SCIENCE CHINA
Information Sciences

• RESEARCH PAPER •
Special Focus on Mobile Network Virtualization

April 2017, Vol. 60 040305:1–040305:11
doi: 10.1007/s11432-016-9028-0

A resilient trust management scheme for defending against reputation time-varying attacks based on BETA distribution

Weidong FANG[1], Wuxiong ZHANG[1,2]*, Yang YANG[1,2], Yang LIU[1,2] & Wei CHEN[3]

[1]*Key Laboratory of Wireless Sensor Network & Communication, Shanghai Institute of Microsystem and Information Technology, Chinese Academy of Sciences, Shanghai* 201899*, China;*
[2]*Shanghai Research Center for Wireless Communication, Shanghai* 201210*, China;*
[3]*School of Computer Science and Technology, China University of Mining and Technology, Xuzhou* 221116*, China*

Received December 7, 2016; accepted January 23, 2017; published online March 6, 2017

Abstract Compared with the encryption and the authentication which can prevent the external attacks, the trust management schemes are the better approaches for defending against the internal attacks in wireless sensor network (WSN). The reputation time-varying (RTV) attacks are internal attacks. In the reputation time-varying attacks, the reputation value of nodes is manipulated to adjust dynamically by the compromised nodes or malicious attackers. Hence, these attacks have greater covert and invasive. In this paper, we propose a Time-window-based Resilient Trust Management Scheme (TRTMS) to defend against the reputation time-varying attacks in wireless sensor network. In this scheme, based on BETA distribution, the behaviors of compromised nodes are analyzed for a period of time, and then the difference judgment and the trend analysis are utilized to identify the abnormality of nodes' reputation value, meanwhile, the control factor F_c and the time window are introduced to verify and remove the compromised modes from the suspected malicious nodes, which refer to those nodes' reputation value changes are caused by the wireless channel changes. The result of simulation shows that our proposed scheme can defend reputation time-varying attacks effectively and it is convenient to implement.

Keywords wireless sensor network (WSN), reputation time-varying attack, trust value, trust management, time window

Citation Fang W D, Zhang W X, Yang Y, et al. A resilient trust management scheme for defending against reputation time-varying attacks based on BETA distribution. Sci China Inf Sci, 2017, 60(4): 040305, doi: 10.1007/s11432-016-9028-0

1 Introduction

The wireless sensor network (WSN) originates from military fields, and has been widely applied to the industry, the commerce, and the transportation. For the wireless sensor network, the industry focuses on its applications, which involve the smart city [1], the intelligent transportation [2], the environmental monitoring [3], and so on, meanwhile, the academia aims at its key technologies. They include the routing protocols and access protocols [4], the image processing and the target tracking [5], the cooperative

* Corresponding author (email: wuxiong.zhang@mail.sim.ac.cn)

communication [6], the energy balance and energy efficiency [7]. However, there is an issue that is concerned by both academia and industry. This issue is the information security. Recently, many security incidents are disclosed in WSN, and its security issues have been a hot spot.

The requirements of the security come from the attacks. For the wireless sensor network, the attacks are classified as the external attacks and the internal attacks. The researches have shown that the internal attacks are more danger than the external attacks. The internal attacks involve the internal nodes' (compromised node, Byzantine node, etc.) attack behavior and some internal nodes in order to save energy to take selfish behavior. The traditional security scheme (encryption scheme, authentication scheme) is invalid for the internal malicious nodes. Hence, the internal attacks are more easily to intrude and destroy the wireless sensor network.

The trust management is an effective approach to detect and defend against the internal attacks. Some trust managements are mainly proposed to defend against the Sybil attack, the wormhole attack, the slander attack, and the conspiracy attack. Currently, many trust managements focus on the specific attack behaviors, the behavior analysis of the suspected malicious nodes is seldom concerned over a period of time. In this paper, a Time-window-based Resilient Trust Management Scheme (TRTMS) to defend against the reputation time-varying attacks is proposed in wireless sensor network. In the proposed scheme, the communication trust and the data trust are focused on. On the basis of the analysis of the BRSN (BETA Reputation system for Sensor Networks) [8], the abnormality of nodes' reputation value is identified by the difference judgment and the trend analysis, the time window is introduced to judge the attack behavior. The rest of this paper is organized as follows: a brief review of trust managements and trust models are given in Section 2. The proposed scheme is presented to defend against the RTV attacks in Section 3. Then, the TRTMS is simulated and analyzed in Section 4. Finally, some concluding remarks are provided in Section 5.

2 Related works

The reputation is based on the events and the evaluation of the neighbor nodes, and the trust is a reputation-derived entity. The trust is the quantification of reputation, which is a specific value, and itself is built on time. Based on the historical behavior, it may provide positive or negative evaluation. Meanwhile, the trust management system is a broad concept, contains all the content related to trust. In the wireless sensor network, the management system is an effective approach to detect and defend against the internal attacks in recent years. At present, the researches on the WSN's trust management system mainly focus on the trust model and the trust management scheme.

