Yin and Li *EURASIP Journal on Wireless Communications and Networking* (2019) 2019:198
https://doi.org/10.1186/s13638-019-1524-z

EURASIP Journal on Wireless Communications and Networking

RESEARCH Open Access

Trust evaluation model with entropy-based weight assignment for malicious node's detection in wireless sensor networks

Xueqiang Yin[1,2*] and Shining Li[1]

Abstract

Trust management is considered as an effective complementary mechanism to ensure the security of sensor networks. Based on historical behavior, the trust value can be evaluated and applied to estimate the reliability of the node. For the analysis of the possible attack behavior of malicious nodes, we proposed a trust evaluation model with entropy-based weight assignment for malicious node's detection in wireless sensor networks. To mitigate the malicious attacks such as packet dropping or packet modifications, multidimensional trust indicators are derived from communication between adjacent sensor nodes, and direct and indirect trust values will be estimated based on the corresponding behaviors of those sensor nodes. In order to improve the validity of trust quantification and ensure the objectivity of evaluation, the entropy weight method is applied to determine the proper value of the weight. Finally, the indirect trust value and direct trust value are synthesized to obtain the overall trust. Experimental results show that the proposed scheme performs well in terms of the identification of malicious node.

Keywords: Trust evaluation model, Entropy, Weight assignment, Security, Wireless sensor networks

1 Introduction

Nowadays, wireless sensor networks (WSNs) have become one of the most useful technologies and attracted more and more attention from researchers [1]. Owing to the capabilities of data acquisition, processing, and transmission, the sensor nodes can be deployed in many application scenarios, such as environmental monitoring, battlefield detection, industrial safety monitoring and health care, etc. However, due to the unmanned environment and the characteristics of energy-constrained, the sensors are vulnerable to various attacks. By capturing some normal nodes, the attackers can change their behavior and then insert false data or decisions to mislead the decision-making of the whole network. In addition, the sensor nodes may be problem-prone to non-malicious errors, such as inadequate residual energy and faults of wireless transceiver or components, and then, result in unreliable data generation [2]. Especially, to improve the energy efficiency, data aggregation in sensor networks is needed. Once a node is captured, the errors or forged data sent by the fault node will impact the entire fusion result. Therefore, network security of WSNs is a crucial problem to be solved [3].

In the field of network security, asymmetric cryptography is widely used to deal with external attacks in the Internet, peer-to-peer, and ad hoc networks. However, due to the complexity and demand of huge computational memory, the encryption algorithm is not suitable for WSNs due to limited processing power and resource constraints [4]. In addition, the security mechanism based on encryption can only solve external security problems and cannot effectively deal with internal attacks. In WSNs, the particularity of nodes, different from other networks, can refuse to cooperate with service requesters to save energy, and those nodes are being called selfish nodes. Although they do not actively attack the network, a large number of selfish nodes may cause serious consequences. Obviously, the existing encryption mechanism is incapable to identify the risks caused by authenticated selfish nodes. Therefore, it is necessary to establish an effective security mechanism to solve those problems [5]. In recent years, trust management has

* Correspondence: yinxueqiang@mail.nwpu.edu.cn
[1] School of Computer Science, Northwestern Polytechnical University, Xi'an 710029, People's Republic of China
[2] The 15th Research Institute of China Electronic Technology Group Corporation, Beijing 100083, People's Republic of China

been regarded as an effective complementary mechanism to ensure the security of sensor networks. Based on historical behavior, the trust value of a node can be evaluated to estimate the reliability based on the performance of specific tasks. At present, many typical trust models have been proposed for WSNs, which derives from game theory [6], Bayesian estimation [7], D-S evidence [8], fuzzy logic [9], etc. The above models all identify malicious nodes through trust evaluation to a certain extent and provide a theoretical basis for further research. Under the open network environment, the trust between sensor nodes will vary dynamically with time and behavior The trust value obtained by the trust model should also change with the communication behavior between nodes, thus effectively restrain the abnormal increase or decrease of trust value and resist the influence of flattery or slander between nodes. How to define the trust relationship in the model as well as improve the efficiency of the model implementation becomes an important issue.

The rest of this paper is organized as follows: after the related works are summarized in Section 2, the trust evaluation model is presented in detail in Section 3. In Section 4, we present the steps of secure communication under the proposed model. We evaluate the performance of our trust evaluation model in Section 5. And finally, we conclude this paper in Section 6.

2 Related work

For internal malicious node attacks, most of the effective defense measures are often built on trust model management. Trust evaluation can be abstractly referred to as the estimation of the relevant evidence affecting the trust of the subject. Generally, trust can be measured in a way similar to information or knowledge and formulated as degree of trust. The trust value can be defined as the combination of direct trust and indirect trust, which can be given a certain weight according to the specific application requirements [10]. Behavior-based trust evaluation models can be divided into centralized and distributed trust evaluation model. Different working modes directly affect the data exchange mode between participants in trust assessment, as well as the data processing, trust calculation during the phase of trust assessment.

