Journal of Network and Computer Applications 59 (2016) 88–94

Contents lists available at ScienceDirect

Journal of Network and Computer Applications

journal homepage: www.elsevier.com/locate/jnca

BTRES: Beta-based Trust and Reputation Evaluation System for wireless sensor networks

Weidong Fang [a,c], Chuanlei Zhang [b,*], Zhidong Shi [a], Qing Zhao [b], Lianhai Shan [c,d]

[a] Key Laboratory of Specialty Fiber Optics and Optical Access Networks, Shanghai University, Shanghai 200444, China
[b] School of Computer Science and Information Engineering, Tianjin University of Science & Technology, Tianjin 300222, China
[c] Key Laboratory of Wireless Sensor Network & Communication, Shanghai Institute of Microsystem and Information Technology, Chinese Academy of Sciences, Shanghai 200051, China
[d] Shanghai Research Center for Wireless Communications. Shanghai 200335, China

ARTICLE INFO

Available online 7 July 2015

Keywords:
WSNs
Trust evaluation
Beta distribution
Compromised nodes

ABSTRACT

Unlike traditional networks, the wireless sensor networks (WSNs) are very vulnerable to internal attacks from compromised nodes. The trust management system is the most effective way to defend the attack inside the network. The Beta-based Trust and Reputation Evaluation System (BTRES) is proposed in this paper for WSNs' node trust and reputation evaluation. BTRES is based on monitoring nodes' behavior, and beta distribution is used to describe the distribution of nodes' credibility. The node trust values are used to guide the selection of relay nodes, mitigating internal attacks risks. Simulation results show that the use of BTRES could effectively maximize the defense of internal attacks from compromised nodes and improve the WSNs' information security. In this paper, we mainly focus on the communication trust and data trust, and energy trust can be easily integrated into BTRES.

1. Introduction

Wireless Sensor Networks (WSNs) is widely used in military, industrial, agriculture and commercial fields. The security of WSNs is an important issue and they are getting more and more attention (Prathap et al., 2012). WSNs security issues in certain applications will cause economic loss and privacy issues. Therefore, WSNs security has become a hot research topic recently (Shashikala and Kavitha, 2012).

The cheap WSNs node, which is deployed in the local area, can easily be captured and attacked. What is more, due to the limitation of nodes' energy, computing and storage capability, it easily leads to a node failure or low competitiveness of selfish nodes. The attacks to WSNs are from external attacks and internal attacks. The traditional encryption and authentication schemes are mainly used against external attacks (Li et al., 2013, 2011; Meena and Jha, 2015). However, once a node is captured, it could cause key leak very easily, which cause encryption and authentication schemes failure. Therefore, for the purposes of defense against internal attack, current encryption and authentication schemes cannot satisfy WSNs' security requirements. How to defend the attack from compromised nodes or problematic nodes becomes one of the major directions in WSNs security mechanism research.

At present, the most effective way to defend internal attack is trust management system. The trust management systems are divided into three categories: trust model, trust management scheme and protocol optimization.

In terms of the trust model, Ganeriwal and Srivastava (2004) proposed a reputation-based framework for high integrity sensor networks (RFSN). This framework included five sections: direct reputation evaluation, indirect reputation evaluation, reputation synthesis, conversion and node behavior trust, which gave a complete evaluation of the general process of sensor nodes trust. Then, based on the Beta distribution and Bayesian formula, the Beta Reputation-system for Sensor Networks (BRSN) was proposed. The feasibility of Beta distribution was verified by derivation and detailed explanation of calculations for the reputation of the update, aging, indirect information and trust were elaborated. BRSN was a simple trust evaluation system and it has been widely studied and used. Jiang et al. (2015) proposed the Efficient Distributed Trust Model (EDTM) for WSNs. In this model, according to the number of packets received by sensor nodes, direct trust and recommendation trust were selectively calculated. Communication trust, energy trust and data trust were considered during the calculation of direct trust, and trust reliability and familiarity were defined to improve the accuracy of recommendation trust. Sinha and Jagannatham (2014) proposed the Gaussian trust and reputation for fading Multiple-Input Multiple-Output (MIMO) WSNs. Based on multivariate Gaussian distribution and Bayesian theorem, considering the impact of the MIMO wireless fading

* Correspondence to: 1038, Da Gu Nan Lu, 300222, Tianjin, China. Tel.: +8602262070083.
E-mail address: a17647@gmail.com (C. Zhang).

http://dx.doi.org/10.1016/j.jnca.2015.06.013
1084-8045/

channel, the authors combined the direct and indirect reputation information. The reputation and trust value was also calculated. This method could effectively isolate the malicious node, but the calculation process was too complex for energy-limited WSNs. There were some other representative researches. Zhang et al. (2010) put forward a dynamic trust establishment and management framework for WSNs. On basis of the previous trust management system of WSNs, some new measurements (for example, nodes only communicate with the cluster head and use cluster head trusted information.) were considered, which made the trust management system better. Zhu et al. (2010) put forward a Rank-based Application-driven Resilient Reputation framework Model for wireless sensor networks (RARRM). The model was application-driven and different requirements could have different trust value rank.

