SECURITY AND COMMUNICATION NETWORKS
Security Comm. Networks (2012)
Published online in Wiley Online Library (wileyonlinelibrary.com). DOI: 10.1002/sec.597

REVIEW ARTICLE

Comparative study of trust and reputation systems for wireless sensor networks

Osman Khalid[1], Samee U. Khan[1], Sajjad A. Madani[2], Khizar Hayat[2], Majid I. Khan[2], Nasro Min-Allah[2], Joanna Kolodziej[3], Lizhe Wang[4], Sherali Zeadally[5] and Dan Chen[6]

[1] North Dakota State University, Fargo, ND, U.S.A.
[2] COMSATS Institute of Information Technology, Islamabad, Pakistan
[3] Cracow University of Technology, Cracow, Poland
[4] Center for Earth Observation and Digital Earth, Chinese Academy of Sciences, Beijing, China
[5] University of the District of Columbia, Washington DC, U.S.A.
[6] China University of Geosciences, Wuhan, China

ABSTRACT

Wireless sensor networks (WSNs) are emerging as useful technology for information extraction from the surrounding environment by using numerous small-sized sensor nodes that are mostly deployed in sensitive, unattended, and (sometimes) hostile territories. Traditional cryptographic approaches are widely used to provide security in WSN. However, because of unattended and insecure deployment, a sensor node may be physically captured by an adversary who may acquire the underlying secret keys, or a subset thereof, to access the critical data and/or other nodes present in the network. Moreover, a node may not properly operate because of insufficient resources or problems in the network link. In recent years, the basic ideas of trust and reputation have been applied to WSNs to monitor the changing behaviors of nodes in a network. Several trust and reputation monitoring (TRM) systems have been proposed, to integrate the concepts of trust in networks as an additional security measure, and various surveys are conducted on the aforementioned system. However, the existing surveys lack a comprehensive discussion on trust application specific to the WSNs. This survey attempts to provide a thorough understanding of trust and reputation as well as their applications in the context of WSNs. The survey discusses the components required to build a TRM and the trust computation phases explained with a study of various security attacks. The study investigates the recent advances in TRMs and includes a concise comparison of various TRMs. Finally, a discussion on open issues and challenges in the implementation of trust-based systems is also presented. Copyright © 2012 John Wiley & Sons, Ltd.

KEYWORDS
trust; repute; WSN; trust and reputation systems

***Correspondence**
Samee Khan, Electrical & Computer Engineering Dept, 1411 Centennial Blvd, North Dakota State University, Fargo, ND 58102, U.S.A.
E-mail: samee.khan@ndsu.edu

1. INTRODUCTION

Wireless sensor networks (WSNs) consist of thousands of tiny embedded computers known as motes. Each mote is equipped with a specific type of sensor to sense information from surrounding environment. The collected information is relayed from sensor to sensor, using a secure multihop routing protocol, until the data reaches the desired destination, known as sink, as shown in Figure 1. At the sink, the data aggregation and analysis takes place [1,2]. The WSN technology has applications in many areas, such as industry, environment, seismology, construction, transportation, military warfare, traffic control, and agriculture [3,4]. Despite their quick deployment and significant advantages over traditional methods, WSNs have to overcome various security problems because of the possibility of the presence of one or more faulty and malicious nodes in the network. A sensor node is always at risk of being compromised by an adversary, who may capture the node's cryptographic keys. Such an attack is also referred as *insider* attack [5] in which an adversary node would appear to be a legitimate member of the network. Once a sensor node is captured, an adversary may sniff and inject packets with falsified data that may compromise the node's data integrity. The adversary may reprogram the sensor node to carry out various tasks that may eventually prove detrimental to the overall system. Therefore, security and privacy challenges of WSN must

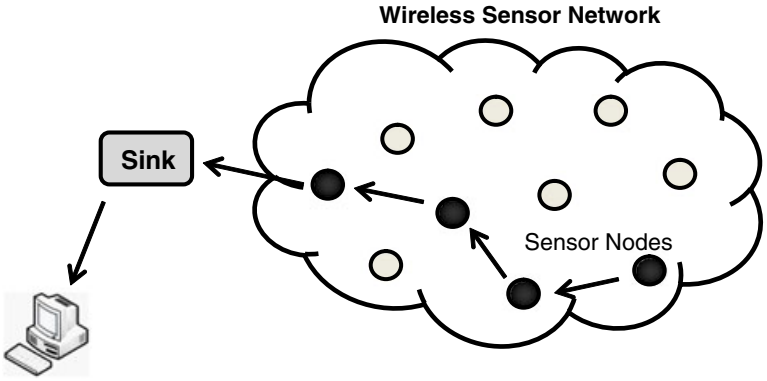

Figure 1. A wireless sensor network consists of numerous autonomous nodes where each node collects data from environment and sends to a sink for analysis by the user.

be addressed to prevent the system from turning against those for whom the system has to render benefit. Although external security attacks on WSN may be countered by the use of cryptographic techniques, cryptography is not that effective against the internal insider attacks by the malicious node. In addition, the nodes are constrained by their limited resources in the form of processing capability, bandwidth, and storage. Therefore, the nodes cannot support the heavy computations of cryptography-based protocols. The aforementioned limitations necessitate the design of security protocols that are resource economical, provide acceptable degree of protection at node-level decision making, and meet the security demands of the application.

One approach that has gained global recognition in providing an additional means of security for decision making in WSNs (i.e., to trust a node for communication or not) is the trust and reputation monitoring (TRM) system. TRM deals with the problem of uncertainty in decision making, by keeping the history of a node's previous behavior (repute). A node is trusted and will be forwarded with the packets only if the node holds a good repute; otherwise, the node will be considered untrustworthy. TRM provides a natural choice for security in open systems—the Internet and social networking—for being computationally tractable.

For the past few years, there has been much research in the area of TRMs for WSNs [6–16]. In the literature, the concepts of trust have been applied to various network layers to enable the nodes to take appropriate decisions in identifying the adversaries. Numerous surveys have been conducted on the subject in various network domains [17–26]. In [17,18,23], the authors restricted their analysis to various trust models in the context of mobile ad hoc networks (MANETs). In [21,24], the authors discussed different applications of trust in a general wireless communication environment, whereas in [22], the authors presented an overview of trust applications in various other domains (not specific to WSN). In [25], the authors surveyed the trust protocols for secure localization in WSN. The authors in [26] compared some TRMs, but most of the techniques presented in the paper are not recent. In [20], the authors indicated some best practices in developing a trust model for WSN, but the thorough discussion is lacking on actual working of the models referenced in the paper.

Most of the aforementioned surveys focus on either trust application for MANETs or other domains but do not specifically target WSNs. In contrast, this survey attempts to address these deficiencies and provides a focused study on the application of trust and reputation in WSNs. We describe in detail how a TRM is modeled, what major elements a TRM is made of, and what phases are involved in modeling a TRM. Through various examples, we illustrate how trust and reputation have the potential to be effective for providing an increased security in WSNs, along with the cryptography. After providing a general understanding of trust and reputation modeling, we compare some of the latest proposals for TRMs. The survey highlights the important characteristics of selected TRMs and discusses their pros and cons.

The rest of the survey is organized as follows. Section 2 presents an overview of the current network security techniques followed by an introduction to trust and reputation. This section further discusses the security threats a WSN may encounter. Section 3 treats the TRM in detail by exploring the various components. Section 4 presents a comparison of various state-of-the-art TRMs with a taxonomy presented in Section 5. The hot open issues and recent challenges in the implementation of trust-based systems in future-generation WSNs are discussed in Section 6. The paper is concluded in Section 7.

2. SECURITY, TRUST, AND REPUTATION

In a computer network, it is very important to control the authentication and authorization of data and services. Using authentication, only valid users must have access to the system, and only those resources should be allowed to a user for which the user is authorized. Similarly, to maintain the confidentiality and integrity of data, some form of data encryption/decryption using techniques such as cryptography may also be required (Figure 2). Much research has been done to ensure a secure and reliable communication among

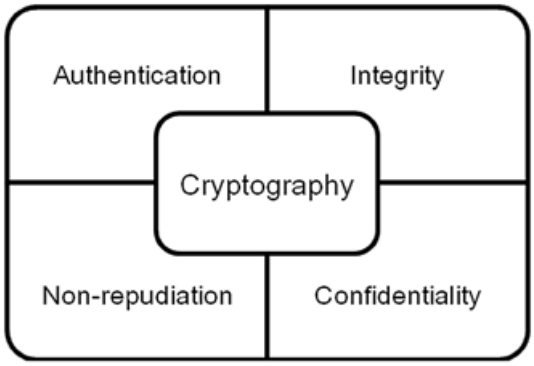

Figure 2. The various services in terms of security provided by cryptography technique.

the network devices, and many security protocols have been devised. In this section, we first present a brief overview of the existing security methods and then discuss the notions of trust and reputation and their applications in WSN

2.1. Security

In practice, to ensure the secure communication among devices, cryptography is considered one of the most reliable tools. Cryptographic protocols are designed to securely encrypt data for safe transfer across a network, by using some cipher (encryption algorithm) to generate a cipher text (encrypted data). Normally, the encryption is carried out using some secret key(s), known to the sender and/or recipient. The two basic approaches of cryptography are the following: (i) symmetric key cryptography and (ii) asymmetric key cryptography [27]. In the symmetric key cryptography, both sender and receiver share a commonly shared secret key that is used to encrypt and decrypt the data. In contrast, the asymmetric key cryptography implies the use of two different keys: (i) public key and (ii) private key. The sender encrypts the message by using recipient's public key, and the recipient decrypts the message by using private key. The popular algorithms for the asymmetric key cryptography are Rivest, Shamir, and Adleman [28] and Diffie–Hellman [27].

In WSNs, the symmetric key cryptographic techniques are mostly used, and the most commonly referred cryptographic protocols are elaborated in Table I. The sensor node authentication is usually performed by the use of hash functions and digital signatures. The application of asymmetric cryptography is limited to secure the distribution of lightweight secret keys, shared among the participating nodes. This is because asymmetric key cryptography requires intense mathematical computations beyond the capability of a sensor node that is limited because of lesser resources, be it processing, space, or battery power. Even if all sensors have sufficient memory and processing power, the necessary cryptographic procedures and primitives based on the symmetric and asymmetric protocols are usually too expensive for the most resource-constrained network devices.