In the centralized trust evaluation model, the center obtains global information such as exchange records between sensor nodes or user's feedback and calculates trust according to a certain rule. Ganeriwal et al. [11] proposed a reputation-based framework for high integrity sensor networks, and they introduced beta function to calculate reputation and trust value. In [12], Probst et al. introduced a statistical method into a trust management model. Trust value can be estimated based on the direct and indirect experience of nodes and confidence interval is applied to identify malicious behavior. Cheng et al. [13] presented a trust model based on D-S evidence theory, in which the comprehensive trust value can be obtained by D-S combination rules. According to historical behavior, trust fluctuation, and recommendation inconsistency in a certain period of time, Anita et al. [14] proposed a routing trust prediction model based on fuzzy theory. The model can predict the subsequent behavior of neighbor nodes, but it may lead to the loss of information. Aivaloglou et al. [15] proposed a hybrid trust and reputation management model based on the certificate-based method and behavior-based mechanism. The model utilizes the knowledge of network topology and data flow to support the highly diversified needs of node's roles. Combining fuzzy and gray theory, Wu et al. [16] proposed a trust model with incentive mechanism to evaluate the reliability of nodes. However, because of the complexity of model calculation, it is not suitable for sensor networks with limited processing capacity of nodes. Generally, the centralized trust evaluation model has the characteristics of a relatively simple structure and less difficulty to implement. However, due to overwhelmingly dependent on central nodes, load balancing and robustness become the bottleneck of further exploitation.

In contrast, in the distributed trust evaluation model, the trust degree does not depend on the support of the central entity. Through the direct interaction with the evaluated entity, the recommendation of the direct interaction from all entities can be synthesized to estimate the trust degree. In [17], Jiang et al. proposed an efficient distributed trust model according to the exchange messages from all sensor nodes, and the trust metrics include communication overhead, energy consumption, and data validity. In [18], Bao et al. proposed a hierarchical dynamic trust management protocol for clustered wireless sensor networks and develop a probability model using stochastic Petri net techniques to analyze the performance. Zhang et al. [19] proposed a multi-level trust management framework. In this framework, three levels of trust, namely subjective trust, objective reputation, and recommendation trust, are used to establish trust relationships among nodes. The shortcomings lie in the lack of trust sharing and update mechanism. To ensure the security of data forwarding and improve energy efficiency, Tang et al. [20] proposed a trust-based secure routing scheme using the trace back approach, in which the data and notification employ a dynamic probability of marking and logging during routing selection. Based on the hierarchical network structure, Liao et al. [21] proposed a weighted trust evaluation strategy, which updates the weighted trust value continuously by comparing the data collected by sensor nodes and the final data fusion results. The anomaly nodes detection and trusted data filtering mechanism can obtain good performance and scalability. To achieve the tradeoff between energy conservation and network security, Liao et al. [21] presented a mixed and continuous monitor-forward model based on game theory to mitigate the selective-forwarding attack, in which the monitoring node conducts a strategy continuously to determine the duration of behavior surveillance. However, the selfishness and rationality of sensor nodes are not thoroughly considered.

Taking into account of energy consumption and secure routing, many studies combine the construction of trust model with the clustering management mechanism of nodes. Shaikh et al. [22] proposed a group-based trust management mechanism and applied it to cluster-structured wireless sensor networks. The calculation of trust value is achieved by monitoring the communication behavior between neighbor nodes, including member node's trust, cluster head's trust, cluster trust, and base station trust. The trust model can effectively resist malicious node attacks and protect malicious nodes from defamation and defamation attacks as well as keep energy-efficiency. Zhou et al. [23] proposed a trust evaluation model based on the autonomous behavior of sensor nodes. Sensor nodes acquire direct or indirect trust values by monitoring the behavior of neighbor nodes. Cluster heads calculate comprehensive trust values according to D-S evidence theory. By trust evaluation, malicious nodes can be effectively identified and malicious nodes can be restricted to become cluster heads. Crosby et al. [24] designed a distributed trust-based cluster head election mechanism. The trust table was constructed by monitoring the transmission process of neighbor nodes, and the trust degree was calculated. Then, the reliable cluster head was elected according to the trust degree, which ensured the reliability of data fusion and network security. For secured data fusion, Fu et al. [25] introduced a cluster-based trust model with double cluster heads structure, in which the dissimilarity coefficient is defined to evaluate the data fusion results. If the fusion results exceed the threshold value, it demonstrates that the cluster head is possible to be compromised nodes and then to be added to the blacklist.

3 Trust model

3.1 Trust indicators

The purpose of trust evaluation is to provide support for trust decision-making to establish a reliable relationship between the entities. Combining with the implementation of security strategy, it can form a general trust management system. In WSNs, the sensor's authentication depends not only on the historical data of the node itself, but also on the adjacent nodes with spatio-temporal correlation. The characteristics of node behavior often vary with time, and the regularity has some statistical characteristics. Therefore, the behavior of nodes can be analyzed, and a quantitative evaluation model can be established through the history of interaction between nodes. Specifically, the sensor nodes in adjacent areas monitor each other and calculate their trust, which can effectively identify malicious nodes to resist network attacks.

The selection of trust factors is the premise and foundation of calculating node's direct trust, and the trust elements should conform to the characteristics of WSNS. Malicious attacks launched by nodes mainly include stealing, tampering with perceptual information, injecting a lot of error information, etc. Therefore, we can analyze the data repetition rate, the number of data packets, data correlation, and the volatility of data latency.

Definition 1: *Data repetition rate*. The data repetition rate of samples can reflect the node's abnormal behavior owing to repeat sending packets continuously.

$$\mathrm{DRR}_{i,j}(u,v,t)=\frac{S_{u,v}(t)-SP_{u,v}(t)}{S_{u,v}(t)} \tag{1}$$

where $S_{u,\ v}(t)$ is the number of sent samples at time t, and $SP_{u,\ v}(t)$ is the number of the repeated samples.

Definition 2: *Packet size abnormality*. If the number of samples during the monitoring cycle is too large, it may be a denial of service attack. On the other hand, if the number is too small, the possibility of selfish behavior is high.

$$\mathrm{PSA}(u,v,t)=\frac{\mid S_{u,v}(t)-\Delta S(t)\mid}{S_{u,v}(t)} \tag{2}$$

where $\Delta S(t)$ denotes the expected value for the number of samples.

