IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received November 17, 2017, accepted December 15, 2017, date of publication December 27, 2017,
date of current version February 28, 2018.

Digital Object Identifier 10.1109/ACCESS.2017.2786944

A Comprehensive Trust-Aware Routing Protocol With Multi-Attributes for WSNs

BOYUAN SUN AND DONGHUI LI
School of Electrical and Information Engineering, Tianjin University, Tianjin 300072, China
Corresponding author: Boyuan Sun (pierrotnebura@tju.edu.cn)

This work was supported by the National Natural Science Foundation of China under Grant 61403274.

ABSTRACT Due to the impact of an open deployment environment, severe restrictions in power with poor hardware equipment, and a lack of centralized administration in management, wireless sensor networks (WSNs) are extremely vulnerable to malicious attacks aimed at routing and other aspects. To face this problem, we propose a novel trust-aware routing protocol for WSNs which incorporates multiattributes (TRPM) of sensor nodes in terms of communication, data, energy, and recommendation. The proposed trust model relies on an improved sliding time window considering attack frequency to facilitate the discovery of malicious behaviors of attackers. Combined with effective routing detection and maintenance protocol, the performance of our solution is tested through a wide set of simulation experiments. Extensive results reveal that an average packet transfer rate of TRPM is increased by about 19% and time consumption on the routing update is shortened by about 11% in case 20% of all sensor nodes are malicious compared with other existing trust-based routing protocols.

INDEX TERMS Malicious attacks, routing security, trust management mechanism, wireless sensor networks.

I. INTRODUCTION

With the rapid development of wireless communication technology, researchers have already placed a high degree of emphasis on wireless sensor networks (WSNs), which become one part of the core next-generation application field and are widely used in industry, environmental monitoring, military, and many other domains [1]–[4]. However, the capacity-constraint features of sensor nodes caused by limitation of energy, radius of communication and storage make WSNs extremely susceptible to malicious attackers aiming at disturbing the normal function of the whole network. In this case, techniques including cryptography-authentication mechanism and intrusion detection [4]–[7] are proposed by related researchers to enhance network security, but such conventional approaches are insufficient to tackle with attacks from nodes captured by adversaries.

To protect WSNs from potential attacks and distinguish trustable nodes from compromised ones, researchers introduced trust management mechanism into WSNs [8], [9]. Trust-aware models, which are firstly proposed in electronic commence to identify reliable participants, are more efficient to detect compromised nodes in network, because the evaluation of node trust is linked with past behaviors of suspicious node and the recommendation data from trustworthy neighbor ones. Based upon such rational, trust-based routing strategies are proposed to further enhance network security. The prime consideration during the design phase of related strategies is how to select optimal intermediate nodes of secure routing in light of trust values. Moreover, to get access to routes with better quality, some trust-aware models even add factors including energy cost [10], [11], distances from neighbors to sink node [12], [13] or number of hops [14], [15] into secure routing evaluation.

Nevertheless, the current trust-aware routing protocols still have a lot to be promoted [16], [17]. Among such issues, we focus on the following shortcomings:

1) In related research work, some models [18], [19] take factors like data and energy as references in trust evaluation process, but most of them ignore recommendation as a direct criterion for the trust value. In that case, compromised nodes, which collude with each other or opt to be selfish, will not be punished.
2) Increasingly intelligent compromised nodes are likely to combine mutable intensity and frequency of attacks with different strategies to weaken the reliability and validity of security mechanisms of WSNs. In fact, most

trust-based routing protocols in [20] and [21] neglect such threat, even though defense ability of proposed models against attacks with single strategy is verified.

3) In case established secure routing is attacked or even disabled by adversaries, some existing studies [22], [23] provide routing maintenance and update mechanisms to re-establish new routes. However, such routing models do not make an analysis on potential reasons for current routing failure, which might restrain the efficiency of update process.

In this paper, we propose a comprehensive Trust-aware Routing Protocol considering Multi-attributes of sensor nodes (TRPM) in terms of communication, data, energy, and recommendation for WSNs and make innovative contributions in the following aspects:

1) In TRPM, recommendations derived from evaluated nodes are considered to strengthen the robustness of trustworthiness evaluation. In this view, participation in recommending process and accuracy of provided recommendation data are regarded as direct references for trust value assessment.
2) We enrich TRPM with a fixed-width sliding time window model considering attack frequency of malicious nodes. Following this approach, attack frequency of malicious node is defined as the proportion of time units recording obvious abnormal behaviors to the total number of time units.
3) As regards the decrease of one or more intermediate nodes' trust values in optimal route, TRPM is capable of adjusting current route by adopting two attack avoidance strategies with the help of warning messages from trustworthy intermediate nodes and periodic feedback from sink node.

The rest of the paper is organized as follows: Section II reviews some related work. Section III gives a brief description of different malicious attacks appearing in trust-based secure routing and discusses the resistance of some comprehensive models against such attacks. Section IV proposes our TRPM in detail. Section V presents various simulation scenarios designed to compare the performance of TRPM with that of other models and analysis of simulation results are also given in this section. Last but not least, conclusion and further research issues are proposed in Section VI.

II. RELATED WORK

As a significant and complex concept borrowed from social relationship, trust, which includes assumption, assessment, expectation, feedback, and many other factors, is widely used in peer-to-peer and self-organizing networks. According to Josang's definition [24] in 1996, trustworthiness of individual arises from benign performance and absence of malicious behavior, while trustworthiness of entirety is based upon resistance against malicious attacks. With the increasing popularity of trust management mechanism among researches of WSNs, some literature further improve the network by proposing secure routing models based on trust. Actually, in terms of their focus, such models are broadly divided into two categories. One is to offer the network a higher level of comprehensive security; the other is to tackle some kinds of special attacks existing in network.

As far as we know, Lewis and Foukia [25] proposed the first trust-aware secure routing model in WSNs. In the literature, authors mainly discussed the approach to make the optimal routing selection based on routing trust values and data transmission cost in case there were multiple trustworthy routes between source node and sink node. Authors put forward an excellent method to optimize secure routing selection. However, as network threats have become increasingly complex, the proposed model seems too simplistic to establish trustworthy routing nowadays.

A non-deterministic secure routing protocol based on time-space redundancy and continuous adaptation of WSN was proposed by Moya *et al.* [26]. The trust value was calculated by using time-space continuous change of data detected by evaluated node, while sink node computed the reputation value by comparing the collected information transmitted from evaluated node and neighbor nodes. Authors also adopted cluster structure with multiple software agents to further enhance the performance of security model. However, the requirement of network layout is difficult to fulfill, since the proposed model builds upon the assumption that a sufficient number of bone nodes with high-level hardware are deployed in advance.

Based on the energy-effective routing protocol LEACH, a trust-based secure routing model named LEACH-TM was presented [27]. Network applied with LEACH-TM established a relatively reliable cluster structure according to trust statues and residual energy of nodes during the setup phase. Instead of gaining trustworthiness of routing via multiplying trust values of nodes, source node selected the best route by calculating the average trust in LEACH-TM. The adoption of such computing method reduce the difficulty of gathering and processing trust information to a certain extent, but in the case of malicious nodes colluding with each other, authors neglect relevant issues, which results in the vulnerability of LEACH-TM to such kind of threat. It is worth stressing that malicious cluster head with low trust value is restricted in data transmission, which means that the probability of the optimal neighbor cluster head forwarding packets from malicious one is greatly reduced. However, such punishment has no effect on attackers issuing conflicting behavior attack.

Compared with the above-mentioned models employed to improve the overall security of network, some researches make worthwhile contributions to enhance network robustness against certain types of attacks. Zhan *et al.* [28] studied security threats derived from wormhole attack and sinkhole attack, which focus on misleading normal nodes. Meanwhile, they proposed a secure routing model that was able to avoid such negative factors and built up effective data link between source node and base station. Intermediate nodes employed energy observer and trust manager to evaluate energy consumption and trustworthiness of neighbor nodes, and then

picked out the best next-hop node. Furthermore, base station sent feedback with sequence number of received and unreceived packets periodically to assist source node in updating current route. However, source node tended to treat the closest forwarding node as a compromised one and completely abandoned the current route on condition that malicious node appeared in established route and invalidated the function of data transmission. As a result, malicious node cannot be accurately detected and circumvented, while potential routes and reliable neighbors are also discarded.

Ahmed *et al.* [29] further classified untrustworthy intermediate nodes into two categories. One was error node that launched grey hole attack passively and the other was malicious node that launched black hole attack actively. Despite difference detection methods adopted to implement the identification of two types of untrustworthy nodes in the proposed TERP, similar to the model presented by Ahmed *et al.* [20], TERP was still built upon the idea that there was no collusion between malicious nodes, which was inconsistent with actual situation in real deployment. Besides, authors supposed that it was not allowed to add or to remove sensor nodes after the network was established. Such assumption also limits the application of TERP to some extent.

Liu *et al.* [30] proposed an energy-efficient secure routing model based on active trust, which performed well on black hole attacker detection. Authors proved that the model could reduce energy consumption of nodes and extend network lifetime. However, such model only considers how to resist black hole attack during the process of trust assessment, which makes it have no defense against other attacks.

Different from trust-based routing models only effective on coping with specific attacks, a number of comprehensive routing models are presented to further enhance the security of data transmission for WSNs. Compared with aforementioned related work, such models are greatly improved to shield against attacks targeting secure routing and trust management.

Zahariadis *et al.* [21] proposed ambient trust sensor routing solution (ATSR) combined with geographical routing scheme. Although the protocol contributed to taking multiple factors like energy and data into trust evaluation, it was built upon the premise that all sensor nodes fully understood their precise location and had the capacity of judging the accuracy of location data from neighbor nodes, which was a great test of sensor nodes under the condition of limited hardware resources. Moreover, with the wide application of cluster head election mechanism, the alteration of cluster head becomes a salient factor of WSNs, thus the way of rapidly finding out neighbor node closest to cluster head obstructs the practical application of ATSR. For this reason, we refine the performance of TRPM by improving calculation method and revising routing protocol reasonably instead of referring to the location information of source and sink node in routing establishment.

Trust prediction and trust-based source routing (TSR) was proposed by Xia *et al.* [22]. In TSR, each node only took packet accuracy rate as evaluation criterion when it computed the trust value of neighbor node. However, compared with most trust-based routing protocols, TSR ignores recommendations from third-party nodes throughout the calculation process of trustworthiness. Moreover, the task of selecting the optimal route is completely executed by sink node in TSR. The adoption of such strategy seriously consumes the residual energy of sink node, which shortens network lifetime to a certain extent.

To establish a trust model that had the capacity of tackling diverse malicious attacks against trust management and routing protocol, Duan *et al.* [23] proposed trust-aware security routing framework (TSRF). In this scheme, authors analyzed different attacks appearing in trust-based routing, put forward specific trust deviation method, and built up secure routing referring to network QoS requirements. Despite the validity of above steps in security enhancement, authors miss the protection mechanism of node energy. Meanwhile, the deficiency in recommendation framework also risks trust evaluation process.