An interesting method of improvement of the well-known cryptographic server or base station-based solutions was proposed by Dutertre *et al.* in [29]. The authors defined the autonomous key-management services that allow to share the small sets of secret keys among the neighboring sensors and improve the scalability of the system (the number of keys required does not increase with the network size). Xiao *et al.* presented in [30] a detailed survey and taxonomy of key management methods in WSN classified into seven main categories, namely, (i) single network-wide key, (ii) pairwise key establishment, (iii) trusted base station, (iv) public key schemes (elliptic curve cryptography), (v) key predistribution schemes, (vi) dynamic key management, and (vii) hierarchical key management.

Despite all that significant volume of research that has been published and implemented [31,95] in the domain of the effective key management in WSN, it seems that cryptography still may not be sufficient to provide complete security to the sensor nodes. Therefore, in many realistic approaches, some additional security layer is required. In the next subsection, we discuss the usage of trust and reputation as a supplement for the current cryptographic security mechanisms.

2.2. Trust and reputation

In recent years, TRMs have emerged as useful methodologies for the provision of security in WSNs. The use of the words "trust" and "reputation" is commonplace in our daily lives. The repute of a person is established from previously performed actions. If a person is consistently honest, then

Table I. Example proposals, from the literature for cryptographic security implementation of WSNs.

Proposal	Description
SPINS [59]	Provides data confidentiality, authentication, and freshness (SNEP) and authenticated broadcast (μTESLA)
TinySec [60]	Provides security at the link layer and is implanted on TinyOS
SERP [61]	Use of cryptographic keys to authenticate an event report
TinyPK [62]	Use of RSA public key techniques for security on TinyOS
SEF [63]	Message validation through multiple-keyed MACs and additional filtering in sink node
INSENS [64]	Use of hash-chained MAC to secure the routing

WSN, wireless sensor network; SNEP, secure network encryption protocol; RSA, Rivest, Shamir, and Adleman; MAC, message authentication code; SPINS, security protocols for sensor network; SERP, secure event reporting protocol; SEF, statistical en-route filtering; INSENS, INtrusion-tolerant routing protocol for wireless SEnsor NetworkS.

with time, his or her reputation would be good, and everybody would trust him or her. The same concept is applied in TRMs; a node will prefer to interact with a well-reputed neighboring node. In the context of WSNs, from different literature resources, one can find various definitions of trust [32,24], all with the same implications.

In practice, *trust* is defined as how much a node matches the expectations of another node. The concept of trust is especially important in an environment where there is some degree of uncertainty. In WSNs, the nodes are always at risk of being compromised by an adversary. The most common applications of trust in WSNs include, but are not limited to, malicious node identification, secure routing, secure cluster head selection, and secure data collection [33].

In contrast to trust, the term *reputation* may be defined as the global perception about a node of being trustworthy, or otherwise, in a network [24]. The reputation is the collective trust opinion of other nodes about the behavior of a subject node. In other words, reputation may be understood as the trustworthiness of a node [34]. Repute is the measure of belief in a node that cannot be physically quantified through discrete values. Moreover, the reputation is used to perform statistical prediction of a node's behavior. In TRMs, the repute is usually represented as R_{ij}—the reputation of node j is computed by node i. Unlike trust, the reputation is computed and stored as a probabilistic distribution [6,35–37]. In a network, each sensor node maintains the repute of neighboring network nodes, in a data structure, called a reputation table RT_i (reputation table for node i) [6]. We will explore different methodologies used for measuring trust and reputation parameters in Section 3.

2.3. Characteristics of trust

The notions of trust and reputation originated from the field of social sciences that studies the deportments of human communities. To better understand, we must know certain characteristics that the "trust" must have.

- ***Asymmetry***: Trust is unidirectional and asymmetric, that is, if *Person A* trusts *Person B*, then it does not necessarily imply that *B* trusts *A*.
- ***Subjectivity***: Trust is subject to the expectations one person has from another. The opinion that *Person A* holds about *Person B* depends on two factors: (i) how well *Person B* is responding to the queries of *Person A* and (ii) how much of extra demanding *Person A* is. Assume that a community's common opinion about *Person B* is that *Person B* is well behaved. However, it may still be possible that *Person A* holds quite an opposite opinion about *Person B* because of the former's more demanding nature. Therefore, *Person A*'s trust is subject, probably, to the high expectations that *Person A* has from *Person B*.
- ***Partial Transitivity***: Trust may or may not be transitive. If *Person A* trusts *Person B* and *Person B* trusts *Person C*, then it is not necessary that *Person A* would trust *Person C* (and vice versa). This scenario indicates that *Person A* might have quite a different degree of trust from *Person B*'s trust assessment of others. To have trust on the trust assessment of a *Person X* is also called the credibility of *Person X* [38]. Credibility is an important factor for the establishment of trust in a system with no central trust management.
- ***Context Sensitivity***: Whenever *Person A* establishes a trust opinion about *Person B*, the opinion also depends on the context *Person A* has formed that opinion [24]. For example, *Person A* might trust *Person B* in some task T_1. However, *Person A* may not trust *Person B* in tasks T_2 and T_3. Therefore, the context must also be considered on the basis of which *Person A* will hold a trust rating for *Person B*.

In Figure 3(a,b), we graphically define the properties intransitivity and subjectivity, respectively. Figure 3(a) indicates that the transitive relationship cannot hold in the case of trust, where *A* and *B*, and *B* and *C* may trust each other but *A* and *C* may not. In Figure 3(b), *A* has higher trust rating for *B* in one task but has lower trust rating for *B* in another task. Figure 3(c) gives a summary of the various characteristics of trust discussed in the preceding paragraphs.

In daily life, we find the applications of trust wherever decision making is involved. Trust and reputation is applied in various domains, especially when the entities are interacting in a network. The network may be a social network, a simple computer network, or any other advanced form. Trust has been applied by researchers in various domains, namely, (i) peer-to-peer (P2P) systems, (ii) grid computing, (iii) opportunistic computing, (iv) e-commerce, (v) social networking, and (vi) WSNs. A few proposals on application of trust in specific areas are indicated in Table II.

In **P2P** systems, the network consists of distributed equally privileged peers that may share the disk partitions, processing resources, and computation workloads (e.g., P-Grid, Freenet, Usenet, and Kazaa) [39]. There is no central authority to regulate security and protection measures among the peers. Moreover, the peers frequently join and leave the network. Therefore, the network is vulnerable to various security threats by malicious peers. Aberer and Despotovic [40] devised a repute computation technique for P2P systems. In the technique, repute is computed on the basis of a peer's behavior in earlier transactions with other peers. The probability that a peer may cheat is computed by applying data mining techniques and statistical data analysis techniques on an agent's previous transactions.

In **grid computing**, a network of loosely coupled heterogeneous systems is designed by the use of (middleware) software libraries [41]. The workloads on a grid are generally noninteractive. Apart from a local infrastructure, a grid may be designed by using computing resources provided by individuals (volunteers) outside the organization (e.g., Berkeley Open Infrastructure for Network Computing). A drawback of such approaches is the fact that the participating nodes may not be exclusively trustworthy. Therefore, the designers of the grid system must employ some security measures, such as the integration of trust and

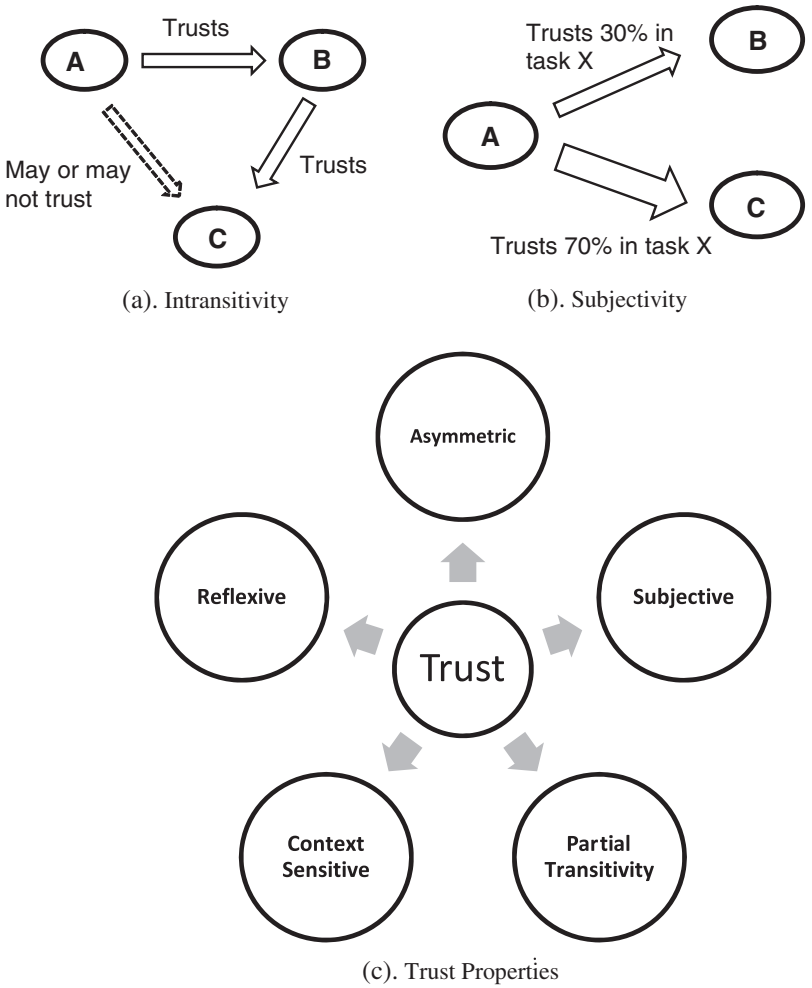

Figure 3. Various characteristics and attributes of trust.

Table II. Application of trust and reputation in various domains.

Area	References
E-commerce	[65–71]
Social networking	[72–75,47,76,77]
Peer-to-peer systems	[78–83,40]
Grid computing	[84–86,42,87,88]
Opportunistic computing	[44,89–92]

reputation, to identify the nodes producing the false and misleading results. Papalilo and Freisleben [42] presented a scheme for applying the trust factor in a grid computing environment. With simple statistical methods used, the deviations in the participating nodes' behaviors are computed, and the malicious nodes are identified.

