Journal of Computer and System Sciences 80 (2014) 602–617

Contents lists available at SciVerse ScienceDirect

Journal of Computer and System Sciences

www.elsevier.com/locate/jcss

Management and applications of trust in Wireless Sensor Networks: A survey

Guangjie Han [a,b,*], Jinfang Jiang [a,b], Lei Shu [c], Jianwei Niu [d], Han-Chieh Chao [e,f,g]

[a] Department of Information & Communication Systems, Hohai University, Changzhou, China
[b] Changzhou Key Laboratory of Sensor Networks and Environmental Sensing, Changzhou, China
[c] College of Electronic Information and Computer, Guangdong University of Petrochemical Technology, China
[d] School of Computer Science and Engineering, Beihang University, Beijing, China
[e] Institute of Computer Science and Information Engineering, Taiwan
[f] Department of Electronic Engineering, National Ilan University, I-Lan, Taiwan
[g] Department of Electrical Engineering, National Dong Hwa University, Hualien, Taiwan

ARTICLE INFO

Article history:
Received 30 November 2012
Received in revised form 30 April 2013
Accepted 14 June 2013
Available online 4 July 2013

Keywords:
Wireless Sensor Networks
Trust models
Cluster-based WSNs

ABSTRACT

Wireless Sensors Networks (WSNs) are susceptible to many security threats, and because of communication, computation and delay constraints of WSNs, traditional security mechanisms cannot be used. Trust management models have been recently suggested as an effective security mechanism for WSNs. Considerable research has been done on modeling and managing trust. In this paper, we present a detailed survey on various trust models that are geared towards WSNs. Then, we analyze various applications of trust models. They are malicious attack detection, secure routing, secure data aggregation, secure localization and secure node selection. In addition, we categorize various types of malicious attacks against trust models and analyze whether the existing trust models can resist these attacks or not. Finally, based on all the analysis and comparisons, we list several trust best practices that are essential for developing a robust trust model for WSNs.

1. Introduction

WSNs are emerging technologies that have a variety of potential applications such as battlefield surveillance, emergency response [1], healthcare monitoring [2] and accident detection, e.g., elderly falling detection [3,4]. However, WSNs are often deployed in unattended or even hostile environments. The wireless and resource-constraint nature of a sensor network makes it an ideal medium for attackers to do any kinds of vicious things. Therefore, providing security in WSNs is a major requirement for acceptance and deployment of WSNs. However, because WSNs are resource and bandwidth limited, achieving an acceptable level of security has been a difficult problem.

Various safety mechanisms, e.g., authentication, confidentiality, and message integrity, have been proposed to avoid security threats such as eavesdropping, message replay, and fabrication of messages. However, these approaches cannot adequately defend against network insider attacks, although they are effective to outsider attacks. This is because sensor nodes launching inside attacks can possess all the corresponding cryptographic keys and become legitimate network members. Therefore, these safety mechanisms based on cryptographic schemes need robust and secure key exchange mechanism. If one or multiple communicating nodes are compromised before successful key exchange, any subsequent safety

* Corresponding author at: Department of Information & Communication Systems, Hohai University, Changzhou, China.
E-mail addresses: hanguangjie@gmail.com (G. Han), jiangjinfang1989@gmail.com (J. Jiang), lei.shu@live.ie (L. Shu), niujianwei@buaa.edu.cn (J. Niu), hcc@niu.edu.tw (H.-C. Chao).

0022-0000/$ – see front matter
http://dx.doi.org/10.1016/j.jcss.2013.06.014

mechanisms are rendered ineffective. To guarantee secure key exchange and establish secure communications, we need to ensure that all communicating nodes are trusted. This highlights the fact that it is critical to establish trust between two communicating nodes.

Nowadays, existing trust management mechanisms [5,6] designed originally for wired networks, e.g., P2P network, and traditional trust management mechanisms [7,8] that have been developed for wireless ad-hoc networks are not suitable for WSNs because of higher consumption of resources such as memory and power. Therefore, many trust management mechanisms, e.g., RFSN [9], PLUS [10] and ATRM [11], have been proposed for WSNs. The purpose of this paper is to highlight summary and comparisons of trust models for WSNs. It is known that WSNs are energy constraint and vulnerable to malicious attacks. In order to save energy and improve security, many WSNs are organized into clusters [12]. Therefore, in this paper, we will discuss trust models in ordinary WSNs and cluster-based WSNs separately. This paper is organized as follows: In Section 2 and Section 3, we analyze and summarize trust models and applications of them in ordinary WSNs. Section 4 introduces trust models in cluster-based WSNs. Section 5 describes applications of trust models in cluster-based WSNs. In Section 6, we present security analysis based on malicious attacks. Finally, Section 7 gives the conclusions and open research problems.

2. Trust models in ordinary WSNs

In this section, we first discuss trust models in ordinary WSNs. Trust models are classified into two categories: 1) node trust models and 2) data trust models.

2.1. Node trust models

2.1.1. Analysis about node trust models

Generally speaking, node trust models can be classified into two categories: centralized and distributed models. In centralized trust models, a particular trusted intermediary or base station is used to calculate trust values of sensor nodes. In distributed trust models, sensor nodes calculate trust values by themselves.

Tae Kyung Kim, and Hee Suk Seo proposed a Trust Computation method using Fuzzy Logic (TCFL) for WSN in [13]. TCFL scheme uses nodes' trust values to calculate the trust values of paths. Then, the path with highest trust value is chosen to transmit the packets. Using fuzzy logical deduction can quantize uncertain or imprecise data. Therefore, TCFL scheme can be used to choose the proper path from source to destination node. However, in most applications, WSNs are either distributed or hierarchical dynamic network with large-scale sensor nodes. A sensor node mainly cares about trustworthiness of its neighbor nodes due to the multi-hop transmission nature. In addition, centralized approaches are always high energy consumption. Therefore, the proposed centralized scheme may not be suitable for practical applications. Even if the WSN is centralized, how to calculate sensor nodes' trust are not mentioned in TCFL.

From the above analysis, we know that distributed mechanisms are much more suitable for WSNs. For example, a distributed Reputation-based Framework for Sensor Networks (RFSN) is proposed in [9]. Two key building blocks of RFSN are Watchdog and Reputation System. Watchdog is responsible for monitoring actions of neighbor nodes and characterizing their actions as cooperative or non-cooperative. Reputation System is responsible for maintaining the reputation of a node. Based on related works [6,12,14,30,32], reputation of a sensor node is the neighbor nodes' perception of its past behaviors. Trust of a sensor node is the neighbor nodes' belief about its future behaviors. Given a reputation metric R_{ij}, the trust metric T_{ij} is obtained by:

$$T_{ij} = E[R_{ij}] = E\big[\text{Beta}(\alpha_j, \beta_j)\big] = \frac{\alpha_j}{\alpha_j + \beta_j} \tag{1}$$

In RFSN, an aging mechanism is proposed for trust updating, thus a node's trustworthiness is reevaluated continuously. However, RFSN assumes that each node has enough interactions with neighbor nodes so that reputation can reach a stationary state. If the movement speed of a sensor node is higher, reputation information will not stabilize. In regards to bad mouthing attacks, RFSN scheme only propagates good reputation information about other nodes. In this case, sensor nodes cannot resist against conflicting behavior attack because they cannot share their bad reputation information with each other.

Another distributed trust computation scheme, named Parameterized and Localized trust management Scheme (PLUS) is proposed in [10]. In PLUS, personal reference and recommendation are used to build reasonable trust relationship among sensor nodes. The personal reference value $T_{pr(i)}$ of node i is computed based on the node's availability and the proportion of correct packets. The recommendation value $T_{r(i)}$ is calculated based on neighbor nodes' trust values and the number of neighbor nodes. Therefore, the trustworthiness of node i can be expressed as: $T_{(i)} = T_{pr(i)} \times W_{pr} + T_{r(i)} \times W_r$, where $W_{pr} + W_r = 1$.

In PLUS, each sensor node maintains highly abstracted parameters, rates the trustworthiness of its interested neighbor nodes and identifies malicious nodes. However, the authors assume that all important control packets generated by a base station must contain a hashed sequence number (HSN). Inclusion of HSN in control packets not only increases size of packets but also increases energy consumption of transmission and reception. Whenever a judge node (the node which performs evaluation) receives a packet from suspect node (the node which is in radio range of the judge node and will be evaluated), it always check the integrity of the packet. If the integrity check fails, the trust value of suspect node will be decreased irrespective of whether it was really involved in malicious behaviors or not. Therefore, suspect node may get unfair penalty.

In addition, PLUS is not suitable for WSNs with high traffic rate promoting a need for a simple solution to detect malicious nodes.

Another similar trust evaluation algorithm defined as NBBTE (Node Behavioral strategies Banding belief theory of the Trust Evaluation algorithm) is proposed based on behavior strategy banding D–S belief theory [14]. NBBTE algorithm firstly establishes various trust factors depending on the interactions between two neighbor nodes. Then the trust value is obtained by combining network security degree and correlation of time context. Secondly, it applies the fuzzy set theory to measure how much the trust value of node belongs to each trust degree. Finally, considering the recommendation of neighbor nodes, D–S evidence theory method is adopted to obtain integrated trust value instead of simple weighted-average one.

