unreliable nodes very smooth and transparent. The creation, operation, management and survival of a WSN are dependent upon the cooperative and trusting nature of its nodes, therefore the trust establishment between nodes is a must. However, using the traditional tools such as cryptographic tools to generate trust evidence and establish trust and traditional protocols to exchange and distribute keys is not possible in a WSN, due to the resource limitations of sensor nodes [47]. Therefore, new innovative methods to secure communication and distribution of trust values between nodes are needed. Trust in WSNs, has been studied lightly by current researchers and is still an open and challenging field.

Reputation and trust systems in the context of sensor networks prior to this research have received little attention from researchers, however, recently researchers have started to make efforts on the trust topic, as sensor networks are becoming more popular. Ganeriwal and Srivastava were the first to introduce a reputation model specific to sensor networks in [55]; the RFSN (Reputation-based Framework for High Integrity Sensor Networks) model uses the Beta distribution,

as a mathematical tool to represent and continuously update trust and reputation. The model classifies the actions as cooperative and non-cooperative (binary) and uses direct and indirect (second-hand) information to calculate the reputation. The second-hand information is weighted by giving more weight to the information coming from very reliable nodes. Trust is calculated as an expected value of the reputation and the behaviour of the node is decided upon a global threshold; if the trust value is below a threshold, the node is uncooperative, otherwise it is cooperative. The system propagates only the positive reputation information about other nodes [55], and by doing so, it eliminates the bad-mouthing attack, but at the same time it will affect the system's efficiency, as nodes will not be able to exchange their bad experience with malicious nodes. The aging factor is also introduced to differently weight the old and new interactions; more weight is given to recent interactions.

The DRBTS (Distributed Reputation-based Beacon Trust System) presented in [56] is an extension to the system introduced in [100], which presented a suite of techniques that detect and revoke malicious beacon nodes that provide misleading location information. It is a distributed security protocol designed to provide a method in which beacon nodes can monitor each other and provide information so that sensor nodes can choose to trust, using a voting approach. Every beacon node monitors its one hope neighbourhood for misbehaving beacon nodes and accordingly updates the reputation of the corresponding beacon node in the neighbour-reputation table. Beacon nodes use second-hand information for updating the reputation of their neighbours after the second-hand information passes a deviation test. A sensor node uses the neighbour-reputation table to

determine whether or not to use a given beacon's location information based on a simple majority voting scheme. The DRBTS models the network as an undirected graph, uses first-hand and second-hand information to build trust.

Garth et al., [101] proposed a distributed trust-based framework and a mechanism for the election of trustworthy cluster heads in a cluster-based WSN. The model uses direct and indirect information coming from trusted nodes. Trust is modelled using the traditional weighting mechanism of the parameters: packet drop rate, data packets and control packets. Each node stores a trust table for all the surrounding nodes and these values are reported to the cluster head only and upon request. This approach is not based on second-hand information, so it reduces the effect of bad-mouthing. Hur et al., proposed a trust model in [102], to identify the trustworthiness of sensor nodes and to filter out (remove) the data received from malicious nodes. In their model, they assume that each sensor node has knowledge of its own location, time is synchronised and nodes are densely deployed. They computed trust in a traditional way, weighting the trust factors (depending on the application) and there is no update of trust.

The proposed reputation-based trust model in WSNs by Chen et al., in [103], borrows tools from probability, statistics and mathematical analysis. They argued that the positive and/or negative outcomes for a certain event are not enough to make a decision in a WSN. They built up a reputation space and trust space in WSNs, and defined a transformation from the reputation space to the trust space [103]. The same approach presented in RFSN [55] is followed; a watchdog mechanism to monitor the other nodes and to calculate the reputation and

eventually to calculate trust, and Bayes' theorem is used to describe the binary events, successful and unsuccessful transactions, with the introduction of uncertainty. Initially, the trust between strangers is set to (0) and the uncertainty is set to (1). The model does not use second-hand information, and how to refresh the reputation value is an issue. Xiao et al., in [104] developed a mechanism called SensorRank for rating sensors in terms of correlation by exploring Markov Chains in the network. A network voting algorithm called TrustVoting was also proposed to determine faulty sensor readings. The TrustVoting algorithm consists of two phases: self diagnose (direct reading) and neighbour diagnose (indirect reading), and if the reading is faulty then the node will not participate in the voting.

Crosby and Pissinou, in [105], proposed a secure cluster formation algorithm to facilitate the establishment of trusted clusters via pre-distributed keys and to prevent the election of compromised or malicious nodes as cluster heads. They used Beta distribution to model trust, based on successful and unsuccessful interactions. The updating occurs through incorporating the successful/unsuccessful interactions at time $t+1$ with those of time t. Their trust framework is designed in the context of a cluster-based network model with nodes that have unique local IDs. The authors of [106] proposed the TIBFIT protocol to diagnose and mask arbitrary node failures in an event-driven wireless sensor network. The TIBFIT protocol is designed to determine whether an event has occurred or not through analysing the binary reports from the event neighbours. The protocol outperforms the standard voting scheme for event detection.

A few other systems related to trust in WSNs, have been proposed in the literature such as [107-113], which use one or more of the techniques mentioned before to calculate trust. The proposed model in [107] uses a single trust value for a whole group (cluster), assuming that sensor nodes mostly fulfil their responsibilities in a cooperative manner rather than individually. In [108], the model is based on a distributed trust model to produce a trust relationship for sensor networks and uses the weighting approach to combine trust from different sources. In [109], a trust-based routing scheme is presented, which finds a forwarding path based on packet trust requirements, also using the weighting approach. In [110], a stochastic process formulation based on a number of assumptions is proposed to investigate the impact of liars on their peers' reputation about a subject. In [111], the authors proposed a new fault-intrusion tolerant routing mechanism called MVMP (multi-version multi-path) for WSNs to provide both fault tolerance and intrusion tolerance at the same time. The proposed model in [112] is an application-independent framework, built on the alert-based detection mechanisms provided by applications, to identify the malicious (compromised) nodes in WSNs. In [113], a parameterised and localised trust management scheme for sensor networks security (PLUS) is presented, whereby each sensor node rates the trustworthiness of its interested neighbours, identifies the malicious nodes and shares the opinion locally.

From the above survey, which has introduced most of the work undertaken in the area of trust in different domains, it can be noticed that researchers are using many types of methodologies borrowed from different domains to calculate trust, based on different criteria. Table 2.1 below summarises most of the above-mentioned

trust models and the methodologies used to model trust, also the factors used to update trust, direct and indirect trust are summarised in Table 2.2.

Table 2.1. Methodologies used to model trust and their references

Methodology	References
Ratings	[40, 60, 63, 64, 90]
Weighting	[35, 62, 78, 79, 81, 95, 101, 108, 109]
Probability	[51, 55, 61, 88-90, 96-98, 103-105, 110]
Bayesian network	[67-70, 87]
Neural network	[82, 83]
Game theory	[44, 52]
Fuzzy logic	[65, 66]
Swarm intelligence	[23, 71, 72, 99]
Directed and undirected graph	[48, 56, 92-94]

Table 2.2. Factors used to updating trust and their references

Factor	References
Direct only	[103]
Indirect only	[90, 101]
Indirect positive	[52, 55]
Both	[51, 56, 60-62, 68-70, 81, 87]

It is also worth mentioning that almost all the work undertaken on trust is based on successful and unsuccessful (binary) transactions between entities, that is, trust has been modelled in networks in general from a communication point of view, with no exception for WSNs, which is characterised by a unique feature: sensing events and reporting data. This unique characteristic is the basis of this research, which is focusing on modelling and calculating trust between nodes in WSNs based on continuous data (sensed events) and will eventually introduce communication as a second factor of trust. Accordingly, a trust classification for WSNs has been introduced in [114] and in [115, 116] a new risk assessment algorithm to establish trust in WSNs has been introduced, using the traditional weighting approach to combine direct and indirect trust. In [117], the sensed data was introduced as the decisive factor of trust, that is, trust in WSNs was modelled from the sensor reliability perspective. The recursive Bayesian approach to trust management in wireless sensor networks (RBATMWSN) model introduced in [118], represents a new trust model and a reputation system for WSNs, based on sensed continuous data. The trust model establishes the continuous version of the Beta reputation system applied to binary events and presents a new Gaussian Trust and Reputation System for Sensor Networks (GTRSSN), as introduced in [119], which introduces a theoretically sound Bayesian probabilistic approach for mixing second-hand information from neighbouring nodes with directly observed information to calculate trust between nodes in WSNs, and finally a Bayesian fusion approach was introduced in [120], to combine continuous data trust based on sensed events and binary communication trust based on successful and unsuccessful transactions between nodes.

2.5. Conclusion

Trust as an essential attribute in building a relationship between entities has been studied for a long time by scientists from disparate scientific fields. Every field has examined modelling and calculating trust using different techniques, and one of the most prominent and promising techniques is the use of statistics, mainly probabilities to solve the problem, especially in dynamic networks where the topology is changing rapidly.

This chapter has briefly introduced wireless sensor networks and the challenges associated with deploying them in unattended and difficult environments. It has also introduced the security issues in WSNs and the need for new innovative approaches to solve these issues. In the notion of trust, the difference between trust and security has been discussed and it has been explained that trust is not the same as security, even though they are sometimes used interchangeably to describe a secure system. The difference between reputation and trust has also been discussed; the former only partially affects the latter, which means, based on reputation, a level of trust is bestowed upon an entity.

A concise and closely related survey of trust models in different domains – social science and e-commerce, distributed and peer-to-peer networks, ad-hoc networks and wireless sensor networks has also been presented, showing the methodology used to formulate trust in each model, and the way in which the trust updating process is achieved has also been discussed and summarised. Finally, the survey has also shown that, even though researchers have started to explore the issue of

trust in wireless sensor networks, they are still following almost the same approaches used by researchers in other fields to model trust; examining the issue of trust from a binary communication point of view (routing). This is in contrast to our research, which takes into consideration not only the communication side but also the continuous sensed data, which is a unique characteristic of sensor networks and has never been addressed by trust researchers in WSNs.

3. Trust Properties

This chapter explains the trust properties: definitions, classifications, characteristics and values, as a prerequisite to understanding trust. It reviews most of the definitions of trust and states that trust in wireless sensor networks can accommodate different definitions based on the application and the deployed environment, as there is no formal trust definition exists, and introduces few definitions of trust. It also presents the classification of trust in WSNs including trust types and trust constructs and produces the trust typology in WSNs. This chapter also introduces the characteristics of trust in WSNs and concludes with the possible trust values, which can be assigned between nodes in a WSN.

Effective and comprehensive understanding of the notion of trust requires someone to familiarise herself/himself with the meaning of trust and the characteristics of trust. The person must be able to classify trust and also assign reasonable values to trust. To facilitate the contributions in the research area of trust in WSNs, all trust properties from different domains must be categorised into different categories and extended to reflect the nature of trust in WSNs. The following is a list of all the categories addressed:

- Trust Definitions

- Trust Classifications
- Trust Characteristics
- Trust Values

3.1. Trust Definitions

There have been attempts to define trust and introduce axioms that a formal definition must observe. The authors of [36], [121] and [41] have conducted very thorough research to address the issue of divergent trust definitions and provided a concise overview of the conceptual and measurable constructs that are related to trust. They also built a typology of trust across the various disciplines, which is an open typology for researchers to implement in different scenarios.

Trust in general is a directional relationship between two nodes and plays a major role in building a relationship between nodes in a network. Even though trust has been formalised as a computational model, it still means different things for different research communities. Even in the same research field trust can be defined in different ways, depending on the applications and the methodologies used to calculate trust. As discussed before, some researchers use the same definition to refer to trust and reputation, others differentiate between them and refer to them by using two different definitions. This section presents some of the trust and reputation definitions most frequently used by researchers from different sciences, which are more related to this research.

The authors of [60, 80, 87, 105] defined trust as a subjective probability and use the trust definition given by Gambetta in [122]:

> *Trust (or, symmetrically, distrust) is a particular level of the subjective probability with which an agent will perform a particular action, both before [we] can monitor such action (or independently of his capacity of ever to be able to monitor it) and in a context in which it affects [our] own action*

Other researchers, such as the authors of [34, 52, 53, 55, 68, 81, 90], defined trust as a belief in the competence of others and more or less use the definition given by Azzedin and Maheswaran in [81]:

> *Trust is the firm belief in the competence(reliability, timeliness, honesty and integrity) of an entity to act as expected such that this firm belief is not a fixed value associated with the entity but rather it is subject to the entity's behaviour and applies only within a specific context at a given time*

Reputation was defined by [52, 55, 60, 81, 90] as an expectation about an agent's behaviour, as given by Azzedin and Maheswaran in [81]:

> *The reputation of an entity is an expectation of its behaviour based on other entities' observations or information*

about the entity's past behaviour within a specific context at a given time

It has been argued that defining trust in WSNs, which has not yet been properly achieved, is the key to understand the meaning of trust and to easily model trust. So initially a definition of trust in WSN is presented and from that definition, the properties of trust will be extracted.

Trust in WSNs has been mainly defined as given by the definition in [109] and [101]:

The degree of trustworthiness in forwarding packets

or as defined by researchers from other domains using one of the above-mentioned definitions. We argue that, the above definition for trust in WSNs given in [109] and [101], should have the word reliability instead of trustworthiness, as trust definition cannot have trust in it.

In this thesis, the sensed data has been introduced for the first time as a trust component, as mentioned before, and as will be discussed in later chapters, so trust needs to be redefined to reflect the newly introduced trust component. Based on that, trust in WSNs will accommodate more than one definition, depend on the applications and/or the attributes involved in calculating trust. Accordingly, trust between two nodes can be defined as:

The node's belief in the competence and reliability of other nodes

The trust between two nodes, node A and Node B, is therefore "node's A belief in the competence and the reliability of node B". It can also be defined as given in [117]:

> *The subjective probability by which node A depends on node B to fulfil its promises in performing an action and at the same time being reliable in reporting its sensed data*

Here, the competence of the node and its reliability and truthfulness in reporting data have been checked.

3.2. Trust Classifications

Trust in general was categorised by [36] into two categories: a classification system for types of trust and a set of related trust constructs that form a model. The first category is a sensible method of differentiating one conceptual type from another and the second category is a group of constructs that are conceptually distinguishable, but relate to each other in specified ways. In the following sub-sections, the two categories are introduced and modified, so that they can be applied to WSNs.

3.2.1. Trust Types

There are three general types of trust according to [95], basic, general and situational trust, which can be applied to any network, including WSNs.

Basic Trust: this is based on the previous experience of the node in all situations. If two sensor nodes, node A and node B, are to communicate with each other, then the basic trust is not the amount of trust node A has in node B, rather it is the general dispositional trust node A has in other nodes. The higher the value of trust, the more trusting the node is. For example, Node A trusts every other node 20% as a start up trust value.

General Trust: represents the amount of trust node A has in node B, but is not specific to a particular situation. For example, node A trusts node B 50% in general.

Situational trust in nodes: represents the amount of trust node A has in node B in a particular situation. Situational trust is the most important type of trust in cooperative networks such as WSNs. For example, node A trusts node B 70% in forwarding messages to other nodes.

3.2.3. Trust Constructs

The six most important trust constructs of a node in WSNs, driven from the general trust constructs given in [36], are: trusting intention of a node, trusting behaviour of a node, trusting beliefs in nodes, system trust in nodes, dispositional trust of a node and situational decision to trust a node. Figure 3.1, below, shows

the relationships between these constructs as presented in [36], followed by a description of these constructs in WSNs.

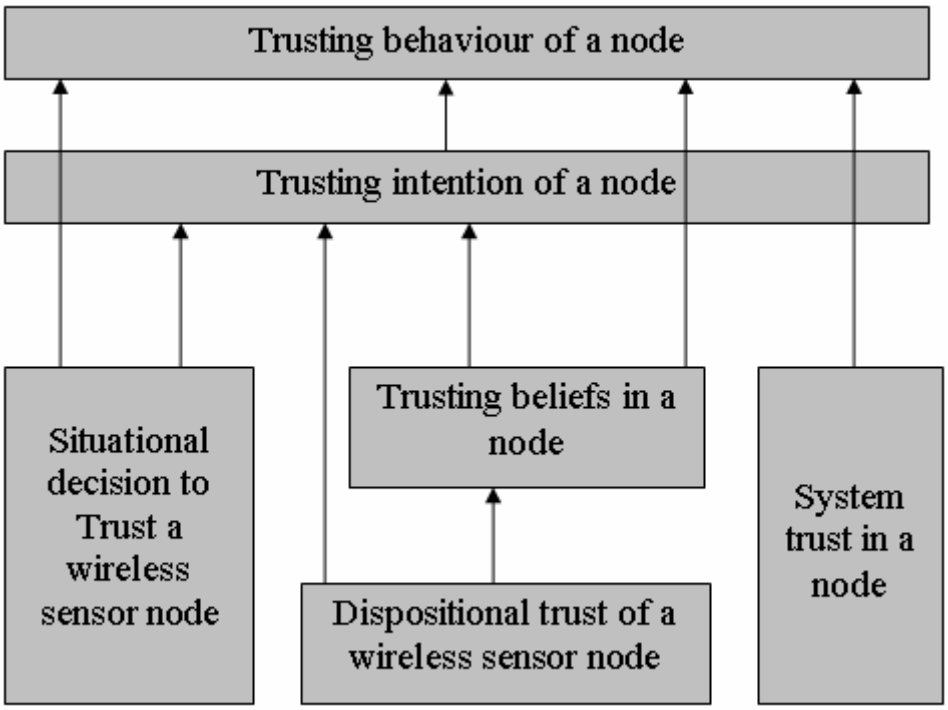

Figure 3.1. Relationships among trust constructs

Trusting intention of a node: is the willingness of one node to depend on another node in a specific situation despite the existence of the risk. This means that node A is willing to depend on node B in a WSN. The trusting intention consists of essential elements, such as experience of reliability, evidence of security, recommendations from another trusted node or entity.

Trusting behaviour of a node: is a voluntary dependence of one node on another node in a specific situation with the existence of risk. It means that node A voluntarily depends on node B in a WSN. Figure 3.1 shows that the trusting

intention of a node supports trusting behaviour, which means that willingness to be dependent leads one node to actually depend (behaviourally) on the other node.

Trusting beliefs in nodes: is the confidence and belief of one node that the other node is trustworthy in a specific situation, that is, when node A believes node B is trustworthy. Therefore the trusting beliefs in nodes consist of four categories:

- Benevolence – the node is acting in the other node's interests
- Ability of the node to fulfil any promises made. Promises can be expressed, for example as a function of the quality of services on offer, such as calculation power, memory, data rate, error rate, etc.
- Competence or the ability of the node to do what is expected or required of it to do, such as reporting sensed data and relaying messages.
- Predictability – is the ability to forecast what a node will do in a specific situation.

System trust in nodes: occurs when nodes believe that proper impersonal structures are in place to encourage successful interactions, such as monitoring and dealing with improper behaviour, that is, node A impersonally trusts the structure of which node B is a part. Thus system trust can depend strongly on the network structure and on the nodes that are part of it.

Dispositional trust of a node: is the node's general expectation about the trustworthiness of other nodes across different situations, that is, when node A is naturally inclined to trust, it has a general trust in other nodes. This is normally the risk a node initially takes when interacting with a new or unknown node.

Situational decision to trust a node: occurs when the node intends to depend on a non-specific other node in a given situation. It means that node A trusts a particular situation or scenario. As illustrated in Figure 3.2 below, if node B wants to communicate with node A, then it should communicate with a trusted third-party management system, which is also trusted by node A. Therefore, the trusted management system acts as a trust broker for the nodes.

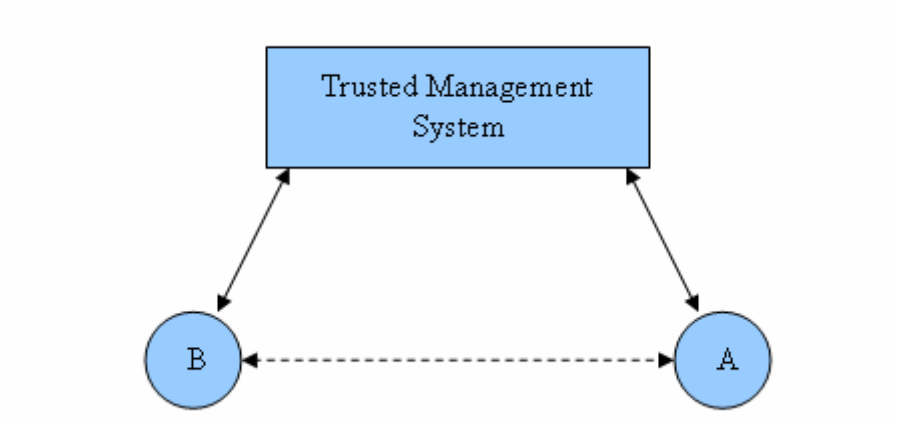

Figure 3.2: Situational decision to trust

3.2.2. Distrust Constructs

Each of the above trust constructs has its opposite distrust construct [39]. These are separate constructs, defined briefly as mirror definitions of trust constructs for simplicity.

Distrusting intention: means that one node is not willing to depend on another node with a feeling of relative security in a situation in which negative

consequences are possible. That is, node A is not willing to depend on node B in a WSN.

Distrusting behaviour: occurs when one node is not willing to voluntarily depend on another node in a specific situation with the existence of risk. That is node A is not willing to voluntarily depend on node B in a WSN.

Distrusting beliefs: the confidence and belief of one node that the other node is not trustworthy in a specific situation, that is, when node A believes node B is not trustworthy.

System distrust: when nodes believe that proper impersonal structures are not in place to encourage successful interactions, that is, when node A distrusts the structure of which node B is a part.

Dispositional distrust: a node has a general tendency to distrust across a broad spectrum of situations. That is, node A is naturally inclined to distrust and has a general distrust in other nodes.

Decision not to trust: when a node has made a decision to distrust in a particular situation. That is, node A distrust a particular situation or scenario.

Having said all of the above regarding trust and distrust constructs, they can be represented mathematically as shown in equation (3.1).

$$T + D = 1 \tag{3.1}$$

where T represents the trust value and D represents the value of distrust.

3.2.4. Trust Typology

Due to the broad concept of trust and the divergent trust definitions in the current literature, the key to move the trust research forward is to build a good theoretical and conceptual view of trust specific to a discipline through a typology of trust constructs.

McKnight and Chervany, in [41], analysed the existing trust definitions and produced an acceptable trust typology by categorising trust definitions into two broad groups. The first group can be categorised as different conceptual types, such as attitudes, beliefs, behaviours and dispositions, and the second group can be categorised as reflecting different referents, such as trust in something, trust in someone or trust in a specific characteristic of someone or something. The two groups of trust definitions seem relatively exclusive but do not overlap, in that the first refers to what type of construct the trust is, while the second refers to the object of trust [41].

From the mapping of the two groups and from the analysis of how trust types relate to each other, an interdisciplinary model of trust types has been built, as shown below in Figure 3.3 presented in [41]. It is almost the same as the relationships model presented in Figure 3.1, with two changes: the system trust constructs and situational decision to trust constructs are merged into one construct as they are related to each other and the trusting behaviour construct was

dropped, due to the endless duplication that is likely to happen, as trusting behaviour depends on trusting intentions.

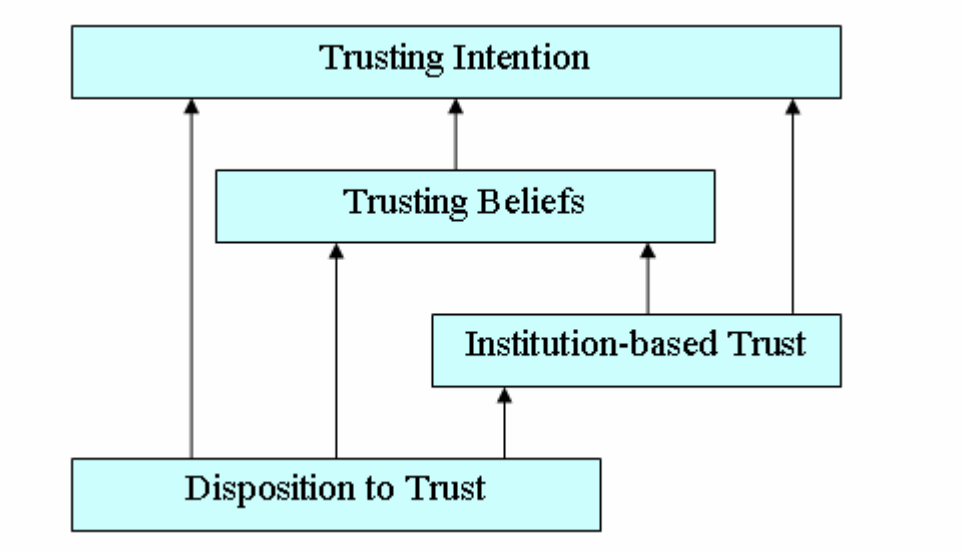

Figure 3.3. Interdisciplinary trust constructs model

The trust relationships model for WSNs has been built based on the interdisciplinary trust constructs model shown in Figure 3.3, to create the typology of related trust constructs in WSNs and to link trust variables to two sensor network trust constructs, as illustrated in Figure 3.4 below. The trust model in Figure 3.4 uses six constructs: disposition to trust, institution-based trust, trusting beliefs, trusting intention, trust-related sensor node behaviour and sensor network interventions. The first four constructs of Figure 3.4 are identical to those in Figure 3.3, and have been discussed in section 3.2.2.

The main link is from trusting intentions and trusting beliefs to trust-related sensor node behaviour. This construct is defined as behaviours that demonstrate a node is willing to communicate with other nodes in the sensor networks, share resources

with them, cooperate with them, exchange sensed information or interact with them. Trust-related sensor node behaviour is not a trust construct, but it is a following consequent of the trust constructs [41]. Trusting beliefs and trusting intention will influence nodes to actually communicate and share resources with other nodes in the sensor network.

The actual network can also influence nodes to collaborate and share resources through the network interventions, as shown in Figure 3.4. These are actions or characteristics the network may take to provide assurance to nodes about the network itself, such as reputation-building, security policies, quality of services, network reliability and inter-networking (links to other networks). The relationships between trust constructs and the sensor network constructs are described below.

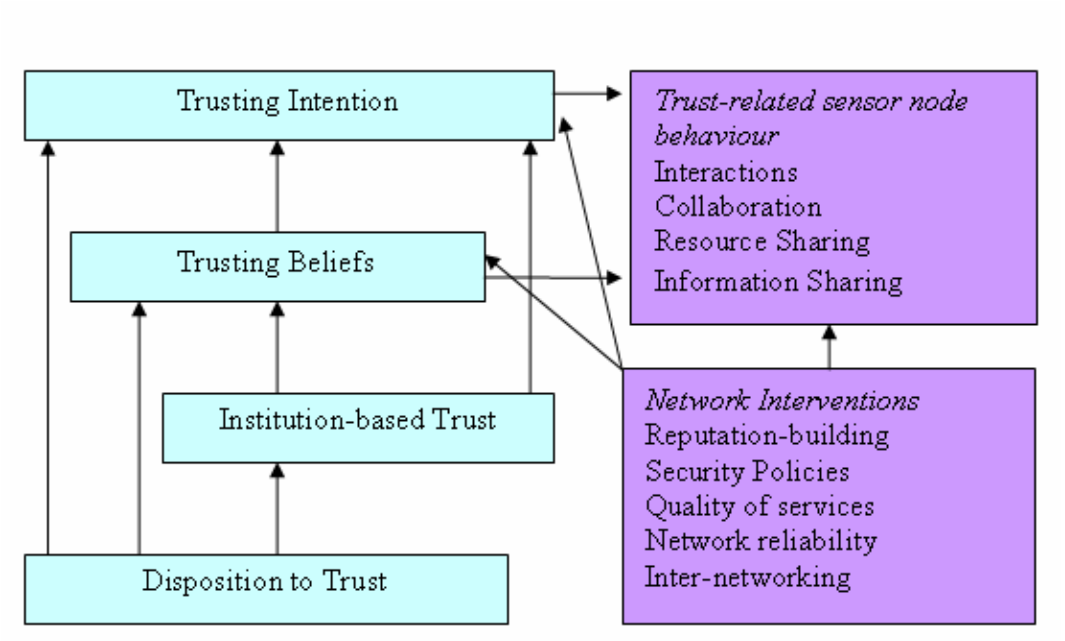

Figure 3.4. Sensor network relationships trust model

Reputation is one of the main sources of trust information about another node or entity [123]: observation, recommendation and reputation. In the absence of direct observations or recommendations, the reputation of a node can be consulted.