For the purposes of the trust model, Saurabh and Mani put forward the Reputation-based framework for high integrity sensor network, which revealed that the node owns the reputation from other nodes and evaluated their trust value. It could solve the problem from malicious and wrong node by extensible, diverse, and generalized solutions. Based on the framework, they put forward the BETA Reputation system for Sensor Network (BRSN) [8]. And then, Yang et al. [9] proposed a reputation-based model for malicious node detection to resist Byzantine behaviors and selfish behaviors of internal nodes in WSN. In the proposed modelthe indirect reliability of the third-party nodes was introducedand the trust values of nodes belonging to different types of attacks were integrated. Jiang et al. [10] presented the Efficient Distributed Trust Model (EDTM), which contained direct trust (including communication trust, energy trust and data trust), recommendation trust and indirect trust. He et al. [11] put forward an application-independent and distributed trust evaluation model for the medical sensor networks. In the model, the trust management was carried out through the use of simple cryptographic techniques. The proposed model could effectively identify malicious behaviors of nodes, and thereby exclude them. Meghanathan [12] designed and proposed a distributed trust evaluation model for data aggregation in mobile sensor networks. In the model, due to the dynamic nature of the network topology, each node maintained a trust score estimate list for its neighbor nodes, based on the beacon data gathered in the neighborhood. Once the estimated trust score for one of its neighbor node fell below a threshold, this

sensor node classified it as a "Compromised or Faulty" (CF) node, then, all forward data was discarded or filtered via this CF node. UmaRani et al. [13] proposed an Enhanced Beta Trust Model (EBTM) to detect the malicious attack. The proposed model could improve the collaboration among sensor nodes by trust value, and prolong lifetime of network by recovery phase. Wang and Liu [14] presented a trust model based on changeable sampling frequency. In this model, the dynamic character of nodes in WSN was provided to help decide the weight between interactive factors. The trust model could be used in fault detection. Additionally, Xia et al. [15] presented an information theoretic framework to quantitatively measure trust, and then built a novel trust model (FAPtrust) with multiple trust decision factors, which were incorporated to reflect trust relationship's complexity and uncertainty in various angles. Meanwhile, the weight of these factors was set up using fuzzy analytic hierarchy process theory based on entropy weight method, which made the model better rationality. Moreover, the fuzzy logic rules prediction mechanism was adopted to update a node's trust for future decision-making. From above mentions, since the BRSN was proposed, some subsequent researchers on trust model have mainly concerned about identifying the high-reputed malicious nodes, the malicious recommendation and the slander behavior of the high-reputed nodes, such as EDTM, EBTM, FAPtrust, etc. Although, from the current perspective, there were some imperfections in BRSN, it gave us a basis for abstract analysis, as well as the trust modeling approach. So far, many researches on the trust model still introduce and use BRSN.

In terms of the trust management scheme, Gheorghe et al. [16] presented an Adaptive Trust Management (ATM) scheme, which was to adjust trust and reputation value based on node's behavior. It involved the following three parts: the learning phase, the exchanging phase and the updating phase. The ATM's adaptation and cooperation made it easy to overcome the large range of attacks in the network. Fang et al. [17] put forward a reputation management scheme based on multi-factors, which described the initialization, the update, the storage of reputation value and the punishment and redemption for malicious nodes. The principle was based on the perception behavior of the sensor node, the packet forwarding and the data fusion. Labraoui [18] proposed a Trust Model based on Risk evaluation (TMR). The TMR could effectively evaluate the overall trust value of a node by its reputation value, and overcome conflicting behaviors of malicious nodes. Su and Liao [19] presented a jury-based trust management mechanism for distributed cognitive radio networks. In this mechanism, the JURY USER was defined and designed to examine the cognitive user's reputation, and to perform the data convergence and the spectrum allocation for the target networks. Ren et al. [20] proposed a trust management scheme to provide the trust data storage and the trust generation for the unattended wireless sensor networks. For the former, a geographic hash table was deployed to identify storage nodes, and to decrease storage cost. For the latter, the subjective logic based consensus techniques was used to mitigate trust fluctuations caused by environmental factors. Reshmi and Sajitha [21] proposed an energy efficient hierarchical trust management scheme. This scheme could reduce the nodes' energy consumption rate by calculating the trust values on demand, and make the system more robust. Zhu et al. [22] put forward a novel authenticated trust and reputation calculation and management (ATRCM) system for cloud computing and WSN integration. In the ATRCM system, the following three functions were addressed: (1) authenticating the cloud service provider (CSP) and the sensor network provider (SNP) to avoid malicious impersonation attacks; (2) calculating and managing trust and reputation regarding the service of CSP and SNP; (3) helping the cloud service user (CSU) choose desirable CSP and assisting CSP in selecting appropriate SNP. The proposed ATRCM acted as the security scheme between the heterogeneous networks/applications. Fang et al. [23] presented a Beta-based trust and reputation Evaluation system (BTRES) for nodes' trust and reputation evaluation in WSN. The proposed BTRES could achieve the reputation evaluation by monitoring nodes' behavior, select the normal forwards node, and reduce the internal attacks risks. From above analysis, some trust managements, such as TMR, ATRCM, BTRES and so on, mainly detect and defend against the internal attacks, the others focus on selecting the relay nodes, removing the malicious nodes and optimizing the routing protocols.