In above-mentioned distributed trust computation mechanisms, each sensor node is responsible for trust computation. Therefore, much energy is exhausted for massage exchange and trust computation. In order to prolong life time of WSNs, using some special nodes instead of sensor nodes to calculate trust value may be a better choose. For example, an Agent-based Trust model is proposed in WSNs (ATSN) [15]. In ATSN, agent nodes use promiscuous mode to monitor behaviors of sensor nodes and classify the behaviors into good or bad ones. Then, agent nodes count all the number of good behaviors and bad behaviors respectively. Using p and n to denote the numbers of good behaviors and bad behaviors respectively, the reputation space is defined as:

$$RS = \left\{ \langle p, n \rangle \;\middle|\; p, n \in R;\ p, n \geqslant 0;\ t = p + n \right\} \tag{2}$$

The trust space is defined as $TS = \{(pt, nt, ut)\}$, where pt, nt and ut denote positive trust, negative trust and uncertainty, respectively. ATSN has some advantages. First, using agent nodes to monitor sensor nodes and calculate their trust values can minimize memory and computational complexity on ordinary sensor nodes. Second, only using direct neighbor sensing to calculate nodes' trust values, ATSN can limited negative effect of malicious recommendations injecting by some attacks such as bad mouthing attack and on–off attack. However, neighbor nodes' behaviors may not be fully recorded due to heavy traffic, packets lost or faults of cheap hardware in WSNs. Uncertainty in trust and reputation system should be considered [16]. Without consideration of recommendation and uncertainty, ATSN cannot calculate nodes' trust accurately. In addition, the performance of ATSN heavily relies on the agent nodes. The assumption that the agent nodes are resilient against any security threats is not make sense in realistic WSN applications. Additionally, how to refresh reputation and trust value has not been solved in ATSN.

In WSNs, each node may execute different tasks towards different neighbor nodes. A sensor node should have different trustworthiness for different tasks and different neighbor nodes. However, in above-mentioned trust computation mechanisms, a node always only has one trust value. In [17], a Task-based Trust framework for Sensor Networks (TTSN) is proposed, where sensor nodes maintain reputation for neighbor nodes of several different tasks and use the reputation to evaluate their trustworthiness. TTSN builds trust through an entity called Task and Trust Manager Module. The Task and Trust Manager Module involves three main components: (1) monitoring module; (2) reputation handling module and (3) task and trust handling module. The method for trust calculation is almost the same as described in RSFN [9]. Each sensor node in TTSN has several trust values. Relatively speaking, TTSN is more suitable for trust computation in WSNs. In addition, TTSN can be used in large scale WSNs.

2.1.2. Comparisons

A detailed comparison of different node trust models with respect to 1) methodology, 2) trust values, 3) advantages, 4) performance limitations and 5) complexity is provided in Table 1.

2.2. Data trust models

The fundamental functions of WSNs are data sensing, processing, and reporting, not to learn information of nodes. However, as the vulnerability of the wireless communication channel, an attacker can easily attack transmitting information through a wireless link, and conduct eavesdropping, forgery, tamper and even launch denial of service attacks. The propagation of false data will cause grievous damage and waste a lot of system energy. While in above-mentioned node trust models, data security is neglected. Therefore, it is important to evaluate trust value of data. Traditional data trust models to evaluate information in WSNs, such as SEF [18] and BSEF [19], are realized by MAC (Message Authentication Code). MAC can protect data integrity. However, once false data starts from attackers, these trust models will be invalid. Therefore, new data trust models is needed for WSNs.

2.2.1. Analysis about data trust models

A trust model is proposed to Distinguish Forged Data of Illegal nodes from innocent data of legal nodes (DFDI) in [20]. First, authors divide a sensing area into some logical grids and assign a unique identification to each grid. Then, sensor nodes deployed in each grid verify location information of neighbor nodes using ECHO protocol [21], and evaluate trustworthiness of their neighbor nodes by crosschecking the neighbor nodes' redundant sensing data with their own result. The trust value is calculated through a weighted summation of the three types of parameters: the consistency value of sensing data, the communication ability and the remained lifetime of a node. Finally, special nodes, aggregators, aggregate sensing data from their grids and transmit the aggregated results to the sink node. In this step, inconsistent data from malicious or compromised nodes can be detected.

Table 1
Comparison of node trust models.

Trust mechanisms	Methodology	Trust values	Advantages	Limitations	Complexity
TCFL [13]	Fuzzy logic; Trust is calculated based on sensor nodes' past actions.	[0, 1]; The trust values of paths are calculated.	Using fuzzy deduction can quantize uncertain or imprecise data.	Centralized scheme is not suitable for most WSNs.	Memory requirement to store past actions of sensor nodes.
RFSN [9]	Probability theory and Bayesian network; Using Watchdog to monitor neighbor nodes' actions.	[0, 1]; The implementation complexity and the energy/memory overhead of RFSN are analyzed.	Trust computation is precise without single point failure.	Can improve security of each node, but cannot improve system robustness.	Bayesian calculation requires memory and computational complexity.
PLUS [10]	Weighting; Trust is calculated based on personal reference and recommendation.	[0, 1]; Several malicious attacks, computational and communication overhead of PLUS are analyzed.	Efficiently detect malicious nodes.	Trust convergence time is high; PLUS is not suitable for WSNs with high traffic rate.	Computational complexity in implementing a set of recommendation protocols; Extra memory to store the recommendations.
NBBTE [14]	Weighting; Fuzzy theory and D–S Evidence Theory; Trust is calculated by observing the neighbor nodes' packet forwarding behavior.	[0, 1]; The influence of Malicious Nodes is analyzed.	By combining network security degree and correlation of time context, the trust computation is precise.	Need excess energy and time costs due to the cooperation and communication with neighbors; Memory costs also increase with network density.	Need excess memory and energy costs to monitor the packet forward event of neighbor nodes.
ATSN [15]	Weighting; Probability theory; Trust is calculated based on reputation space and trust space.	Use the binary event (p, n) to denote the reputation value. Then, transform reputation space to trust space.	Energy efficiency; Can limited effect of malicious node attack such as bad mouthing attack, on–off attack and conflicting behavior attack.	Performance heavily relies on agent nodes; Vulnerable to malicious agent nodes.	No memory and computational complexity on ordinary sensor nodes.
TTSN [17]	Weighting; Bayes Theorem and Beta Distribution; Trust is calculated by monitoring neighbor nodes' behaviors.	Use the binary event (p, n) to denote the reputation value; The trust metric of a node about the task is the statistical expectation of the posterior probability function.	Trust calculation is based on task. Hence this approach is generic enough to be applied in different WSNs.	Use neither recommendations nor past observations; Calculated trust is totally instantaneous.	Task collection and Bayesian calculations requires memory and computational complexity.

However, the DFDI might have some performance problems. First of all, it is only suitable for dense networks. If nodes become sparse, then it is possible that there are not enough neighbor nodes within their communication range. In such cases, when it is unable to verify location information of neighbor nodes, it cannot evaluate trust of sensor nodes accurately. Second, using the ECHO protocol, each sensor node can only verify that whether its neighbor nodes are within their claimed distance, that is, in a specific range. Sensor nodes are in capable of verifying exact positions of their neighbor nodes. Finally, it assumes that the locations of all sensor nodes are already known, which also reduces the flexibility of the network. In addition, this centralized approach may not be practical due to limited energy budget in sensor nodes. If readings are sent to the sink all the time, sensor nodes may soon exhaust their energy.

In [22], the problem of Determining Faulty Readings (DFR) is studied. Both arbitrary and noisy readings are viewed as faulty readings. First, by exploring correlations between readings of sensors, a correlation network is built based on similarity between readings of two sensors. The correlation network is modeled as a graph $G = (V, E)$, where V represents the sensor nodes in the deployment region and E represents the correlation between two nodes. If two neighbor nodes do not have any similarity in their readings, these two nodes do not have an edge connected. Once the correlation network of sensors is constructed, it is easily to deduce the correlations among sensor nodes. By exploring Markov Chain in the network, a mechanism for rating sensor nodes in terms of the correlation, called SensorRank, is developed. SensorRank represents the trustworthiness of sensor nodes. In light of SensorRank, an efficient in-network voting algorithm, called Trust Voting, is proposed to determine faulty sensor readings. Compared with some centralized approaches, e.g., DFDI, DFR are much more practical. Simply filtering out unusual readings may compromise monitoring accuracy of some important events, while using SensorRank to determine faulty readings can avoid this problem effectively.

Inconsistent, unusual or faulty readings are usually caused by two different reasons: intentional misbehavior and unintentional errors. Intentional misbehavior is caused by malicious nodes, while unintentional errors are caused by some

Table 2
Comparison of data trust models.

