Trust Management Scheme Based on D-S Evidence Theory for Wireless Sensor Networks

Renjian Feng, Shenyun Che, Xiao Wang, and Ning Yu

School of Instrumentation Science and Opto-Electronics Engineering, Beihang University, Beijing 100191, China
Science and Technology on Communication Information Security Control Laboratory, Jiaxing 314033, China

Correspondence should be addressed to Renjian Feng; rjfeng@buaa.edu.cn

Received 9 January 2013; Revised 29 May 2013; Accepted 5 June 2013

Abstract

Trust management scheme has been regarded as a powerful tool to defend against the wide set of security attacks and identify malicious nodes. In this paper, we propose a trust management scheme based on revised Dempster-Shafer (D-S) evidence theory. D-S theory is preponderant in tackling both random and subjective uncertainty in the trust mechanism. A trust propagation mechanism including conditional trust transitivity and dynamic recommendation aggregation is developed for obtaining the recommended trust values from third part nodes. We adopt a flexible synthesis method that uses recommended trust only when no direct trust exists to keep a good trust-energy consumption balance. We also consider on-off attack and bad mouthing attack in our simulation. The simulation results and analysis show that the proposed method has excellent ability to deal with typical network attacks, better security, and longer network lifetime.

1. Introduction

Wireless sensor networks (WSNs) consist of plentiful tiny, sensing capabilities, and resource-constrained sensor nodes, and are often deployed in unattended and hostile environments to perform various monitoring tasks [1, 2]. However, due to the wireless and unattended deployment nature of WSNs, there is a risk of unique threats [3]. Hence, security plays a vital role in guaranteeing the normal running of the whole network. Although security requirements of WSNs are quite similar with those of conventional networks, the security strategies based on the traditional authentication and encryption mechanisms are unsuitable to apply to WSNs because of the nodes’ resource constraints [4]. Therefore, the trust management scheme has attracted more and more research attentions as a complementary security mechanism [5]. The basic idea of the trust management scheme is to calculate trust values that are used to describe the trustworthiness, reliability, or competence of individual nodes, based on some monitoring schemes [6]. Then the trust information can be applied to higher layer decisions such as routing [7, 8], data aggregation [9], and cluster head election [10, 11]. To the best of our knowledge, a number of trust management schemes have been proposed for WSNs [12–22], but most of them failed to establish a reasonable trust management scheme to express the subjectivity, uncertainty, and transitivity of trust characteristics in WSNs.

To resolve the problems, this paper puts forward a trust management scheme (TMS) based on revised D-S evidence theory in WSNs and achieves main contributions as follows. (1) A trust propagation mechanism including conditional trust transitivity and dynamic recommendation aggregation using the revised D-S evidence theory is proposed, which maintains the subjectivity, uncertainty, and transitivity of trust characteristics. (2) An adaptive time factor is adopted to dynamically weight history experience against current information, which enhances the accuracy of trust calculation. (3) To keep a good trust-energy consumption balance, a synthesis method that uses recommended trust only when no direct trust exists is proposed. (4) We address the issue of TMS performance in terms of ability to defeat some attacks (on-off attack, bad mouthing attack), detection of malicious nodes, and energy consumption, comparing with NBBTE [15] and BRSN [16]. Simulation results demonstrate that TMS has excellent ability to deal with typical network attacks, better security, and longer network lifetime.
The model proposed in this work extends our prior work [15] which integrated the approach of nodes behavioral strategies and modified evidence theory. In this paper, we improve the previous model with mechanisms for the propagation of nodes’ recommendation and the synthesis of nodes’ trust value. Moreover, we refine the algorithm of direct trust value, evaluate our scheme’s ability to defeat on-off attack and bad-mouthing attack, and study the security and energy consumption of the model.

The rest of this paper is organized as follows. Section 2 presents related work on trust establishment for WSNs. Section 3 describes the D-S evidence theory and the process of TMS, including computation of nodes’ trust value. In Section 4, comparing with NBBTE and BRSN, the superiority of TMS is shown by simulations. Finally, the conclusions are presented in Section 5.

2. Related Works

The research on establishing trusts can be classified into two categories, reputation-based [16–19] and trust establishment [20–22]. In the former category, trust is evaluated by direct observation and second-hand information distributed among a network. In the latter category, trust in neighbors is evaluated by direct observation and trust relations between two nodes.

Reputation-based framework for sensor networks (RFSN) [16] used watchdog mechanism to build trust rating. Within the framework of RFSN, a beta reputation system for sensor networks (BRSN) that used a Bayesian formulation was employed. Since then, many researches have been done based on the BRSN model such as MA&TP-BRSN, and RFM-WSN [17]. However, in RFSN, the stipulation that no node is allowed to disseminate bad reputation information makes it unable to cope with uncertain situations. Aivaloglou and Gritzalis [18] proposed a hybrid trust and reputation management protocol by exploiting the predeployment knowledge on the network topology and the information flows. But it is not easy to get the predeployment knowledge. In [19], the authors proposed a behavior reputation method which defined the similarity and the similarity matrix by using normal differences of the status estimate vectors. However, the initialization stage of the model is based on the authentication key which is prone to attacks.