The **opportunistic computing** provides an opportunity for communication and computation by exploring unused computing resources within a network without any prior knowledge about the location and capacity of the resources [43]. An opportunistic network is ubiquitous with intermittently communicating devices cooperating with each other in certain tasks by using middleware services architecture. The middleware services manage disconnections, heterogeneous computing resources, delay tolerance, and data services. It is very important to establish a secure communication in such an environment where devices do not have *a priori* information about each other. Trust establishment is one of the most challenging areas of opportunistic computing [43]. Vinel *et al.* [44] have discussed the application of trust on VANETs. The authors have explored the minimum communication latency required to guarantee trustworthiness in VANETs by using parameters such as the number of vehicles and the number of intruders.

In **e-commerce**, the applications have a centralized reputation management system [45]. Most frequent uses of trust and reputation in e-commerce are found in Web-based online shopping applications (e.g., Amazon.com). In such applications, the business is performed on the basis of trustworthy relationship between the buyer and the seller. If the seller is coming up to the expectations of the buyer, then more customers would be attracted towards the business. In

some scenarios, an online seller may hire the services of some well-reputed third party (e.g., PayPal), which the clients may trust more. Few systems (e.g., eBay and Yahoo auctions [45]) employ trust-based ranking techniques in which a seller's repute is updated (by a buyer) depending on the quality of service delivered. Therefore, the buyers would, in general, prefer to participate in bidding by a well-reputed seller.

A **social networking** site is an online application that allows people to build social relationships, share ideas, and join various communities on the basis of similar interests [46]. Trust and reputation systems have also been applied in various social networking applications. Skopik *et al.* [47] had discussed a model to assign trust and reputation for virtual communities. The model is based on the repute calculation for the participants of an online discussion forum (slashdot.org). When a participant posts some comment, then different viewers rate the comment positively or negatively and may post the replies. A reply can be further rated and commented by other users. Therefore, a chain of comment/reply threads is formed. The parameters, such as the total replies and the number of replies with positive ratings, are used to establish the trust opinions about a participant. Moreover, the participants that are more frequent in posting comments are assigned more trust ratings. Data mining techniques are applied to extract relations among more trusted participants and overall reputation of various participants. However, there are no natural language processing techniques applied by the authors to verify the quality of the comment.

In a **WSN**, the securing of each node is very important. A malicious overtaking of some node may eventually prove catastrophic and lead to the collapse of the whole network at worst, beside the disclosure of some vital network information. Normally, a node misbehaves if the node either is hacked or becomes resource deficient. Therefore, prior to securing a network, we must understand the various types of node misbehaviors that WSNs may usually encounter.

2.4. Types of node misbehaviors

There are two common types of misbehaving nodes: (i) selfish nodes and (ii) malicious nodes. A node is called selfish if the node does not cooperate with another node because of some resource constraint (such as low battery). A *selfish* node may have no intention to cause harm to the system. There is also a possibility that an adversary reprograms a captured node to act selfishly. On the contrary, a *malicious* node has an intention to cause maximum harm to the system, even at the cost of node's own resources [48,17]. The following are some basic types of node misbehaviors.

- ***Black hole***: The malicious node advertises that the node has the shortest routes to the destinations. However, when the malicious node receives a packet, the packet is dropped.
- ***Gray hole***: The malicious node may selectively forward packets depending on the packet type. For example, the malicious node may participate in routing by forwarding the routing packets. However, the node may not forward active data packets.
- ***Bad-mouth***: A few malicious nodes may collude to propagate false information about a normal node [49]. Therefore, the trust rating of a well-reputed node may decrease.
- ***False praising***: In false praising or *ballot stuffing* attack, in sharp contrast to the bad-mouth attack, the malicious nodes collude to propagate a false positive information about another malicious node. This collusion helps the malicious nodes to maintain better trust ratings and stay longer in the network.
- ***Routing loop***: A captured node may change route information of the packets that may lead to routing loops in the network. Too many packets in the network because of routing loops may cause congestion and denial-of-service problems.
- ***Wormhole***: A group of adversaries may collude to redirect traffic to a slow link that may cause congestion and increased latency in the network.
- ***Packet injection***: A packet may be injected, with falsified data, such as false source and destination identifiers.
- ***Packet delay***: A malicious node may randomly delay the packets received for forwarding. The random behavior of a node would keep the trust rating of the node above a certain threshold. Therefore, the malicious node may not be detected easily.
- ***Sybil attacks***: In such attacks, the node masquerades its identity to appear as multiple identities to represent more than one node. Therefore, it is difficult to detect such a node acting maliciously when the node is frequently changing its identities.
- ***ID spoofing***: An intruder may alternatively spoof the source ID of the routed packets, leading to the disruption of routing. In such a scenario, it would also be difficult to locate the intruder node.
- ***Transient behavior***: A node may alternate between the roles of being adversary and well behaving (in an on–off manner) to keep the repute of the node above a certain threshold. Therefore, the node may not be screened out as a malicious node.
- ***Nodes collusion***: A node may misbehave with one group of nodes (cluster) and well behave with another group. Such node behavior may create an environment of mistrust between the two groups.
- ***Selfishness***: Low battery is the most common example of resource constraint a node may experience in a WSN. A node with low battery may participate in the route discovery process. However, the node may decline participation in the packet forwarding, which renders the node becoming indistinguishable from the packet-dropping malicious nodes.

Owing to the ongoing research and continued interest, in the security of WSN, various computationally tractable models have been proposed for the TRMs [15,10,13,12,6,7,34,50,35,36,51]. Such models require a lower resource consumption to

establish a defense system against various security threats that have been mentioned in the previous paragraphs. In the following section, we study the internal components and the operational details of a TRM.

3. TRUST AND REPUTATION MONITORING SYSTEM

A system that makes the use of trust and reputation information to calculate the trustworthiness of a node is called a TRM. Such a system must be able to judge a node's misbehavior and effectively distinguish between normal operating and malicious node. In TRMs, the positive and negative effects of a node's action are observed. The observations are aggregated in a specific trust table maintained by the node. Statistical analysis is performed on the trust table data to generate the node reputation.

3.1. Bootstrapping

A TRM may be initialized in three ways by considering the following: (i) each network node as trustworthy, (ii) all nodes as untrustworthy, and (iii) each node having a neutral trust rating. The summary of initialization methods discussed in various literatures is presented in Table III. In each interaction, the trust rating of a node either increases or decreases, depending on the node's behavior. The TRM must acquire and process some information, to be discussed subsequently, to make the relevant change to a node's trust rating.

3.2. Observation—firsthand and secondhand information

In a TRM, the nodes may share two types of information, namely, *firsthand* and *secondhand*. Firsthand information is the node's personal experience through a direct interaction with the neighboring node. Alternatively, indirect information is provided to the node by other nodes on the basis of their own experiences with the subject node. To understand the aforementioned definition, we assume that there are four nodes, namely, *A*, *B*, *C*, and *D*, in the network. The secondhand information node *A* holds about node *B* is the information provided to node *A* by nodes *C* and *D*. Nodes *C* and *D* had the information as a result of some recent direct interactions they had, with node *B*. Hence, the secondhand information is the indirect information node *A* acquires from other nodes about another node *B*, with which node *A* is going to interact. In practice, most of the TRMs use both firsthand and secondhand information in the system [36]. However, some TRMs only apply to the firsthand information mechanism [52,53]. Still, some TRMs only utilize the secondhand information [34].

3.3. Centralized and distributed trust and reputation monitoring

If trust and reputation are accumulated and stored by a single entity in the whole network, then the TRM is called centralized. Examples of such a centralized approach in e-commerce are Yahoo and eBay [45]. Alternatively, in a distributed case, the trust accumulation and calculation task is distributed over all the participating nodes [13,12,7,34,36,51].

3.4. Trust computation steps

Typically, a TRM performs the following steps for the computation of trust:

- information collection,
- information dissemination,
- information mapping to trust model, and
- decision making [48].

3.4.1. Information collection

In this step, the nodes collect the firsthand trust information. When a sensor node transmits a packet, the node observes the neighboring node through a *watchdog mechanism*. The watchdog mechanism requires that, after sending the packet to a neighbor, the node must observe the neighbor in a promiscuous mode, as illustrated in Figure 4, to verify whether the neighbor has forwarded or intentionally dropped the packet [13,12,51]. If the neighboring node forwards the packet, then trust rating is incremented and updated in the sender node's database. On the contrary, if the neighboring node drops the packet, then trust rating is decremented in the sender node's database. In a different network setup with nodes having directional (instead of omnidirectional) antennas, the watchdog approach may not be as effective. This is because a neighbor node may forward the packet in a direction such that the sender node may not be in the path of the signal.

3.4.2. Information dissemination

In a TRM, the network nodes disseminate their firsthand information to the neighboring nodes. Such kind of disseminated information is called secondhand information, as represented in Figure 5. The use of secondhand information is beneficial, and the reputation buildup process is faster. This is because the secondhand information establishes a global view of trust in the network. The nodes disseminate secondhand information either *proactively*, after some fixed time intervals, or *reactively*, on the occurrence of some event or when there is some substantial change in the network.

A node may share only the positive experiences that it had with neighbors. However, the TRM may become the target of ballot stuffing or false praise attacks (Section 2.4). Alternatively, a node may share only the negative experiences that may expose the system to bad-mouth attacks (e.g., [50]). In TRM frameworks [34,36], the nodes share both positive

and negative experiences. Some reputation frameworks (e.g., [52]) do not use the secondhand information altogether. In such systems, the false report attack is avoided. However, the reputation buildup process may take more time.

Shared information may be *local*—a node may share the information only with the next-hop neighbors through multicast [34]. Alternatively, shared information may be *global*—each node may share the information with all nodes in the network. Global information sharing is mostly applied in MANETs for the uniform distribution of trust [23,17]. Because of the node mobility in MANETs, network topology changes continuously.

In practice, information dissemination is performed by piggybacking trust information along with the normal network traffic. The process may involve adding the payload of trust information on the reply messages and location request messages. To maintain secondhand information, each node stores a local copy of the reputation table. Certain weighting functions may be applied to the raw information to mitigate the effect of false report attacks [51,34]. Figure 5 shows an example of information dissemination.