Definition 3: *Data correlation*. The data collected by neighbor nodes have certain correlation, and the difference between normal nodes should be within a certain range.

$$\mathrm{DC}(u,v,t)=\alpha e^{-r[D_u(t)-D_v(t)]^2} \tag{3}$$

where α is the attractiveness parameter, and r represents the distance between node s_u and s_v. $D_u(t)$ and $D_v(t)$ represent the measured value of node s_u and s_v, respectively.

Definition 4: *Volatility of transmission delay*. Due to signal interference and other factors in wireless communication, data transmission delay will occur in nodes. The neighboring nodes have temporal and spatial correlation. The transmission delay of networks should fluctuate within a certain range.

$$VTD(u,v,t)=\frac{\sum_{k=1}^{h}RT(u,k)-ST(u,k)}{\sum_{k=1}^{h}RT(v,k)-ST(v,k)} \tag{4}$$

where h denotes the average number of hops between node s_u and s_v, and $RT(i,k)$, and $ST(i,k)$ represents the time of receipt and delivery of samples, respectively.

3.2 Clustering objective function

Quantification of trust relationship needs to meet the dynamic requirements of the environment, and it should also show the exact emphasis according to the impact of measurement indicators [26, 27]. Generally, under the condition of multiple monitoring indicators, the weight value has certain experience and subjectivity, which is not conducive to the validity of trust quantification and evaluation [28, 29].

In this paper, the trust evaluation model divides the nodes into categories of normal nodes, relay nodes, and base station in the perception layer. In the process of evaluating node behavior trust, only relay nodes generate recommended trust values among themselves, and it is assumed that the base station is fully trusted. Let s_1, s_2, $\cdots$, s_n denote n adjacent relay nodes of the evaluated target. According to the index mentioned above, the observation vector $(r_{i1}\ \ r_{i2}\ \ \cdots\ \ r_{im})$ is obtained at the ith relay node. The evaluation matrix $R_{n\times m}$ can be constructed, in which r_{ij} represents the evaluation result of jth indicator from ith relay node, $1 \le i \le n$, $1 \le j \le m$.

Generally, under the condition of multiple monitoring indicators, the establishment of weights has certain experience and subjectivity, which is disadvantageous to the validity of trust quantification and evaluation [30, 31]. In this paper, the weight of monitoring index will be solved based on the method of entropy weight.

First, the membership matrix $U_{m\times n}$ is defined, and the matrix element u_{ij} represents the degree of membership of r_{ij} with constraint of

$$\sum_{j=1}^{m}u_{ij}=1, 0\le u_{ij}\le 1. \tag{5}$$

Next, to indicate the difference between the recommendation entity and the expectation caused by the objective deviation, we define the recommended deviation Δ as:

$$\Delta_j=\frac{1}{n}\sqrt{\sum_{i=1}^{n}u_{ij}\sum_{j=1}^{m}\left(r_{ij}-\bar{r}_j\right)^2} \tag{6}$$

where $\bar{r}_j$ represents the average value of jth indicator, and $\bar{r}_j=\frac{1}{m}\sum_{i=1}^{m}r_{ij}$

The objective of clustering is to find the optimal clustering vector so as to minimize the overall recommended deviation, and the objective function can be expressed as:

$$\min\left\{\Delta^2\right\}=\min\{\sum_{j=1}^{m}\sum_{i=1}^{n}u_{ij}\sum_{i=1}^{m}\left[\frac{1}{n}\left(r_{ij}-\bar{r}_j\right)\right]^2\} \tag{7}$$

According to the definition of membership matrix $U_{m\times n}$, u_{ij} can be regarded as the probability that the ith entity belongs to the jth monitoring index. Therefore, the information entropy of jth monitoring index for the relay node s_i can be calculated as:

$$H=-u_{ij}\ln\left(u_{ij}\right) \tag{8}$$

Accordingly, the total information entropy of the matrix $U_{m\times n}$ can be expressed as:

$$H^*=-\sum_{j=1}^{m}\sum_{i=1}^{n}u_{ij}\ln\left(u_{ij}\right) \tag{9}$$

In order to minimize the clustering function and optimize the overall information entropy, the optimization process can be described as follows:

$$\min\{-\sum_{j=1}^{m}\sum_{i=1}^{n}u_{ij}(\sum_{i=1}^{m}\left[\frac{1}{n}\left(r_{ij}-\bar{r}_j\right)\right]^2)+\frac{1}{\rho}\sum_{j=1}^{m}\sum_{i=1}^{n}u_{ij}\ \ln\left(u_{ij}\right)\} \tag{10}$$

where ρ is the equilibrium factor of the equation.