For the purposes of trust management scheme, Yu et al. (2010) summarized the Trust and Reputation Management (TRM) systems in wireless communication systems. The authors divided the existing TRM systems into two categories: individual-level trust models and system-level trust models. Individual-level trust models mainly focused on the trust evaluation of one node to another node; but the system-level trust models included trust and reputation evaluation model and protocol, where reward and punishment were made based on the node's reputation. Through the examples of the major individual level model, the author introduced the trust and credibility of the initial stage, evaluated the reputation of the direct and indirect aspects of synthesis and guided trust evaluation and decision-making. The authors also presented several reward and punishment mechanism for system-level trust model. At last, the advantage and disadvantage of TRM systems were summarized. Duan et al. (2014) proposed the trust derivation scheme based on game theory. At first, the authors analyzed the network security requirements and mechanisms. Then, under the premise of ensuring network security, a risk model was exhibited to stimulate the cooperation of WSNs node to derive an optimal number of cooperating nodes. At last, the game theoretic approach was applied to the trust derivation process to reduce the overhead of the process. Li et al. (2013) proposed a Lightweight and Dependable Trust System (LDTS) for clustered WSNs. Firstly, the author proposed a lightweight trust decision scheme based on node identity clustering of WSNs. Then, by eliminating feedback between cluster members and Cluster Heads (CHs), the system efficiency was greatly improved and the harm of malicious nodes was reduced. At last, because of the significance of cluster head which undertakes a lot of data transition tasks, a trust evaluation method was defined for interaction of CHs. What is more, an adaptive weighting method was defined. Hui-hui et al. (2009) summarized the trust evaluation in WSNs as: communication trust, data trust and energy trust. Communication trust meant the relationship value calculated between two cooperation nodes in a wireless sensor network which can send or receive information from each other. Data trust refered to the trust assessment of the fault tolerance and consistency of data. Energy trust in WSNs refered to the relationship between the remaining energy of a node and the energy threshold necessary to complete a new communications and data-processing tasks. In addition, Li et al., (2010) presented a data-centric trust evaluation mechanism in WSNs (DTSN). Because WSN was a data-centric network, the traditional trust evaluation based on entities could not apply to WSNs. Shaikh et al. (2009) proposed a group-based trust management scheme for clustered WSNs. In this trust management scheme, energy consumption was considered firstly. The approach reduced the cost of trust evaluation. Zia and Islam (2010) presented a solution based on Communal Reputation and Individual Trust (CRIT) for WSNs. The nodes' behaviors were monitored by a watch dog, and each node had a trust table and a reputation table for its adjacent nodes. Ukil (2010) proposed a trust and reputation based collaborating computation, and the optimum path could be chosen by this scheme. Ishmanov and Kim (2011) presented a secure trust establishment for WSNs. Unlike traditional trust evaluation mechanism, this mechanism only considered the impact of the abnormal node behavior. Bao et al. (2011), (2012) proposed the trust-based intrusion detection and a hierarchical trust management for WSNs which is applied to trust-based routing and intrusion detection. In addition, the selection of minimum trust threshold was also analyzed, where Zhu et al. (2014) built a trust and reputation management system for cloud and sensor networks integration.

In protocol optimization, Gheorghe et al. (2013) proposed an Adaptive Trust Management Protocol (ATMP) based on intrusion detection. The ATMP, which was applied to TinyOS system, could defend varous kinds of attack with combination of TinyAFD common intrusion detection framework. The protocol included three phases: (1) Learning phase, in which experience was computed based on these alerts received from TinyAFD, (2) exchanging phase, in which experience associations were exchanged between neighbor nodes and (3) updating phase, in which trust and reputation were updated based on experience. This protocol was simple and could only be applied in TinyOS system. But it did not take into account the node residual energy problems. According to the sensor nodes' behaviors on event perception, packet forwarding and data aggregation, Fang et al. (2013) proposed a reputation management scheme, which described the initialization, update, and storage of the reputation value and the punishment and redemption of malicious nodes. When the scheme was applied to the Security Privacy In Sensor Network (SPIN) protocol, a new trust enhanced routing protocol based-on reputation was propose the results of the simulation indicated that the trust enhanced routing protocol improved the data forwarding rate and delivery success rate in distrusted environment for WSNs. Tajeddine et al. (2011) put forward a centralized TRust And Competence-based Energy-efficient routing scheme for wireless sensor networks (TRACE). In TRACE, using centralized management of sinks made routing more efficient and secure. On this basis, Tajeddine et al. (2012) proposed a CENtralized Trust-based Efficient Routing protocol for wireless sensor networks (CENTER). In the protocol, the BS calculated different quality metrics - namely the maliciousness, cooperation, compatibility and approximation of the battery life, which could evaluate the Data Trust and Forwarding Trust values of each node. Then, the BS used an effective technique to isolate all “bad” nodes, which was misbehaving or malicious based on their history. At last, the BS used an efficient method to disseminate updated routing information, indicating the uplinks and the next hop downlink for each node. Others include: Li et al. (2015) proposed a new authentication protocol for healthcare applications using wireless medical sensor networks with user anonymity. Gerrigagoitia et al. (2012) proposed a new IDS design based on reputation and trust of the different nodes of a network for decision-making and analysis of possible sources of malicious attacks. Arijit (2010) put forward a trust and reputation based collaborating computing model. The detection of malicious nodes along with trust and reputation analysis of WSNs made this model robust and secure.