Reputation-building: is based on the current information about the node or from the observational experience of its past behaviour. Reputation information is not just based on the opinion of others but also includes an individual agent's own personal experiences, that is, a reputation information is a combination of personal opinions and opinions of others on the same subject [60]. Propagating reputation is a form of social control, whereby the behaviour of a node in a network is influenced by other nodes acting collaboratively. Improving the network reputation will also improve the trusting beliefs and the trusting intention and will encourage other nodes to join and cooperate and share resources and information. Network reputation can be improved through security policies, quality of service, network reliability and inter-networking.

Security policies: good security policies in the sensor network will keep the network available, protected against the denial of service attacks, the integrity of the message is intact, and the confidentiality and privacy protected. This will raise the trusting beliefs in the security of the network and, as a consequence, increase the willingness to depend on that network.

Quality of services: the high quality of services assured by a WSN will provide guarantees on the ability of a network to deliver predictable results and will encourage other nodes to have high trusting intentions towards the network and improve their behaviours.

Network reliability: the trusting beliefs in the network will increase if the network is reliable, generating a willingness to depend on that network, that is, persuade nodes to interact with the network and share resources and information.

Inter-networking: links to other reputable sensor networks will broaden the services of the network and will provide assurance of enabling collaboration and/or any of the other node behaviours.

In summary, each sensor network trust-building intervention tends to influence and produce trust-related sensor node behaviours by building trusting beliefs and intentions.

3.3. Trust Characteristics

For WSNs as self-organising networks to be built and work, there must be some sort of trust between nodes to communicate and exchange information. Trust in such networks is regarded as a self-organising mechanism that places specific requirements on nodes. According to [41, 54], these requirements are:

- Mutual Causality

  Interactions between nodes influence their behaviour and lead to updating their trust value by recommendation exchanges and direct observation.

- Autocatalysis

  Nodes exchange references about other nodes, affecting the trust and the number of interactions between them. Positive evidence reinforces trust

and increases the number of interactions and negative evidence decreases trust and decreases the number of interactions.

- Far-from equilibrium condition

  Nodes as part of a highly changing environment need a trust-based network to integrate new nodes and update information and trust about leaving nodes, in order to free resources such as power supply, network links and memory.

- Morphogenetic change

  Networks with no infrastructure, such as WSNs, are always confronted with random conditions affecting the environment and the resources, such as broken network links, join/leave nodes, power supply, memory and others.

Based on the above-mentioned information regarding trust, and from other works such as [54, 74, 95, 124], trust in WSN can be characterised by the following attributes:

1. Trust is subjective:

   It is based on observations made by a node and evidence made available to a node in a specific situation.

2. Trust is linked with risk:

   There is no reason to trust if there is no risk involved. Although the benefits of interaction are often worth the risk, the higher the risk is, the less cooperation is likely to occur.

3. Trust is intransitive:

   If node (A) trusts node (B) and node (B) trusts node (C), this does not necessarily imply node (A) trusts node (C). However, this does not rule out the possibility of the transfer of trust information.

4. Trust is dynamic:

   It may decrease or increase by time, based on new evidence or experience. It increases through successful interactions and decreases through misuse or unsuccessful interactions.

5. Trust is asymmetric:

   Two nodes do not need to have similar trust in each other or about the trustworthiness of another node. Even if the two nodes obtain the same evidence, they might interpret it in a different way.

6. Trust is reflexive:

   A node always trusts itself (self-trust).

7. Trust is not absolute:

   Trust is represented as levels of trust, which means node A will never trust node B to perform any possible action it may choose, but it will trust it to perform a specific action in a specific context.

3.4. Trust Values

Trust levels have been represented differently by researchers from different domains, based on the adopted trust definition and/or the applications or environments in which it is implemented. They can be represented as a continuous value in the range of (-1, +1), as per [35, 52, 95, 96, 102, 125], or as a discrete value with labels rather than numbers, such as “very trustworthy”, “trustworthy”, “untrustworthy” and “very untrustworthy”, as per [60, 81], or as some probability measurements in the range of (0, 1), as per [48]. Trust models presented in [46, 77], use integral trust values varying from (-1 to 4) signifying discrete levels of trust from complete distrust (-1) to complete trust (4). In [49], six different values from (0 to 5), compromised node (0) to highest trust (1), are used and, based on the message importance, the node with the corresponding trust level required is a candidate to route the message. According to [35], trust degrees can be represented as simple values, such as trusted and distrusted or as structured values of at least two elements, where the first element represents an action, such as, access a file, and the second element represents the trust level associated to that action.

Trust levels can also be computed based on the effort that one node is willing to expend for another node. This effort can be in terms of battery consumption, packets forwarded or dropped or

any other such parameter that helps to establish a mutual trust level [1].

Based on the above illustration regarding trust values from different domains, WSNs can accommodate all sorts of trust values, continuous and/or discrete, depending on the applications and the deployed environment. It is also worth mentioning that continuous trust values can be partitioned into discrete trust values based on the implementation, as discussed in later chapters. Possible continuous and discrete trust values in WSNs are shown below in Table 3.1.

Table 3.1. Possible trust values used in WSN

Value	Label	Description
+1	Blind trust	Based on previous experience
> 0.75	Very high trust	Based on experience and recommendation
.5 to .75	High trust	Based on recommendation
.25 to .5	Medium trust	Based on recommendation and risk
0 to .25	Low trust	Based on dispositional trust (risk) only

-.25 to 0	Low distrust	Based on dispositional trust (risk) only
-.5 to -.25	Medium distrust	Based on recommendation and risk
-.75 to -.5	High distrust	Based on recommendation
< -.75	Very high distrust	Based on experience and recommendation
-1	Complete distrust	Based on previous experience

As can be seen from Table 3.1, trust levels in WSN can take any form within the range from (-1 to 1), continuous or discrete. That is, they can take values in the range (0 to 1) continuous or discrete and so on. It is also notable that direct observation has more influence on the trust level. The benefit of using values for trust is that they reflect the continuous nature of trust in WSN and this allows easy implementation and experimentation. The drawback is that the subjectivity is more difficult to understand and the sensitivity may be a problem, because small differences in individual values may produce relatively large differences in the overall result.

3.5. Conclusions

Understanding trust properties is a prerequisite to understanding the notion of trust. In this chapter, a summary of all trust properties – definitions, classifications, characteristics and values from different domains – has been

discussed and extended to reflect those properties of trust in WSNs. It has been stated that a formal trust definition in general and specifically in WSNs does not exist as such, so a definition of trust can be different based on the application and the deployed environment. That is to say that WSNs can accommodate different trust definitions in different implementations and few definitions were introduced. The chapter has also presented the two general categories of trust: trust types and trust constructs. The relationships among trust constructs models in WSNs have been defined and a trust typology in WSNs has also been presented as the key to move the research on trust forward with the introduction of two new constructs specific to WSNs: trust-related sensor node behaviour and sensor network interventions. It has also been stated that trusting beliefs and trusting intention will influence nodes' behaviour to cooperate and share resources with other nodes in the sensor network, and the actual network can also influence nodes to collaborate and share resources through the network interventions. Characteristics of trust in WSNs as self-organised networks have been discussed and finally the possible levels of trust in WSNs have also been presented. Due to the nature of WSNs deployment, trust can adopt any range of values between (-1 and 1), continuous and/or discrete, based on the applications.

4. Risk Assessment Algorithm for Establishing Trust in Wireless Sensor Networks

This chapter presents a new risk assessment algorithm for establishing trust in WSNs based on the quality of services characteristics of sensor nodes. The algorithm uses the traditional weighting approach to calculate trust and asses risk. This chapter also reviews the trust factors, which play a major role in building trust in WSNs and explains the dynamic aspects of trust. The Beta distribution is also introduced as a novel technique to weight direct and indirect trust, due to its simplicity, flexibility and easy estimation, which makes it widely used in risk and decision analysis.

Trust establishment is a prerequisite for any network to function, that is, establishing trust between nodes is the first step in building the actual WSN, as the creation, operation, management and survival of the WSN are dependent upon the cooperative and trusting nature of its nodes. Modelling trust requires a thorough understanding of the dynamic aspects of trust and the factors that affect trust. So, in this chapter a new risk assessment algorithm for establishing trust in WSNs is presented after introducing the trust factors and the main aspects of trust. This algorithm still uses the traditional weighting approach to calculate the combined trust, which will be developed further to adopt new techniques unique to WSNs.

Whenever a node in a WSN decides on whether or not to communicate with other nodes, it has to assess the other nodes' trustworthiness. Trust-modelling represents the trustworthiness of each node in the opinion of another node; thus each node associates a trust value with every other node [75], and, based on that trust value, a risk value required from the node to finish a job can be calculated. As illustrated in Figure 4.1 proposed by [75], which represents a simple trust model, node X might believe that node Y will fulfil 40% of the promises made, while node Z might believe that node Y will fulfil 50% of the promises made. Calculation of these values will be discussed in detail later in section 4.3.

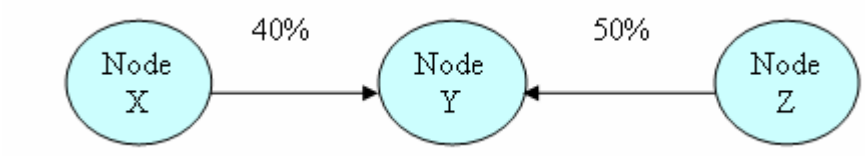

Figure 4.1. A simple trust map

4.1. Trust Factors

The main factors that affect the trust evaluation process of one node about other nodes are:

- Direct interactions
- Indirect interactions
- Reputation
- Risk

Direct interactions are based on self-experience or observations by one node of the other node's behaviour. A watchdog mechanism is required on each node to monitor the behaviour of other nodes in the surrounding.

Indirect interactions are based on recommendations from other trusted nodes in the surrounding area about that other node. A propagation mechanism is required to propagate the recommendations.

Reputation represents the past behaviour of a node in the absence of direct experience or recommendations.

Risk refers to the amount of risk the node is ready to take in the case of forming trust with new or unknown nodes, or in case the trust value between nodes is less than a required trust value to finish a job.

Every node in the network keeps a trust table for all the surrounding nodes it interacts with, which can include the direct trust with each node, the indirect trust, the update on both trusts, the total or combined trust and eventually the risk associated with each node.

4.2. Dynamic Aspects of Trust

One of the trust characteristics is dynamism, that is, trust is dependent on time, it can increase or decrease as new evidence becomes available, so the process needs to be evaluated continuously. Most of the definitions of trust in the literature focus

on what trust is used for in a static fashion, and not on the dynamic aspects of trust, such as the formation, evolution, revocation and propagation of trust [123]. A brief discussion about these aspects in WSNs is presented below.

4.2.1. Trust Formation

Establishing trust between nodes in WSNs is the most important dynamic aspect of trust. Trust formation in WSN is the process of establishing the initial trust between nodes and in general it involves the assessment of the two main sources for calculating trust, direct and indirect interactions. Figure 4.2, below, shows a general trust computational model used to calculate trust in WSNs. The reputation factor is omitted from Figure 4.2, because it represents the past direct and indirect trust and this will be discussed in later chapters. The dispositional trust (risk) is introduced as a third source for trust calculations. The total trust is calculated by combining both trust values, direct and indirect. Knowing the trust value will lead to the risk involved in the interaction: the lower the trust value, the higher the risk, and the higher the trust value, the lower the risk.

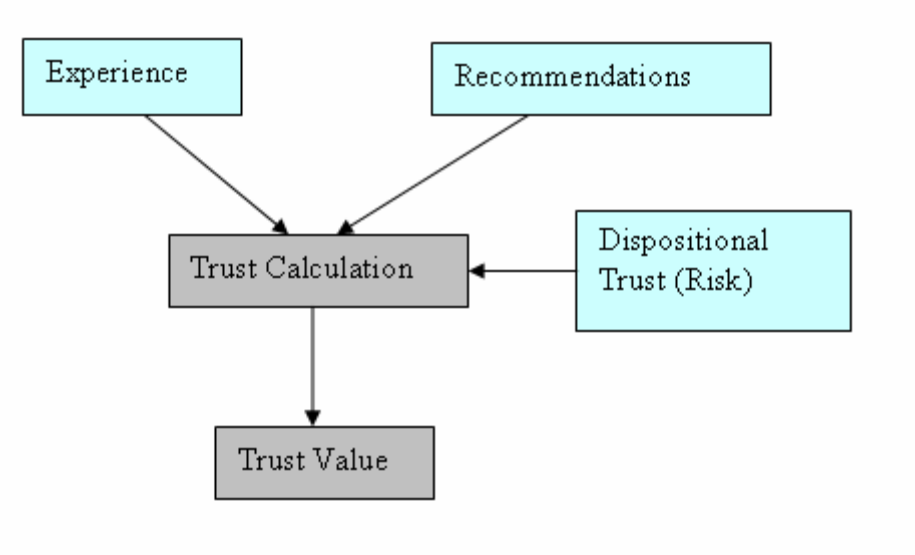

Figure 4.2. General trust computational model

Initially, when nodes are just being deployed for the first time or when new nodes are introduced to the network, the presence of some optimistic nodes willing to take risks is required, as there is no evidence of nodes' past behaviour. Initial trust value between nodes can be assigned based on the applications and/or the deployed environment, using one of the following methods:

1) All nodes are considered to be trustworthy. This is the quickest method of establishing trust and building a functional network, but it is very risky, as malicious nodes can be given a high trust value. It is a practical method when the network deployment is not for a critical mission application – sensing temperature, for example.

2) All nodes are considered to be untrustworthy. It is a very slow method; trust formation takes a very long time to be established, but on the other hand it is very robust and can be used in critical mission networks: battlefields, for example.

3) All nodes are neutral; they are neither trustworthy nor untrustworthy. This is in between in terms of establishing trust compared to the other mentioned methods.

4.2.2. Trust Evolution

The evolution process is another important dynamic aspect of trust and can be regarded as iterating the process of trust formation as additional evidence becomes available. It is the process of updating the trust level between nodes. Trust values regarding other nodes should be maintained locally and updated periodically as new evidence becomes available, and that will eventually change the risk assessment of the node. In order for nodes in a network to receive updates regarding the trusted behaviours of nodes or even threats, a mechanism for trust reporting is necessary.

As previously discussed in Chapter 2, updating trust can be achieved using the first-hand information only: direct trust, as in [103], the second-hand information only: indirect trust, as in [90, 101], the indirect positive trust only, as in [52, 55]; and/or both: direct and indirect trust, as in [51, 56, 60-62, 68-70, 81, 87]. As can be seen, most systems proposed so far use both: first-hand and second-hand information. The main issue here is how to combine these two trust sources to achieve the total trust. The traditional answer to this question is to combine them using the “weighting” approach. Some trust systems give more weights to the old experience, some give more weight to recent experience and others give more weight to direct trust rather than to indirect trust. More detail about the issue and

other approaches to combining trust from different sources will be discussed in later chapters.

In summary, the trust evolution process involves:

- Updating direct trust
- Updating indirect trust
- Updating total trust, based on the updated values of direct and indirect trust.

4.2.2. Trust Revocation

Trust revocation is another important dynamic aspect of trust and is especially essential in WSNs and mobile ad-hoc environments, due to the rapid changes in the network topology. Mechanisms should be utilised to monitor the behaviour of network nodes, and distrusted and/or faulty nodes should be excluded from the network. Fast response and update is required when faulty or compromised nodes are discovered in the network to free resources and to minimise the potential risk in case of compromised nodes. Some protocols exist to manage the network restructuring in case of nodes being introduced to or discarded from a network, but they are outside the scope of this research [126-128].

4.3. Risk Assessment Algorithm

Based on the above discussion regarding trust factors and dynamic aspects of trust, a new algorithm for establishing trust in WSNs is presented in Figure 4.3 as a flowchart, and is based on the algorithm from our work presented in [129], with new modifications to facilitate the simulation process. It is assumed at this stage that trust is computed using the traditional weighting approach of the quality of service (QoS) characteristics offered by nodes in WSNs such as packet forwarded, data rate, error rate, power consumption, reliability, competence, etc. These characteristics are classified in different categories by the node itself and trust values are assigned to these categories based upon the node's own criteria, circumstances and the situations in which it finds itself. Each node will calculate trust for all its surrounding nodes and store these values locally for later usage and, as mentioned before, these values should be updated in a specific time period based on new interactions.

The whole idea of the algorithm given in Figure 4.3 is that there is a risk value associated with every job to be processed by a node, which is derived from the trust value required to do a specific task. The first thing a node will do if it has been asked to perform a task, is to compare the predefined risk value associated the task with the actual risk between the two nodes, and if the risk value is less than the predefined threshold, then the task will be performed, otherwise the task will be declined unless the node is ready to take that risk. The algorithm is just comparing risk values and combining direct trust and indirect trust to achieve the total trust and eventually calculate the actual risk associated, that is, it does not

calculate the direct or indirect trust, but the node itself does that. How to calculate the direct trust and indirect trust between nodes is the basis of the next chapter. Here, just the assessment of the trust and the risk of nodes are discussed. A more detailed illustration of the algorithm follows. It is assumed that there is a required trust value (T) associated with each job to be processed by a node and eventually a risk value is derived from that trust value. The trust value (T) is then tested against the sources of trust, the direct trust value (A), the indirect trust value (B), and the total trust value (C) and at the same time calculates the risk value (R). If any combination of these values is greater than or equal to the required trust value, that is, the risk value is less than or equals to the predefined risk value (threshold), then the job will be processed, otherwise it will be declined. In other words if a node (X) wants a job to be processed by another node (Y), then node (Y) will first check to see if it has had any previous experience with node (X) and if so, then, is that trust value (A) as given in equation (4.1) enough to do the job: (A) is greater than or equal to (T). If so, the associated risk is less than the risk threshold, then node (Y) will do the job for node (X), otherwise node (Y) will check to see if there are any recommendations about node (X) from the surrounding nodes, and if so, is that trust value (B) as given in equation (4.2) enough: (B) is greater than or equal to (T). If so, the associated risk is less than the risk threshold, then node (Y) will do the job for node (X), otherwise node (Y) will check to see if the combined trust value (C) of (A) and (B), as given in equation (4.3), is enough: (C) is greater than or equal to (T). If so, the associated risk is less than the risk threshold, then node (Y) will do the job for node (X), otherwise the job will be declined unless the node is ready to take the risk associated with that job.

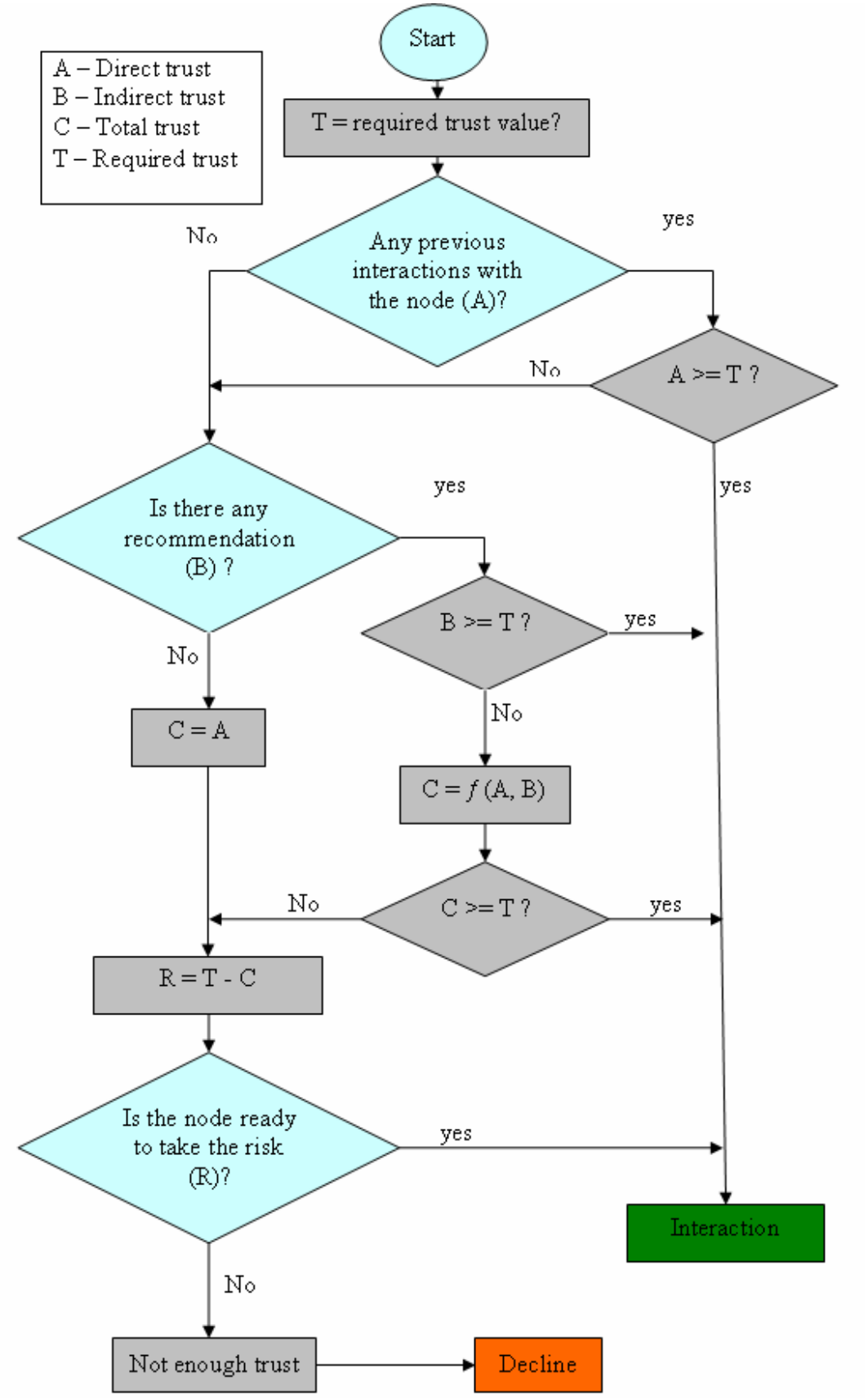

Figure 4.3. Algorithm for calculating trust in WSN

From the above illustration and by referring to the actual algorithm given in Figure 4.3, the trust value $T_y(x)$, of node (Y) on node (X) regarding a specific task can take any of the following values (A, B, C).

$$T_y(x) = \begin{cases} \text{A, if the trust from previous interactions is enough} \\ \text{B, if the trust from recommendations is enough} \\ \text{C, if the combined trust value is enough} \end{cases}$$

There are different ways for calculating each trust value. Here, the traditional approaches presented in [35, 130] are implemented; that is, trust value (A), shown in equation (4.1), involves the assignment of weights (utility/importance factor) to the events that were monitored and quantified. All nodes dynamically assign these weights based upon their own criteria and circumstances. These weights have a continuous range from (0 to +1), representing the significance of a particular event from unimportant to most important. The trust values for all the events from a node can then be combined to determine the aggregate trust level for another node. The total number of trust categories (n) is dependent on the protocol and scenario to which the trust model is being applied.

$$A = \sum_{i=1}^{n} T_{y_i}(x) \tag{4.1}$$

where:

$T_{y_i}(x)$ – trust value of the i[th] trust category; this value is assigned by nodes using their own criteria and can be different for different nodes.

n – number of trust categories.

Trust value (B), given in equation (4.2), represents the average trust reported from all the surrounding nodes that have had previous experience with the node. There are some implications in the timing of interactions or reporting and these will be addressed in future work.

$$B = \frac{\sum_{y=1}^{m} T_y(x)}{m} \tag{4.2}$$

where:

$T_y(x)$ – trust value of node Y on Node X and is calculated separately for each node in a way similar to (A) in equation (1).

m – number of the surrounding nodes.

Total trust value (C), given in equation (4.3), is a function of direct trust value (A) and indirect trust value (B). Here, it is calculated by assigning different weights for (A) and (B); it represents a data fusion, and methods of how to combine these two values together will be discussed later.

$$C = f(A, B) \tag{4.3}$$

Calculating the risk (R) given in equation (4.4) is similar to calculating trust value (A) in equation (4.1), but instead of assigning situational trust or rating to the event, the node assigns the risk associated with the event.

$$R = \sum_{k=1}^{n} R_{y_k}(x) \tag{4.4}$$

where:

$R_{y_k}(x)$ — the risk value of k[th] trust category the node is ready to take to perform the task. This value is assigned by nodes too, using their own criteria and can be different for different nodes.

n — number of trust categories.

Risk value (R) can also be calculated as the difference between the required trust to perform the task (T) and the available trust from previous experience (A) and/or recommendations (B), as shown in equation (4.5):

$$R = T - C \tag{4.5}$$

where:

T — trust value required to do the job.

C — total trust value available. (C), can be in the range from (0 to 1); (0), in case of a new node with no previous interactions with any other node in the network, and (1); complete trust, in case of very reliable nodes over a long time period.

It is assumed that nodes are capable of calculating (A), (B) and (R) using their own criteria, be this as presented in [35] using weight and situational trust or as presented in [130] using weight and rating or any other criteria specific to a node. The challenge here, as discussed before, is how to calculate the combined trust value (C) given in equation (4.3), as it represents a data fusion. At this stage, it is calculated using the traditional approach of combining two weighted trust values from two different sources. Trust value (A) is assigned a weight (W_A), and trust value (B) is assigned a weight (W_B). Based on these weights, the combined trust (C) is calculated as shown in equation (4.6):

$$C = A * W_A + B * W_B \tag{4.6}$$

These weights, (W_A) and (W_B), can be assigned using different approaches. Initially they were assigned based on the nodes' own criteria; that is, some nodes might give more weight to direct trust, others might give more weight to recent indirect trust and so on. In the following section a new statistical approach is presented to weight the direct and indirect trust.

4.4. Combined Trust

Combining direct trust and indirect trust to obtain the total trust of one node on the others was and still is the issue for many researchers. Most of the models, which use the weighting approach, assign different weights to each trust type without describing the methodology behind their assignments. Here, a new methodology

using the Beta distribution is introduced to weight different trust components – direct trust value (A) and indirect trust value (B) in equation (4.6) – and eventually to calculate the total trust. The reason behind using the Beta distribution is that, it is being used widely in risk and decision analysis, due to its flexibility, and also it can be estimated very easily [55, 61].