By using the Lagrange multiplier method [32, 33], the constraint $\sum_{j=1}^{m}u_{ij}=1$ can be introduced into the Lagrange multiplier λ, and the Eq. (9) can be transformed to

$$\begin{aligned}L\left(u_{ij},\lambda,t_j\right)=&\sum_{j=1}^{m}\sum_{i=1}^{n}u_{ij}(\sum_{i=1}^{m}\left[\frac{1}{n}\left(r_{ij}-\bar{r}_j\right)\right]^2)\\&+\frac{1}{\rho}\sum_{j=1}^{m}\sum_{i=1}^{n}u_{ij}\ \ln\left(u_{ij}\right)\\&+\lambda\left|\sum_{i=1}^{n}u_{ij}-1\right|\end{aligned} \tag{11}$$

Solving the objective function $L\left(u_{ij},\lambda,\bar{r}_j\right)$, u_{ij} can be derived as

$$u_{ij}=\frac{\exp(-\rho\sum_{i=1}^{n}\left(r_{ij}-\bar{r}_j\right)^2}{\sum_{j=1}^{m}\exp(-\rho\sum_{i=1}^{n}\left(r_{ij}-\bar{r}_j\right)^2)} \tag{12}$$

According to the membership degree and recommendation deviation degree, the weight values of monitoring indicators with normalization can be obtained as

$$\begin{cases} CR_j = \bar{r}_j \times \left(1 - k_j\right) \\ w_i = \dfrac{CR_j}{\sum\limits_{i=1}^{n} CR_j} \end{cases} \tag{13}$$

where CR represents the comprehensive recommendation for jth indicator from entities.

Finally, based on recommendation trust and corresponding weight value, the quantitative results of direct trust evaluation between relay node k and monitored node can be estimated as:

$$D\mathrm{Trust}_k = \sum_{j=1}^{m} w_j r_{kj} \tag{14}$$

3.3 Indirect trust

The indirect trust can be regarded as the recommendation from the third party [34]. The indirect trust value of node s_u to node s_v is composed of the direct trust value of all recommendation nodes to node s_v, and the recommended nodes are referred to as the common neighbor nodes of node s_u and s_v. However, not all recommendation nodes are trustworthy, and unreliable recommendation will provide false information to evaluate the trustworthiness of the nodes, which will affect the trust of the sensor nodes that create and manipulate the data.

In order to calculate the indirect trust value accurately through recommendation nodes, it is necessary to select trusted neighbors as recommendation nodes. First, we define a specified trust threshold δ, and the nodes with direct trust higher than δ will be selected as the recommended neighbors set. As multiple nodes push trust values to a single node at the same time, it may bring opportunities to malicious nodes. Malicious nodes intentionally elevate or degrade the trust of a node by sending false or conflicting recommendation trust values. Therefore, multiple recommendation trust problems must be solved through trust merge rules. Suppose Ω denote represents the set of trusted neighbor nodes of the evaluated node and relay node s_k, and $|\Omega|$ represents the number of nodes in set Ω. Firstly, the average value of all evaluation result will be calculated as

$$\bar{r}_{ij} = \frac{\sum\limits_{i \in \Omega} r_{ij}}{|\Omega|} \tag{15}$$

Next, the weight ω_i of the recommendation node can be obtained as:

$$\omega_i = \frac{\sum\limits_{j=1}^{m} \left| r_{ij} - \bar{r}_{ij} \right|}{\sum\limits_{i \in \Omega} \sum\limits_{j=1}^{m} \left| r_{ij} - \bar{r}_{ij} \right|} \tag{16}$$

Then, the indirect trust can be estimated as

$$I\mathrm{Trust}_k = \frac{\sum\limits_{i \in \Omega} \omega_i D\mathrm{Trust}_i}{|\Omega|} \tag{17}$$

Definition 5: *Total trust.* By synthesizing indirect trust with direct trust, the total trust can be obtained as follows:

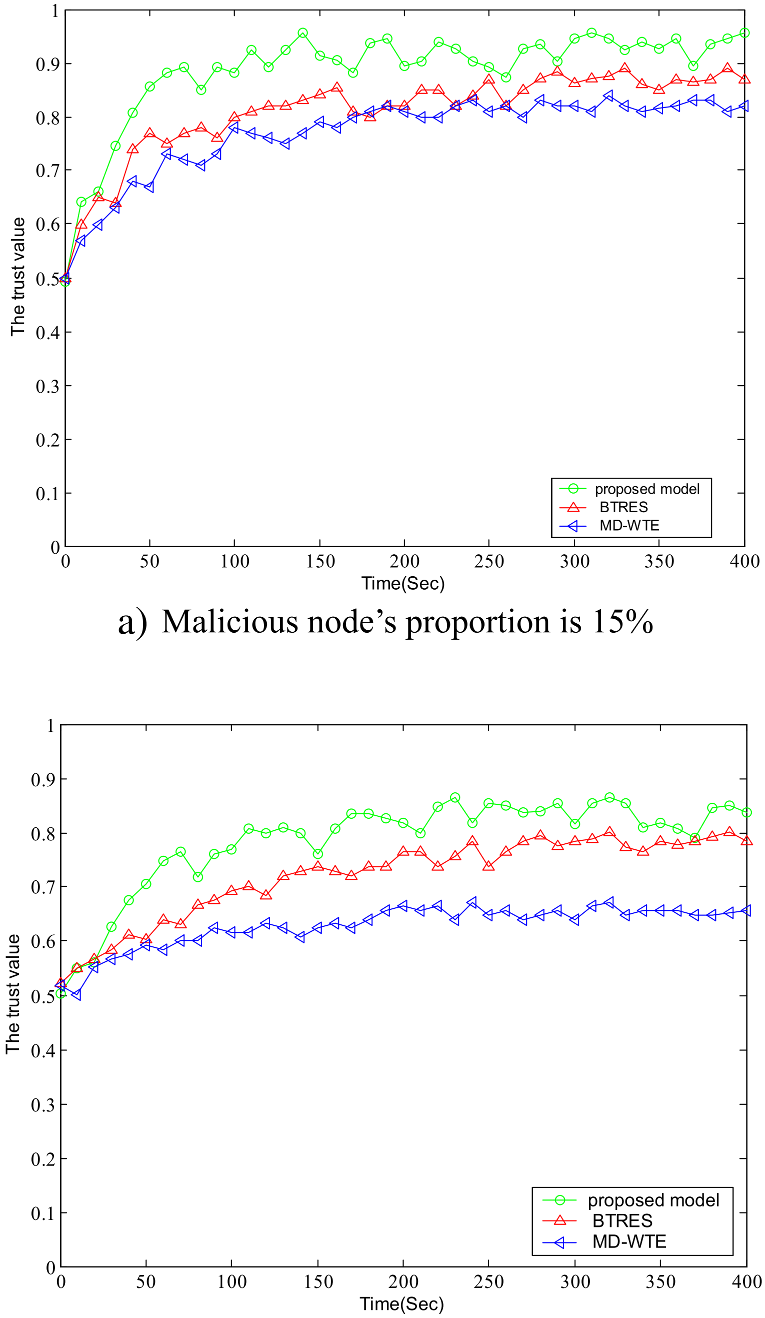
$$T\mathrm{Trust} = \theta D\mathrm{Trust} + (1 - \theta) I\mathrm{Trust} \tag{18}$$

