EURASIP Journal on Wireless Communications and Networking

RESEARCH

Open Access

An emerging intelligent optimization algorithm based on trust sensing model for wireless sensor networks

Yongmei Wang[1*], Min Zhang[2] and Wanneng Shu[3]

Abstract

Due to the limitation of battery power, processing capacity, and storage, the sensor nodes are easy to be captured, destroyed, or attacked in an open environment. As a result, the security and reliability of data transmission cannot be guaranteed. In order to resist the internal attacks from malicious nodes, an ant colony optimization algorithm for secured routing based on trust sensing model (ACOSR) in wireless sensor networks is proposed. Firstly, a reliable evaluation model of trust perception is presented, which can estimate the node's trust value derived from its behavior to identify or isolate the malicious nodes effectively. The penalty function and regulator function are applied to reflect the effect of state changes on the trust value according to the node's behavior in the process of the communication. Secondly, the trust evaluation model is introduced into the ant colony routing algorithm to improve the security for data forwarding. The simulation results show that the proposed algorithm has improved the performance significantly in terms of packet loss rate, end to end delay, throughput, and energy consumption and demonstrates good resistance to black hole attack.

Keywords: Edge-of-things computing, Wireless sensor networks, Internet of things, Energy consumption, Emerging intelligent optimization algorithm

1 Introduction

The rapid developments of Internet of things (IoT) give impetus to the construction of cloud computing and constantly promote the popularization of applications for social network service and even the smart city [1]. Depending on different types of distributed smart equipment, smart city can offer wide applications for urban residents in aspects of telemedicine diagnosis, intelligent community, environmental monitoring, and surveillance; owing to the characteristics of low cost, easy-to-deploy and specialized wireless sensor networks (WSNs) have played a crucial role in promoting the various facilities of the smart city. On the one hand, the ubiquitous sensor nodes can be used for collecting the physical information around the environment. On the other hand, they can make use of the widely distributed facilities to realize unattended management. However, the inherent characteristics of an open and distributed system, WSNs are of vulnerability due to the simplicity and limitation of design in the structure of hardware units [2]. In addition, the communication of the wireless channel makes the attack more convenient. Since the traditional secure routing protocols are usually complex and energy-consuming, the existing protocol design is not suitable for resource-constrained WSNs [3].

At present, the researches on wireless sensor network security have made many achievements, and the security measures mainly include authentication, encryption, information integrity verification, and intrusion detection. Nevertheless, most of the above security mechanisms can only deal with the intrusion or attack from the network outside, and the malicious nodes will enter into the network smoothly and launch the specific attacks inside the network while the occurrence of the internal attacks of wireless sensor networks [4]. The typical malicious attacks include selfish node, malicious forwarding, black hole, rushing, or worm attack [5, 6]. In view of the malicious node attack in WSNs, the trust

* Correspondence: wangymfddsy@hfnu.edu.cn
[1]School of Computer Science and Technology, Hefei Normal University, Hefei 230031, China
Full list of author information is available at the end of the article

model-based management mechanism is proven to be a popular and effective method [7]. Besides, trust evaluation model has low computation and communication load, which demonstrate a significant advantage in respect of solving the internal attacks and identifying the malicious nodes [8].

The rest of this paper is organized as follows: In Section 2, we briefly introduce the related work. In Sections 3 and 4, the assumptions and explanations of the details of our method are described. The experiment methods are shown, and the result is discussed regarding the performance evaluation in Section 5. Finally, Section 6 concludes this paper and discusses the future work.

2 Related works

To protect the security of the link or constrain the malicious attack within a certain range, researchers have proposed different defense strategies, such as TTSS, SPINS, and INSENS [9–11]. Generally, those protocols usually adopt the technology of encryption, authentication, or key management mechanism to resist the attacks, including selective forwarding, SYBIL attack, wormhole attack, and HELLO flooding [12, 13].

Ganeriwal et al. [14, 15] presented a reputation-based trust management framework (RFSN) and applied to wireless sensor networks, which uses Watchdog system to monitor the neighbor node communication behavior. Besides, the trust value of sensor node is generated by putting the monitoring results into the credit system module, and reputation value is measured by Bayes formula for quantitative analysis of node's uncertainty. The trust framework is complete and robust, but requires a priori distribution of the subjective assumption of reputation value. Shaikh et al. [16] presented a trust management scheme for hierarchical WSNs. The trust value is obtained by monitoring the communication behavior between the neighbor nodes by the predefined detective node. The trust mechanism can be established from several aspects to resist attack of malicious nodes, and it can consume less communication overhead as well as efficient memory usage. Feng et al. [17] put forward a credible trust management scheme for WSNs based on Bayesian theory. Firstly, the trust value can be estimated by RFSN model. Then, they utilized statistical data and Bayesian method to acquire the comprehensive trust value. Moreover, considering the influence of the uncertain factors of third parties on the value of trust in the process of evaluation, time sliding window is applied for trust value's renovation. Jiang et al. [18] proposed a distributed trust evaluation model for WSNs, in which the direct trust value and the recommended trust value are selectively evaluated depending on the number of normal packets received by the sensor nodes.