Jiang *et al.* [18] contributed to reforming trust management model by proposing an efficient distributed trust model (EDTM), which took the factors including communication, data, and energy into account simultaneously. The multi-hop indirect trust calculation method in EDTM promotes the accuracy of trustworthy routing selection, but the literature focuses on only constructing robust trust model, which leads to a lack of relevant research on approaches of assessing trustworthiness of routes.

Trust sensing-based secure routing mechanism (TSSRM) derived from TSRF added energy consumption and mobility of sensor node into trust value calculation process [19]. Compared with TSRF, TSSRM has better defense performance against networks threats like energy-targeting attack and on-off attack, but it is short of a deeper consideration of trust management, which results in model's vulnerability to collusion and selfish attack.

It's evident that the trust evaluation approach directly affects the quality of secure routes between source node and sink node in WSNs. Underestimating the significance and comprehensiveness of trust assessment may bring the route unavoidable blind spots under different attack strategies from malicious nodes. To this end, it is necessary to propose a robust and thorough model to cope with existing threats.

III. ANALYSIS OF MALICIOUS ATTACKS

In this section, we analyze the potential malicious attacks and attack modes in trust-based routing for WSNs. Following such analysis, we compare defense abilities of some comprehensive secure routing model against all types of attacks. In general, common attacks in WSNs are distinguished in attacks aimed at routing and trust management. Here we attempt to explain and study two types of attacks respectively.

As one of the main concerns of researchers, routing protocols are designed to solve the problem of how to implement effective and accurate data transmission. In most cases,

TABLE 1. Performances of Trust-based models against various malicious attacks.

	Attacks Targeting Routing					Attacks Targeting Trust Management				
	Black hole	Grey hole	Sinkhole	Tamper	Energy draining	On-off	Conflicting behavior	Unfair rating	Collusion	Selfish
ATSR	√	√	×	√	√	√	×	√	×	√
TSR	√	√	√	√	×	×	×			
TSRF	√	√	√	√	×	√	√	√	×	×
EDTM	×	×	×	√	√	√	√	√	×	×
TSSRM	√	√	√	√	√	√	√	√	×	×

conventional routing protocol researches are based upon the assumption that all sensor nodes are credible and the network is free of attack, hence such routing models may not be adapted to the requirement of network security. In this view, enhancing routing security is an importance prerequisite for normal network function. Here malicious attacks for routing are classified as follows:

1) Black hole attack: Malicious node denies to participating in data transmission tasks and discards all packets it receives.
2) Grey hole attack: Malicious node selectively forwards the packets it receives and abandons remains.
3) Tamper attack: Malicious node tampers with contents of the packet before forwarding it.
4) Energy draining attack: Captured node wastes the energy of sensor node by sending invalid packets.
5) Sinkhole attack: Captured node attracts traffic in network by broadcasting wrong routing information.
6) Eavesdropping attack: Malicious node intercepts and steals information transmitted over a network.
7) Sybil attack: A single malicious node forgeries multiple virtual identities simultaneously.

As described in [6], routing-targeting attacks ranging from 1) to 5) cannot be effectively detected in WSNs only adopting encryption and authentication mechanisms in the sense that such attackers stem from the inner network, hence trust management mechanism is proposed to cancel the functionality of attackers via evaluating their trustworthiness. It is worth mentioning that eavesdropping attack and Sybil attack can be avoided through the assistance from received signal strength indicator [31], so these two attacks will not be discussed in this paper. Additionally, WSNs also have to face another kind of attacks aimed at trust model, thus effective countermeasures to enhance the robustness of trust evaluation process becomes a current research hotpot. The trust-targeting attacks are classified as followed:

1) On-off attack: Compromised node alternately behaves normally and maliciously while maintaining its credibility at a high level by concentrated attacks.
2) Conflicting behavior attack: Malicious node behaves differently with different neighbor nodes, which affects trust recommendation process of others.
3) Unfair rating attack: In case malicious node serves as a recommender, it offers recommendations that are not consistent with the real trust level of evaluated node. As regards malicious attackers providing negative (positive) recommendations of normal (compromised) node, they are referred to as black-mouthing (ballot-stuffing) attackers.
4) Collusion attack: Malicious nodes work in collusion to impair the trust evaluation function of nodes.
5) Selfish attack: Selfish node denies to transmitting recommendation response to the requesters.

Based upon aforementioned two groups of malicious attacks on routing and trust, we compare the defense capability of comprehensive secure routing models mentioned in Section II through Table 1. It is worth stressing that five models can cope with most attacks from malicious nodes, especially tamper attack and unfair rating attack (except TSR [22] without adoption of third-party recommendations). Meanwhile, five models are defective with their own security problems, especially in dealing with collusion attack and selfish attack. With the increasing complication of deployment environment, many intelligent attackers even adjust attack frequency to avoid detection of network security mechanism. In terms of the above-mentioned issues, we describe the detailed functions of our TRPM in the sequel.

IV. TRUST-AWARE ROUTING PROTOCOL WITH MULTI-ATTRIBUTES

A. NETWORK MODEL

In this paper, we suggest that the cluster structure is adopted to divide sensor nodes into clusters based upon their distance and adjacent relationship during the setup phase of network. Meanwhile, optimal nodes with enough energy are elected as cluster head, which are mainly responsible for processing and fusion of data collected from nodes within the same cluster. Since cluster head has a higher energy consumption rate than normal nodes in cluster, many researches on cluster head election laid a higher emphasis on residual energy over other factors to prolong the lifetime of network [32]. Therefore, we suggest that secure routing has to be re-established based on the most recent trust evaluation results and cluster information after a round of cluster head election.

During trust value evaluation process, we use ''subject node'' to represent the evaluating node and ''object node'' to represent the evaluated node for the convenience

of expression. Meanwhile, Watchdog mechanism is employed to monitor the communication behaviors of object node, where subject node temporarily stores the forwarding packets in the buffer and turns on promiscuous mode to perform a real-time analysis on received data from object node. Based upon the result of analysis, subject node defines the trustworthiness of all its one-hop distance neighbors. After finishing trust evaluation, source node establishes a real-time update route to sink node by sending routing detection packet. In this process, source node or intermediate node picks out the most trustworthy next-hop neighbor and continuously monitors the behaviors of neighbor nodes. Based on monitoring results, trust values of nodes are updated and the route is adjusted in time. Fig. 1 shows the work flow of sensor node in routing establishment. In the following design, we carry out the implementation approaches of TRPM. First, the quantification process of three main trust components–direct trust, indirect trust, and total trust—are detailed as follows.

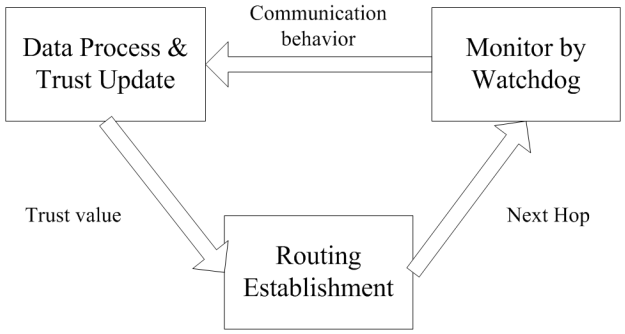


FIGURE 1. Work flow of sensor nodes in routing establishment.

B. DIRECT TRUST

In contrast with other trust management models, subject node evaluates communication, data, energy, and recommendation such four attributes of object node respectively in direct trust computation of TRPM. In most cases, sensor nodes cooperate with each other and perform timely detection of events happened in surrounding areas. Hence communication trust often works as the primary indicator of whether object node is trustworthy or not in related work [33]. Due to the fact that communication trust can only defend against part of the attacks, some malicious behaviors that interfere with the normal function of network by forging tampered data or shorten the lifetime of nodes by rapidly depleting residual energy are not able to be discovered accurately. Under such circumstances, it's necessary to introduce data and energy attributes into trust management models. Besides, a number of compromised nodes attempt to affect the operation of trust evaluation by undermining the recommendation process. In fact, if recommendation attribute is not regarded as a factor of direct trust computation, intelligent attacker may continuously launch unfair rating attack without any effect on its trust value. Therefore, it's critical to evaluate degree of participation in recommending and authenticity of recommendation data to ensure the accuracy of direct trust calculation of object node. To enhance the perception of attackers with different attack frequency, we introduce a sliding time window with attack frequency measurement function to assist subject node in analyzing direct trust condition in each time interval, examining the persistent malicious behavior, and adjusting trustworthiness of object node.

1) COMMUNICATION TRUST ASSESSMENT

Communication trust is the most basic factor to examine the credibility of object node in trust evaluation. In order to detect black hole attack and grey hole attack by communication trust, we adopt two communication trust metrics as follows:

Packet received feedback: When subject node sends a routing probe or packet forwarding request to object node, subject node waits for a response message from object node. If a feedback is received within a limited time interval, it will be counted as a successful communication interaction, otherwise counted as a failure.

Packet forwarding: When subject node receives a feedback from object node, subject node enters the promiscuous mode to monitor the communication behaviors of object node by Watchdog mechanism. If the certain packet from subject node is forwarded on time, it will be counted as a successful communication interaction, otherwise counted as a failure.

Since communication trust predicts whether object node will behave normally or not in the future and the process of trust calculation should be simple enough to save node energy. Here in this paper, the expectation of Beta distribution is adopted to compute communication trust:

$$CT^{i,j} = \frac{SCT^{i,j} + 1}{\left(SCT^{i,j} + 1\right) + \left(UCT^{i,j} + 1\right)} \tag{1}$$

where $CT^{i,j}$ represents the communication trust of subject node i to object node j, while $SCT^{i,j}$ and $UCT^{i,j}$ denote the total numbers of successful and unsuccessful communication interactions between i and j via communication trust metrics respectively.

2) DATA TRUST ASSESSMENT

Attacks aimed at data security of WSNs can be roughly divided into two categories. In one kind of attacks, compromised node forges data packets whose contents are largely or totally different from the fact to influence the judgment of sink node on the deployment environment. The other kind is that malicious node partially or completely replaces received packets before forwarding them to bring about tamper attack. Based upon above-mentioned issues, two data trust metrics are proposed as follows:

Perceived data accuracy: When subject node receives packet forwarding request from object node serving as source node, subject node compares data detected by object node with data collected by itself (assume that

the two nodes have the same perceived data type). If the variation between two data packets is smaller than a certain threshold σ, it will be counted as a successful data interaction, otherwise counted as a failure.

Packet accuracy: When subject node sends a routing probe or packet forwarding request to object node, subject node stores the message in its buffer and then enables the promiscuous mode. After object node forwards the corresponding packet, subject node makes comparison between the intercepted data from object node and the data in buffer. If two data packets are consistent with each other, it will be counted as a successful data interaction, otherwise counted as a failure.

Based on such two trust metrics, data trust is computed by employing Beta distribution:

$$DT^{i,j} = \frac{SDT^{i,j} + 1}{\left(SDT^{i,j} + 1\right) + \left(UDT^{i,j} + 1\right)} \tag{2}$$

where $DT^{i,j}$ represents the data trust of i to j, while $SDT^{i,j}$ and $UDT^{i,j}$ denote the total numbers of successful and unsuccessful data interactions between i and j via data trust metrics respectively.