3.4.3. Information mapping to the trust model

During this phase, the network nodes combine the firsthand and secondhand information to generate a trust and reputation metric. The firsthand information is direct information, and not much computation is required to incorporate firsthand information into the reputation metric.

In contrast, authenticity of the secondhand information is dubious, and more processing is needed to parse the secondhand information into the reputation metric. However, there must be some way to check the credibility of the reporting node as it might be the case that the adversary node report falsely about a normal node. To assess the credibility of the reporting node, various techniques have been proposed in the literature. One such technique called the *deviation test* has been proposed by Yu and Zhen [24] and is represented by the following inequality:

$$| E(Beta(\alpha, \beta)) - E(Beta(\alpha_F, \beta_F))| \geq d \qquad (1)$$

where d is a threshold, the value of which is set heuristically. In the inequality given in Equation (1), α and β are the two parameters of the statistical *Beta* distribution. The *Beta* distribution is applied for decision making in a situation when some kind of risk factor is involved. Here, α and β define a node's good and bad behaviors, respectively. The expectation value $E(Beta(\alpha, \beta))$ is the measure of the *current* trust information node A has about node B, whereas $E(Beta(\alpha_F, \beta_F))$ refers to the *new* trust information provided by some node C to the node A (about node B). The reporting node C would be considered trustworthy if and only if the left-hand side of inequality (1) produces a value that is less than threshold d.

Various TRMs use a variety of statistical models to evaluate the correctness of the secondhand information, depending on the application and security requirements. The most commonly used approach is the Beta distribution [50,36] whose probability density function is expressed using the Gamma function as

$$P(x) = Beta(\alpha, \beta) = \frac{\Gamma(\alpha + \beta)}{\Gamma(\alpha)\Gamma(\beta)} x^{\alpha-1}(1-x)^{\beta-1}, \forall 0 \leq x \leq 1, \alpha \geq 0, \beta \geq 0 \qquad (2)$$

where α denotes the good behavior and β represents the bad behavior of a node. Equation (2) presents another way of measuring the consistency of data by a reporting node. As an example, let us suppose a node B provides the trust information to node A for $p + q$ times. If information is consistent for p times, then $P(x)$ is represented as the probability that the information would be consistent in the next observation. If $P(x)$ results in 1, then the reported information is consistent and authentic; otherwise, the information is considered as unauthentic information. The other statistical distributions that are used in practice are Poisson, binomial, and Gaussian distributions.

Another important aspect in the evaluation of trust is how much weight factor must be assigned to the *recently collected* trust information and the information collected in *past*. Some frameworks may assign more weight to the trust information collected in the past (e.g., [51]). In the scheme defined in [51], the authors reported that a node may not receive severe punishment if the misbehavior is for brief intervals of times. Such node misbehaviors may occur because of temporary link failures or some other resource constraints. The drawback with the past information collection approach is that, if some malicious node settles itself in the network and stays undetected for a while, then it may not be easy to identify such a node because of shorter misbehaviors performed by the malicious node.

In contrast, some frameworks assign more weight to the recently reported trust information [36]. This may require the nodes to continuously contribute to the network traffic for their survival. In such systems, the node reputation decrements automatically after a specific interval of time. Therefore, problems may occur at times when there is low network activity. In [34], beacon nodes are used to generate traffic in low network activity areas. The technique prevents the node reputation from falling below a certain threshold, whenever there is low network activity.

3.4.4. Decision making

The final step involves the decision-making process. The decision is based on the precompiled trust values. A decision may be one of the two binary values, where a "1" means to cooperate and forward the packet and a "0" means not to cooperate. Figure 6 graphically illustrates the decision-making process.

Another aspect that may affect the decision-making process is the *functional reputation* of the node. For example, two nodes A and B are exchanging data in a specific application *App*, such that the application is hosted on node A. Assume that *App* is running two services S_1 and S_2. Service

S_1 requires more resources compared with S_2. Now, there is a possibility that, after some time, because of resource constraints, node *A* may cease to cooperate with node *B* for service S_1. However, node *A* may resume cooperation with node *B* for service S_2. This implies that node *B* may have different trust ratings (functional reputations) for node *A* for the two services S_1 and S_2. In practice, the functional reputation is implemented by assigning trust rating for each service that a node is sharing with another node.

4. STATE OF THE ART TRMs

For many years, there has been an ongoing research in the design of "nature-inspired" protocols, and as a result, considerable achievements in the improvement of communications and resource conservations in various domains of computer networks have been observed. The application of trust in computer networks is also based on such inspiration. Security researchers develop trust and reputation-based models by leveraging results from other areas including mathematics, statistics, social sciences, and computer sciences. In this section, we discuss some of the existing TRMs along with their features and operations in detail.

4.1. Collaborative reputation mechanism [51]

Collaborative reputation mechanism (CORE) is a distributed trust model, in which reputation is calculated from the firsthand and secondhand information. Each node within the system maintains a trust table that holds the positive or negative repute for other nodes. During the network initialization, the route discovery is performed using dynamic source routing [54], and the nodes are assigned a neutral trust value. After sending a packet forwarding request, each node operates in a *watchdog promiscuous* mode to collect the direct trust value of the neighboring node. If the neighboring node responds positively, then the sender increments the positive trust value for the recipient; otherwise, the node decrements the trust rating. The indirect reputation of a node is collected by sending a request to the neighboring nodes and receiving the corresponding replies. To counter the bad-mouth attack, a node can only send positive information about other nodes. The nodes also compute the functional reputation that determines the trustworthiness of a neighboring node by utilizing specific functional parameters, such as routing and packet forwarding. Different weights may be assigned to different functions, depending on the application requirements. Finally, the total trust value of a node is computed by combining direct, indirect, and functional trust information. If the total trust computed by node *A* for node *B* is positive, then, and only then, will node *A* consider node *B* trustworthy. To survive within the network, a node must continuously contribute to network traffic. This is because, after a certain interval of time, the trust values of nodes decrement to prevent the existence of selfishness within the network. CORE gives more weightage to past observations than the recent interactions. Therefore, if a node fails because of temporary network problem, then this will not cause a major change in the node's overall reputation. However, if a node continuously misbehaves, then the trust rating will decrease until becoming negative whereby the node will be considered malicious. The implementation of the functional reputation by CORE has another advantage. A node may behave selfishly for a specific task that requires more memory and high battery power. However, the same node may behave well for another task with low computational requirements. Therefore, nodes with scarce resources are not excluded from the network and keep on interacting for tasks with lower resource demands.

4.2. Task-based trust for sensor networks [6]

In this technique, the authors further enhanced the framework proposed by Boukerche and Li [55]. Boukerche and Li suggested that when an intruder node is detected, then the intruder is blocked by all of the neighbors, regardless of the specific task in which the intruder node was misbehaving. In task-based trust for sensor networks, a node maintains the task-based trust value of the neighboring nodes. For example, when node *A* communicates with node *B*, then node *A* may perform well in some tasks (e.g., time synchronization with node *B*). However, node *A* may misbehave in other tasks (e.g., packet forwarding to node *B*). Therefore, node *B* may only block the packet forwarding task for node *A*. As a result, the trust ratings are decreased only for a specific task. The trust metric is computed by using Bayesian theorem and Beta distribution because of low processing capabilities of sensor nodes.

4.3. Lightweight secure trust-based localization [10]

Pandarinath *et al.* [10] presented a mechanism to detect those malicious nodes that may tamper with the location information of nodes. Each sensor node maintains the history and normalized count of the nodes traversed by the packets within the network. A history of most frequently used paths between the sender and receiver nodes is also maintained. When a new packet arrives at the receiver, the receiving node compares the path traversed by the packet with a predicted path. A large deviation value of the path indicates the suspected presence of some malicious node. In contrast, if the packet arrives through the expected path, the trust counter value (for the source node) is incremented in the receiver's trust table.

In the aforementioned scheme, whenever a node needs to communicate, the node sends the route request packet to the destination. The route request packet contains the source ID, destination ID, source location, and message authentication code (MAC). The MAC value is computed on the basis of a secret key *K*, shared between the source and destination

Table III. A taxonomy of comparison and features of commonly used TRMs for WSNs.

Ref	Network initialization	Observation	Weight assignment	Trust computation	Security attack prevention
CORE [51]	New nodes are assigned neutral trust value. Frequent contributions by nodes are required.	Firsthand and secondhand trusts are used. Watchdog mechanism is used to collect direct trust.	More weights are assigned to the past observations. Functional reputation is used.	A weighted mean is calculated for the observation's rating factor.	Bad-mouth attacks
TTSN [6]	New nodes are assigned a neutral trust value. Task-based node cooperation is observed.	Only Firsthand information is used.	More weights are assigned to the recent observations.	Beta distribution is applied.	Bad-mouthing and ballot stuffing attacks
LSTL [10]	All nodes are assigned neutral trust rating.	The path traversed by a packet from source to destination is observed.	More weights are assigned to the past information.	Distance estimation techniques are used.	Localization attacks
ATSR [13]	Nodes are assigned neutral trust rating.	Periodic requests are sent for firsthand and secondhand information collection.	More weight is assigned to the distance metric, where distance is minimum between two nodes.	A weighted sum of energy and distance metric is calculated to compute trust.	Routing attacks, gray hole attacks, black hole attack, bad-mouth attack, network analysis attack
DETM [7]	Nodes are assigned neutral trust rating.	This is an event-triggered repute update process. Firsthand and secondhand information is used.	More weight is assigned to the energy metric.	Gaussian distribution is used.	Bad-mouth and ballot stuffing attacks
iTrust [12]	Each node is assigned a neutral trust rating.	Firsthand and secondhand information are used. Watchdog mechanism is used.	Not addressed.	Weighted trust computation is used.	False repute attacks.
CONFIDANT [50]	Nodes are initialized with positive trust rating.	Firsthand and secondhand trust information are maintained. Watchdog mechanism is used.	More weight is assigned to the past information and direct observation. Only negative information is shared.	Various metrics such as throughput, goodput, and dropped packets are considered for trust computation.	False praise attacks are avoided.
RRS [35]	A neutral reputation value is assigned to newcomer nodes. Frequency of interaction among nodes is assumed to be high.	Both firsthand and secondhand information are used.	More weight assigned to the recent information. Both positive and negative are shared by the nodes.	Beta distribution is applied.	Both false praise and bad-mouth attacks are avoided.
RFSN [36]	New nodes are assigned low reputation value. Nodes have	Firsthand and secondhand experiences are used	Only positive information is shared to prevent bad-	Beta distribution is applied.	Higher weight is assigned to secondhand information