The density function for a beta random variable X on domain [0,1] is given by equation (4.7):

$$f(\alpha,\beta)=\frac{\Gamma(\alpha+\beta)}{\Gamma(\alpha)\Gamma(\beta)}x^{\alpha-1}(1-x)^{\beta-1} \tag{4.7}$$

p is the probability that the event occurs

$$p \sim Beta\ (\alpha,\beta) \tag{4.8}$$

Substituting equation (4.8) in equation (4.7), will result in the following density function given in (4.9):

$$f(p)=\frac{\Gamma(\alpha+\beta)}{\Gamma(\alpha)\Gamma(\beta)}p^{\alpha-1}(1-p)^{\beta-1} \tag{4.9}$$

The expected value μ is given in equation (4.10):

$$E(p)=\frac{\alpha}{\alpha+\beta} \tag{4.10}$$

and the variance σ^2 is given in equation (4.11):

$$V(p) = \frac{(\alpha * \beta)}{(\alpha + \beta + 1) * (\alpha + \beta)^2} \tag{4.11}$$

It is assumed that trust value (A) in equation (4.6) provides the prior estimate for *p*, as given in equation (4.12):

$$E_A(p) = \frac{\alpha_A}{\alpha_A + \beta_A} = \hat{P}_A \tag{4.12}$$

and the variance value, as given in equation (4.13):

$$V_A(p) = \sigma_A^2 \tag{4.13}$$

From the above illustration in equations (4.12) and (4.13), α_A and β_A can be represented as in equations (4.14) and (4.15) respectively:

$$\alpha_A = \hat{P}_A \left[\frac{\hat{P}_A(1-\hat{P}_A)}{\sigma_A^2} - 1 \right] \tag{4.14}$$

$$\beta_A = \frac{\alpha_A * (1-\hat{P}_A)}{\hat{P}_A} \tag{4.15}$$

Trust value (B) in equation (4.6) provides the estimate $\hat{p}_B$ of p, as given in equation (4.16):

$$E_B(p) = \frac{\alpha_B}{\alpha_B + \beta_B} = \hat{P}_B \tag{4.16}$$

and the variance value as given in equation (4.17):

$$V_B(P) = \sigma_B^2 \tag{4.17}$$

From equations (4.16) and (4.17), α_B and β_B can be represented as in equations (4.18) and (4.19) respectively:

$$\alpha_B = \hat{P}_B \left[\frac{\hat{P}_B(1-\hat{P}_B)}{\sigma_B^2} - 1 \right] \tag{4.18}$$

$$\beta_B = \frac{\alpha_B * (1-\hat{P}_B)}{\hat{P}_B} \tag{4.19}$$

Assuming that trust value (A) in equation (4.6) represents the prior, then according to Bayes' theorem discussed in appendix A,

$$P(p \mid \hat{P}_B) \propto P(\hat{P}_B \mid p) * P(p) \tag{4.20}$$

where, $P(p)$ represents the prior and equals to $Beta\ (\alpha_A,\beta_A)$, and $P(\hat{P}_B \mid p)$ is the likelihood, which needs to be modelled.

From the above discussion, equation (4.20) can be rewritten as shown in equation (4.21):

$$\begin{aligned} P(p \mid \hat{P}_B) &\propto p^{\alpha_B - 1}(1-p)^{\beta_B - 1}\, p^{\alpha_A - 1}(1-p)^{\beta_A - 1} \\ &\propto p^{(\alpha_A + \alpha_B - 1 - 1)}(1-p)^{(\beta_A + \beta_B)} \\ &\sim Beta(\alpha_A + \alpha_B - 1 \ \ , \ \ \beta_A + \beta_B - 1) \end{aligned} \tag{4.21}$$

Substituting equation (4.21) in equation (4.10), the following expected value will result, as shown in equation (4.22):

$$E(p \mid \hat{P}_B) = \frac{\alpha_A + \alpha_B - 1}{\alpha_A + \alpha_B + \beta_A + \beta_B - 2} = \frac{\alpha_A + \alpha_B - 1}{K} \tag{4.22}$$

Let *K* in equation (4.22) be represented as given in equation (4.23):

$$K = \alpha_A + \alpha_B + \beta_A + \beta_B - 2 \tag{4.23}$$

So, equation (4.22) can be written as given in equation (4.24):

$$E(p \mid \hat{P}_B) = \frac{\alpha_A}{\alpha_A + \beta_A} * \frac{\alpha_A + \beta_A}{K} + \frac{\alpha_B}{\alpha_B + \beta_B} * \frac{(\alpha_B + \beta_B)(\alpha_B - 1)}{\alpha_B * K} \quad (4.24)$$

$E(p \mid \hat{P}_B)$ in equation (4.24) simply represents the combined trust value as given in equation (4.6), and can be written as shown below in equation (4.25):

$$E(P \mid \hat{P}_B) = \hat{P}_A * W_A + \hat{P}_B * W_B \quad (4.25)$$

and, as can be seen from equations (4.24) and (4.25), the weights for direct trust W_A and indirect trust W_B are represented in equations (4.26) and (4.27) respectively:

$$W_A = \frac{\alpha_A + \beta_A}{K} \quad (4.26)$$

$$W_B = \frac{(\alpha_B + \beta_B)(\alpha_B - 1)}{\alpha_B * K} \quad (4.27)$$

If the trust values (A) and (B) are known, then it is very easy to calculate α_A, β_A, α_B and β_B, as shown in equations (4.14), (4.15), (4.18) and (4.19), and eventually W_A and W_B will be calculated using equations (4.26) and (4.27) respectively.

As discussed before, the total trust value is a combination of direct trust and indirect trust values. One way of combining these trust values using the

probability theory has been presented here, and other methodologies on how to calculate the total trust will be discussed in the following chapters.

4.5. Simulation Results

This section presents two example simulations conducted on two different networks using MATLAB. The first network consists of three nodes for simplicity, and to be able to verify the algorithm and show the results in tables as illustrated below. The second simulation is for a network of fifteen nodes to further verify the algorithm when the number of nodes is high, and to show the results in a graph, as described below.

4.5.1. Three Nodes Network Simulation

Figure 4.4 below depicts a network topology of three nodes with their associated trust values. These trust values are asymmetric, which means that the trust value from node (1) to node (2) is different from the trust value from node (2) to node (1). The complete direct trust values between nodes are shown in Table 4.2. The required trust values between nodes to perform the task are also given in Table 4.1. Table 4.1 and Table 4.2 reflect the trust values (T) and (A) respectively in the algorithm shown in Figure 4.1. The indirect trust values (B) from the surrounding nodes are given in Table 4.3, the combined trust values (C) are shown in Table 4.4 and finally the risk values (R) are presented in Table 4.5, based on the above results.

As can be seen from the tables below, the diagonal values in Tables 4.1 and Table 4.5 are always zeros, which reflects the required trust value and the risk value associated with the node to itself; that is, there is no required trust value or risk associated with a node when it is doing a job for itself. The same is valid for Table 4.2, Table 4.3 and Table 4.4, which have the diagonal values set to ones, which means the node blindly trusts itself; all the values in the diagonals in all tables are from the node to itself and they do not participate in the calculations. In each table, the first row represents the trust values of node (1) on the other nodes connected to it in the network, the second row represents the trust values of node (2) on the other nodes connected to it in the network and so on. Table 4.5, for example, shows that, node (1) needs to take the risk values of (0) and (0.2319) to be able to finish the task with node (2) and node (3) respectively, node (2) needs to take the risk values of (0.0741) and (0) to be able to finish the task with node (1) and node (3) respectively, and node (3) needs to take the risk values of (0) and (0) – no risk is associated – to perform the task with node (2) and node (3) respectively. The risk value (R) of (0) in the diagonal means the risk from the node to itself as mentioned before, and the other (0) values, not in the diagonal, mean the actual trust is greater than or equal to the required trust and there is no need for any risk to be taken.

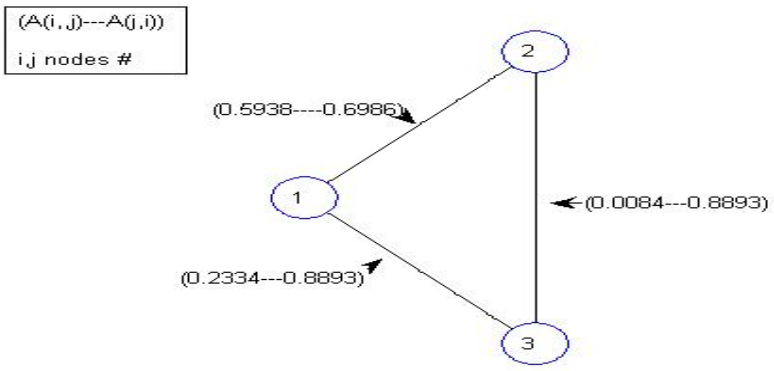

Figure 4.4. Network graph of three nodes and the associated trust between the nodes

Table 4.1. Required trust values

$$T = \begin{bmatrix} 0 & 0.4546 & 0.7148 \\ 0.7688 & 0 & 0.5383 \\ 0.5846 & 0.2413 & 0 \end{bmatrix}$$

Table 4.2. Trust values from previous experience

$$A = \begin{bmatrix} 1 & 0.5938 & 0.2334 \\ 0.6986 & 1 & 0.0084 \\ 0.8893 & 0.3167 & 1 \end{bmatrix}$$

Table 4.3. Trust values from recommendations

$$B = \begin{bmatrix} 1 & 0 & 0.5938 \\ 0.0084 & 1 & 0.6986 \\ 0 & 0 & 1 \end{bmatrix}$$

Table 4.4. Trust values from combined A and B

$$C = \begin{bmatrix} 1 & 0 & 0.4829 \\ 0.6947 & 1 & 0.5383 \\ 0 & 0 & 1 \end{bmatrix}$$

Table 4.5. Risk values associated with nodes

$$R = \begin{bmatrix} 0 & 0 & 0.2319 \\ 0.0741 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$$

In summary, the above illustrated figure and tables in this section show the trust values between nodes and the risk associated with each node on the others connected to it in a network.

4.5.2. Fifteen Nodes Network Simulation

To further verify the algorithm and see the effect on the trust values when many nodes exist in the surrounding area, the network should consist of a large number of nodes. Here, a simulated network consisting of fifteen nodes is presented as illustrated in Figure 4.5. Results are presented in a different way from the previous simulation, that is, trust values between nodes are not shown on the graph, for simplicity, and tables showing the results are also not shown, due to the large number of nodes. Instead a graph is presented in Figure 4.6. It is also assumed that the required trust value to perform the task (T) is equal to (0.7) for all nodes. The graph presented in Figure 4.6 shows the risk between every node and the other (14) nodes in the network. If there is a direct connection between any two nodes, then there will be a certain risk value, otherwise, the risk value will be equal to

zero. Each graph in Figure 4.6 represents one node in the network; the first graph is for node (1), the second graph is for node (2), etc. The results here clearly show the risk associated between nodes, due to the large number of nodes.

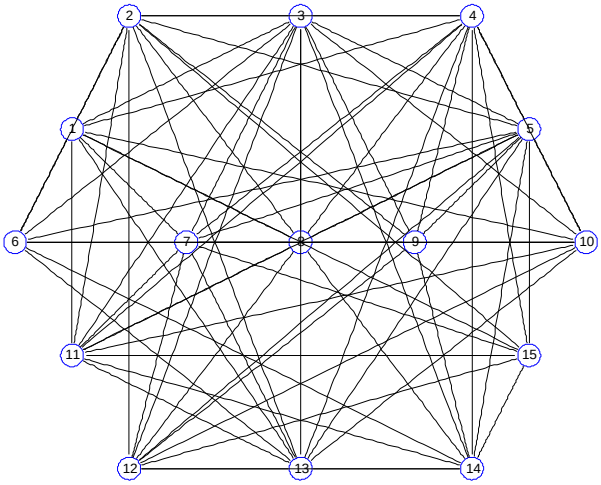

Figure 4.5. Network graph of fifteen nodes and the associated trust between the nodes

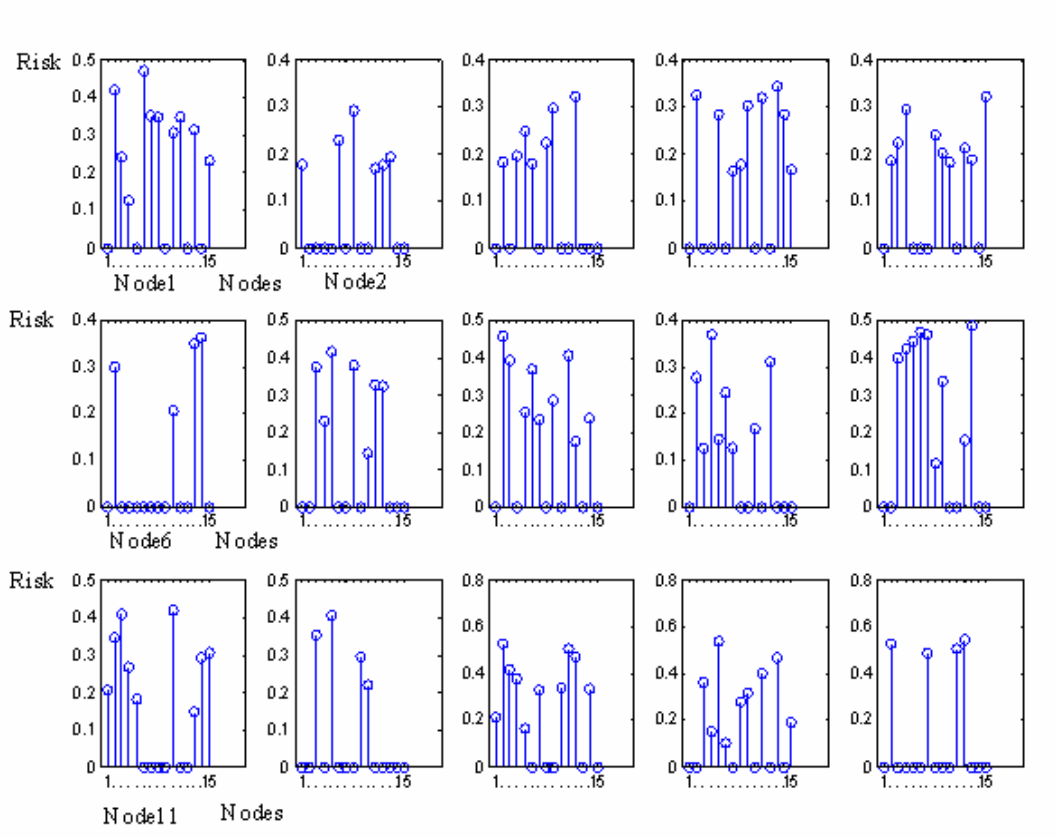

Figure 4.6. Risk between each node and the other 14 nodes.

4.6. Conclusions

It has been stated that modelling trust requires a thorough understanding of the dynamic aspects of trust and the factors affecting trust. This chapter has introduced those two topics and briefly discussed the main factors of trust - direct trust, indirect trust, reputation and risk- with more attention given to the direct and indirect trusts as the most important factors, which can produce the other factors. Dynamic aspects of trust – trust formation, trust updating and trust revocation – are also presented, with great attention being paid to the trust formation process as the most important aspect. A new generic algorithm for calculating trust between

nodes and the risk associated with each node, based on the nodes' QoS characteristics, which have been categorised by nodes themselves into different categories based on their own criteria and the scenario in which they find themselves is also presented. The algorithm presented here represents a new framework for establishing trust in WSNs and calculating the risk required by the node to take in case the trust value is not enough to perform the task. At this stage, the framework assumes that direct trust values, indirect trust values and the required trust are given or already calculated by the node, and still uses the traditional weighting approach to calculate the combined trust, with the introduction of a new approach to weight the direct and indirect trust using the realm of statistics. This will be developed further to adopt new techniques unique to WSNs. Preliminary simulation results were also presented, which simply show the trust relationship between nodes and the risk associated with them. The results have been presented in tables and in graphic format for easy observation and interpretation, showing that, the higher the trust between nodes, the lower the risk between them, and vice versa.

5. Modelling Trust in Wireless Sensor Networks

This chapter introduces a new Bayesian probabilistic approach for modelling trust and reputation in WSNs. It represents a breakthrough in the way trust is modelled in WSNs. It introduces the continuous sensed data as a core component when deciding to trust nodes in WSNs, as all the previous studies on trust were based on binary events. It also presents a new Gaussian trust model and a reputation system for wireless sensor networks (GTRSSN) to address the uncertainty characteristic of trust-modelling in WSNs.

5.1. Introduction

Wireless Sensor Networks closely resemble a human behaviour model, in which a number of nodes that have just met are able to communicate with each other based on mutual trust levels developed over a period of time. WSNs are characterised by their performance of an additional function to the traditional functions of an ad-hoc network, which is monitoring events and reporting data and, as such, the sensed data represent the core component of trust-modelling in this research.

The trust-modelling problem in wireless networks is characterised by uncertainty. It is a decision problem under uncertainty and the only coherent way to deal with

uncertainty is through probability. There are several frameworks for reasoning under uncertainty, but it is well accepted that the probabilistic paradigm is the theoretically sound framework for solving a decision problem involving uncertainty. Some of the trust models introduced for sensor networks employ probabilistic solutions mixed with ad-hoc approaches. None of them produces a full probabilistic answer to the problem. Each node's reliability is an unknown quantity. The ensuing decision problems concern is which nodes are to be trusted. It is these decision problems; regarding when to terminate nodes, that motivate research in trust models.

We look at applying trust evaluation to WSNs, providing continuous data in the form of a new reputation system we call GTRSSN: *Gaussian Trust and Reputation System for Sensor Networks*. It has been argued that previous studies on WSNs focused on the trust associated with the routing and the successful performance of a sensor node in some predetermined task. This resulted in looking at binary events. The trustworthiness and reliability of the nodes of a WSN, when the sensed data are continuous, has not been addressed. Our main contribution is therefore the introduction of a statistical approach; a theoretically sound Bayesian probabilistic approach for modelling trust in WSNs in the case of continuous sensor data; that is, we derive a Bayesian probabilistic reputation system and trust model for WSNs, as presented in our work in [117] and [118].

5.2. Node Misbehaviour Classification

The main idea behind reputation and trust-based systems is to discover and exclude misbehaving nodes and to minimise the damage caused by inside attackers. Node misbehaviour can be classified in two categories: communication misbehaviour and data misinforming. Most of the researchers classify node misbehaviour in the same way they model trust: from the communication point of view. However, as discussed so far, WSNs are deployed to sense events and report data, so the node misbehaviour diagram presented in [131] is extended by introducing a new branch addressing sensor data misbehaviour; misinforming, as a second category of nodes' misbehaviour classification in WSNs, as illustrated below in Figure 5.1, to reflect the way trust is being modelled here.

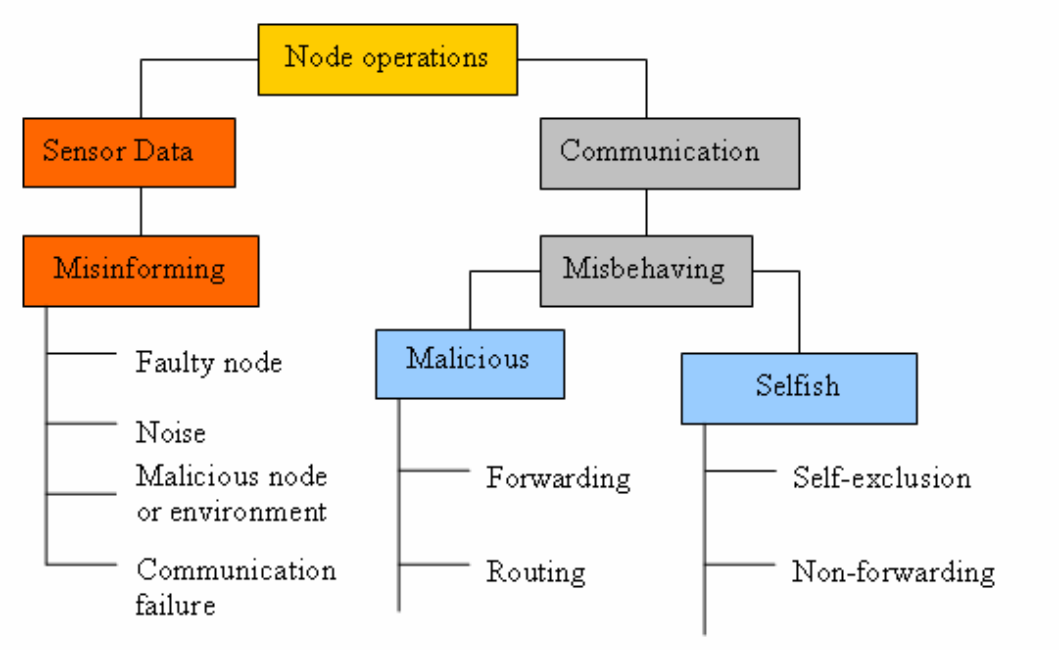

Figure 5.1. Node misbehaviour classification

As can be seen from the diagram in Figure 5.1, the new branch dealing with sensor data includes the misinforming behaviour of a sensor node. This can be caused due to a faulty node, a node that is damaged or has expired, or due to a noise, as sensor data are not without noise, a malicious node or environment. The node might have been captured or the environment is malfunctioning or there might have been a communication failure, or there has been interference or the communication between nodes is cut off for some reason. The communication misbehaviour classification is due to the node being malicious, an intruder attacking and damaging the network, or the node is selfish, trying to save resources for later usage. Further detailed information regarding the node misbehaviour communication branch is provided in [56].

5.3. Modelling Trust

Initially, the primary focus of the research on trust in WSNs was on whether a node will detect appropriately, will or will not report the detected event(s), and will route information. The uncertainty in these actions warranted the development of reputation systems and corresponding trust models. Modelling trust in general, as introduced very briefly in Chapter 4, is the process of representing the trustworthiness of one node in the opinion of another node, that is, how much one node trusts every other node in the surrounding area, and it has been the focus of many researchers from different domains, as stated in Chapter 2, which has surveyed most of the existing trust models in different disciplines. In other words, trust-modelling is simply the mathematical representation of a node's

opinion of another node in a network. Figure 5.2 below shows the two main sources for trust formation in WSNs: the observation of the behaviour of the surrounding nodes, direct trust and the recommendation from other nodes, indirect trust.

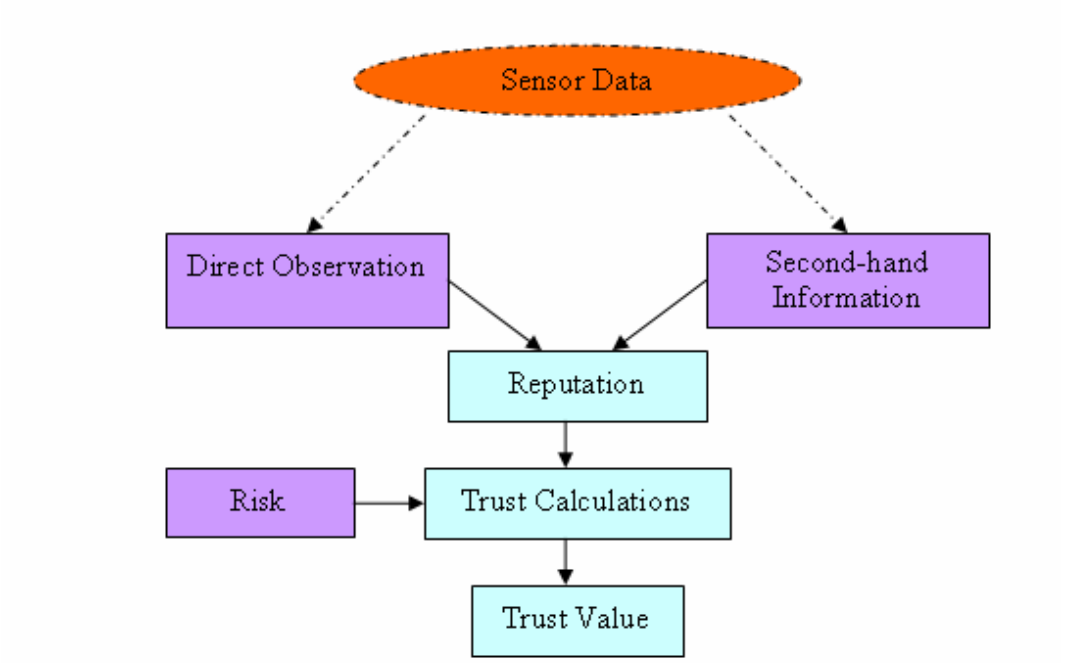

Figure 5.2. Trust computational model for WSN

5.3.1. Direct Observations

A node will observe a neighbouring node's behaviour and build a reputation for that node based on the observed data. The neighbouring node's transactions data are direct observations referred to as *first-hand information*. By their nature, the considered events are binary, and the mathematical trust models developed for WSNs are for binary transactions. We argue that the problem of assessing a reputation based on observed data is a statistical problem. Some trust models make use of this observation and introduce a probabilistic modelling. For

example, the reputation-based framework for high integrity sensor networks (RFSN) trust model presented in [55] by Ganeriwal and Srivastava uses a Bayesian updating scheme known as the *Beta Reputation System* for assessing and updating the nodes' reputations. The Beta reputation system was introduced by Josang and Ismail [61], who used the Beta distribution to model binary statistical events.

5.3.2. Second-hand Information

A second source of information in trust-modelling is information provided by other nodes. This source of information is referred to as *second-hand information*. It consists of information gathered by nodes as first-hand information and converted into an assessment. Due to the limitations of a WSN, the second-hand information is summarised before being shared. For example, the RFSN in [55] uses the Beta probability model and share the values of the parameters of the probability distributions as second-hand information. This shared information is not hard data for the node receiving the information. A proper way is required to incorporate this new information into the trust model by combining it with observed data. While some trust models build reputations purely on the basis of observations, most of them attempt to use the second-hand information. The reasons are obvious from a statistical point of view. But the interest is also motivated by the desire to speed up the assessment of reputations. Due to the asymmetric transactions in a network, some nodes may not have enough observations about all neighbouring nodes.

Using shared information improves the efficiency and speed of reputation assessment, however, combining the two sources of information is handled differently by different trust models. For example, the RFSN uses the Dempster-Shafer Belief Theory. The Belief Theory is a framework for reasoning under uncertainty that differs from the probabilistic framework. The discussion of the fundamental differences between these two theories is beyond the scope of this research. Although the two approaches can be joined in some cases, they differ in their philosophies on how to treat uncertainty. The RFSN uses both of them in the same problem. We propose a probabilistic treatment of trust, and apply it to the case of continuous sensor data.

Although a reputation system is designed to reduce the harmful effect of an unreliable or malicious node, such a system can be used by a malicious node to harm the network. Systems such as the RFSN in [55] and the distributed reputation-based beacon trust system (DRBTS) in [56] are confronted with the issue of what second-hand information is allowed to be shared. For example, some prohibit negative second-hand information to be shared, in order to reduce the risk of a negative campaign by malicious nodes. Our proposed model incorporates all of the second-hand information. To resolve the issue of the validity of the information source, the information is modulated using the reputation of the source. This probabilistic approach rigorously answers the question of how to combine the two types of data in the exercise of assessing reputations in a sensor network. It is based on work undertaken in modelling *Expert Opinion* [132-134]. Expert opinions are used whenever few data are observed. The expert opinion is second-hand information that is merged with hard

data according to the laws of probability. Information provided by knowledgeable sources is known as "expert opinion" in the statistical literature. These opinions are modulated by existing knowledge about the experts themselves, to provide a calibrated answer.

5.4. The Beta Reputation System

The Beta Reputation System was proposed by Josang and Ismail in [61] to derive reputation ratings in the context of e-commerce. It was presented as a flexible system with foundations in the theory of statistics, and is based on the Beta probability density function. The Beta distribution can be used in the probability modelling of binary events. Let θ be a random variable representing a binary event, $\theta = 0; 1$, and p the probability that the event occurs, $\theta = 1$. Then the Beta-family of probability distributions, a continuous family of functions indexed by two parameters α and β, can be used to represent the probability density distribution of p, noted as $Beta(\alpha, \beta)$, as shown in equation (5.1):

$$f(p \mid \alpha, \beta) = \frac{\Gamma(\alpha + \beta)}{\Gamma(\alpha)\Gamma(\beta)} p^{\alpha-1}(1-p)^{\beta-1} \tag{5.1}$$

where $0 \leq p \leq 1$; $\alpha > 0$; $\beta > 0$. If the number of outcomes where there are r occurrences and s non-occurrences of the event is observed, then using a Bayesian probabilistic argument, the probability density function of p can be expressed as a Beta distribution, where $\alpha = r + 1$ and $\beta = s + 1$. This probabilistic mechanism is applied to model the reputation of an entity using events of completion of a task

by the assessed entity. The reputation system counts the number r of successful transactions, and the number s of failed transactions, and applies the Beta probability model. This provides for an easily updatable system, since it is easy to update both r and s in the model. Each new transaction results either in r or s being augmented by 1.