3) ENERGY TRUST ASSESSMENT

As one of the most important characteristics in WSNs, energy directly determines the service life of network. Meanwhile, energy consumption can also identify whether a suspicious node launches malicious attack against energy security or not. Therefore, two energy trust metrics are employed as follows:

Residual energy ratio: When object node transmits data packets to subject node, the residual energy ratio of object node re^t is added to the packets. In case subject node discovers that the residual power of object node is lower than a certain threshold ε [18], object node will be treated as an invalidate node which is not able to participate in normal data transmission any more. Thus its energy trust value will be set to 0.

Energy consumption rate variation: Object node transmits its current energy consumption rate along with residual energy information periodically. Due to the fact that the locations of sensor nodes in network and the number of neighbor nodes vary widely, energy consumption rates of different nodes are not exactly the same. Since some researches see energy consumption rate as the criterion of energy trustworthiness evaluation [13], [19], here we utilize the energy consumption rate variation equation $\Delta p = \left|p^t - p^{t-1}\right| / p^{t-1}$ to detect abnormal conditions. If Δp exceeds a certain threshold υ, subject node determines that object node behaves abnormally and sets the energy trust of object node to 0.

Therefore, the energy trust value of object node is expressed as:

$$ET^{i,j} = \begin{cases} re^t\,(1 - \Delta p) & re^t \geq \varepsilon \&\& \Delta p \leq \upsilon \\ 0 & re^t < \varepsilon \,||\, \Delta p > \upsilon \end{cases} \tag{3}$$

where $ET^{i,j}$ represents the energy trust of i to j. In fact, there is no effective inspection mechanism to judge the accuracy of energy information provided by object node in TRPM. However, if malicious node falsely reports its residual energy or energy consumption rate to maintain its energy trust, the node may be selected by more neighbor nodes as a trustworthy next-hop node. In other words, the malicious node has to undertake more data-relay tasks under the condition of insufficient energy or anomalous energy consumption, which will certainly bring about a rapid drop of communication or data trustworthiness due to hardware or energy constrains. As a result, such misleading behavior may increase the probability of being detected. Following this logic, here we suggest that malicious node would report energy information truthfully. In subsequent simulation scenarios, we are about to verify the assumption by experiment results.

4) RECOMMENDATION TRUST ASSESSMENT

Recommendation from third-party node, which is an important factor to assist trust evaluation process, often becomes the main target of some malicious attacks like unfair rating attack. When assessing recommendation data, models in some researches adopt negative strategies where subject node removes suspicious recommendations largely deviated from integrated data. Such approach enhances the validity of indirect trust to a certain extent, but there is no further punishment for potential attackers. To deal with the above-mentioned problems, TRPM introduces the following two recommendation trust metrics to effectively compute recommendation trust:

Response of recommendation request: When subject node sends a recommendation request for a common neighbor to object node, subject node checks whether a response message of the recommendation request from the same object node is received within a limited time interval. If it is true, it will be counted as a successful recommending participation; otherwise counted as a failure.

Recommendation accuracy: If subject node receives recommendation data from object node which serves as a recommender, it compares the recommendation data with the direct trust of recommended neighbor node. If the difference between two kinds of data is lower than a certain threshold φ, it will be counted as a successful recommending participation; otherwise counted as a failure.

According to such two metrics, recommendation trust of object node is shown as:

$$RT^{i,j} = \frac{SRT^{i,j} + 1}{\left(SRT^{i,j} + 1\right) + \left(URT^{i,j} + 1\right)} \tag{4}$$

where $RT^{i,j}$ represents the recommendation trust of i to j, while $SRT^{i,j}$ and $URT^{i,j}$ denote the total numbers of successful and unsuccessful recommending participation via recommendation trust metrics respectively.

5) DIRECT TRUST VALUE COMPUTATION

Before the calculation of direct trust, it is worth stressing that the sliding time window considering attack frequency is employed in TRPM. Fig. 2 shows an example of the time window created by subject node. The entire sliding time window has four rows in terms of four trust attributes of object node corresponding to communication, data, energy, and recommendation. Meanwhile, each row is composed of multiple time units, which records a direct trust value of specific attribute at a moment. After one time interval Δ elapses, the time window slides to the right, adds the current trust data into an empty time unit and drops the oldest one. In order to effectively detect on-off attack that may exist in a certain length L of the sliding time window t_k, the concept of malicious behavior weight is adopted to compare the data in each time unit. Here communication malicious behavior weight wct^{t_k} is expressed as:

$$wct^{t_k} = \max[\alpha_1(1 - CT^{i,j}_{t=1}), \alpha_2(1 - CT^{i,j}_{t=2}), \ldots, \alpha_m(1 - CT^{i,j}_{t=m}), \alpha_L(1 - CT^{i,j}_{t=L})] \quad (5)$$

In the equation, decay factor α ranging from 0 to 1 is used to assign higher emphasis on current data over past records. Moreover, α satisfies the requirement of $\alpha_1 < \ldots < \alpha_m < \ldots < \alpha_L$ and may be calculated by equation $\alpha = \Phi^{L-m}$ $(0 < \Phi < 1)$. Following this approach, subject node is able to discover malicious attacks in time window by checking wct^{t_k}. Here we take the recommendation rows of sliding windows t_3 and t_4 in Fig. 2 as an example. In case Φ is equal to 0.9 [19], malicious behavior weights of recommendation in two time windows are 0.3645 and 0.55 respectively, thus it is obvious that recommendation-targeting attacks in t_4 are more serious.

If malicious node takes a sustained but non-obvious attack strategy so that malicious behavior weight is maintained at a low level, it's evidently inadequate to tackle such intelligent threat by only (5). Hence the attack frequency detection mechanism is required to help subject node i identify whether object node j is an on-off attacker via data recorded in time unit m. Take communication time unit m_c as an example:

$$m_c = \begin{cases} normal & if\ CT^{i,j}_{t=m} < \zeta_c \\ abnormal & otherwise \end{cases} \quad (6)$$

In (6), if communication trust value is lower than a specific threshold ζ_c, then m_c is considered as a normal time unit which is not affected by malicious attacks, otherwise m_c is abnormal. After examining states of all the time units, attack frequency in sliding window of communication is evaluated based upon the following equation:

$$cf^{t_k} = \frac{ce^{t_k}}{ce^{t_k} + cn^{t_k}} \quad (7)$$

where ce^{t_k} and cn^{t_k} represents the total numbers of normal and abnormal time units respectively. Once again

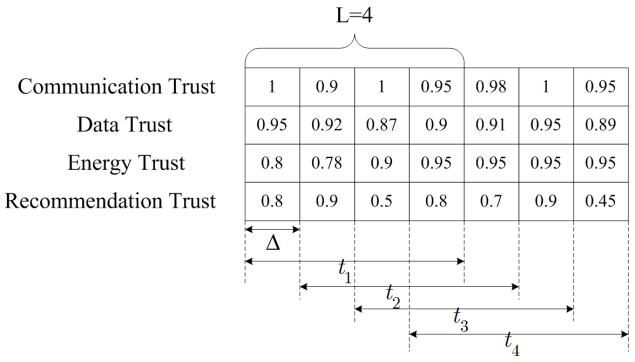


FIGURE 2. An example of sliding trust window.

we take the sliding windows t_3 and t_4 of recommendation trust in Fig. 2 as an example. In case $\zeta_r = 0.8$, recommendation-targeting attack frequencies in t_3 and t_4 are equal to 0.75, which indicates that the object node is indeed an unfair rater.

By measuring malicious attack weight and attack frequency in sliding window t_k, sliding trust of object node is calculated in the following formula (e.g. communication sliding trust $SCT^{i,j}$):

$$SCT^{i,j} = \begin{cases} 1 - wct^{t_k} & if\ wct^{t_k} > cf^{t_k} \\ \beta\left(1 - wct^{t_k}\right) + (1-\beta)\left(1 - cf^{t_k}\right) & otherwise \end{cases} \quad (8)$$

where wct^{t_k} and cf^{t_k} are summed up adopting parameter β as weight, while such parameter ranges from 0.5 to 1 [34]. As shown in (8), in case malicious behaviors of object node are obvious ($wct^{t_k} > cf^{t_k}$), only malicious behavior weight is employed in sliding trust computation; if suspicious object node tends to issue high-frequency and low-intensity attack ($wct^{t_k} \leq cf^{t_k}$), malicious behavior weight and attack frequency are combined in a weighted sum to calculate sliding trust. Following this process, the communication, data, energy, and recommendation sliding trust of object node $SCT^{i,j}$, $SDT^{i,j}$, $SET^{i,j}$, and $SRT^{i,j}$ can be measured by analyzing trust data in time windows of corresponding node attributes. Finally, direct trust of object node is described as:

$$Td^{i,j} = \omega_1 SCT^{i,j} + \omega_2 SDT^{i,j} + \omega_3 SET^{i,j} + \omega_4 SRT^{i,j} \quad if\ \min\left\{SCT^{i,j}, SDT^{i,j}, SET^{i,j}, SRT^{i,j}\right\} \geq \eta \quad (9)$$

where ω_1, ω_2, ω_3, and ω_4 stand for weights of four node attributes in direct trust calculation and all weight sum up to 1 so direct trust ranges from 1 to 0. By default, the weights are assigned with same value to emphasize the necessity of each node attribute in trustworthiness assessment. In fact, these weights may be varied according to applications' requirement [20]. Parameter η is used to judge whether four types of sliding trusts are reliable or not. In case one or more of the sliding trust values are lower than η, the object node will be directly identified as a malicious one and direct trust will be set as 0 [22].

C. INDIRECT TRUST COMPUTATION

In order to cover the shortages in direct trust, trust-based routing models proposed in related work mostly employ recommendation data from neighbor nodes as indirect trust. As can be seen from Table 1, most models are unable to deal with all malicious attack aimed at trust management mechanism, thus TRPM here is presented to make full use of recommendation data and to ensure network security under complex environment by observing the following three principles:

1) Considering unfair rating attack and collusion attack, recommendation data should be filtered before further application in indirect trust calculation. Meanwhile, recommendations from unreliable neighbors need to be compared with direct trust value of object node for the purpose of shielding against potential conflicting behavior attack.
2) Recommendation trust from direct trust affects the confidence of recommendation data in indirect trust calculation, so the filtered recommendation data should be further weighted via trust chain.
3) The adoption of indirect trust is relied upon the fact that direct trust is not sufficient enough to evaluate trust value of object node accurately. In other words, if the credibility of direct trust increases over time, the weight of indirect trust in total trust should decrease towards 0.

Based upon such principles, normal recommender set $G^{i,j}$, which represents one-hop neighbors of object and subject node, send direct trust evaluation result of j to i as recommendations. When i receives recommendation from $G^{i,j}$, it is necessary to evaluate the credibility of all the recommendation data. Here we adopt divergence detection degree $DC^{i,j}$ to analyze such recommendation data:

$$DC^{i,j} = \frac{\sum_{z \in G^{i,j}} Td^{z,j} + \lambda Td^{i,j}}{\left|G^{i,j}\right| + \lambda} \tag{10}$$

where z denotes a node in $G^{i,j}$, while parameter λ is used to vary the weight of direct trust in divergence detection degree. In case $\left|DC^{i,j} - Td^{z,j}\right| > \gamma$, the difference between recommendation and detection degree is too large to accept, otherwise the recommendation data will be treated as one of the indirect trust elements. Parameter γ as divergence detection threshold should be predetermined in light of the network condition [21].