where $\theta \in [0,1]$ and indicate the trustworthiness degree to the trust value.

4 Secure communication

Based on the proposed trust evaluation model, the secure communication is introduced based on AODV protocol. In the initial stage, the identity-based cryptography mechanism is applied to verify the legitimacy of nodes and establish a trusted network environment. Then, the specific flow of its secure communication is as follows:

Step 1: Initially, all nodes broadcast their own identity information in the network. All neighbor nodes in the communication range can calculate their shared keys according to the private keys and identification, which can be used to encrypt and decrypt exchange message between them.
Step 2: If the source node s_S prepares to communicate with the destination node s_D, it will query the local routing table whether exists a route to the destination. If not, the route to node s_D should be established by the following steps.
Step 3: s_S broadcasts query message RREQ to its neighbor s_k, and s_k will determine whether the same query information has been processed. If so, the current request message is discarded. Otherwise, the number of hops in the query message will plus 1.
Step 4: Then, s_S will retrieve the direct trust of neighbor s_k in its local storage module and broadcast a trust query message to its neighbor nodes. All the nodes receiving the source node trust query information check whether they have the trust value of the node s_k. If so, the trust response message encrypted with the shared secret key between itself and the source node s_S will be returned.



a) Malicious node's proportion is 15%

b) Malicious node's proportion is 30%

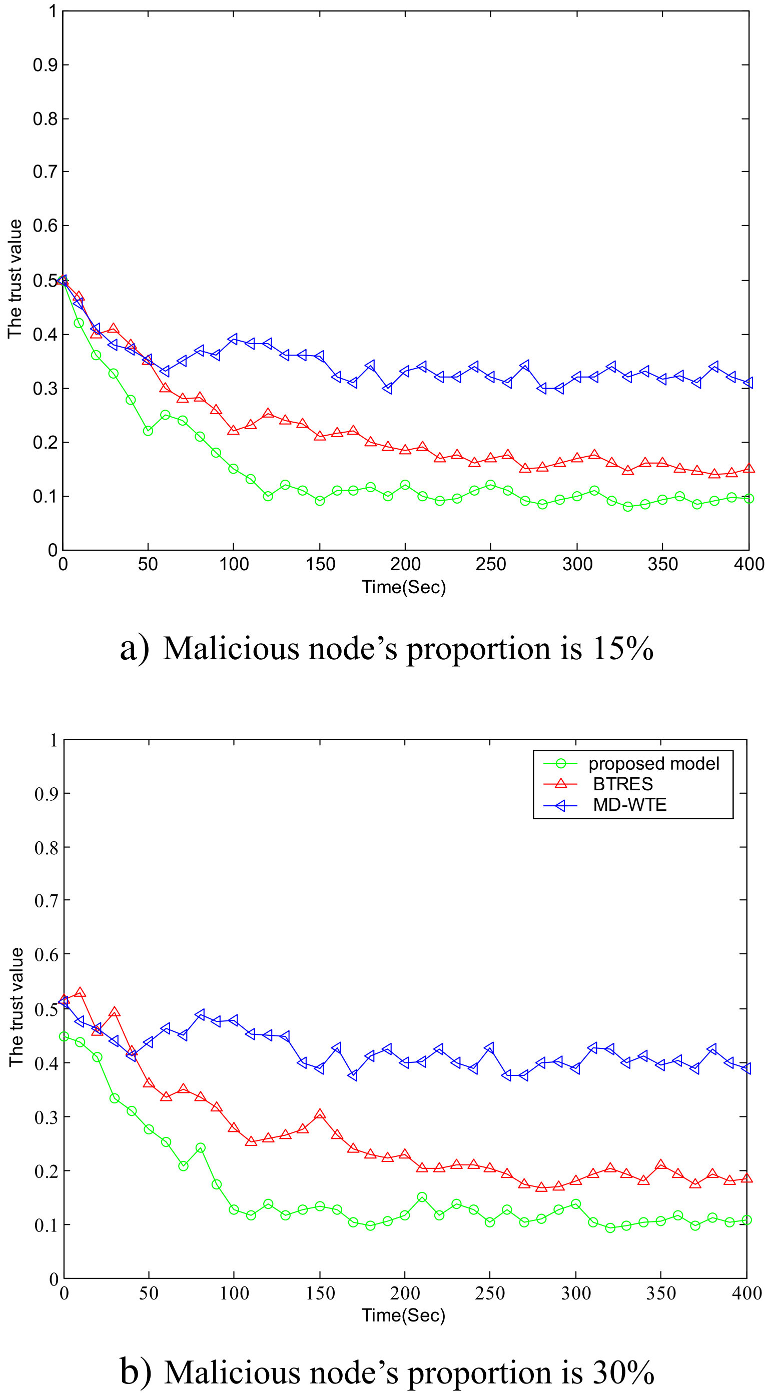
Fig. 1 The trust value of normal node with time. **a** Malicious node's proportion is 15%. **b** Malicious node's proportion is 30%

Step 5: Finally, s_S can obtain the comprehensive trust of the node s_k. If trustworthy, it will be regarded as the next hop node and continue to forward the routing query message RREQ. Otherwise, return to execute Step 2.