For the RFSN [55] Ganeriwal and Srivastava used the work of Josang and Ismail presented in [61], in their trust model for WSNs. For each node n_j, a reputation R_{ij} can be carried by a neighbouring node n_i. The reputation is embodied in the Beta model and carried by two parameters α_{ij} and β_{ij}. α_{ij} represents the number of successful transactions node n_i had with n_j, and β_{ij} represents the number of unsuccessful transactions. The reputation of node n_j maintained by node n_i is $R_{ij} = Beta(\alpha_{ij} + 1, \beta_{ij} + 1)$. The trust is defined as the expected value of the reputation, as shown in equation (5.2):

$$T_{ij} = E(R_{ij}) = E(Beta(\alpha_{ij} + 1, \beta_{ij} + 1)) = \frac{\alpha_{ij} + 1}{\alpha_{ij} + \beta_{ij} + 2} \tag{5.2}$$

Second-hand information is presented to node n_i by another neighbouring node n_k. Node n_i receives the reputation of node n_j by node n_k, R_{kj}, in the form of the two parameters α_{kj} and β_{kj}. Using this new information, node n_i combines it with its current assessment R_{ij} to obtain a new reputation R_{ij}^{new}, as given in equation (5.3):

$$R_{ij}^{new} = Beta(\alpha_{ij}^{new}, \beta_{ij}^{new}) \tag{5.3}$$

where

$$\alpha_{ij}^{new} = \alpha_{ij} + \frac{2\alpha_{ik}\alpha_{kj}}{(\beta_{ik}+2)(\alpha_{kj}+\beta_{kj}+2)(2\alpha_{ik})} \tag{5.4}$$

$$\beta_{ij}^{new} = \beta_{ij} + \frac{2\alpha_{ik}\beta_{kj}}{(\beta_{ik}+2)(\alpha_{kj}+\beta_{kj}+2)(2\alpha_{ik})} \tag{5.5}$$

Note that node n_i uses its reputation of node n_k in the combination process. The authors of the RFSN defined how their trust model can be used in practice. They brought out some important points concerning the way information is to be used to avoid two major problems: (i) data incest, and (ii) a game theoretic set-up. Some researchers [135, 136] have looked into the game theory aspect, which is no doubt inherent in a problem with malicious nodes in the network. However, a game theory solution might be difficult to obtain, in view of the large number of nodes. The RFSN forces the WSNs protocols into an exchange of information that limits any game aspect. The effectiveness of the notion of reputation and trust resides in the assumption that the majority of nodes in any neighbourhood is trustworthy, therefore creating a resilience of the system. Trust assessment is used to flush out the bad nodes. In combining information, the authors of the RFSN followed the approach of [61], by mapping the problem into a Dempster-Shafer belief theory model [137], solving it using the concept of belief discounting, and conducting a reverse mapping from belief theory to probability. In our work we find it unnecessary to use the Belief theory. Rather, probability theory, and the ensuing work on expert opinion provide a way to combine the two types of information.

5.5. Expert Opinion Theory

The use of expert opinion has received much attention in the statistical literature. It allows for the formal incorporation of informed knowledge into a statistical analysis. Expert opinion, or informed judgement, is often available in the form of vendor information, engineering knowledge, manufacturer's knowledge, or simply an opinion formed over time. It is often a subjective opinion based on knowledge. Its main departure from hard data is that it cannot be claimed as objectively observed data. Nevertheless, it is often valuable information that has been formed over the course of time. In our case, reputation is offered to neighbouring nodes as an opinion. The node making the assessment has not observed that reputation, and therefore treats it as an opinion. Early work to formalise ad-hoc procedures for the use of expert opinion includes [132, 138]. Morris [139] recognised the importance of treating the expert opinion as data, stating the general principle on which subsequent work was based. The topic was further enlarged by the Bayesian statistical community to the problem of reconciliation prior information from different sources [140-143], a topic that dated back to Winkler [144]. Lindley [145] highlighted the theory in the statistical arena, with others following with work on reliability [146-148], on maintenance optimization [149-151] and on nuclear safety [152].

The probabilistic approach adopted in the elicitation and use of expert opinion considers the opinion given by the expert as data and treats it according to the laws of probability. If θ is a random variable, and μ represents an opinion from an

expert about θ, then $P(\theta|\mu)$ obtains, using Bayes' theorem as discussed in appendix A, the following formula, as shown in equation (5.6):

$$P(\theta \mid \mu) = \frac{P(\mu \mid \theta)P(\theta)}{P(\mu)} \tag{5.6}$$

$$P(\mu) = \int_{\theta} P(\mu \mid \theta)P(\theta)d\theta \tag{5.7}$$

- $P(\mu \mid \theta)$ is the likelihood function, and represents the analyst model of the expert's input
- $P(\theta)$ is the distribution that represents any prior knowledge the analyst may have about the quantity of interest
- $P(\mu)$ is the normalising constant

Bayes' theorem inverses the probability, so that the evidence μ highlights the value of θ that is most likely. The likelihood function $L(\theta) = P(\mu \mid \theta)$ refers to where the expert opinion is modelled. As an example, consider the reliability scenario of [146]. In it, an expert provides reliability estimates for a device or machine. The work was undertaken in the context of maintenance optimisation.

Figure 5.3 shows the expert's input along the unknown reliability curve that the analyst wants to estimate. Each assessment by the expert is about the reliability as a time t_i, in the form of a value $0 < r_i < 1$. If the expert was perfect, and assuming that the reliability at time t_i is $e^{-\lambda t_i^{\beta}}$, then

$$r_i = e^{-\lambda t_i^{\beta}} \tag{5.8}$$

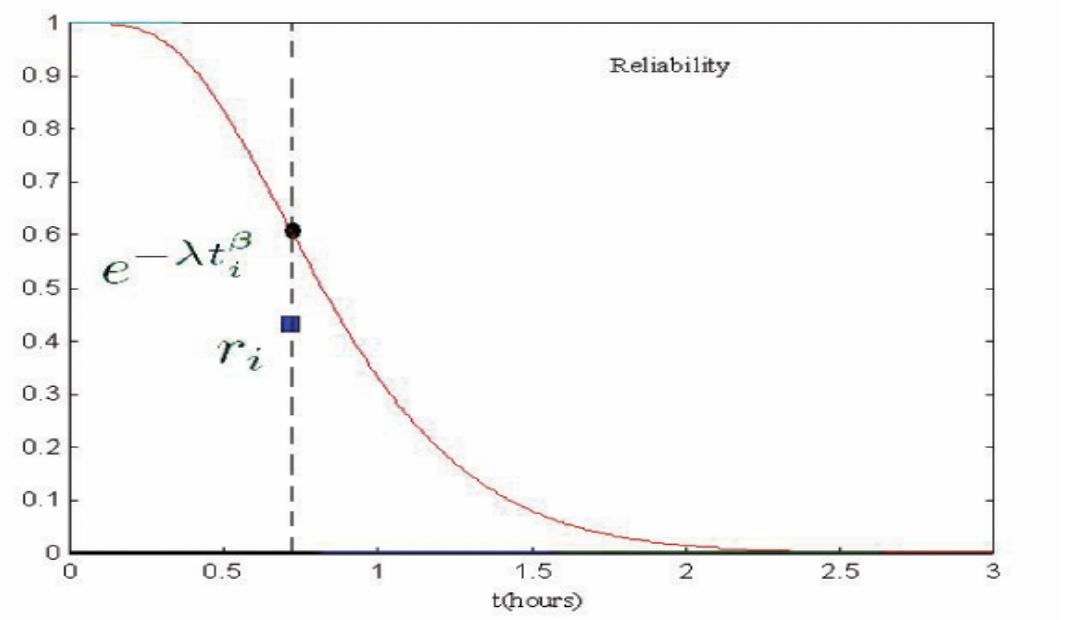

Figure 5.3. Expert opinion r_i for reliability at time t_i

However, it will not necessarily be the case, and a probability distribution is needed to model the input. That probability distribution is the likelihood function, in this case

$$L(\lambda, \beta) = P(r_i \mid \lambda, \beta) \tag{5.9}$$

The authors of [146] modelled it using a Beta distribution, such that

$$E(r_i \mid \lambda, \beta) = \alpha_i + \sigma_i e^{-\lambda t_i^{\beta}} \tag{5.10}$$

where σ_i and α_i are inflation and bias, respectively, carried by the expert about the reliability at time t_i. These two values reflect the analyst's modulation of the expert opinion. To model several correlated inputs, a Dirichlet model is used.

Once the likelihood function is built, then it can be used to combine the actual expert opinion with any existing knowledge about the random variable of interest. The analyst may not only have prior knowledge but also some observed data y about a random variable of interest, θ. Bayes' theorem is applied to combine the three sources of information, as shown in equation (5.11):

$$P(\theta \mid y, \mu) = \frac{P(y \mid \theta, \mu) P(\mu \mid \theta) P(\theta)}{P(y, \mu)} \tag{5.11}$$

One often writes, $P(\theta \mid y, \mu) \propto P(y \mid \theta, \mu)\ P(\mu \mid \theta)\ P(\theta)$, the denominator being a normalising constant that does not affect the combination occurring in the numerator. This seemingly simple operation can effectively combine many sources of information. We use it to model the reputation of a node when opinions about that node are provided by other nodes.

5.6. GTRSSN: Gaussian Trust and Reputation System for Wireless Sensor Networks

Taking into consideration the above discussion, let us assume that the wireless sensor network shown in Figure 5.4 consists of N nodes $(n_1, n_2, ..., n_N)$, and the corresponding matrix $\Gamma = [\Gamma_{i,j}]$ is given as follows:

$$\Gamma = [\Gamma_{i,j}] = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix}$$

If node n_i is connected to node n_j, then $\Gamma_{i,j} = \Gamma_{j,i} = 1$, otherwise it is equal to (0). Let (X) be a field variable monitored in the environment where the WSN is deployed. This variable, might represent temperature, chemical component or atmospheric value, is detected and estimated by the sensor nodes and it is assumed to be of a continuous nature. The nodes are synchronised and can report at discrete times $t = 0, 1, 2, …., k$.

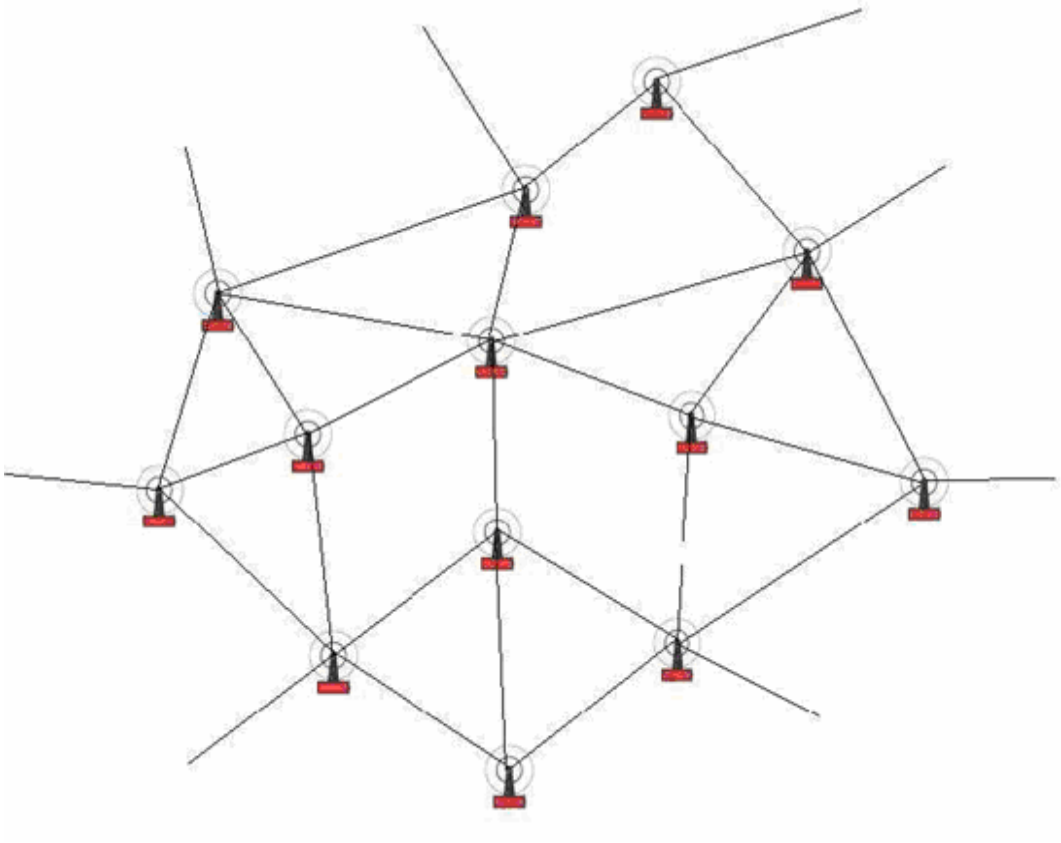

Figure 5.4. Network of wireless sensor nodes

The random variable $(X_{n_i} = X_i)$ is the sensed value reported by node n_i, i = 1, ..., N. $x_i(t)$ is the realisation of that random variable at time t. Each node n_i, i = 1, ….. , N has a time series ($x_i(t)$). These time series are most likely different, as nodes are requested to provide readings at different times, depending on the sources of the requests. It could also be that the nodes provide such readings when triggered by particular events. We assume that each time a node provides a reading, its one-hop neighbours that route its report see that report, and can evaluate the reported value. For example, if node n_j reports $x_j(t)$ at some time t, then node n_i, such that $\Gamma_{i,j}$ = 1, obtains a copy of that report for routing purposes, and has its own assessment $x_i(t)$ of the sensed variable. Let $y_{i,j}(t) = x_j(t)$-$x_i(t)$. From the node n_i

perspective, $X_i(t)$ is known, and $Y_{i,j}(t) = X_j(t) - X_i(t)$ represents the error that node n_j commits in reporting the sensed field value $X_j(t)$ at time t. $Y_{i,j}(t)$ is a random variable modelled as a Normal (Gaussian), as shown in equation (5.12):

$$Y_{i,j}(t) \sim N(\theta_{i,j}, \tau^2) \tag{5.12}$$

where τ is assumed to be known (error variance), and it is the same for all nodes. If we let $\overline{y}_{i,j}$ be the mean of the observed error, as observed by n_i about n_j reporting, as in equation (5.13):

$$\overline{y}_{i,j} = \sum_{t=1}^{k} y_{i,j}(t) / k \tag{5.13}$$

then

$$(\theta_{i,j} \mid y_{i,j}) \sim N(\overline{y}_{i,j}, \tau^2 / k) \tag{5.14}$$

where $y_{i,j} = \{y_{i,j}(t)$, for all t values at which a report is issued by n_j and routed through $n_i\}$. This is a well-known straightforward Bayesian updating where a diffuse prior is used.

We let $\mu_{i,j} = \overline{y}_{i,j}$ and $\sigma_{i,j}^2 = \tau^2 / k$. Recall that k is node-dependent. It is the number of reports issued by node n_j and routed through n_i, and differs from node to node. We define the reputation as the probability density function, as in equation (5.15):

$$R_{i,j} = N(\mu_{i,j}, \sigma_{i,j}^2) \tag{5.15}$$

where $\mu_{i,j} = \overline{y}_{i,j}$ and $\sigma_{i,j}^2 = \tau^2 / k$ are the equivalent of α_{ij} and β_{ij} in RFSN [55].

Trust is defined differently, since we want it to remain between (0) and (1), a convention that seems to be unanimous among researchers, except for the occasional translation to the scale [-1, 1]. In our trust model, we define the trust to be the probability, as shown in equations (5.16) and (5.17):

$$T_{i,j} = \text{Prob}\{|\theta_{i,j}| < \varepsilon\} \tag{5.16}$$

$$\begin{aligned} T_{i,j} &= \text{Prob}\{-\varepsilon < \theta_{i,j} < +\varepsilon\} \\ &= \phi\left(\frac{\varepsilon - \overline{y}_{i,j}}{\tau / \sqrt{k}}\right) - \phi\left(\frac{-\varepsilon - \overline{y}_{i,j}}{\tau / \sqrt{k}}\right) \\ &= \phi\left(\frac{\varepsilon - \mu_{i,j}}{\sigma}\right) - \phi\left(\frac{-\varepsilon - \mu_{i,j}}{\sigma}\right) \end{aligned} \tag{5.17}$$

where ϕ is the cumulative probability distribution (cdf) of the Normal $N(0, 1)$. As shown in Figure 5.5, the area under the *Gaussian* curve $N(\mu_{i,j}, \sigma_{i,j}^2)$ within the interval $[-\varepsilon, +\varepsilon]$ is the trust value. The bigger the error θ_{ij} is, meaning its mean shifting to the right or left of 0, and the more spread that error is, the lower the trust value is. Each node n_i maintains a line of reputation assessments composed of T_{ij} for each j, such that $\Gamma_{i,j} \neq 0$ (one-hop connection). T_{ij} is updated for each time period t for which data is received from some connecting node j. The filled areas in Figure 5.5 represent the Gaussian Trust T_{ij} in two cases.

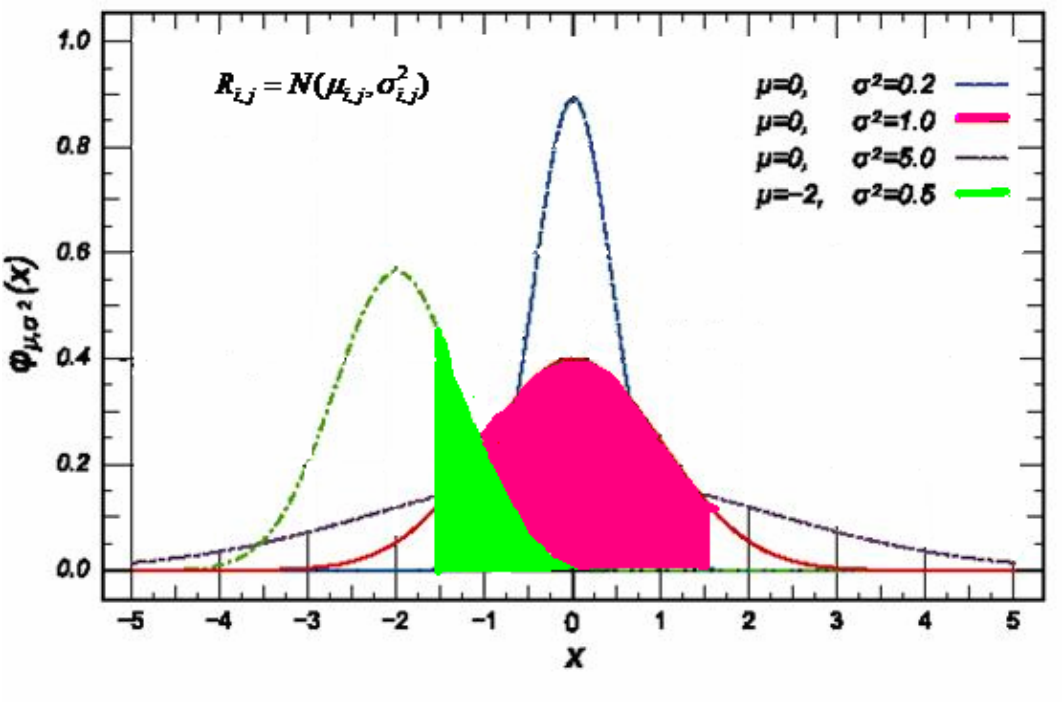

Figure 5.5. Normal (Gaussian) distribution example

In addition to data observed in form of $y_{i,j} = \{y_{i,j}(t)$, for all t values at which a report is issued by n_j and routed through $n_i\}$, node n_i uses *second-hand information* in the form of $(\mu_{l_s,j}, \sigma_{l_s,j})$, s = 1, …, m, from the m nodes connected to n_j and n_i, as shown in Figure 5.6, below. This is an "expert opinion", that is, soft information from external sources. Each of these m nodes has observed node n_j reports and produced assessments of its error in the form of $(\mu_{l_s,j}, \sigma_{l_s,j})$, s = 1,…, m, and consequently $T_{ls,j}$, s = 1, …, m. In using the expert opinion theory, one needs to modulate it. Node n_i uses its own assessment of the nodes $n_{l_1},...,n_{l_m}$, in the form of $(\mu_{i,l_s}, \sigma_{i,l_s})$, s = 1, … , m, and consequently $T_{i,ls}$, s = 1, …, m.

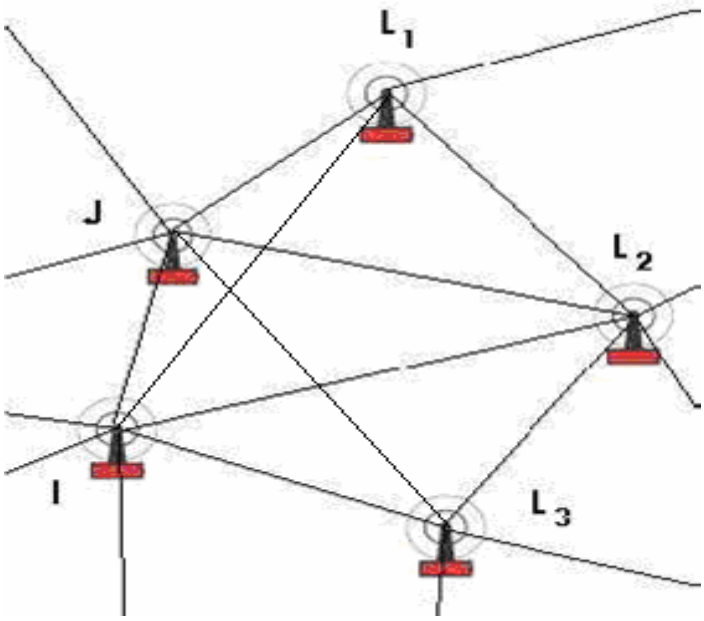

Figure 5.6. Nodes that provide second-hand information

Using Bayes' theorem, the probability distribution of $\theta_{i,j}$ is obtained using the observed data along with the second-hand modulated information, as shown in equation (5.18):

$$P(\theta_{i,j} \mid y_{i,j}, (\mu_{l_1,j}, \sigma_{l_1,j}), ..., (\mu_{l_m,j}, \sigma_{l_m,j}) \\ , (\mu_{i,l_1}, \sigma_{i,l_1}), ..., (\mu_{i,l_m}, \sigma_{i,l_m})) \tag{5.18}$$

and it is proportional to the product of three terms shown in equations (5.19), (5.20) and (5.21):

$$P(y_{i,j} \mid \theta_{i,j}, (\mu_{l_1,j}, \sigma_{l_1,j}), ..., (\mu_{l_m,j}, \sigma_{l_m,j}), \\ (\mu_{i,l_1}, \sigma_{i,l_1}), ..., (\mu_{i,l_m}, \sigma_{i,l_m})) \tag{5.19}$$

$$P((\mu_{l_1,j},\sigma_{l_1,j}),...,(\mu_{l_m,j},\sigma_{l_m,j})\,|\,\theta_{i,j},(\mu_{i,l_1},\sigma_{i,l_1}),...,(\mu_{i,l_m},\sigma_{i,l_m})) \tag{5.20}$$

and

$$P(\theta_{i,j}\,|\,(\mu_{i,l_1},\sigma_{i,l_1}),...,(\mu_{i,l_m},\sigma_{i,l_m})) \tag{5.21}$$

The first term, equation (5.19), reduces to $P(y_{i,j}\,|\,\theta_{i,j})$ through conditional independence, and is equal to the product of the likelihoods

$$\prod_{t=1}^{k} N(\theta_{i,j},\tau^2) \tag{5.22}$$

The third term, equation (5.21), also reduces to $P(\theta_{i,j})$, due to the conditional independence of $\theta_{i,j}$ from $(\mu_{i,l_1},\sigma_{i,l_1}),...,(\mu_{i,l_m},\sigma_{i,l_m})$, and it represents the prior distribution of $\theta_{i,j}$ which we model as a diffuse prior $N(0,\infty)$.

The second term, equation (5.20), models the use of the second-hand information. This term requires some elaboration and can be reduced to the product of equation (5.23) through conditional independence arguments.

$$\prod_{s=1}^{m} P((\mu_{l_s,j},\sigma_{l_s,j})\,|\,\theta_{i,j},(\mu_{i,l_s},\sigma_{i,l_s})) \tag{5.23}$$

To derive $P((\mu_{l_s,j},\sigma_{l_s,j})\,|\,\theta_{i,j},(\mu_{i,l_s},\sigma_{i,l_s}))$ for each s = 1, …, m, we observe the following:

for some *t*'s,

$$\theta_{i,j} = x_j(t) - x_i(t) \tag{5.24}$$

and for some *t*'s

$$\theta_{l,j} = x_j(t) - x_l(t) \tag{5.25}$$

and, if all *t*'s were the same, then

$$\theta_{i,j} = x_j(t) - x_i(t) = (x_j - x_l) + (x_l - x_i) = \theta_{l,j} + \theta_{i,l} \tag{5.26}$$

But not all *t*'s are the same, so all data are not used for all assessments. We inspire ourselves from this relationship to model the expert opinion likelihood. We assume that

$$\theta_{l,j} \simeq \theta_{i,j} - \theta_{i,l} \tag{5.27}$$

$$\mu_{l,j} \simeq \theta_{i,j} - \mu_{i,l} \tag{5. 28}$$

and we model

$$\mu_{l,j} \sim N(\theta_{i,j} - \mu_{i,l}, var) \tag{5.29}$$

where we choose *var* to be inversely related to node's n_i assessment of the reputation of node n_l, that is

$$var = \left(\frac{1}{T_{i,l}} - 1 \right) \psi \tag{5.30}$$

where ψ is a model parameter.

$$\mu_{l,j} \sim N(\theta_{i,j} - \mu_{i,l}, \left(\frac{1}{T_{i,l}} - 1 \right) \psi) \tag{5.31}$$

leads to equation (5.32):

$$\prod_{s=1}^{m} P((\mu_{l_s,j},\sigma_{l_s,j}) \mid \theta_{i,j},(\mu_{i,l_s},\sigma_{i,l_s})) = \prod_{s=1}^{m} N(\theta_{i,j}-\mu_{i,l_s},\left(\frac{1}{T_{i,l_s}}-1\right)\psi) \qquad (5.32)$$

and consequently proves that equation (5.33)

$$P(\theta_{i,j} \mid y_{i,j},(\mu_{l_1,j},\sigma_{l_1,j}),...,(\mu_{l_m,j},\sigma_{l_m,j}),(\mu_{i,l_1},\sigma_{i,l_1}),...,(\mu_{i,l_m},\sigma_{i,l_m})) \qquad (5.33)$$

is a Normal (Gaussian) distribution with mean and variance as shown in equations (5.34) and (5.35) respectively:

$$\mu_{i,j}^{new} = \frac{\sum_{s=1}^{m} \frac{(\mu_{l_s,j}+\mu_{i,l_s})}{\left(\frac{1}{T_{i,l_s}}-1\right)\psi} + (k\bar{y}/\tau^2)}{\sum_{s=1}^{m} \frac{1}{\left(\frac{1}{T_{i,l_s}}-1\right)\psi} + (k/\tau^2)} \qquad (5.34)$$

$$\sigma_{i,j}^{2\ new} = \frac{1}{\sum_{s=1}^{m} \frac{1}{\left(\frac{1}{T_{i,l_s}}-1\right)\psi} + (k/\tau^2)} \qquad (5.35)$$

These values $(\mu_{i,j}^{new},\sigma_{i,j}^{new})$, along with $(\mu_{i,j},\sigma_{i,j})$, are easily updatable values that represent the continuous Gaussian version of the $(\alpha_{i,j},\beta_{i,j})$ and $(\alpha_{i,j}^{new},\beta_{i,j}^{new})$ of the binary approach in [55], as derived from the approach in [61]. The solution

presented is simple and easily computed, keeping in mind that the solution applies to networks with limited computational power. In the binary work, $(\alpha_{i,j}, \beta_{i,j})$ are obtained through a Bayesian approach, while $(\alpha_{i,j}^{new}, \beta_{i,j}^{new})$ are obtained through the combination approach of Belief functions. The Gaussian solution provides a full probabilistic approach in the case of continuous sensor data.

