TRANSACTIONS ON EMERGING TELECOMMUNICATIONS TECHNOLOGIES
Trans. Emerging Tel. Tech. 2015; **26**:107–130
Published online 19 June 2013 in Wiley Online Library (wileyonlinelibrary.com). DOI: 10.1002/ett.2674

RESEARCH ARTICLE

Trust management system in wireless sensor networks: design considerations and research challenges

Farruh Ishmanov[1], Aamir Saeed Malik[2], Sung Won Kim[1]* and Bahodir Begalov[3]

[1] Department of Information and Communication Engineering, Yeungnam University, Korea
[2] Department of Electrical and Electronics Engineering, Universiti Teknologi PETRONAS, Malaysia
[3] Department of Information Systems in Economics, Tashkent State University of Economics, Uzbekistan

ABSTRACT

Trust is an important factor in wireless sensor networks (WSNs) in terms of security enhancement and successful collaboration. Trust management (TM) can ensure that all communicating nodes are trustworthy during authentication, authorisation, or key management, which makes traditional security services more robust and reliable. Moreover, by helping to find reliable nodes, TM improves cooperation among nodes, which is vital for improvement of system performance. Trust estimations and management are highly challenging issues because of the unique features and susceptibility of WSNs to different attacks. These factors prevent direct application of schemes suited to other networks and require careful design in a TM system. Hence, our objective is to discuss and present the concept and design factors of TM in WSNs in detail. Moreover, we explore the current state of research as well as open research issues by reviewing proposed trust computation and management schemes in WSNs. Copyright © 2013 John Wiley & Sons, Ltd.

***Correspondence**
S. W. Kim, Department of Information and Communication Engineering, Yeungnam University, Korea.
E-mail: swon@yu.ac.kr

Received 9 December 2012; Revised 24 April 2013; Accepted 14 May 2013

1. INTRODUCTION

The power of wireless sensor networks (WSNs) relies on distributed collaboration among sensor nodes for various tasks, such as event monitoring, relaying data, and so on [1, 2]. Hence, it is important to maintain successful collaboration to maintain network functionality. Successful collaboration is assured only when all nodes operate in a trustworthy manner [3, 4]. Trust management (TM) detects trustworthy and untrustworthy nodes by evaluating them on the basis of their past behaviour/performance. Moreover, it ensures nodes collaborate through rewards and punishment. Because sensor nodes often lack tamper-resistant hardware and are easily compromised, cryptographic solutions cannot assure full protection of the network. Hence, TM improves security by continuously monitoring node behaviour/performance, evaluating the trustworthiness of the nodes and finding trustworthy nodes to collaborate with. Specifically, establishing trust in the network provides many benefits such as the following [5]:

- Trust provides a solution for granting corresponding access control based on the quality of sensor nodes and their services, which cannot be solved through traditional security mechanisms.
- Trust assists routing by providing reliable routing paths that do not contain any malicious, selfish, or faulty nodes.
- Trust makes traditional security more robust and reliable by ensuring that only trustworthy nodes participate in authentication, authorisation, or key management.

Trust management and estimations are highly challenging issues because of the unique features of WSNs, which require customisation of applications suited to other networks. Specifically, because of the following features of WSNs, TM and estimations are challenging.

- Deployed environment and network topology. Sensor nodes are usually deployed in a hostile and unattended environment. Moreover, network topology is dynamic

Copyright © 2013 John Wiley & Sons, Ltd.

in WSNs. These factors cause several complexities for TM. First, hostile environments can cause damage, or at least physically impact, to a sensor node, which leads it to operate improperly. Secondly, because the environment is remote and unattended, sensors can be captured physically and compromised easily. This causes a node to misbehave intelligently, which makes the problem more complicated. Finally, the topology of the network is dynamic, which means the neighbourhood also changes dynamically. It makes it difficult for nodes to establish trust with new neighbouring nodes, compared with establishing trust with nodes with which they already interact. Thus, estimated trust value is influenced not only by node behaviour but also by several aforementioned factors, which will have an impact on the accuracy of the trust value. Hence, TM and estimation must consider several factors to obtain an accurate trust value and to establish proper trust relationships.

- Sensor node constraints. Because the number of nodes can be in the hundreds or thousands in WSNs, it becomes imperative to produce sensors at very low cost, which limits their capabilities in terms of computation, communication range and battery capacity. Hence, considering such factors, providing optimal trust estimations (TEs) should be a lightweight and energy-efficient process to meet the computational capability and energy constraints of the sensor nodes yet robust enough to meet the security requirements of TM. Moreover, an exchange of trust values among nodes might also be limited because the overhead of messages can cause high energy consumption and congestion in limited bandwidth. Proposing TM while keeping in mind the aforementioned factors can be challenging.
- Scalability. Another unique feature of WSNs is the vast number of nodes in the network, which raises scalability issues. As the number of nodes increases, the complexity of monitoring behaviour of the nodes and estimating and managing trust values will increase nonlinearly. Therefore, performing TE and management by each node for this great number of neighbourhood nodes can be challenging. Although several works have been proposed, related computational schemes do not consider all of the necessary design considerations for TM. Moreover, because TM is still in its infancy, there are still many research issues that need to be addressed, such as the notion whereby the term TM is used interchangeably with reputation management or trust establishment. Moreover, current surveys show that it is necessary to discuss design factors for features of TM and WSNs and to state them in detail.

Recently, literature surveys have been proposed on trust in various fields, including WSNs [6–8]. Nevertheless, surveys focused on design factors and current research issues are still lacking. There was a recent survey on trust mechanisms in WSNs by Lopez and colleagues [6]. However, the paper mainly focused on security and attack analysis issues rather than design considerations and the current state of research. Another survey on trust and reputation management systems in wireless communications was proposed by Han and colleagues [9]. Because that paper dealt with general surveying on trust in different wireless communication domains, unique aspects of trust in WSNs were outside the scope of the paper. Hence, a survey focusing on important design factors and on the current state of research is necessary.

There are two clear objectives of this study: understanding the concept and design factors of TM in WSNs and exploring current research as well as open research issues. To achieve the former, we discuss the concept of trust and TM in WSNs by analysing and summarising the definitions for these phenomena. Moreover, we define basic functional blocks and design factors of TM. The basic functional blocks (such as monitoring, trust evaluation, and trust propagation) and their basic functions are presented and discussed in detail. The design factors are proposed on the basis of WSN features and TM security requirements. To provide reliable security services by TM, TM should be robust against attacks, and the trust values produced should be accurate. Hence, robustness and accuracy are primary design factors, which are extensively described in Section 2. Moreover, TM that considers sensor node constraints, such as limited computation, storage, and battery capability, is vital for WSNs. For example, complex trust computations can go against the computation capability of the sensor nodes. Furthermore, TM should be scalable enough because of the great number of nodes in the network. Otherwise, the feasibility of TM can be degraded significantly. Specifically, the number of messages and interactions in TM should be taken into account. Therefore, energy efficiency, lightness, and scalability are other primary design factors. The last, but not the least, design factor is considering TM as a system. Considering TM as a system that consists of basic blocks allows maximum benefit from the TM system and contributes to the robustness of the design. Operation of those basic blocks is dependent on each other, and so considering the interoperation of the basic blocks of TM at the time of design is important. To achieve the second goal, first, we review the literature on TM in WSNs by categorising them into four areas: probability, weighting, fuzzy logic, and miscellaneous. Second, we perform comprehensive analyses and comparisons on proposed TM schemes based on a defined TM framework and design factors.

The remainder of the paper is organised as follows. In Section 2, we discuss the basics of trust, the notion of TM, attacks and defense mechanisms related TM, and the design factors and applications of TM. In Section 3, we focus on presentations, discussions, and comparisons of proposed TM schemes. Section 4 presents discussions and open research issues, and Section 5 concludes the paper.

Trans. Emerging Tel. Tech. **26**:107–130 (2015) © 2013 John Wiley & Sons, Ltd.
DOI: 10.1002/ett

2. TRUST MANAGEMENT IN WIRELESS SENSOR NETWORKS

This section deals with the basics of trust and the notions and design factors of TM in WSNs. In addition, it presents TM-related attacks, defense mechanisms, and application domains of TM in WSNs. Because it is important to understand fundamentals such as definition, values, and properties of the trust to design a TE scheme correctly, we state such basics of trust initially. After this, we attempt to clarify the concept of TM in WSNs by analysing the given definitions for TM in existing publications. Moreover, TM-related attacks, defense mechanisms, and application domains of TM are stated to provide broader insight about TM. Important design factors and considerations are presented at the end of the section.

2.1. Definition, values, and properties of trust

To estimate the trust level of the nodes, it is important to understand fundamentals such as definition, values, and properties of trust.

Definition of trust. The definitions of trust in WSNs as given in the literature are similar. In Yan and colleagues [10], trust is defined as the belief by one node that another node will behave in a certain way. According to Shaikh and colleagues [5], trust is the competence of a node to provide a required service. Trust is a degree of belief on the future behaviour of other nodes, which is based on past experience and observations of the nodes' actions [11]. We can summarise definition of trust in WSNs as follows:

Node A's trust in Node B describes the belief or expectation or assurance of sincerity, competence, and integrity of Node B's future activity/behaviour.

Trust values. To represent trust and trust relations, various forms and ranges are used [5, 6, 10–12]. For instance, a range of trust values is given between 0 and 1 [12], or it is given as a range (0–100) [5]. Forms of a trust value can be categorised in two ways [7]: discrete and continuous. The discrete form of trust value can be an integer number or an integer number with labels. Other than that, the rest are considered as a continuous form of trust value. The form of the trust value is important in WSNs because of the constraints of the sensor nodes. Depending on the form of the trust value, the required memory space can be greater or lesser. For example, an unsigned integer number (1 byte) can save 75% in memory, compared with a real number (4 bytes).

Trust properties. Another important factor for TE and establishment is trust properties. We consider the following trust properties for WSNs [8, 13, 14].

- Subjective. This property implies that nodes may have different trust values for one node.
- Composable. This allows that nodes can aggregate the trust values for a certain node from different sources.
- History-dependent. This assumes that a history of experience may have an influence on the present trust level.
- Context-dependent. This is effective only in a particular context.
- Dynamic. Trust values might increase and decrease over time.

2.2. Notion of trust management

To develop a robust and secure TM system for WSNs, it is important to have a clear understanding of TM. Nevertheless, the term *trust management* is rarely defined and is used interchangeably with the terms *trust establishment* and *reputation system*. Trust establishment and reputation system are in fact parts of a TM system, and TM has a wider meaning. According to Zheng and Holtmanns [15], TM addresses managing trust relationships, such as information collection, to make decisions related to trust, assessment of the criteria related to the trust relationship, and observation and reassessment of existing relationships. For Zheng [16], autonomic TM includes four aspects:

- Trust establishment: the process of establishing a trust relationship between communicating pairs.
- Trust monitoring: the process of observing and recording performance or behaviour of the trustee by the trustor or by a delegate of the trustor.
- Trust assessment: the evaluation process of trustworthiness of the trustee by the trustor or by a delegate of the trustor based on the recorded information.
- Trust control and re-establishment: On the basis of the trust evaluation, trust relationships are re-established, or corresponding measures are taken to control trust relationships.

According to Efthimia [17], TM deals with issues such as the formulation of trust evaluation rules and policies, representation of trust, and management of trust relationships. Trust establishment is defined in the same reference as a process that deals with representation, assessment, maintenance, and propagation of trust among nodes. In Jsang and colleagues [18], the main differences between trust system and reputation system are as follows:

- Trust systems provide a value that shows the individual view of trustworthiness of a trustee, whereas reputation systems produce a trustee's reputation value, which shows the view of the community of the trustee;
- Transitivity is an implicit component in trust systems, whereas it is an explicit component in reputation systems;
- As input to trust systems, subjective and general measures of reliability are used, whereas information on and evaluations of certain events are used as input to reputation systems.