	to frequently interact to hold good trust rating.	to generate trust rating. Watchdog mechanism is used to collect direct trust.	mouth attack. Functional Reputation is used.		from a well-reputed node to prevent ballot stuffing attack.
DRBTS [57]	New nodes are assigned neutral reputation value. Nodes have to frequently interact to hold good trust rating. Beacon nodes are used to establish trust.	Both firsthand and secondhand information are used.	Not addressed.	Beta distribution is used for decision making.	A deviation test is used to prevent bad-mouth and ballot-stuffing attacks.
ATSN [93]	Neutral reputation value is assigned to newcomer nodes. High frequency of interaction between nodes is required.	Only firsthand observations are used.	An adaptive forget factor is used.	Ranking-based and weight-based computations are used.	Assuming the agents evaluating the reputation of the nodes are from the trusted third party, they would not engage in bad-mouthing or ballot stuffing attacks.
Qin *et al.* [94]	Neutral reputation value is assigned to newcomer nodes. High frequency of interaction between nodes is required.	Only firsthand observations are used.	More weight is assigned to the past observation.	Beta distribution is applied.	Not addressed.
PTM [37]	Neutral reputation value is assigned to newcomer nodes.	Both firsthand and second information are used.	More weight is given to the recent information.	Beta distribution is applied.	Not addressed.

TRM, trust and reputation monitoring; WSN, wireless sensor network; CORE, collaborative reputation mechanism; TTSN, task-based trust for sensor nodes; LSTL, lightweight secure trust-based localization; ATSR, ambient trust sensor routing; DETM, distributed event-triggered trust management; CONFIDANT, cooperation of nodes—fairness in dynamic ad hoc networks; RRS, robust reputation system; RFSN, reputation framework for sensor networks; DRBTS, distributed reputation-based beacon trust system; ATSN, agent-based trust model for wireless sensor networks; PTM, pervasive trust management.

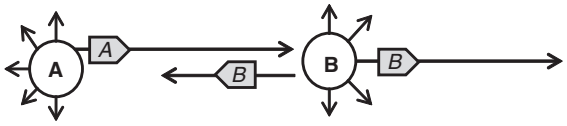

Figure 4. Description of promiscuous mode. Node *A* transmits a packet and observes node *B* in promiscuous mode. When node *B* forwards the packet, a copy of packet is also received by node *A* that verify the packet contents and then updates the trust rating for node *B*.

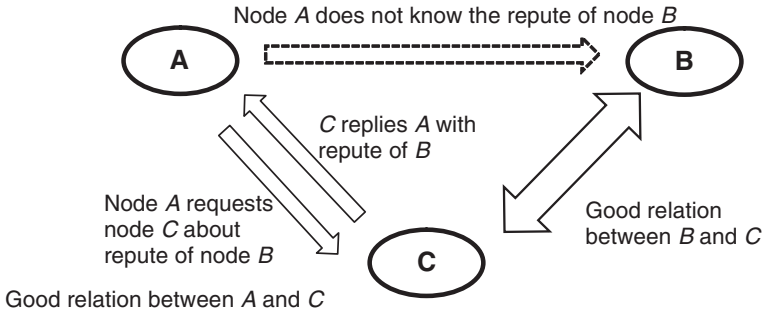

Figure 5. Secondhand trust information dissemination.

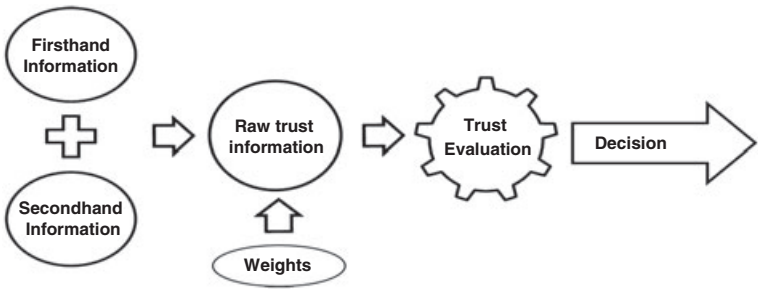

Figure 6. Trust computation process. The weights are applied to set the trust thresholds.

nodes. The intermediate nodes, on receiving the message, extract path information from the packet (the IDs of nodes traversed by packet) and store path information into the database. The intermediate node then appends the message with the node's own ID and new MAC value and forwards the packet. In this manner, the hop-to-hop security is implemented. If the route traversed by the packet is within a certain threshold value of distance, then and only then the destination node will send a route reply message.

4.4. Ambient trust sensor routing [13]

The ambient trust sensor routing (ATSR) framework presents a distributed trust management system for the secure routing of packets among sensor nodes. Each node, within the network, periodically broadcasts beacon messages to announce the node ID and the energy of the node. Another periodic multicast message by the node is the reputation request message that is sent directly to the neighboring nodes for the collection of indirect trust (reputation) information. The neighbors respond with a unicast reputation reply. Each node maintains some trust metrics to evaluate the neighboring nodes, namely, (i) forwarding, (ii) remaining energy, and (iii) distance. The forwarding metric is equal to the total received packets divided by the total forwarded packets and indicates whether the neighboring node is forwarding the packet sent by the source node. After sending the packet to a neighbor, the node enters into the *promiscuous mode* to observe whether the neighbor has forwarded the packet or not. With the use of the aforementioned procedure, the credibility of the neighbor is judged for the forwarding metric.

A node combines the direct and indirect trust values to calculate total trust information. In addition, each node computes a distance metric with one-hop neighbor nodes whose value is maximum for the closest neighbor. The packet is forwarded for routing to the neighbor nodes having the maximum value of combined trust and distance metric. Node *A* can detect a *bad-mouth attack* by comparing the reputation response received from node *C* about node *B*. The previous trust value is stored in node *A*'s reputation table (direct and combined indirect trust values). If there is a significant difference between the stored and reported trust values (by node *C*), then node *C* is considered as a vicious node performing *bad-mouth attack*.

The ATSR technique behaves in a similar manner to the nontrust location-based greedy perimeter stateless routing (GPSR) protocol [56], provided that there are no malicious nodes within the network. GPSR selects the closest node to forward packets. The simulation comparison between ATSR and GPSR protocols demonstrate that with the increase in malicious nodes within the network, the packet loss in GPSR significantly increases. However, when comparing the packet latency, ATSR has more delays compared with GPSR due to the alternate route selection process due to the presence of malicious node in neighborhood.

Energy conservation in ATSR is achieved by considering the energy metric of the next-hop node before forwarding the packet towards the node. In this manner, during an established session, the data flow may change routes multiple times to achieve proper load balancing. The technique has the additional advantage of preventing the network *traffic analysis* attack. The emulation results for ATSR illustrate that, for the implementation of indirect trust mechanism, the memory requirements may also increase. Moreover, the nodes' mobility may increase packet loss. Therefore, if the node mobility is higher, then the trust buildup will also take more time within the network.

4.5. Distributed event-triggered trust management [7]

Liu *et al.* [7] suggested a model in which each network node has a set of modules to parse and store trust-related information for the neighboring nodes. A network node maintains a set of information parameters that consists of (i) a public key (shared among neighbors), (ii) reputation, (iii) remaining energy, and (iv) network paths. A Gaussian distribution is applied for the trust computation. To conserve energy, the repute update process of the system is event triggered, instead of relying on periodic broadcasts. A node's decision to cooperate with another node depends on the combined trust (firsthand and secondhand) information as well as the remaining energy of the node.

The distributed event-triggered trust management model works in the following manner. If a node *A* needs to communicate with node *B*, then node *A* inquires about the reputation information of node *B* by sending a broadcast message to neighboring nodes *C*, *D*, and *E*. Suppose node *C* has the required information available, node *C* will encrypt the information using node *A*'s public key and will send the message back to node *A* as a unicast transmission. However, there might be a possibility that node *C* is a malicious node that has the public key of node *A*. Therefore, node *A* first checks the credibility of node *C* by looking into the trust table. If there is no entry for node *C*, then node *A* discards the message sent by node *C*. The other information that may accompany node *B*'s trust information is the remaining energy of node *B*. Using the aforementioned procedure, node *A* receives the (node *B*'s) trust and remaining energy information from nodes *D* and *E*. Node *A* parses the acquired trust information into a computational metric and applies some weights (e.g., remaining energy of node *B*) to the information. The information is then passed to a Gaussian distribution to extract the final trust value. If the resulting value is above a certain threshold, then and only then node *A* makes the decision of forwarding packet towards node *B*. Packets may reach node *B* via nodes *C*, *D* or *E* depending on which one of the nodes has the maximum remaining energy.

4.6. Integrated trust framework (iTrust) [12]

The iTrust model is proposed as a distributed trust model. The model categorizes the network nodes in two types, namely, (i) monitor nodes and (ii) sensor nodes. The monitor nodes are responsible for the accumulation of the trust information. A monitor node stores and computes the reputation of all of the sensor nodes in the vicinity. Initially, each sensor node within the network is assigned a neutral trust rating. A learning phase is performed during which the monitor nodes collect information for various parameters from the neighbor nodes by acting *promiscuously*. The monitor nodes calculate trust values for specific parameters and update the trust tables. At the end of the learning phase, the monitor nodes publish and share trust tables with neighbor nodes.

When a sensor node *A* needs to communicate with node *B*, node *A* requests the monitor node for the repute of node *B*. Node *A* then parses the repute of node *B* into a trust metric to obtain the final trust value and initiates communication with *B* only if the trust value of *B* is above a certain threshold. There is a possibility that a monitor node becomes compromised by some adversary and begins to act as a malicious node. Therefore, a compromised monitor node may perform the *false repute reporting* attacks. In the iTrust framework, the aforementioned problem is handled by the use of firsthand information within the system. If a monitor node continuously misbehaves, then the reputation of the monitor node would gradually decrease, and eventually, the monitor node would be declared as a malicious node by other sensor nodes.