Some would object to the use of a diffuse prior, which, in effect, forces a null prior trust value, regardless of the ε value. A way to remedy to this is to start with a $N(\mu_0, \sigma_0^2)$ prior distribution for all θ_{ij}, such that the prior trust is (1/2). This choice not only answers the diffuse prior issue, but also allows the choice of the parameters involved. ε can be determined: given μ_0 and σ_0, μ_0 is most likely to be set to (0). Therefore, σ_0 and ε determine each other. Once one is set, the other is automatically deducted. Note that the prior is really node-dependent, making our definition of trust, and therefore **ε**, node-dependent. In practice, it is most likely that all priors are tuned to the same values so that the prior trusts are started at some level, say (1/2), with a proper prior $\theta_{i,j}$, as shown in equation (5.36):

$$\theta_{i,j} \sim N(\mu_0, \sigma_0^2) \tag{5.36}$$

The reputation parameters $\mu_{i,j}$ and $\sigma_{i,j}^2$ are presented in equations (5.37) and (5.38):

$$\mu_{i,j} = \frac{(\mu_0 / \sigma_0^2) + (k\overline{y}_{i,j} / \tau^2)}{(1/\sigma_0^2) + (k/\tau^2)} \tag{5.37}$$

$$\sigma_{i,j}^2 = \frac{1}{(1/\sigma_0^2)+(k/\tau^2)} \tag{5.38}$$

and the updated values are presented in equations (5.39) and (5.40) respectively:

$$\mu_{i,j}^{new} = \frac{(\mu_0/\sigma_0^2)+\sum_{s=1}^{m}\frac{(\mu_{l_s,j}+\mu_{i,l_s})}{\left(\frac{1}{T_{i,l_s}}-1\right)\psi}+(k\overline{y}_{i,j}/\tau^2)}{(1/\sigma_0^2)+\sum_{s=1}^{m}\frac{1}{\left(\frac{1}{T_{i,l_s}}-1\right)\psi}+(k/\tau^2)} \tag{5.39}$$

$$\sigma_{i,j}^{2\ new} = \frac{1}{(1/\sigma_0^2)+\sum_{s=1}^{m}\frac{1}{\left(\frac{1}{T_{i,l_s}}-1\right)\psi}+(k/\tau^2)} \tag{5.40}$$

Once $\mu_{i,j}^{new}$ and $\sigma_{i,j}^{2\ new}$ are formulated, the new trust value $T_{i,j}^{new}$ will be presented as shown in equation (5.41):

$$T_{i,j}^{new} = \phi\left(\frac{\varepsilon-\mu_{i,j}^{new}}{\sigma_{i,j}^{new}}\right)-\phi\left(\frac{-\varepsilon-\mu_{i,j}^{new}}{\sigma_{i,j}^{new}}\right) \tag{5.41}$$

We call this trust and reputation system (GTRSSN), which stands for Gaussian Trust and Reputation System for Sensor Networks. It can be seen as an extension of the concepts of RFSN and DRBTS for sensor data and it introduces a full

probabilistic approach to the combination of information in the reputation assessment.

5.7. Simulation Results

To verify the theory introduced in this chapter, several simulation experiments in different scenarios were developed. The results from the simulations conducted on the network shown in Figure 5.7, for one scenario, where only a random region from the network is selected to report data on every time series, are presented in this section. In all simulation experiments, the trust relationship between four nodes (1, 6, 7 and 13) in a sub-network of the fifteen-node network shown in Figure 5.7 is calculated.

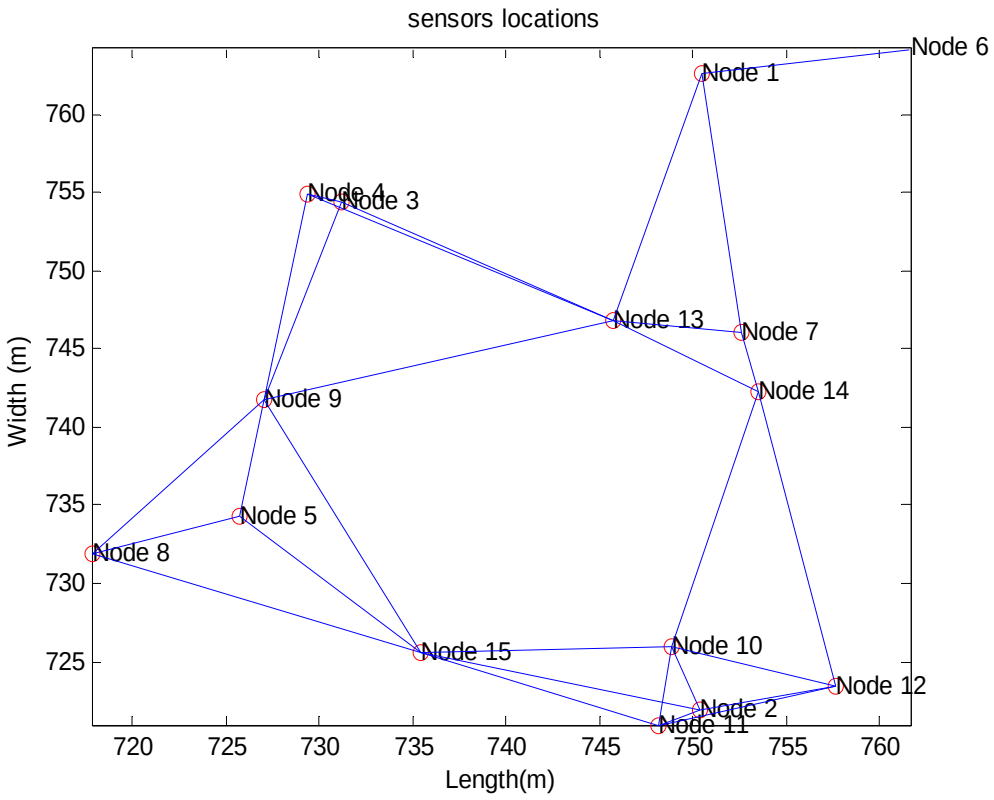

Figure 5.7. Wireless Sensor Network Diagram

In this scenario and as stated before, it is assumed that, at each time slot a group of nodes are selected to report their sensed data, and when one node is sending its own reading to a specific node in the group, all the surrounding nodes connected to the sending node hear the reported value and start to send the output of that reading as a second-hand information to the receiving node regarding the sending node. The output of that reading between the sending and the receiving nodes is regarded as the direct observation, as discussed before. In other words, and in the case of selected sub-network, when node (7) is sending its reading to node (1), nodes (6) and (13) hear the reported data, use it to find the trust between them and node (1) and report that trust to node (1) as second-hand information about node

(7). Node (1), at the same time, uses the reading reported directly from node (7) to calculate the direct trust between node (1) and node (7).

5.7.1. No faulty or malicious nodes are present in the network

At the beginning, it is assumed that all nodes are working properly, that no faulty or malicious nodes exist in the network, and report the sensed event (temperature) with minimum error. Figure 5.8 below presents the result of the simulation and shows the trust value between node (1) and the other nodes (6, 7 and 13). At first node (1) assesses node (13) based on the direct interactions only between the two nodes, without second-hand information, and then node (1) assesses node (13) based on the direct information between the two nodes and the second-hand information received from node (7) about node (13), with second-hand information. Node (1) performs the same assessment procedure for all nodes directly connected to it.

It can be seen from Figure 5.8 that trust values between node (1) and nodes (7) and (13) are slightly different but they eventually all converge to the value of one. The trust value between node (1) and node (6) is the same in both cases, with and without second-hand information as there is no second-hand information for node (6). Node (6) is not connected to any other node other than node (1).

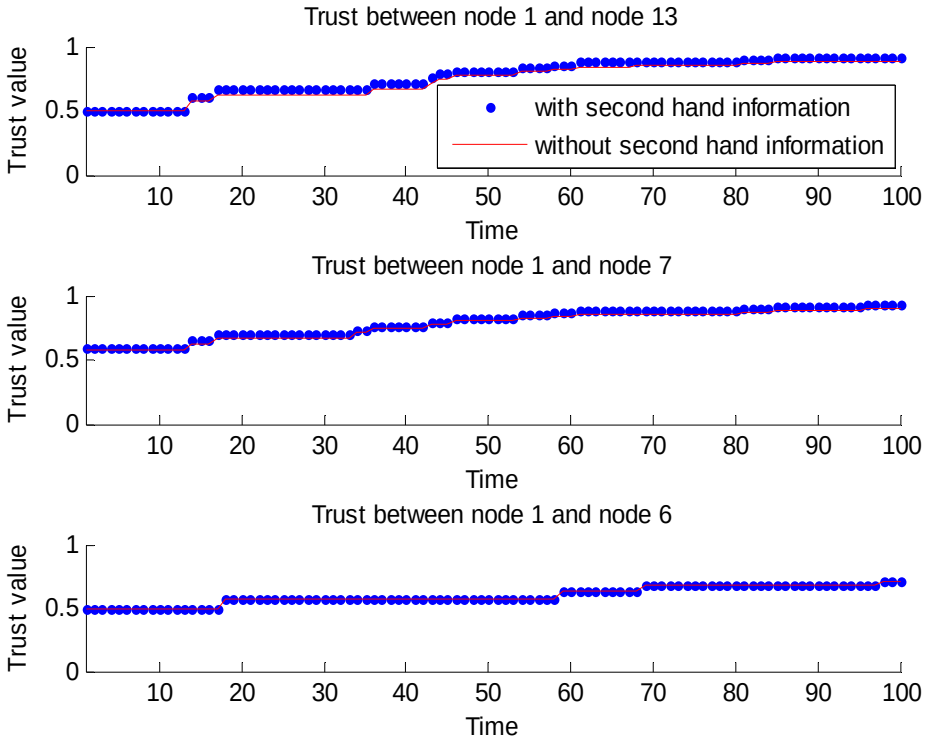

Figure 5.8. All nodes are normal

5.7.2. Node (13) is Faulty or Malicious

In another experiment, the same network was simulated, but with the introduction of a significant error in node (13) readings, that is, node (13) is faulty or malicious. Simulation results are shown in Figure 5.9, below and, as can be seen from Figure 5.9, the trust value between node (1) and node (13) dropped to almost zero for both cases, with and without second-hand information, which means node (7) is assessing node (13) as a faulty or malicious node. The situation for node (6) is not affected, as there is no connection between node (6) and node (13). The interesting result here is that the trust value between node (1) and node (7) is not

affected in either case even though there is a connection between node (7) and node (13). Node (13) is faulty, and one would think that it could harm the reputation of node (7), but that was not the case, which proves that the modulation in the approach makes the reputation system robust to bad-mouthing attacks.

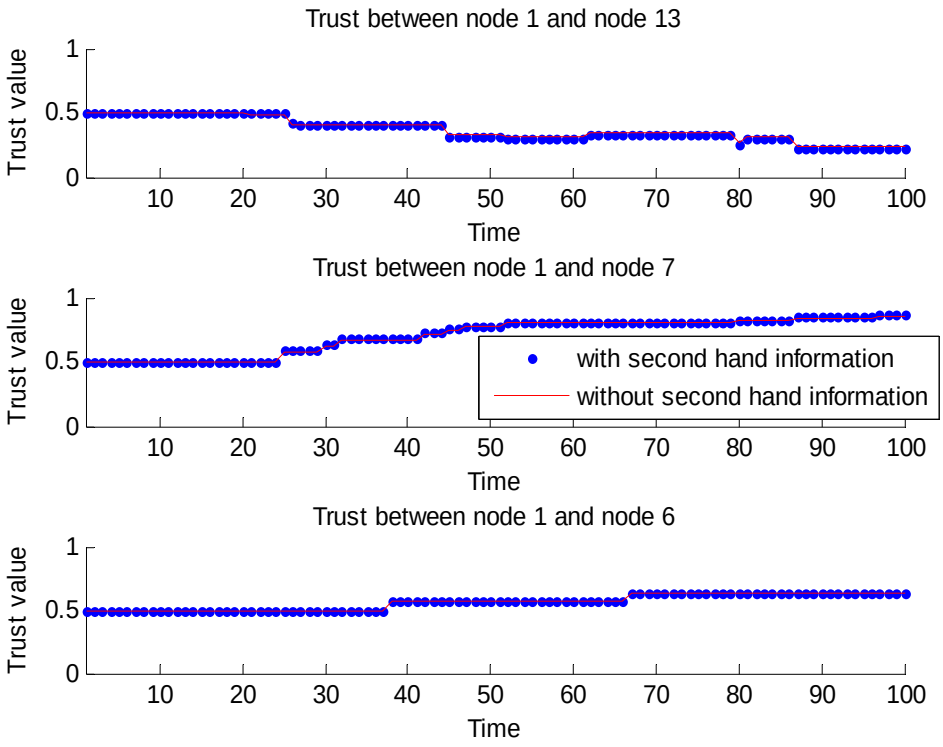

Figure 5.9. Node (13) is faulty

5.7.3. Node (7) and Node (13) are Faulty

In this simulation experiment, it has been assumed that node (7) and node (13) are faulty. The results of the simulation are presented in Figure 5.10, showing that the trust values for both nodes (7) and (13) are dropping to zero in both cases. Node

(6) is assumed reliable and the trust value associated with it is the same in both cases, as there is no connection between node (6) and the other faulty nodes, (7) or (13), to affect that trust value.

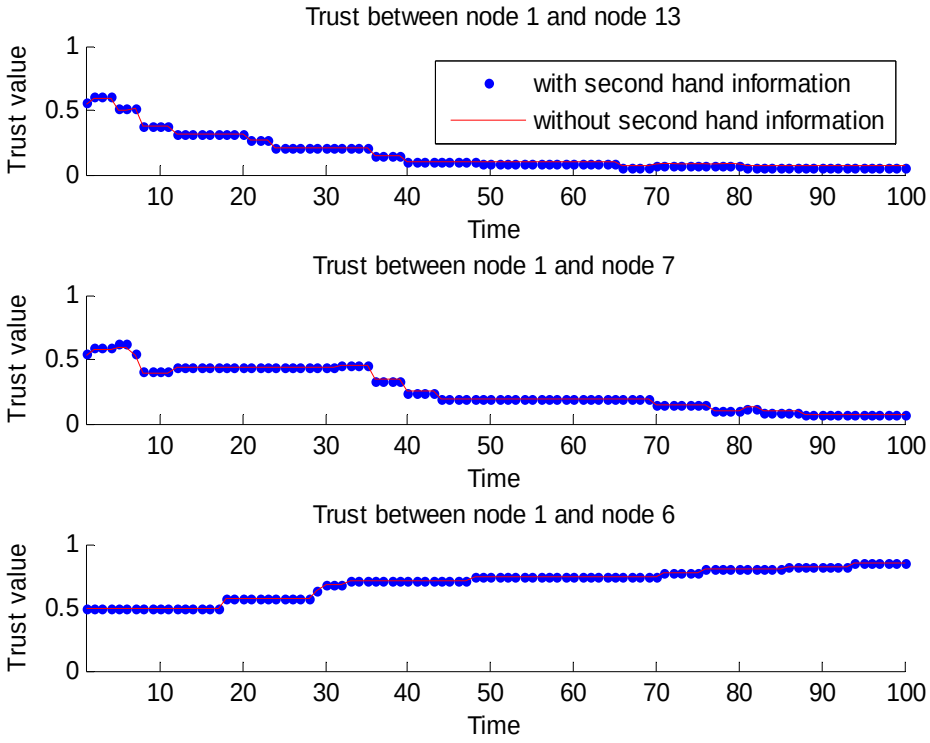

Figure 5.10. Node (7) and node (13) are faulty

5.7.4. Node (6) is Faulty or Malicious

The simulation results presented in Figure 5.11 below show that when node (6) is faulty or malicious, nothing almost will change in the trust values between node (1) and either of nodes (7) and (13), as there is no direct or indirect connection between them. In other words, when node (6) is faulty, node (1) will discover that, as it has a direct connection with node (6) and the direct trust with node (6) will be

affected. As there is no indirect trust for node (6), both trust values will stay on the initial trust value or will decrease to the value of zero.

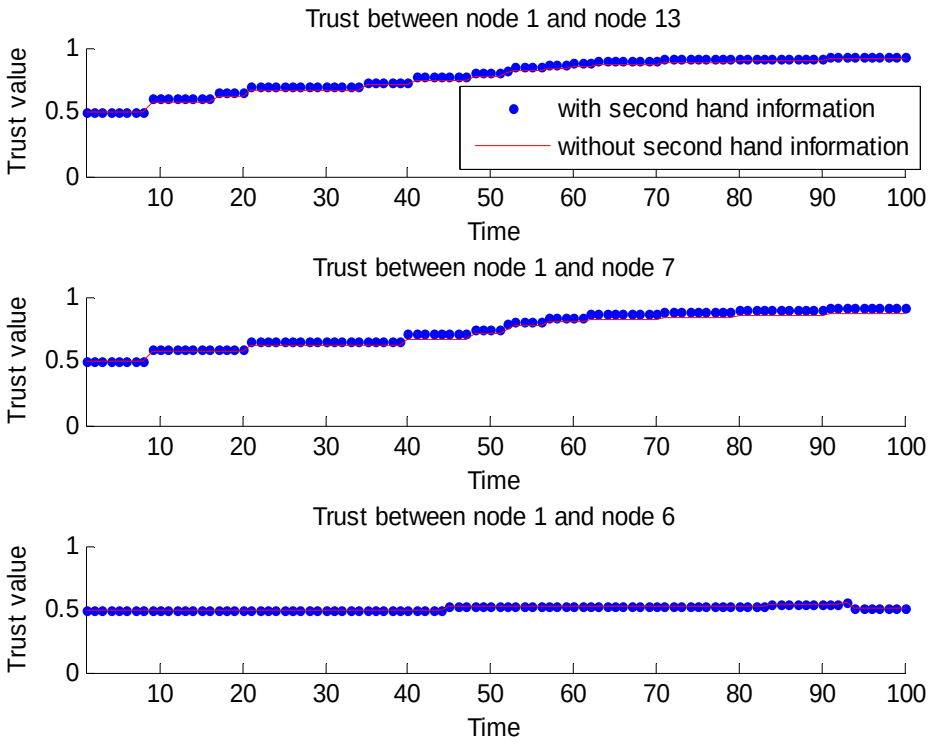

Figure 5.11. Node (6) is faulty

5.7.5. Node (1) is Faulty or Malicious

It is assumed in this experiment that node (1) is faulty or malicious. Node (1) is the main node in the sub-network and is acting as the receiving node, and all the simulations show the trust relationship between node (1) and all the other nodes connected to it. As can be seen from Figure 5.12, the direct trust value for both nodes (7) and (13), is declining to the value of zero, as node 1 is faulty. That will leave the two nodes (7) and (13) to assess each other indirectly, which is a very interesting case again, as both nodes (7) and (13) are now assessing node (1) as a

faulty node, so the indirect trust value for both nodes are slowly converging to the value of one. The trust value for node (6) is set to the initial value (0.5) and will decrease on both values to zero, as there is no second-hand information available to node (6) and node (1) is a faulty node.

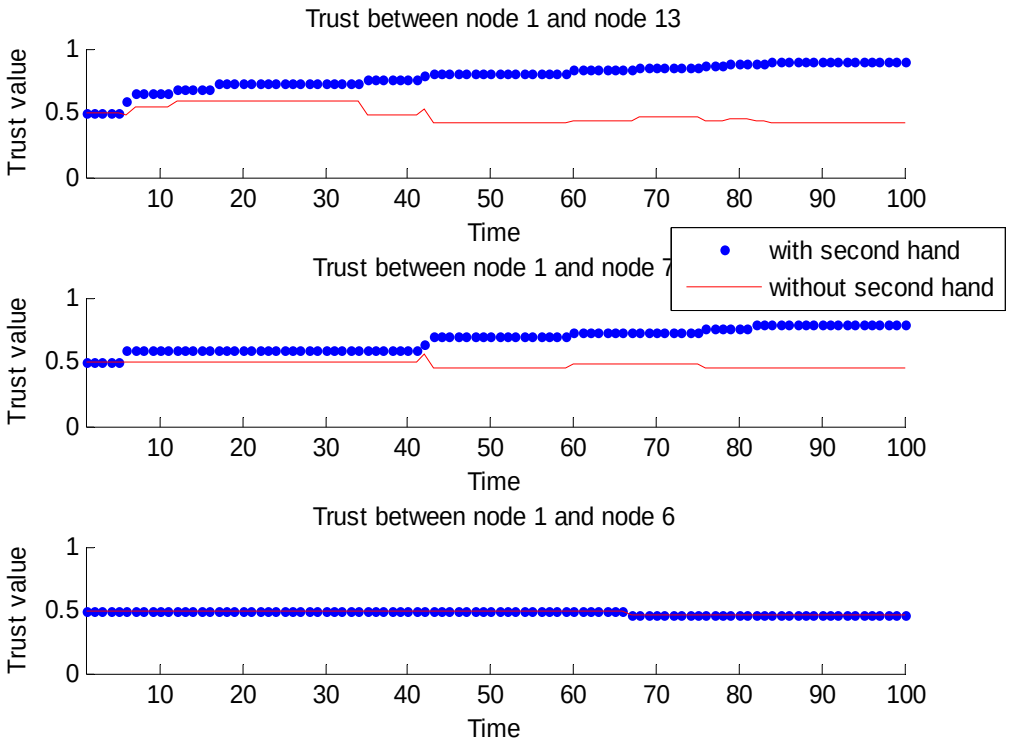

Figure 5.12. Node (1) is a malicious node

The last example shows precisely the reason the trust system is instituted. It allows the classification of nodes into separate sets according to their trustworthiness. In the last example, it is known that node (1) is faulty, since it is a simulation exercise. The results should clearly indicate to the network that node (1) is faulty. However, it could also be the case that the nodes (7) and (13) are malicious. The trust system works on the assumption that a majority of nodes in a

neighbourhood are reliable. This principle helps purge the system of bad elements. In this case, at this point, it is observed that the developed trust system is effective in distinguishing among nodes.

5.8. Conclusion

It has been argued that the trust-modelling problem is characterised by uncertainty, and the only coherent way to deal with uncertainty is through probability. Even though some of the trust models introduced for sensor networks employ probabilistic solutions mixed with ad-hoc approaches, none of them produces a full probabilistic answer to the problem. In this chapter we introduced a theoretically sound Bayesian probabilistic approach for calculating trust and reputation systems in WSNs. We introduced a new Gaussian Trust and Reputation System for Sensor Networks (GTRSSN), which we believe is a breakthrough in modelling trust in WSNs, as previous studies in WSNs focused on the trust associated with the routing and the successful performance of a sensor node in some predetermined task, that is, looking at binary events to model trust and the trustworthiness and reliability of the nodes of a WSN when the sensed data is continuous has not been addressed before. Having said that, introducing the sensor data as a major component of trust leads to the modification of node misbehaviour classification, the trust computational model and the way first-hand and second-hand information is formulated. These issues have been presented in this chapter. Also, a brief summary about the Beta reputation system and the expert opinion theory has been presented. A very detailed GTRSSN, which is the significant

contribution of this research, has also been presented, with some simulation results. The simulation results show the implications of sensor data for the direct and indirect trust relationship between nodes, which helps to distinguish among nodes and purge the bad nodes from the network.

6. Bayesian Fusion Algorithm for Combining Communication Trust and Data Trust in Wireless Sensor Networks

This chapter introduces a new Bayesian fusion algorithm to combine more than one trust component (data trust and communication trust) to infer the overall trust between nodes. It argues that one trust component is not enough when deciding on whether or not to trust a specific node in a sensor network. It discusses and analyses the results from the communication trust component (binary) and the data trust component (continuous) and proves that either component by itself, can mislead the network and eventually cause a total breakdown of the network. So, new algorithms are needed to combine more than one trust component to produce the overall trust.

Trust management in WSNs, as mentioned so far, has predominantly been based on routing messages, whether the communication has happened or not, which is called “Communication Trust”. The introduction of sensed data, as discussed in Chapter 5, as a new core component when deciding to trust nodes in WSNs, represents a new challenge on “how much trust is enough, and which components should be included to decide on trust”. This new core component is called “Data Trust”.

It has been argued that, if the overall trust is based on just the communication trust, then the network might be misled and untrustworthy nodes in terms of data trust can be classified as trusted nodes due to their communication capabilities and vice versa. That is, approaching the trust problem from one angle is not enough to decide on whether or not to trust a specific node in a WSN. So new trust models to be developed to address the issue of which components are to be involved when calculating trust and how to combine these components to achieve the overall trust applied to different scenarios and applications.

In this chapter, the previously designed trust model for WSNs, as discussed in Chapter 5, is extended to include both communication trust and data trust. Here, the work presented in [118, 119], the data trust model, is simulated and compared with the work presented in [55], the communication trust model, and the results have proven that modelling trust using only one component might not be enough to decide on the trustworthiness of nodes in a WSN. So a new Bayesian fusion algorithm is introduced to address the issue and to combine both data trust and communication trust to calculate the overall trust. The algorithm is generic and allows more trust components to be plugged into the model to produce the total trust for different scenarios.

6.1. Trust Components

To further illustrate the above discussion and to differentiate between the communication trust and the data trust as mentioned before, let us consider the

following scenario, which assumes that a WSN consists of three nodes (1, 2 and 3) and a fusion centre (FC), as presented in Figure 6.1. Nodes are deployed to monitor an event and report the sensed data to the (FC). Nodes can communicate, send and receive messages, even if some of them are adversary, but for unseen reasons they do not report their sensed data and, vice versa, nodes do report their sensed data but do not route messages. In other words, node (3) in Figure 6.1, for example, is forwarding all messages from node (1) and node (2) to the (FC), which means node (3) is very trustworthy from the communication point of view, but for some reason it is not reporting its actual data to other nodes in the network. For example, if node (3) is a malicious node and because the reported data will affect it somehow, imagine that the sensed data are pointing to intruder personnel from the same group as node (3) entering and leaving a battle-field: of course node (3) is not going to report it. And the same thing is valid when all three nodes are sending their sensed data, temperature, for example, but due to the communication's high cost in such networks and because of node (3) being selfish, it is not routing messages from nodes (1) and (2). In this situation, node (3) is trusted from the data point of view but not from the communication point of view. So a mechanism to judge and predict the behaviour of node (3) and to report it to the other nodes and/or to the (FC) is needed.

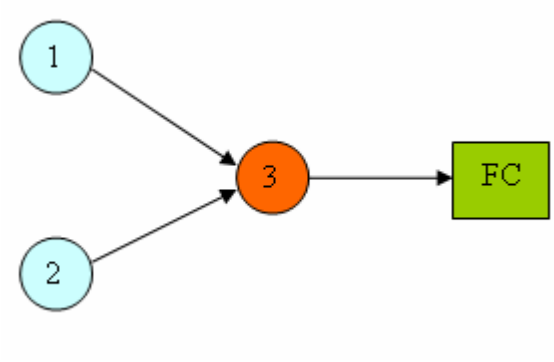

Figure 6.1. Wireless sensor network scenario

Based on the above illustration, the trust computational model for WSNs presented in [116, 117], is extended to reflect the new challenges, using more than one criterion to decide on trust. The extended trust computational model for WSNs, presented in Figure 6.2, is a generic trust model, that is, new trust components affecting nodes' trustworthiness in a network can be added to or removed from the model and the overall trust can be recalculated very easily.