Zarei et al. [20] presented a novel congestion control scheme based on fuzzy logic systems. The proposed scheme enabled the nodes to investigate the behavior of their neighbors and isolated them upon malfunctioning, decreasing congestion problem, and buffering capacity shortage. However, the use of fuzzy logic makes it easy to lose some information and may lead to an inaccurate result. In [21], the authors proposed a new lightweight group-based trust management scheme. In this model, each sensor node (SN) performed peer evaluation based on direct observations or recommendations, and each cluster head (CH) evaluated other CHs as well as SNs under its own cluster. However, trust in their case is assessed only based on past interaction experiences in message delivery. Lopez et al. [22] listed the best practices that were essential for developing a good trust management system and made an analysis of the state of the art related to these practices. The reference makes an excellent summary, proposes many profound viewpoints, and shows an additional insight on the trust evaluation field.

3. TMS Algorithm

Refer to [4], we define trust as the confidence that node \( i \) (denoted as \( n_i \)) has on node \( j \) (denoted as \( n_j \)) about how \( n_j \) will perform as expected. A complete trustworthiness consists of subject entity’s observation and recommendation from third party. The TMS algorithm firstly establishes various trust factors based on our previous work [15]. Next, direct trust is calculated on the base of trust factors. Then, the recommendations of several neighbor nodes are acquired in accordance with the revised D-S rule and the trust difference between pieces of evidence. Finally, the overall trust value is computed through a flexible synthesis method that guarantees a good trust-energy consumption balance. Figure 1 shows the structure of TMS algorithm.

3.1. D-S Evidence Theory. Due to the subjectivity of trust evaluation, it is unsuitable to simply establish the recommended trust value by weighted average. D-S evidence theory can briefly express the important conceptions, such as “uncertainty,” and make right judgments by efficiently integrating many-sided uncertain information. Hence, in our proposed algorithm, we calculate trust value and the average weight of recommendations based on the D-S rule. The basic definitions of D-S theory are defined as follows [23].

**Definition 1.** Let \( \Omega \) be the identification frame, denoting a set of mutually exclusive and exhaustive hypotheses about problem domains. Correspondingly, \( 2^\Omega \) is the power set of \( \Omega \).

**Definition 2.** Mass stands for a belief mapping from \( 2^\Omega \) to the interval between 0 and 1, represented as \( m: 2^\Omega \rightarrow [0, 1] \) is called the BPA (Basic Probability Assignment) and is defined as below:

\[
m(\emptyset) = 0, \quad \sum_{A \in \Omega} m(A) = 1, \quad A \neq \emptyset. \tag{1}
\]

**Definition 3.** The belief of a hypothesis is the sum of the beliefs for those hypotheses that are its subsets. Its definition is given as

\[
\text{Bel}(A) = \sum_{B \subseteq A} m(B), \quad \forall A \subseteq \Omega, \tag{2}
\]

where \( A \) is named focal element and \( m(A) > 0 \) is the basic confidence level of \( A \), representing how much the evidence supports \( A \) to happen.

3.2. Trust Factors. To defeat various attacks, we had better take all kinds of factors that depend on the interactions between neighbor nodes into consideration. However, there is an obvious trade-off between the number of factors and the
energy consumption. We select four trust factors from our previous work [15]. Suppose $n_i$ evaluates the trust degree on $n_j$; the trust factors are Received Packets Rate $RPF_{i,j}(t)$, Successfully Sending Packets Rate $SPF_{i,j}(t)$, Packets Forwarding Rate $TPF_{i,j}(t)$, and Node Availability $HPF_{i,j}(t)$.

### 3.3. Direct Trust Evaluation Approach

Subject $n_i$ monitors the behaviors of object $n_j$ in one cycle and acquires the current trust value $CDT_{i,j}(t)$ based on the following expression:

$$m^C_{i,j}([T]) = f_1\left(RPF_{i,j}, SPF_{i,j}, TPF_{i,j}, HPF_{i,j}\right),$$
$$m^C_{i,j}([-T]) = f_2\left(RPF_{i,j}, SPF_{i,j}, TPF_{i,j}, HPF_{i,j}\right),$$
$$m^C_{i,j}([T,-T]) = 1 - m^C_{i,j}([T]) - m^C_{i,j}([-T]).$$

The functions $f_1$ and $f_2$ are chosen in advance according to the specific assignments of network.

Furthermore, the direct trust value is recalculated in accordance with history records. The update of direct trust value is calculated as follows:

$$DT_{i,j} = \beta \times HDT_{i,j} + (1 - \beta) \times CDT_{i,j},$$

where $DT_{i,j}$ is the direct trust value of subject $n_i$ on object $n_j$ in current cycle; $HDT_{i,j}$ is the direct trust value of latest cycle; parameter $\beta$ is the adaptive time factor used to weight history experience against current information. To keep $\beta$ preferably dynamic, it is satisfied as follows:

$$\beta = \begin{cases} 
\beta_s, & m^H_{i,j}([T]) \geq m^C_{i,j}([T]), \\
\beta_l, & m^H_{i,j}([T]) < m^C_{i,j}([T]),
\end{cases}$$

where $0 < \beta_s < \beta_l < 1$. The parameter $m^C_{i,j}([T])$ and $m^H_{i,j}([T])$ represent the trust components of $CDT_{i,j}$ and $HDT_{i,j}$, respectively.