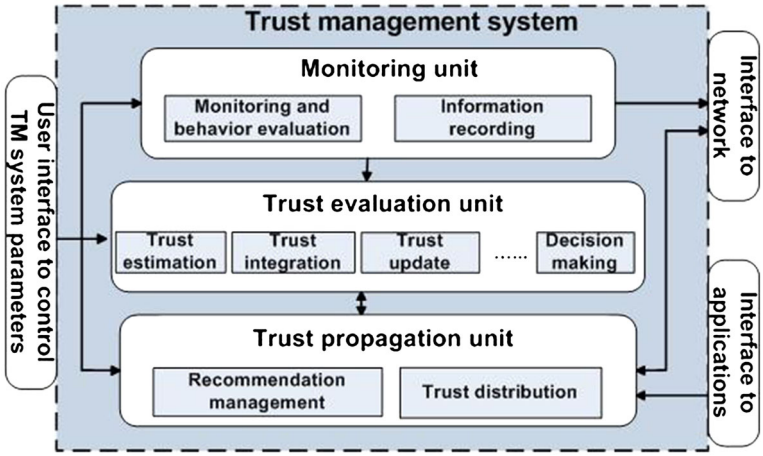

Figure 1. Basic elements in TM and relationships between them.

On the basis of the previous definitions and features of WSNs, we can give a definition for TM in WSNs as follows:

Trust management deals with monitoring the performance/behaviour of nodes and recording it; estimating the trust and establishing trust relationships; managing trust relationships, TE rules and policies; assisting security services, such as access control, key management and misbehaviour detection (Figure 1).

Thus, we propose that the TM system may have three basic functional blocks that allow efficient TM. Later, we define briefly the functions of each of the blocks.

- Monitoring and learning: Monitor and learn node behaviour/performance and provide input to the trust evaluation unit. This is connected to a network interface to collect information about nodes.
- Trust evaluation: This is a central unit of the TM system, which performs estimation and integration of trust and reputation values, decision-making trust value quantisation, information aging, and so on. It provides output to the recommendation management unit.
- Recommendation management: This deals with the distribution and reception of recommendations (trust values). In addition, it provides trust values of nodes for various applications.

2.3. Trust management-related attacks and defense mechanisms

In this section, we briefly present the most prominent attacks related to TM and the corresponding defense mechanisms. The susceptibility of WSNs to various attacks requires the design to be robust and the algorithms to be secure. Attacks can be broadly categorised as follows (Figure 2):

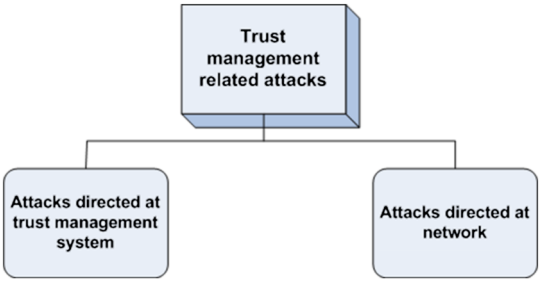

Figure 2. Classification of TM-related attacks.

- Attacks directed at TM system,
- Attacks directed at network.

2.3.1. Attacks directed at trust management system.

Attacks directed at TM system degrade TM system performance and lead to incorrect decisions. Accordingly, the attack will degrade network performance as well. For example, in secure routing, if TM cannot properly detect malicious nodes because of on–off or bad mouthing attacks, then those malicious nodes can be selected as routing nodes to send packets. As a consequence, the packet drop rate in the network will increase. TM can be configured through several parameters, such as TE interval, rewarding and punishing mechanisms, trust threshold, forgetting factor, changing trust parameters dynamically, trust aggregation parameters, and so on. The best configuration of TM depends on the application of TM, the security situation in the network, and design purpose. However, there are basic requirements for a TM system, and one of them is that it should be immune to basic attacks. Otherwise, the operation of TM is meaningless. The most prominent and harmful basic attacks are as follows [13, 19]:

Trans. Emerging Tel. Tech. **26**:107–130 (2015) © 2013 John Wiley & Sons, Ltd.
DOI: 10.1002/ett

- Bad mouthing attack. In this kind of attack, malicious nodes try to decrease the trustworthiness of reliable nodes and/or increase the trustworthiness of malicious nodes by providing dishonest recommendations.

  Defense mechanism. Trustworthiness of the nodes is evaluated in terms of providing an honest recommendation separately from a common trustworthiness evaluation, so that malicious nodes are not used as recommendation providers [19, 20].
- On–off attack. Malicious nodes alternately behave well or badly, either in random or in increasing/decreasing patterns to remain undetected while causing damage.

  Defense mechanism. To handle this kind of attack, history observations should not carry the same weight as current observations. Hence, a forgetting mechanism is used to tackle this issue [19].
- Conflicting behaviour attack. An attacking node shows different behaviours to each group of nodes. For example, a malicious node always shows good behaviour to one group of nodes and bad behaviour to another group of nodes. As a consequence of this attack, there will be conflicts between recommendations on that attacking node, and trusted peers might decrease their trust in each other as recommendation providers. Another example of this kind of attack is where a malicious node provides different recommendations on a certain node to each group of nodes.

  Defense mechanism. Detection and prevention of such attacks can be complicated, especially if they are launched in collaboration. Yan and colleagues [19] proposed not using recommendation trust when there is a conflict among recommendations, so that reliable nodes do not decrease each other's recommendations. Although this technique prevents the consequences of the attack to some extent, it cannot defend against the attack completely.
- Sybil and newcomer attack. These attacks share similar characteristics, such as illegitimately creating fake node identities. With a Sybil attack, the malicious node uses multiple fake network identities [19,21,22]. In the context of TM, the malicious node uses fake identities to take or share bad history. For example, it can use one fake identity to attack the network until it is detected and then change its identity, deleting the previous fake identity so that it can continue launching attacks. In a newcomer attack, a malicious node leaves the system and registers again as a new node so that it can remove its bad history [19].

  Defense mechanism. According to Yan and colleagues [19], the solution for these problems relies on authentication and access control, rather than TM. Newsome and colleagues [21] showed that a random key distribution technique can tackle the Sybil attack. Microsoft and colleagues [22] demonstrated that if there is no centralised authority, it is always easy to launch a Sybil attack.
- Time synchronisation attacks. Time synchronisation is critical to WSNs. Many applications and protocols, such as measuring time of flight for positioning, forming time division multiple access radio scheduling, coordinating sensors' sleep/wakeup schedules, preventing replay attacks, collaborative signal processing, and many others, strongly depend on precise timing [23, 24]. The malicious node's main objective is to make other sensors set the wrong clock time (i.e. to desynchronise clock times).

  Defense mechanism. Yang and Sun [24] propose a set of defense mechanisms that are collectively referred to as detection, analysis, and self-healing (DAS). The defense is divided into four steps:

  - Step 1: After the level discovery phase, each sensor knows its level and its parent node on the sync-tree. DAS requires each sensor to send the information of its level, parent, and children to the base station (BS).
  - Step 2: To detect abnormalities, self verification and local verification are performed. After each round of time synchronisation, a sensor performs self verification on the basis of end-to-end delay and the clock offset calculated previously. If a node finds that the risk of being attacked is higher than a threshold, it will start local verification, in which it exchanges information on clock time with its neighbours. If it finds inconsistencies among sensors' clock times, it will send warning reports to the BS.
  - Step 3: The BS examines the reports and determines the sensors that are causing the synchronisation abnormality. After determining the malicious nodes, BS will decrease those nodes' trust values via the trust model.
  - Step 4: To recover from synchronisation errors, the BS orders sensors to change their locations on the sync-tree such that they are less likely to be affected by malicious nodes. In addition, the BS will isolate the sensors with very low trust values, such that they cannot launch attacks. The proposed scheme can be more effective and robust if the authors address malicious nodes sending false reports to the BS. The authors themselves admit that can be a serious threat to performance. Hence, they assume that the misbehaviour detection process always assigns a negative mark to the sender of the report. This can mitigate the attack but cannot help a good node recover from a frame-up attack.

2.3.2. Attacks directed at network.

These kinds of attacks are not directed at the TM system, and they can be detected and prevented by the TM system [25]. Examples of such attacks can be intentional data dropping, energy drain, time desynchronisation, incorrect sensor data reporting, and other malicious activities that are discussed broadly by Yanli and colleagues [7]. They can be categorised as follows:

- Packet dropping attacks,
- Different misbehaviours.

To tackle such attacks and malicious behaviour is one of the main objectives of TM system [25–27]. Defense mechanism against those attacks follows typical procedure:

(1) Node performance is monitored or learned and recorded periodically. This part of the defense mechanism is mainly modified when it is applied to tackle different types of attacks. For routing-related attacks, packet dropping by the malicious node is monitored by using promiscuous listening on transmission. Specifically, a monitoring node checks the different fields in forwarded packets as to the number of received and forwarded packets. On the other hand, for malicious behaviour such as a wrong sensor data report, the monitoring node uses outlier mechanisms to detect wrong sensor data. Moreover, the monitoring period can be different depending on the applied attack.
(2) On the basis of the recorded information, trust is estimated periodically. In this part of the defense procedure, only the TE period can differ. Other parameters will be the same.
(3) Depending on the estimated trust value, a node is considered to be malicious (an attacker) or normal (trustworthy).
(4) On the basis of TM policy, a malicious node is punished or eliminated from participating in activities.

Because the defense procedure is typical for all attacks, we state later only a description of the attacks and misbehaviours.

Packet dropping attacks. Malicious nodes try to degrade network performance by dropping packets through different means. Some examples of such packet dropping attacks are as follows:

- Blackhole attack. An attacker node attracts the traffic to be routed through it and drops all received packets [28].
- Grayhole attack. If the malicious node attempts to drop all packets that come in, the attack can be discovered very quickly and avoided. So, in this attack, a malicious node drops packets selectively [25, 28].
- Wormhole attack. Attackers create a low latency link between two endings in the network. After establishing the link, it collects all packets at one end of the link, sends them through the low latency link, and replays them at the other end, causing disruption in normal traffic load and flow [9, 29].

Different misbehaviours. In this section, we describe the different misbehaviours with brief examples. For more detailed information, refer to Yanli and colleagues [7]. Generally, misbehaving nodes can be divided into selfish nodes, which try to maximise their own gain at the expense of others, and malicious nodes, which try to degrade the system or node performance with no explicit intention to maximise their own benefit [9]. Depending on the misbehaving nodes' intention, attacks can be various. For example, if a malicious node intends to drain the energy of the nodes, it will send a large amount of traffic and require other nodes to reply. Another example is sending spoofed, altered, or replayed routing information in which the malicious node's goals are to create routing loops, attract or repel network traffic, extend or shorten source routes, generate false error messages, partition the network, increase end-to-end latency, and so on [7].

2.4. Application domains of trust management

The literature on trust shows that TM is applied in various security and network services in WSNs [23, 24, 30–45]. We can illustrate the necessity of establishing trust by simple reasoning. In WSNs, nodes accomplish the network mission or task collectively, which means that success of the mission or the task depends on each node. Simply, the mission can be accomplished fruitfully when the nodes are honest or good. The role of TM in those missions is to provide honest or good nodes for cooperation. As the goal of TM is to decrease the impact of misbehaving or faulty nodes [9], it can be applied in various fields with different goals. Hence, there are many areas in which TM is applied in WSNs, such as general misbehaviour and selfish behaviour detection [5, 9, 10], secure localisation [43, 44, 46], access control [30, 34–36], secure routing [31–33], intrusion detection [41, 42], and secure data aggregation [37–40]. Later, we describe some of these application examples.