Due to the diversity and complexity of the internal attacks, the above mentioned trust management schemes are not invulnerable. For BRSN, it can effectively defend against the selective forwarding attacks, the black hole attacks, and indentify the compromised nodes effectively. But for the high reputation node,

it cannot effectively prevent its malicious behavior. The merits of EDTM are taking the advantage of factors (such as communication, energy, etc.) and providing accurate trust value. But it is a big challenge to measure the weight of each factor. For ATM, it relies on the accumulation of experience, which will require a lot of storage. However, the ATM has good adaptability and coordination. Furthermore, from our analysis of existing research results, a noteworthy fact is that many research foundations of resisting attacks derive from the single attack behavior of the malicious nodes, and it seems that the consecutive behavior analysis for the suspected malicious nodes is seldom concerned over a period of time.

In the next section, we will describe the characteristic of RTV attack, analyze its behavior, improve the BRSN model, and propose a time-window-based resilient trust management scheme to defend against the reputation time-varying attack effectively. The RTV attack is a kind of malicious impersonation attacks which hard to detect and avoid by other state-of-art works. When RTV attacks are implemented, the reputation of malicious nodes gets obviously reduced, and they can perform good activity in a period of time to improve its reputation value. We propose an approach to mitigate the risk of the reputation time-varying attacks, as well as detect and remove the attack nodes.

3 Time-window-based resilient trust management scheme

3.1 Analysis and modeling

Saurabh and Mani put forward BRSN in the wireless sensor network. They use the mathematic model to represent the reputation and update the reputation according to the new direct/indirect observations, finally, transform the reputation to the trust value. In BRSN, the first step is that use the Bayesian equation to analyze the trust distribution and BETA distribution, and the reputation distribution can be substituted by BETA distribution. The Bayesian equation is (1), which is used to calculate the trust probability after given observation.

$$P(B/O) = \frac{P(B/O)P(B)}{\text{Normalization constant}}. \tag{1}$$

The priori probability is used to estimate the future unknown quantity and to provide a joint distribution $P(O, B)^2$ to describe how these quantities interact. Similarly, B represents the reputation of the node; O is a direct observation from a node to another node. When the node i gets some of the output from the watchdog mechanism D_{ij}, which is used to recursively update the reputation of node j at node i, it updates node j's reputation as R_{ij} as follow:

$$R_{ij} = \frac{P(D_{ij}/R_{ij})R_{ij}}{\sum P(D_{ij}/R_{ij})R_{ij}}, \tag{2}$$

where R_{ij} is the reputation between nodes i and j. We use BETA distribution to represent node reputation distribution, instead of Gaussian distribution or binomial distribution because of BETA distribution's adaptability and simplicity, as well as its statistical theory. The BETA distribution is introduced into two parameters, and is expressed by the gamma function:

$$P(x) = \frac{\Gamma(\alpha+\beta)}{\Gamma(\alpha)\Gamma(\beta)}x^{\alpha-1}(1-x)^{\beta-1}, \quad \forall 0 \leqslant x \leqslant 1,\ \alpha \geqslant 0,\ \beta \geqslant 0. \tag{3}$$

Firstly, we assume that the node i and node j interact in the $m+n$ events, where m represent cooperation events and n represent non-cooperation event. Based on these given messages, node i predict the next event behavior θ (cooperation/non-cooperation) of node j. Without any priori information, $\theta \in [0, 1]$ obeys uniform distribution. Therefore, $P(\theta) = \text{uni}(0, 1) = \text{Beta}(1, 1)$. We can emulate a priori interaction by binomial distribution, and then calculate posteriori θ by

$$P(\theta) = \frac{\text{Bin}(m+n, m)\text{Beta}(1, 1)}{\text{Normalization constant}}, \tag{4}$$

where posterior distribution of θ in (4) is BETA distribution.

The reputation of node i for node j is represented as

$$R_{ij} = \text{Beta}(\alpha_j + 1,\ \beta_j + 1), \tag{5}$$

where, for node i, α_j and β_j represent the cooperation and non-cooperation respectively. When there is no priori observation, $\alpha_j = 0$, $\beta_j = 0$. Therefore, $R_{ij} = \text{Beta}(1, 1) = \text{uni}(0, 1)$. Here, we put forward a hypothesis that without a priori knowledge, the majority of reasonable reputation distribution is uniform distribution. Since the BETA distribution is defined for a non-integer, Eq. (5) is valid for all non-negative real numbers α_j and β_j. The reputation metrics here is the expectation of the reputation function as

$$T_{ij} = E(R_{ij}) = E(\text{Beta}\{\alpha_j + 1,\ \beta_j + 1\}) = \frac{\alpha_j + 1}{\alpha_j + \beta_j + 2}, \tag{6}$$

where T_{ij} is the trust value between nodes i and j. Updating the reputation is shown as

$$R_{ij} = \frac{\text{Bin}(r + s,\ r)\text{Beta}(\alpha_j + 1,\ \beta_j + 1))}{\text{Normalization constant}} = \text{Beta}(\alpha_j + r + 1,\ \beta_j + s + 1). \tag{7}$$

The reputation's update is equivalent to the value of two parameters α_j and β_j:

$$\alpha_j^{\text{new}} = \alpha_j + r, \quad \beta_j^{\text{new}} = \beta_j + s. \tag{8}$$

Node i and node j interact with the $r + s$ event again, where r is the cooperating event and s is non-cooperating event. The aging of the node's reputation value is obtained by

$$\alpha_j^{\text{new}} = (\omega_{\text{age}} \times \alpha_j) + r, \quad \beta_j^{\text{new}} = (\omega_{\text{age}} \times \beta_j) + s, \tag{9}$$

where ω_{age} is called the weight of aging, and its value range is (0, 1). The weight of aging ensures all nodes to cooperate always. However, the malicious nodes can choose the best cooperative policy, and use the initial obtained reputation to disturb the target system. Therefore, the appropriate update of the aging weight will ensure that the aging of the reputation message, meanwhile, the nodes need to subsequent cooperation to maintain a higher reputation.