4.7. CONFIDANT framework [50]

The distributed trust nature of "Cooperation of Nodes—Fairness in Dynamic Ad hoc NeTworks" (CONFIDANT) allows each node in the network to maintain both firsthand and secondhand trust information about the neighboring nodes. For network routing, the dynamic source routing protocol is implemented. After sending the packet to a neighbor, each node in the network enters in a *promiscuous mode* to detect the behavior of the neighboring node. Each node in CONFIDANT scheme consists of four major components, namely, (i) Monitor, (ii) Trust Manager, (iii) Reputation System, and (iv) Path Manager. Using the Monitor, when a node transmits a packet, the node keeps a copy of the original packet and passively monitors the packet retransmission by the neighbor to detect any change in the packet content. Any modification in the packet content is reported to the Reputation System with an *alarm* sent to the Trust Manager. The Reputation System maintains a table that holds node

entries and nodes' trust ratings. The trust rating for a node changes only when there is a significant number of misbehaviors (as per threshold) performed by the node. Therefore, a node is not penalized for momentary misbehavior (e.g., link failure).

The Path Manager component of the node serves as a decision maker. The Path Manager deletes the paths to the malicious nodes by analyzing the trust rankings and denies the requests for path by any adversary node. In CONFIDANT, when a malicious node is excluded from network, then the node may reenter the system after a certain timeout. Therefore, the malicious node may acquire further chances to attack. However, when the repeated attempts to reenter and attack reaches a certain threshold, then the malicious node is permanently expelled from the network.

In the system, different weights are also assigned to the accumulated trust ratings. A node's direct observation about a neighbor is assigned a higher weight as compared with the indirect trust information. For the information dissemination, the nodes share only the bad experiences. Therefore, the indirect trust information is only the negative information shared between the nodes. However, the major disadvantage of this approach is that a node may easily become the target of the *bad-mouth* attack. If the nodes collude to perform *bad-mouth* attacks, then the whole network may be under threat. There is also an advantage of sharing only the negative information. The nodes may never come under the *false praise* attack that may help the malicious nodes to act in unison to increase each other's survival time in network.

4.8. Robust reputation system [35]

Robust reputation system is an improved version of CONFIDANT, presented by the same authors (Buchegger *et al.*). In the proposed scheme, the authors have included both positive and negative reputation values to avoid *false praise* and *bad-mouth* attacks. For the computation of repute, Bayesian framework is used along with the Beta distribution. Whenever a node receives secondhand information, the latter is subjected to a deviation test, the success of which indicates authenticity of the information. In the robust reputation system, more weight is assigned to the recent experience, unlike CORE [51] in which more weight is given to past experience to preclude a malicious node from staying longer in the network because a malicious node may initially behave positively but may start to misbehave after the establishment of repute. Therefore, more weight to recent observations would produce more correct results in predicting node's behavior.

4.9. Reputation framework for sensor networks [36]

Ganeriwal and Srivastava [36] proposed reputation framework for sensor networks (RFSN) as a distributed and symmetric trust framework for the WSNs. The nodes within RFSN framework share both firsthand and secondhand trust information. The other reputation metric a node may maintain is the *functional reputation*. In RFSN, the nodes share only the positive trust information. A weight factor is applied to the secondhand information. A higher weight factor will be applied to the secondhand information received from a well-reputed node. The trust computation is performed in RFSN by using the *Beta* distribution. In the proposed framework, R_{AB} is the reputation information node A computes about node B. Moreover, nodes A and B have a total number of $a+b$ interactions, where a and b are *positive* and *negative* interactions, respectively. The reputation of node B computed by node A is given by the following:

$$R_{AB} = Beta\left(\alpha_B^{\text{new}} + 1,\ \beta_B^{\text{new}} + 1\right) \tag{3}$$

$$\alpha_B^{\text{new}} = \left(w_{\text{age}} \times \alpha_B\right) + a \tag{4}$$

$$\beta_B^{\text{new}} = \left(w_{\text{age}} \times \alpha_B\right) + b \tag{5}$$

where w_{age} is the aging factor. The value of w_{age} is proportional to the duration of stay of node B. In Equation (4), α_B^{new} (the chance that node B has good repute) is computed by multiplying the weight w_{age} with the positive behaviors α_B of node B and then adding up with positive outcomes a of recent interactions that node B performed with A. In the same way, β_B^{new} is computed using Equation (5). The decision that a node must cooperate is a binary value 1.

4.10. Distributed reputation-based beacon trust system trust framework [57]

In a WSN, it is important for the nodes to transmit accurate location information. A compromised sensor node may propagate incorrect coordinates to keep itself undetected. Therefore, the application of trust in secure localization of nodes is imperative. In the distributed reputation-based beacon trust system framework, Srinivasan *et al.* [57] proposed a distributed trust model for secure localization of nodes within a WSN. The model consists of two major components, namely, (i) the beacon nodes and (ii) the sensor nodes. Beacon nodes have pre-identified locations, whereas the location of a sensor node is computed using a mathematical *triangulation* method. In triangulation, a sensor node broadcasts the location request and enters into a *promiscuous mode*. On receiving the location request message, the beacon nodes reply with the coordinates at which the beacon nodes are located. When the aforementioned coordinate's information is received by the sensor node, the node verifies the information authenticity. The verification process involves a deviation test in which the sensor node compares new information with the pre-stored location information (of the beacon nodes). A low deviation verifies the information authenticity and the node correctly computes the coordinates. The distributed reputation-based beacon trust system model is distributed and each beacon node shares the location information with the neighboring beacon nodes. Whenever a beacon node replies to a location request, the neighboring beacon nodes also increase the trust rating for the subject beacon node.

4.11. Agent-based trust and reputation monitoring scheme [32]

In the agent-based trust and reputation monitoring framework, Boukerch *et al.* [32] applied trust and reputation to a clustered WSN. In the system, each node is installed with a software component, known as *mobile agent*, that is responsible for the computation of trust. Whenever two nodes need to interact, the mobile agents on the respective nodes perform a one-to-one communication to exchange reputation information. To understand the procedure, suppose a *requestor* node *A* needs to interact with a *provider* node *B* for some service. The mobile agent on node *A* queries the reputation information from the mobile agent on node *B*. If the reputation of node *B* is acceptable for node *A*, then and only then node *A* interacts with node *B*. After a certain interaction, node *A* generates a trust rating for node *B* that may depend on the quality of service provided by node *B* to node *A*. The mobile agent on node *A* forwards the trust rating to the corresponding mobile agent on node *B*, where the new reputation is updated. Therefore, with an agent-to-agent direct interaction implemented, there is no need to flood the network with broadcast reputation request messages. However, the authors did not comment on how various security attacks must be countered, when any of the requestor or the provider nodes are compromised by an adversary.

5. TAXONOMY OF TRMs

In Table III, the taxonomy of various trust models is presented. The comparisons are made on certain parameters such as (i) network initialization, (ii) type of observation, (iii) weight assignment to trust information, (iv) trust computation approach, and (v) the type of security attacks that are addressed by the TRM. From the comparisons, we note that most of the frameworks imply neutral trust rating for the newly deployed nodes in the network. Moreover, in most of the presented models, both firsthand and secondhand information are used in the reputation calculation. In the most recent models, the recently observed information is given greater weightage as compared to the past information. The comparison provides a quick reference to the current trends in the research and design of various TRMs. In Table IV, some common strengths and weaknesses for a few selected TRMs are discussed.

6. FUTURE DIRECTIONS

Although there is much research work conducted in application of trust and reputation in various network domains, the task is still in evolutionary phases in the case of WSNs, where node security is the biggest challenge because of low resources of node. Every proposed TRM has some limitations and covers only a subset of various issues and challenges in providing complete security to a WSN. In this survey, we identified some of the hot issues for research in the field of TRMs, which are discussed in the subsequent paragraphs.

- One of the significant issues in TRMs is the bootstrapping problem. Bootstrapping is the time a TRM may require for the trust buildup in the network. In practice, the nodes in a WSN are deployed with some initial security measures, such as predeployment and key distributions [58]. However, it may still take some time to establish a global trust view of the network. This delay may not be acceptable for time-critical applications.
- In a few TRMs (e.g., [51]), to survive in the network, a node must continuously contribute to the network traffic. Nodes in the low activity areas of a network may suffer because of their gradual decrease in reputation. Therefore, a mechanism must be devised to keep the repute above a threshold in such low activity areas.
- In most of the trust models, a node calculates the direct trust through *promiscuous* learning mode. However, when directional antennas are used, the technique becomes difficult to implement. Similarly, noise may be another factor that can cause hindrances to *watchdog* mechanisms.
- In mobile WSNs, because of the mobility of nodes, the trust information cannot be symmetric. Therefore, WSNs are further exposed to security threats, because of the frequent change of neighbors. Some mobile nodes with greater resources (acting as beacon nodes) must be dedicated to hold the security and reputation information for the rest of the nodes. Therefore, a choreographic mobility pattern may also be required by the beacons for the uniform distribution of the trust information.
- The implementation of trust, in a WSN, may require additional data structures and resources on each node. Scalability is one of major challenges for a TRM, and most of the literature works have not discussed this issue. Most of the TRMs that we discussed in this survey use a flooding approach for trust information dissemination, and this may lead to high traffic over the network. With the addition of more nodes in the network, the performance may further degrade. Therefore, the real implementation of trust and reputation on a WSN with large number of nodes may be a challenging task and requires further research in balancing the trust benefits and communication overheads.

7. CONCLUSIONS

Trust is an important tool for self-configuring and autonomous systems, such as WSNs, to make effective decisions in detecting a misbehaving node. The task of establishing trust and reputation becomes more challenging when the nodes are mobile. In this survey, we presented an in-depth description of trust and reputation to use as a basis for understanding of the functionality of TRMs. We defined various cryptography techniques and illustrated the reasons

Table IV. A comparison of strengths and weaknesses for a few selected TRMs.