The trust management system has been developed for many years. The definitions of trust and credibility are dependent on the specific application (Momani 2010). In WSNs, the trust generally refers to the reliability of forecasting future behavior of one node to another one. Trust generally is a fixed value. Whether two nodes interact or not is decided by the trust value. On the other hand, although BRSN has been widely studied and used, it only defend several classical internal attacks, such as black hole attack, Sybil attack, and so on. In this paper, based on the interaction of nodes and beta distribution, we propose the Beta-based Trust and Reputation Evaluation System (BTRES) to guide the interaction of

nodes, which can avoid the attack from internal nodes. In the proposed scheme, we mainly focus on the communication trust and data trust. Energy trust can be easily integrated into our system. Optimization is made based on the BRSN, which makes the algorithm of the trust evaluation system more effective, and can effective defend collusion attack. The rest of this paper is organized as follows: Section 2 gives a brief review of BRTES. The simulation results and analyses of the proposed system are presented in Section 3. Finally, some concluding remarks are provided in Section 4.

2. Preliminary knowledge

In this section, we give a brief introduction of the Beta Distribution (Ganeriwal and Srivastava, 2004), which is the security basis of our enhanced scheme. The detailed information about the Beta Distribution and Beta reputation system for sensor networks can be found in literature (Ganeriwal and Srivastava, 2004). Here we briefly introduce the Beta Distribution.

When the interaction between two nodes happens, there are two cases. For communication trust, the cases generally refer to transmission of data, which include cooperation and noncooperation cases. For data trust, the cases generally refer to the aggregation of data, which include correct transmission and error transmission. Therefore, binomial distribution can be employed to simulate the interaction between two nodes. But for the Bayes analysis, beta distribution is usually used for the conjugate prior distribution of binomial distribution parameters, where the beta distribution is flexible and simple, so it can be used for simulating the trust distribution.

There are two parameters (a, b) in beta distribution, which can be described by gamma function:

$$P(x)=\frac{\Gamma(a+b)}{\Gamma(a)\Gamma(b)}x^{a-1}(1-x)^{b-1} \quad \forall 0\le x\le 1, a\ge 0, b\ge 0 \tag{1}$$

Suppose there are $(a+b)$ times interactions between the nodes. For the communication aspect, a is the number of cooperation interaction, and b represents the number of noncooperation interaction. For the data trust aspect, a represents the number of normal data transmission interaction, and b represents the number of error data transmission interaction. Usually, the distribution of sensor nodes is concentrated, and the correlation of interproximal nodes is very high, so we define a threshold valueη. When the difference of one node and its adjunct node is higher than the threshold valueη, it it means data error happens. When there is no prior information, the action of nodes complies with uniform distribution,$P(x)=uni(0,1)=Beta(1,1)$. For the prediction of node's action, beta distribution can be utilized to get the probability distribution of node reputation P:

$$P(x)=\frac{Bin(a+b,a)*Beta(1,1)}{Normalization}=\frac{Bin(a+b,a)*Beta(1,1)}{a+b+1}$$
$$=Beta(a+1,b+1) \tag{2}$$

Eq. (2) shows that the interactions of nodes are subject to beta distribution. Therefore, beta distribution meets the requirements of trust evaluation.

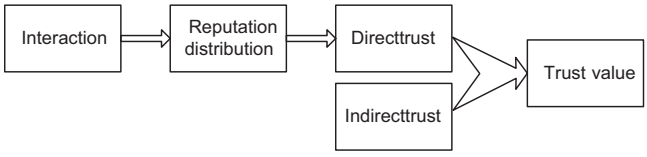

Fig. 1. The process of node trust evaluation.

3. Beta-based Trust and Reputation Evaluation System (BTRES)

The Beta-based Trust and Reputation Evaluation System is proposed in this section and the process of establishing the BTRES is given in detail.

3.1. Trust evaluation process

When the interaction between node i and node j happens, node i will evaluate the trust value of node j, and then decide whether to interact or not. The process of trust evaluation is shown in Fig. 1. At first, node i calculates the reputation distribution of node j based on the existing interaction information. Then, the direct trust value is obtained based on the reputation distribution. At last, a broadcast signaling is transmitted from node i to the adjacent node to ask for the trust value of node j, which will be used for the final trust value calculation as the indirect trust value. The whole process is shown in Fig. 2.

3.2. Simulation of reputation and trust

When we calculate the trust and reputation values, both communication trust and data trust are considered. Based on the beta distribution, the reputation of node i to node j is expressed as

$$R_{ij}=Beta(a+1,b+1) \tag{3}$$

Direct trust evaluation refers to the statistical expectation of reputation function is:

$$DT_{ij}=E(R_{ij})=\frac{a+1}{a+b+2} \tag{4}$$

Eq. (3) shows that only a and b are stored when a node is evaluated.