For the indirect reputation, it is evaluated by reputation from third-party node k to node j . The indirect observation is represented by $(\alpha_j^k,\ \beta_j^k)$. The priori reputation from node i to node j and k are represented by $(\alpha_j,\ \beta_j)$ and $(\alpha_k,\ \beta_k)$, respectively. The new reputation value $(\alpha_j^{\text{new}},\ \beta_j^{\text{new}})$ is obtained by combining with above information we have known. The specifical method is to map the issue into an equivalent problem in the field of D-S belief theory [24], and then solve it using the concept of belief discounting [25]. Eq. (10) is obtained by doing a reverse mapping from belief theory to continuous probability distributions, and it is shown as follows:

$$\begin{aligned} \alpha_j^{\text{new}} &= \alpha_j + \frac{\{2 \times \alpha_k \times \alpha_j^k\}}{\{(\beta_k + 2) \times (\alpha_j^k + \beta_j^k + 2)\} + \{2 \times \alpha_k\}}, \\ \beta_j^{\text{new}} &= \beta_j + \frac{\{2 \times \alpha_k \times \beta_j^k\}}{\{(\beta_k + 2) \times (\alpha_j^k + \beta_j^k + 2)\} + \{2 \times \alpha_k\}}. \end{aligned} \tag{10}$$

Finally, the trust value is

$$T_{ij} = \frac{\alpha_j^{\text{new}} + 1}{\alpha_j^{\text{new}} + \beta_j^{\text{new}} + 2}. \tag{11}$$

3.2 Time-window-based resilient trust management scheme (TRTMS)

In the paper, we describe the reputation time-varying attack: This is a class of such attacks, which rapidly grow the node's trust value, and slowly reduce its trust value. These changes in trust value come from two aspects: one is a malicious node's active behaviors, and the other is from neighbor malicious nodes'

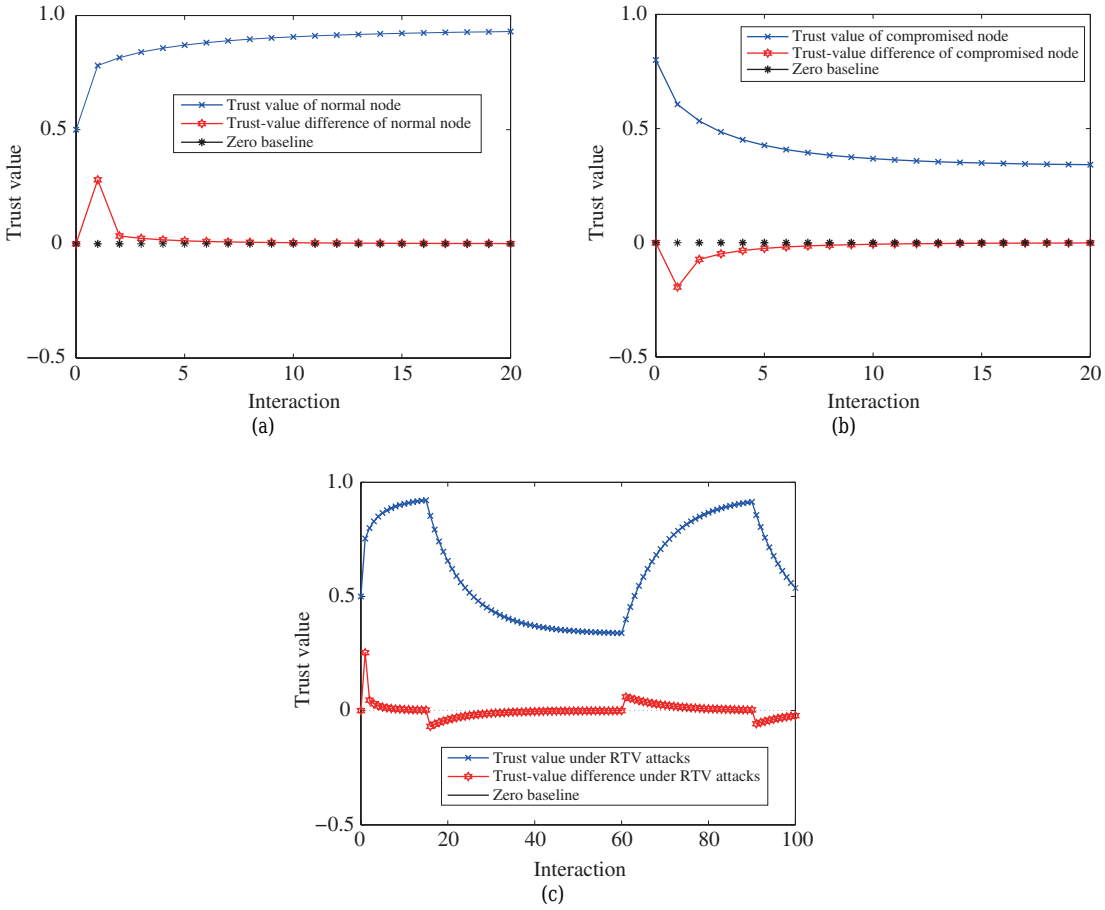

Figure 1 (Color online) Changes in trust value and its difference under different status. (a) Change in trust value and its difference for normal node; (b) change in trust value and its difference for compromised node; (c) change in trust value and its difference under RTV attacks.