Step 6: Execute Step 3 repeatedly until a trusted route from s_S to destination s_D can be resolved.

5 Experimental results

In order to verify the validity of the proposed trust model for wireless sensor networks, simulation experiments are conducted. The size of the network is 100m × 100m. One hundred sensor nodes are randomly distributed in the region, and the base station is located in the center of the monitoring area. The perception



a) Malicious node’s proportion is 15%

b) Malicious node’s proportion is 30%

Fig. 2 The trust value of malicious node with time. **a** Malicious node’s proportion is 15%. **b** Malicious node’s proportion is 30%

radius of nodes is 20 m and the communication range is set to 40 m. In the simulation experiment, the proportion of malicious nodes is arranged from 0 to 40%, and they simulated by the several kinds of attacks, including selective forwarding attack, data forgery attack, DoS attack, and on/off attack. Each simulation time is 400 s, and the time period of trust update is equal to 10 s. The assignment of other parameters is as $m = 4$, $\theta = 0.5$ and $\delta = 0.7$.

The performance of the proposed method is compared with that of MD-WTE [34] and BTRES [35]. Figures 1 and 2 show the trust value of the normal node and malicious node with time as malicious node proportion is 15% and 30%, respectively. The experimental results

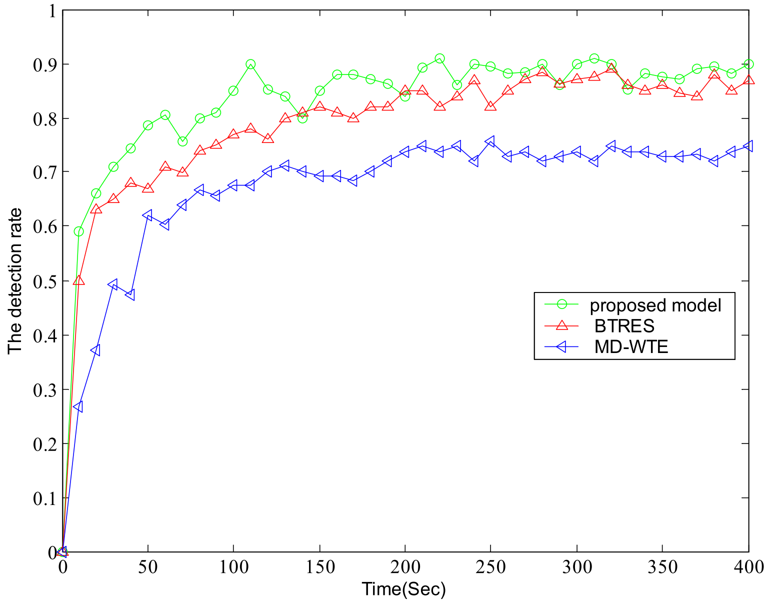


Fig. 3 The detection rate with time as malicious node's proportion is 15%

show that in MD-WTE, the average trust value of normal nodes is similar, but the trust value of abnormal nodes is obviously higher than that of other methods. As a result, the malicious nodes cannot be distinguished clearly. That is because only one trust value is applied in MD-WTE, and the malicious sensor nodes can hide malicious behavior of their sensing through trusted transfer function. The nodes can still maintain high reliability by masking malicious packet loss via trusted sensing behavior. In our proposed model and BTRES, the direct trust values are closer to the object trust values compared with the integrated trust values since the integrated trust values are more or less influenced by the malicious recommendations. However, they take communication behavior into account to calculate sensor nodes' trust value and improve the accuracy of recommendation trust against the selective forwarding attack and the data forgery attack.

As can be seen from Fig. 2, when the proportion of malicious nodes is about 30%, the trust value of normal