Secure routing. One of the most applied areas of trust and reputation is routing in WSNs. Routing in WSNs is purely a cooperative task because of the limited communication range of the nodes, and data should be delivered from all sensor nodes to the BS, which is usually far from most of the nodes. Malicious packet drops can degrade system performance significantly because of the importance of the dropped packet. For example, for military or medical applications, sensor data can be time critical, and each of the data has significance. Hence, reliable data delivery is important. TM monitors each node's packet drop rate over a certain time and sets a trust level for each node so that nodes can choose the node with the least packet dropping (or the most trustworthy node). Some examples of secure routing using TM are given [31–33]. A trust-aware routing framework (TARF) for WSNs, to secure multihop routing in WSNs against intruders exploiting the replay of routing information, is proposed by Zahn and colleagues [31]. It integrates trustworthiness and energy efficiency in making routing decisions. Two components are defined: energy watcher and trust manager. Energy watcher is responsible for recording the energy cost for each known neighbour, based on node's observation of one-hop transmission to

Trans. Emerging Tel. Tech. **26**:107–130 (2015) © 2013 John Wiley & Sons, Ltd.
DOI: 10.1002/ett

reach its neighbours and the energy cost report from those neighbours. Trust manager deals with tracking trust level values of neighbours based on network loop discovery and broadcast messages from the BS about undelivered data packets. Performance evaluation results show that achieved throughput is high in TARF. Moreover, energy efficiency is a good indicator for WSNs. Although the authors claim that TARF is scalable, they did not demonstrate it through results.

Access control. To prevent malicious nodes from joining the sensor network, access control is required [34, 35]. Trust can also be applied in determining whether or not to provide access to certain resources or rights [30, 36]. It can enhance access control by granting only trustworthy nodes access to the resources. Misra and Vaish [30] propose a reputation-based role-assigning scheme for role-based access control. The authors assume that different nodes have to play different roles in a single network. On the basis of three parameters reputation, bootstrap time and node energy roles are dynamically mapped to different nodes. The scheme is divided into two processes: reputation management and role assignment. In the reputation management process, a node estimates the reputation of its neighbourhood periodically. The objective of role assignment is to assign appropriate levels to nodes according to their parameters. It is performed after a predetermined timeout value, or if the energy of the cluster head (CH) falls below a certain threshold. Presented results show that throughput can be improved in the network. Considering basic attacks against trust, such as on–off and bad mouthing, is important because malicious nodes can obtain access to higher roles, which will degrade system performance significantly.

Secure data aggregation. Because the battery lifetime of sensor nodes is limited and nonrechargeable, it is important to minimise the amount of data transmission so that average sensor lifetime and overall bandwidth utilisation are improved. Data aggregation is summarising and combining sensor data to reduce the number of data transmissions in the network [37]. Compromised nodes distort the integrity of data by injecting false data reports, injecting false data during data aggregation, and disrupting transmission of aggregated data. Thus, trust can be used to prevent participation of such nodes during data aggregation [37–40]. Moreover, a trusted aggregator can be selected among nodes on the basis of performance using trust. Reliable data aggregation and transmission (RDAT) protocol was proposed [37]. To assess a sensor node for each specific task, it uses a respective functional reputation value rather than a single general reputation value. Because RDAT selects trusted data aggregators using aggregation functional reputation, and by weighting sensor data using sensing functional reputation, security of aggregated data is provided in this way. Moreover, the security of aggregated data transmission to the BS is attained using a multipath data transmission algorithm that is based on routing functional reputation. In addition, the multipath data transmission algorithm selects data paths in a hidden manner and uses a fault-tolerant Reed–Solomon coding scheme, which improves the security of transmission of aggregated data.

Intrusion detection. Intrusion detection system (IDS) is a system that aims at detecting and warning against attempted intrusions into a system or a network. Intrusion is a set of malicious activities that violate security aspects (including integrity, confidentiality, availability, and authenticity) of network's resources. Three main functionalities of IDS are defined: monitoring, analysing, and reacting to occurring attacks on computer systems and networks [41, 42]. TM can be merged with IDS to protect IDS from malicious attacks and to locate expert IDS about intrusion assessments [41]. Moreover, TM itself can be used as an IDS [41]. TM for evaluating the trustworthiness of a host-based IDS (HIDS) in a collaborative intrusion detection network (CIDN) is proposed by Fung and colleagues [41]. The scheme adapts Dirichlet density functions for estimating trust. It measures the uncertainty in estimating likely future behaviour of an HIDS. The forgetting factor method is also proposed against on–off attacks. An acquaintance management algorithm is proposed for an HIDS in the CIDN to maintain a list of acquaintances from which it can ask for consultation on intrusions. The HIDS sends test or consultation messages to its acquaintances and updates the trust values based on the satisfaction level it obtains from their responses. The results demonstrated that the success rate of the proposed scheme is higher than that of other schemes. Moreover, the acquaintance management algorithm is also shown to have the properties of fairness and convergence.

2.5. Design factors and considerations of trust management

Considering the properties and features of both TM systems and WSNs, we propose the following important design factors:

- Robustness
- Accuracy
- Energy efficiency and lightness
- Scalability
- TM as a system

Later, we discuss and present each of the stated factors in detail:

Robustness. Robustness is crucial not only to TM systems but also to all security systems. As TM is a kind of security entity, it must be robust against attacks. If the TM system is not resilient against attacks, its performance is meaningless. Moreover, robustness of the TM system has an impact on the security requirements of WSNs. As for main security requirements of WSNs, they are as follows [7]:

- Confidentiality
- Integrity
- Authenticity
- Privacy

Table I. Specification of some recent motes.

Mote platform	uProcessor	Bus (bit)	Clock (MHz)	RAM (K)	Flash (K)
TelosB/Tmote Sky	TI MSP430F161116	16	4–8	10	48
MicaZ/Mica2	Atmel Atmega 128L	8	8	4	128
SHIMMER	MSP430F1611	16	4–8	10	48
IRIS	Atmel ATmega 1281	8	8	8	640
EZ-RF2480/2500	TI MSP430F2274	16	160	1	32

For the details of the security requirements, we refer to Yanli and colleagues [7]. It is obvious that robust TM can help attain the security requirements of WSNs. On the other hand, it will degrade security of the WSNs if the robustness of TM is degraded. Hence, a TM system should have an inbuilt mechanism against basic attacks at least. Robustness should be considered in the following operations.

- TE. TE should be resilient against on–off attacks. While estimating trust, keeping history information properly and combining it with current information can help to track on–off attacks. Moreover, tracking the node behaviour and assigning accurate trust values are vital to system performance.
- Trust integration. Trust integration deals with aggregating trust values based on direct and indirect sources. The issue in this operation is that trust value based on indirect sources can be dishonest. That is, a malicious node can intentionally provide a wrong recommendation on a legitimate/malicious node to decrease/increase trust, which is called bad mouthing attack. Hence, the TM system should have an inbuilt mechanism that can detect reliability of the provided recommendation before integrating it.
- Trust update interval. To set a proper interval helps to assess and detect the malicious nodes in time. Moreover, changing it dynamically according to the security situation can improve TM performance.
- Secure channel to receive and send recommendations. It is important to have a secure channel because it provides integrity of received and sent recommendations.
- Adaptive trust parameters. Instead of using fixed trust parameters, adaptive parameters can improve and optimise TM performance. Because the network is dynamic and the security situation changes over time, it is better to adapt trust parameters according to the need of the network and of security. On the other hand, it requires an additional cognitive component that learns the network and the security situation and reports it to TM.
- Bootstrapping and initial trust values. At the very beginning of the network, nodes do not have any knowledge about each other, and with few interactions to build trust, relationships will be difficult. Hence, initially, the same trust values are assigned to each node. However, determining the trust values can be a difficult issue because high trust values can cause some problems that malicious nodes can use to attack the network. On the other hand, low trust values degrade cooperation and cause long bootstrapping. Hence, initial trust values should be defined according to application need and security level.

Accuracy. Accuracy of the produced trust values is important because it traces node behaviour correctly and assigns correct trust values to each node. Accordingly, TM performance will be improved. Accuracy of the produced trust values can be affected by dynamics of the network and node behaviour. Hence, TE methods should have the ability to consider dynamics of the network and node behaviour to produce accurate trust values. Moreover, trust update and integration methods also impact the produced trust values.

Energy efficiency and lightness. Because WSN applications require a great number of nodes in the network, costly sensor nodes will be unaffordable. As a consequence, hardware of a sensor node has limited capabilities in terms of computation, communication, storage, and power. To have general insight about capabilities of those sensor nodes, we can see some specifications of recently available motes for WSNs in Table I [47]. As we can see, although specifications of the motes vary depending on application needs, in general, their capabilities are very limited. In general, computational capabilities of sensor nodes can support basic TM operations because TE and aggregation usually involve simple addition, multiplication, subtraction, and division. However, an increased number of such operations may require more energy consumption and more memory. Moreover, if the estimations are more complex, the more space they use in the processor, and the more power dissipates. For example, the square root of a number or logarithmic equations might require much more work and energy than simple addition and subtraction. Hence, computational complexity of the trust equations can be determined on the basis of the number and complexity of the operations to be performed. Specifically, the following issues, among others, should be considered:

- Behaviour monitoring. Behaviour monitoring involves overhearing neighbourhood transmissions continuously. Because it might require nodes to always be on, it is important to set up monitoring efficiently so that necessary information is overheard while keeping energy consumption to a minimum. Moreover, behaviour monitoring involves classifying the

Trans. Emerging Tel. Tech. **26**:107–130 (2015) © 2013 John Wiley & Sons, Ltd.
DOI: 10.1002/ett

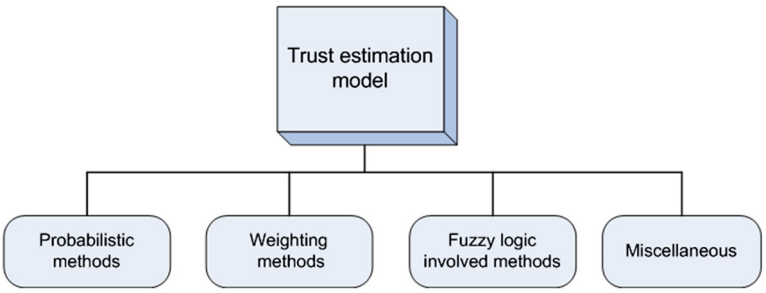

Figure 3. Classification of trust estimation models.

overheard information. Therefore, information classifying methods should be simple and energy efficient as well.

- TE, update, and integration. Although energy consumption for processing operations can be negligible [48, 49], frequent and complex computations might require high energy consumption. Furthermore, complex estimations tax the capability of the sensor node. Because trust update and integration are performed periodically, there can be trade-off between energy efficiency and robustness of the produced trust value.
- Recommendation distribution and reception. Recommendation distribution and reception can be among the most energy-consuming operations of TM. Because sensor nodes consume energy mainly for sending and receiving data [48], attaining the optimum between energy efficiency and recommendation need is an important issue.

Scalability. Scalability shows the practical applicability of TM. As the number of nodes is high in WSNs, the number of exchanged messages is also expected to be high. If we denote the amount of exchanged messages per unit of time per peer as $R(n)$, where n is the total number of peers in the network, $R(n)$ increases rapidly with the network size [e.g. $(O(n))$] [50].

Trust management as a system. Considering TM as a system that comprises basic blocks as stated in Section 2.2 allows the system to benefit from TM fully and contributes to robustness of the design. Because those basic blocks are dependent on each other, considering interoperation of the basic blocks of TM during design is important

3. OVERVIEW OF TRUST MANAGEMENT APPROACHES

Recently, many TM and reputation schemes have been proposed in various fields such as e-commerce, web-based services, peer-to-peer networks, and WSNs, which shows the significance of TM and reputation systems for these fields. To know the current state of the field and open research issues, it is important to review state-of-the-art TM schemes proposed for WSNs. Hence, in this section, we present proposed TM schemes, taxonomy, and comparisons. On the basis of the type of TE model, proposed TM schemes can be divided into the following categories (Figure 3):

- Probability-based TE model [12, 26, 46, 51–54]
- Fuzzy logic-based TE model [55–61]
- Weighting-based TE model [5, 62–64]
- Miscellaneous [48, 65–67]

Because TE is the core of TM, many research works are focused on TE modelling. Hence, we categorise the proposed TM approaches on the basis of TE model. Furthermore, trust can be estimated at two levels [9]:

- Node level. Nodes estimate trust for each other on the basis of direct and indirect observations.
- System level. In system-level TE, the CH or BS calculates the global trust value of the node by means of trust aggregation and integration.