passive behaviors. We also proposed an approach to mitigate the risk of the reputation time-varying attacks, as well as detect and remove the attack nodes which other state-of-art works did not consider and would be unable to detect.

The BRSN can defend against the conspiracy attacks and the slander attacks effectively, but cannot defend against the reputation time-varying attacks. The reasons are that the reputation time-varying attacks are the malicious nodes to perform good or bad behavior intermittently, that is, when the RTV attacks are implemented, the reputation of malicious nodes get obviously reduced, they can perform good activity in a period of time to improve its reputation value; when the reputation value reached a certain level, they begin to execute malicious behavior. Therefore, it is difficult to detect the malicious nodes by using the traditional model. In the paper, our main work is to defend against the malicious node's reputation time-varying attack. First, we introduce (12) that is the difference of trust value to observe the trend of trust value.

$$\Delta T_n = T(n+1) - T(n). \tag{12}$$

In the above equation, $T(n)$ represents the trust value of nodes in the nth inspection cycle. Here, the node itself behavior is only considered. For the normal node, its trust value will converge and reach a maximum, and the trend of ΔT_n will eventually become 0, showed in Figure 1(a). The trust value and its difference of the compromised node are showed in Figure 1(b). From Figure 1(b), the trust value of compromised node reduces gradually, and its difference ΔT_n is always less than zero. According to Figure 1(c), we can draw a conclusion that, the trust value fluctuates and its difference undulates without any discipline. On the other hand, when the trust value of malicious nodes reduces to some extent level,

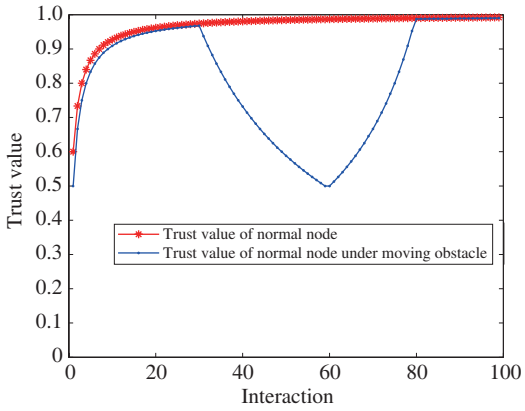

Figure 2 (Color online) Comparison of normal nodes' trust value under different conditions.

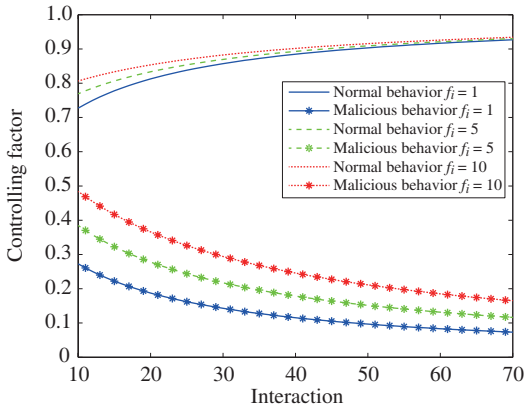

Figure 3 (Color online) Controlling factor changes under different f_i.

they can perform good activity in a period of time to improve its reputation value, meanwhile, its trust value raise following it; once the trust value raises and reaches a certain level, the neighbor node will choose it as the next node. Thus, defending against the reputation time-varying attack is difficult.

Owing to the complex topology of WSN and the instability of wireless channel, the malicious nodes that launch the RTV attacks cannot be judged by the variation of the trust value. This is due to that, when a mobile obstacle is located between two nodes, the wireless signal is attenuated, the packet loss rate (PLR) increases. Hence, for one of the nodes, its changes in behavior and trust value are similar to the RTV attacks' (see in Figure 2).

In TRTMS, one approach is proposed to mitigate the risk of RTV attack, the other approach is given to detect and remove the malicious nodes, which could launch the RTV attack.

1. Mitigating the risk of RTV attacks. In this approach, we can control the changes in reputation value by limiting the degree of change in the trust value for the malicious nodes. Hence, in order to resiliently control the changes and adapt to different scenarios and phases, we introduce two parameters: the controlling factor (F_c), and the impact factor (f_i). The purpose of the controlling factor F_c is to limit the rapid growth of the trust value, and can make the node's trust value fall quickly. The value of F_c is related to node's reputation, see (13). The purpose of introducing the controlling factor F_c is to consider the effect of all the interaction of the nodes. For good behavior, it has a positive effect on the reputation value, malicious versa. The purpose of the impact factor (f_i) is to make the controlling factor suit different scenarios and phases. In some scenarios or phases where the trust value of malicious node grows rapidly, the controlling factor (F_c) of malicious behavior could be decreased resiliently while it has acceptable inference on the truth value of normal behavior. The selection of different impact factors (f_i) makes the controlling factor (F_c) more resilient (see Figure 3).

$$F_c = \frac{\partial + f_i}{\partial + \gamma + (f_i + 1)}, \tag{13}$$

where ∂ and γ represent the sum of good and bad reputation in the interaction.