Ref	Strengths	Weaknesses
CORE [51]	Because both firsthand and secondhand information is shared, the system has defense against false praise attacks and bad-mouth attacks.	The system requires frequent contribution by nodes in network traffic. The nodes in areas with low traffic will have a gradual decrease in trust rating, until the trust rating may reach zero.
TTSN [6]	The system provides more granularities by observing a node's misbehavior in a specific task, rather than blocking all communications with the node.	The trust buildup process at whole network level is slow because only firsthand information is used. More weights are assigned to the recent observations and due which a node receives severe punishment for a temporary misbehavior, for example, link problem.
LSTL [10]	The localization attacks in which a malicious node provides false information about its location are prevented.	Each node has to maintain the information of the complete path traversed by the packet. This can cause overload on memory, in a memory-constrained sensor node.
ATSR [13]	The packet drop rate in GPSR due to malicious nodes in the network is decreased. The network throughput is increased.	Periodic requests are sent for firsthand and secondhand information collection that may cause the high volume of traffic over the network.
DETM [7]	Event-triggered repute update process is introduced to save the nodes energy, which is consumed more in the case of periodic repute update.	The system uses public key cryptography. This may decrease the overall throughput in a large network because of high computations required by the nodes.
CONFIDANT [50]	There is improvement in the routing protocol DSR to cope with the malicious nodes in the network.	As secondhand information, the negative information (experiences) is only shared by the nodes. The disadvantage of this approach is that a node may easily become the target of the bad-mouth attack.

TRM, trust and reputation monitoring; CORE, collaborative reputation mechanism; TTSN, task-based trust for sensor networks; LSTL, lightweight secure trust-based localization; ATSR, ambient trust sensor routing; DETM, distributed event-triggered trust management; CONFIDANT, cooperation of nodes—fairness in dynamic ad hoc networks; GPSR, greedy perimeter stateless routing; DSR, dynamic source routing.

DOI: 10.1002/sec

why just cryptography is not sufficient to provide complete security for WSNs. The survey discussed in detail the characteristics of trust and the different types of misbehaviors the nodes may perform in a WSN so that a carefully designed TRM system must tackle all the security challenges. The trust computation steps and the reputation model buildup processes are illustrated with thorough details. An overview of state of the art of modern TRM systems in WSN is presented, and the survey is concluded with a concise comparison table for selected TRMs over various parameters and another tabular presentation of some strengths and weaknesses for the selected models.

ACKNOWLEDGEMENTS

The authors thank Kashif Bilal and Saif Malik for their valuable comments and feedback in this survey. Samee U. Khan's work was partly supported by the Young International Scientist Fellowship of the Chinese Academy of Sciences, (Grant No. 2011Y2GA01).

REFERENCES

1. Khan AR, Madani SA, Hayat K, Khan SU. Clustering-based power controlled routing for mobile wireless sensor networks. *International Journal of Communication Systems* 2012; **25**(4):529–542.
2. Yick J, Mukherjee B, Ghosal D. Wireless sensor network survey. *Computer Networks: The International Journal of Computer and Telecommunications Networking, Elsevier* 2008; **52**(12):2292–2330.
3. Akyildiz IF, Su W, Sankarasubramaniam Y, Cayirci E. A survey on sensor networks. *IEEE Communications Magazine* 2002; **40**(8):104–112.
4. Khan SU. Approximate optimal sensor placements in grid sensor fields. *65th Semi-annual IEEE Vehicular Technology Conference* (VTC), Dublin, Ireland, April 2007; 248–251.
5. Srinivasan A, Li F, Wu J. A novel CDS-based reputation monitoring system for wireless sensor networks. *28th International Conference on Distributed Computing Systems* (ICDCS '08) Workshop, 2008.
6. Chen H. Task-based trust management for wireless sensor networks. *International Journal of Security and its Applications* 2009; **3**(2):21–26.
7. Liu S, Pang L, Pei Q, Ma H, Peng Q. Distributed event-triggered trust management for wireless sensor networks. *Fifth International Conference on Information Assurance and Security*, 2009.
8. Arenas AE, Aziz B, Silaghi GC. Reputation management in collaborative computing systems. *Security and Communication Networks* 2010; **3**(6):546–564.
9. Bistarelli S, Foley SN, O'Sullivan B, Santini F. Semiring-based frameworks for trust propagation in small-world networks and coalition formation criteria. *Security and Communication Networks* 2010; **3**(6):595–610.
10. Pandarinath P, Shashi M, Rao A. A lightweight secure trust-based localization scheme for wireless sensor networks. *International Journal of Computer Science and Information Security (IJCSIS)* 2010; **8**(3).
11. Balfe S, Yau P, Paterson KG. A guide to trust in mobile ad hoc networks. *Security and Communication Networks* 2010; **3**(6):503–516.
12. Yadav K, Srinivasan A. iTrust: an integrated trust framework for wireless sensor networks. *25th ACM Symposium on Applied Computing* (SAC'10), Switzerland, March 22–26, 2010.
13. Zahariadis T, Leligou H, Karkazis P, *et al*. Design and implementation of a trust-aware routing protocol for large WSNs. *International Journal of Network Security and Its Applications (IJNSA)* 2010; **2**(3):52–68.
14. Glynos D, Argyroudis P, Douligeris C. Collaborative service evaluation with the TwoHop trust framework. *Security and Communication Networks*. DOI: 10.1002/sec.355, Article first published online: 29 July, 2011.
15. Mana M, Feham M, Bensaber BA. Trust key management scheme for wireless body area networks. *International Journal of Network Security* 2011; **12**(2):71–79.
16. Ren Y, Li M, Sakurai K. FineTrust: a fine-grained trust model for peer-to-peer networks. *Security and Communication Networks* 2011; **4**(1):61–69.
17. Cho J, Chen I, Swami A. A Survey on trust management for mobile ad hoc networks. *IEEE Communications Surveys and Tutorials* 2010; **13**(4):562–583.
18. Govindan K, Mohapatra P. Trust computations and trust dynamics in mobile adhoc networks: a survey. *IEEE Communications Surveys and Tutorials* 2011; **99**:1–20.
19. El-Hajj W, Safa H, Guizani M. Survey of security issues in cognitive radio networks. *Journal of Internet Technology* 2011; **12**(2):181–198.
20. Lopez J, Roman R, Agudo I, Fernandez-Gago C. Trust management systems for wireless sensor networks: best practices. *Computer Communications* 2010; **33**(9):1086–1093.
21. Esch J. A Survey of trust and reputation management systems in wireless communications. *Proceedings of the IEEE* 2010; **98**(10):1755–1772.
22. Momani M, Challa S. Survey of trust models in different network domains. *International Journal of Ad hoc Sensor and Ubiquitous Computing (IJASUC)* 2010; **1**(3):1–19.
23. Ramana KS, Chari A, Kasiviswanth N. A survey on trust management for mobile ad hoc networks. *International Journal of Network Security and Its Applications (IJNSA)* 2010; **13**(4): 562–583.

24. Yu H, Shen Z. A survey of trust and reputation management systems in wireless communications. *Proceedings of the IEEE, School of Computer Engineering, Nanyang Technology University, Singapore* 2010; **98**(10):1755–1772.
25. Srinivasan A, Wu J. A survey on secure localization in wireless sensor networks. In *Encyclopedia of Wireless and Mobile Communications*, Furht B (ed). CRC Press, Taylor and Francis Group: Florida, USA, 2007.
26. Fernandez-Gago C, Roman R, Lopez J. A survey on the applicability of trust management systems for wireless sensor networks. *3rd International Workshop on Security, Privacy and Trust in Pervasive and Ubiquitous Computing* (SecPerU'07), 2007; 25–30.
27. Forouzan BA. *Data Communications and Networking* (4th edn). McGraw-Hill: New York, USA, 2007.
28. Rivest R, Shamir A, Adleman L. a method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM* 1978; **21**(2):120–126.
29. Dutertre B, Cheung S, Levy J. Lightweight key management in wireless sensor networks by leveraging initial trust. *System Design Laboratory SRI International Technical Report*, 2004; 1–18.
30. Xiao Y, Rayi VK, Sun B, Du X, Hu F, Galloway M. A survey of key management schemes in wireless sensor networks. *Computer Communications* 2007; **30**(11–12):2314–2341.
31. Zhou L, Chao H. Multimedia traffic security architecture for internet of things. *IEEE Network* 2011; **25**(3):29–34.
32. Boukerch A, Xu L, El-Khatib K. Trust-based security for wireless ad-hoc and sensor networks. *Computer Communications- Elsevier* 2007; **30**(11–12):2413–2427.
33. Yang L, Mu D, Cai X. Study on intrusion detection for wireless sensor network. *Journal of Application Research of Computers* 2008; **25**(11):2304–2308.
34. Srinivasan A, Teitelbaum J, Liang H, Wu J, Cardei M. Reputation and trust based system for ad hoc and sensor networks. In *Algorithms and Protocols for Wireless Ad-Hoc and Sensor Networks*, Boukerche A (ed). Wiley & Sons: New Jersey, 2008.
35. Buchegger S, Boudec JYL. A robust reputation system for peer-to-peer and mobile ad-hoc networks. *Proceedings of P2PEcon*, June 2004.
36. Ganeriwal S, Srivastava M. Reputation-based framework for high integrity sensor networks. *Proceedings of the 2nd ACM Workshop on Security of Ad Hoc and Sensor Networks* (SASN '04), October 2004; 66–77.
37. Almenarez F, Marin A, Diaz D, Sanchez J. Developing a model for trust management in pervasive devices. *4th Annual IEEE International Conference on Pervasive Computation Communication*, Washington DC, 2006; 267–271.
38. Weng J, Miao C, Goh A. An entropy-based approach to protecting rating systems from unfair testimonies. *The Institute of Electronics and Information Communication Engineers (IEICE) Transactions on Information and Systems* 2006; **E89-D**(9):2502–2511.
39. Khan SU, Loukopoulos T, Li H. Advances in wireless, mobile and P2P based internet protocols, applications, and architectures. *International Journal of Internet Protocol Technology* 2011; **6**(1–2):1–2.
40. Aberer K, Despotovic Z. Managing trust in a peer-2-peer information system. *Proceedings of the 10th international conference on Information and knowledge management ACM*, New York, 2001.
41. Khan SU, Bouvry P. Energy-efficient communications for high-performance distributed systems. *International Journal of Communication Networks and Distributed Systems* 2011; **6**(1):1–2.
42. Papalilo E, Freisleben B. Managing behavior trust in grid computing environments. *Journal of Information Assurance and Security* 2008; **1**:27–37.
43. Conti M, Kumar M. Opportunities in opportunistic computing. *IEEE Computer* 2010; **43**(1):42–50.
44. Vinel A, Campolo C, Petit J, Koucheryavy Y. Trustworthy broadcasting in IEEE 802.11p/WAVE vehicular networks: delay analysis. *IEEE Communications Letters* 2011; **15**(9):1010–1012.
45. Resnick P, Kuwabara K, Zeckhauser R, Friedman E. Reputation systems: facilitating trust in e-commerce systems. *Communications of the ACM* 2006; **43** (12):45–48.
46. Li J, Wang H, Khan SU. A semantics-based approach to large-scale mobile social networking. *ACM/ Springer Mobile Networks and Applications* 2012; **17** (2):192–205.
47. Skopik F, Truong H, Dustdar S. Trust and reputation mining in professional virtual communities. *International Conference on Web Engineering* (ICWE '9), 2009; 76–90.
48. Srinivasan A. Reputation and trust-based security in wireless sensor networks. *PhD Thesis*, Florida Atlantic University, 2008.
49. Hadjichristofi GC, Adams WJ, Davis NJ. A framework for key management in a mobile ad hoc network. *Proceedings of International Conference on Information Technology: Coding and Computing*, China, Vol. **2**, 4–6 April 2005; 568–573.
50. Buchegger S, Boudec L. Performance analysis of the CONFIDANT protocol (cooperation of nodes—fairness in dynamic ad-hoc networks). *3rd ACM International Symposium on MobiHoc*, Lausanne, June 2002.
51. Michiardi P, Molva R. CORE: a collaborative reputation mechanism to enforce node cooperation in mobile