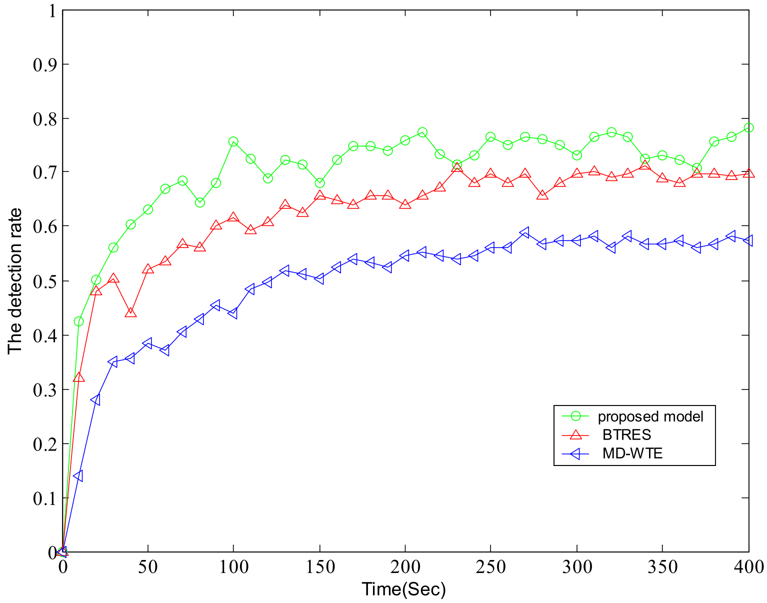


Fig. 4 The detection rate with time as malicious node's proportion is 30%

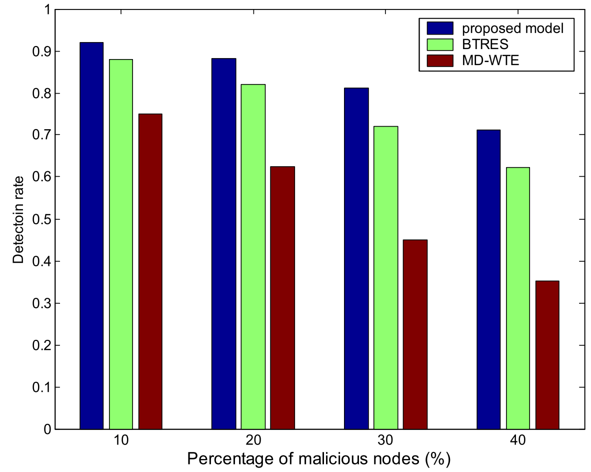


Fig. 5 The detection rate with different percentage of malicious nodes

nodes decreases obviously; meanwhile, the trust value of malicious nodes increase. This trend also shows that when malicious nodes reach a certain proportion, the normal nodes in the network cannot effectively detect the abnormal behavior of malicious nodes. Hence, the average trust value of malicious nodes increases. Compared with the other methods, our proposed model can reduce the impact of malicious nodes more effectively. It illustrates that the direct trust and recommendation trust should be dynamically adjusted based on the proportion of malicious nodes. Once the percent of malicious nodes exceeds the extent, the normal behavior of nodes may be mistaken as abnormal. That will not be conducive to the delivery of data by normal nodes in the network.

Furthermore, we evaluate the detection rate and false error rate of malicious nodes. Due to open environment and the performance of nodes being uncertain, not all nodes can be judged as trusted or untrustworthy state. Figures 3 and 4 show the differences in detection rate when malicious nodes are 15% and 30%, respectively. As can be seen from the results, our proposed model and BTRES have risen rapidly from the beginning of different scenarios and have maintained a high detection rate in the process of operation. The reason is that both of the methods can reduce the dependence on prior experience and the assumption of prior distribution, which improves the speed and accuracy of identifying the malicious nodes. Comparatively, after accumulating a certain amount of records, the detection rate in MD-WTE increases gradually. In our proposed model, entropy-based weight assignment improves the objectivity of trust evaluation and obtains fast convergence rate.

Next, we analyze and compare the detection rate and false alarm rate under different percentage of malicious nodes. As can be seen from Figs. 5 and 6, our proposed model and BTRES have higher detection rate and lower false alarm rate when the proportion of malicious nodes is small. As the proportion of malicious nodes increases, the detection rate of MD-WTE decreases rapidly, and the false alarm rate also increases sharply. The detection rate of our proposed model decreases slowly and gradually stabilizes, and the promotion of false alarm rate is relatively small. The reason is that the fuzziness and conflict of evidence increase as the proportion of

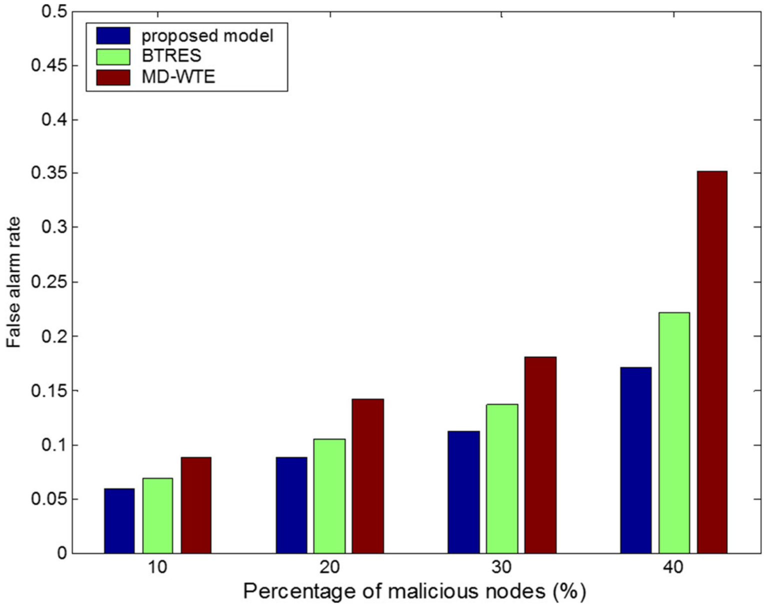


Fig. 6 The false alarm rate with different percentage of malicious nodes

malicious nodes increases. By means of selecting the proper value of the weight of direct trust and indirect trust, our proposed model improves the accuracy of the malicious node's detection and robustness of trust evaluation model.

6 Conclusions

In this paper, we proposed a trust evaluation model with entropy-based weight assignment for malicious node's detection in wireless sensor networks. Multidimensional trust indicators are derived from communication between adjacent sensor nodes, and direct and indirect trust values will be estimated based on the corresponding behaviors of those sensor nodes. To improve the validity of trust quantification and ensure the objectivity of evaluation, the entropy weight method is applied to determine the proper value of the weight. In our future work, we will devote to evaluate the trust level of sensor nodes in clustered WSNs and combine the trust model with secure data fusion. Besides, some professional techniques, e.g., fuzzy logic or pattern recognition, will be employed and discussed to reduce the fuzziness of behavior evidences.