2. Detecting and removing malicious nodes. In this approach, we can detect the RTV attacks by accumulating the number of ΔT_n one-way reversal and judging this number exceeds a threshold within a certain time window. For this purpose, two parameters are introduced: the reversed number (N_R) and the length of time window (L_{TW}). The reversed number (N_R) is associated with the reversal of the trust value difference. When the trend of trust value changes, the trust value differences will change between the positive and negative (see in Figure 1(c)). In this paper, the reversed number (N_R) is the number of negative reversal, which is the change in from the positive to negative. The expression of N_R is (14). The length of time window (L_{TW}) is represented as the time length of the monitoring window, namely, the nodes behavioral parameters are completed to accumulate within a given time range. The different length of time window (L_{TW}) can meet the requirements of various applications, even different scenarios

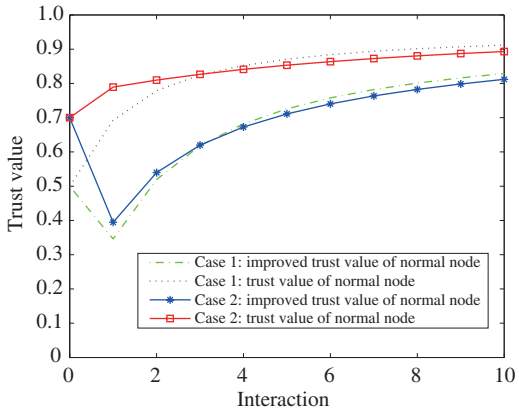

Figure 4 (Color online) Changes in trust value of normal node.

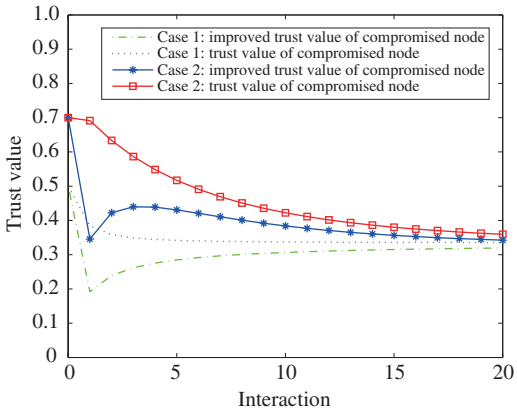

Figure 5 (Color online) Changes in trust value of compromised node.

of the same application. When a new time window is activated, the reversed number (N_R) will be set to zero. Eq. (15) is to judge the malicious node by judging the value of N_R in a same time window. When the threshold is reached, the node is judged to be a malicious node.

$$N_R = \begin{cases} N_R + 1, & \text{if } \Delta T_{n-1} > 0 \text{ and } \Delta T_n \leqslant 0 \text{ and } \Delta T_{n+1} < 0, \\ N_R, & \text{else}, \end{cases} \tag{14}$$

$$T_c = \begin{cases} T_n, & N_R < \tau, \\ 0, & N_R \geqslant \tau, \end{cases} \tag{15}$$

where τ is the threshold of a maximum reversal number of trust value and T_c represents the trust value of malicious nodes. The threshold τ is introduced to judge the node's properties by reversal number of trust value, meanwhile, to avoid erroneous judgment due to a temporary deterioration of wireless channel.

Finally, when f_i is zero, the trust value of node j is

$$T = F_c \times T_{ij} = \frac{\partial}{\partial + \gamma + 1} \times \frac{\alpha_j^{\text{new}} + 1}{\alpha_j^{\text{new}} + \beta_j^{\text{new}} + 2}. \tag{16}$$

4 Simulations and analysis

Due to the special characteristics of wireless sensor network, the information interaction between nodes is likely to be influenced by many factors, such as the instability of wireless channel. Here, we assume that the node's reputation is related to the behavior of the node itself, and ignore the environment, wireless channel and energy consumption, and so on. For simulation parameters (some parameters refer to [23]), two cases are set up:

Case 1: Node j is not the first time to participate. The initial reputation value of node i to node j is set to (5, 1).The initial reputation value of node j to node k is set to (6, 2). The initial reputation value of node k to node j is set to (5, 1). The initial trust value of node j is $T = 0.7$. Weight ω_{age} is 0.9 (the selection of α and ω_{age} is determined by the specific application).

Case 2: New node participates. The initial reputation value of node i to node j is set to (0, 0). The initial reputation value of node k to node j is set to (0, 0). The initial reputation value of node k to node j is set to (0, 0). The initial reputation value of node j is $T = 0.5$.

The result is simulated in Figures 4 and 5 by MATLAB.