3.3. Reputation update

Suppose that the reputation indicator R_{ij} of node i and node j is established. Interaction between node i and node j remains $(r+s)$ times, where r represents the number of normal cooperation and s represents the number of data transmission error. The target is to obtain the reputation R_{ij} of node j.

$$R_{ij}=\frac{Bin(r+s,r)*Beta(a+1,b+1)}{Normalization}=\frac{Bin(r+s,r)*Beta(a+1,b+1)}{\frac{(a+r)!(b+s)!(r+s)!(a+b+1)!}{a!b!r!s!(a+b+r+s+1)!}}$$
$$=Beta(a+r+1,b+s+1) \tag{5}$$

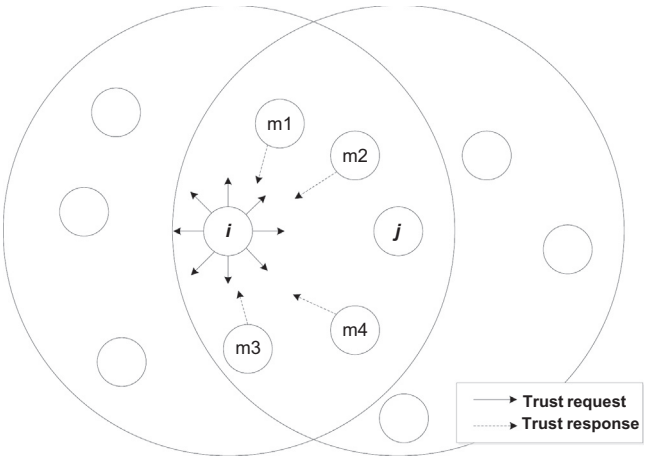

Fig. 2. The process of indirect trust request.

Eq. (5) is normalization operation. We expand $Bin(r+s,r)$ and $Beta(a+1,b+1)$on the left side of the equation, and compare the expansion products with that of $Beta(a+r+1,b+s+1)$on the right side. Then we can derive that the *Normalization* term is

$$\frac{(a+r)!(b+s)!(r+s)!(a+b+1)!}{a!b!r!s!(a+b+r+s+1)!}.$$

Therefore, the update of reputation includes two parameters:

$$a^{new}=a+r\ ,\ \ b^{new}=b+s \tag{6}$$

3.4. Aging

The new data has more weight, so the aging weight value is added:

$$a^{new}=(w_{age}*a)+r\ ,\ \ b^{new}=(w_{age}*b)+s \tag{7}$$

w_{age} is aging weight, and its value range is (0, 1). The aging weight makes sure that all the nodes cooperate together. One compromised node can choose the start strategy, and then the data can be used to describe the reputation-destroyed network. The suitable aging weight value can keep the data from being old. Nodes need to cooperate together to keep a good reputation.

3.5. Indirect information

Suppose node i can evaluate the trust value of adjacent m nodes and node i receive an indirect trust evaluation of node j from these nodes. The indirect information of node x to node j can be expressed as$\left(a_j^x,b_j^x\right)$. Node i already have the reputation information of node j and other adjacent nodes, which can be described as (a_j,b_j) and (a_k,b_k). We combine this information together to get the new reputation of node j as$\left(a_j^{new},b_j^{new}\right)$. New reputation value $\left(a_j^{new},b_j^{new}\right)$ is other node's trust value

$$T_{ij}=\alpha\cdot DT_{ij}+\sum_{x=1}^{m}\beta_x\cdot IT_{xj}=\alpha\cdot DT_{ij}+\beta\cdot\sum_{x=1}^{m}\gamma_x\cdot$$
$$DT_{xj}=\alpha\cdot\frac{a_j+1}{a_j+b_j+2}+\beta\cdot\sum_{x=1}^{m}\gamma_x\cdot\frac{a_j^x+1}{a_j^x+b_j^x+2} \tag{8}$$

Eq. (8) shows that the trust value of node is composed of indirect trust and direct trust. $IT_{xj}$is the indirect trust value of node x to node j; where m means the number of adjacent nodes. α and β are weights of direct evaluation and indirect evaluations respectively, where $\alpha+\beta=1$. Generally speaking, direct evaluation has more weight. γ_x represents the weight of every adjacent node, which is related to the direct evaluation of node i to each of its adjacent nodes. $\sum_{x=1}^{m}\beta_x\cdot IT_{xj}$represents the sum of adjacent nodes' indirect evolution, where it equals. $(a_j+1)/(a_j+b_j+2)$ and $(a_j^x+1)/(a_j^x+b_j^x+2)$ are direct evaluation and adjacent nodes' indirect evaluations.

$$\gamma_x=\frac{DT_{ix}}{\sum_{x=1}^{m}DT_{ix}}=\frac{\frac{a_x+1}{a_x+b_x+2}}{\sum_{x=1}^{m}\frac{a_x+1}{a_x+b_x+2}} \tag{9}$$

3.6. Reputation transfer

Because node will use the indirect information to calculate the trust value, there is information transmission between nodes. In order to avoid an information loop, only direct trust can be transferred between nodes. The direct trust value of one node is the indirect trust value of another node. Then the value will be combined with its direct value to obtain the final trust value.