For the filtered recommendation data, indirect trust $Ti^{i,j}$ of object node is computed by trust chain as follows:

$$Ti^{i,j} = \frac{\sum_{z \in G^{i,j}} Td^{i,z} \times Td^{z,j}}{\left|G^{i,j}\right|} \tag{11}$$

D. TOTAL TRUST COMPUTATION

Combining direct trust and indirect trust, the total trust value of object node can be obtained through the following equation:

$$Tt^{i,j} = C^{i,j} Td^{i,j} + \left(1 - C^{i,j}\right) Ti^{i,j} \tag{12}$$

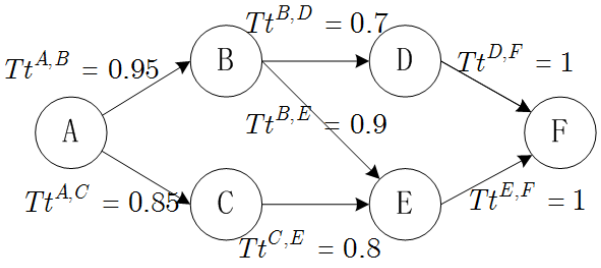


FIGURE 3. Routing trust calculation.

where $C^{i,j}$ stands for the confidence weight of direct trust in total trust, which is calculated based upon following equation:

$$C^{i,j} = \frac{Ni^{i,j}}{Ni^{i,j} + n} \tag{13}$$

where $Ni^{i,j}$ represents the total number of direct interactions, while parameter n is a positive integer, whose value affects the variation rate of $C^{i,j}$. From (12) and (13), it is worth pointing out that the necessity of indirect trust depends entirely on the confidence weight of direct trust. As time wears on, the increasing number of direct interactions between subject and object node brings about the declining proportion of indirect trust in total trust, which enhances network security against recommendation-targeting attacks to some extent.

E. ROUTING TRUST COMPUTATION

After mutual trust evaluation process among sensor nodes in the network, it is necessary to evaluate routing trust based upon trust data of nodes before the establishment of secure routing, which is used to fulfill multi-hop packet transmission from source node to sink node. According to the criterion of routing trust assessment proposed in [35], routing trust value is required to keep lower than the trust value of any intermediate node. Since trust is regarded as a significant factor in quite a few researches on cluster structure of WSNs [36], [37], selected cluster heads are always considered to be reliable enough to aggregate data from nodes in the same cluster. Hence we assume that sink node (cluster head) is completely trustworthy and its trust value evaluated by any neighbor node is equal to 1. Following the assumption, trust value of a certain route *rou* is expressed as:

$$Tp^{rou} = \prod \left(\left\{ Tt^{o,p} | o, p \in rou, o \to p \right\} \right) \tag{14}$$

where p is the next-hop node of o in *rou*. Here we attempt to analyze specific secure routing cases according to an example of partial network proposed in Fig. 3. It's evident that there are three available routes from source node A to sink node F, while the trust values of such routes are $Tp^{A,B,D,F} = 0.665$, $Tp^{A,B,E,F} = 0.855$, and $Tp^{A,C,E,F} = 0.68$ respectively. Therefore, route $A \to B \to E \to F$ is selected as the optimal one with highest routing trust value.

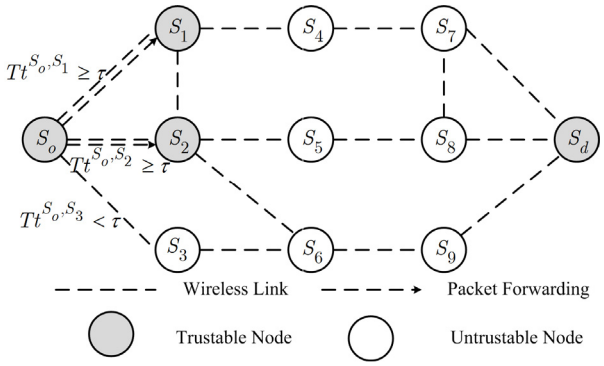


FIGURE 4. Step 1 of secure routing establishment.

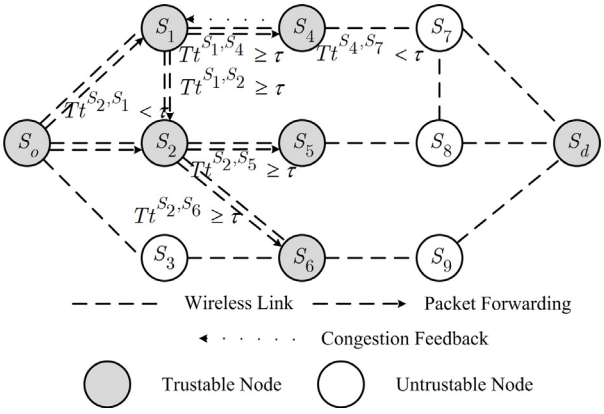


FIGURE 5. Step 2 of secure routing establishment.

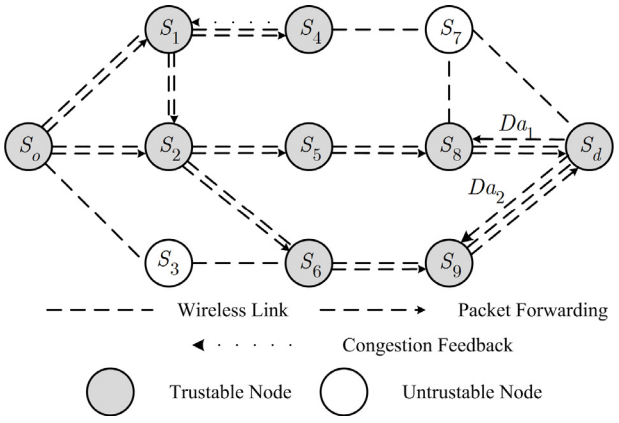


FIGURE 6. Step 3 of secure routing establishment.

F. STRATEGY FOR SECURE ROUTING ESTABLISHMENT

After the network completes the process of cluster division, cluster head election, and cluster head identification broadcasting, a highly effective and self-adjusting routing establishing model is required to discover the optimal route between two nodes. Fig. 4 to Fig. 7 represent an example of partial network used to show the basic steps of secure routing detection in TRPM after cluster head election process, which is expressed as follows:

1) Source node S_o, which is usually manifested as a sensor node in cluster, makes real-time analysis on the trust values of neighbor nodes. If the trust value of a neighbor is less than a threshold τ [23], the node will be identified as an untrustworthy node, otherwise it will be regarded as a trustworthy one and receive a routing detection packet unicasted by S_o. The structure of such packet is:

$$Dr = \langle pid, id_o, id_d, id_t, id_r, \tau, ts, hc \rangle \qquad (15)$$

where pid represents id of the packet, while id_o, id_d, id_t, and id_r denote the node id of source node, sink node, forwarding node, and next-hop node respectively. ts stands for time stamp, while parameter hc, which represents the number of times the packet has been forwarded, is set to be a certain positive integer. As the packet is forwarded once, hc is reduced by 1. In case $hc = 0$, the routing detection packet is no longer forwarded to the next-hop node. As shown in Fig. 4, S_1 and S_2 receives detection packets from S_o since their trust values exceeds τ, while S_3 is judged as an untrustworthy node based upon the evaluation results.

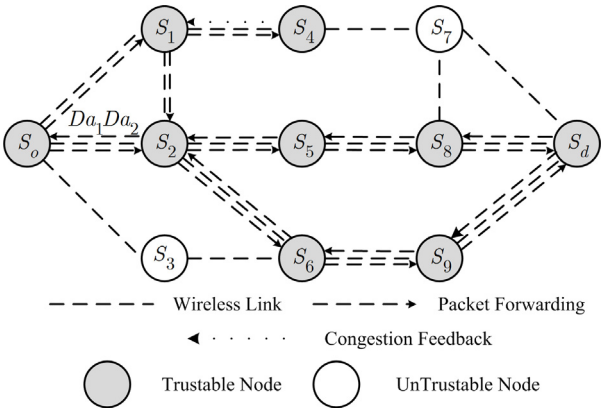


FIGURE 7. Step 4 of secure routing establishment.

2) When receiving routing detection packet from source node, intermediate node timely responses to it for the purpose of maintaining its trust value, and then filter neighbor nodes through τ recorded in the packet. Similar to the procedure in Step 1, intermediate node picks out trustworthy neighbors and inform them about the routing detection mission via modulating id_t and id_r in the packet. It is important to note that routing loop, which appears during packet delivery process, may seriously affect the efficiency of routing detection. To avoid such issue, sensor node employed with TRPM compares the id of current packet with the id list of packets received before. If the packet is obtained for the first time, it will be forwarded to next-hop node after the packet id is recorded, otherwise the packet will be discarded directly. Additionally, in case an intermediate node finds that there is no trustworthy neighbor after receiving routing detection packet, it will notify previous hop of the situation. Then previous hop attempts to transmit the packet to other trustworthy node within its

communication range. As shown in Fig. 5, S_1 and S_2 continue to forward probe request to their neighbors. Meanwhile, S_2 receives the same detection packet once again from S_1, which causes the loop of $S_o \rightarrow S_1 \rightarrow S_2$. As a result, S_2 drops the request immediately. Since S_4 finds that its only neighbor S_7 is not trustworthy enough, S_4 gives timely feedback depended upon such circumstance to S_1.

3) Intermediate node receiving routing detection request keeps looking for trustworthy next-hop node as described in Step 2 until the routing packet is forwarded to S_d. Sink node S_d, which is usually manifested as cluster head, generates a response message Da immediately after receiving request from S_o and transmit it to the previous hop. The structure of receipt is as follows:

$$Da = \langle pid, id_d, id_o, ts \rangle \tag{16}$$

After obtaining the message, intermediate node appends its id and the trust value of previous-hop node to the end of the message. According to the id of detection packet recorded in Da, the intermediate node then figures out the next hop by checking its neighbor table and unicasts Da to that node. The step is described in Fig. 6.

4) The response message is transmitted successively and trust values of intermediate nodes are added to the message hop by hop as described in Step 3. After S_o acquires the response from S_d, it calculates the trust value of current route via the approach proposed in last section. Since there might be some secure routes between S_o and S_d, route with the highest trust value is selected to accomplish data transmission, whereas route with second highest trust value is treated as alternative stored in S_o. When there are two or more secure routes with same trust value, the one with least number of hops is considered to be more trustworthy in TRPM. As shown in Fig. 7, S_o receives response message Da_1 and Da_2 corresponding to routes $S_o \rightarrow S_2 \rightarrow S_5 \rightarrow S_8 \rightarrow S_d$ and $S_o \rightarrow S_2 \rightarrow S_6 \rightarrow S_9 \rightarrow S_d$, then one will be selected as optimal route and the other as alternate route.

Following the above-mentioned steps, source node transmits the perceived data to sink node after the establishment of optimal route. In fact, source node maintains the normal operation of the same route in addition to two cases. The first one is the variation of cluster head based on cluster structure mechanism, which means source node is required to detect new route in the light of the latest situation of network. The other one is that current secure route is under the threat of malicious attacks, and the countermeasures on such problem will be presented in following part.