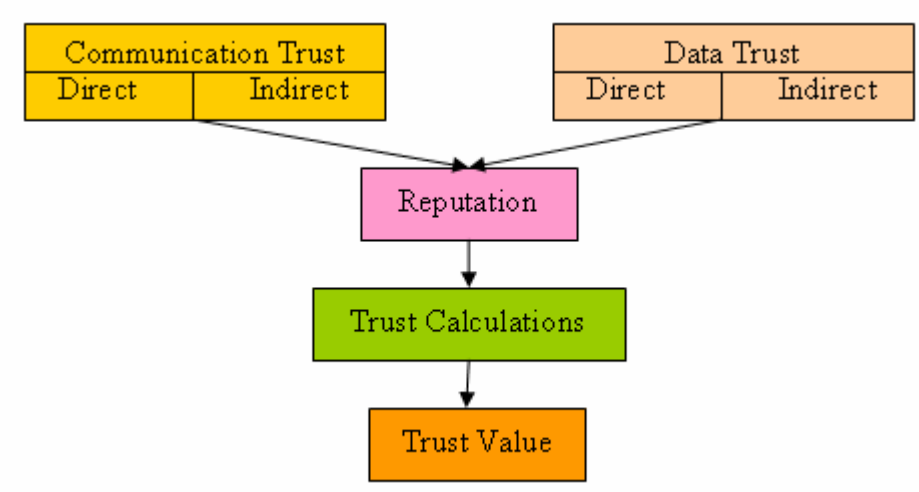

Figure 6.2. Extended trust computational model in WSNs

As can be seen from Figure 6.2, trust in WSNs is a combination of communication trust and data trust, which are presented in the following sub-sections.

6.1.1. Communication Trust in WSNs

Communication trust (CT), here, means the trust value calculated between nodes based on their cooperation in routing messages to other nodes in the network. In their trust model for sensor networks, Ganeriwal and Srivastava, in [55], extended the work of Josang and Ismail presented in [61] as a model to derive reputation ratings in the context of e-commerce. And, as discussed in the previous chapter, the Beta reputation system is based on the Beta probability density function, *Beta* (α, *β*), and is given in equation (6.1):

$$f(p \mid \alpha, \beta) = \frac{\Gamma(\alpha + \beta)}{\Gamma(\alpha)\Gamma(\beta)} p^{\alpha-1}(1-p)^{\beta-1} \tag{6.1}$$

For each node n_j, a reputation R_{ij} can be carried by a neighbouring node n_i. The reputation is embodied in the Beta model and carried by two parameters α_{ij} and β_{ij}. α_{ij} represents the number of successful transactions node n_i had with, or observed about n_j, and β_{ij} the number of unsuccessful transactions. The reputation of node n_j, maintained by node n_i, is shown in equation (6.2):

$$R_{ij} = Beta(\alpha_{ij} + 1, \beta_{ij} + 1) \tag{6.2}$$

Trust is defined as the expected value of the reputation and is given in equation (6.3):

$$T_{ij} = E(R_{ij}) = E\{Beta(\alpha_{ij} + 1, \beta_{ij} + 1)\} = \frac{(\alpha_{ij} + 1)}{(\alpha_{ij} + \beta_{ij} + 2)} \quad (6.3)$$

Second-hand information is presented to node n_i by another neighbouring node, n_k. Node n_i receives the reputation of node n_j by node n_k, R_{kj} , in the form of the two parameters α_{kj} and β_{kj}. Using this new information, node n_i combines it with its current assessment, R_{ij}, to obtain a new reputation, R_{ij}^{new}, as in equation (6.4):

$$R_{ij}^{new} = Beta(\alpha_{ij}^{new}, \beta_{ij}^{new}) \quad (6.4)$$

where node n_i uses its reputation of node n_k in the combination process. α_{ij}^{new} and β_{ij}^{new}, shown in equations (6.5) and (6.6) respectively, are the updated values for α_{ij} and β_{ij} given by the authors of [55] by mapping the problem into a Dempster-Shaffer belief theory model [137], solving it using the concept of belief discounting, and undertaking a reverse mapping from belief theory to continuous probability. For more details on all these equations, readers are encouraged to refer to [55, 57, 61]. Tc_{ij}^{new}, given in equation (6.7), is the updated CT value based on α_{ij}^{new} and β_{ij}^{new} values.

$$\alpha_{ij}^{new} = \alpha_{ij} + \frac{2 * \alpha_{ik} * \alpha_{kj}}{(\beta_{ik} + 2) * (\alpha_{kj} + \beta_{kj} + 2) + (2 * \alpha_{ik})} \tag{6.5}$$

$$\beta_{ij}^{new} = \beta_{ij} + \frac{2 * \alpha_{ik} * \beta_{kj}}{(\beta_{ik} + 2) * (\alpha_{kj} + \beta_{kj} + 2) + (2 * \alpha_{ik})} \tag{6.6}$$

$$\begin{aligned} Tc_{ij}^{new} &= E(R_{ij}^{new}) = E\{Beta(\alpha_{ij}^{new} + 1, \beta_{ij}^{new} + 1)\} \\ &= \frac{(\alpha_{ij}^{new} + 1)}{(\alpha_{ij}^{new} + \beta_{ij}^{new} + 2)} \end{aligned} \tag{6.7}$$

6.1.2. Data Trust in WSNs

Data trust (DT) is a new concept introduced in the previous chapter to calculate trust in WSNs based on the actual sensed data of the sensors, and it is recommended that readers refer to the previous chapter for a detailed explanation on the equations presented here, in order to avoid repetition. Reputation $R_{i,j}$ and trust $T_{i,j}$ between node n_i and node n_j are defined as discussed in the previous chapter and given in equations (6.8) and (6.9) respectively:

$$R_{i,j} = N(\mu_{i,j}, \sigma_{i,j}^{2}) \tag{6.8}$$

$$
\begin{aligned}
T_{i,j} &= \text{Prob}\{|\theta_{i,j}| < \varepsilon\} \\
&= \text{Prob}\{-\varepsilon < \theta_{i,j} < +\varepsilon\} \\
&= \phi\left(\frac{\varepsilon - \mu_{i,j}}{\sigma_{i,j}}\right) - \phi\left(\frac{-\varepsilon - \mu_{i,j}}{\sigma_{i,j}}\right)
\end{aligned}
\tag{6.9}
$$

where $\mu_{i,j}$ and $\sigma^2_{i,j}$, represent the mean and variance as shown in equations (6.10) and (6.11):

$$
\mu_{i,j} = \frac{(\mu_0/\sigma_0^2) + (k\bar{y}_{i,j}/\tau^2)}{(1/\sigma_0^2) + (k/\tau^2)} \tag{6.10}
$$

$$
\sigma^2_{i,j} = \frac{1}{(1/\sigma_0^2) + (k/\tau^2)} \tag{6.11}
$$

It is also argued that the second-hand information represents a Normal, Gaussian distribution with updated mean $\mu^{new}_{i,j}$ and variance $\sigma^{2\,new}_{i,j}$, given in equations (6.12) and (6.13) respectively:

$$
\mu^{new}_{i,j} = \frac{(\mu_0/\sigma_0^2) + \sum_{s=1}^{m} \frac{(\mu_{l_s,j} + \mu_{i,l_s})}{\left(\frac{1}{T_{i,l_s}} - 1\right)\psi} + (k\bar{y}_{i,j}/\tau^2)}{(1/\sigma_0^2) + \sum_{s=1}^{m} \frac{1}{\left(\frac{1}{T_{i,l_s}} - 1\right)\psi} + (k/\tau^2)} \tag{6.12}
$$

$$\sigma_{i,j}^{2\ new} = \frac{1}{(1/\sigma_0^2) + \sum_{s=1}^{m} \frac{1}{\left(\frac{1}{T_{i,l_s}} - 1\right)\psi} + (k/\tau^2)} \tag{6.13}$$

based on the above discussion, the newly updated DT value $Td_{i,j}^{new}$ between node n_i and node n_j will be calculated using the equation (6.14):

$$Td_{i,j}^{new} = \phi\left(\frac{\varepsilon - \mu_{i,j}^{new}}{\sigma_{i,j}^{new}}\right) - \phi\left(\frac{-\varepsilon - \mu_{i,j}^{new}}{\sigma_{i,j}^{new}}\right) \tag{6.14}$$

Simulation experiments to verify the argument "one trust component might mislead nodes in a WSN, and distrusted nodes can be seen as very trustworthy", were developed and conducted to calculate CT and DT between four nodes (1, 6, 7, and 13) in a sub-network of fifteen nodes, as shown in Figure 6.3.

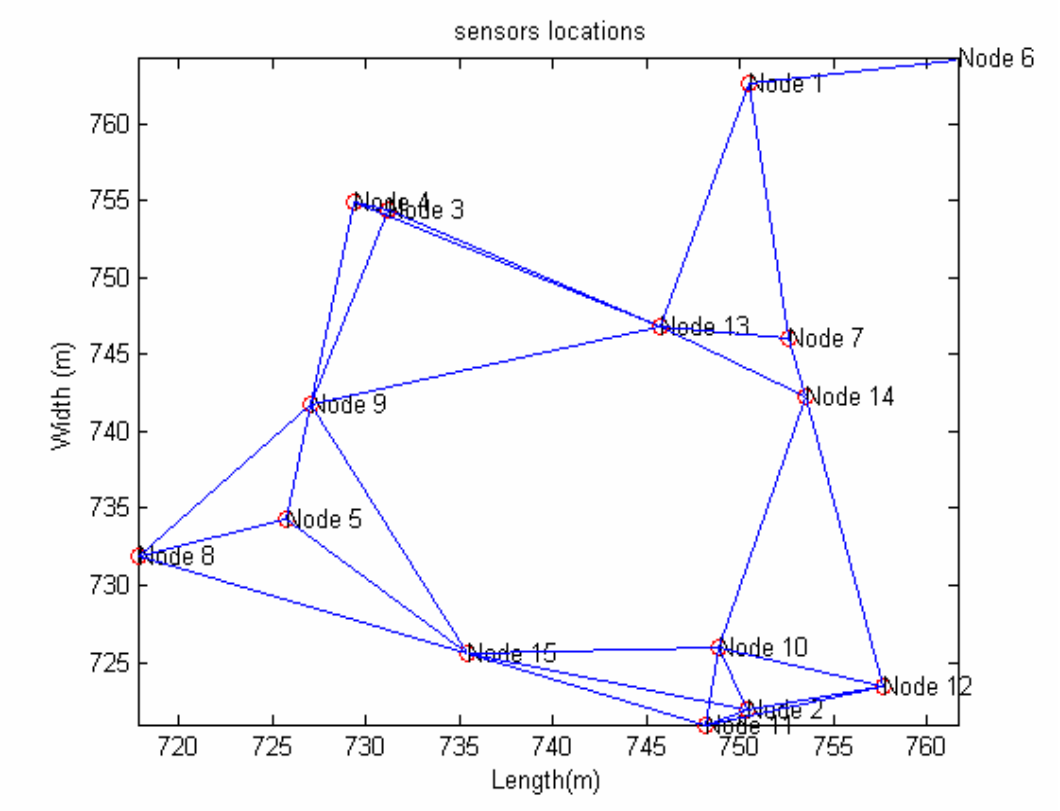

Figure 6.3. Wireless sensor network diagram

Initially, it is assumed that all nodes are normal; no faulty or malicious nodes exist in the network, so all nodes report their sensed data and route messages normally. The results presented in Figure 6.4 demonstrate that all nodes in the sub-network trust each other and the trust value is increasing gradually until it reaches the maximum value for both DT and CT.

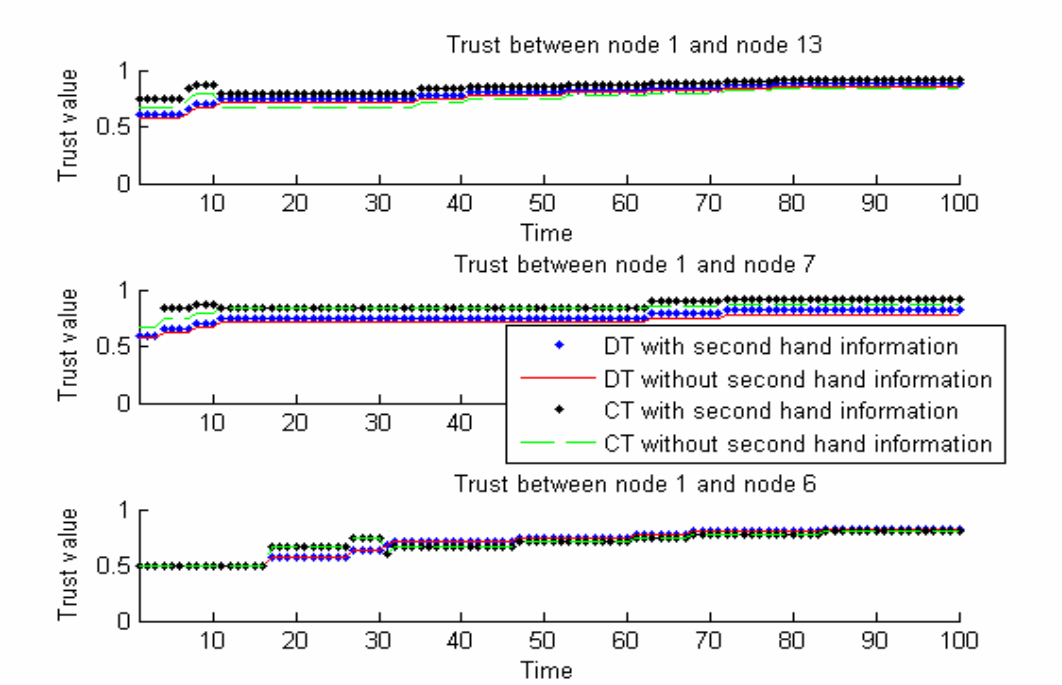

Figure 6.4. All nodes are normal

In a second simulation, whose results are presented in Figure 6.5, node (13) is assumed to be malicious, not reporting data, so it is noticeable that the CT is gradually increasing to the maximum value between all nodes, as there is no communication error between nodes, while the DT trust is decreasing to the minimum value for node (13) as it is a malicious node, not reporting its sensed data to other nodes. In other words, node (13) is assumed to be a trusted node from a communication point of view, but in reality it is not, as can be seen from the data point of view.

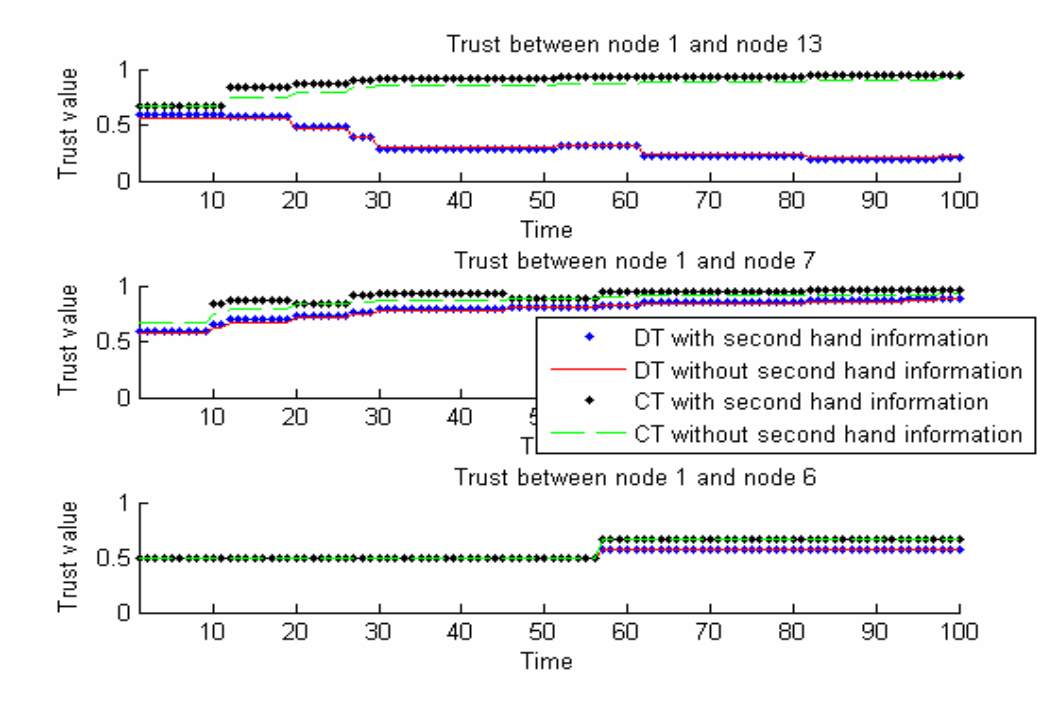

Figure 6.5. Node 13 is not reporting data

In a third simulation experiment, it is assumed that a communication error exists between nodes, so nodes can report their sensed data but are not routing messages between themselves, and the results presented in Figure 6.6 below indicate that the CT is gradually decreasing to the minimum value between all nodes and the DT is gradually increasing to the maximum value, as all nodes are reporting their sensed data. So again, nodes are assumed to be trusted from the data point of view, while in reality they are not, as they are not routing messages between themselves and the communication trust is decreasing to the minimum value.

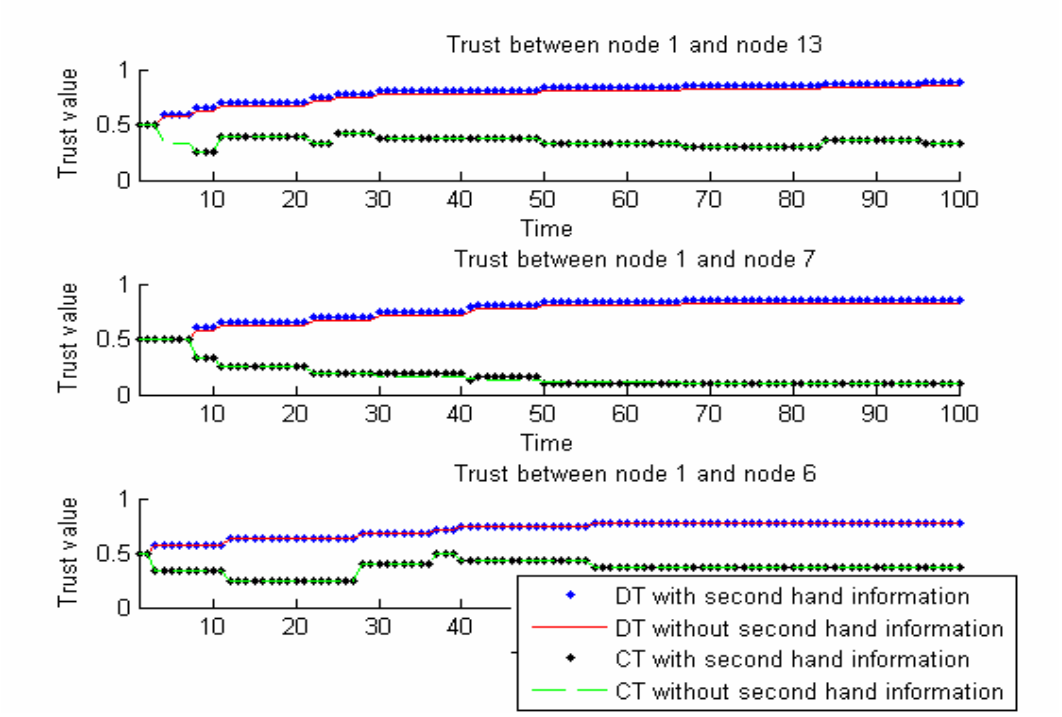

Figure 6.6. All nodes have a with communication error

From the previous simulation results, it has been proven that one component for calculating trust in WSNs might not be enough, as it could mislead the whole network, so a new technique is required to combine more than one trust component to achieve the overall trust. It has been argued that Bayesian fusion algorithms are the most suitable tools to combine trust components, as discussed in the following section.

6.2. Bayesian Fusion Algorithm

The Bayesian fusion structure illustrated in Figure 6.7 is a representation of the newly created trust model given in Figure 6.2, where C represents the communication trust, D represents the data trust and T represents the total trust.

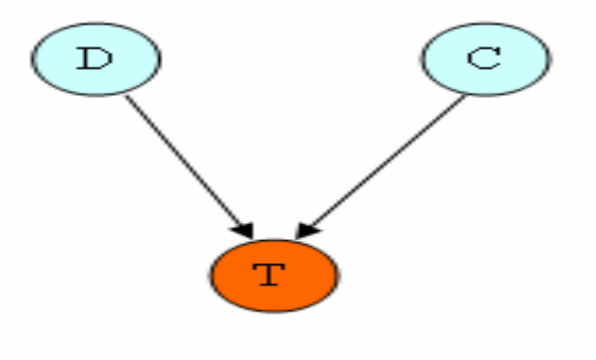

Figure 6.7. Bayesian Fusion structure

Using Bayes' theorem as discussed in appendix A, the probability of the total trust, given the data trust and communication trust, can be presented, as shown in equation (6.15):

$$P(T \mid D, C) = \frac{P(D \mid T, C) * P(T \mid C)}{P(D \mid C)} \tag{6.15}$$

As discussed previously in the intrusion detection scenario illustrated in Figure 6.1, in the case of a node always communicating but not reporting the data, C and

D are independent. Because of that independence, the likelihood function $P(D|T,C)$ in equation (6.15) can be presented, as in equation (6.16):

$$P(D|T,C) = P(D|T) \tag{6.16}$$

By substituting equation (6.16) in equation (6.15), the probability of the total trust will be as given in equation (6.17):

$$P(T|D,C) = \frac{P(D|T) * P(T|C)}{P(D|C)} \tag{6.17}$$

Applying Bayes' theorem, $P(D|T)$ can be calculated as in equation (6.18):

$$P(D|T) = \frac{P(T|D) * P(D)}{P(T)} \tag{6.18}$$

By substituting equation (6.18) in equation (6.17), the result is given in equation (6.19):

$$P(T|D,C) = \frac{P(T|D) * P(T|C) * P(D)}{P(D|C) * P(T)} \tag{6.19}$$

From equation (6.19), after ignoring the normalising factor and the other constants, it can be seen that the probability of the combined trust T is mainly

equal to the multiplication of the probabilities of both trust components, C and D, as shown in equation (6.20):

$$P(T \mid D, C) = P(T \mid D) * P(T \mid C) \tag{6.20}$$

In other words, the resulting distribution of both distributions – the Beta distribution used to calculate communication trust and the Normal distribution used to calculate data trust – is equal to the multiplication of both distributions, as illustrated in Figure 6.8.

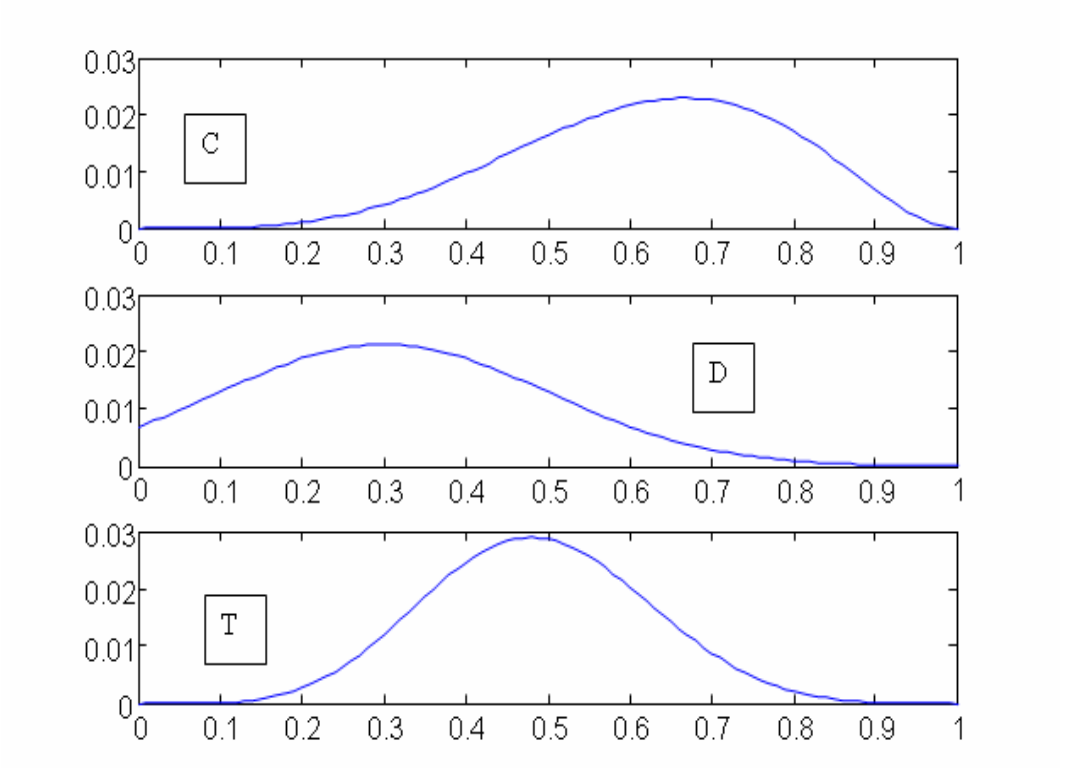

Figure 6.8. Multiplication of Beta and normal distributions

The first distribution represents a Beta distribution, the second distribution represents a normal distribution and the third distribution represents the resulting distribution, the multiplication of the Beta and normal distributions.

6.3. Simulation Results

To verify the theory given in the previous section, several simulations were conducted on the same sub-network of nodes (1, 6, 7 and 13) from the network diagram presented in Figure 6.3.

6.3.1. All nodes are normal

Figure 6.9 below displays the results when all nodes in the sub-network are normal from both the communication and data point of view. The total trust value is increasing to the maximum value of one, as for the other trust values: data trust and communication trust.

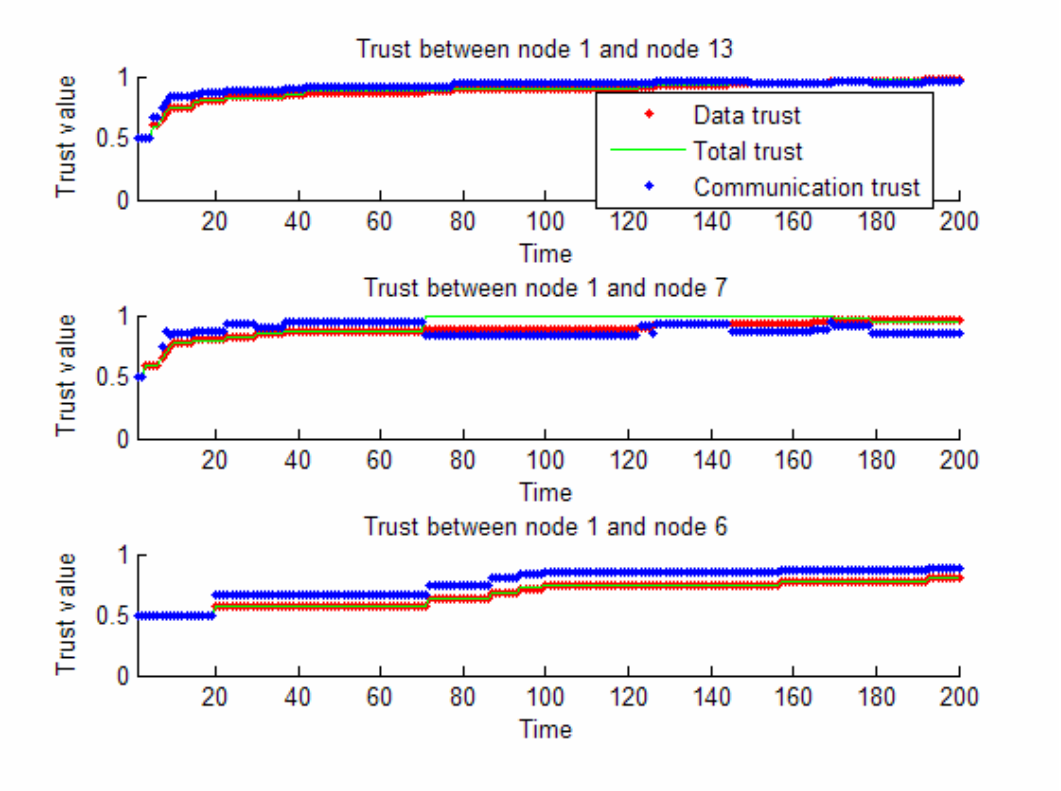

Figure 6.9. All nodes in the sub-network are normal

6.3.2. Node 13 is not reporting data

Figure 6.10 shows the results when node 13 is faulty from the data point of view, That is, node 13 is routing messages but not reporting sensed data. The data trust is decreasing to zero and the communication trust is increasing to one, the total trust is in between, which is reasonable; the total trust stays on the initial trust value assigned to the node. In other simulations the total trust might be higher or lower, depending on how long the node stays in the same situation.