3.7. Defense of internal attacks

The selective forwarding attack is defined when the compromised node selectively discards part of packets which is necessary to forward. The selective forwarding attack is one of the major security threats of WSNs. If a compromised node discards all the packets, it is defined as black hole attack. Through the above analysis, we can see that, based on the interaction of nodes, utilizing our trust evaluation system could effectively defend both the selective forwarding attack and black hole attack. Briefly, the reputation value of these compromised nodes will continue to decrease with time going.

Slander attack is defined as the action that a compromised node transfers the unfair deny evaluation of normal node to decrease its reputation. What is more, a compromised node can also work like a normal node and cumulate high enough reputation in order to provide trust evaluation error for other compromised nodes, which is defined as collusion attack. The threshold value θ can be set to filter the indirect evaluation, where difference is too much. By this way, the slander attack and the collusion attack can be reduced. The diagram is shown in Fig. 3.

4. Simulation and analyses

In the initial stages, the initial trust value is 0.5, $a=b=0$. Suppose node i will assess the trust value of adjacent node j, and the trust value is updated for each interaction. Assume that the signal channel is ideal, and there is no packet loss. The aging weight w_{age} is 0.9. Suppose the adjacent node number of node j is 3, and the weight values$\alpha=0.6$, $\beta=0.4$. Threshold value$\theta=20\%$. The cases of normal node, compromised node, adjunct nodes including compromised node are respectively evaluated and compared with BRSN.

4.1. Scene 1

Suppose node i and node j are normal, and the adjacent node of node i is normal. Node i wants to interact with node j, so node j will do the trust evaluation to node i. (Table 1).

Because node j is normal, it can interact with node i. and update the trust value of node i to node j as $(r, s)=(1, 0)$. Suppose the trust value of node i to adjacent three nodes as (1, 7), (4, 4) and (7, 1), which represent the trust evaluation as being good, medium, poor respectively. For the trust evaluation of adjacent nodes to node j, we consider two cases:

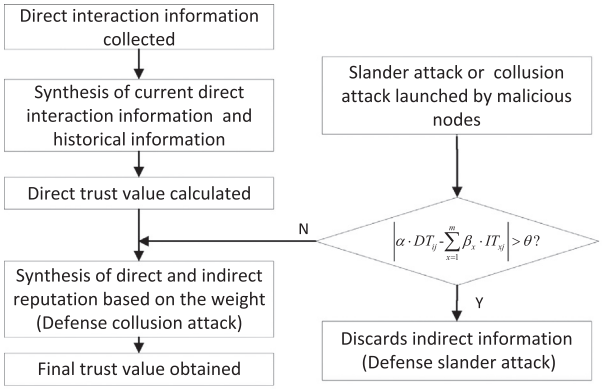

Fig. 3. Trust evolution process as well as attack and defense.

Table 1
Simulation parameters for scene 1 and scene 2.

Evaluation node's to target node's initial interaction information (a,b)	(0,0)
Direct and indirect reputation information weights (α,β)	(60%,40%)
Aging weight w_{age}	0.9
Threshold value.θ	20%
Evaluation node to three adjacent node's initial reputation information	(1,7), (4,4), (7,1)
Target node to three adjacent node's initial interaction information (initial values are not the same)	(1,5), (2,0), (10,1)
Target node to three adjacent node's initial interaction information (initial values are the same)	(0,0), (0,0), (0,0)

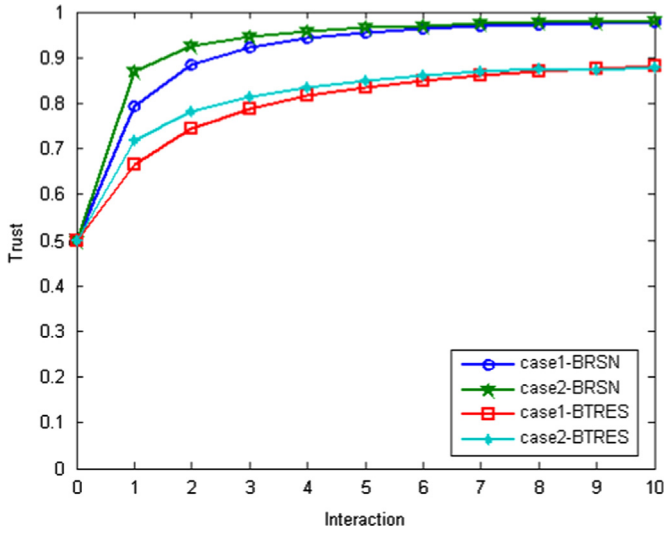

Fig. 4. Trust evaluations of normal nodes.

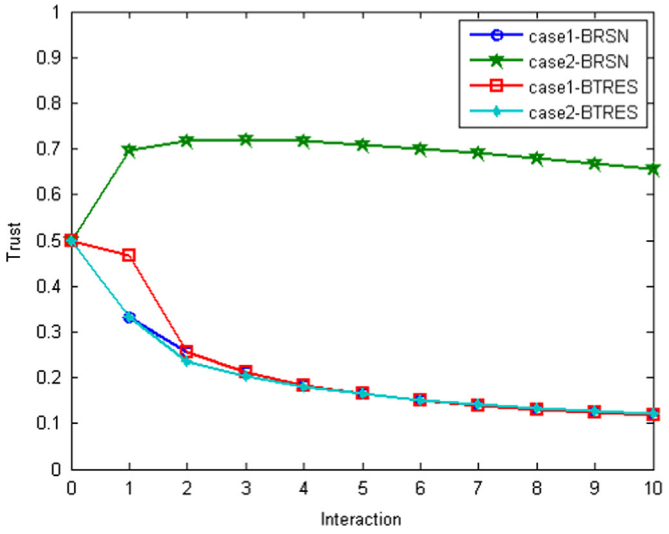

Fig. 5. Trust evaluations of compromised nodes.