G. SECURE ROUTING MAINTENANCE

In case trust value of secure routing drops quickly due to the impact from malicious attacks, an effective routing maintenance approach should be carried out to promote routing defense against attackers. Following such principle, we propose the secure routing maintenance mechanism of TRPM to update route with potential threats in time.

In fact, reasons for the reduction of routing trust value is roughly distinguished in following two categories: (1) Trust value of an intermediate node in security routing decreases to trust threshold τ. (2) Trust values of multiple intermediate nodes in secure routing drop at the same time, which leads to a decline in the total trust of secure routing. Since the second case is much more difficult to figure out the id of malicious nodes and attackers are more likely to collude with each other compared with the first case, two cases are tackled by different strategies in TRPM.

When an intermediate node in secure routing discovers that its next hop node is untrustworthy, it reports immediately to source node. After receiving the warning, source node first checks the alternate route created during routing detection process. Since malicious node may intentionally slander a normal node, alternate route without reporting node and suspicious node will be directly used to replace current route. If the alternate route contains such two nodes, source node stops data transmission and repeats secure routing detection process based upon aforementioned four steps.

To shield against second type of threat, sink node periodically reports the summary information of received packets to source node throughout validity period of current route. In case source node finds that the number of data received by sink node is significantly less than number of data sent by itself or it does not receive a report from sink node exceeding predefined time limit, malicious nodes which drop forwarding packets or response messages deliberately may exist in network. Hence source node resends secure routing detection packet to neighbors to establish new route.

Here we take Fig. 7 as an example to illustrate the detailed process of secure routing maintenance. Assume that there are secure route $S_o \rightarrow S_2 \rightarrow S_5 \rightarrow S_8 \rightarrow S_d$ and $S_o \rightarrow S_2 \rightarrow S_6 \rightarrow S_9 \rightarrow S_d$ between source node and sink node, which meets the condition of $Tp^{o,2,5,8,d} > Tp^{o,2,6,9,d}$. After secure routing is established, source node transmits the data packets through optimal route, while intermediate nodes update the trust value of next-hop nodes based upon interaction results. In case trust value of S_8 evaluated by S_5 is lower than trust threshold, S_o will directly switch the current route $S_o \rightarrow S_2 \rightarrow S_5 \rightarrow S_8 \rightarrow S_d$ to $S_o \rightarrow S_2 \rightarrow S_6 \rightarrow S_9 \rightarrow S_d$ after receiving a trust reduction warning from S_5. Similarly, if S_o doesn't obtain feedback messages from sink node S_d for a period of time or the content of feedback is seriously inconsistent with the data sent by S_o, source node immediately sends routing probe request to trustworthy neighbors and strives to reestablish another secure route.

V. SIMULATION EXPERIMENTS AND MODEL PERFORMANCE EVALUATION

In this section, we adopt NS-2 as simulation platform to test the performance of TRPM. Combined with various types of malicious attacks given in Section III, several sets of

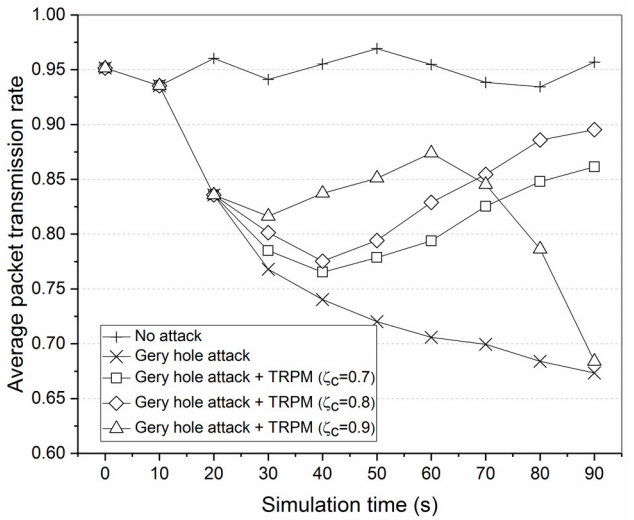


FIGURE 8. A comparison of communication trust selection.

simulation scenarios are proposed to draw a comparison between TRPM and other comprehensive trust-based routing models. The resistance of models against 4 types of malicious attacks aimed at node attributes is tested in the first 4 scenario sets. Collusion between compromised nodes and conflicting behavior launched by single attacker may affect trust mechanism corporately, thus we carry out the 5th scenario to analyze such threat. Then we introduce on-off attacker with mutable attack frequency into simulation environment to conduct a check on validity of sliding time window. Effectiveness of models in harsh and complex environment with a variety of potential attacks is proved in the 7th experiment. Furthermore, we also test the relative performance of TRPM against other trust-based secure routing models in terms of network throughout, average end-to-end latency, routing overhead and network lifetime. At last, the self-maintenance ability of TRPM is evaluated after current route turns to be untrustworthy. In addition, it is worth pointing out that WSNs are under the threat from sinkhole attack from Table 1. Compared with some trust-based routing models in references, the number of hops is regarded as a criterion for evaluating the priority of secure routing if and only if the trust values of two routes are equivalent in TRPM. Thus, sinkhole attackers, which attract routing to themselves via forged number of hops towards sink node, does not work in our proposed model. Here we abandon sinkhole attack testing in the following simulation scenarios. All related parameter and network settings are recorded in Table 2. Among such list, the default values of some parameters like ε, Φ, β, γ *and* τ derives from corresponding references, while the value selection of other parameters will be analyzed in the following simulation scenarios.

As mentioned earlier, trust threshold ζ is adopted to keep track of malicious behaviors of suspicious node in TRPM. As a significant factor, it is necessary to figure out the influence of ζ variation on network detection performance. Here we take communication trust ζ_c as an example and Fig. 8 shows the trend of average packet transmission rate of

TABLE 2. Experiment parameters.

Parameter	Value
Simulation time	$500s$
Monitoring area	$200m \times 200m$
Number of sensor nodes	100
Proportion of malicious nodes	20%
Deployment of sensor nodes	$random$
Physical propagation model	$two-ray\ ground\ reflection$
MAC layer protocol	$IEEE\ 802.14.4$
Transport layer protocol	UDP
Cluster structure	$LDTS$ [39]
Communication range	$50m$
Length of packet	$100bytes$
Local storage	$50KB$
Initial energy	$25J$
Δ	$10s$
L	4
$\sigma, \upsilon, \varphi$	0.1, 0.3, 0.1
ε	0.3
Φ	0.9
$\zeta_c, \zeta_e, \zeta_d, \zeta_r$	0.8, 0.9, 0.6, 0.8
β	0.3
$\omega_1, \omega_2, \omega_3, \omega_4$	0.25, 0.25, 0.25, 0.25
η	0.4
γ	0.4
τ	0.7

the entire network in case packet loss rate of grey hole attack is 50%. Due to the unavoidable packet loss issue caused by channel congestion, packet transmission rate maintains at 0.95 if there is no attacker in the network. Meanwhile, transmission rate drops rapidly when malicious nodes start to launch attack. However, source node strives to evade attackers and builds up new route via update strategy in TRPM, thus transmission rate returns to a higher level compared with network without any routing protection. Besides, it is evident that the larger ζ_c is, the better resistance of network is against grey hole attackers. However, in case ζ_c exceeds 0.9, non-malicious packet loss caused by normal node is also regarded as an intentional attack, so false positives reported by source node with inappropriate ζ_c may result in a significant decline in average packet transmission rate. In summary, the selection of communication trust threshold should be grounded in the actual situation of network as well as trust thresholds of data, energy, and recommendation.

The first experiment is proposed to verify that TRPM is able to cope with communication-targeting attacks like black hole attack and grey hole attack. Based upon the assumption that the ratio of black and grey hole attackers in WSNs is 1:1 and the packet loss rate of grey hole attackers ranges from 5% to 50%, the variation of average packet transmission rate of TRPM and other contrast models under such circumstance are described in Fig. 9. Transmission rate of TRPM remains relatively flat in the presence of attackers. As sliding time window plays a key role in the communication trust evaluation, black hole attackers with packet loss rate of 100% are

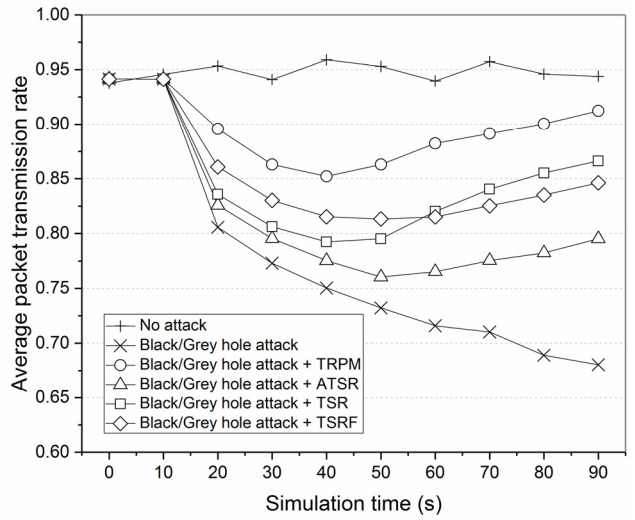


FIGURE 9. Trust-based secure routing models under communication-targeting attacks.

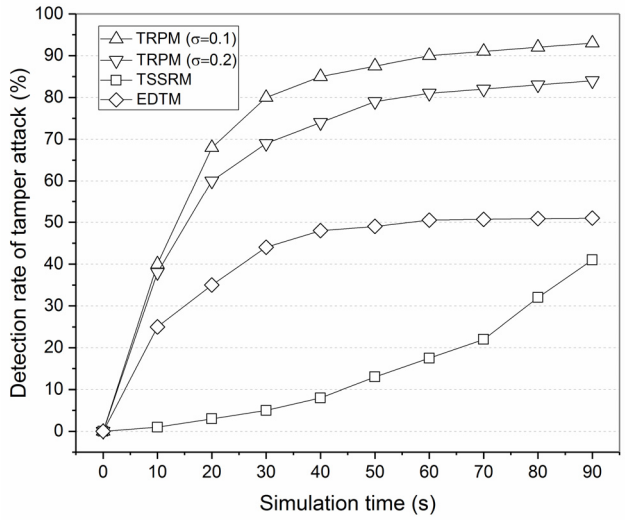


FIGURE 10. Trust-based secure routing models under data-targeting attacks.

quickly removed from secure routing via the detection of the communication trust threshold. In addition, transmission rate starts to rebound after about three time intervals in TRPM, which presents a higher recovery speed of secure routing compared with ATSR, TSR, and TSRF. Finally, when simulation time reaches 90s, average packet transmission rate is stable at about 0.92, which is almost the same as the transmission rate represented in scenario without malicious attacks. Such simulation results show that the good defense performance of TRPM against attacks targeting communication.