For normal node, it can be seen that the trend of trust value in two schemes is alike in Figure 4, and reach to a stable condition finally. The TRTMS scheme is more slowly, which is caused by the change of the value F_c. Figure 5 shows that the changes in the trust value of the compromised node. The

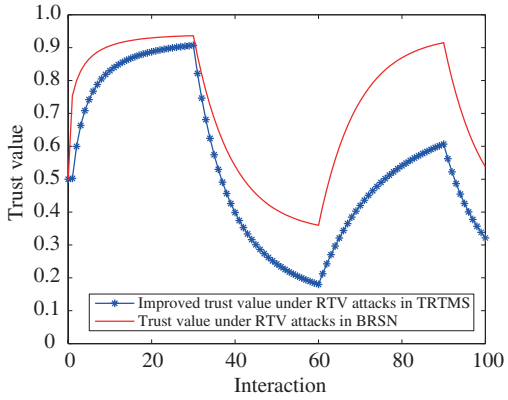

Figure 6 (Color online) Comparison of trust value under RTV attacks.

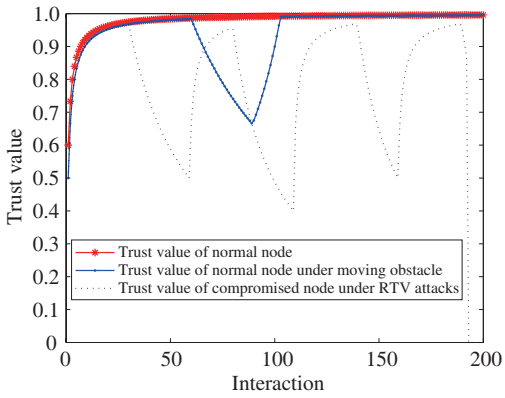

Figure 7 (Color online) Detecting and removing RTV attack nodes.

compromised node's trust value can decrease rapidly, and the magnitude of the decline is about 3.5 times that of BRSN, so it can quickly identify the malicious nodes. Figures 4 and 5 illustrate that the trend of the change is alike, but the TRTMS scheme has a limited effect on the increase of the trust value of the normal nodes, which accelerates the change of the trust value of the compromised nodes. The additional F_c factor has little effect on the trust value of normal nodes, but it can quickly reduce the trust value of compromised nodes. In addition, Figures 4 and 5 show that the newly participated nodes and nodes with a certain trust value are consistent, so the TRTMS scheme can be applied to any node.

From the variation of solid line in Figure 6, it can be known that when the trust values of malicious node reach to 0.92 approximately, it will execute the bad behavior. Using the BRSN method, the node's reputation value drops slowly, causing the attack node can carry out the long time (such as Figure 6, it executed 32 times of information exchange); when the trust value is 0.38, the malicious node starts to cooperate in order to get a high trust value in a short time (executed 26 messages interaction). The TRTMS can quickly make the trust value decrease (as shown in Figure 6, when the trust value dropped to 0.38, it executes 10 messages interaction), and the rise of amplitude is very slow. If the node to reach high trust value such as 0.6, the BRSN scheme needs to perform 6 times to cooperate, and it recovers to 0.6 quickly. However, the TRTMS scheme needs to perform 22 times, and using the TRTMS scheme, the recovery of the trust value is less than optimal conditions (such as 0.9). The slow rise and fall of the node's trust value is influenced by the factor F_c, which is consistent with the expected results. Therefore, the TRTMS scheme makes the time of the execution of the attack node less and the reputation value cannot be recovered quickly.

Figure 7 shows that the RTV attacks are detected, and the malicious nodes are removed, and effectively eliminate erroneous judgments, which cause by the deterioration of wireless channel. This is due to that, the reversal of trust value caused by moving obstacle is far less than the RTV attacks' theoretically. Within a certain time window, once the malicious behavior, namely, the abnormal reversal numbers of the trust value reach to the threshold, the trust value declines quickly, and cannot be restored to a high level for the malicious. In Figure 7, the length of time window is 200, and the threshold τ is 4. When the reversal numbers of trust value accumulate to the threshold τ for the malicious nodes, its trust value is set to 0. The length of time window and the threshold τ are chosen based on practical application environment. For example, in the stable environment in which the wireless channels between each nodes are stable and the trust value of the nodes are consistent, the length of time windows and the threshold τ are set to small values such as 200 and 4 respectively. In some environment with frequently changes, such as a multipath rich indoor environment, passageway with a high flow of people, wireless channel would deteriorate periodically which cause similar changes in trust value compared with malicious nodes, so that the length of time windows and the threshold τ should be set to larger values to reduce erroneous judgments.

In summary, the BRSN scheme and the TRTMS scheme is feasible for normal nodes. For defending

against the RTV attacks, the TRTMS scheme can reduce the trust value of the malicious nodes in a short time, and mitigate the risk of these attacks. Through introduced the time window and reversal threshold, the TRTMS scheme can effectively detect and defend against the RTV attacks.

5 Conclusion

The security is always a hot topic in wireless sensor network. The trust evaluation system based on BETA distribution can defend the internal attacks from compromised nodes in wireless sensor network, but it is lack of effective defense against the RTV attack of the malicious nodes. Therefore, based on the BETA distribution, we mainly introduce the controlling factor F_c and the time window, and propose a TRTMS to defend against the reputation time-varying attacks in wireless sensor network. In TRTMS, the risk of RTV attacks is mitigated by using the controlling factor (F_c) and impact factor (f_i), the malicious nodes are detected and removed by using the length of time window and the reversal number of the trust value. In the future, we mainly focus on the trust evaluation system based on energy efficiency.