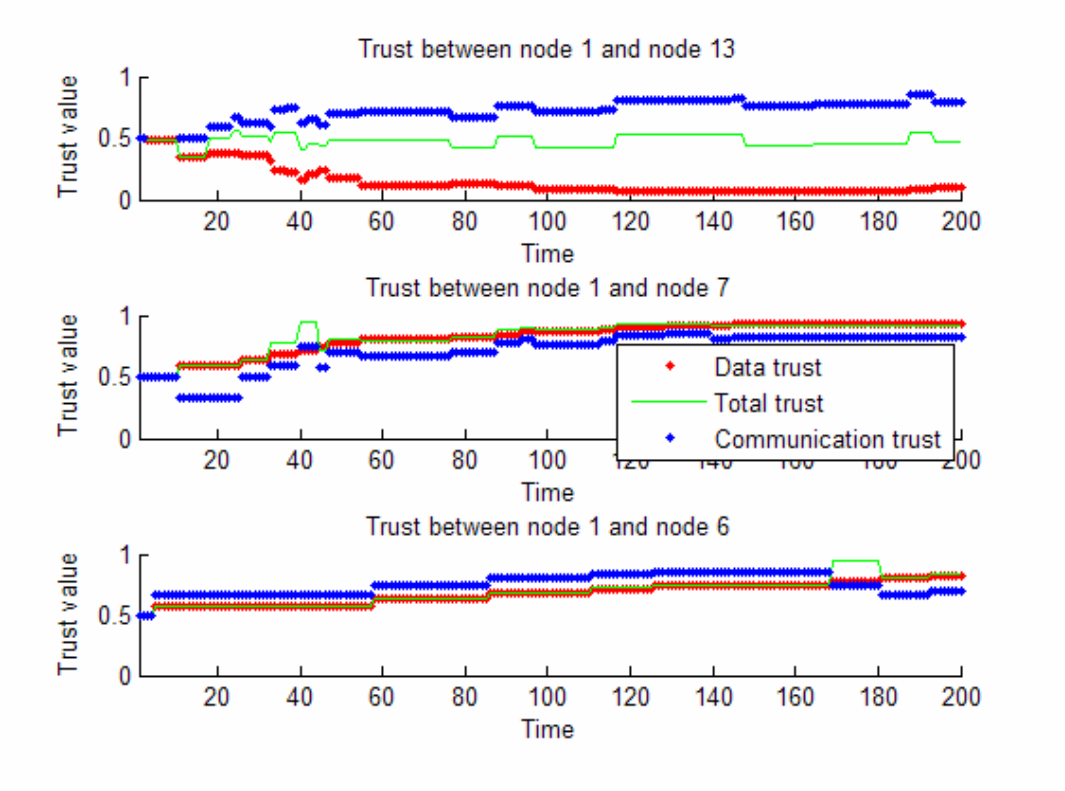

Figure 6.10. Node 13 is faulty (data error)

6.3.3. All nodes have a communication error

Figure 6.11 below shows the results when nodes are not routing messages. It explains the situation when there is a communication error but there is no data error, that is, all nodes are reporting their sensed data, but not routing messages for other nodes. As can be seen, the communication trust value for all nodes is decreasing towards the value of zero, while the data trust value is increasing towards the value of one. The total trust is again in the reasonable range, around the initial assigned value, which is better than being completely trusted or distrusted.

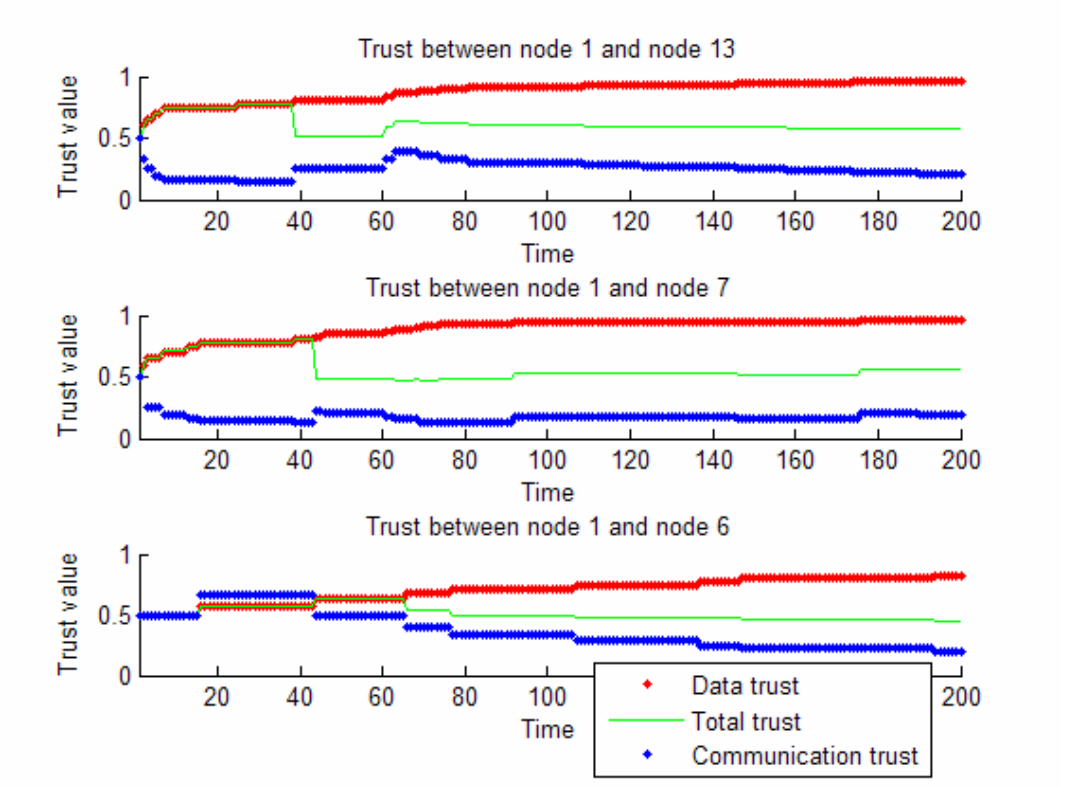

Figure 6.11. All nodes have a communication error

6.3.4. All nodes with communication error and node 13 has also a data error

Figure 6.12 below explains when there is a communication error between all nodes and a data error in node 13, that is, all nodes are not routing messages and node 13 is also not reporting its sensed data properly. As can be seen from Figure 6.12, the communication trust value for all nodes is decreasing towards the value of zero, the data trust values for node 7 and node 6 are increasing towards the value of one, and the total trust value is around the initial assigned trust value. The interesting case here is that, for node 13, the communication trust value and the data trust value are decreasing towards the value of zero and this is also the case for the total trust value.

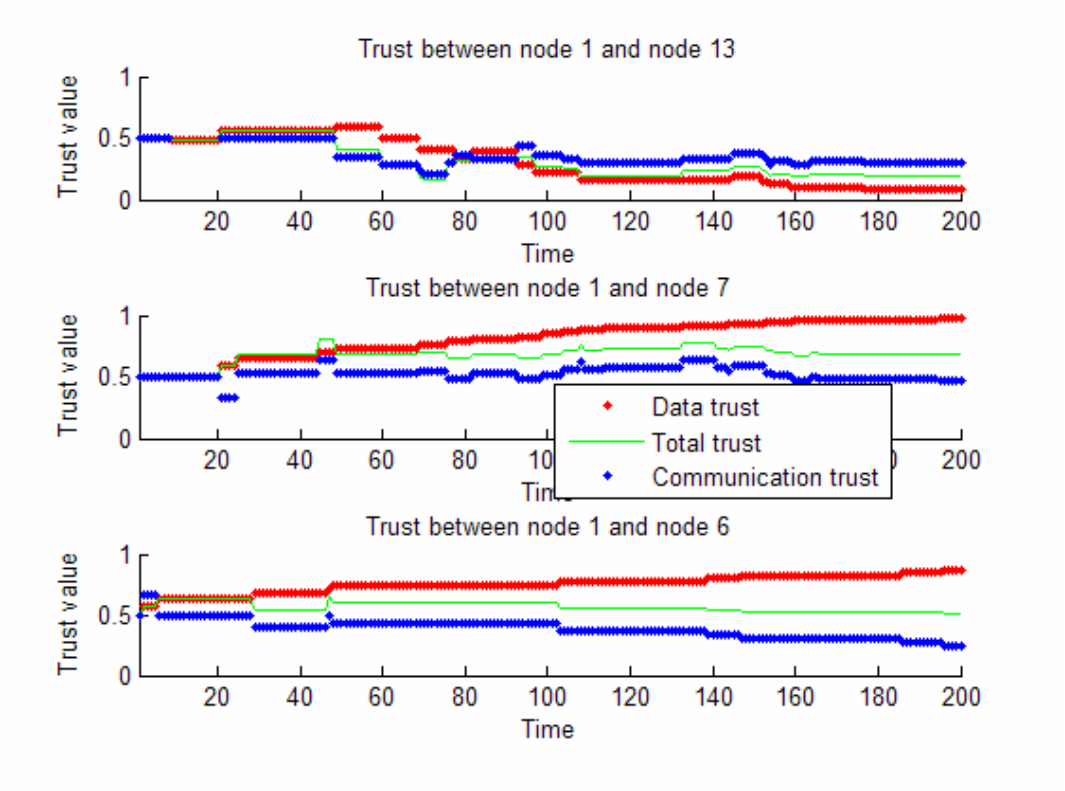

Figure 6.12. All nodes have a communication error and node 13 has also a data error

In summary and as can be seen from the above illustrations, it has been proven that nodes in a WSN can be trusted from a communication point of view but distrusted from a data point of view, and vice versa. In other words, the node can be trusted and distrusted at the same time if only one trust component is considered. Therefore a new Bayesian fusion algorithm is introduced to combine both trust values – data trust and communication trust – and to produce the total trust which defines the node as a trusted or distrusted node.

6.4. Conclusion

It has been argued that using one trust component to decide on the trustworthiness of nodes in WSNs is not enough and can mislead the network. Therefore, more than one component should be considered when deciding on trust. So the two different trust components, the data trust and the communication trust, were reconsidered and a simulation comparison between them was conducted. It has been proven that a trusted node from the data point of view can be distrusted from a communication point of view and vice versa. This led to the extension of the trust computational model in WSNs introduced in Chapter 5 to reflect the new challenges and to include both trust components – data trust and communication trust – as decisive factors regarding the trustworthiness of nodes.

This chapter has also presented a new Bayesian fusion algorithm to combine both trust components. The algorithm is generic and allows more components to be added to and/or deleted from very smoothly and transparently. The simulation results for the newly introduced algorithm show that, if a node is trusted on one component and distrusted on the other component, then the combined trust value will be around the initially assigned trust value. In other words, one trust component by itself cannot fully decide on the trustworthiness of nodes in WSNs. The results have also demonstrated that the node is very trustworthy if it is trusted by both components at the same time and, vice versa, the node is very untrustworthy if it is distrusted by both components.

7. Conclusions and Future Work

It has been argued that existing security measures are not enough to solve all the problems encountered in WSNs, due to their unattended high-volume deployments, mainly in difficult and hostile environments, which forces the sensor nodes to be of low cost and which in turn prevents the implementation of sophisticated security mechanisms. Power constraints and the short-range communication capability characteristics of sensor nodes force them to apply multi-hop routing to finish a task, which, as a result, forces cooperation between nodes. As there is no guarantee that all nodes in the discovered route are capable of cooperating or willing to do so, new mechanisms should be introduced to address these problems. A few approaches have been proposed to solve these problems, but none of them has been able to solve the problem entirely, necessitating the development and introduction of trust and reputation systems, and this is the core contribution of this thesis.

Initially, this work has explained the difference between trust and security and stated that even though they are sometimes used interchangeably to describe a secure system, trust is not the same as security. The difference between reputation and trust has also been discussed and it has been stated that the former only

partially affects the latter, which means that, based on reputation, a level of trust is bestowed upon an entity.

A concise and closely related survey of the state of the art trust-based systems in different domains – social sciences and e-commerce, distributed and peer-to-peer networks, ad-hoc networks and wireless sensor networks – has also been presented, showing the methodology used to formulate trust in each model, as an essential attribute in establishing a relationship between entities. The way in which the trust-updating process is achieved has also been discussed and summarised. The survey has also shown that, even though researchers have started to explore the issue of trust in WSNs, they are still following almost the same approaches used by researchers in other fields to model trust; examining the issue of trust from a binary communication point of view (routing). This is in contrast to our research, which has taken into consideration not only the communication side but also the data side (continuous sensed parameters), which is a unique characteristic of sensor networks and has never been addressed by trust researchers in WSNs. Every field has examined modelling and calculating trust using different techniques, and one of the most prominent and promising techniques is the use of statistics, mainly probabilities, to solve the uncertainty problem, especially in dynamic networks such as WSNs, where the topology is changing very rapidly.

A summary of all trust properties – definitions, classifications, characteristics and values from different domains – has been discussed and extended to reflect those properties of trust in WSNs as a prerequisite to understanding the notion of trust.

It has been stated that a formal and proper trust in WSNs does not exist as such, so few definitions of trust have been presented. That is to say that WSNs can accommodate different trust definitions in different implementations, based on the application and the deployed environment. The relationships among trust construct models in WSNs have been defined and a trust typology in WSNs has also been presented as the key to moving the research on trust forward with the introduction of two new constructs specific to WSNs. This typology will help researchers and developers to build an effective trust relationship model between nodes in such networks and will lead to the advancement of the research in this area. Trust characteristics in WSNs have also been discussed and the possible discrete/continuous values that can be assigned to trust in WSNs have been presented.

Modelling trust requires a thorough understanding of the dynamic aspects of trust and the factors affecting trust. Those two topics have been introduced and the main factors of trust — direct trust, indirect trust, reputation and risk — have been briefly discussed, with more attention given to the direct and indirect trust as the most important factors, which can produce the other factors. Dynamic aspects of trust — trust formation, trust-updating and trust revocation — have also been presented, with considerable attention being paid to the trust formation process as the most important aspect. A new risk assessment algorithm for establishing trust between nodes, based on the nodes' QoS characteristics, which have been categorised by nodes themselves into different categories, based on their own criteria and the scenario in which they find themselves, has also been presented. The algorithm presented here represents a new framework for establishing trust in

WSNs and calculating the risk the node is required to take in case the trust value is not enough to perform the task. The algorithm assumes that direct trust values, indirect trust values and the required trust are given or already calculated by the node, and still uses the traditional weighting approach to calculate the combined trust, with the introduction of a new approach to weight the direct and indirect trust using the Beta distribution, due to its simplicity and flexibility. This has been developed further to adopt the new techniques unique to WSNs. Preliminary simulation results have also been presented, simply showing the trust relationship between nodes and the risk associated with them. The results have been presented in tables and in graphic format for easy observation and interpretation, showing that, the higher the trust between nodes, the lower the risk between them, and vice versa. The model is simple, flexible and easy to be implemented, as can be seen from the simulation results in Chapter 4.

We have argued that the trust-modelling problem is characterised by uncertainty, and the only coherent way to deal with uncertainty is through probability. Even though some of the trust models introduced for sensor networks employ probabilistic solutions mixed with ad-hoc approaches, none of them produces a full probabilistic answer to the problem. In this thesis we introduced a theoretical sound Bayesian probabilistic approach for modelling trust and reputation in WSNs, based on sensed continuous data to address security issues and to deal with malicious and unreliable nodes. It is a statistical answer to problems to which encryption and cryptography keys fail to provide a complete solution. We have extended the Beta Reputation System, which deals with binary, discrete data, to the case of continuous sensor data, and have presented a Gaussian trust model and

a reputation system for wireless sensor networks (GTRSSN). In doing so, we introduced a Bayesian probabilistic approach for incorporating the second-hand information from neighbouring nodes, with directly observed information, and have shown that this leads to a highly reliable network with fast response to emerging attacks from malicious nodes.

The simulation results have shown the implications of sensor data for the direct and indirect trust relationship between nodes, which helps to distinguish among nodes and purge the bad nodes from the network. The trust system works on the assumption that a majority of nodes in a neighbourhood are reliable. This principle helps purge the system of bad elements.

Finally, we have argued that using one trust component to decide on the trustworthiness of nodes in WSNs is not enough and can mislead the network. Therefore, more than one component should be considered when deciding on trust. A thorough analysis of trust components – the data trust and the communication trust – was conducted and it has been proven that a trustworthy node from the data point of view can be untrustworthy from the communication point of view and vice versa. That is, if the overall trust is based on just the communication trust, then this might mislead the network, and untrustworthy nodes in terms of sensed data can be classified as trusted nodes due to their communication capabilities. This led to further extending our trust computational model for WSNs and to the proposal of a new Bayesian fusion algorithm to combine both trust components. The simulation results for the newly introduced algorithm have shown that, if a node is trusted on one component and distrusted

on the other component, then the combined trust value will be around the initially assigned trust value. In other words, one trust component by itself cannot fully decide on the trustworthiness of nodes in WSNs. The results have also demonstrated that the node is very trustworthy if it is trusted by both components at the same time and, vice versa, the node is very untrustworthy if it is distrusted by both components.

In summary, the main contributions of our research are follows:

- Surveying the trust models in different domains, with more attention given to trust models in ad-hoc and sensor networks.
- A detailed illustration of all trust properties in WSNs (trust definitions, trust classification, trust characteristics, trust values) as prerequisites to understanding trust.
- Proposing a new risk assessment algorithm to weight and combine trust from direct and indirect sources using the Beta probability distribution.
- Presenting a Bayesian probabilistic reputation system and trust model for WSNs to calculate and continuously update trust values between nodes in WSNs based on the sensed events.
- Proposing a new Bayesian fusion algorithm to combine different trust components and to produce the overall trust between nodes in different scenarios.

Future Research Directions

In the future, we are planning to extend our work and develop new algorithms for the other dynamic aspects of trust (revocation of trust). In other words, we will address the issue of how to decide on the deletion or keeping of sensor nodes in a network, which is a decision problem under uncertainty, and so far has been handled through a simple threshold. We are also going to introduce the time evolution of trust. That is, trust is dynamic and it can increase or decrease by time, as mentioned before, and the effect of the old trust value between nodes will be introduced as a new trust component as it is not being introduced in our models. We will also try to map the trust network model to a Bayesian network (BN) model. This will address the issue of how other nodes in the network (not directly connected to a specific node) influence its trust relationship with other nodes. A BN in general is a relationship network that uses statistical methods to represent probability relationships between different nodes. It is a compact representation of the joint probability distribution for reasoning under uncertainty. BNs provide a flexible method to present differentiated trust and combine different aspects of trust [68, 153, 154]. They represent a probabilistic framework with sound theoretical foundation, Bayes' rule is the theoretical foundation of BNs, and also represent a computational feasibility for use in real time [155]. Variables can be represented as discrete nodes and/or continuous nodes, which is a good representation of communication trust and data trust in WSNs.

We will also try to implement our designed model in different scenarios, with more trust components added to the model. We are planning to combine the trust

problem and the drift problem in WSNs and design a new model to distinguish between the two problems. The final stage will be the implementation of our designed models in a live sensor network and, if possible, commercialisation of the models.

In summary, the future research directions are as follows:

- Develop new algorithms for the other dynamic aspects of trust (revocation of trust values and excluding nodes from the network).
- Introducing the time evolution of trust as a new trust component (how trust is affected by time).
- Mapping the developed trust network model to a Bayesian network model to address the issue of how other nodes not directly connected to each other can influence their trust relationship with other nodes.
- Combine the trust problem and the drift problem in WSNs and design a new model to distinguish between the two problems.
- Implementation of our designed models in a live sensor network and, if possible, commercialisation of the designed models.

Appendix A. Bayes Theorem

Bayes' theorem is a theorem of probability and was developed by the Reverend Thomas Bayes, an 18th century mathematician and theologian and was first published in 1763. Bayesian inference is the most widely used probability based on reasoning; it utilises the prior knowledge of an event in order to make a posterior inference of that event, and has been used in a wide variety of contexts. The probability of an event *H* conditional on another event *E* is generally different from the probability of *E* conditional on *H*. However, there is a definite relationship between the two, and Bayes' theorem is the statement of that relationship [156]. Bayes' theorem tells how to update or revise beliefs in light of new evidence and relates the conditional and marginal probabilities of events *H* and *E* [157]. Mathematically it is expressed as shown in equation (A.1):

$$P(H \mid E) = \frac{P(E \mid H)P(H)}{P(E)} \qquad \text{(A.1)}$$

where:

- $P(H)$ is the prior probability of *H*. It does not take into account any information about *E*.

- $P(E)$ is the prior probability of evidence *E,* it is independent from *H* and can be regarded as a normalizing or scaling factor.
- $P(H \mid E)$ is the posterior probability of *H* given the evidence *E*.
- $P(E \mid H)$ is the probability of observing E given *H* (the likelihood function).

The posterior probability is the product of the likelihood function and the prior probability. The denominator operates a normalisation constant to make the posterior as a valid probability function. In other words, the theorem can be written as:

Posterior = (Likelihood * Prior) / (Normalising constant)

It is important to note that all of these probabilities are conditional. They specify the degree of belief in some proposition or propositions based on the assumption that some other propositions are true. As such, the theory has no meaning without prior resolution of the probability of these antecedent propositions.

To derive the theorem, let us consider the conditional probability of event *H* given event *E* and the probability of event *E* given event *H*.

$$P(H \mid E) = \frac{P(H, E)}{P(E)} \qquad \text{(A.2)}$$

Likewise,

$$P(E \mid H) = \frac{P(H,E)}{P(E)} \tag{A.3}$$

Combining and rearranging equations (A.2) and (A.3), we obtain equation (A.4):

$$P(H,E) = P(H \mid E) * P(E) = P(E \mid H) * P(E) \tag{A.4}$$

From equation (A.4), we obtain Bayes' theorem as shown in equation (A.5):

$$P(H \mid E) = \frac{P(E \mid H)P(H)}{P(E)} \tag{A.5}$$

Bayes' theorem can be extended to solve problems with more than two variables. For example:

$$P(T \mid D,C) = \frac{P(T \mid D) * P(T \mid C) * P(D)}{P(D \mid C) * P(T)} \tag{A.6}$$

This can be derived in several steps from Bayes' theorem and the definition of conditional probability as discussed in Chapter 6. The general strategy is to work with a decomposition of the joint probability, and to marginalize the variables that are not of interest.

References

[1] S. Marsh and J. Meech, *Trust in Design*. The Hague, The Netherlands ACM Press, 2000.

[2] M. Bohge and W. Trappe, "An Authentication Framework for Hierarchical Ad-hoc Sensor Networks", in *2003 ACM Workshop Wireless security (WiSe '03)*, San Diego, CA, USA, 2003.

[3] C. Karlof and D.Wagner, "Secure Routing in Sensor Networks: Attacks and Countermeasures", in *First IEEE International Workshop on Sensor Network Protocols and Applications*, 2003.

[4] C. Karlof, N. Sastry and D. Wagner, "TinySec: A Link Layer Security Architecture for Wireless Sensor Network ", in *Proceedings of the 2nd International Conference on Embedded Networked Sensor Systems*, Baltimore, MD, USA, 2004.

[5] A. Perrig, R. Zewczyk, V. Wen, D. Culler and D. Tygar, "SPINS: Security Protocols for Sensor Networks", *Wireless Networks*, vol. 8, pp. 521-534, 2002.

[6] F. Ye, H. Luoa, S. Lu and L. Zhang, "Statistical En-route Filtering of Injected False Data in Sensor Networks", *Selected Areas in Communications of the ACM*, vol. 23, 2005.

[7] Y. Zhang, W. Liu, W. Lou and Y. Fang, "Location-based Compromise Tolerant Security Mechanisms for Wireless Sensor Networks", *IEEE Journal on Selected Areas in Communications*, vol. 24, pp. 247-260, 2006.

[8] D. Zhou, "Security Issues in Ad-hoc Networks", in *The Handbook of Ad-hoc Wireless Networks* Boca Raton, FL, USA: CRC Press, Inc. , 2003, pp. 569 - 582.

[9] A. Falchi, "Sensor networks: Performance measurements with motestechnology ", in *Dept. of Information Engineering*, vol. Master's thesis: University of Pisa, 2004.

[10] A. Bharathidasan and V. A. S. Ponduru, "Sensor Networks: An Overview", Technical Report, " *Dept. of Computer Science, University of California at Davis* 2002.

[11] M. Tubaishat and S. Madria, "Sensor networks: an overview", *IEEE Potentials*, vol. 22, pp. 20-23, 2003.

[12] I. F. Akyildiz, Y. S. W. Su and E. Cayirci, " Wireless Sensor Networks: a Survey", *Computer Networks*, vol. 38, pp. 393-422, 2002.

[13] V. Rajaravivarma, Y. Yang and T. Yang, "An Overview of Wireless Sensor Network and Applications ", in *The 35th Southeastern Symposium on System Theory*, 2003.

[14] G.Werner-Allen, K. Lorincz, M. Ruiz, O. Marcillo, J. Johnson, J. Lees and M. Welsh, "Deploying a Wireless Sensor Network on an Active Volcano", *IEEE Internet Computing*, 2005.

[15] G. Werner-Allen, J. Johnson, M. Ruiz, J. Lees and M. Welsh, "Monitoring Volcanic Eruptions with a Wireless Sensor Network", in *Second European Workshop on Wireless Sensor Networks (EWSN05)*, Istanbul, Turkey, 2005.

[16] D. Culler, D. Estrin and M. Srivastava, "Overview of Sensor Networks", *IEEE Computer Journal*, vol. 37, pp. 41-49, 2004.

[17] S. D. Glaser, "Some Real-world Applications of Wireless Sensor Nodes", in *Proceedings of the SPIE Symposium on Smart Structures and Materials NDE*, San Diego, CA, USA, 2004.

[18] J. Paek, O. Gnawali, K.-Y. Jang, D. Nishimura, R. Govindan, J. Caffrey, M. Wahbeh and S. Masri, "A Programmable Wireless Sensing System forStructural Monitoring", in *The 4th World Conference on Structural Control and Monitoring (4WCSCM)*, San Diego, CA, 2006.

[19] T. Gao, D. Greenspan, M. Welsh, R. Juang and A. Alm, "Vital Signs Monitoring and Patient Tracking over a Wireless Network", in *The 27th Annual International Conference of the Engineering in Medicine and Biology Society (IEEE-EMBS '05)*, 2005.

[20] E. Yoneki and J. Bacon, "A Survey of Wireless Sensor Network Technologies: Research Trends and Middlewares Role", *Computer Laboratory, University of Cambridge* Sept. 2005.

[21] E. H. Callaway, *Wireless sensor networks : architectures and protocols*. Boca Raton, Florida CRC Press LLC, 2004.

[22] Y. Wang, G. Attebury and B. Ramamurthy, "A Survey of Security Issues in Wireless Sensor Networks", *IEEE Communications Surveys and Tutorials*, vol. 8, pp. 2-23, 2006.

[23] F. Stajano and R. Anderson, "The Resurrecting Duckling: Security Issues for Ad-hoc Wireless Networks", in *The 8th International Workshop on Security Protocols, Lecture Notes in Computer Science*, Springler-Verlag, Berlin, Germany, 1999.

[24] A. Perrig, J. Stankovic and D. Wagner, "Security in Wireless Sensor Networks", *Communications of the ACM*, vol. 47, pp. 53-57, 2004.

[25] H. Chan and A. Perrig, "Security and Privacy in Sensor Networks", *IEEE Computer Journal*, vol. 36, pp. 103-105, 2003.

[26] T. Zia and A. Zomaya, "Security Issues in Wireless Sensor Networks", in *International Conference on Systems and Networks Communication (ICSNC '06),* , Tahiti, French Polynesia 2006.

[27] J. Newsome, E. Shi, D. Song and A. Perrig, "The Sybil Attack in Sensor Networks: Analysis & Defenses", in *The 3rd International Symposium on Information Processing in Sensor Networks*, NewYork, 2004.