When j node to three adjacent node's initial interaction
1) information are the same, we suppose that the three initial values are (0, 0).
2) When j node to three adjacent node's initial interaction information are different, we suppose that the three initial values are (1, 5), (2, 0) and (10, 1).

The simulation result of node i to node j is shown in Fig. 4.

4.2. Scene 2

Suppose the adjacent node j of node i is a compromised one, and the other adjacent node of node i is normal. When node i want to interact with node j, it will do the trust evaluation to node j.

Because the node j is compromised, the interaction between node i and j will not happen. Trust value of node i to node j is $(r, s)=(0, 1)$. Suppose the reputation of three adjacent nodes of node i is (1, 7), (4, 4) and (7, 1), which represent the evaluation results as being good, medium and poor respectively. For the reputation evaluation of adjacent nodes to node j, we consider two cases:

1) When node j's initial interaction information with its three adjacent nodes are the same, we suppose that the three initial values are (0, 0).
2) When node j's initial interaction information with its three adjacent nodes are different, we suppose that the three initial values are (10, 1), (2, 0) and (1, 5).

Simulation of trust value of node j is shown in Fig. 5. (Table 2).

4.3. Scene 3

Suppose the adjacent nodes of node j are compromised nodes. There are compromised nodes in its adjacent nodes. The node i wants to interact with node j and it need do the trust evaluation to node j.

Because node j is normal one, so node i will not interact normally. The reputation value of node i to node j is updated as $(r, s)=(0, 1)$. Suppose the trust evaluation results of the node i to its adjacent three nodes are (7, 1), one of the adjacent nodes is normal node, and the other two are compromised nodes. Suppose the initial trust evaluation results of node j are (2, 2), (3, 1) and (3, 1). Then the normal nodes make the correct evaluation to node j, and the compromised nodes will do the collusion attack. Compared with BRSN, the proposed BTRES can quickly reduce the trust value of compromised nodes to achieve the rapid identification purposes. And the simulation results of trust value of node i to node j is shown in Fig. 6.

4.4. Scene 4

Suppose node j is normal to node i, and there are compromised ones in its adjacent nodes. The node i wants to interact with node j and it will do the trust evaluation to node j.

Because node j is normal, so node j can interact with node i normally. Trust value is updated as $(r, s)=(1, 0)$. Suppose that the evaluation value of the node i to adjacent three nodes are all (7, 1), one of its adjacent nodes is normal node, and other two nodes are compromised ones. Suppose that the initial results of node j are (2, 2), (1, 3) and (1, 3), then the normal nodes do the correct reputation evaluation to node j, and compromised node does the slander attack to node j. The proposed BTRES can achieve better identification purpose than BRSN. The simulation results of trust value of node i to node j is shown in Fig. 7.

In the early network establishment process, the interaction between nodes is infrequent and the trust value between them has not been stabilized yet. However, due to the energy

Table 2
Simulation parameters for scene 3 and scene 4.

Evaluation node's to target node's initial interaction information (a,b)	(0,0)
Direct and indirect reputation information weights (α,β)	(60%, 40%)
Aging weight w_{age}	0.9
Threshold value θ	20%
Evaluation node to three adjacent node's initial reputation information	(7,1), (7,1), (7,1)
Target node to three adjacent node's initial interaction information (initial values are not the same)	(2,2), (3,1), (1,3)
Normal adjacent node	1
Malicious adjacent node	2, 3

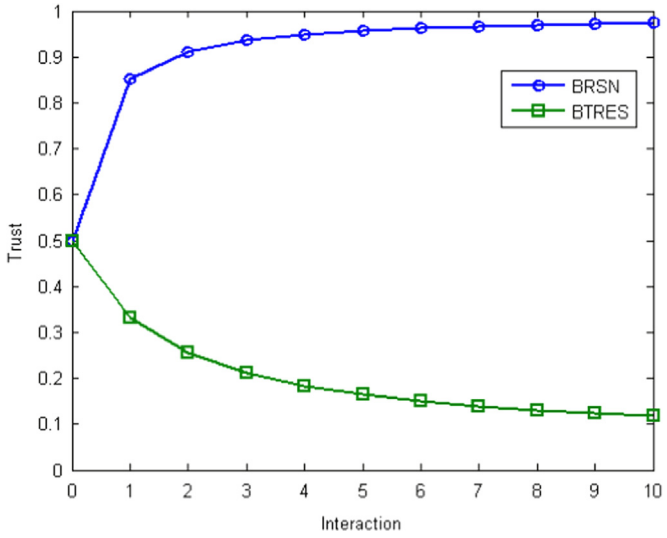

Fig. 6. Trust evaluations of compromised nodes when the collusion attack happens.