Fig. 10 shows the detection capacity of TRPM in network environment continuously threatened by malicious attackers aiming at data security. In this scenario, we assume that the numbers of attackers tampering with received data packets are roughly the same as the numbers of the ones that provide forged sensing information. Simulation results demonstrate that detection rate of attackers rapidly increases and eventually stabilizes at about 80% during the operation of network under the condition of $\sigma = 0.2$. Meanwhile, attack detection rate finally reaches 90% in case $\sigma = 0.1$. However, since the sensing data acquired by neighbor nodes may still be slightly different due to their locations, the threshold selection should not be too extreme in order to prevent the normal nodes from being identified as malicious ones. Hence we choose $\sigma = 0.1$ rather than σ with a smaller value here and the process of selecting other thresholds like υ and φ follows the same principle. Compared with TRPM, networks applied TSSRM and EDTM are only capable of dealing part of the attacks, so it is difficult to maintain data security of network by adopting one of the two models.

To analyze the capability of TRPM dealing with energy-targeting attackers, we assume that malicious nodes in network all launch energy draining attack with the variation of energy consumption rate ranging from 10% to 50% in the third experiment. Meanwhile, residual energy threshold is set to be 0.3 according to [29]. Compromised nodes

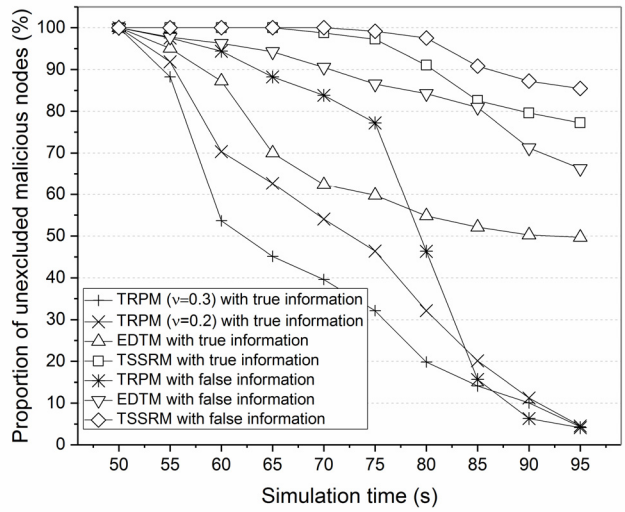


FIGURE 11. Trust-based secure routing models under energy-targeting attacks.

pretending to be normal start to attack when the simulation time approaches 50s. Here we adopt the percentage of malicious nodes that have not been removed from secure routing to compare the processing capacity of TRPM with those of EDTM and TSSRM. As shown in Fig. 11, TRPM with $\nu = 0.2$ can achieve rapid detection of malicious nodes with obvious change in energy consumption rate and more than 90% of attackers are excluded from the secure routing after 95s. TRPM with $\nu = 0.3$, however, is more efficient in removing malicious nodes during the same time intervals. On the contrary, EDTM is not sensitive enough to the frequency of energy-targeting attacks while TSSRM only assesses the residual energy of nodes to filter the malicious ones, thus there is still room for improvement in such two models. Additionally, we carry out another scenario to verify the hypothesis that TRPM is effective in detecting malicious

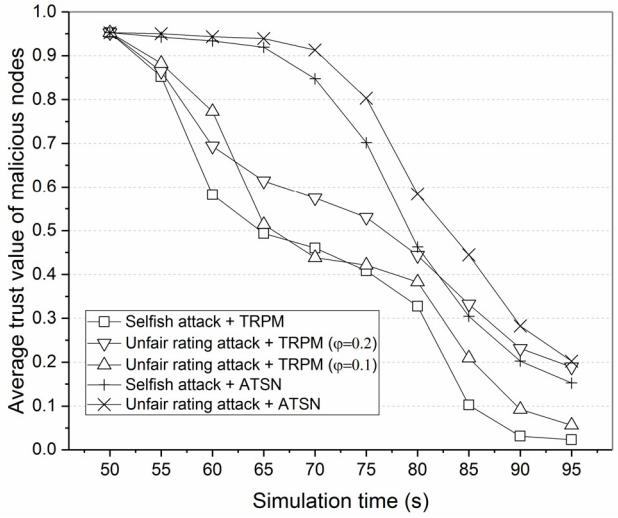


FIGURE 12. Trust-based secure routing models under recommendation-targeting attacks.

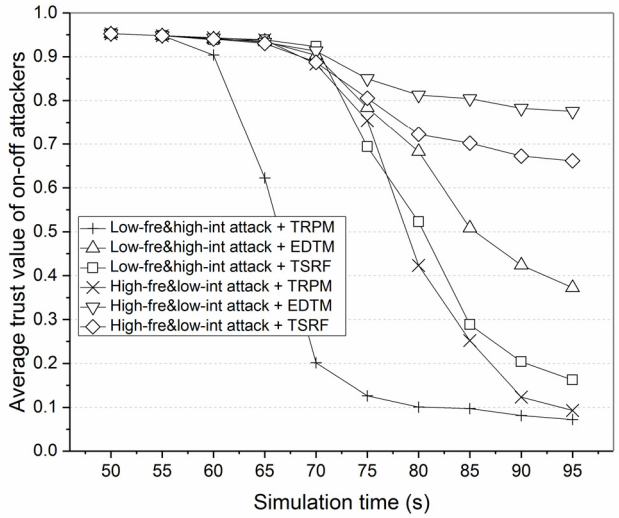


FIGURE 13. Trust-based secure routing models under on-off attack.

nodes with false reports of energy information. As can been seen in Fig. 11, the identification of lying attackers is inferior to that of normal circumstances before simulation time reaches 75s, however, the attacker detection rate then rapidly rises and eventually reaches about 95%. In fact, invalid information sent by energy-draining attackers does have a slight effect on the data exchange process in communication, data or recommendation trust evaluation due to the limitation of nodes' transmission capacity. Such minor abnormalities are recorded in sliding trust window. Meanwhile, attackers will be excluded from network when sufficient evidence is accumulated and the sliding trust of communication, data or recommendation is lower than threshold in TRPM, which validates the accuracy of our proposed hypothesis.

In the fourth experiment, we compare ATSR with TRPM and analyze the performance of our proposed model against recommendation-targeting attacks like unfair rating attack and selfish attack. Assume that attackers in network disguise as normal nodes to maintain trust values at a high level in the first 50s and then start to launch unfair rating attack or selfish attack respectively with proportion of malicious attack varying from 10% to 50%. Meanwhile, the difference between recommendation data provided by unfair rating attackers and the real trustworthiness of object node also varies from 10% to 50%. The experiment results are shown in Fig. 12. As a result of the introduction of the recommendation threshold detection mechanism, TPRM is able to correctly evaluate the trust value of compromised nodes with high proportion of malicious behaviors. Similarly, when simulation time reaches 80s, the sliding time window of subject node accumulates sufficient evidence which effectively identifies attackers with low proportion of malicious behaviors. However, TRPM with $\varphi = 0.1$ is more effective than TRPM with $\varphi = 0.2$ since some unobvious unfair rating attackers are not able to be detected with the threshold set to a relatively large value. Furthermore, through the adoption of both recommendation accuracy check and recommendation threshold, TRPM outperforms ATSR when dealing with attacks aimed at recommendation.

As demonstrated in Fig. 13, in case well-behaved attackers suddenly launch on-off attack, average trust value of all malicious nodes varies according to the applied models. In the fifth scenario, we assume that malicious attackers perform on-off attack threatening communication, data, energy, and recommendation security of normal nodes. Meanwhile, on-off attackers adopt low-frequency & high-intensity (proportion and probability of malicious behaviors equal to 70% and 10% respectively) or high-frequency & low-intensity (proportion and probability of malicious behavior equal to 10% and 70% respectively) such two types of attack strategies. Under such simulation circumstances, when on-off attacker with low frequency and high intensity appears, sliding time window of TRPM is capable of reflecting the intensity of attack so that the average trust value of malicious nodes rapidly drops to a completely untrustworthy level within one time interval (from 60s to 70s). In case compromised nodes launch on-off attack with high frequency and low intensity, attackers are also effectively detected via time sliding window, though it is relatively time-consuming to accurately evaluate the trust values of malicious nodes. Compared with EDTM and TSFR, TRPM would be more suitable for on-off attack detection.

Since WSNs lack fully trusted third-party units, it is important to note that the network is vulnerable to interference from conflicting behavior attack and collusion attack, which are difficult to accurately be identified through trust management mechanism. Hence we adopt parameter λ in (10) to balance their impact. Fig. 14 reflects the relationship between the trust value variations of object node and attacks under different λ. Assume that subject node takes five neighbors as recommenders to evaluate object node trust. In case $\lambda = 25$, normal object node still maintains its trustworthiness at a high

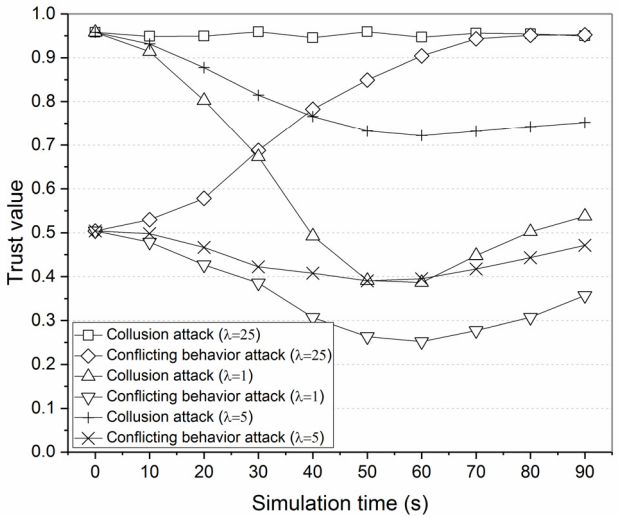


FIGURE 14. A comparison of different λ selection under conflicting behavior and collusion attacks.

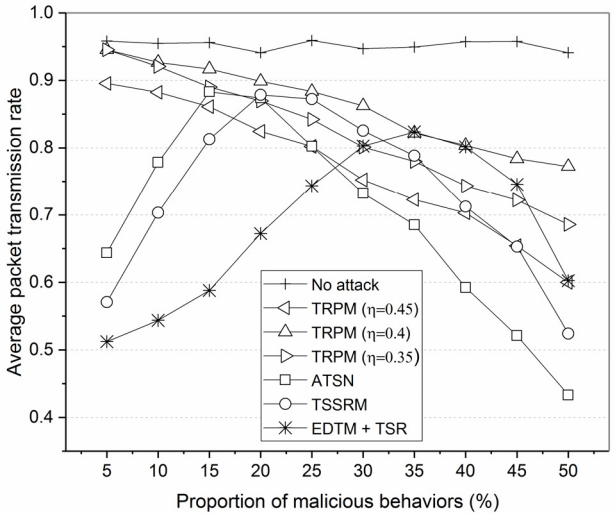


FIGURE 15. Trust-based secure routing models under a combination of multiple malicious attacks.

level, though it is under recommendation-targeting attacks from colluding nodes. Meanwhile, since recommendation data from normal neighbors are nearly completely discarded, the trust value of malicious subject node launching conflicting behavior attack gradually rises. Following this logic, as λ is much larger than the number of recommenders, trust management model has a stronger defense against collusion attack than conflicting behavior attack. In contrast, in case λ is much smaller than the number of recommenders ($\lambda = 1$), TRPM keeps conflicting behavior attacker at untrustworthy level, while it is severely disturbed by collusion attackers. Besides, in case λ is equal to the number of recommenders ($\lambda = 5$), TRPM is capable of coping such two types of attacks to a certain extent, but it is inferior to part of the performance with $\lambda = 25$ and $\lambda = 1$. In summary, the value of λ should be selected based upon the intensity of conflicting behavior attack or collusion attack when applying TRPM.