3.1. Probabilistic trust estimation-based trust management

In this type of TM, trust is modelled using a probability distribution together with Bayesian theory [12, 26, 46, 51–54]. Trust value is represented as probability, which expresses expectation of a node's future behaviour. Because Bayesian theory is mathematically sound and fully compatible with trust evaluation procedures, it prompted many researchers to develop TE models on the basis of this theory. It uses the prior probability of an event, which is then updated in light of updated relevant events, to make a posterior inference of that event. Beta distribution is often used to estimate trust value. In this subsection, we present some representative TM schemes based on a probabilistic TE model.

Ganewarial and colleagues [12] propose a reputation-based framework for high-integrity sensor networks in which sensor malfunction problems are addressed by means of developing a community of trust. Each node builds a reputation for other nodes by monitoring their behaviour on the basis of the watchdog mechanism.

Initially, reputation of the node before any transactions is estimated as follows [12]:

$$P(\theta) = \frac{\Gamma(\alpha+\beta)}{\Gamma(\alpha)+\Gamma(\beta)}\theta^{\alpha-1}(1-\theta)^{\beta-1} \quad \forall \quad 0 \leqslant \theta \leqslant 1$$
$$\alpha \geqslant 0, \beta \geqslant 0 \tag{1}$$

for some choice of α and β, where $\Gamma(\cdot)$ is the gamma function. Given θ, the reputation is updated after each transaction according to one of the two proposed approaches: binary and interval ratings. In the binary rating approach, binary ratings are first modelled as Bernoulli observations with a success probability. Let $X \in [0,1]$ denote node i's rating of node j for a single transaction. Then, the probability that node j will be cooperative is given as follows [12]:

$$p(X|\theta) = \theta^X(1-\theta)^{1-X} \tag{2}$$

Once the transaction is finished, the reputation is updated using a posterior distribution for θ [12]:

$$p(\theta|X) = \frac{p(X|\theta)p(\theta)}{\int_{[0.1]} p(X|\theta)p(\theta)d\theta} \propto p(X/\theta)p(\theta) \tag{3}$$

Another approach for updating reputation is based on a Dirichlet process. Let $D(\delta)$ be a Dirichlet process with base measure, and let it be a prior distribution for reputation. Given observations $X_1, ..., X_n \in [0,1]$, posterior distribution is a Dirichlet process with base measure [12]:

$$\delta(x) + \sum_{i-1}^{n} I_{X_i}(x) \tag{4}$$

where I is an indicator of a point mass at the location of observation X_i. In both approaches, the mean value of a posterior distribution is taken. Then, a trust value of node j is obtained by taking an expectation of the reputation of node j [12]

$$T_{ij} = E\left[R_{ij}\right] = E\left[Beta\left(\alpha_j, \beta_j\right)\right] = \frac{\alpha_j}{\alpha_j + \beta_j} \tag{5}$$

T_{ij} expresses node i's prediction of the expected future behaviour of node j, whereas α and β are number of successful and unsuccessful transactions. Furthermore, the authors propose defense mechanisms against a bad mouthing attack and ballot stuffing, in which direct observations are given more weight than indirect observations, and recommendations are weighted on the basis of the reputation of the reputation provider. Although updating reputation after each transaction between two nodes can help to efficiently counter any arbitrary behaviour, it might cause energy inefficiency because of frequent reputation estimation, especially if nodes are active in cooperation.

Mohammad and Subhash [26] proposed a Gaussian trust and reputation system for sensor networks. Bayesian theory and Gaussian distribution are used to estimate reputation and trust as well as to integrate reputation values. It is assumed that each time a node provides sensor data, one-hop neighbours that route its report see that report and can evaluate the reported sensor data. On the basis of the evaluation of the reported sensor data of node n_j, a reputation of node n_j by node n_i is defined as a probability density function [26]:

$$R_{i,j} = N\left(\mu_{i,j}, \sigma_{i,j}^2\right) \tag{6}$$

where $\mu_{i,j}$ is the mean of the observed error, as observed by n_i about n_j reporting, $\sigma_{i,j}^2 = \tau^2/k$ is average error variance, where τ is error variance and k is the number of reports by node n_j. Trust value of node n_i is estimated by node n_j as follows [26]:

$$T_{i,j} = \text{Prob}\{|\theta_{i,j}| < \varepsilon\} \tag{7}$$

$$T_{i,j} = \text{Prob}\{-\varepsilon < \theta_{i,j} < \varepsilon\} = \phi\left[\frac{\varepsilon - \bar{y}_{i,j}}{\tau/\sqrt{k}}\right] - \phi\left[\frac{-\varepsilon - \bar{y}_{i,j}}{\tau/\sqrt{k}}\right] \tag{8}$$
$$= \phi\left[\frac{\varepsilon - \mu_{i,j}}{\sigma}\right] - \phi\left[\frac{-\varepsilon - \mu_{i,j}}{\sigma}\right]$$

where ϕ the cumulative probability distribution of the Normal $N(0, 1)$, $\theta_{i,j}$ is probability of error, $\mu_{i,j} = \bar{y}_{i,j}$ is the mean of the observed error, k is the number of reports by node n_j, τ is error variance, and $[-\varepsilon, +\varepsilon]$ is trust interval. Furthermore, authors demonstrated how to integrate indirect observations (recommendations) with direct observations on the basis of Bayes theorem. The proposed scheme in Mohammad and Subhash [26] is specific to some types of WSNs in which sensor data should be continuous. Furthermore, reputation and trust update involves complex equations, which goes against constraints of the sensor node.

Objective TM framework (OTMF), which is based on a modified Bayesian approach, is developed by Jie and colleagues [51]. Although this framework is proposed for mobile *ad hoc* networks, it can be applied to WSNs without complication as it is a general framework. OTMF works according to the following steps:

- Step 1: Update initial trust form through direct information. To delete effects of the old observation's influence, an exponential decrease method is used.
- Step 2: Propagation and process of second-hand information. Nodes receiving second-hand information (recommendation) will check the correctness by a deviation test and use the trustworthiness of the information provider as the weight for this information.
- Step 3: Trust and confidence value computation. Trust value is computed as the expectation value of a beta distribution, whereas confidence value is computed as a value related to the standard deviation of a beta distribution.

Trans. Emerging Tel. Tech. **26**:107–130 (2015) © 2013 John Wiley & Sons, Ltd.
DOI: 10.1002/ett

- Step 4: Evaluate trustworthiness. By combining parameters formed in Step 3, trustworthiness is evaluated. Depending on the situation, different weights are put on trust value, and a confidence value is used in the formation of trustworthiness. Although the proposed scheme is claimed to be immune against attacks such as bad mouthing or on–off attack, it needs to be comprehensively verified by simulation or other means.

Trusted cluster-based TM is developed by Garth and colleagues [52]. In this work, the authors also consider Bayesian theory and beta distribution to estimate trust and reputation of the node. The differences from other developed models are initialisation, an information-aging mechanism, a compromised node detection and isolation method, and the architecture design of TM. Initialisation is an important part of a TM system that should be carefully designed. According to the proposed scheme in Garth and colleagues, to initialise the system, authenticated messages are exchanged among nodes to discover the neighbourhood node. These authenticated messages contain the ID and location of the sender node. For aging observations, exponential averaging is used. Compromised node detection is performed by finding the least-trust-value node and checking its confidence. The node is broadcast as untrustworthy unless its confidence value is above a predetermined threshold. Upon receiving a broadcast message, each node looks in its trust table for a match. The untrustworthy node is blacklisted by other nodes by changing its trust value to -1 if the following conditions are met:

- The untrustworthy node has a lower trust value than the broadcaster.
- The broadcaster trust level is above a certain threshold.

Table II. Comparison of probabilistic trust estimation-based TM approaches.

TM approach	Brief description	Objective	Advantages	Disadvantage
RFSN [12]	Trust is estimated as expectation value of beta distribution. On other hand, reputation is estimated as beta distribution probability and updated using either Bayes theorem or Dirichlet process.	Detection of malfunctioning and malicious node that provides wrong or false sensor data.	Models with almost all required aspects of TM, such as node monitoring, trust estimation and update, trust propagation, and basic attack resistance.	Reputation estimation and update are highly computationally complex, which might not meet requirements of WSNs.
GTRSSN [26]	Trust and reputation are estimated on the basis of Gaussian distribution. They are updated using Bayes theorem.	Detection of malfunctioning and malicious nodes that provide wrong or false sensor data.	Different probability distribution (Gaussian) is used to model trust, which might have advantages over beta distribution, although it is not verified.	The scheme is limited only to trust and reputation estimation and update. Moreover, Bayesian and reputation calculation requires computational complexity.
OTMF [51]	Modified Bayes theorem is used to estimate trust. Confidence value is incorporated with trust to find trustworthiness of node. Moreover, several defense mechanisms are proposed.	Defense and robust techniques of TM against attacks.	Robustness and security of the TM are the main focus of the paper. Hence, it proposes several techniques to defend TM against attacks.	Although paper proposes several defense mechanisms, they are not verified.
Garth V *et al.* [52]	Reputation and trust are estimated using beta distribution function. Trust-based compromised node detection and isolation protocol.	Compromised node detection and isolation.	System initialisation and compromised node isolation are important part of TM, which are taken into account in the paper.	Untrustworthy node detection and reputation update techniques are not comprehensive.

TM, trust management; WSNs, wireless sensor networks; RFSN, reputation-based framework for high-integrity sensor network; GTRSSN, Gaussian trust and reputation system for sensor network; OTMF, objective TM framework.

Nodes with a −1 trust value are isolated, and there is no more cooperation with those nodes. However, this method allows a chance for colluding nodes to effectively launch a colluding attack in which the attack nodes collude to put down trustworthy nodes. In Table II, we summarise and compare the aforementioned TM schemes.

3.2. Weighting trust estimation method based trust management

In weighting TE, trust and reputation are estimated by weighting behaviour/performance of the node over time [5, 62–64]. This method makes it simple to estimate trust, and its implementation is easy, but it does not have a strong statistical or mathematical foundation. Shaikh and colleagues [5] propose a group-based TM scheme (GTMS) for clustered WSNs. The scheme works in three phases:

- Trust calculation at the node level,
- Trust calculation at the cluster-head level,
- Trust calculation at the BS level.

Nodes calculate the trust value based on direct or indirect observations. A timing window mechanism is used to eliminate the effect of time on trust values. The timing window Δt, which has several units, counts the number of successful and unsuccessful interactions. The interactions that occur in each time unit are recorded. After a unit of time elapses, the window shifts one time unit to the right, thereby deleting the interactions carried out during the previous unit. Using information in the time window, the time-based past interaction trust value *Tx,y* of node *y* at node *x* [5] is

$$T_{x,y} = \left[100 \left(\frac{(S_{x,y})^2}{(S_{x,y} + U_{x,y})(S_{x,y} + 1)} \right) \right] \quad (9)$$

where $[\cdot]$ is the nearest integer function, *Sx,y* is the total number of successful interactions of node *x* with node *y* during time Δt, *Ux,y* is the total number of unsuccessful interactions of node *x* with node *y* during time Δt. After estimating the trust value, a node will quantise trust into three states on the basis of the proposed mechanism: trusted, uncertain, and untrusted.

Each CH will periodically broadcast the request packet within its cluster to estimate global trust for its members. Upon receiving trust states from member nodes on their neighbour nodes, the CH will maintain these states in matrix form as follows [5]:

$$TM_{ch} = \begin{pmatrix} s_{ch,1} & \cdots & s_{n,1} \\ \vdots & \ddots & \vdots \\ s_{ch,n} & \cdots & s_{n,n-1} \end{pmatrix} \quad (10)$$

where TM_{ch} is the trust state matrix of cluster head *ch* and $s_{ch,1}$ is the state of node 1 at cluster head *ch*. After determining the relative difference in trust states of a node, its global value is assigned by the CH. The relative difference is emulated through a standard normal distribution.