To promote the accuracy of recommendation trust, multiple indicators, such as communication behavior, node's residual energy, and the number of normal packets, are taken into consideration. Then, the model defines the trust reliability and familiarity to evaluate node's trustworthiness. Hossein et al. [19] proposed a distributed trust management system with fuzzy theory to measure the trust value of nodes in WSNs. Yenumula et al. [20] examined the behavior of malicious nodes under the attack of selective forwarding and conducted the performance evaluation of the impact quantitatively. Due to the packets from normal nodes be selectively discarded, it will result in network failure or even collapse. To ensure the authenticity and reliability of the aggregated data, Hu et al. [21] proposed a security model based on trusted data fusion to resist the capacity of the risks derived from data tampering. Amol R et al. [22] presented a trust evaluation model for intrusion detection to identify malicious nodes or selfish nodes effectively, and the trusted routing is allowed by eliminating malicious nodes. Zhang et al. [23] proposed a dynamic trust establishment and management framework, and a trust varying function is defined to generate certain weight value for adapting to the dynamic changes of the network. Mejia et al. [24] proposed a trust evaluation model with game theoretic for online distributed evolution. Considering that the game theory is an auxiliary method for decision making rather than a prediction tool, it may not be suitable for resolving the trust problem of the sensor node. Bao et al. [25] presented a hierarchical trust management protocol by formulating social trust and QoS (quality of service) trust, which regards intimacy or honesty as a metric of trust evaluation and selects QoS' trust by energy dissipation and node selfishness.

The existing trust evaluation methods are proposed for the characteristics of the node's past behavior and different application scenarios. However, it is not enough to consider the trust assessment which combines subjective judgment and objective evaluation. In addition, the trust value is expressed by floating point number instead of integer value with single byte, which will result in excessive energy consumption between the nodes while passing the recommendation trust.

3 Trust sensing model

3.1 Direct trust value

Direct trust value is the immediate evaluation given by node i to node j through direct communication behavior, which can be obtained by Bayesian Statistical theory [26]. In this way, the Watchdog mechanism will be applied to monitor the behavior of the neighbor nodes during interactive communication, and the monitoring results can be used to obtain the trust values of each node. In addition, the uncertainty of a random signal or event can be estimated by entropy theory. Based on information entropy theory, the uncertainty of a random signal or event can be measured.

Assuming that the prior distribution obeys the Beta distribution, the trust value between the nodes can be measured by the expected value, and the following formula is obtained.

$$T_{\mathrm{dir}}(i,j)=\frac{\alpha_{ij}+1}{\alpha_{ij}+\beta_{ij}+2} \tag{1}$$

where α_{ij} and β_{ij} denote the record number of successful or failed communication interaction between node i and j at the time interval Δt, respectively.

In the actual environment, the communication behavior between nodes is easily affected by the uncertain factors such as network congestion and noise. It is essential to introduce valid regulatory mechanism to reflect the impact of these uncertainties on the value of trust. Most trust models do not take these factors into consideration. As a result, the trust value of the nodes is often ideal and not true. Considering that the number of failed exchange between the sensor nodes increase in a short time, the node's behavior indicates as malicious, and the trust value of the node will be reduced quickly. In order to suppress malicious nodes more quickly and effectively, penalty function is the punishment of trust value through dynamic changes of malicious behaviors in communication between nodes. Here, the penalty function is defined as:

$$\delta=1-e^{\frac{\beta_{ij}}{\alpha_{ij}+\beta_{ij}}} \tag{2}$$

By introducing penalty function, the trust value of the suspected node should be punished according to its abnormal behavior, which can identify malicious behaviors of nodes quickly and accurately. In addition, to avoid rapid promotion of trust values of malicious nodes through conspiracy or mutual touting, a regulator function should be applied to modify the trust value to prevent irregular swift growth. The regulator function can be defined as:

$$\mu=1-\frac{1}{\ln\left(\alpha_{ij}+1\right)} \tag{3}$$

With the increasing number of successful interactive communication between nodes, the value of the regulator function is more and more close to one with steady growth. It reflects the actual situation that the dynamic changes in the behavior of successful communication between nodes should be a long-term stable process, and the steady increase of node's trust value can alleviate the possibility of conspiracy attacks on the system.

Based on above analysis, the formula of the direct trust value can be modified.

$$T_{\mathrm{dir}}(i,j)=\frac{\mu\alpha_{ij}+1}{\mu\alpha_{ij}+\beta_{ij}+2}\delta \tag{4}$$

3.2 Indirect trust value

The indirect trust value refers to the evaluation of the node's behavior from the recommendation nodes, which are composed of the neighbor nodes of node i and node j. It should be noted that not all recommended nodes are trustworthy, and the false recommendation from untrusted nodes will impair the quality of the true credibility of the node. Therefore, to obtain the right evaluation of the indirect trust value through the recommended nodes, it is necessary to select a set of credible nodes from common neighbors as the recommendation ones.

Initially, the trust value of all nodes is assigned to 0.5, and the threshold of trust value as recommendation node is λ. According to theoretical analysis, the nodes from common neighbors of node i and j with the trust value no less than λ can be selected as the recommendation ones. Assuming that k neighbors of node i and j meet the requirement of trust value threshold, and the trust value is T_{i1}, T_{i2}, $\cdots$, T_{is}. On the basis of the transitivity of the trust value, the indirect trust value can be given as:

$$T_{\mathrm{ind}}(i,j)=\frac{\sum\limits_{m\in N_s, m\neq i} T_{\mathrm{dir}}(i,m)\times T_{\mathrm{dir}}(m,j)}{|N(i)\cap N(j)|} \tag{5}$$

where $T_{\mathrm{dir}}(i,m)$ denotes the direct trust value of node i to node m, $T_{\mathrm{dir}}(m,j)$represents the direct trust value of node m to node j, and $|N(i)\cap N(j)|$ indicates that the number of common recommendation nodes by nodes i and j.