Trust mechanisms	Methodology	Trust values	Advantages	Limitations	Complexity
DFDI [20]	Weighting; Inconsistent data is detected by nodes' trustworthiness.	[0, 1]; Trust is calculated based on consistency value, sensing communication value and battery value.	Inconsistent data from malicious or compromised nodes can be detected.	ECHO protocol consumes extra energy and time costs.	Computational complexity of ECHO protocol.
DFR [22]	Based on TrustVoting algorithm and correlations between readings of sensors.	Use SensorRank to represent the trustworthiness of sensor nodes.	Trust computation is precise using SensorRank.	Vulnerable to collusion attacks.	Complexity of building the correlation network.
MDLC [23]	Weighting; Subjective logic framework based on the D–S evidence theory.	In each sensor data's life cycle, trust of raw, routed and processed sensor data are calculated.	Trust values calculated based on data life cycle are precise.	Do not consider malicious attacks.	Minimal complexity.
TMCDE [24]	Use the Beta Trust Model to calculate the communication trust; Combine TIBFIT and the security data fusion algorithm to calculate data trust value.	Multi-angle trust includes communication trust, data trust and node's energy trust.	Integration value based on communication trust, data trust and energy trust is more reliable.	Do not consider how to update trust values.	Minimal complexity.

external factors in the data processing, e.g., malfunctioning hardware or exhausted batteries. The above-mentioned approaches all focus on to determine faulty readings, but barely address erroneous data processing. In order to properly assess trustworthiness of sensor data, a novel Mechanisms based on Data Life Cycle (MDLC) is proposed in [23]. There are three states for sensor data: 1) raw, 2) routed and 3) processed. A sensor data is raw as long as it has been acquired (sensed) by a node without any additional routing or processing. As soon as a sensor data is sent to another node, it is considered as routed. Processing means data manipulation such as filtering, fusion or aggregation. Based on subjective logic [13], trust of raw data, routed data and processed data are calculated.

The above-mentioned trust models are established only base on interactions between neighbor nodes. The trusty WSNs based on interactions is trustworthy only when sensing data is normal and energy is evenly consumed. Once the sensing data and energy have the crisis of trust, malicious, selfish and low competitiveness nodes appeared in WSNs will lead to trusty nodes no longer reliable. In [24], a Trust Model base on Communication trust, Energy trust and Data trust is proposed for WSNs (TMCDE). Communication trust means the relationship value calculated between two cooperation nodes, which is computed based on the rate of successful transactions. Energy trust refers to the residual energy of node whether enough to complete new communications and data processing tasks. Data trust is the trust assessment of the fault tolerance and consistency of data. It is calculated by: $T_d = W_1 T_f + W_2 T_u + W_3 T_v$, where T_f, T_u and T_v are the fault-tolerant trust value of node, the credibility trust value of the event report and the consistency trust value of data respectively. By use of the energy trust, TMCDE can effectively detect DoS attack. Once malicious nodes carry out DoS attack, it will consume a lot of energy. The energy trust becomes lower than that of normal nodes. Therefore, malicious nodes with much lower energy trust can be detected.

2.2.2. Comparisons

A detailed comparison of different data trust models with respect to 1) methodology, 2) trust values, 3) advantages, 4) performance limitations and 5) complexity is provided in Table 2.

3. Applications of trust models in ordinary WSNs

WSNs consist of hundreds to thousands of inexpensive sensor nodes to detect environmental events either continuously or intermittently whenever the occurrence of event triggers the signal detection process. The data picketed up is either lightly processed locally by the sensor node or sent to a sink node or a base station. This kind of environment presents several security challenges. First, when monitoring physical or environmental events, a sensor node can be captured and manipulated by the adversary. Then, in the communication process which transfers data from sensor nodes to a sink node or a base station, data aggregation is usually used to reduce the amount of transmitted data. Sensor nodes always cooperate with each other to resist against malicious attacks or are scheduled to work alternatively to improve energy efficiency and prolong network lifetime. Thus the adversary may attack related routing protocols, data aggregation, and node sleeping schedule schemes. In addition, location information is critical to some routing protocols, e.g., geographical routing. Therefore, in this section, we discuss the applications of trust models in WSNs from the following five aspects: 1) malicious attack detection, 2) secure routing, 3) secure data aggregation, 4) secure localization and 5) secure node selection.

3.1. Malicious attack detection

Deployed in a hostile environment, individual nodes of WSNs could be easily attacked by the adversary due to the constraints such as limited battery lifetime, memory space and computing capability. It is critical to detect malicious attacks in order to avoid being misled by the falsified information injected by the adversary through compromised nodes. In addition, malicious nodes may drop some of packets to start a selective forwarding attack, refuse forwarding any packet or implement Denial of Service (DoS) attacks.

In [25], in order to avoid the selective forwarding attack, a secure data transmission scheme (SDTS) which can forward the data safely is proposed. First, the trust value of each node is judged to select a secure path for message forwarding. Then, the watermark technology is used to detect the malicious nodes which are suspected to launch selective forwarding attack. At the beginning of the network initialization, the trust value of every node is set as the same value tv_i. If a node is detected as a malicious one, the trust value will be decreased a half of tv_i: $tv_i = tv_i - \frac{1}{2}tv_i$. When a node's trust value decreases, it does not mean the node will not be used anymore. The trust value of the node will increase linearly by time $tv_i = tv_i + k$, where k is a environment parameter can be dynamically adjusted in different network conditions. Therefore, if a node is doubted by mistake, it will be used again later.

In order to avoid selfish nodes that are likely to refuse forwarding packets, a Data-centric Dempster–Shafer theory-based Selfishness Thwarting via Trust evaluation ($D^2S^2T^2$) is proposed in [26]. $D^2S^2T^2$ defines trust in regard to forwarding (T_{ij}^F) and in regard to recommendations (T_{ij}^R). T_{ij}^{F+} and T_{ij}^{F-} are defined to reflect how much node i trusts node j to forward or not forward node i's packets, respectively. Then, node i can use a threshold heuristic to treat node i as selfish ($T_{ij}^{F-} \geqslant ST$) or non-selfish ($T_{ij}^{F+} \geqslant ST$), where $ST \in (0.5, 1]$ is a selfishness threshold. In most selfishness detection mechanisms, in order to speed up detection of selfishly misbehaving nodes, nodes share their opinions with neighbor nodes in the form of recommendation messages. However, false recommendations are always ignored. Therefore, in $D^2S^2T^2$, trust associated with recommendation message is diminished. T_{ij}^R is obtained by using node i's Evidence Manager Component to filter and weigh received recommendations. $D^2S^2T^2$ cannot only detect selfish nodes, but also effectively control the impact of false recommendations to make the system more robust against malicious attacks.

3.2. Secure routing protocols

Secure routing is especially important for WSNs. However, there are many attacks towards WSN routing protocol. Traditional routing mechanism, e.g., GR (geographic routing) and GEAR protocols, could not do anything against malicious attack, because they are just response for searching a routing to transfer messages. Therefore, secure routing is needed.

3.2.1. Modified routing protocols

In [27], the security of geographic routing (GR) protocols is considered. A trust management scheme for Resilient Geographic Routing (T-RGR) is proposed. The trust algorithm works in a fully distributed manner, in which each node monitors the one-hop neighbor nodes' behaviors. If the source node detects that a neighbor node i has successfully forwarded a packet, it will increase the trust level of node i with a predefined step size. Otherwise, the trust level of node i will be decreased with a predefined step size.

In T-RGR protocols, each sensor node needs to continuously monitor its environment. This is considered to be a costly operation for a WSN because of its resource scarcity. In [28], based on GEAR protocol, authors propose a trust-aware routing, which implements a new monitoring strategy called an Efficient Monitoring Procedure in a Reputation system (EMPIRE). The reputation system consists of three main components, that is, monitoring, rating and response components. Monitoring component is response for observing packet forwarding events. Every sensor node alternates between ON state and OFF state. Only the nodes that are in the ON state perform monitoring activities. Rating component evaluates the amount of risk an observed node provides for the routing operation. The risk value is a quantity that represents previous misbehaving activities that a malicious node (a node that drops packets) has obtained. Finally, in response component, the risk values computed by the rating component are incorporated with distance and energy information to choose the best next hop for the routing operation.

3.2.2. New trust-aware routing protocols

In [29], the authors add mobile nodes to a WSN and propose an Efficient Reputation-based Routing Mechanism (ERRM). When a node A has collected the required number of reputation values for a given neighbor B, it aggregates the information. First it finds the median of the collected reputation values. It then discards reputations that are beyond a threshold from the median. The remaining reputations are then weighted before being averaged. The weighted reputation contribution is calculated as follows:

$$RW_{C\to B} = TN_{A\to C} \times R_{C\to B} \times AG_{C\to B} \tag{3}$$

where $TN_{A\to C}$ is the trust value that node A grants node C, $R_{C\to B}$ is the reputation value that node C grants node B and was transmitted to node A. $AG_{C\to B}$ is the age of the reputation information $R_{C\to B}$ that has been collected by node A. The final weighted average of all reputations for node B is given as follows:

$$TN_{A\to B} = \frac{\sum_{C\in Contributor} RW_{C\to B}}{\sum_{C\in Contributor} (TN_{A\to C} \times AG_{C\to B})} \tag{4}$$

This mechanism can maintain a very high success rate. Success rate is the number of packets sent by the normal nodes which reach the BS in sequential order and are not corrupted by any malicious node. However, in the process of choosing the best route, if there are more than two routes, it needs to compare every two routes and discard the route with the higher expenditure until it has eliminated all but one route. This choosing process will consume plenty of energy. In addition, the problem "how the rout and cost of a route is computed" is not addressed. The most trusted route will be selected very frequently which may lead in bad load balancing and power exhaustion, which shortens the lifetime of the network.