Acknowledgements This work was partially supported by National Natural Science Foundation of China (Grant No. 61471346), Shanghai Natural Science Foundation (Grant No. 17ZR1429100), International Science and Technology Cooperation Program of China (Grant No. 2014DFA11640), National Program of International Science and Technology Cooperation (Grant No. 2014DFE10160), National Science and Technology Major Project (Grant No. 2014ZX03005001), and National Natural Science Foundation and Shanxi Provincial People's Government Jointly Funded Project of China for Coal Base and Low Carbon (Grant No. U1510115).

Conflict of interest The authors declare that they have no conflict of interest.

References

1 Guo M J, Liu Y H, Yu H B, et al. An overview of smart city in China. China Commun, 2016, 13: 203–211
2 Xiong Z, Sheng H, Rong W G, et al. Intelligent transportation systems for smart cities: a progress review. Sci China Inf Sci, 2012, 55: 2908–2914
3 Mois G, Sanislav T, Folea S C. A cyber-physical system for environmental monitoring. IEEE Trans Instrum Meas, 2016, 65: 1463–1471
4 Yang Y, Zhao C, Yao S, et al. Delay performance of network-coding-based epidemic routing. IEEE Trans Veh Technol, 2016, 65: 3676–3684
5 Chen W, Jiang X R, Tang Z B, et al. Context-based global multi-class semantic image segmentation by wireless multimedia sensor networks. Artif Intell Rev, 2015, 43: 579–591
6 Tao X F, Xu X D, Cui Q M. An overview of cooperative communications. IEEE Commun Mag, 2012 50: 65–71
7 Yang Y, Zhang W X, Wei K, et al. Power reduction for mobile devices by deploying low-power base stations. IET Commun, 2014, 8: 3372–3380
8 Saurabh G, Mani B S. Reputation-based framework for high integrity sensor network. In: Proceedings of ACM Workshop on Security of ad hoc and Sensor Network. New York: ACM, 2004. 66–77
9 Yang G, Yin G S, Yang W, et al. A reputation-based model for malicious node detection in WSNs (in Chinese). J Harbin Inst Technol, 2009, 41: 158–162
10 Jiang J F, Han G J, Wang F, et al. An efficient distributed trust model for wireless sensor network. IEEE Trans Parall Distrib Syst, 2015, 26: 1228–1337
11 He D J, Chen C, Chan S, et al. A distributed trust evaluation model and its application scenarios for medical sensor networks. IEEE Trans Inform Technol Biomed, 2012, 16: 1164–1175
12 Meghanathan N. A distributed trust evaluation model for wireless mobile sensor networks. In: Proceedings of International Conference on Information Technology: New Generations (ITNG), Las Vegas, 2014. 186–191
13 UmaRani V, Sundaram K S, Jayashree D. Enhanced beta trust model in wireless sensor networks. In: Proceedings of International Conference on Information Communication and Embedded Systems (ICICES), Tamil Nadu, 2016. 1–5
14 Wang N, Liu D Q. Trust model based on changeable sampling frequency for wireless sensor network. In: Proceedings of IEEE/ACIS 15th International Conference on Computer and Information Science (ICIS), Okayama, 2016. 1–4
15 Xia H, Jia Z P, Sha E H-M. Research of trust model based on fuzzy theory in mobile ad hoc networks. IET Inform Secur, 2014, 8: 88–103
16 Gheorghe L, Rughinis R, Tataroiu R. Adaptive trust management protocol based on intrusion detection for wireless sensor network. In: Proceedings of RoEduNet International Conference on Networking in Education and Research, Constanta, 2013. 1–7

17 Fang F, Li J F, Li J. A reputation management scheme based on multi-factor in WSN. In: Proceeding of IEEE International Conference on Mechatronic Sciences, Electric Engineering and Computer (MEC). Shenyang, 2013. 3843–3848
18 Labraoui N. A reliable trust management scheme in wireless sensor networks. In: Proceedings of IEEE International Symposium on Programming and Systems (ISPS), Algiers, 2015. 1–6
19 Su W G, Liao Y. A jury-based trust management mechanism in distributed cognitive radio networks. China Commun, 2015, 12: 119–126
20 Ren Y, Zadorozhny V I, Oleshchuk V A, et al. A novel approach to trust management in unattended wireless sensor networks. IEEE Trans Mob Comput, 2014, 13: 1409–1423
21 Reshmi V, Sajitha M. Energy efficient hierarchical trust management scheme for solving cluster head compromising problem in wireless sensor networks. In: Proceeding of IEEE International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS), Coimbatore, 2015. 1–6
22 Zhu C S, Nicanfar H, Leung V C M, et al. An authenticated trust and reputation calculation and management system for cloud and sensor networks integration. IEEE Trans Inform Forens Secur, 2015, 10: 118–131
23 Fang W D, Zhang C L, Shi Z D, et al. BTRES: beta-based trust and reputation evaluation system for wireless sensor networks. J Netw Comput Appl, 2016, 59: 88–94
24 Shafer G. A Mathematical Theory of Evidence. Princeton: Princeton University, 1976
25 Jøsang A. A logic for uncertain probabilities. Int J Uncertain Fuzz Knowl-Based Syst, 2011, 9: 279–311