Next, the comprehensive trust value of the node can be estimated by the sum of direct trust and indirect trust, which will be given as:

$$T_{\mathrm{total}}(i,j)=\theta T_{\mathrm{dir}}+(1-\theta)T_{\mathrm{ind}} \tag{6}$$

where $T_{\mathrm{total}}(i,j)$ indicates the comprehensive trust value of node i to node j. T_{dir} and T_{ind} represent the direct and indirect trust values, respectively. θ denotes the weight of direct trust.

4 Secured routing method

Ant colony optimization algorithm (ACO) is proposed by Marco Dorigo, which is a heuristic intelligent algorithm for finding optimal paths in graphs [27, 28]. During the process, the collective behavior of ant colony shows a positive feedback of information, and finally, the whole ant colony will obtain the optimal path. It is very suitable for the characteristics of wireless sensor network routing.

To resist the possible attacks from malicious nodes, the node trust evaluation model is introduced into the ant colony algorithm, and the security and energy consumption of nodes should be regarded as the optimization objective. The main idea is to select the next hop neighbor node j of node i according to pheromone, sensor node's residual energy and evaluated trust value. Usually, the selection of the node in the next hop should be satisfied with higher trust value and more residual energy.

Assuming that m ants are generated from source node, the initial pheromone of the path and the node's energy are equal. Each ant tries to find the optimal path with minimum cost, and the transition probability of the ant k moving from node i to node j for the next hop can be given as:

$$p_{ij}^{k}(t) = \begin{cases} \dfrac{\left[\tau_{ij}(t)\right]^{\alpha}\cdot\left[\eta_{ij}(t)\right]^{\beta}\cdot\left[\psi_{j}(t)\right]^{\gamma}}{\sum\limits_{u\in N_k(i)}\left[\tau_{iu}(t)\right]^{\alpha}\cdot\left[\eta_{iu}(t)\right]^{\beta}\cdot\left[\psi_{u}(t)\right]^{\gamma}}, j\in N(i) \\ 0, \quad \text{otherwise} \end{cases} \tag{7}$$

where $\tau_{ij}(t)$ denotes the amount of pheromone in the path at time t, $\eta_{ij}(t)$ denotes the heuristic value of the path, and $\psi_j(t)$ is the factor of residual energy of node j. α, β, γ are the weight value of pheromone, heuristic value, and factor of residual energy, respectively. They should satisfy the condition that $0 < \alpha, \beta, \gamma \le 1$ and $\alpha + \beta + \gamma = 1$.

During the data forwarding, energy-efficiency should be referred to as important aspect by which the network lifetime prolongs. The transition probability should reflect the superiority of the node with more residual energy among the neighbors of node i. Therefore, the factor $\psi_j(t)$ can be defined as:

$$= |N(i)| * E_{\text{res}}(j)/\sum\nolimits_{s\in N(i)}(E_{\text{res}}(s)) \tag{8}$$

By selecting the node with the highest comprehensive trust value from the neighbor nodes set as the next hop, the heuristic factor will be derived as:

$$\eta_{ij}(t) = \arg\max\nolimits_{j\in N(i)}\{\theta T_{\text{dir}} + (1-\theta)T_{\text{ind}}\} \tag{9}$$

Since the direct trust relationship between nodes is unable to involve all nodes, the estimation of the indirect trust value from the adjacent recommendation node. Besides, the smaller the weight value γ is, the more obvious the effect of the indirect trust demonstrates.

As the energy of the sensor node is constrained, the residual energy of the nodes located in the path and the link length should be taken into account during the phase of updating the pheromone. It can effectively balance the network energy load and reduce the residual energy gap between the nodes. Thus, when the residual energy of the nodes from different link is the same, the shortest path routing will be selected. Therefore, after k ants arrive in the aggregation node, the increment of the pheromone can be obtained according to:

$$\Delta\tau_k(t) = \frac{E_{\text{res}}^{(t)}(i)/\text{avg}_{s\in N(i)}(E_{\text{res}}(s))}{E_0 - \max_{s\in N(i)}\{(E_{\text{res}}(s))\}} \tag{10}$$

where $\text{avg}_{s\in N(i)}(E_{\text{res}}(s))$ and $\max_{s\in N(i)}\{(E_{\text{res}}(s))\}$ represent the average residual energy and maximum residual energy of all neighbor nodes from node i, respectively. E_0 represents the initial energy of all sensor node.

The pheromone factor on the path will be updated according to formula (10):

$$\tau_{ij}(t) = (1-\rho)\tau_{ij}(t) + \Delta\tau_k(t) \tag{11}$$

where ρ represents the volatilization coefficient of pheromone and $0 \le \rho < 1$. $\Delta\tau_k(t)$ represents the increment of the pheromone during the current round.

5 Results and discussion

To verify the performance of proposed algorithm for secured routing, the simulation experiments are conducted with MATLAB. Firstly, the influence of punishment and regulation mechanism on direct trust value is verified with dynamic change of communication behavior between nodes in our trust model. Then, our model compares with DDR (Detecting Dishonest Recommendation) [29] in terms of trust value under the condition of no attack or malicious node's attack. Subsequently, the comparison of ACOSR, DDR, and SRC (Secure and Robust Clustering) [30] algorithm demonstrates in aspects of the average energy consumption, the average time delay, throughput, and the packet loss rate. We use the energy model presented in [31], and the specific parameters are shown in Table 1.