Another routing protocol incorporating trust was proposed in [30], which is called Trust-Aware dynamic Routing Framework (TARF). TARF consists of four components, namely, Trust Metrics model, Behavior Detection model, Trust Evaluation model, and Trust-Aware Routing model. In Trust Evaluation Metrics model, a set of performance metrics are defined such as packet forwarding observation, packet modification observation and routing message verification. These performance metrics are used as the input to the Behavior Detection model to quantify the monitored neighbor nodes' activities and attempt to detect compromised node's behaviors. The output of Behavior Detection model is the individual trust evaluation parameter, which is used to compute trustworthiness by Trust Evaluation model. The trustworthiness T is directly derived from two parts: reputation R_E and risk R_I:

$$T = \begin{cases} (1-\alpha,\alpha)\times(R_E,R_I)^T, & 0<\alpha<1 \\ R_I, & \text{if } \alpha = 1 \\ R_E, & \text{if } \alpha = 0 \end{cases} \tag{5}$$

The most direct policy to consider trust when making the route decision is to select the next hop with the maximum trustworthiness value. However, this may result in an extremely large delay. Therefore, the authors propose a trust-aware routing criterion to integrate the trust model with routing protocols while avoiding the introduction of large delays. The routing criterion (RC) is defined as:

$$RC = \frac{C}{T} \quad \text{or} \quad RC = C \times T \tag{6}$$

where C is the original routing criterion value for a sensor node to make routing decision. T is the trustworthiness value of the sensor node. The first formula is applied if C represents the routing criteria such as hop count, delay, cost, etc. The second formula is applied if C represents the routing criteria such as bandwidth, etc. We can easily see that minimizing the RC can achieve both minimum delay and maximum trustworthiness. In addition, TARF is not limited to any particular routing protocol. Therefore, it can be easily integrated into existing routing protocols with minor modifications.

In the work conducted in [31], a Trust-based Cross-Layer Model (TCLM) is presented, which uses a cross-layer concept (ACKs from data link layer and TCP layer) to design trust-based model for sensor networks that guarantee trust route from source to sink and isolate the malicious node. The packet statistics can be used to compute a pair of values associated with each neighbor node, which are trust (denoted as t) and treatment ratio (denoted as r). The trust value characterizes the degree of belief that the neighbor node is reliable with respect to packet delivery. The treatment ratio characterizes the statistical confidence in this belief. Let L denote the cumulative number of packets which are correctly forwarded by a sensor node, and let N denote the cumulative number of packets which are sent by the sensor node. The trust (t) and treatment ratio (r) are defined as follows:

$$t = \frac{L}{N}, \qquad r = 1 - \frac{\sqrt{12L(N-L)}}{(N+1)N^2} \tag{7}$$

3.2.3. Comparisons

A detailed comparison of secure routing protocols with respect to 1) methodology, 2) trust values, 3) advantages, 4) performance limitations and 5) complexity is provided in Table 3.

3.3. Secure data aggregation

Data aggregation in sensor networks is the process of gathering data from different sensor nodes and expressing the data in a summary form before it is sent to a sink node or a base station. Data aggregation is essential in WSNs as it minimizes the number of transmissions, therefore improve energy efficiency and prolong network lifetime. Especially when sensor nodes are located relatively close to each other and far from the base station, much more energy can be saved. However, sensor nodes may be deployed in remote and hostile environments where attackers inject false information or forge aggregation values without being detected. Thus, security issue becomes an important research field in data aggregation for WSNs.

Sensor nodes in WSN interact with each other with different roles. A secure data aggregation based on Social Estrangement Trust Management model (SETM) is proposed in [32], where a node is assigned with the role of sensor, aggregator, or forwarder. A sensor node senses environment and passes readings to its local aggregator. An aggregator aggregates the

Table 3
Comparison of secure routing protocols.

Trust mechanisms	Methodology	Trust values	Advantages	Limitations	Complexity
T-RGR [27]	The exact details of the trust mechanism are not considered.	[0, 1].	Sybil attacks, Black hole and selective forwarding attacks are considered.	Vulnerable against collaborative attacks.	Need excess memory and energy costs to monitor the packet forward event of neighbor nodes.
EMPIRE [28]	The exact details of the trust mechanism are not considered.	Not mentioned.	Reduce monitoring activities per node.	Only consider non-forwarding attack.	Complexity of managing the ON state and OFF state.
ERRM [29]	Weighting.	Calculated based on the recommendations from neighbor nodes.	Can prevent the effect of hostile nodes whether sensor nodes are mobile or not.	Choosing the best route consumes plenty of energy.	Minimal complexity.
TARF [30]	Matrix theory.	Calculated based on reputation and risk.	Robust against selective forwarding attack, message modification attack and black hole attack.	Using the trust evaluation metrics to characterize routing misbehaviors is still an open problem.	Need excess memory and energy costs to monitor neighbor nodes' behaviors.
TCLM [31]	Bayesian statistics and Beta distribution.	[0, 1]. Trust and treatment ratio are calculated.	Can work excellently even if the percent of malicious nodes is high.	Only scalable for dense WSNs with big number of sensor nodes.	Additional hardware (like watchdog) to watch data sending and receiving between neighbor nodes.

readings from sensor nodes and sends them to another aggregator or forwarder. A forwarder simply forwards the data to another aggregator or a base station. Therefore, three kinds of trust, namely, aggregation trust, forwarding trust, and sensing trust are taken into account in SETM. SETM can efficiently undermine several misbehavior attacks, e.g., selective forwarding attack. However, it cannot predict future behavior. If a node behaved satisfactorily in the past, it is likely that it is reliable.

3.4. Secure localization

In WSNs, localization is one of the most important technologies since it plays a critical role in many applications. If the users cannot obtain the accurate location information, the related applications cannot be accomplished. The main idea in most localization methods is that some deployed nodes (called anchor nodes) with known coordinates (e.g., GPS-equipped nodes) transmit beacons with their coordinates in order to help other nodes localize themselves. Thus, it is important to exclude malicious anchor nodes that provide false location information.

In [33], a Distributed Reputation-based Beacon Trust System (DRBTS) is proposed. To the best of our knowledge, DRBTS is the first model to use the concept of reputation for excluding anchor nodes. In DRBTS, every anchor node monitors its one hop neighborhood for misbehaving anchor nodes and accordingly updates reputation of the corresponding anchor nodes in Neighbor-Reputation-Table (NRT). The details of reputation updating are: when a sensor node asks for location information, all anchor nodes within the range of the requesting node responds with their locations. An anchor node can overhear the responses of neighbor anchor nodes. It can then determine its location using these claimed locations of neighbor anchor nodes and comparing them against its true location. If the difference is within a certain margin of error, then the corresponding anchor node is considered benign, and its reputation increases. If the difference is greater than the margin of error, then that anchor node is considered malicious and its reputation is decreased. Finally, sensor nodes use the NRT information to determine whether or not to use a given beacon node's location information, based on a simple majority voting scheme. In order to trust a beacon node's information, a sensor node must get votes for its trustworthiness from at least half of their neighbor nodes. DRBTS can reduce the impact of attacks from malicious beacon nodes to a certain degree, but it cannot resist conspiracy attack. Another drawback of DRBTS is that anchor nodes update their reputation by themselves. If anchor nodes are compromised, they may maliciously distort reputation value and cannot update reputation normally. Therefore, DRBTS is vulnerable to compromised anchor nodes. Also, DRBTS has not mentioned the details about how the reputation of an anchor node is calculated.

Another similar trust based secure localization (TBSL) scheme is proposed in [34]. The difference between DRBTS and TBSL is that an anchor node's reputation in TBSL is evaluated through detecting identity and behavior of the anchor node. Therefore, TBSL can fight effectively against attacks from compromised anchor nodes. Another difference is that after evaluating trust values of anchor nodes, each unknown node in TSBL collects the evaluation values from neighbor anchor nodes and computes the average evaluation value. Then, each unknown node selects the trustworthiness anchor nodes whose trust values are above a threshold value and estimates its own position using the position information provided by these trusted

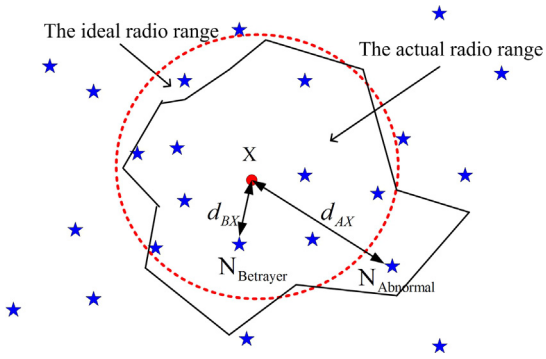

Fig. 1. The reputation-based revising scheme.

anchor nodes through maximum likelihood estimation. Compared with the majority voting scheme used in DRBTS, TSBL are much simple and energy efficiency for WSNs.