As in a trust calculation at the node level, nodes maintain a record of past interactions. The BS also maintains a record of past interactions with CHs, and the BS estimates trust for CHs as follows [5]:

$$T_{BS,ch_i} = \left[100 \left(\frac{(S_{BS,ch_i})^2}{(S_{BS,ch_i} + U_{BS,ch_i})(S_{BS,ch_i} + 1)} \right) \right] \quad (11)$$

where S_{BS,ch_i} is the total number of successful interactions of BS with CH ch_i and U_{BS,ch_i} is the total number of unsuccessful interactions of BS with CH ch_i.

Advantages of this scheme are that it is lightweight and energy aware, which meets requirements of WSNs. Furthermore, the authors proved that GTMS is resilient against cheating, bad behaviour, and group attack under the assumption that the number of unsuccessful interactions is equal to or greater than the number of successful interactions. However, this may not always be true because the attack node usually attempts to go undetected as long as possible.

A parameterised and localised TM scheme (PLUS) for sensor network security is proposed by Yao and colleagues [62]. PLUS works with four components: routing operator, security responser, parameter database, and trust estimator. A routing operator provides packet handling. The next component, security responser, deals with managing parameter policies. To store parameters, a parameter database component is proposed. A core component of the PLUS is the trust estimator. Trust is established for nodes based on several parameters, such as integrity, freshness, and meaning of the packet. Moreover, parameters such as packet forwarding ratio, availability, and positivity of the node are added to the estimated trust. Hence, direct observation-based trust is estimated as follows [62]:

$$T_{pr(i)} = T_{cp(i)} \times W_{cp} + T_{av(i)} \times W_{av} \quad (12)$$

where $W_{cp} + W_{av} = 1$, $T_{cp(i)}$ shows the correctness of the incoming packet from node *i*, $T_{av(i)}$ shows availability of node *i*, and both parameters are formulated as follows [62]:

$$T_{cp(i)} = T_{or(i)} \times \left(T_{ai(i)} + T_{co(i)} \right) \quad (13)$$

$$T_{av(i)} = T_{po(i)} \times W_{po} + T_{re(i)} \times W_{re} + T_{coo(i)} \times W_{coo} \quad (14)$$

where $T_{or(i)}$ indicates freshness of the packet, $T_{ai(i)}$ indicates integrity of the packet, $T_{co(i)}$ indicates whether the cipher text received can be decrypted into meaningful plain text, $T_{po(i)}$ is for checking nodes' positivity by BS, $T_{re(i)}$ indicates whether node *j* can receive reply from the BS through node *i*, $T_{coo(i)}$ is forwarding ratio, and W_{po}, W_{re},

Table III. Trust level regulation table.

Trust level	Name	Description	Trust value
1	Distrust	Untrustworthy	(0,r1]
2	Minimal	Low trust	(r1,r2]
3	Average	Common trustworthy	(r2,r3]
4	Good	Trustworthy	(r3,r4]

W_{coo} are weighting parameters. Recommendation-based TE is performed as follows [62]:

$$T_{r(i)} = \frac{\sum_{k=1}^{m} AF_{lk} \times T_{(i)k}}{m} \tag{15}$$

This formula shows integration of recommendations from several nodes on a certain node. Here, AF_{lk} is the recommendation providers' adjustment factor, which corresponds to trust level where $l = 1, 2, 3, 4, \ldots, m$ is the number of recommendation providers and $T_{(i)k}$ is provided recommendation by recommendation provider k on node i. To integrate a direct observation-based trust value with an indirect-observation (recommendation) trust value, the following equation is used [62]:

$$T_{(i)} = T_{pr(i)} \times W_{pr} + T_{r(i)} \times W_r \tag{16}$$

where $T_{pr(i)}$ is a direct observation-based trust value, which is defined in (12), $T_{r(i)}$ is a recommendation-based trust, and $W_{pr} + W_r = 1$. After estimating the trust value of the node, nodes can determine its trust level based on Table III.

The merit of PLUS is that it has the security responser, which manages trust parameters based on the current security situation and provides flexible parameters to estimate trust. This kind of assistant component is important to more efficiently operate TM. However, including all parameters to estimate trust may not be always meaningful because trust has a property whereby it is context dependent. For example, a malicious node might launch only a certain kind of attack but for other activities, it behaves well. So, in this case, the malicious node can maintain a good trust value because it is good in other network activities. Another problem in PLUS is that forwarding nodes can be accused unfairly. For example, when forwarding node *A* receives a packet from node *B*, and if the integrity check fails, node *A* accuses node *B* of modifying the packet content and decreases its trust value. However, node *B* received that packet from node *C*, and the originator of the packet is node *D*.

Another multiparameter-based trust establishment method is proposed by Han and colleagues [63]. In this TM scheme, the authors consider the energy level of a node to estimate trust. Because nodes with higher trust value will work more than other nodes and die out early, an energy-consumption unbalancing issue arises. To avoid this issue, the energy level of a node is considered as a restrictive factor to decrease its trust value. The node with less energy decreases its opportunity for cooperation to make the network system stable. As in a traditional TE, trust is estimated in three ways: direct, indirect, and integrated. The trust value for attribute A_i can be computed as follows [63]:

$$T_{A_i} = \frac{S_i}{C_i} \tag{17}$$

where S_i is the number of the successes $(S_i, i = 1, 2, ..., n)$, and C_i is the number of total cooperation $(C_i, i = 1, 2, ..., n)$. The overall trust value for the node with n attributes $A_i = 1, 2, ..., n$ can be estimated as follows [63]:

$$T_{\text{node}} = \frac{\prod_{i}^{n} T_{A_i}}{\prod_{i}^{n} T_{A_i}} + \prod_{i}^{n} \left(1 - T_{A_i}\right) \tag{18}$$

For indirect TE, recommendations are received from three types of nodes: reliable, strange, and unreliable nodes. Recommendations are combined from only reliable and strange nodes as follows [63]:

$$T_{\text{indtrust}} = T_{\text{rel}} \times W_{\text{rel}} + T_{\text{str}} \times W_{\text{str}} \tag{19}$$

where T_{rel} and T_{str} are provided trust values by reliable and strange nodes, respectively. W_{rel} and W_{str} are corresponding weighting parameter for each trust value.

The integrated trust value can be calculated as follows [63]:

$$\begin{aligned} T_{\text{integtrust}} = & T_{\text{directtrust}} \times W_{\text{dtrust}} \\ & + T_{\text{indirecttrust}} \times W_{\text{itrust}} \end{aligned} \tag{20}$$

where $T_{\text{directtrust}}$ and $T_{\text{indirecttrust}}$ are obtained trust values through direct and indirect way and W_{dtrust} and W_{itrust} are corresponding weighting parameters for each type of trust value.

Including the energy level in TE is a good idea, but determining the energy level of the neighbouring nodes is a problem. Because it is not possible to be aware of the energy level of neighbouring nodes, malicious nodes can lie about their energy level and exclude themselves from cooperation, which degrades system performance.

To secure data sensing and data aggregation, a TM scheme is proposed [64]. On the basis of three parameters, trust is determined: data consistency, communication ratio, and battery level. Data consistency of the reported data is checked by using a reverse sense function, which produces an expected sensing value of a node using the distance between a node and an event. A communication ratio shows the selfishness and normal behaviour of the node. It is determined on the basis of the number of successful and unsuccessful communications. Battery level represents the remaining lifetime of a sensor node. It is possible to prevent

Table IV. Comparison of weighting trust estimation-based TM approaches.

TM approach	Brief description	Objective	Advantages	Disadvantage
GTMS [5]	Trust is estimated in three levels using a weighting method: node level, CH level, and BS level. A sliding window scheme is used to update trust. CH integrates trust values obtained from nodes using standard normal distribution and identifies trustworthy, uncertain, and untrustworthy nodes.	Detection of malicious node that acts uncooperatively.	The scheme has several merits: Node memory and capability constraints are considered by choosing an unsigned integer and proposing a lightweight scheme; TM is envisioned as a system of estimation, update, use, and management of trust.	Resilience of the scheme against attacks should be considered because a malicious node can maintain an equal number of successful and unsuccessful operations and it is not considered untrustworthy. It might degrade system performance, especially when the cooperation rate is high between nodes.
PLUS [62]	Proposed TM consists of four components: routing operator, trust estimator, security responser, and parameter database. Trust estimate is based on two parameters: (i) correctness of cryptographic operations of the node and (ii) interactive behaviour of the node.	Security enhancement by evaluating trustworthiness of node and secure routing protocol.	TM is envisioned as a system that assists security significantly by analysing current security situation and adjusting trust parameters accordingly. Consideration of recommendation protocol is another merit, which is rarely considered in other schemes.	Although trust estimation parameters are comprehensively taken into account, combining trust values from different contexts might not give a desirable result. Attacks directed at TM are not considered.
Han *et al.* [63]	Trust is estimated on the basis of several node attributes using a weighting method. Range of trust values is between 0 and 1.	Power-aware and reliable cooperative node selection.	Unlike other schemes, in trust estimation, only the successful number of operations is considered, which does not allow malicious node to manipulate the number of successful and unsuccessful operations.	Attacks directed at TM are not considered.
Junbeom *et al.* [64]	Trust is estimated on the basis of energy level, cooperation rate, and secure sensing.	Secure data sensing and aggregation.	Monitoring and learning unit of TM is comprehensive.	Determining the energy level of the node to estimate trust may not be feasible.

TM, trust management; CH, cluster head; BS, base station; PLUS, parameterised and localised TM scheme.

biased battery exhaustion and reduce additional processes, which would be necessary to handle some power managing policies. Thus, trust is estimated by the following equation [64]:

$$T_i = \frac{W_1 C_i + W_2 S_i + W_3 B_i}{\sum_{i=1}^{3} W_i} \tag{21}$$

where W_1, W_2, and W_3 are weight parameters that represent the importance of a particular factor from 0, unimportant, to 1, most important, C_i is data consistency value, S_i is communication ratio, and B_i is battery level. Trust values from several nodes on certain node are aggregated as follows [64]:

$$T_i = \frac{\sum_{j=1}^{k} (T_j + 1) \times T_{i,j}}{\sum_{j=1}^{k} (T_j + 1)} \tag{22}$$

where k is the number of repliers and $T_{i,j}$ is a trust value for node i received from node j. The advantage of

Trans. Emerging Tel. Tech. **26**:107–130 (2015) © 2013 John Wiley & Sons, Ltd.
DOI: 10.1002/ett

this scheme is that it defines data consistency checking in detail, which is important for the monitoring and learning unit of TM as shown in Table IV. So, the monitoring and learning block monitors and checks the data, in this case, and reports to the TE unit as input. Hence, correctness of the report is important to obtain correct trust value. A flaw in the scheme is that it advocates for combination of different attributes to estimate trust, which goes against the context-dependent property of trust. In addition, the authors assume that malicious nodes do not collude with each other, which is not always realistic.

Table V. Example of fuzzy rules.

		Required service attribute				
		VL	**L**	**M**	**H**	**VH**
Server goodness	**VL**	M	H	VH	VH	VH
	L	L	M	H	VH	VH
	M	VL	L	M	H	VH
	H	VL	VL	L	M	H
	VH	VL	VL	VL	L	M

VL, very low; L, low; M, medium; H, high; VH, very high.

3.3. Fuzzy logic trust-based trust management

In fuzzy logic trust modelling, trustworthiness of the node is determined on the basis of a membership function and estimated trust value [56–60]. The trust value is estimated by means of a TE method and is based on the obtained trust value. The trustworthiness degree of the node is determined using fuzzy logic. Predefined labels are used for assigning values, in which each label represents a range of possible values. The steps to determine the trustworthiness degree of the node using fuzzy logic are as follows [57]:

- Fuzzy matching: estimate the level to input.
- Inference: calculate the rule's conclusion based on its matching degree.
- Combination: combine the conclusion inferred by all fuzzy rules into a final conclusion.