Figures 1 and 2 illustrate the comparison of direct trust value and comprehensive trust value in the case of no attack. In the absence of malicious nodes, the number of node's successful communication increases steadily over time. The trust value and the comprehensive trust value of the node are also increasing. Comparatively speaking, when the number of successful interaction increases rapidly, the growth of trust value in ACOSR is restricted and the trust value between nodes is unable to be quickly raised in a short time. The reason is that the regulator function of ACOSR can effectively avoid the rapid increase of trust value by the number of

Table 1 The specific parameters

Parameters	Value
E_0	0.5 J
Initial trust value	0.5
Packet length	2000 bits
d_0	37 m
E_{elec}	50 nJ/bit
E_{DA}	5 nJ/(bit·signal)
λ	0.6
θ	0.6
MAC protocol	MAC 802.11
Queue type	PriQueue
Data flow rate	448 kbit/s
α	0.2
β	0.5
γ	0.3
ρ	0.3

successful interactions in a short time. The design goal of slow growth of trust value is more adaptable to the effect of normal behaviors on the trust relationship between the nodes in wireless sensor networks than in traditional network.

The direct and comprehensive trust value in the case of malicious node's attack is depicted in Figs. 3 and 4. Due to the malicious nodes' attack behavior, the number of nodes' unsuccessful interaction continues to increase. For ACOSR, the penalty function operates on the trust value due to the attack behavior from malicious nodes. As can be illustrated from the results, when the number of unsuccessful interaction increases rapidly, the trust value between nodes is reduced quickly, and the goal of fast decline of trust value is realized.

In this scenario, the trust value of the proposed algorithm is always lower than the trust value of DDR. It fully reflects that the trust value of ACOSR is more sensitive to malicious communication behavior and malicious attacks than DDR as the frequent occurrence of unsuccessful interactions. It also evaluates the trust relationship between nodes in ACOSR more accurately and reliably and identifies malicious nodes more quickly and effectively.

Next, the performance of each algorithm is simulated under black hole attack. As shown in Fig. 5, the total trend of the packet loss rate of all algorithms increase as the increase of the malicious nodes with aggressive behaviors. When there are no attacks in the network, the packet loss rates of SRC, DDR, and ACOSR is 1.94, 2.87, and 3.93%, respectively. Owing of the low complexity and small delay, the packet loss rate of SRC is slightly lower than that of the other algorithms. However, SRC does not adopt trust mechanism, which is incapable to resist black hole attack, and thus, its packet loss rate has increased dramatically with the continuous growth of the attack nodes. ACOSR and DDR utilize the trust model to evaluate the node's behavior, and the trend of package loss is relative slow. In general, the trust model can isolate malicious nodes to some extent. However, the nodes launching the black hole attack as selfish nodes who can affect the forwarding of data packets, and it will still cause a certain number of packet loss.