The above-mentioned secure localization schemes are range-based localization. Generally speaking, range-based algorithms can achieve higher localization accuracy. However, they are always high energy consumption. In contrast, range-free algorithms do not need to measure distance or angle information between unknown nodes and anchor nodes. However, in practical circumstance, range-free information is usually unreliable due to combined factors such as irregular signal patterns, environment noise and so on. To make matters worse, the unreliable localization information will lead to the reduction of localization accuracy. In order to tackle this problem, the authors propose a Reputation-based Revising Scheme (RRS) [35] to preprocess the raw localization information before applying any positioning algorithm. In RRS, authors reevaluate the reliability of raw information. As shown in Fig. 1, the ideal radio range is a circle, while the actual radio range is irregular caused by Irregular Signal Model. It is assumed the raw neighbor set of node X is NS_X. It is easy to find out that node $N_{Betrayer}$ is able to overhear more members of NS_X than $N_{Abnormal}$ for it is closer to node X ($d_{BX} < d_{AX}$). Thus, RRS endows $N_{Betrayer}$ a higher reputation than $N_{Abnormal}$. In this way, we can exclude the abnormal nodes from the neighbor set and include the betrayer ones by comparing nodes' reputation with the predetermined threshold. Obviously, RRS should be an iterative process. After one round iteration, new NS_X is obtained. The process repeats until the neighbor set does not change any more.

After being processed through RRS, the raw information is close to the information collected in ideal environment. Based on the revised information, the classical range-free localization algorithms can achieve higher localization accuracy. It is shown that RRS can restore the network to an ideal environment, but has failed to sufficiently consider malicious attacks.

3.5. Secure node selection

In WSNs, sensor nodes cooperate with each other to perform target tasks such as localization and tracking. However, the cooperative characteristic among nodes can be easily utilized to attack the whole network by malicious nodes. If inappropriate nodes are chosen, they have no ability to accomplish the task, or cannot complete the task in a satisfying way. Therefore, based on trust mechanism, Han et al. proposed a Reliable Sensor Selection algorithm with power-aware [36,37].

In the trust model, a sensor node is denoted by $Node\langle ID, A, V, T\rangle$, where ID denotes the identity of the node, A denotes the attribute set of node ID, V denotes the value set of the attributes and T denotes the trust value set of the attributes (every attribute has its own trust value). The trust value for attribute A_i can be computed as: $T_{A_i} = \frac{S_i}{C_i}$, where C_i is the number of the cooperation between neighbor nodes, S_i is the successful cooperation. The trust model consists of direct trust module, indirect trust module and integrated trust module. The direct trust value is calculated by:

$$T_{direct} = \frac{\prod_{i=1}^{n} T_{A_i}}{\prod_{i=1}^{n} T_{A_i} + \prod_{i=1}^{n}(1 - T_{A_i})} \tag{8}$$

The indirect trust value is calculated by:

$$T_{indirect} = W_{reliable} \times T_{reliable} + W_{strange} \times T_{strange} \tag{9}$$

where $T_{reliable}$ and $T_{strange}$ denote as the trust value returned by the reliable third-party nodes and the strange third-party nodes respectively, $W_{reliable}$ and $W_{strange}$ denote as the weight of the reliable third-party nodes and the strange third-party nodes respectively, $W_{reliable} + W_{strange} = 1$. Finally, the integrated trust value can be calculated by weighting the direct trust and the indirect trust.

4. Trust models in cluster-based WSNs

Many WSNs in real scenarios are organized hierarchically to lower energy consumption of communication overhead, and to raise network security and connectivity [38]. In this section, we discuss trust models in cluster-based WSNs.

4.1. Analysis about trust models

Totally distributed trust computation mechanisms are not suitable for WSNs because each sensor node has limited memory and computation power. In a distributed approach, each node needs to maintain message records about trust values of entire network. Therefore, totally distributed trust computation mechanisms are not possible for a large scale WSN. We believe that neither completely centralized nor completely distributed trust computation mechanisms are suitable for WSNs.

In [39,40], authors propose a hybrid trust computation scheme; named Group based Trust Management Scheme (GTMS), in which the whole group will get a single trust value. Within each group, all sensor nodes calculate individual trust values for all group members. Cluster head will aggregate these trust values and forward them to a base station. Then, the base station will calculate cumulative trust value of the whole group. Depending upon that trust value, the base station will assign one out of three possible states, namely: trusted, untrusted and uncertain to the whole group. In this way, the state of all the groups will be calculated and stored at the base station. After that, the base station periodically multicasts current state of each group to all cluster heads.

GTMS is very simple and flexible, and does not require large storage of data and complex computations at sensor nodes. For sensor nodes, the size of each record is 22 bytes. If there are 10 sensor nodes in a cluster, the size of trust database requires 198 bytes of sensor nodes' memory space. For cluster heads, the size of each record is 22 bytes. If there are 10 nodes in each cluster and 20 groups in the WSN, then each cluster head needs 616 bytes of memory to store these values. Also, we believe that sensor nodes mostly fulfill their responsibilities in a cooperative manner rather than individually. Therefore instead of calculating individual trust, it is more appropriate to calculate the trust for the entire group. In addition, GTMS is intrusion tolerant and provides protection against malicious, selfish, and faulty nodes. By dishonest behavior, a node provides false information about another node. The information might be a higher trust value or a lower trust value than the actual trust value. Therefore the malicious nodes with dishonest behavior can be detected by GTMS. However, GTMS scheme has some other limitations such as the unrealistic assumption. In order to protect the trust values from attacks, GTMS assumes a secure communication channel and does not take malicious attacks against trust models into account.

Another Hybrid Trust computation scheme for Cluster-based WSNs (HTCW) is proposed in [41], where surveillance nodes are selected by cluster head to monitor the behaviors of sensor nodes and to compute the reputation and trust rating for these sensor nodes. In HTCW scheme, the storage requirement of surveillance nodes is determined by the number of cluster nodes. This number depends on the cluster size, the communication range of sensor nodes, and the network density but independent of the network size. So, to restrict the size of cluster is not only conducive to ensure whole network security, but also conducive to save the storage room on the sensor nodes. By using the distance-based outlier detection and the watchdog mechanism, the surveillance nodes can detect the presence of invalid data resulting from compromised and faulty nodes. Furthermore, HTCW scheme is robust against some malicious attacks through rating cluster node behavior and predict the future behavior of the nodes. Although surveillance nodes can monitor the behaviors of cluster heads, cluster heads are very vulnerable to malicious attacks because the trust value of cluster heads is neglected.

Existing generic trust models are often difficult to meet the characteristics of multi-hop routing. In their research in [42], Liu et al. proposed a Trust Model based on Bayes Theorem (TMBBT), in which nodes are divided into two categories: the first is the node which communicates with the other node by single hop routing only, the second is that not only communicates through single hop routing, but also communicates with nodes cannot be reached by single hop through multi-hop routing. In TMBBT, trust assessment consists of two parts: communications trust and data trust. The communications trust is a value calculated based on cooperated routing information. The reputation and trust of data are calculated based on the ratio of the successfully received data. As to the first kind of nodes, there are only direct communication and direct date without counting indirect communication and indirect data through which can save this part of energy consumption. However, the trust computation without neighbor nodes' recommendation is not accurate enough. In addition, how to combine the communications trust and data trust are not studied in the paper.

4.2. Comparisons

A detailed comparison of different trust models in cluster-based WSNs with respect to 1) methodology, 2) trust values, 3) advantages, 4) performance limitations and 5) complexity is provided in Table 4.

5. Applications of trust in cluster-based WSNs

5.1. Malicious attack detection

Distributed WSNs have problems on detecting and preventing malicious nodes, which always bring destructive threats and compromise multiple sensor nodes. Therefore, I. Atakli et al. [43] proposed a weighted-trust evaluation (WTE) to detect malicious nodes in a hierarchical sensor network. In WTE, the weighted-trust, W_n, is computed as follows:

$$W_n = \begin{cases} W_n - \theta \times r_n, & \text{if } (U_n \neq E) \\ W_n, & \text{otherwise} \end{cases} \tag{10}$$

Table 4
Comparison of trust models in cluster-based WSNs.

Trust mechanisms	Methodology	Trust values	Advantages	Limitations	Complexity
GTMS [39,40]	Calculated based on time-based past interaction and recommendations.	An integer between [0, 100].	Doesn't require large storage of data and complex computations at sensor nodes.	Do not consider malicious attacks against trust models.	Minimal complexity.
HTCW [41]	Classical beta-binomial framework.	Reputation is estimated based on transaction data.	Save cluster heads' resources by using surveillance node to monitor sensor nodes.	The number of sensor nodes in each cluster is limited. Cluster heads can easily be attacked.	Using surveillance node introduces extra messages and time delay.
TMBBT [42]	Bayes Theorem.	Reputation is obtained through history communication and data.	Available for multi-hop routing.	How to combine the communication and data trust has not been considered.	Minimal complexity.

where U_n is the sensing data of the evaluated node, E is the aggregated data at the cluster head, θ is the penalty ratio. $r_n = \frac{m}{s}$, where m is the number of nodes that produce inconsistent data and s is the total number of nodes under the cluster head. Their proposed system works well when a relatively small fraction of the nodes are compromised. However, when over a quarter of the nodes are compromised, the performance is not satisfactory.

5.2. Secure routing

5.2.1. Modified routing protocols

In [44], the proposed system of TLEACH (trust-based LEACH) consists of two main modules: trust management module and trust-based routing module. For any operation O_A, upon receiving a misbehavior report, the direct trust of node i on node j is defined as follows according to the beta distribution:

$$DT(i, j, O_A) = \frac{N_o + 1}{N_o + N_m + 2} \tag{11}$$

where N_m and N_o represent the number of misbehaviors and normal-behaviors of the operation O_A. Upon receiving the second hand trust from neighbor node k, node i computes indirect trust on node j according to the following formula:

$$IDT(i, j, O_A) = TS(i, k, O_A) \times ST(k, j, O_A) + \big(1 - TS(i, k, O_A)\big) \times TS(i, j, O_A) \tag{12}$$

where $ST(k, j, O_A)$ is the trust value from node k to node i on node j. $TS(i, k, O_A)$ and $TS(i, j, O_A)$ are the trust value of node i on node k and node j. Compared with LEACH, TLEACH is much more robust against malicious nodes. However, TLEACH is vulnerable to collusion attacks.