ad hoc networks. *Communication and Multimedia Security*, September, 2002.
52. Bansal S, Baker M. Observation-based cooperation enforcement in ad hoc networks. *Proceedings of Computing Research Repository* (CoRR), 2003.
53. Marti S, Giuli TJ, Lai K, Baker M. Mitigating routing misbehaviour in mobile ad hoc networks. *Proceedings of the 6th Annual International Conference on Mobile Computing and Networking* (MobiCom), 2000.
54. Johnson DB, Maltz DA. DSR: the dynamic source routing protocol for multi-hop wireless ad hoc networks. In *Ad Hoc Networking*, Chapter 5, Perkins CE (ed). Addison-Wesley: Boston, Massachusetts, USA, 2001; 139–172.
55. Boukerche A, Li X. An agent-based trust and reputation management scheme . *IEEE Global Telecommunications Conference*, 2005; pp. 5.
56. Karp B, Kung HT. GPSR: greedy perimeter stateless routing for wireless networks. *Proceedings of the 6th Annual International Conference on Mobile Computing and Networking* (MobiCom'00), 2000.
57. Srinivasan A, Wu J, Teitelbaum J. DRBTS: distributed reputation based beacon trust system. *2nd IEEE International Symposium on Dependable, Autonomic and Secure Computing* (DASC'06), 2006; 277–283.
58. Chan H, Perrig A, Song D. Random key predistribution schemes for sensor networks. *Proceedings of Symposium on Security and Privacy*, May 2003; 197–213.
59. Perrig A, Szewczyk R, Wen V, Culler D, Tygar D. SPINS: security protocols for sensor networks. *Wireless Networks Journal* 2002; **8**(5):189–199.
60. Karlof C, Sastry N, Wagner D. TinySec: link layer encryption for tiny devices. *Proceedings of the Second ACM Conference on Embedded Networked Sensor Systems* (SenSys), 2004.
61. Ganeriwal S, Kumar R, Han C, Lee S, Srivastava MB. Location and identity based secure event report generation for sensor networks. *Nested Data-Parallel Language (NESL) Technical Report*, May 2004.
62. Watro R, Kong D, Cuti SF, Gardiner C, Lynn C, Kruus P. TinyPK: securing sensor networks with public key technology. S*econd workshop on Security in Sensor and Ad-hoc Networks*, 2004.
63. Ye F, Luo H, Lu S, Zhang L. Statistical en-route detection and filtering of injected false data in sensor networks. In *Proceedings of IEEE Infocom*, 2004.
64. Deng J, Han R, Mishra S. INSENS: intrusion-tolerant routing for wireless sensor networks. *Journal of Computer Communications* 2006; **29**(2):216–230.
65. Hazard CJ, Singh MP. Intertemporal discount factors as a measure of trustworthiness in electronic commerce. *IEEE Transactions on Knowledge and Data Engineering* 2011; **23**(5):699–721.
66. Benamati J, Fuller MA, Serva MA, Baroudi J. Clarifying the integration of trust and TAM in e-commerce environments: implications for systems design and management. *IEEE Transactions on Engineering Management* 2010; **57**(3):380–393.
67. Symeonidis P, Nanopoulos A, Manolopoulos Y. Providing justifications in recommender systems. *IEEE Transactions on Systems, Man and Cybernetics, Part A: Systems and Humans* 2008; **38**(6):1262–1272.
68. Wang Y, Lin K. Reputation-oriented trustworthy computing in e-commerce environments. *IEEE Internet Computing* 2008; **12**(4):55–59.
69. Josang A, Ismail R. The beta reputation system. *The 15th Bled Electronic Commerce Conference*, Slovenia, 2002.
70. Resnick P, Kuwabara K, Zeckhauser R, Friedman E. Reputation systems. *Communications of the ACM* 2000; **43**(12):45–48.
71. Blaze M, Feigenbaum J, Ioannidis J, Keromytis A. The keynote trust management system. *University of Pennsylvania*, 1999.
72. Xu S, Li X, Parker TP, Wang X. Exploiting trust-based social networks for distributed protection of sensitive data. *IEEE Transactions on Information Forensics and Security* 2011; **6**(1):39–52.
73. Dijiang H, Xiaoyan H, Gerla M. Situation-aware trust architecture for vehicular networks. *IEEE Communications Magazine* 2010; **48**(11):128–135.
74. Cutillo LA, Molva R, Strufe T. Safebook: a privacy-preserving online social network leveraging on real-life trust. *IEEE Communications Magazine* 2009; **47** (12):94–101.
75. Trier M, Bobrik A. Social search: exploring and searching social architectures in digital networks. *IEEE Internet Computing* 2009; **13**(2):51–59.
76. Yu H, Kaminsky M, Gibbons PB, Flaxman AD. SybilGuard: defending against sybil attacks via social networks. *IEEE/ACM Transactions on Networking* 2008; **16**(3).
77. Abdul-Rahman A, Hailes S. Supporting trust in virtual communities. *33rd Hawaii International Conference on System Sciences*, Hawaii, 2000.
78. Chen S, Zhang Y, Yang G. Parameter-estimation based trust model for unstructured peer-to-peer networks. *IET Communications* 2011; **5**(7):922–928.
79. Chen K, Hwang K, Chen G. Heuristic discovery of role-based trust chains in peer-to-peer networks. *IEEE Transactions on Parallel and Distributed Systems* 2009; **20**(1):83–96.
80. Lu L, Han J, Liu Y, *et al*. Pseudo trust: zero-knowledge authentication in anonymous P2Ps. *IEEE Transactions on Parallel and Distributed Systems* 2008; **19**(10):1–13.

81. Zhou R, Hwang K. PowerTrust: a robust and scalable reputation system for trusted peer-to-peer computing. *IEEE Transactions on Parallel and Distributed Systems* 2007; **18**(5):1–14.
82. Lu Y, Wang W, Bhargava B, Xu D. Trust-based privacy preservation for peer-to-peer data sharing. *IEEE Transactions on Systems, Man and Cybernetics, Part A: Systems and Humans* 2006; **36**(3):498–502.
83. Xiong L, Liu L. PeerTrust: supporting reputation-based trust for peer-to-peer electronic communities. *IEEE Transactions on Knowledge and Data Engineering* 2004; **16**(7):843–857.
84. Borowski JF, Hopkinson KM, Humphries JW, Borghetti BJ. Reputation-based trust for a cooperative agent-based backup protection scheme. *IEEE Transactions on Smart Grid* 2011; **2**(2):287–301.
85. Lin L, Huai J. QGrid: an adaptive trust aware resource management framework. *IEEE Systems Journal* 2009; **3**(1):78–90.
86. Blanquer I, Hernandez V, Segrelles D, Torres E. Enhancing privacy and authorization control scalability in the grid through ontologies. *IEEE Transactions on Information Technology in Biomedicine* 2009; **13**(1):16–24.
87. Song S, Hwang K, Kwok Y. Risk-resilient heuristics and genetic algorithms for security-assured grid job scheduling. *IEEE Transactions on Computers* 2006; **55**(6):703–719.
88. Song S, Hwang K, Kwok Y. Trusted grid computing with security binding and trust integration. *Journal of Grid Computing* 2005; **3**(1–2):53–73.
89. Das A, Islam MM, Sorwar G. Dynamic trust model for reliable transactions in multi-agent systems. *13th International Conference on Advanced Communication Technology* (ICACT), 2011; 1101–1106.
90. Wang B, Huang C, Yang W, Wang T. Trust opportunistic routing protocol in multi-hop wireless networks. *IEEE International Conference on Wireless Communications, Networking and Information Security* (WCNIS), 2010; 563–567.
91. Goncalves MRP, Moreira EDS, Martimiano LAF. Trust management in opportunistic networks. *9th International Conference on Networks* (ICN), 2010; 209–214.
92. Denko MK, Woungang I, Obaidat MS. Trust management in opportunistic pervasive healthcare systems. *16th IEEE International Conference on Electronics, Circuits and Systems* (ICECS), 2009; 832–835.
93. Chen H, Zhou X, Gao C. Agent-based trust model in wireless sensor networks. *8th ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing*, 2007; 119–124.
94. Qin T, Yu H, Leung C, Shen Z, Miao C. Towards a trust aware cognitive radio architecture. *ACM Sigmobile Mobile Computing and Communications* 2009; **13** (2):86–95.
95. Chen C-Y, Chao H-C. A survey of key distribution in wireless sensor networks. *Security and Communication Networks*. DOI: 10.1002/sec.354, article first published online, July 2011.