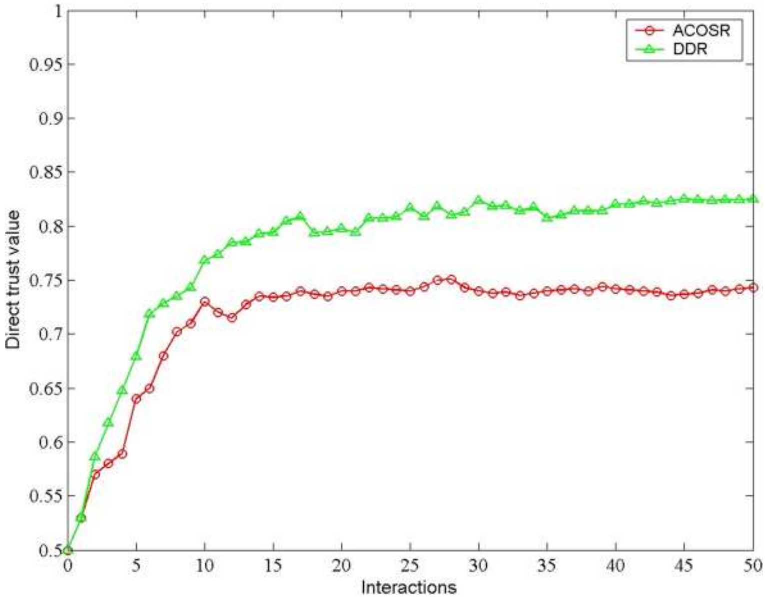

Fig. 1 Direct trust value in the case of no attack

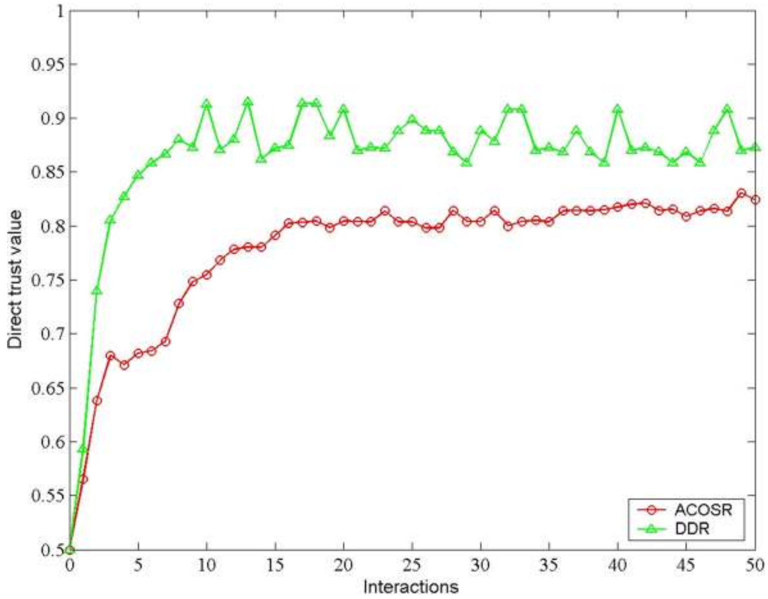

Fig. 2 Comprehensive trust value in the case of no attack

The final packet loss rate of the ACOSR algorithm is 13.8% lower than that of the DDR algorithm. That is because that ACOSR algorithm considers the distance the ants walk when the pheromone updates and make the path pheromone concentration closer to the convergence node. It will increase the speed of path search and reduce the time delay, and then, the packet loss rate can be reduced.

Figure 6 shows the average time delay as well as the increment of the number of malicious nodes. Due to frequent packet loss in the scenario, the upper layer of transmission protocol needs to wait for the establishment of links and the packet re-transmission between the nodes, which results in the increase of time delay. When there is no attack node, the time delay of the SRC is 19 ms, which is lower than that of the ACOSR and the DDR. That is because the other two algorithms need to acquire the sensor's trust value for a long time. When the number of malicious nodes increases in ACOSR, the routing stability drops sharply due to the excess packet

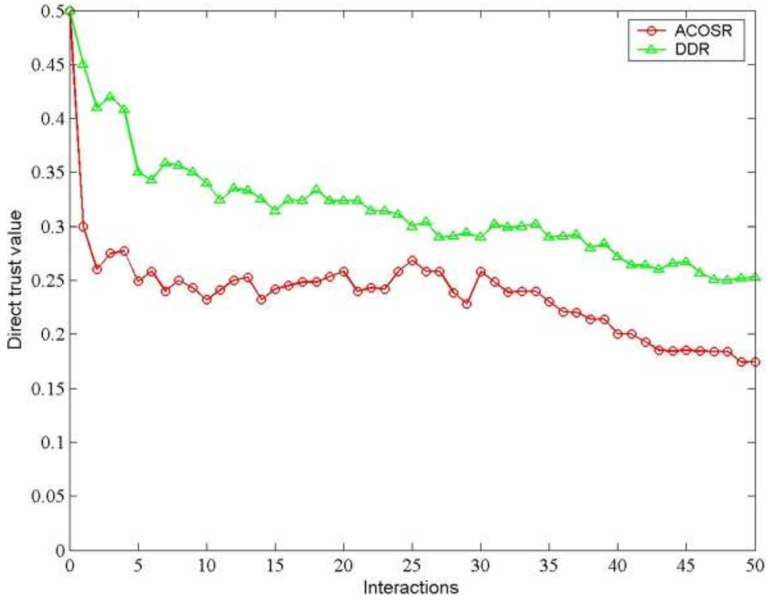

Fig. 3 Direct trust value in the case of malicious node's attack

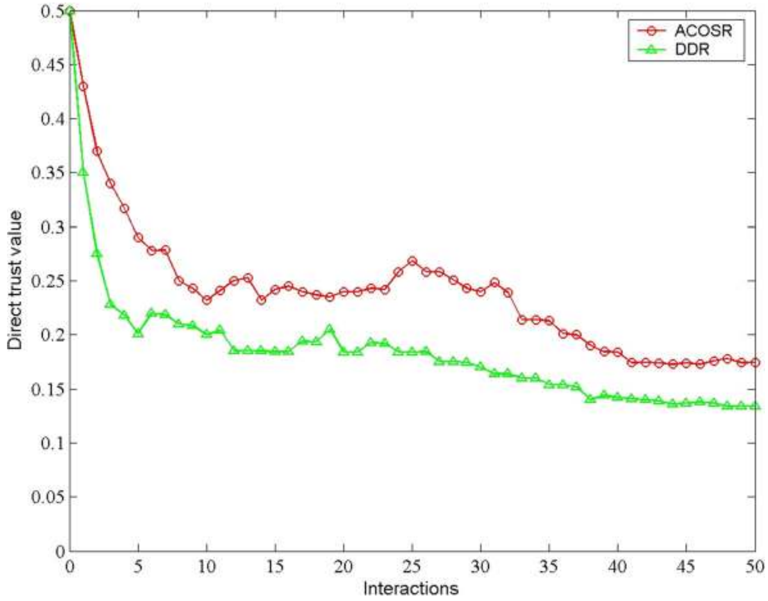

Fig. 4 Comprehensive trust value in the case of malicious node's attack

loss and it will increase the delay of packet packets arriving at the destination. In comparison, the trust evaluation model is used in both ACOSR and DDR, and the time delay trend is relatively close. Since ACOSR takes the residual energy directly as a selection probability factor, it can effectively improve the search efficiency and obtain the optimal path, it can achieve lower delay than DDR.

Figure 7 illustrates the comparison of throughput of the network. The overall trend of network throughput is decreasing. The reason is that the black hole attack being produced by malicious nodes makes the packets routing more and more difficult to remain stable, and large amount of data packet loss leads to the reduction of throughput. As can be seen from Fig. 7, the throughput of the network is rapidly reduced from 69.87 to 22.45 kbit/s in SRC. The trust evaluation model applied in ACOSR and DDR effectively guarantees the stability of the network, which avoids the sharp decline of throughput caused by the massive loss of data packets.