In [45], authors present a new framework called T-SNIPER for sensor node clustering and routing that is based on socio-economic banking model. T-SNIPER draws on the features demonstrated in LEACH and HEED. Unlike other routing protocols, T-SNIPER does not guarantee data transfer but focuses on determining the best route for data. Simulation results show that T-SNIPER offers several benefits, primarily in respect to energy and resource savings and contributing to extension of the life-time of the WSN. However, T-SNIPER algorithm may not represent an optimal solution for real-time data delivery requirements.

5.2.2. New trust-aware routing protocols

In above mentioned trust-aware hierarchical routing schemes, e.g., TLEACH and T-SNIPER, the following problems exist: 1) energy will be consumed rapidly and network lifetime is decreased because of long distance communication between two cluster heads; 2) the trust evaluations is just considered in packet forwarding phase without considering the cluster heads selection; 3) energy consumption for cluster heads communication is neglected; 4) the trust model cannot detect and isolate malicious nodes. In [46], a novel Routing Algorithm based on Trustworthiness Core Tree (RATCT) is proposed for cluster-based WSNs. RATCT uses the Core Tree structure to avoid long distance communication between two cluster heads. Then, a trust model integrated with RATCT is proposed to evaluate the trust values of nodes. The proposed trust model can efficiently detect malicious nodes. However, building trustworthy core tree and calculating trust values with centralized method will consume extra energy.

5.3. Secure data aggregation

For data aggregation, a compromised node cannot only send forged sensory data, but also alter aggregation results. It introduces uncertainty in the aggregation results. Thus, in [47], authors propose an approach to secure aggregation process

against compromised node attacks and quantify uncertainty in the aggregation results. In [47], aggregators are responsible for measuring each individual sensor node's trustworthiness by examining its reported sensory data against others' data. Moreover, for each aggregation result, it is associated with an opinion, a measure of uncertainty, to represent the degree of trust in the aggregation result. The trustworthiness of each sensor node is evaluated by using an information theoretic concept, Kullback–Leibler (KL) distance. Let $\prod = (0, 1)$, where 0 represents data falls out of the range and 1 otherwise. Consider two distributions s and t on $\prod$, $p, q \in [0, 1]$ represent the probability of data falling within the range for s and t, respectively. The KL-distance between distribution s and t is defined as:

$$D(s||t) = (1-p)\log\left(\frac{1-p}{1-q}\right) + p\log\frac{p}{q} \tag{13}$$

In [47], the cluster head can check sensor nodes' trustworthiness to detect compromised nodes while sensor nodes can use the trustworthiness to elect new aggregators or cluster head in case that they are behaving abnormally. Compared with the network model used in SAPC [48], the network model used in [47] is much more secure. Since in [47], data aggregation in each cluster are independent, while in SAPC, the upper aggregator node has no way to check if the aggregation result sent by the down aggregator is valid or not. However, in [47], only spatial-correlated data are used to compute reputation. In fact, the data is not only spatial-correlated but also temporal-correlated. That is, the sensed data not only correlated with the other data in the same region (spatial-correlation), but also correlates with the history of data itself (temporal-correlation). Similarly, node behavior is also spatial-correlated and temporal-correlated. Therefore, in [49], the authors propose a secure Behavior Trust Data Aggregation (BTDA) algorithm. BTDA not only controls interference caused by false data of sensor nodes but also identifies malicious attacks disguised as legitimate nodes. Similar secure data aggregation is proposed in [50]. After the formation of cluster structure, relay nodes will be chosen based on their residual energy level. The selected relay nodes are responsible for data aggregation. Choosing other nodes for data aggregation can efficiently reduce the burden of cluster heads. However, when the relay node's energy is below the threshold value, it will lose the right to carry out data fusion. In addition, the value of the threshold has not been discussed.

In above mentioned secure data aggregation mechanisms, only one type of trust is considered. For example, data trust is used in [47] and behavior trust is used in BTDA and SETM. In fact, we can use Multi-Criteria to calculate the trust value. The Multi-Criteria can be a combination of data trust, node trust, behavior trust, link trust and so on. Multi-Criteria (MC) have been proposed in [51], however, no details are presented.

5.4. Secure node selection

In order to prolong network lifetime, cluster-based approaches are well-known methods used to enhance the lifetime and performance of large scale networks. The election of a malicious or compromised node as the cluster head is one of the most significant breaches in cluster-based WSNs. In light of this, [52] introduces a distributed trust-based framework (DTF) and a mechanism for the election of trustworthy cluster heads, where each node has a watchdog mechanism that allows it to monitor network events of neighbor nodes. Using the information obtained through monitoring enable the nodes to compute and store trust levels for its neighbor nodes. The trust level is computed as follows:

$$T = \omega_1 d_1 + \omega_2 d_2 + \omega_3 d_3 + \omega_4 c_1 + \omega_5 c_2 + \omega_1 c_3 + \gamma \tag{14}$$

where γ is a predetermined constant that is set to equal to the average packet drop rate of the network. d_1, d_2, d_3 and c_1, c_2, c_3 are related to the data packets and control packets respectively. The mechanism can prevent malicious nodes from being selected as cluster heads. However, it cannot detect malicious nodes in the process of selection cluster head. In addition, this approach involves all nodes in the selection process, increasing the communication and computational overhead. The performance is also affected adversely as communication packet sizes increase in large scale WSNs.

The above mentioned cluster header selection schemes is only appropriate for one-hop network model (where all sensor nodes are directly connected with the cluster head), while in [53], a new Multi-parameter Group Leader Selection scheme (MGLS) is proposed for Multi-hop WSNs, which using four different weighting factors to select a new group leader: available energy at each sensor node, number of neighbor nodes, a node's distance from the current group leader and its trust value. Sensor nodes with the highest weighted and combined factor value will be selected as the new group leader node. Moreover, the scheme only involves a few sensor nodes in the new group leader selection process, which helps to reduce the overall cost. Simulation results shown this scheme increases group lifetime and performs well in multi-hop network models and smaller/larger groups. However, in the process of selection, one node will be ruled out as a future group leader if its trust value is less then the threshold value, whatever how much the values of other three factors are. This means that the scheme cannot detect malicious nodes sending false information (energy, the number of neighbor nodes, trust, etc.). Furthermore, the exact details of the trust mechanism are not considered.

6. Security resiliency of trust models

Trust is always used to detect malicious nodes and improve network security. For example, if a selfish node does not participate in communication, its trust value will be degraded in the trust models. Therefore, this selfish node can be

Table 5
Security resiliency of trust models.

Trust models	DoS attack	Bad mouthing attack	On–off attack	Conflicting behavior attack	Sybil attack	Replication attack	Attack on information	Collusion attack
RFSN [9]	×	✓	×	×	×	×	×	✓
PLUS [10]	×	×	✓	×	×	×	×	×
NBBTE [14]	×	×	✓	×	×	×	×	×
ATSN [15]	×	✓	✓	✓	×	×	×	✓
TTSN [17]	×	✓	✓	✓	×	×	×	✓
DFDI [20]	✓	✓	×	✓	✓	✓	✓	×
DFR [22]	×	×	×	×	×	×	✓	×
MDLC [23]	×	×	×	×	×	×	✓	×
TMCDE [24]	✓	×	×	×	×	×	✓	×
GTMS [39,40]	×	✓	×	×	✓	✓	✓	✓
HTCW [41]	×	×	×	×	✓	✓	×	×
TMBBT [42]	×	✓	×	✓	×	×	✓	×

detected by its trust value. However, trust computations models can be attractive target for attackers. In this section, we identify some possible attacks for the trust models in WSNs and analyze their security resiliency with respect to the attack modes. Based on the analysis, some design practices for trust models are discussed.

6.1. Malicious attacks against trust models

In this section, the possible attacks against the trust models can be classified into eight categories: DoS attack, bad mouthing attack, on–off attack, conflicting behavior attack, Sybil attack, replication attack, attack on information and collusion attack. A comparison of trust computation methods with respect to the malicious attack models is provided in Table 5, where ✓ denotes successful handling and × denotes unsuccessful handling.