Feng and colleagues [56] propose a node behavioural strategies belief theory of the trust evaluation algorithm, which combines the methods of nodes behavioural strategy and modified evidence theory. On the basis of the behaviours of sensor nodes, a variety of trust factors and coefficients related to network application direct and indirect trust values are obtained through calculating a weighted average of trust factors. Specifically, the following factors are considered to estimate direct trust:

- Received packet rate
- Successfully sent packet rate
- Packet forwarding rate
- Data consistency
- Time relativity of context content in period *t*
- Node availability
- Security grade

Indirect trust is estimated by simply multiplying the trust value of the recommendation provider with the provided trust value. To integrate direct and indirect trust, Dempster–Shafer evidence theory is used. After obtaining trust values, fuzzy classifications of trust values are performed. First, trust is divided into three states: completely distrust, uncertain, and completely trust. Second, according to the three states, three fuzzy subsets *T1*, *T2*, and *T3* are marked on the universe of nodes' trust value *T* ([0,1]). The corresponding membership functions are $u1(t)$, $u2(t)$, and $u3(t)$; $u1(t) + u2(t) + u3(t) = 1$.

Fuzzy logic enhancement of a trust mechanism for distributed networks is also proposed [58]. This trust scheme is an enhancement of BTRM-WSN (Bio-inspired Trust and Reputation Model for Wireless Sensor Networks), which is a bio-inspired algorithm based on the ant colony system. First, the trust value of the service provider is weighted on the basis of BTRM-WSN. Because the proposed trust model includes several service attributes, such as client satisfaction, service price, service cost, and delivery time, trust assessment is carried out on the basis of these parameters. To combine these parameters correctly and obtain a single trust state, linguistic fuzzy logic and reasoning are applied. The fuzzy logic operators, AND, OR, and NOT are adapted to allow for partial truth. Fuzzy operators also apply a partial-truth value to the whole logic expression. A typical if-then linguistic fuzzy rule would look like as

If quality is Good AND price is Low THEN satisfaction is Very High.

Different fuzzy grids are used in the proposed model. A fuzzy grid is a collection of fuzzy rules in a matrix form (Table V). In Table V, level of server goodness and required service attribute from very low, low, medium, high to very high is defined. Each row/column represents one of the input variables. To represent the whole input space, each row and column includes all the linguistic labels defined over the represented input variables. Several fuzzy grids are composed, similar to the grid in Table V, to define quality of service, cost, price, delivery time, and client conformity. Thus, on the basis of the quality of service, price and delivery time, and client conformity, a final client satisfaction is determined. Client satisfaction with client goodness parameters will decide the final level of reward/punishment to the service provider.

Several fuzzy grids are composed similar to previous grid (Table V) to define quality of service, cost, price, delivery time, and client conformity. Thus, on the basis of the quality of service, price and delivery time, and client conformity, a final client satisfaction is determined. Finally, client satisfaction with client goodness parameters will decide level of reward/punishment to service provider.

Fuzzy sets are important for defining and proving accuracy because it shows the trust degree of a node. However,

Table VI. Example table of cluster head.

	Agent1	Agent2	Agent3	Agent4
Send	0	12	13	8
Receive	14	0	14	11

Table VII. Node classification using fuzzy rules.

		RECEIVE		
SEND	Low	Low Trust	Medium Distrust	High Enemy
	Medium	Distrust	Trust	Distrust
	High	Enemy	Distrust	Distrust

in this work, only inference rules are defined in detail without a fuzzy membership function. As in many works, several trust-of-service attributes are combined to obtain a single trust value, which contradicts the context-dependent property of trust.

Shahaboddin and colleagues introduce another fuzzy logic-involved TM [60]. In this scheme, the network is assumed to be clustered, and each cluster has a CH, which is changed periodically. Each node maintains a table for sent and received packets of its neighbours. At every t period, the nodes in the cluster send their reports to the CH. Upon receiving the reports, the CH forms another table summing up all the reports (Table VI). After creating the table, the CH, using a Mamdani fuzzy inference system, labels fuzzy linguistic variables based on the number of sent and received packets. Moreover, using again Mamdani fuzzy inference (Table VII), it classifies nodes into trust, distrust, and enemy.

In the end, authentication is performed on suspicious nodes asking for a code that is unique. No one has access to this code. If the system receives the correct answer, then it will consider the suspicious node safe. Otherwise, the CH informs the whole network of the presence of the enemy node. Table VIII briefly explains advantages and disadvantages in the aforementioned fuzzy logic-involved TE-based TM schemes. Moreover, it provides brief descriptions and objectives of each TM scheme.

3.4. Miscellaneous trust management schemes

Felix and colleagues [61] propose trust modelling using a bio-inspired technique to obtain the most trustworthy path to a trustworthy node. It is also based on a bio-inspired algorithm of an ant colony system. It includes the following five generic steps.

(1) Gathering information. When the algorithm is launched, a set of artificial ants are deployed over the network. Each ant adds the first sensor to its solution. On the basis of a transition rule, moving direction is determined.
(2) Scoring and ranking. Once the ants have found a path leading to a node providing the requested service, a score has to be given to each of those paths. The client compares solutions and keeps the best.
(3) Entity selection. The path S_i with the highest value of $Q(Si)$ is selected by the algorithm as the one leading to the most trustworthy server in the network.
(4) Transaction. After finishing the transaction, the client then evaluates the received service and computes its satisfaction with the performed transaction.
(5) Reward and punish. Depending on the satisfaction of the client, the pheromone of the path is increased or evaporated.

Ants' pheromone degree and percentage of ants that have selected the same path show the quality. So, on the basis of service satisfaction by the server, the pheromone (trust) degree of the path is determined. Unlike other TM schemes, the scheme considers only the trust degree of the path, and there can be trustworthy nodes in the path that are punished unfairly by decreasing the trust value of the path. Hence, nodes in the path also should be considered in choosing the path. On other hand, the proposed algorithm attempts to find the best path. The weakness in this work is that it does not consider attacks such as bad mouthing, on–off attack, and so on. We believe that developing TM without considering such attacks will be meaningless because it will not allow the TM system to work properly.

Statistical trust establishment for WSNs is proposed in [68]. Behaviour of neighbourhood node is observed, and trust is determined on the basis of the observation. Mean trust value and a confidence interval about the mean are used as trust. The mean value of these trust values over time n is given as follows [68]:

$$\bar{x} = \sum_{i}^{n} \left(\frac{W_i}{\sum_i^n W_i} x_i \right) \tag{23}$$

where x_i represents the trust value of node y by node x on experience i with node y and W_i is weight factor, which depends on the behaviour of node y at experience i. Unweighted variance around the mean is determined as follows [68]:

$$\sigma_W^2 = \frac{\sigma^2 \sum W_i^2}{\left(\sum W_i\right)^2} \tag{24}$$

where σ^2 is the unweighted variance

This weighted variance is used to determine a confidence interval about the mean as follows [68]:

$$\bar{x} \pm t_{n-1,1-\alpha/2} \sqrt{\sigma_w^2 / n} \tag{25}$$

where α is 0.10 for a 90% confidence interval, 0.05 for a 95% confidence interval, for example. The t is the student t distribution. Node x will proceed with its decision-making

Trans. Emerging Tel. Tech. **26**:107–130 (2015) © 2013 John Wiley & Sons, Ltd.
DOI: 10.1002/ett

Table VIII. Comparison of fuzzy logic trust estimation-based TM approaches.

TM approach	Brief description	Objective	Advantages	Disadvantage
NBBTE [56]	Trust is estimated on the basis of seven parameters using weighting method. On the basis of fuzzy membership function, trust values are classified into different states. Dempster–Shafer combination rule applied to combine direct and indirect trust.	Security enhancement using TM.	Because Dempster–Shafer combination rule rooted mathematically, it accurately combines trust values and provides reasonable result. It might degrade system performance especially, when cooperation rate is high between nodes.	No attack consideration against TM. Computational complexity is involved in Dempster–Shafer evidence combination rule.
Felix *et al.* [58]	Trust is estimated on the basis of several parameters including quality of provided service using bio-inspired technique. Fuzzy inference rules applied to assess the quality of provided service.	Finding the path that leads to most trustworthy node.	Implementation of punishment/reward, which urges nodes to cooperate. Fully distributed.	Platform specific that is the scheme only works for finding path leading to the most trustworthy node.
Shahaboddin *et al.* [60]	Trust is estimated on the basis of the number of received and sent packets of the node using fuzzy logic method.	Detection of packet dropping and illegitimate nodes.	Trust estimation method is sound although it is not comprehensively studied.	Cluster head can be single point of failure. Bad mouthing attack is not considered in trust estimation.

TM, trust management; NBBTE, node behavioural strategies belief theory of the trust evaluation.

process unless the confidence interval is narrow. Otherwise, if the confidence interval is too wide, then additional observations are gathered. Like other TM schemes, this approach deals with only the TE, which weakens the TM system. Moreover, the authors assume that there will not be collusion attacks, which is not realistic. The merit of the proposed scheme is that it has a sound mathematical foundation, which helps to obtain accurate trust values and estimations.

A trust-based routing mechanism implementation is presented by Eissa and colleagues [69]. Although this is proposed for mobile *ad hoc* networks, implementation aspects can be used for WSNs as well. A secure *ad hoc* on-demand distance vector (AODV) routing protocol friendship mechanism is proposed, which is based on a trust feature. The idea behind the friendship mechanism is that whenever a node receives route request (RREQ) or route reply (RREP) messages, it will check whether it is from a friend list or not. If it is from a friend, then it will compare the friendship value of the route from which it received the RREQ or RREP messages with other existing routes' friendship values. Finally, it will choose the highest friendship trust value route. However, a TE of the friendship values of each hop is not demonstrated. Moreover, intermediate nodes in the route can be cooperative malicious nodes. For example, a node can forward all received packets to its malicious friends, so those malicious nodes can drop all the packets. For the implementation, the authors implement the proposed scheme in the ns-2 network simulator and a real test bed using the Java-based implementation of AODV protocol (JADHOC) framework. Because the proposed work focuses on how to build a friendship mechanism and its implementation, it does not include TE or management aspects.

Trust management is used in secure localisation [46]. One common method of localisation is to use specialty nodes known as beacon nodes, which assist other sensor nodes to determine location. If the beacon nodes are compromised or malicious, they will provide wrong information about location and mislead the other nodes. To find trustworthy beacon nodes, it uses a quorum voting approach. Specifically, a sensor must obtain votes for its trustworthiness from at least half the common neighbours. It is demonstrated that the proposed scheme is

Table IX. Trust estimation model comparison.

TE model	Trust estimation method	Assumption	Advantages	Limitations
Probabilistic-based method	Mainly using Bayesian approach with beta distributions.	It is assumed that binary ratings follow probability distributions.	Mathematically sound.	High computation complexity.
Weighting-based method	Weight misbehaviour and good behaviour using a certain proposed method.	It is assumed that produced trust values represent trustworthiness and trust relationships accurately.	Simple to implement and low computation complexity.	Accurateness of the estimated trust value and granularity of expressing the trust relationships should be verified.
Fuzzy-logic involved method	Estimate trust by means of weighting-based method or any other method and quantise trust values using fuzzy logic rules.	Membership function assumptions.	Fuzzy part is mathematically sound and easy to implement. Moreover, it allows trust value classifications to be more accurate.	Fixed membership functions might not correctly represent the trustworthiness of the node because of dynamism of the trust phenomena.

TE, trust estimation.

resilient against attack provided that the percentage of malicious nodes is less than 30 and the neighbourhood is dense enough. Robustness of the proposed scheme can be improved further if bad mouthing attacks are considered in second-hand information (recommendation) aggregation.

4. DISCUSSIONS AND OPEN RESEARCH ISSUES

In this section, we will compare and discuss TE models. Moreover, we will explore the current state of research of TM in WSNs by comparing and discussing selected state-of-the-art TM approaches.