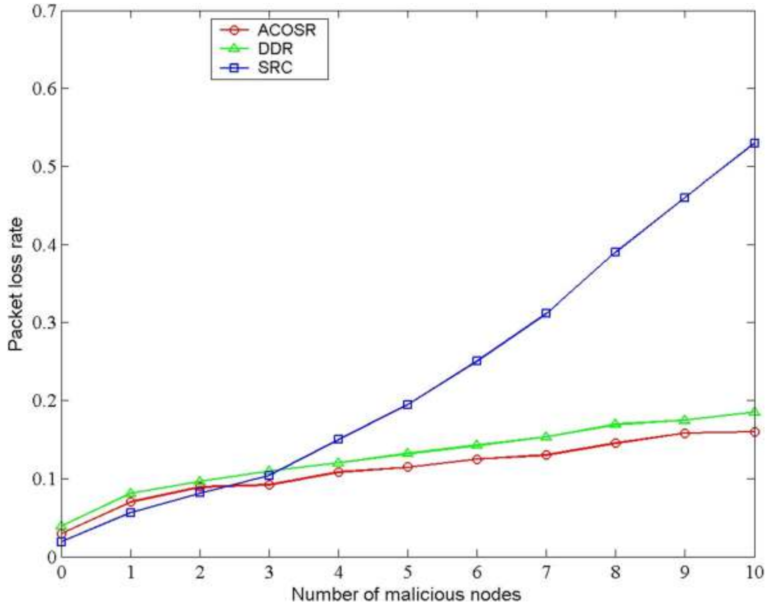

Fig. 5 Packet loss rate

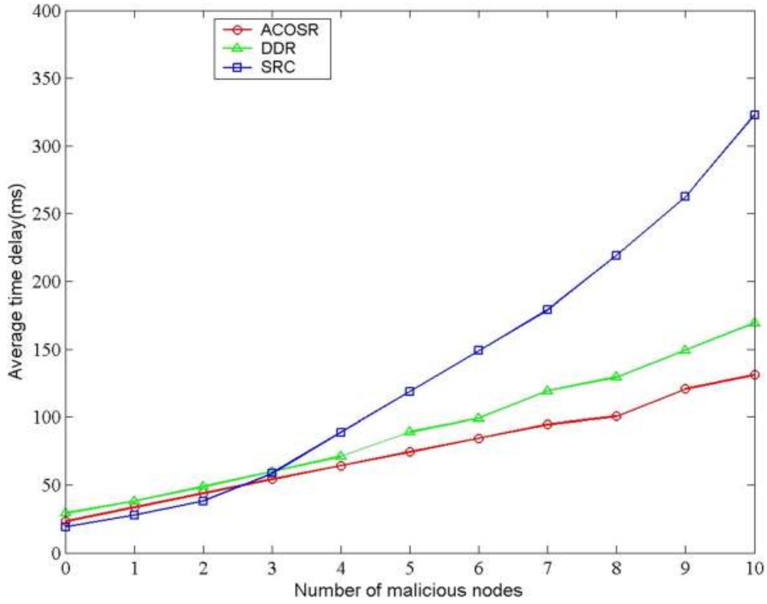

Fig. 6 Average time delay

Since the packet loss rate of ACOSR is less than that of DDR, the overall throughput can demonstrate better performance.

Figure 8 is the comparison of average energy consumption as different number of malicious nodes. Since the energy consumption of the network mainly depends on the number of times of the data packet interaction, the increase of packet loss rate makes the number of interactions decline. Thus, the average energy consumption of sensor nodes decreases. SRC has no resistance to malicious node attacks, and then, the packets will be largely lost owing to the existence of malicious nodes undertaking the data relay and result in a sharp decrease in average energy consumption from 13.1 to 10.9 J. Compared with DDR, the residual energy of the node is taken as the key factor of the selection probability in ACOSR in terms of updating pheromone. It can effectively balance the energy expenditure among all sensor nodes and reduce the average energy consumption of the whole network.