- DoS attack: In DoS attack, malicious nodes send misleading information, e.g., misleading recommendations, as much as possible to consume large amount of computing resources. Therefore, DoS attack can be successfully handled in the trust model with power-aware, e.g., TMCDE [24] and DFDI [20]. However, the rest of the trust methods based on event reports can be affected by DoS attack.
- Bad mouthing attack: In this attack model, malicious nodes intentionally give dishonest recommendation for neighbor nodes, even if the neighbor nodes are normal ones. Thus, recommendations under bad mouthing attack cannot reflect the real opinion of the recommender. The trust models based on recommendations can be attacked by bad mouthing attack. Therefore, RFSN scheme [9] which only propagates good reputation information about other nodes can efficiently resist against bad mouthing attack. In addition, the trust methods which based on direct neighbor sensing (e.g., ATSN [15] and TTSN [17]) or aggregations of multiple observations (e.g., DFDI [20] and TMBBT [42]) can handle bad mouthing attack very well.
- On–off attack: In this type of attacks, malicious nodes can opportunistically behave good or bad. Thus, malicious nodes can remain trusted while behaving badly. To handle the on–off attack, the observation made long time ago should not carry the same weight as that of recent one. Therefore, On–off attack can be successfully defended by the trust methods using a forgetting factor (e.g., ATSN [15]), in which the observation made long time ago carry smaller weight than that of recent one. In addition, on–off attack can be handled by the trust methods which only use current observation to calculate sensor nodes' trust (e.g., PLUS [10], NBBTE [14] and TTSN [17]).
- Conflicting behavior attack: In this attack, malicious nodes behave differently towards different nodes. For example, malicious nodes can give good recommendations about node A to node B, and give bad recommendation about node A to node C. This way, the conflicting recommendations about the node A can confuse the trust model to evaluate trustworthiness of node A. For the same reasons as that of bad mouthing attack, conflicting behavior attack can be handled by the trust methods which based on direct neighbor sensing (e.g., ATSN [15] and TTSN [17]) or aggregations of multiple observations (e.g., DFDI [20] and TMBBT [42]).
- Sybil attack: In Sybil attack, malicious nodes can create several fake IDs, then emulate or impersonate different nodes in the network. The Sybil nodes can manipulate the recommendations and promote themselves as trust nodes. Therefore, Sybil attack can be successfully handled by ID identification (e.g., DFDI [20]) or centralized trust methods (e.g., GTMS [39,40]), in which the base station can detect the fake identities.
- Replication attack: If an adversary manages to capture a node and extract the authentication/encryption keys, it can produce a large number of replicas having the same identity (ID) from the captured node and integrate them into the WSN at chosen locations, which is called the node replication attack. Since the credentials of replicas are all the clones from the captured nodes, the replicas can be considered as legitimate members of the network [54]. Similar with malicious nodes under Sybil attack, malicious nodes under replication attack can also manipulate the recommendations

and promote themselves as trust nodes. Therefore, replication attack can also be handled by the ID identification (e.g., DFDI [20]) and centralized trust methods (e.g., GTMS [39,40]), in which the base station can detect the clone nodes.
- Attack on information: Malicious node can forge, alter, flood or selectively forwarding information. Therefore, the trust models based on communication behaviors may obtain false information, thus the evaluated trustworthiness becomes untrusted. All the data trust models, GTMS [39,40] and TMBBT [42] can handle attack on information well because they can detect packet forwarding and data integrity efficiently.
- Collusion attack: Collusion attacks are engendered by more than one malicious node collaborating and giving false recommendations about normal nodes. Collusion attacks are much more destructive than above mentioned attack models which implemented by one malicious node. Trust models based on direct observation of each node (e.g., RFSN [9], ATSN [15], TTSN [17] and GTMS [39,40]) are not prone to collusion attacks. All other trust computation methods suffer significantly by collusion attacks.

6.2. Basic trust best practices

Based on above analyses, we conclude that in order to improve robustness of trust models, the following set of trust best practices needed to be considered:

- Trust models of WSNs should be as simple as possible, i.e. without constraints on software, hardware, memory usage, computing, processing speed, communication bandwidth, and detect the different attacks easily, and update trust relations accordingly. Especially, energy efficiency should be considered.
- In trust models, trust and reputation should be evaluated at the same time, since reputation is a node's opinion of other nodes in the network. Trust can be defined as the mathematical representation of reputation. Therefore, trust is a derivation of the reputation of an entity. Compare to calculating trust directly, using reputation to calculated trust can get a reliable trust value.
- Trust models of WSNs should calculate direct trust and indirect trust separately. Direct trust is calculated based on First-Hand Information, while indirect trust is calculated based on Second-Hand Information or recommendations from neighbor nodes. Only calculating direct or indirect trust in not sufficient enough for trust evaluation.
- Trust models based on only one type of feedback are insufficient. The trust models based on previous positive feedbacks only can be cheated in a way that, colluded sensors send good reports for each other. Thus, positive and negative feedbacks should be taken into account at the same time.
- In WSNs, sensor nodes are always responsible for several tasks. Therefore, trust models should consider designing different trust computation methods for different tasks.
- Trust models are designed to improve network security. However, when trust models defend against malicious nodes, they may also be attacked by adversaries. Therefore, in order to improve the robustness of trust models, the related malicious attacked models which have been discussed in Section 6.1 should be taken into account.

7. Conclusions

Trust management scheme consist a powerful tool for the detection of unexpected node behaviors (either faulty or malicious). Once misbehaving nodes are detected, their neighbors can use trust information to avoid cooperating with them either for data forwarding, data aggregation or any other cooperative function. In this paper, the details of trust models and their applications are analyzed. Based on the above discussion, we can conclude that:

- In above trust management mechanisms, evaluation of node trust is based on the past behavior evidence or the recommendations from neighbor nodes. How to predict future node trust based on past node trust is ignored.
- In WSNs, all nodes share common sensing tasks. This implies that not all sensors are needed to calculate trustworthiness during the whole system lifetime. Choosing some nodes does not affect the overall trust management system. Therefore, if we can schedule sensors to work alternatively, the system lifetime can be prolonged.
- Most existing trust mechanism is entity-centric, while WSNs are data-centric networks. How to efficiently evaluate trustworthiness of data is still a problem.
- In order to improve accuracy of trust value, more trust metrics can be considered, such as, transmission range/radio range, packet loss, energy consumption, ling latency, path quality, hop count and so on.
- To defeat attacks against WSNs, several secure protocols based on trust management mechanisms were proposed in the literatures. However, these protocols introduce some heavy communication or computation overheads, and provide a limited resilience against malicious attacks, e.g., DoS attack, Sybil attack, and collusion attack.
- Some trust management mechanisms are suspicious in practice, where the predefined threshold parameter may deviate significantly from the practical situation.
- Most trust management mechanisms evaluate trustworthiness based on interactions among sensor nodes while pay little attention to privacy preserving in the computation of trust value.
- In the future, trust models can be extended into other type of WSNs with new environment, e.g., heterogeneous WSNs, spare WSNs, dynamic WSNs, and WSNs with duty-cycle and so on.

Acknowledgments

The work is supported by "the Applied Basic Research Program of Changzhou Science and Technology Bureau, No. CJ20120028", "the Scientific Research Foundation for the Returned Overseas Chinese Scholars, State Education Ministry" and "the Innovative Research Program for Graduates of Hohai Univ., No. CGB014-09".