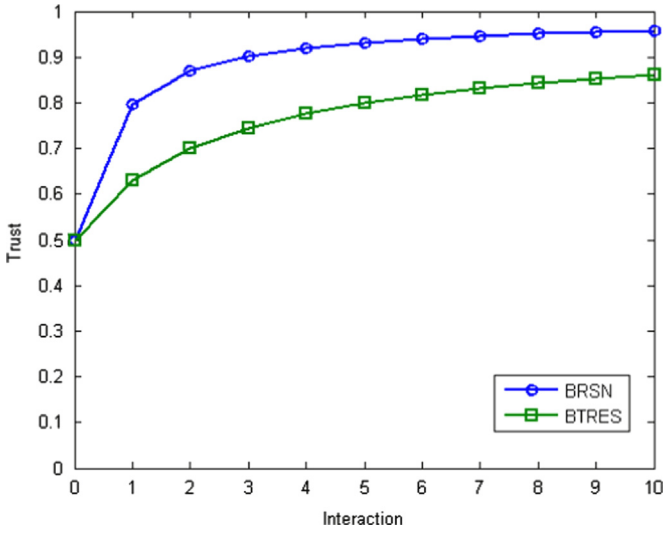

Fig. 7. Trust evaluations of compromised nodes when a Slander attack happens.

consumption problems of WSNs, there will be failure nodes and new added nodes. Therefore, these cases will affect the trust evaluation and cause the inaccurate results.

Based on the above simulation results, when BRSN and BTRES are applied to normal node evaluation, the trust value of normal nodes is increasing and the performance of BRSN and BTRES are both good, as shown in Fig. 4. But for the compromised node evaluation, as shown in Fig. 5, we can see that adjacent nodes have smaller influence in our proposed scheme than BRSN. Fig. 6 shows that BRSN cannot defend collusion attack, but BTRES can defend collusion attack effectively. Fig. 7 shows that, for slander attack, although BRSN and BTRES have the similar performance, the proposed scheme BTRES postpone the recovery of trust value, compared with the BRSN, and can effectively mitigate the impact of attack.

In brief, for the prevention of normal nodes evaluation from slander attack, BTRES and BRSN have the similar performance. But for the compromised nodes, BTRES performs better on the defense of adjacent nodes affect than BRSN, which makes the results more accurate. And BTRES solve the collusion attack problems which BRSN cannot solve.

5. Conclusions

This paper proposed a trust reputation evaluation system based on the beta distribution for WSNs to defend the internal attack of compromised nodes. The BTRES uses the beta distribution to simulate the nodes′ reputation, and then calculate the trust value. By setting weight and threshold value, collusion attack of compromised nodes can be effectively defended. The trust value of nodes can be utilized in routing protocols or the mechanism of aggregation. The node with higher trust value will be considered first in the selection of routing path or aggregating data, and the proposed system can ensure network security. Because the WSNs nodes have constraint in resources, include computing, storage and energy supply, the energy consumption will be considered for the research of trust management system in the future.

Acknowledgment

This work is partially supported by the National Natural Science Foundation of China (61302113), the Shanghai Natural Science Foundation (13ZR1440800), the Shanghai Rising-Star Program (14QB1404400) and Shanghai Key Laboratory of Specialty Fiber Optics and Optical Access Networks (SKLSFO 2014-03). It was partly funded by the Young Academic Team Construction Projects of the 'Twelve Five' Integrated Investment Planning in Tianjin University of Science and Technology.

References

Arijit U. Trust and reputation based collaborating computing in wireless sensor networks[C]//computational intelligence, modelling and simulation. In: Proceedings of the second international conference on IEEE. 2010. p. 464–469.

Bao F., Chen R., Chang M.J., et al. Trust-based intrusion detection in wireless sensor networks[C]//communications (ICC). In: Proceedings of the 2011 international conference on IEEE. 2011. p. 1–6.

Bao F, Chen R, Chang MJ, et al. Hierarchical trust management for wireless sensor networks and its applications to trust-based routing and intrusion detection. Network and Service Management, IEEE Trans 2012;9(2):169–83.

Duan J, Gao D, Yang D, et al. An energy-aware trust derivation scheme with game theoretic approach in wireless sensor networks for iot applications. Internet Things J, IEEE 2014;1(1):58–69.

Fang F., Li J., Li J. A reputation management scheme based on multi-factor in WSNs [C]//mechatronic sciences, electric engineering and computer. In: Proceedings of the international conference on. IEEE. 2013. p. 3843–3848.