In the seventh experiment, we propose a combination of aforementioned malicious attacks to simulate the real deployment of WSNs with extremely high security threats. Assume that the probability of the malicious attacks aimed at communication, data, energy, and recommendation are equal to 25%. Meanwhile, attackers are able to influence the normal trust assessment process through collusion, conflicting behavior, and on-off attacks with mutual attack frequency. Fig. 15 reflects the variation of average packet transmission rate with the increase of proportion of malicious behaviors. As can be seen from the figure, TRPM with $\eta = 0.4$ effectively avoids malicious nodes in secure routing even if the proportion of attacks is relatively low via the introduction of sliding time window and attack frequency detection mechanism. Meanwhile, TRPM with $\eta = 0.35$ and $\eta = 0.45$ show low transmission rates compared with $\eta = 0.4$ especially in case that the proportion of malicious behaviors is high. In fact, the reason is that a relatively high time window threshold may misjudge normal nodes as compromised ones while a relatively low time window threshold is not effective enough to detect malicious node accurately. With the proportion of malicious attacks increasing, other contrast models start to show relatively strong resistance against attacks, but in case the proportion rises to 50%, some of the untested malicious nodes launch collusion or conflicting behavior attacks, which result in breakdown of network traffic after secure routing is severely damaged. On the contrary, thanks to the countermeasures presented in TRPM, transmission rate still maintains at a high level. In general, average packet transfer rate of TRPM is increased by nearly 19% compared with TSSRM, which proves that TRPM is secure enough to deal with the combination of multiple attacks in harsh environment.

In addition to the effectiveness of TRPM against various attack combinations, overall performance should also be evaluated to verify the superiority of TRPM over other trust-based routing models like TSR, TSRF and TSSRM. In TSR, after trust evaluation process is finished based upon historical and current interaction information, nodes whose trust values are lower than 0.7 are moved into black list. Then trust values of optional routes between source and sink node are listed in order of priority, from those with smallest hop count to those with highest single-hop trust. Following the principle that the most current data should have the greatest impact on trust, past well-behaved interactions, past malicious behavior and assessment of current behavior constitute trust assessment criteria in TSRF. After avoiding compromised nodes with trustworthiness lower than 0.4, source node adopted TSRF strives to find out the first route to sink node meeting threshold requirements and treat it as the secure routing. Compared with TSRF, TSSRM further employs the remaining energy of sensor node as another criterion to evaluate its reliability.

In this simulation scenario, we adopt four metrics including average throughput, average end-to-end latency, normalized

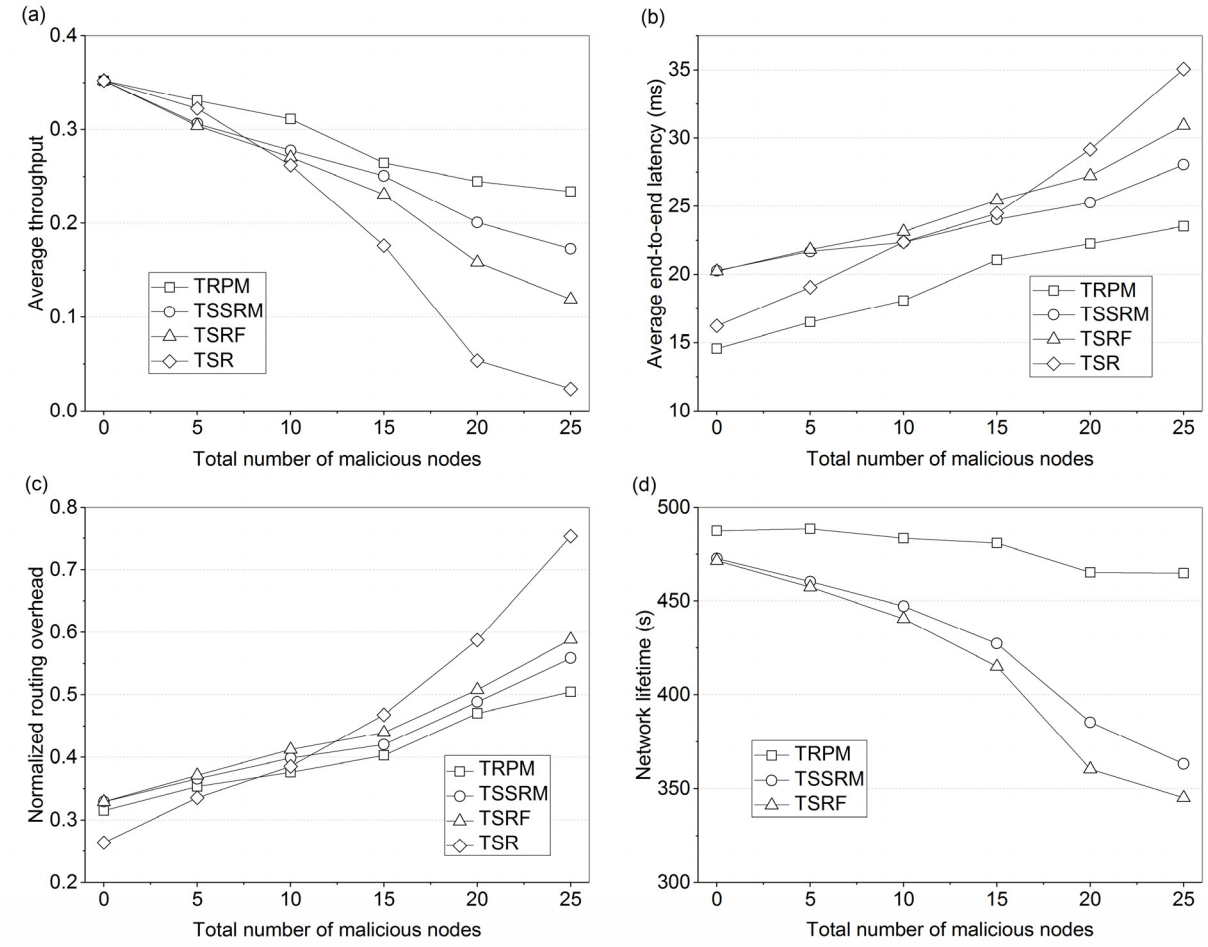


FIGURE 16. Overall performance evaluation under varying number of malicious nodes.

routing overhead and network lifetime to test TRPM in the case of the total number of malicious nodes gradually changing. Among such metrics, throughput represents the average amount of data packets transmitted per second in each secure routing, which indicates the efficiency of network in data collecting and delivering. As shown in Fig. 16(a), average throughputs of models are adjusted to the same level when no malicious node exists in network. Due to the vulnerability of TSR to various attacks shown in Table 1, it represents a rapid decline in average throughput and the model turns to be nearly invalid when number of attackers finally reaches 25. Meanwhile, TRPM outperforms other schemes in throughput metric because of its comprehensive trust evaluation mechanism and proper trust routing detection approach. Besides, both TSSRM and TSRF overlook the penalties for selfish nodes that do not offer recommendation data in a timely manner, therefore throughput is reduced to a certain extent when selfish attack is frequently launched by compromised node in network. Fig. 16(b) represents the simulation results of all schemes in terms of the average time consumed by data packets from source nodes to sink nodes. Along with the increase of malicious nodes, TSSRM tends to have a lower end-to-end latency than TSRF thanks to its resistance against energy draining attack. Even though such two schemes have to rely on some long routes due to the lack of efficient routing selection strategy when there are no attackers in network, they still outperform TSR in case that node collusion combined with various attack means makes it really difficult for models to establish reliable routing. Furthermore, TRPM maintains its advantage over others with the assistance of both robust trust assessment and loop-free routing setup approach. Normalized routing overhead indicates the ratio of the number of control packets to the number of data packets. As shown in Fig. 16(c), routing overhead of TSR is the lowest one among the four schemes in case no compromised node exists, which is attributed to no recommendation exchange is required in TSR. However, the incompleteness of trust evaluation mechanism leads to the serious decrease of data transmission efficiency and rapid rise in overhead. On the contrary, TRPM, TSSRM and TSRF are more stable in terms of routing overhead with the addition of malicious nodes. Moreover, TRPM shows the best performance as the adoption of alternative secure routing strategy combined with optimal routing selection approach, which is capable of maintaining

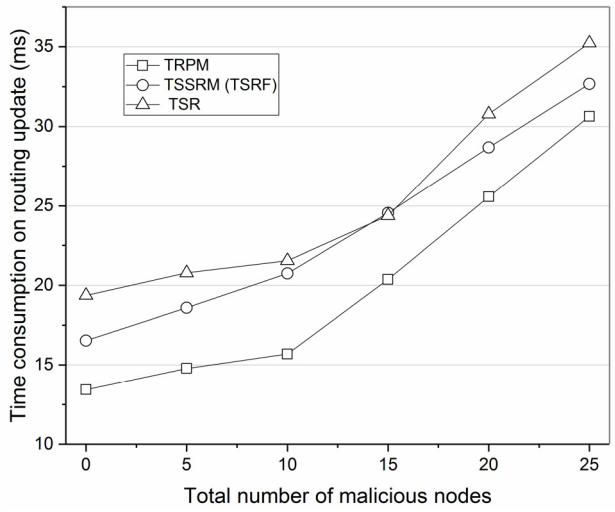


FIGURE 17. Time consumptions on routing update in case malicious attackers appear in current routing.

trustable and short routing requiring fewer wireless retransmissions. In Fig. 16(d), we compare the network lifetime of three energy-constrained schemes employed in WSNs. As in TRPM, lifetime stabilizes at 470s in case there is a small amount of malicious nodes in network. Since more compromised nodes tend to collude with each other, periodic data feedback from sink node starts to function as the alternative secure routing becomes invalid, which results in a slight decline of lifetime when number of attackers reaches 20. Meanwhile, trust assessment parts in TSSRM and TSRF are not sustainable to compromised node collusion as well as potential attackers with mutable strategies, thus an obvious falling trend has been found in network lifetime of such two models as the total number of malicious nodes continues to increase.

In case malicious nodes appear in established secure routing, some secure routing models including TRPM update current route via warning reports from intermediate nodes timely. In the last scenario, we compare TRPM with TSR and TSSRM to analyze the required time of rebuilding secure routing in case source or sink node receives a routing update notification caused by malicious node. As shown in Fig. 17, source node employed with TRPM directly adopts the alternate secure route when the number of malicious nodes is small, thus the routing update speed is much faster than that of other models. With the increase of malicious nodes in network, source node in TRPM judges the severity of malicious attacks via periodical feedback from sink node and then selects to reestablish reliable route with less time. Compared with TSR where secure routing update performed by overburdened sink node and TSSRM with oversimplified attack-feedback mechanism, time consumption on routing update of TRPM is shorten by about 11%, which shows a great advantage in secure routing maintenance.