References

[1] H. Chan, A. Perrig, Security and privacy in sensor networks, IEEE Computer 36 (10) (2003) 103–105.
[2] Y.M. Huang, M.Y. Hsieh, H.C. Chao, S.H. Hung, J.H. Park, Pervasive, secure access to a hierarchical-based healthcare monitoring architecture in wireless heterogeneous sensor networks, IEEE Journal on Selected Areas of Communications 27 (4) (2009) 400–411.
[3] C.F. Lai, Y.M. Huang, J.H. Park, H.C. Chao, Adaptive body posture analysis using collaborative multi-sensors for elderly falling detection, IEEE Intelligent Systems 25 (2) (March/April 2010) 20–30.
[4] C.F. Lai, S.Y. Chang, H.C. Chao, Y.M. Huang, Detection of cognitive injured body region using multiple triaxial accelerometers for elderly falling, IEEE Sensors Journal 11 (3) (2011) 763–770.
[5] M. Gupta, P. Judge, M. Ammar, A reputation system for peer-to peer networks, in: Proceedings of the 13th International Workshop on Network and Operating Systems Support for Digital Audio and Video, 2003, pp. 144–152.
[6] S.D. Kamvar, M.T. Schlosser, H. GarciaMolina, The eigentrust algorithm for reputation management in P2P networks, in: Proceedings of the 12th International Conference on World Wide Web, 2003, pp. 640–651.
[7] Z. Liu, A.W. Joy, R.A. Thompson, A dynamic trust model for mobile ad hoc networks, in: Proceedings of the 10th IEEE International Workshop on Future Trends of Distributed Computing Systems, 2004, pp. 80–85.
[8] A.A. Pirzada, C. McDonald, Establishing trust in pure ad-hoc networks, in: Proceeding of 27th Australasian Computer Science Conference, Dunedin, New Zealand, 2004, pp. 47–54.
[9] S. Ganeriwal, L.K. Balzano, M.B. Srivastava, Reputation-based framework for high integrity sensor networks, in: Proceedings of the 2nd ACM Workshop on Security of ad hoc and Sensor Networks, 2004, pp. 66–77.
[10] Z. Yao, D. Kim, Y. Doh, PLUS: Parameterized and localized trust management scheme for sensor networks security, in: IEEE International Conference on Mobile ad-hoc and Sensor Systems, MASS, 2008, pp. 437–446.
[11] A. Boukerch, L. Xu, K. EL-Khatib, Trust-based security for wireless ad hoc and sensor networks, Computer Communications (2007) 2413–2427.
[12] X. Chen, K. Makki, K. Yen, N. Pissinou, Sensor network security: A survey, IEEE Communications Surveys & Tutorials 11 (2) (2009) 52–73.
[13] T.K. Kim, H.S. Seo, A trust model using fuzzy logic in wireless sensor network, in: Proceedings of World Academy of Science Engineering and Technology, 2008, pp. 63–66.
[14] R. Feng, X. Xu, X. Zhou, J. Wan, A trust evaluation algorithm for wireless sensor networks based on node behaviors and D–S evidence theory, Sensors (2011) 1345–1360.
[15] H. Chen, H. Wu, X. Zhou, C. Gao, Agent-based trust model in wireless sensor networks, in: 8th ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing, 2007, pp. 119–124.
[16] H. Chen, G. Gu, H. Wu, C. Gao, Reputation and trust mathematical approach for wireless sensor networks, International Journal of Multimedia and Ubiquitous Engineering 2 (3) (2007) 23–32.
[17] H. Chen, Task-based trust management for wireless sensor networks, International Journal of Security and Its Applications 3 (2) (2009) 21–26.
[18] F. Ye, H. Luo, L. Zhang, Statistical en-route filtering of injected false data in sensor networks, in: Proceedings of INFOCOM, 2004, pp. 839–850.
[19] X. Zhou, L. Tang, Design and evaluation of blacklist aided false data filtering scheme for wireless sensor networks, Master degree thesis, Peking University, 2007.
[20] J. Hur, Y. Lee, H. Yoon, D. Choi, S. Jin, Trust evaluation model for wireless sensor networks, in: The 7th International Conference on Advanced Communication Technology, 2005, pp. 491–496.
[21] N. Sastry, U. Shankar, D. Wagner, Secure verification of location claims, in: Proceedings of the 2nd ACM Workshop on Wireless Security, 2003, pp. 1–10.
[22] X. Xiao, W.C. Peng, C.C. Hung, W.C. Lee, Using sensorranks for in-network detection of faulty readings in wireless sensor networks, in: Proceedings of the 6th ACM International Workshop on Data Engineering for Wireless and Mobile Access, 2007, pp. 1–8.
[23] L. Gomez, A. Laube, A. Sorniotti, Trustworthiness assessment of wireless sensor data for business applications, in: Proceedings of the 2009 International Conference on Advanced Information Networking and Applications, 2009, pp. 355–362.
[24] H. Dong, Y. Guo, Z. Yu, H. Chen, A wireless sensor networks based on multi-angle trust of node, in: Proceedings of the 2009 International Forum on Information Technology and Applications, 2009, pp. 28–31.
[25] H. Deng, X. Sun, B. Wang, Y. Cao, Selective forwarding attack detection using watermark in WSNs, in: 2009 ISECS International Colloquium on Computing, Communication, Control, and Management, 2009, pp. 109–113.
[26] J. Konorski, R. Orlikowski, Data-centric Dempster–Shafer theory-based selfishness thwarting via trust evaluation in MANETs and WSNs, in: Proceedings of the 3rd International Conference on New Technologies, Mobility and Security, 2009, pp. 74–78.
[27] K. Liu, N. Abu-Ghazaleh, K.D. Kang, Location verification and trust management for resilient geographic routing, Journal of Parallel and Distributed Computing 67 (2) (2007) 215–228.
[28] I. Maarouf, U. Baroudi, A.R. Naseer, Efficient monitoring approach for reputation system-based trust-aware routing in wireless sensor networks, IET Communications 3 (5) (2009) 846–858.
[29] N. Lewis, N. Foukia, An efficient reputation-based routing mechanism for wireless sensor networks: Testing the impact of mobility and hostile nodes, in: Sixth Annual Conference on Privacy, Security and Trust, 2008, pp. 151–155.
[30] H. Deng, Y. Yang, G. Jin, R. Xu, W. Shi, Building a trust-aware dynamic routing solution for wireless sensor networks, in: IEEE Globecom 2010 Workshop on Heterogeneous, Multi-Hop Wireless and Mobile Networks, 2010, pp. 153–157.
[31] H.A. Rahhal, I.A. Ali, S. Shaheen, A novel trust-based cross-layer model for wireless sensor networks, in: 28th National Radio Science Conference, NRSC, 2011, pp. 1–10.
[32] N. Poolsappasit, S. Madria, A secure data aggregation based trust management approach for dealing with untrustworthy motes in sensor network, in: 2011 International Conference on Parallel Processing, 2011, pp. 138–147.
[33] A. Srinivasan, J. Teitelbaum, J. Wu, DRBTS: Distributed reputation-based beacon trust system, in: 2nd IEEE International Symposium on Dependable, Autonomic and Secure Computing, 2006, pp. 277–283.
[34] T. Zhang, J. He, Y. Zhang, Trust based secure localization in wireless sensor networks, in: 2nd International Symposium on Intelligence Information Processing and Trusted Computing, IPTC, 2011, pp. 55–58.
[35] X. Xu, H. Jiang, L. Huang, H. Xu, M. Xiao, A reputation-based revising scheme for localization in wireless sensor networks, in: IEEE Wireless Communications and Networking Conference, WCNC, 2010, pp. 1–6.

[36] G. Han, D. Choi, T.V. Nguyen, A reliable sensor selection algorithm for wireless sensor networks, in: 3rd IEEE/IFIP International Conference in Central Asia on Internet, 2007, pp. 1–4.
[37] G. Han, D. Choi, W. Lim, A novel sensor node selection method based on trust for wireless sensor networks, in: International Conference on Wireless Communications, Networking and Mobile Computing, 2007, pp. 2397–2400.
[38] M.Y. Hsieh, Y.M. Huang, H.C. Chao, Adaptive security design with malicious node detection in cluster-based sensor networks, Computer Communications 30 (11–12) (2007) 2385–2400.
[39] R.A. Shaikh, H. Jameel, S. Lee, S. Rajput, Y.J. Song, Trust management problem in distributed wireless sensor networks, in: 12th IEEE International Conference on Embedded and Real-Time Computing Systems and Applications, 2006, pp. 411–414.
[40] R.A. Shaikh, H. Jameel, B.J. d'Auriol, H. Lee, S. Lee, Y.J. Song, Group-based trust management scheme for clustered wireless sensor networks, IEEE Transactions on Parallel and Distributed Systems 20 (11) (2009) 1698–1712.
[41] Y. Zhou, T. Huang, W. Wang, A trust establishment scheme for cluster-based sensor networks, in: 5th International Conference on Wireless Communications, Networking and Mobile Computing, 2009, pp. 1–4.
[42] Z. Liu, Z. Zhang, S. Liu, Y. Ke, J. Chen, A trust model based on Bayes theorem in WSNs, in: 7th International Conference on Wireless Communications, Networking and Mobile Computing, WiCOM, 2011, pp. 1–4.
[43] I.M. Atakli, H. Hu, Y. Chen, W.S. Ku, Z. Su, Malicious node detection in wireless sensor networks using weighted trust evaluation, in: Proceedings of the 2008 Spring Simulation Multiconference, 2008, pp. 836–843.
[44] F. Song, B. Zhao, Trust-based LEACH protocol for wireless sensor networks, in: 2nd International Conference on Future Generation Communication and Networking, 2008, pp. 202–207.
[45] S. Sinha, Z. Chaczko, T-SNIPER trust-aware sensor network information protocol for efficient routing, in: IEEE 24th International Conference on Advanced Information Networking and Applications Workshops, 2010, pp. 686–691.
[46] J. Wang, L. Li, Z. Chen, A routing algorithm based on trustworthy core tree for WSN, in: IEEE/IFIP 8th International Conference on Embedded and Ubiquitous Computing, EUC, 2010, pp. 763–770.
[47] W. Zhang, S.K. Das, Y. Liu, A trust based framework for secure data aggregation in wireless sensor networks, in: 3rd Annual IEEE Communications Society on Sensor and ad hoc Communications and Networks, 2006, pp. 60–69.
[48] C. Bekara, M. Laurent-Maknavicius, K. Bekara, SAPC: A secure aggregation protocol for cluster-based wireless sensor networks, in: Proceedings of the 3rd International Conference on Mobile ad-hoc and Sensor Networks, 2007, pp. 784–798.
[49] M. Zhou, J. Xu, C. Zhu, A secure data aggregation algorithm based on behavior trust in wireless sensor networks, in: 5th IEEE International Symposium on Embedded Computing, 2008, pp. 61–66.
[50] Y. Ni, L. Tian, X. Shen, The research of dynamic data fusion based-on node behavior trust for WSNs, in: International Conference on Computer Design and Applications, ICCDA, 2010, pp. 534–538.
[51] B. Stelte, A. Matheus, Secure trust reputation with multi-criteria decision making for wireless sensor networks data aggregation, Sensors (2011) 920–923.
[52] G.V. Crosby, N. Pissinou, J. Gadze, A framework for trust-based cluster head election in wireless sensor networks, in: 2nd IEEE Workshop on Dependability and Security in Sensor Networks and Systems, 2006, pp. 1–10.
[53] K. Kifayat, M. Merabti, Q. Shi, D. Llewellyn-Jones, An efficient multi-parameter group leader selection scheme for wireless sensor networks, in: International Conference on Network and Service Security, 2009, pp. 1–5.
[54] C. Yu, C. Lu, S. Kuo, Efficient and distributed detection of node replication attacks in mobile sensor networks, in: Proceedings of Vehicular Technology Conference Fall, VTC Fall, 2009, pp. 1–5.