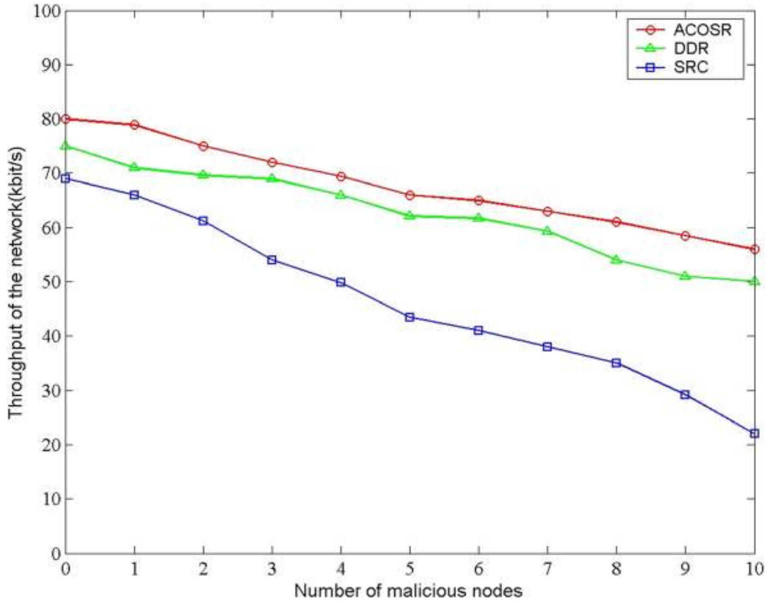

Fig. 7 Throughput of the network

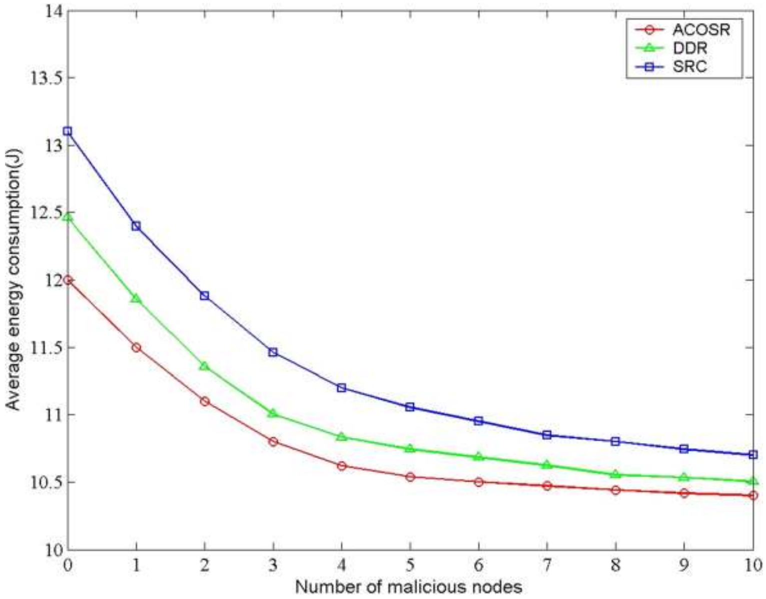

Fig. 8 Average energy consumption

6 Conclusions

In order to resist internal attacks from malicious nodes, this paper proposes an ant colony optimization algorithm for secured routing based on trust sensing model in WSNs. Firstly, aiming at the problems of internal attacks such as black hole attacks, the ACOSR adopts the trust evaluation model to isolate malicious nodes effectively according to the behavior of nodes, which can reduce the packet loss rate and establish secure routing. In addition, by adopting the residual energy of the node as the key factor of the selection probability and taking into account of the node's average energy when updating pheromone, it can effectively balance the energy expenditure among all nodes and reduce the average energy consumption of the whole network. In the future work, we will expand the model for node's behavior evaluation under more complex attack mode as well as reducing the energy consumption of exchange of recommendation trust.

Abbreviations

ACO: Ant colony optimization; ACOSR: Ant colony optimization algorithm for secured routing; DDR: Detecting dishonest recommendation; INSENS: Intrusion-tolerant routing in wireless sensor networks; QoS: Quality of service; SPINS: Security protocols for sensor networks; SRC: Secure and robust clustering; TTSS: Three-tier security scheme; WSNs: Wireless sensor network

Acknowledgements

The authors thank the reviewers for giving the helpful comments and suggestions, which help to improve the quality of the manuscript.

Funding

This work was supported by the National Natural Science Foundation of China under grant no. 61603420.

Authors' contributions

YW and WS contributed to the conception and algorithm design of the study. YW and MZ contributed to the acquisition of simulation. YW, MZ, and WS contributed to the analysis of simulation data and approved the final manuscript.

Authors' information

Yongmei Wang received a M.S. degree from Anhui University, in 2011. She is an experimentalist in School of Computer Science and Technology, Hefei Normal University, Hefei, China. His research interests lie in computer application, intelligent arithmetic, and Internet of things.

Min Zhang received a M.S. degree from Anhui University, in 2011. She is an experimentalist in College of Information and Computer, Anhui Agricultural University, Hefei, China. His research interests lie in network of computer and Internet of things.

Wanneng Shu received a M.S. and Ph.D. degree from Central China Normal University and Wuhan University, in 2007 and 2013. He is an assistant professor in the College of Computer Science, South-Central University for Nationalities, Wuhan 430074, China. His research interests lie in Green cloud computing, parallel computing, and Internet of things.

Competing interests

The authors declare that they have no competing interests.

Publisher's Note

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

Author details

[1]School of Computer Science and Technology, Hefei Normal University, Hefei 230031, China. [2]College of Information and Computer, Anhui Agricultural University, Heifei 230036, China. [3]College of Computer Science, South-Central University for Nationalities, Wuhan 430074, China.

Received: 17 April 2018 Accepted: 4 June 2018
Published online: 13 June 2018

References

1. MR Eslaminejad, M Sookhak, SA Razak, M Haghparast, A review of routing mechanisms in wireless sensor networks. Int. J Comput. Sci. Telecommun. **10**(2), 1–9 (2011)