VI. CONCLUSION

In this paper, we first distinguish WSN threats into two categories and then analyze the defensive capability of trust-based secure routing models proposed in related work against various malicious attacks. We also propose a robust trust-aware routing protocol with multi-attributes (TRPM) in terms of communication, data, energy, and recommendation to assist sensor nodes in establishing reliable routes, while sliding time window model combined with attack frequency detection mechanism is applied to identify attackers with mutable attack frequency. Simulation results indicate that network employed with TRPM shows good performance in dealing with various routing-targeting or trust-targeting attacks. Additionally, in case there are malicious attackers appearing in established secure route, the routing maintenance method introduced in TRPM has higher speed of routing update outperforming contrast models. In the future, we consider applying TRPM into real deployment with simplified calculation process and further enhance the performance of the model in security protection of WSNs by proposing a comprehensive trust-aware cluster head selection scheme with multi-attributes.

REFERENCES

[1] P. Rawat, K. D. Singh, H. Chaouchi, and J. M. Bonnin, "Wireless sensor networks: A survey on recent developments and potential synergies," *J. Supercomput.*, vol. 68, no. 1, pp. 1–48, 2014.

[2] B. Rashid and M. H. Rehmani, "Applications of wireless sensor networks for urban areas: A survey," *J. Netw. Comput. Appl.*, vol. 60, pp. 192–219, Jan. 2016.

[3] J. Granjal, E. Monteiro, and J. S. Silva, "Security in the integration of low-power Wireless Sensor Networks with the Internet: A survey," *Ad Hoc Netw.*, vol. 24, pp. 264–287, Jan. 2015.

[4] M. A. Mahmood, W. K. G. Seah, and I. Welch, "Reliability in wireless sensor networks: A survey and challenges ahead," *Comput. Netw.*, vol. 79, pp. 166–187, Mar. 2015.

[5] K.-A. Shim, "A survey of public-key cryptographic primitives in wireless sensor networks," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 1, pp. 577–601, 1st Quart., 2016.

[6] Y. Yu, K. Li, W. Zhou, and P. Li, "Trust mechanisms in wireless sensor networks: Attack analysis and countermeasures," *J. Netw. Comput. Appl.*, vol. 35, no. 3, pp. 867–880, 2012.

[7] I. Butun, S. D. Morgera, and R. Sankar, "A survey of intrusion detection systems in wireless sensor networks," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 1, pp. 266–282, 1st Quart., 2014.

[8] H. Rathore, V. Badarla, and S. Shit, "Consensus-aware sociopsychological trust model for wireless sensor networks," *ACM Trans. Sensor Netw.*, vol. 12, no. 3, 2016, Art. no. 21.

[9] W. Fang, W. Zhang, Y. Yang, Y. Liu, and W. Chen, "A resilient trust management scheme for defending against reputation time-varying attacks based on BETA distribution," *Sci. China Inf. Sci.*, vol. 60, no. 4, p. 040305, 2017.

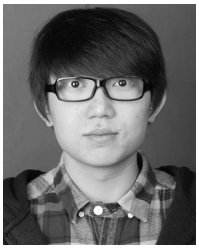
[10] H. Chen, Z. Han, and Z. Fu, "Quantitative trustworthy evaluation scheme for trust routing scheme in wireless sensor networks," in *Proc. Trustcom/BigDataSE/ISPA*, Helsinki, Finland, Aug. 2015, pp. 1272–1278.

[11] M. Zhang, R. Zheng, Q. Wu, W. Wei, X. Bai, and H. Zhao, "B-iTRS: A bio-inspired trusted routing scheme for wireless sensor networks," *J. Sensors*, vol. 2015, 2015, Art. no. 156843, doi: 10.1155/2015/156843.2015.

[12] J. Choi, J. Bang, L. Kim, M. Ahn, and T. Kwon, "Location-based key management strong against insider threats in wireless sensor networks," *IEEE Syst. J.*, vol. 11, no. 2, pp. 494–502, Jun. 2017.

[13] Z. Chen, M. He, W. Liang, and K. Chen, "Trust-aware and low energy consumption security topology protocol of wireless sensor network," *J. Sensors*, vol. 2015, 2015, Art. no. 716468, doi: 10.1155/2015/716468.2015.

[14] Z. Hu, Y. Bie, and H. Zhao, "Trusted tree-based trust management scheme for secure routing in wireless sensor networks," *Int. J. Distrib. Sensor Netw.*, vol. 2015, Jan. 2015, Art. no. 243.
[15] P. Gong, T. M. Chen, and Q. Xu, "ETARP: An energy efficient trust-aware routing protocol for wireless sensor networks," *J. Sensors*, vol. 2015, 2015, Art. no. 469793, doi: 10.1155/2015/469793.2015.
[16] J. Wang, Y. Liu, and Y. Jiao, "Building a trusted route in a mobile ad hoc network considering communication reliability and path length," *J. Netw. Comput. Appl.*, vol. 34, no. 4, pp. 1138–1149, 2011.
[17] F. Ishmanov and Y. B. Zikria, "Trust mechanisms to secure routing in wireless sensor networks: Current state of the research and open research issues," *J. Sensors*, vol. 2017, 2017, Art. no. 4724852, doi: 10.1155/2017/4724852.2017.
[18] J. Jiang, G. Han, F. Wang, L. Shu, and M. Guizani, "An efficient distributed trust model for wireless sensor networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 26, no. 5, pp. 1228–1237, May 2015.
[19] D. Qin, S. Yang, S. Jia, Y. Zhang, J. Ma, and Q. Ding, "Research on trust sensing based secure routing mechanism for wireless sensor network," *IEEE Access*, vol. 5, pp. 9599–9609, 2017, doi: 10.1109/ACCESS.2017.2706973.2017.
[20] A. Ahmed, K. A. Bakar, M. I. Channa, K. Haseeb, and A. W. Khan, "TERP: A trust and energy aware routing protocol for wireless sensor network," *IEEE Sensors J.*, vol. 15, no. 12, pp. 6962–6972, Dec. 2015.
[21] T. Zahariadis, P. Trakadas, H. C. Leligou, S. Maniatis, and P. Karkazis, "A novel trust-aware geographical routing scheme for wireless sensor networks," *Wireless Pers. Commun.*, vol. 69, no. 2, pp. 805–826, 2013.
[22] H. Xia, Z. Jia, X. Li, L. Ju, and E. H.-M. Sha, "Trust prediction and trust-based source routing in mobile ad hoc networks," *Ad Hoc Netw.*, vol. 11, no. 7, pp. 2096–2114, 2013.
[23] J. Duan, D. Yang, H. Zhu, S. Zhang, and J. Zhao, "TSRF: A trust-aware secure routing framework in wireless sensor networks," *Int. J. Distrib. Sensor Netw.*, to be published, doi: 10.1155/2014/209436.2014.
[24] A. Jøsang, "The right type of trust for distributed systems," in *Proc. Workshop New Secur. Paradigms*, Lake Arrowhead, CA, USA, 1996, pp. 119–131.
[25] N. Lewis and N. Foukia, "An efficient reputation-based routing mechanism for wireless sensor networks: Testing the impact of mobility and hostile nodes," in *Proc. 6th Annu. Conf. IEEE, Privacy, Secur. Trust*, Fredericton, NB, Canada, Oct. 2008, pp. 151–155.
[26] J. M. Moya *et al.*, "Using reputation systems and non-deterministic routing to secure wireless sensor networks," *Sensors*, vol. 9, no. 5, pp. 3958–3980, 2009.
[27] W. Wang, F. Du, and Q. Xu, "An improvement of LEACH routing protocol based on trust for wireless sensor networks," in *Proc. 5th Int. Conf. IEEE Wireless Commun., Netw. Mobile Comput.*, Beijing, China, Sep. 2009, pp. 1–4.
[28] G. Zhan, W. Shi, and J. Deng, "Design and implementation of TARF: A trust-aware routing framework for WSNs," *IEEE Trans. Dependable Secure Comput.*, vol. 9, no. 2, pp. 184–197, Mar./Apr. 2012.
[29] A. Ahmed, K. A. Bakar, M. I. Channa, K. Haseeb, and A. W. Khan, "A trust aware routing protocol for energy constrained wireless sensor network," *Telecommun. Syst.*, vol. 61, no. 1, pp. 123–140, 2016.
[30] Y. Liu, M. Dong, K. Ota, and A. Liu, "ActiveTrust: Secure and trustable routing in wireless sensor networks," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 9, pp. 2013–2027, Sep. 2016.
[31] M. A. Jan, P. Nanda, X.He, and R. P. Liu, "A Sybil attack detection scheme for a forest wildfire monitoring application," *Future Gen. Comput. Syst.*, vol. 80, pp. 613–626, Mar. 2018, doi: 10.1016/j.future.2016.05.034.2016.
[32] A. Mehmood *et al.*, "Energy-efficient multi-level and distance-aware clustering mechanism for WSNs," *Int. J. Commun. Syst.*, vol. 28, no. 5, pp. 972–989, 2015.
[33] G. Han, J. Jiang, L. Shu, J. Niu, and H.-C. Chao, "Management and applications of trust in wireless sensor networks: A survey," *J. Comput. Syst. Sci.*, vol. 80, no. 3, pp. 602–617, 2014.
[34] F. Ishmanov, S. W. Kim, and S. Y. Nam, "A robust trust establishment scheme for wireless sensor networks," *Sensors*, vol. 15, no. 3, pp. 7040–7061, 2015.
[35] A. Ahmed, K. A. Bakar, M. I. Channa, A. W. Khan, and K. Haseeb, "Energy-aware and secure routing with trust for disaster response wireless sensor network," *Peer-to-Peer Netw. Appl.*, vol. 10, no. 1, pp. 216–237, 2017.
[36] P. Zhou, S. Jiang, A. Irissappane, J. Zhang, J. Zhou, and J. C. M. Teo, "Toward energy-efficient trust system through watchdog optimization for WSNs," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 3, pp. 613–625, Mar. 2015.
[37] H. Jadidoleslamy, "TMS-HCW: A trust management system in hierarchical clustered wireless sensor networks," *Secur. Commun. Netw.*, vol. 8, no. 18, pp. 4110–4122, 2015.
[38] X. Li, F. Zhou, and J. Du, "LDTS: A lightweight and dependable trust system for clustered wireless sensor networks," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 6, pp. 924–935, Jun. 2013.



BOYUAN SUN received the B.S. degree from Shandong University, Shandong, China, in 2015. He is currently pursuing the M.S. degree in electrical engineering with the School of Electrical and Information Engineering, Tianjin University, Tianjin, China. His research interests include wireless sensor network securities and intelligent control.

DONGHUI LI was born in Jixi, China, in 1962. He received the M.S. and Ph.D. degrees in automation engineering from the China University of Mining and Technology, Jiangsu, China, in 1987 and 1994, respectively. He is currently a Doctoral Tutor with the School of Electrical and Information Engineering, Tianjin University, China. He has authored over 50 articles and holds four national inventions and patents. His research interests include wireless sensor network securities, intelligent control, power electronics applications, and building automation.