Ganeriwal S., Srivastava M.B. Reputation-based framework for high integrity sensor networks. In: proceedings of the second ACM workshop on security of ad hoc and sensor networks (SASN'04). Washington (D.C., USA): ACM; 2004. p. 66–77.
Gerrigagoitia K, Uribeetxeberria R, Zurutuza U, et al. Reputation-based intrusion detection system for wireless sensor networks[C]//complexity in engineering. IEEE 2012:1–5.
Gheorghe L., Rughinis R., Tataroiu R. Adaptive trust management protocol based on intrusion detection for wireless sensor networks. In: proceedings of the networking in education and research, 2013 RoEduNet international conference 12th Edition IEEE. 2013. p. 1–7.
Hui-hui D., Ya-jun G., Zhong-qiang Y., et al. A wireless sensor networks based on multi-angle trust of node. In: Proceedings of the international forum on information technology and applications IFITA'09, 2009, IEEE. 1, 2009. p. 28–31.
Ishmanov F., Kim S.W. A secure trust establishment in wireless sensor networks [C]//electrical engineering and informatics (ICEEI). In: Proceedings of the 2011 international conference on. IEEE. 2011. p. 1–6.
Jiang J, Han G, Wang F, et al. An efficient distributed trust model for wireless sensor networks. IEEE Trans Parallel Distrib Syst 2015;26(5):1228–37.
Li M., Hu J., Du J. A data-centric trust evaluation mechanism in wireless sensor networks[C]//distributed computing and applications to business engineering and science (DCABES). In: Proceedings of the ninth international symposium on 2010 IEEE. 2010. p. 466–470.
Li X, Zhou F, Du J. LDTS: a lightweight and dependable trust system for clustered wireless sensor networks. IEEE Trans Inf. Forensics Secur 2013;8(6):924–35.
Li Xiong, Niu Jianwei, Ma Jian, Wang Wendong, Liu Chenglian. Cryptanalysis and improvement of a biometrics-based remote user authentication scheme using smart cards. J Netw Comput Appl 2011;34(1):73–9.
Li Xiong, Niu Jianwei, Khurram Khan Muhammad, Liao Junguo. An enhanced smart card based remote user password authentication scheme. J Netw Comput Appl 2013;36(5):1365–71.
Li Xiong, Niu Jianwei, Kumari Saru, Liao Junguo, Liang Wei, Khurram Khan Muhammad. A new authentication protocol for healthcare applications using wireless medical sensor networks with user anonymity. Secur Commun Netw 2015, . http://dx.doi.org/10.1002/sec.1214 accepted, Jan..
Meena, U.m.a., Jha, M.K. An efficiency model for authentication approaches in WBAN. In: Proceedings of the 2015 second international conference on computing for sustainable global development (INDIACom), IEEE. 2015. p. 476–481.
Momani M. Trust models in wireless sensor networks: a survey. Recent Trends in Network Security and Applications. Berlin Heidelberg: Springer; 37–46.
Prathap U., Shenoy D.P., Venugopal K.R., et al. Wireless sensor networks applications and routing protocols: survey and research challenges. In: Proceedings of the 2012 IEEE international symposium on cloud and services computing (ISCOS). 2012. p. 49–56.
Shaikh RA, Jameel H, d'Auriol BJ, et al. Group-based trust management scheme for clustered wireless sensor networks. Parallel Distrib Syst, IEEE Trans 2009;20 (11):1698–712.
Shashikala, Kavitha, C.. A survey on secured routing protocols for wireless sensor network. In: Proceedings of the 2012 IEEE third international conference on. computing communication & networking technologies (ICCCNT). 2012. p. 1–8.
Sinha R.K., Jagannatham A.K., Gaussian trust and reputation for fading MIMO wireless sensor networks. In: Proceedings of the 2014 IEEE international conference on electronics, computing and communication technologies (IEEE CONECCT). 2014. p. 1–6.
Tajeddine A., Kayssi A., Chehab A. TRACE: a centralized trust and competence-based energy-efficient routing scheme for wireless sensor networks[C]//wireless communications and mobile computing conference (IWCMC). In: Proceedings of the 2011 seventh international conference on IEEE. 2011. p. 953–958.
Tajeddine A., Kayssi A., Chehab A. CENTER: a centralized trust-based efficient routing protocol for wireless sensor networks[C]//privacy, security and trust. In: Proceedings of the tenth annual international conference on IEEE. 2012. p. 195–202.
A. Ukil, Trust and reputation based collaborating computing in wireless sensor networks[C]//computational intelligence, modelling and simulation (CIMSiM). In: Proceedings of the 2010 s international conference on IEEE. 2010. p. 464–469.
Yu H, Shen Z, Miao C, et al. A survey of trust and reputation management systems in wireless communications. Proc IEEE 2010;98(10):1755–72.
Zhang J., Shankaran R., Orgun M.A., et al. A dynamic trust establishment and management framework for wireless sensor networks[C]//embedded and ubiquitous computing (EUC). In: Proceedings of the 2010 IEEE/IFIP eighth international conference on. IEEE. 2010. p. 484–491.
Zhu C., Nicanfar H., Leung V., et al. A trust and reputation management system for cloud and sensor networks integration[C]//communications (ICC). In: Proceedings of the 2014 IEEE international conference on IEEE. 2014. p. 557–562.
Zhu M., Chen H., Wu H. A rank-based application-driven resilient reputation framework model for wireless sensor networks[C]//computer application and system modeling (ICCASM). In: Proceedings of the 2010 international conference on IEEE. 2010. 9, V9-125-V9-129.
Zia T.A., Islam M.Z. Communal reputation and individual trust (CRIT) in wireless sensor networks[C]//availability, reliability, and security. In: Proceedings of the 2010 ARES'10 international conference on IEEE. 2010. p. 347–352.