Abbreviation

WSNs: Wireless sensor networks

Acknowledgements

The authors acknowledged the anonymous reviewers and editors for their efforts in valuable comments and suggestions.

Authors' contributions

XY proposed the innovation ideas and theoretical analysis, and he carried out the experiments and data analysis. SL conceived of the study, participated in its design and coordination, and helped to draft the manuscript. All authors read and approved the final manuscript.

Availability of data and materials

Data sharing is not applicable to this article as no datasets were generated or analyzed during the current study.

Competing interests

The authors declare that they have no competing interests.

Received: 29 March 2019 Accepted: 22 July 2019
Published online: 06 August 2019

References

1. G. Han, J. Jiang, L. Shu, J. Niu, J. Comput. Syst. Sci. **80**(3), 602–617 (2014)
2. A. Ahmed, K.A. Bakar, M.I. Channa, A.W. Khan, K. Haseeb, Peer-Peer Netw. Appl. **10**(1), 216–237 (2017)
3. B. Wu, X. Yan, Y. Wang, C. Guedes Soares, Risk Anal. **37**(10), 1936–1957 (2017)
4. M.A. Simplício, P. Barreto, C.B. Margi, Comput. Netw. **54**(1), 2591–2612 (2010)
5. Y.M. Huang, M.Y. Hsieh, H.C. Chao, IEEE J. Sel. Areas Commun. **24**(7), 400–411 (2009)
6. J. Duan, D. Gao, D. Yang, C.H. Foh, IEEE Internet Things J. **1**(1), 58–69 (2014)
7. M.K. Denko, T. Sun, I. Woungang, Comput. Commun. **34**(3), 398–406 (2011)
8. W. Zhang, S. Zhu, J. Tang, J. Supercomput. **74**, 1779–1801 (2018)
9. B. Wu, L. Zong, X. Yan, C. Guedes Soares, Ocean Eng. **164**, 590–603 (2018)
10. D. He, S. Zeadally, N. Kumar, J.H. Lee, IEEE Syst. J. **11**(4), 2590–2601 (2016)
11. S. Ganeriwal, M. Srivastava, *Proceedings of the 2nd ACM Workshop on Security of Ad-Hoc and Sensor Networks Washington DC* (2004), pp. 66–77
12. M.J. Probst, S.K. Kasera, *Proceedings of 2007 International Conference on Parallel and Distributed Systems* (2007), pp. 1–8
13. R. Feng, S. Che, X. Wang, Int. J. Distrib. Sens. Netw. **9**(6), 1–9 (2013)
14. X. Anita, M.A. Bhagyaveni, J. Manickam, Sci. World J. **8**(1), 341–356 (2014)
15. E. Aivaloglou, S. Gritzalis, Wirel. Netw **16**(5), 1493–1510 (2010)
16. G. Wu, Z. Du, Y. Hu, et al., Soft. Comput. **18**(9), 1829–1840 (2014)
17. J. Jiang, G. Han, F. Wang, L. Shu, IEEE Trans. IEEE **26**(5), 1228–1237 (2014)
18. F. Bao, I.R. Chen, M.J. Chang, et al., IEEE Trans. Netw. Serv. Manag. **9**(2), 169–183 (2012)
19. T. Zhou, C. Wu, J. Zhang, D. Zhang, Saf. Sci. **96**, 183–191 (2017)
20. J. Tang, A. Liu, J. Zhang, Sensors **18**(3), 751 (2018)
21. H. Liao, S. Ding, Int. J. Distrib. Sensor Netw. **1**, 1–13 (2015)
22. R.A. Shaikh, H. Jameel, B.J. D'Auriol, et al., IEEE Trans. Parallel Distrib. Syst. **20**(11), 1698–1712 (2008)
23. J.M. Zhou, F. Liu, Q.Y. Lu, J. Sensors **68**(9), 907–913 (2014)
24. G.V. Crosby, N. Pissinou, J. Gadze, *Proceedings of Second IEEE Workshop on Dependability and Security in Sensor Networks and Systems* (IEEE, Columbia, 2006), pp. 13–22
25. J.S. Fu, Y. Liu, Sensors **15**(1), 2021–2040 (2015)
26. A. Boukerch, L. Xu, K. El-Khatib, Comput. Commun. **30**(12), 2413–2427 (2007)
27. M. Al Ameen, J. Liu, K. Kwak, J. Med. Syst. **36**(1), 93–101 (2012)
28. H. Marzi, A. Marzi, *Proc. of IEEE CIVEMSA* (2014), pp. 64–69
29. B.K. Kannan, S.N. Kramer, J. Mech. Des. **116**(2), 405–411 (1994)
30. H. Oh, C.T. Ngo, IEEE Sensors J. **18**(5), 2184–2194 (2018)
31. Y. Wang, E. Zio, X. Wei, D. Zhang, B. Wu, Int. J. Disaster Risk Reduct. **33**, 343–354 (2019)
32. C. Wan, X. Yan, D. Zhang, Z. Qu, Z. Yang, Transport. Res. E-Log **125**, 222–240 (2019)
33. M.Y. Zhang, D. Zhang, F. Goerlandt, X. Yan, P. Kujala, Saf. Sci. **111**, 128–143 (2018)
34. I.M. Atakli, H. Hu, Y. Chen, et al., *Proceedings of the International Symposium on Simulation of Systems Security* (2008), pp. 836–843
35. W. Fang, C. Zhang, Z. Shi, J. Netw. Comput. Appl. **59**, 88–94 (2016)

Publisher's Note

Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.