4.1. Discussions

Table IX shows comparisons and descriptions of TE models. As we stated, because TE is central to TM, researchers were mainly focused on developing TE methods that can be classified as probabilistic, weighting, and fuzzy logic-based methods. In probabilistic TE, trust is envisioned as a probability of expected behaviour (normal behaviour) of a node. Beta probability distribution is mainly used because of its compatibility with TE parameters and procedure. To update trust, Bayesian theory or a simple summing method is used. One of the advantages of such an approach is its compatibility with TE parameters. For example, beta distribution is defined on the interval [0, 1] parameterised by two positive shape parameters, denoted by α and β, for good and bad behaviour over a certain time. Moreover, because it is rooted mathematically, it can express trust relations accurately and provide accurate trust values. However, one of the disadvantages of the probabilistic TE method is high computational complexity. Because sensor node capability may not allow complex computations and complex computations may require high energy consumption, it is not desirable and might not be feasible as well. Furthermore, it is assumed that binary ratings will follow probability distributions. On the other hand, weighting-based TE schemes provide a lightweight and simple method to estimate and update trust, although they are not deeply rooted mathematically. Granularity of the trust relationships may not be good when trust is modelled using weighting-based methods. Hence, correctness of the trust values, expressing the trust relationships correctly, and trust dynamics should be assured when TE is modelled on the basis of the weighting method. Another simple and lightweight approach to estimate trust is fuzzy logic-based methods. Trust is estimated in this approach using either fuzzy logic tools or any other method and is based on obtained results. Level of obtained trust value is determined using fuzzy logic inference and membership rules. Compatibility of fuzzy logic inference with node state classification and its impact on performance should be studied further.

In Table X, comparison of state-of-the-art TM approaches in terms of TM units, energy awareness, and considered attacks is presented. These three factors are important for TM and WSNs to consider. The defined TM units in Section 2 are essential for TM, and analysing each TM approach in terms of TM units allows us to know how much each unit is considered by researchers. Moreover, it shows how much TM is envisioned by researchers as a complete system rather than a trust estimator or trust relationship manager. The considered attacks in TM approaches show the robustness against attacks and the developed defense mechanisms against each stated attack. Finally, energy efficiency is vital to WSN applications because of the limited capacity of the battery of the sensor node.

Trans. Emerging Tel. Tech. **26**:107–130 (2015) © 2013 John Wiley & Sons, Ltd.
DOI: 10.1002/ett

Table X. Comparison of state-of-the-art TM approaches.

TM scheme	Trust estimation method	Considered TM units			Considered attacks			Energy awareness
		Monitoring and learning	Trust evaluation	Recommendation management	Bad mouthing	On–off	Conflicting behaviour	
RFSN [12]	Probabilistic	v	v	v	v	v	x	Energy efficiency considered in node monitoring as well as in trust estimation.
GTMS [5]	Weighting	/	v	v	v	v	v	A proper format for trust value such as integer value (0–100) is chosen. It requires less memory and energy to store and propagate.
PLUS [62]	Weighting	v	v	v	x	x	x	Energy efficiency is considered in the proposed recommendation exchange protocol.
OTMF [51]	Probabilistic	/	v	/	v	v	v	The paper introduces a framework for TM, and the main focus is robustness and security issues. Hence, details of the work including energy issues are not presented.
NBBTE [56]	Fuzzy logic-involved	/	v	/	x	x	x	Because work focuses on trust modelling only,energy issues are not taken into account.
Yan *et al.* [54]	Probabilistic	/	v	v	v	v	v	Because this work deals with TM security analyses and attacks, energy issues are not discussed.
Garth V *et al.* [52]	Probabilistic	x	v	/	v	x	x	Energy efficiency is outside of the scope of the paper.
Wang *et al.* [67]	Different	v	v	/	x	x	x	Energy issues are not considered in any aspect of trust modelling

TM, trust management; RFSN, reputation-based framework for high-integrity sensor network; GTMS, group-based TM scheme; PLUS, parameterised and localised TM scheme; OTMF, objective TM framework; NBBTE, node behavioural strategies belief theory of the trust evaluation.

Table XI. Feasibility level of proposed TM schemes.

TM scheme	Communication cost	Computation complexity	Scalability
RFSN [12]	Medium	High	Low
GTMS [5]	Low	Low	High
PLUS [62]	—	Medium	Medium
OTMF [51]	—	High	Medium
NBBTE [56]	—	High	High
Yan *et al.* [54]	—	High	Medium
Garth *et al.* [52]	Medium	High	Medium
Wang *et al.* [67]	Medium	High	Medium

TM, trust management; RFSN, reputation-based framework for high-integrity sensor network; GTMS, group-based TM scheme; PLUS, parameterised and localised TM scheme; OTMF, objective TM framework; NBBTE, node behavioural strategies belief theory of the trust evaluation.

In Table X, 'v' means the TM approach includes either a fully developed or a considered mechanism (algorithm) for the TM unit or defense techniques against attacks. On other hand, '/' means the TM approach does not consider comprehensive mechanisms, or it pertains to other references. 'x' means the TM approach does not consider any mechanism (algorithm) but assumes only that such a mechanism exists. Note that the objective of such analyses is not to find disadvantages in the papers but to comprehensively know the state of the research. We can see from the table that many of the TM approaches do not consider all TM units at once. Among TM units, monitoring and learning receive less attention by researchers. On other hand, trust evaluation is comprehensively considered by researchers. Results of the analyses show that trust monitoring and recommendation management need more attention. Our next evaluation parameter for TM approaches is attacks. Although conflicting behaviour receives the least attention by researchers, as Table X shows, other types of attacks also need more comprehensive studies. As we can see, some TM approaches ignore defense mechanisms totally. The next evaluation parameter for TM approaches is energy efficiency. Although energy efficiency is taken into account in the proposed TM approaches, it is not in all aspects of TM. According to our best knowledge, no TM approach considers energy efficiency in each aspect of TM modelling. Because TM management modelling in WSNs is in its infancy, many open issues should be addressed, including energy efficiency. We will discuss those open issues in detail in the next subsection. Table XI shows the general feasibility level of the proposed schemes. Communication cost shows the frequency and overhead of recommendation exchange, and other communication message exchanges to maintain the TM system. Computation complexity demonstrates complexity and frequency of TE, update and aggregation equations, and other computations. Scalability level shows the scalability of the proposed scheme in terms of message exchange and computational cost. Specifically, it shows increasing of the message exchange and computational cost with increasing numbers of nodes.

4.2. Open research issues

After analysing state-of-the-art TM approaches in the previous section, we will discuss open research issues more in detail in this subsection. As we stated, TM is rarely designed as a whole system in published research papers. Rather, it is envisioned as a trust estimator or as trust establishment. However, we believe that to benefit fully from TM and improve system performance, it should be designed as a system with consideration paid to defense mechanisms against attacks. Hence, one of the important open issues is to develop TM as whole system, which includes defense mechanisms and three basic components (Figure 1). Moreover, energy consumption and lightweight factors in the design of TM are rarely considered. To gain more insight about these open issues, we will discuss them unit by unit and then present some other issues.

Monitoring and learning. This component is one of the least studied components of TM. Usually, authors assume that a node can monitor its neighbourhood and detect a malicious node without specifying any method. Although some authors specify some monitoring method, such as a watchdog mechanism, it has limitations that should be considered further [70]. Furthermore, this unit consumes high energy due to monitoring and learning so often. Hence, this requires special attention to efficiently maintain monitoring and detection while staying energy aware.

Trust evaluation. We can say that the TE part of TM received most of the attention in the research because it is the engine of TM. Although it received a lot of attention by researchers, there are issues still to be addressed. Network dynamics usually are not taken into account in the calculation of trust. Because WSNs are deployed in an environment that is usually harsh and dynamic, this factor easily can affect trust values by artificially increasing or decreasing them. Another fundamental issue is including the number of good behaviour/successful operations in a TE. It gives an intelligent attacker node a chance to manipulate its good behaviours/successful operations and obtain a high trust value while launching attacks. Another open

Trans. Emerging Tel. Tech. **26**:107–130 (2015) © 2013 John Wiley & Sons, Ltd.
DOI: 10.1002/ett

research issue is the lack of methods dealing with trust value classification. How to classify trust values is rarely studied in the current literature.

Trust propagation. Message overhead in trust propagation is an important issue, which is generally not considered by the researchers. Moreover, a malicious node can exhaust the energy of the neighbouring nodes and degrade network performance by sending unnecessary recommendations continuously. A trust propagation protocol is required that considers energy efficiency and security.

Attack resistance. Robust defense mechanisms are needed for controversial behaviour and the Sybil attack, which can seriously affect the performance of a TM system. Existing TM literature either ignores these problems or attempts to mitigate the effect of these problems by making different assumptions. Moreover, performance evaluation and comparison of the defense mechanisms are not a well-studied area. It is important to assess the relative strengths and weaknesses of defense mechanisms under a variety of factors.

Performance comparison of TM systems. For the most part in the proposed TM schemes, only qualitative comparisons are provided. These comparisons do not demonstrate relative strengths and weaknesses of the different TM schemes under different scenarios. A set of performance metrics and software test beds should be developed to facilitate such comparisons.

Node mobility and heterogeneity. These factors are generally not taken into consideration in the existing TM literature. Because applications of WSNs might require node mobility or heterogeneity, it is important to design TM that considers these factors. Developing a TM scheme under node mobility can be challenging because monitoring and maintaining trust for a mobile node will not be an easy task.

5. CONCLUSION

Trust and its management in WSNs attract a lot of attention from the researchers. In this paper, we presented and widely discussed TM issues in WSNs. Specifically, the concept of TM, basic functional units of TM, design factors of TM, and TM-related attacks are discussed. One of the goals of this paper is to highlight design factors of TM in WSNs. On the basis of the features of WSNs and requirements of TM, we proposed five important design factors: robustness, accurateness, energy efficiency and lightness, scalability, and the TM as system. Moreover, on the basis of defined design factors and TM units, we demonstrated the current state of research by comparing recently proposed TM schemes. Comparison results show that the monitoring component of TM receives the least attention, and TM is rarely envisioned as a system by researchers. Moreover, energy efficiency is not considered in all aspects of TM. Other open research issues were presented and discussed widely. We hope that this comprehensive survey will help TM researchers to design desirable TM schemes and to shed light on current status and open research issues.

ACKNOWLEDGEMENTS

This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Science, ICT, and Future Planning (NRF-2012R1A1B4000536).

REFERENCES

1. Akyildiz IF, Su W, Sankarasubramaniam Y, Cayirci E. Wireless sensor networks: a survey. *Computer Networks (Elsevier) Journal* 2002; **38**: 393–422.
2. Chee YC, Kumar SP. Sensor networks: evolution, opportunities, and challenges. *Proceedings of the IEEE* 2003; **91**: 1247–1256.
3. Yan S, Wei Y, Zhu H, Ray KJL. Information theoretic framework of trust modeling and evaluation for ad hoc networks. *IEEE JSAC Special Issue on Security in Wireless ad hoc Networks* 2006; **4**: 305–317.
4. Jean MS, Adam S. *Collaborative Computer Security and Trust Management*. IGI Global: Hershey, Pennsylvania (USA), 2010.
5. Shaikh RA, Jameel H, D'Auriol BJ, Lee H, Lee S, Song YJ. Group based trust management scheme for clustered wireless sensor networks. *IEEE Transactions on Parallel and Distributed Systems* 2009; **11**: 1045–9219.
6. Lopez J, Roman R, Alcaraz C. Analysis of security threats, requirements, technologies and standards in wireless sensor networks. *LNCS* 2009; **5705**: 289–338.
7. Yanli Y, Keqiu L, Wanlei Z, Ping L. Trust mechanisms in wireless sensor networks: attack analysis and countermeasures. *Journal of Network and Computer Application* 2011; **35**(3): 867–880.
8. Govindan K, Mohapatra P. Trust dynamics in mobile adhoc networks: a survey. *IEEE Communications Surveys and Tutorials* 2012; **14**(2): 279–298.
9. Han Y, Zhiqi S, Chunyan M, Leung C, Niyato D. Survey of trust and reputation management systems in wireless communications. *Proceedings of the IEEE* 2010; **98**(10): 1755–1772.
10. Yan S, Wei Y, Zhu H, Ray KJL. A trust evaluation framework in distributed networks: vulnerability analysis and defense against attacks, In *Proceeding of IEEE INFOCOM*, Barcelona, Spain, 2006; 1–13.
11. Boukerch A, Xu L, Khatib KE. Trust-based security for wireless ad hoc and sensor networks. *Computer Communications* 2007; **30**: 3905.