2. A Kellner, O Alfandi, DA Hogrefe, Survey on measures for secure routing in wireless sensor networks. Int. J. Sens. Netw. Data Commun **1**(10), 1–17 (2012)
3. A Chakrabarti, V Parekh, A Ruia, A trust based routing scheme for wireless sensor networks. Lect Notes Inst Comput Sci Soc Inf Telecommun Eng **1**(84), 159–168 (2012)
4. J Duan, D Yang, H Zhu, et al., TSRF: a trust-aware secure routing framework in wireless sensor networks. Int. J. Distrib. Sens Netw. **2014**(1), 1–14 (2014)
5. F Ishmanov, AS Malik, SW Kim, et al., Trust management system in wireless sensor networks: design considerations and research challenges. Trans. EmergiTelecommun. Technol. **26**(2), 107–130 (2015)
6. F Lin, JB Xiahou, ZX Xu, TCM clinic records data mining approaches based on weighted-LDA and multi-relationship LDA model. Multimed. Tools. Appl. **75**(22), 14203–14232 (2016)
7. W Wei, Q Yong, Information potential fields navigation in wireless ad-hoc sensor networks. Sensors **11**(5), 4794–4807 (2011)
8. N Marchangl, R Datta, Light-weight trust-based routing protocol for mobile ad hoc networks. IET Inf. Secur.. **6**(2), 77–83 (2012)
9. A Rasheed, RN Mahapatra, The three-tier security scheme in wireless sensor networks with mobile sinks. IEEE. Trans. Parallel. Distrib. Syst. **23**(5), 958–965 (2012)
10. J Deng, R Han, S Mishra, INSENS: intrusion-tolerant routing for wireless sensor networks. Comput. Commun.. **29**(2), 216–230 (2006)
11. A Perrig, R Szewczyk, JD Tygar, et al., SPINS: security protocols for sensor networks. Wirel. Netw **8**(5), 521–534 (2002)
12. MS Syed, HB Safdar, et al., Neighbor node trust based intrusion detection system for WSN. Procedia. Comput. Sci. **8**(3), 183 (2015)
13. H Safa, H Artail, D Tabet, A cluster-based trust-aware routing protocol for mobile ad hoc networks. Wirel. Netw. **16**(2), 969–984 (2010)
14. L Lintao, H Lei, Z Na, Hierarchical routing trust model for wireless sensor networks. Comput. Eng. **23**(6), 101–103 (2010)
15. S Ganeriwal, LK Balzano, MB Srivastava, Reputation-based framework for high integrity sensor networks. ACM. Trans. Sens. Netw. **4**(3), 66–77 (2004)
16. RA Shaikh, H Jameel, BJ D'Auriol, et al., Group-based trust management scheme for clustered wireless sensor networks. IEEE. Trans. Parallel. Distrib. Syst. **20**(11), 1698–1712 (2009)
17. R Feng, X Han, Q Liu, et al., A credible Bayesian-based trust management scheme for wireless sensor networks. Int. J. Distrib. Sens. Netw. **2015**(2), 1–9 (2015)
18. J Jiang, G Han, F Wang, et al., An efficient distributed trust model for wireless sensor networks. IEEE. Trans. Parallel. Distrib. Syst. **26**(5), 1228–1237 (2015)
19. J Hossein, RA Mohammad, et al., A fuzzy fully distributed trust management system in wireless sensor networks. Int. J. Electron. Commun.. **9**(17), 1–10 (2015)
20. Y Reddy, J Durand, S Kafle, in *Proc. of IEEE 7th International Conference on Information Technology, IEEE Press*. Detection of packet dropping in wireless sensor networks (2010), pp. 879–884
21. HU Xiangdong, W Qinfang, T Hui, Model and simulation of creditability-based data aggregation for the internet of things. Chin. J. Sci. Instrum. **31**(11), 2636–2640 (2010)
22. AR Dhakne, PN Chatur, TCNPR: trust calculation based on nodes properties and recommendations for intrusion detection in wireless sensor network. Int. J. Comput. Sci. Netw. Secur. **16**(12), 1–10 (2016)
23. J Zhang, R S Hankaran, MA Orgun, et al., in *Proc. of 2010 IEEE/IFIP 8th International Conference on Embedded and Ubiquitous Computing (EUC), Hong Kong, China*. A dynamic trust establishment and management framework for wireless sensor networks (2010), pp. 484–491
24. M Mejia, N Peña, JL Muñoz, et al., A game theoretic trust model for online distributed evolution of cooperation in MANETs. J. Netw. Comput. Appl.. **34**(1), 39–51 (2011)
25. F Bao, IR Chen, MJ Chang, et al., Hierarchical trust management for wireless sensor networks and its applications to trust-based routing and intrusion detection. IEEE Trans. Netw. Serv. Manag.. **9**(2), 169–183 (2012)
26. MK Denko, T Sun, I Woungang, Trust management in ubiquitous computing: a Bayesian approach. Comput. Commun. **34**(3), 398–406 (2011)
27. M Mendonca, JS Aguilar, N Perozo, *An Emergent Ontology for Ambient Intelligence Based on an Ant Colony Optimization Algorithm, Computing Conference (CLEI), September 15–19, 2014* (IEEE Press, Montevideo, 2014), pp. 1–11
28. F Lin, XZ Zhou, WH Zeng, Sparse online learning for collaborative filtering. Int. J. Comput. Commun. Control. **11**(2), 248–258 (2016)
29. N Iltaf, A Ghafoor, U Zia, A mechanism for detecting dishonest recommendation in indirect trust computation. EURASIP J. Wirel. Commun. Netw. 2013(1), 1–13 (2013)
30. M Majdi, K Lyes, N Hazem, Secure and robust clustering for quantized target tracking in wireless sensor networks. J. Commun. Netw. 15(2), 164–172 (2013)
31. P Padh, RK Dash, K Martinez, A utility-based adaptive sensing and multihop communication protocol for wireless sensor networks. ACM. Trans. Sens. Netw **6**(3), 27–39 (2010)