[28] J. P. Walters, Z. Liang, W. Shi and V. Chaudhary, "Wireless Sensor Network Security: A Survey", in *Security in Distributed, Grid, and Pervasive Computing*, Y. Xiao, Ed.: Auerbach Publications, CRC Press, 2006.

[29] P. Papadimitratos and Z. J. Haas, "Securing Mobile Ad-hoc Networks", in *The Handbook of Ad-hoc Wireless Networks*: CRC Press LLC, 2003.

[30] L. Zhou and Z. J. Haas, "Securing Ad-hoc Networks", *IEEE Network Magazine*, 1999.

[31] B. Przydatek, D. Song and A. Perrig, "SIA: Secure Information Aggregation in Sensor Networks", in *The 1st International Conference on Embedded Networked Sensor Systems* Los Angeles, California, USA 2003.

[32] S. Zhu, S. Setia and S. Jajodia, "LEAP: Efficient Security Mechanisms for Large-Scale Distributed Sensor Networks", in *The 10th ACM Conference*

on Computer and Communications Security, Washington D.C., USA, 2003.

[33] W. Zhang and G. Cao, "Group Rekeying for Filtering False Data in Sensor Networks: A Predistribution and Local Collaboration-based Approach", in *The 24th Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM '05)*, Miami, USA, 2005.

[34] Z. Liu, A. W. Joy and R. A. Thompson, "A Dynamic Trust Model for Mobile Ad Hoc Networks", in *Distributed Computing Systems, 2004. FTDCS 2004.*, 2004.

[35] A. A. Pirzada and C. McDonald, "Establishing Trust in Pure Ad-hoc Networks", in *The 27th Australasian Conference on Computer Science*, Dunedin, New Zealand, 2004.

[36] D. H. McKnight and N. L. Chervany, "The Meanings of Trust": MIS Research Center, Carlson School of Management, University of Minnesota, 1996.

[37] S. Ba and P. A. Pavlou, "Evidence of the Effect of Trust Building Technology in Electronic Markets: Price Premiums and Buyer Behavior", *MIS Quarterly*, vol. 26, pp. 243-268, 2002.

[38] P. Dasgupta, "Trust as a Commodity", in *Trust: Making and Breaking Cooperative Relations*, vol. electronic edition, D. Ingram, Ed.: Department of Sociology, University of Oxford, 2000, pp. 49-72.

[39] D. H. McKnight, L. L. Cummings and N. L. Chervany, "Trust Formation in new Organaizational Relationships": MIS Research Center, Carlson School of Management, University of Minnesota, 1996.

[40] P. Resnick, K. Kuwabara, R. Zeckhauser and E. Friedman, "Reputation systems", *Communications of the ACM*, vol. 43, pp. 45-48, 2000.

[41] D. H. McKnight and N. L. Chervany, "Conceptualizing Trust: A Typology and E-Commerce Customer Relationships Model", in *The 34th Hawaii International Conference on System Sciences*, 2001.

[42] K. Aberer and Z. Despotovic, "Managing Trust in a Peer-2-Peer Information System", in *The Tenth International Conference in Information and Knowledge Management*, Atlanta, Georgia, USA 2001.

[43] M. Blaze, J. Feigenbaum, J. Ioannidis and A. Keromytis, "The KeyNote Trust Management System", *University of Pennsylvania* 1999.

[44] L. Xiong and L. Liu, "A Reputation-based Trust Model for Peer-to-Peer E-Commerce Communities", in *IEEE International Conference on E-Commerce Technology (CEC '03)* 2003, pp. 275-284.

[45] M. Blaze, J. Feigenbaum and J. Lacy, "Decentralized Trust Managament", in *IEEE Symposium on Security and Privacy*, 1996.

[46] R. Chen and W. Yeager, "Poblano: A Distributed Trust Model for Peer-to-Peer Networks", *Sun Microsystems* 2001.

[47] L. Eschenauer, "On Trust Establishment in Mobile Ad-hoc Networks", in *Department of Electrical and Computer Engineering*, vol. Master of Science: University of Maryland, College Park, 2002, pp. 45.

[48] J. S. Baras and T. Jiang, "Dynamic and Distributed Trust for Mobile Ad-hoc Networks", *University of Maryland*, Orlando, Florida, USA 2004.

[49] Z. Liu, A. W. Joy and R. A. Thompson, "A Dynamic Trust Model for Mobile Ad-hoc Networks", in *The 10th IEEE International Workshop on Future Trends of Distributed Computing Systems (FTDCS '04)*, 2004.

[50] C. R. Davis, "A Localized Trust Management Scheme for Ad-hoc Networks", in *The 3rd International Conference on Networking (ICN '04)*, 2004.

[51] S. Buchegger and J. Y. L. Boudec, "Performance analysis of the CONFIDANT protocol (Cooperation Of Nodes- Fairness In Dynamic Ad-hoc NeTworks)", in *The 3rd ACM Internationa symposium Mobile Ad-hoc Networking & Computing (MobiHoc '02)*, Lausanne, CH, 2002.

[52] P. Michiardi and R. Molva, "CORE: A Collaborative Reputation Mechanism to Enforce Node Cooperation in Mobile Ad-hoc Networks", in *The IFIP TC6/TC11 Sixth Joint Working Conference on Communications and Multimedia Security: Advanced Communications and Multimedia Security* Portoroz, Slovenia, 2002.

[53] L. Capra, "Towards a Human Trust Model for Mobile Ad-hoc Networks", in *The 2nd UK-UbiNet Workshop*, Cambridge University, Cambridge, UK, 2004.

[54] G. D. M. Serugendo, "Trust as an Interaction Mechanism for Self-Organising Systems", in *International Conference on Complex Systems (ICCS '04)*, Marriott Boston Quincy, Boston, MA, USA, 2004.

[55] S. Ganeriwal and M. B. Srivastava, "Reputation-based Framework for High Integrity Sensor Networks", in *The 2nd ACM Workshop on Security of Ad-hoc and Sensor Networks* Washington DC, USA 2004.

[56] A. Srinivasan, J. Teitelbaum and J. Wu, "DRBTS: Distributed Reputation-based Beacon Trust System", in *The 2nd IEEE International Symposium on Dependable, Autonomic and Secure Computing (DASC '06)*, 2006.

[57] S. Ganeriwal, L. K. Balzano and M. B. Srivastava, "Reputation-based Framework for High Integrity Sensor Networks", *ACM Transactions on Sensor Networks*, vol. v, 2007.

[58] J. Scott, *Social Network Analysis: A Handbook*, 2nd edition ed. Newberry Park, CA: Sage Publications, 2000.

[59] S. Ries, J. Kangasharju and M. M¨uhlh¨auser, "A Classification of Trust Systems", in *On the Move to Meaningful Internet Systems*, vol. 4277, *Lecture Notes in Computer Science*. Berlin / Heidelberg: Springer, 2006, pp. 894-903.

[60] A. Abdul-Rahman and S. Hailes, "Supporting Trust in Virtual Communities", in *The 33rd Hawaii International Conference on System Sciences*, Maui, Hawaii, 2000.

[61] A. Jøsang and R. Ismail, "The Beta Reputation System", in *The 15th Bled Electronic Commerce Conference*. Bled, Slovenia, 2002.

[62] J. Sabater and C. Sierra, "REGRET: A Reputation Model for Gregarious Societies", in *The Fifth International Conference on Autonomous Agents* Montreal, Quebec, Canada 2001.

[63] C. Jonker and J. Treur, "Formal Analysis of Models for the Dynamics of Trust based on Experiences", in *The 9th European Workshop on Modelling Autonomous Agents in a Multi-Agent World: MultiAgent System Engineering*, Valencia, Spain, 1999.

[64] Catholijn M. Jonker, J. J. P. Schalken, J. Theeuwes and J. Treur, "Human Experiments in Trust Dynamics", in *The Second International Conference on Trust Management (iTrust '04)*, Oxford, UK, 2004.

[65] C. Castelfranchi, R. Falcone and G. Pezzulo, "Integrating Trustfulness and Decision Using Fuzzy Cognitive Maps", in *The First International Conference on Trust Management (iTrust '03)*. Heraklion, Crete, Greece, 2003, pp. 195-210.

[66] C. Castelfranchi and R. Falcone, "Trust is Much More Than Subjective Probability: Mental Components and Sources of Trust", in *The 33rd Hawaii International Conference on System Sciences*, 2000.

[67] S. Barber and J. Kim, "Belief Revision Process based on Trust: Agents Evaluating Reputation of Information Access", in *Trust in Cyber-societies, Lecture Notes in Computer Science*, 2001.

[68] Y. Wang and J. Vassileva, "Bayesian Network-Based Trust Model", in *The International Conference on Web Intelligence (WI '03)*, Halifax, Canada, 2003.

[69] Y. Wang and J. Vassileva, "Bayesian Network Trust Model in Peer-to-Peer Networks", in *Agents and Peer-to-Peer Computing*, vol. 2872, *Lecture Notes in Computer Science*. Berlin, Heidelberg: Springer 2005, pp. 23-34.

[70] Y. Wang and J. Vassileva, "Trust and Reputation Model in Peer-to-Peer Networks", in *The 3rd International Conference on Peer-to-Peer Computing* Linköping, Sweden, 2003.

[71] F. Stajano and R. Anderson, "The Resurrecting Duckling: Security Issues for Ad-hoc Wireless Networks", in *Security Protocols*, vol. 1796. Berlin / Heidelberg: Springer, 2000, pp. 172-182.

[72] D. Balfanz, D. K. Smetters, P. Stewart and H. C. Wong, "Talking to Strangers: Authentication in Ad-hoc Wireless Networks", in *Symposium on Network and Distributed Systems Security (NDSS '02)*, San Diego, California, 2002.

[73] V. Cahill, E. Gray, J.-M. Seigneur, C. D. Jensen, Y. Chen, B. Shand, N. Dimmock, A. Twigg, J. Bacon, C. English, W. Wagealla, S. Terzis, P. Nixon, G. Di Marzo Serugendo, C. Bryce, M. Carbone, K. Krukow and M. Nielson, "Using Trust for Secure Collaboration in Uncertain Environments ", *IEEE Pervasive Computing*, vol. 2, pp. 52-61, 2003.

[74] M. Carbone, M. Nielsen and V. Sassone, "A Formal Model for Trust in Dynamic Networks", in *First International Conference on Software Engineering and Formal Methods (SEFM '03)*, Brisbane, Australia, 2003.

[75] B. N. Shand, "Trust for Resource Control: Self-enforcing Automatic Rational Contracts between Computers", *University of Cambridge Computer Laboratory* UCAM-CL-TR-600, 2004.

[76] S. Weeks, "Understanding Trust Management Systems", in *The 2001 IEEE Symposium on Security and Privacy* Oakland, California, USA, 2001.

[77] A. Abdul-Rahman and S. Hailes, "A Distributed Trust Model", in *The 1997 Workshop on New Security Paradigms*, Langdale, Cumbria, United Kingdom 1997.

[78] Y. Wang and V. Varadharajan, "Trust^2: Developing Trust in Peer-to-Peer Environments", in *The 2005 IEEE International Conference on Services Computing*, Orlando, Florida, USA, 2005.

[79] Y. Wang and V. Varadharajan, "Two-phase Peer Evaluation in P2P E-commerce Environments", in *The 2005 IEEE International Conference on e-Technology, e-Commerce and e-Service (EEE '05)*, Hong Kong, 2005.

[80] M. Kinateder, E. Baschny and K. Rothermel, "Towards a Generic Trust Model - Comparison of various Trust Update Algorithms", in *The Third International Conference on Trust Management (iTrust '05)*, Rocquencourt, France, 2005.

[81] F. Azzedin and M. Maheswaran, "Evolving and Managing Trust in Grid Computing Systems", in *IEEE Canadian Conference on Electrical and Computer Engineering (CCECE '02)*, 2002.

[82] W. Song and V. V. Phoha, "Neural Network-Based Reputation Model in a Distributed System", in *The IEEE International Conference on E-Commerce Technology* San Diego, California, USA, 2004.

[83] H. Baohua, H. Heping and L. Zhengding, "Identifying Local Trust Value with Neural Network in P2P Environment", in *The First IEEE and IFIP International Conference in Central Asia on Internet*, Bishkek, Kyrgyz Republic, 2005.

[84] E. Kotsovinos and A. Williams, "BambooTrust: Practical Scalable Trust Management for Global Public Computing", in *The 2006 ACM Symposium on Applied Computing*, Dijon, France 2006.

[85] B. Dragovic, E. Kotsovinos, S. Hand and P. R. Pietzuch, "XenoTrust: Event-Based Distributed Trust Management", in *The 14th International Workshop on Database and Expert Systems Applications* Prague, Czech Republic, 2003.

[86] B. Shand, N. Dimmock and J. Bacon, "Trust for Ubiquitous, Transparent Collaboration", *Wireless Networks*, vol. 10, pp. 711-721, 2003.

[87] D. Quercia, S. Hailes and L. Capra, "B-trust: Bayesian Trust Framework for Pervasive Computing", in *iTrust 2006 - 4th International Conference on Trust Management*, Pisa, Italy, 2006.

[88] S. Buchegger and J. Y. L. Boudec, "Coping with False Accusations in Misbehavior Reputation Systems for Mobile in Ad-hoc Networks", *EPFL-IC-LCA*, Lausanne, Switzerland IC/2003/31, 2003.

[89] S. Buchegger and J. Y. L. Boudec, "The Effect of Rumor Spreading in Reputation Systems for Mobile Ad-hoc Networks ", in *Modeling and Optimization in Mobile Ad-hoc and Wireless Networks (WiOpt '03)*, INRIA Sophia-Antipolis, France, 2003.

[90] S. Buchegger and J.-Y. L. Boudec, " A Robust Reputation System for Peer-to-Peer and Mobile Ad-hoc Networks", in *P2PEcon '04*, Harvard University, Cambridge MA, U.S.A, 2004.

[91] S. Buchegger, C. Tissieres and J. Y. L. Boudec, "A Test-Bed for Misbehavior Detection in Mobile Ad-hoc Networks - How Much Can Watchdogs Really Do?" in *The Sixth IEEE Workshop on Mobile Computing Systems and Applications (WMCSA '04)*, English Lake District, UK, 2004.

[92] 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.

[93] G. Theodorakopoulos and J. S. Baras, "Trust Evaluation in Ad-hoc Networks", in *The 3rd ACM Workshop on Wireless Security* Philadelphia, PA, USA 2004.

[94] R. Kindermann and J. L. Snell, "Markov Random Fields and their Applications ", in *American Mathematical Society,*. Providence, Rhode Island, 1980.

[95] S. Marsh, "Formalising Trust as a Computational Concept", in *Departmet of Computer Science and Mathematics*, vol. PhD: University of Stirling, 1994, pp. 184.

[96] Y. L. Sun, W. Yu, Z. Han and K. J. R. Liu, "Information Theoretic Framework of Trust Modelling and Evaluation for Ad-hoc Networks", *IEEE Journal on Selected Areas in Communications*, vol. 24, pp. 305-317, 2006.

[97] K. Ren, T. Li, Z. Wan, F. Bao, R. H. Deng and K. Kim, "Highly Reliable Trust Establishment Scheme in Ad-hoc Networks", *Computer Networks*, vol. 45, pp. 687-699 2004.

[98] C. Zouridaki, B. L. Mark, M. Hejmo and R. K. Thomas, "A Quantitative Trust Establishment Framework for Reliable Data Packet Delivery in MANETs", in *The 3rd ACM Workshop on Security of Ad-hoc and Sensor Networks* Alexandria, VA, USA, 2005.

[99] T. Jiang and J. S. Baras, "Ant-based Adaptive Trust Evidence Distribution in MANET", in *The 24th International Conference on Distributed Computing Systems Workshops (ICDCSW '04)*, Tokyo, Japan, 2004.

[100] D. Liu, P. Ning and W. Du, "Detecting Malicious Beacon Nodes for Secure Location Discovery in Wireless Sensor Networks", in *The 25th IEEE International Conference on Distributed Computing Systems (ICDCS '05)*, 2005.

[101] G. V. Crosby, N. Pissinou and J. Gadze, "A Framework for Trust-based Cluster Head Election in Wireless Sensor Networks", in *The Second IEEE Workshop on Dependability and Security in Sensor Networks and Systems (DSSNS '06)*, Columbia, Maryland, 2006.

[102] J. Hur, Y. Lee, H. Yoon, D. Choi and S. Jin, "Trust Evaluation Model for Wireless Sensor Networks", in *The 7th International Conference on Advanced Communication Technology (ICACT '05)*. Gangwon-Do, Korea, 2005.

[103] H. Chen, H. Wu, X. Zhou and C. Gao, "Reputation-based Trust in Wireless Sensor Networks", in *International Conference on Multimedia and Ubiquitous Engineering (MUE '07)*, Seoul, Korea, 2007.

[104] X.-Y. Xiao, W.-C. Peng, C.-C. Hung and W.-C. Lee, "Using SensorRanks for In-Network Detection of Faulty Readings in Wireless Sensor Networks", in *The 6th ACM International Workshop on Data Engineering for Wireless and Mobile Access* Beijing, China, 2007.

[105] G. V. Crosby and N. Pissinou, "Cluster-based Reputation and Trust for Wireless Sensor Networks", in *The 4th IEEE Consumer Communications and Networking Conference (CCNC '07)* Las Vegas, Nivada, 2007.

[106] M. Krasniewski, P. Varadharajan, B. Rabeler and S. Bagchi, "TIBFIT: Trust Index Based Fault Tolerance for Arbitrary Data Faults in Sensor Networks", in *The 2005 International Conference on Dependable Systems and Networks*, Yokohama, Japan, 2005.

[107] R. A. Shaikh, H. Jameel, S. Lee, S. Rajput and Y. J. Song, "Trust Management Problem in Distributed Wireless Sensor Networks", in *The 12th IEEE international conference on Embedded and Real-Time Computing Systems and Applications (RTCSA '06)* Sydney, Australia, 2006.

[108] Z. Yao, D. Kim, I. Lee, K. Kim and J. Jang, "A Security Framework with Trust Management for Sensor Networks", in *The 1st International Conference on Security and Privacy for Emerging Areas in Communication Networks*, 2005.

[109] K.-S. Hung, K.-S. Lui and Y.-K. Kwok, "A Trust-Based Geographical Routing Scheme in Sensor Networks", in *The IEEE Wireless Communications and Networking Conference (WCNC '07)*, Hong Kong, 2007.

[110] J. Mundinger and J.-Y. L. Boudec, "Reputation in Self-Organized Communication Systems and Beyond", in *The 2006 Workshop on Interdisciplinary Systems Approach in Performance Evaluation and Design of Computer & Communications Sytems*, Pisa, Italy 2006.

[111] R. Ma, L. Xing and H. E. Michel, "Fault-Intrusion Tolerant Techniques in Wireless Sensor Networks", in *The 2nd IEEE International Symposium on Dependable, Autonomic and Secure Computing* 2006.

[112] Q. Zhang, T. Yu and P. Ning, "A Framework for Identifying Compromised Nodes in Sensor Networks", *ACM Transactions on Information and System Security (TISSEC)*, vol. 11, 2008.

[113] Z. Yao, D. Kim and Y. Doh, "PLUS: Parameterized and Localized trUst Management Scheme for Sensor Networks Security", in *The Third IEEE International Conference on Mobile Ad-hoc and Sensor Systems (MASS)*. Vancouver, Canada: IEEE, 2006.

[114] M. Momani, J. Agbinya, G. P. Navarrete and M. Akache, "Trust Classification in Wireless Sensor Networks", in *The 8th International Symposium on DSP and Communication Systems (DSPCS '05)*. Noosa Heads, Queensland, Australia, 2005.

[115] M. Momani, J. Agbinya, G. P. Navarrete and M. Akache, "A New Algorithm of Trust Formation in Wireless Sensor Networks", in *The 1st*

IEEE International Conference on Wireless Broadband and Ultra Wideband Communications (AusWireless '06). Sydney, Australia, 2006.

[116] M. Momani, J. Agbinya, R. Alhmouz, G. P. Navarrete and M. Akache, "A New Framework of Establishing Trust in Wireless Sensor Networks", in *International Conference on Computer & Communication Engineering (ICCCE '06)*. Kuala Lumpur, Malaysia, 2006.

[117] M. Momani, S. Challa and K. Aboura, "Modelling Trust in Wireless Sensor Networks from the Sensor Reliability Prospective", in *Innovative Algorithms and Techniques in Automation, Industrial Electronics and Telecommunications*, T. Sobh, K. Elleithy, A. Mahmoodand M. Karim, Eds.: Springer Netherlands, 2007.

[118] M. Momani, K. Aboura and S. Challa, "RBATMWSN: Recursive Bayesian Approach to Trust Management in Wireless Sensor Networks", in *The Third International Conference on Intelligent Sensors, Sensor Networks and Information*, Melbourne, Australia, 2007.

[119] M. Momani and S. Challa, "GTRSSN: Gaussian Trust and Reputation System for Sensor Networks", in *International Joint Conferences on Computer, Information, and Systems Sciences, and Engineering (CISSE '07)*, University of Bridgeport 2007.

[120] M. Momani, S. Challa and R. Alhmouz, "Can we Trust Trusted Nodes in Wireless Sensor Networks?" in *The International Conference on*

Computer and Communication Engineering (ICCCE '08), Kuala Lumpur, Malaysia, 2008.

[121] D. H. McKnight and N. L. Chervany, "Trust and Distrust Definitions: One Bite at a Time", in *Trust In Cyber-societies* vol. 2246, *Lecture Notes in Computer Science*. Berlin / Heidelberg: Springer, 2001, pp. 27-54.

[122] D. Gambetta, "Can We Trust Trust?" in *Trust: Making and Breaking Cooperative Relations*, D. Gambetta, Ed. Oxford: Basil Blackwell, 1990.

[123] C. English, P. Nixon, S. Terzis, A. McGettrick and H. Lowe, "Dynamic Trust Models for Ubiquitous Computing Environments", in *Ubicomp2002 Security Workshop*, GÖTEBORG, SWEDEN, 2002.

[124] P. Nixon, W. Wagealla, C. English and S. Terzis, "Security, Privacy and Trust Issues in Smart Environments", *University of Strathclyde, Computer and Information Sciences, Smartlab Technical Report* 2004.

[125] L. Capra, "Engineering Human Trust in Mobile System Collaborations", *ACM SIGSOFT Software Engineering Notes* vol. 29, pp. 107 - 116, 2004.

[126] C.-F. HUANG, Y.-C. TSENG and H.-L. WU, "Distributed Protocols for Ensuring Both Coverage and Connectivity of a Wireless Sensor Network", *ACM Trans. Sens. Net*, vol. 3, pp. 24, 2007.

[127] A. Lim, "Support for Reliability in Self-organizing Sensor Networks", in *the Fifth International Conference on Information Fusion*, 2002.

[128] J. Staddon, D. Balfanz and G. Durfee, "Efficient Tracing of Failed Nodes in Sensor Networks", in *First ACM International Workshop on Wireless Sensor Networks and Applications*, Atlanta, GA, NY, 2002.

[129] M. Momani, J. Agbinya, G. P. Navarrete and M. Akache, "A New Algorithm of Trust Formation in Wireless Sensor Networks", in *AusWireless'06*. Sydney, Australia, 2006.

[130] Y. Wang and V. Varadharajan, "Trust^2: Developing Trust in Peer-to-Peer Environments", in *Services Computing, 2005 IEEE International Conference* 2005.

[131] A. Srinivasan, J. Teitelbaum, H. Liang, J. Wu and M. Cardei, "Reputation and Trust-based Systems for Ad-hoc and Sensor Networks", in *Algorithms and Protocols for Wireless Ad-hoc and Sensor Networks*, A. Boukerche, Ed.: Wiley & Sons, 2007.

[132] P. A. Morris, "Bayesian Expert Resolution", in *Department of Engineering-Economic Systems*, vol. Ph.D: Stanford University, 1971.

[133] D. V. Lindley and N. D. Singpurwalla, "Reliability (and fault tree) Analysis using Expert Opinions ", *Journal of the American Statistical Association*, vol. 81, pp. 87-90, 1986.

[134] M. West, "Bayesian aggregation", *Journal of the Royal Staistical Society*, vol. 147, pp. 600-607, 1984.

[135] A. Agah, S. K. Das and K. Basu, "A Game Theory based Approach for Security in Wireless Sensor Networks", in *IEEE International Conference on Performance, Computing, and Communications*, Phoenix, Arizona, 2004.

[136] Y. Liu, C. Comaniciu and H. Man, "A Bayesian game approach for intrusion detection in wireless ad hoc networks", in *Proc. 2006 workshop on Game theory for communications and networks, ACM Int. Conf.*, Pissa, Italy, 2004.

[137] G. Shafer, *A Mathematical Theory of Evidence*: Princeton University Press, 1976.

[138] N. C. Dalkey and O. Helmer, "An Experimental Application of Delphi Method to the Use of Experts", *Management Science*, vol. 9, pp. 458-467, 1963.

[139] P. A. Morris, "Decision Analysis Eexpert Use", *Management Science*, vol. 20, pp. 1233-1241, 1974.

[140] A. P. Dawid, "The Difficulty about Conjunction", *The Statistician*, vol. 36, pp. 91-97, 1987.

[141] C. Genest and M. J. Schervish, "Modelling Expert Judgments for Bayesian Updating", *The Annals of Statistics*, vol. 13, pp. 1198-1212, 1985.

[142] D. V. Lindley, A. Tversky and R. V. Brown, "On the Reconciliation of Probability Assessments", *Journal of Royal Statistical Society*, vol. 142, pp. 146-180, 1979.

[143] S. French, "Updating of Belief in the Light of Someone else's Opinion", *Journal of Royal Statistical Society*, vol. 143, pp. 43-48, 1980.

[144] R. L. Winkler, "The Concensus of Subjective Probability Distributions", *Management Science*, vol. 15, pp. B61-B75, 1968.

[145] D. V. Lindley, "Reconciliation of Probability Distributions", *Operations Research Journal*, vol. 31, pp. 866-880, 1983.

[146] K. Aboura and N. I. Robinson, "Optimal Replacement in a Renewal Process", *CSIRO* DMS-C/D 95/100, 1995.

[147] T. A. Mazzuchi and R. Soyer, "A Bayes Method for Assessing Product Reliability during Development Testing", *IEEE Transactions on Reliability*, vol. 42, pp. 503-510, 1993.

[148] N. D. Singpurwalla, "An Interactive PC-Based Procedure for Reliability Assessment Incorporating Expert Opinion and Survival Data", *Journal of the American Statistical Association*, vol. 83, pp. 43-51, 1988.

[149] K. Aboura, "Bayesian Adaptive Maintenance Plans using Initial Expert Reliability Estimates", *CSIRO* DMS-D 95/64, 1995.

[150] T. A. Mazzuchi and R. Soyer, "Adaptive Bayesian Replacement Strategies", *Bayesian Statistics*, vol. 5, pp. 667-674, 1996.

[151] J. M. van Nortwijk, R. Dekker, R. Cooke and T. A. Mazzuchi, "Expert Judgement in Maintenance Optimization", *IEEE Transactions on Reliability*, vol. 41, pp. 427-432, 1992.

[152] R. Cooke, "Uncertainty in Dispersion and Deposition in Accident Consequence Modelling Assessed with Performance-based Expert judgement", *Reliability Engineering and System Safety*, vol. 45, pp. 35-46, 1994.

[153] F. V. Jensen, *An Introduction to Bayesian Networks*. London: UCL Press Limited, 1996.

[154] F. V. Jensen and Y. D. Nielsen, *Bayesian Networks and Decision Graphs*, Second ed: Springer, 2007.

[155] C. Zhong and P. Y. Li, "Bayesian Belief Network Modeling and Diagnosis of Xerographic Systems", in *The ASME Symposium on Controls and Imaging - IMECE*, 2000.

[156] "Bayes' Theorem", in *http://en.wikipedia.org/wiki/Bayes'_theorem Access date [April, 2006]*.

[157] L. A. Klein, *Sensor and Data Fusion Concepts and Applications*, second ed: SPIE Optical Engineering Press, 1999.