12. Ganewarial S, Laura KB, Srivastava MB. Reputation-based framework for high integrity sensor networks. *ACM Transactions on Sensor Networks* 2008; **4**: 1–36.
13. Cho JH, Chen IR. A survey on trust management for mobile ad hoc networks. *IEEE Communications Surveys and Tutorials* 2010; **13**: 562–583.
14. Zheng Y, Holtmanns S. Computer Security and Politics: Computer Security, Privacy and Politics: Current Issues, Challenges and Solutions, 2008.
15. Grandison T, Sloman M. A survey of trust in internet applications. *IEEE Communications Surveys and Tutorials* 2000; **3**(4): 2–16.
16. Zheng Y. Autonomic trust management in a component based software system. *IEEE Transactions on Dependable and Secure Computing* 2010; **8**(6): 810–823.
17. Efthimia A, Gritzalis A, Skianis G. Trust establishment in ad hoc and sensor networks. *CRITIS* 2006; **12**: 179–194.
18. Jsang A, Ismail R, Boyd C. A survey of trust and reputation systems for online service provision. *Decision Support Systems* 2007; **43**(2): 618–644.
19. Yan S, Zhu H, Liu KJR. Defense of trust management vulnerabilities in distributed networks. *IEEE Communications Magazine* 2008; **46**: 112–119.
20. Felix GM, Perez GM. Security threats scenario in trust and reputation models for distributed systems. *Computers and Security* 2009; **28**: 545–556.
21. Newsome J, Shi E, Song D, Perrig A. The sybil attack in sensor networks: analysis and defenses, In *Proceedings of IPSN '04*, Berkeley, California, USA, 2004; 259–268.
22. Microsoft JD, Douceur JR, Donath JS. The Sybil attack, In *IPTPS*, Cambridge, MA, USA, 2002; 251–260.
23. Manzo M, Roosta T, Sastry S. Time synchronization attacks in sensor networks, In *Proceedings of the 3rd ACM Workshop on Security of ad hoc and Sensor Networks*, Alexandria, VA, USA, 2005; 107–116.
24. Yang Y, Sun Y. Securing time-synchronization protocols in sensor networks: attack detection and self-healing, In *Proceeding of Global Telecommunications Conference, IEEE GLOBECOM*, New Orleans, LA, USA, 2008; 1–6.
25. Kaplantzis S, Shilton A, Mani N, Sekercioglu YA. Detecting selective forwarding attacks in wireless sensor networks using support vector machines, In *Proceedings of 3rd International Symposium on Intelligent Sensors, Sensor Networks and Information Processing*, Melbourne, Australia, 2007; 335–340.
26. Mohammad M, Subhash Ch. A GTRSSN: Gaussian trust and reputation system for sensor networks. *SCSS* 2007; **1**: 343–347.
27. Resnick P, Zeckhauser R. Trust among strangers in internet transactions: empirical analysis of ebays reputation system, In *Working Paper for the NBER Workshop on Empirical Studies of Electronic Commerce*, Boston, USA, 2001; 1–26.
28. Roy SD, Singh SA, Choudhury S, Debnath NC. Countering sinkhole and black hole attacks on sensor networks using dynamic trust management, In *Proceedings of ISCC 2008*, Marrakech, Morocco, 2008; 537–542.
29. Meghdadi M, Ozdemir S, Gler I. A survey of wormhole-based attacks and their countermeasures in wireless sensor networks. *IETE Technical Review* 2011; **28**: 89–102.
30. Misra S, Vaish A. Reputation-based role assignment for role-based access control in wireless sensor networks. *Computer Communications* 2011; **34**: 281–294.
31. Zhan G, Shi W, Deng J. Design and implementation of TARF: a trust-aware routing framework for WSNs. *IEEE Transactions on Dependable and Secure Computing* 2012; **9**(2): 184–197.
32. Kiran YB, Mallapur JD, Hiremath JD. Trust based secured routing in wireless multimedia sensor networks, In *Proceeding of Computational Intelligence, Communication Systems and Networks (CICSyN)*, Madrid, Spain, 2012; 53–58.
33. Zheng X. A secure routing scheme for static wireless sensor networks, In *Proceedings of Computational Intelligence and Industrial Application*, Wuhan, China, 2008; 776–780.
34. Faye Y, Niang I, Noel T. A survey of access control schemes in wireless sensor networks. *World Academy of Science, Engineering and Technology* 2011; **59**: 814–823.
35. Aivaloglou E, Gritzalis S. Trust based data disclosure in sensor networks, In *Proceedings of IEEE Communications, ICC '09*, Dresden, Germany, 2009; 1–6.
36. Felkner A. How the role-based trust management can be applied to wireless sensor networks. *Journal of Telecommunications and Information Technology* 2012; **4**: 70–77.
37. Ozdemir S. Functional reputation based reliable data aggregation and transmission for wireless sensor networks. *Computer Communications* 2008; **31**: 3941–3953.
38. Poolsappasit N, Madria S. A secure data aggregation based trust management approach for dealing with untrustworthy motes in sensor network, In *Proceedings of International Conference on Parallel Processing*, Taipei, Taiwan, 2011; 138–147.
39. Ozdemir S, Xiao Y. Secure. Data aggregation in wireless sensor networks: a comprehensive overview. *Computer Networks* 2009; **53**: 2022–2037.
40. Hur J, Lee YH, Hong S, Yoon H. Trust-based secure aggregation in wireless sensor networks. *International Conference on Computing, Communications and Control Technologies* 2005; **3**: 1–6.

41. Fung CJ, Zhang J, Boutaba R. Dirichlet-based trust management for effective collaborative intrusion detection networks. *IEEE Transactions on Network and Service Management* 2011; **8**(2): 79–91.
42. Bao F, Chen I, Chang MJ, Cho JH. Hierarchical trust management for wireless sensor networks and its applications to trust-based routing and intrusion detection. *IEEE Transactions on Network and Service Management* 2012; **9**(2): 169–183.
43. Zhang T, He J, Zhang Y. Trust based secure localization in wireless sensor networks, In *Proceedings of International Symposium on Intelligence Information Processing and Trusted Computing*, 2011; 55–58.
44. Liu K, Abu-Ghazaleh N, Kang KD. Location verication and trust management for resilient geographic routing. *Journal of Parallel Distributed Computing* 2007; **67**: 215–228.
45. Tanachaiwiwat S, Dave P, Bhindwale R, Helmy A. Location-centric isolation of misbehavior and trust routing in energy-constrained sensor networks, In *Proceedings of Performance, Computing, and Communications*, Phoenix, Arizona, USA, 2004; 463–469.
46. Srinivasan A, Teitelbaum J, Wu J. DRBTS: distributed reputation system based beacon trust system, In *Proceedings of Dependable, Autonomic and Secure Computing*, Indianapolis, USA, 2006; 277–283.
47. Healy M, Van de Ven P, Hayes MJ, Nelson J, Newe T, Lewis E. A comparative review of wireless sensor network mote technologies, In *Proceeding of Sensors Conference, IEEE*, Christchurch, New Zealand, 2009; 1439–1442.
48. Ishmanov F, Malik AS, Kim SW. Energy consumption balancing (ECB) issues and mechanisms in wireless sensor networks (WSNs): a comprehensive overview. *European Transactions on Telecommunications* 2011; **22**: 151–167.
49. Shaikh RA, Lee YK, Lee SY. An extended energy consumption analysis of reputation-based trust management schemes of wireless sensor networks. *Journal of Networks, Academy Publishers* 2010; **5**(3): 283–291.
50. Fung CF, Zhang J, Aib I, Boutaba R, Cohen R. Design of a simulation framework to evaluate trust models for collaborative intrusion detection, In *Proceedings of IFIP Network and Service Security Conference (N2S 09)*, Paris, France, 2009; 1–5.
51. Jie L, Ruidong L, Jien K. Future trust management framework for mobile ad hoc network. *IEEE Communications Magazine* 2008; **46**: 108–114.
52. Garth VC, Lance H, Niki P. Location-aware, trust-based detection and isolation of compromised nodes in WSNs. *International Journal of Network Security* 2011; **2**: 107–113.
53. Maarouf UB, Naseer AR. Efficient monitoring approach for reputation system-based trust aware routing wireless sensor networks. *IET Communications* 2009; **3**: 846–858.
54. Yan S, Wei Y, Zhu H, Ray KRL. Information theoretic framework of trust modeling and evaluation for ad hoc networks. *IEEE JSAC* 2006; **24**: 305–317.
55. Rino F, Giovanni P, Cristiano C. A fuzzy approach to belief-based trust computations. *Lecture Notes on Artificial Intelligence* 2003; **11**: 1–15.
56. Feng R, Xu X, Zhou X, Wan J. A trust evaluation algorithm for wireless sensor networks based on node behaviors and D-S evidence theory. *Sensors* 2011; **11**: 1345–1360.
57. Kim TK, Seo HS. A trust model using fuzzy logic in wireless sensor network. *World Academy of Science, Engineering and Technology* 2008; **42**: 63–66.
58. Flix GM, Javier G, Marn B, Gregorio MP. Linguistic fuzzy logic enhancement of trust mechanism for distributed networks, In *Proceedings of International Conference on Computer and Information Technology*, Bradford, West Yorkshire, UK, 2010; 838–845.
59. Hongjun D, Zhiping J, Zhiwei Q. Trust evaluation and dynamic routing decision based on fuzzy theory for MANETs. *Journal of Software* 2009; **4**: 1091–1101.
60. Shahaboddin Sh, Samira K, Zeinab SD, Liang SN. Expert security system in wireless sensor networks based on fuzzy discussion multi-agent system. *Scientific Research and Essays* 2010; **5**: 3840–3849.
61. Felix GM. Providing trust in wireless sensor networks using a bio-inspired technique *NAEC'08*, 2008.
62. Zhiying Y, Ki D, Do YM. PLUS: parameterised localised trust management-based security framework for sensor networks. *International Journal of Sensor Networks* 2008; **3**: 224–236.
63. Han G, Lei S, Ma J, Park JH, Ni J. Power-aware and reliable sensor selection based on trust for wireless sensor networks. *Journal of Communications* 2010; **5**: 23–30.
64. Junbeom H, Lee YH, Hong SM, Yoon HS. Trust management for resilient wireless sensor networks. *Lecture Notes in Computer Science* 2006; **3935**: 56–68.
65. Bin M, Xianzhong X. Smart Wireless Sensor Networks, 2010.
66. Fenye B, Ing-Ray Ch, Moon JC, Jin-Hee Cho. Trust-based intrusion detection in wireless sensor networks, In *IEEE Communications (ICC)*, Kyoto, Japan, 2011; 1–6.
67. Wang X, Ding L, Sheng W. Trust evaluation sensing for wireless sensor networks. *IEEE Transactions on Instrumentation and Measurement* 2011; **60**(6): 2088–2095.
68. Probst MJ, Kasera SK. Statistical trust establishment in WSNs, In *Proceedings of Parallel and Distributed Systems, International Conference*, Hsinchu, Taiwan, 2007; 1–8.

69. Eissa T, Abdul Razak SH, Rashid Kh, Normalia S. Trust-based routing mechanism in MANET: design and implementation. *Mobile Networks and Applications* 2011; **16**: 1–12.

70. Cho Y, Qu G, Wu Y. Insider threats against trust mechanism with watchdog and defending approaches in wireless sensor networks, In *IEEE Security and Privacy Workshops (SPW)*, San Francisco, CA, USA, 2012; 134–141.

Trans. Emerging Tel. Tech. **26**:107–130 (2015) © 2013 John Wiley & Sons, Ltd.
DOI: 10.1002/ett