### 3.4. Recommended Trust Evaluation Approach

#### 3.4.1. Trust Transitivity

Suppose the recommended trust value of $n_i$ on $n_j$ can be obtained through $s$ different paths. And the number of recommendation paths $s$ depends on nodes’ distribution and transmission radius. In order to avoid trust recycle recursion and decrease network communication payload, the recommendation values are confined to direct trust value of the common neighbors owned by both $n_i$ and $n_j$. As shown in Figure 2, $n_i$ can only get the trust recommendation of $n_j$ from $k_1, k_2, k_3, \ldots, k_s$.

Assume that $RT^1_{i,j}$ is the recommended trust value of $n_i$ on $n_j$ through recommendation path $pt1 = \{k_1\}$. The vector forms of $RT^1_{i,j}$, $DT_{i,k_1}$, $DT_{k_1,j}$ are as follows:

$$RT^1_{i,j} = \left(m^D_{i,k_1}([T]), m^D_{i,k_1}([T,-T]), m^D_{i,k_1}([-T])\right),$$
$$DT_{i,k_1} = \left(m^D_{i,k_1}([T]), m^D_{i,k_1}([T,-T]), m^D_{i,k_1}([-T])\right),$$
$$DT_{k_1,j} = \left(m^D_{k_1,j}([T]), m^D_{k_1,j}([T,-T]), m^D_{k_1,j}([-T])\right).$$
4 International Journal of Distributed Sensor Networks

Let us set $\theta = \{\{T\}, \{T,-T\}, \{-T\}\}$. Then, the $RT^{1}_{i,j}$ is calculated as

$$m^{1}_{i,j} (A) = \begin{cases} m^{D}_{s,k_{i}} (A) \times m^{D}_{s,k_{j}} (A), & A = \{T\} \\ \sum_{E \in A} m^{D}_{s,k_{i}} (E) \times m^{D}_{s,k_{j}} (F), & A = \{-T\} \\ 1 - m^{1}_{i,j} (\{T\}) - m^{1}_{i,j} (\{-T\}), & A = \{T,-T\}. \\ \end{cases}$$

Using the symbol $\otimes$ to denote this operation, we can get

$$RT^{1}_{i,j} = DT^{1}_{i,k_{i}} \otimes DT^{1}_{k_{i},j}.$$  

To vividly show the process of trust transitivity, we resort to Figure 3. It is obvious to see that as long as one of $DT^{1}_{i,k_{i}}$ and $DT^{1}_{k_{i},j}$ is distrust, $RT^{1}_{i,j}$ is distrust.

Extending the above transitivity to multihop, we can get recommended trust through complex recommendation paths with many middle nodes as follows:

$$RT^{1,*}_{i,j} = DT^{1,*}_{i,s} \otimes \cdots \otimes DT^{1,*}_{s,j},$$  

where the symbol $\cdot$ indicates anonymous nodes in recommendation paths.

3.4.2. Dynamic Aggregation of Recommended Trust. On the basis of trust transitivity, $n_{i}$ obtains recommended trust values on $n_{j}$ through $s$ recommendation paths; namely:

$$RT^{u}_{i,j} = \left( m^{u}_{i,j} (\{T\}), m^{u}_{i,j} (\{T,-T\}), m^{u}_{i,j} (\{-T\}) \right),$$

$$RT^{2}_{i,j} = \left( m^{2}_{i,j} (\{T\}), m^{2}_{i,j} (\{T,-T\}), m^{2}_{i,j} (\{-T\}) \right),$$

$$\vdots$$

$$RT^{s}_{i,j} = \left( m^{s}_{i,j} (\{T\}), m^{s}_{i,j} (\{T,-T\}), m^{s}_{i,j} (\{-T\}) \right).$$

Then, $n_{i}$ would aggregate these pieces of evidence to get a consensus on $n_{j}$. Due to the existence of malicious nodes that may offer false recommendations, we introduce the revised D-S combination rule which adopts a consistent intensity to adjust weights of recommended trust values. The integration process is described in detail as follows.

Firstly, we compute the corresponding average weight $I_{u,v}$ as follows:

$$I_{u,v} = 1 - \sqrt{\frac{1}{2} \left( \| \vec{m}_{i,j}^{u} \|^{2} + \| \vec{m}_{i,j}^{v} \|^{2} - 2 \langle \vec{m}_{i,j}^{u}, \vec{m}_{i,j}^{v} \rangle \right)},$$

$$\nu = 1,2, \ldots, s; \ u = 1,2, \ldots s,$$

where $\| \vec{m}_{i,j}^{u} \|^{2} = \langle \vec{m}_{i,j}^{u}, \vec{m}_{i,j}^{u} \rangle$, $\| \vec{m}_{i,j}^{v} \|^{2} = \langle \vec{m}_{i,j}^{v}, \vec{m}_{i,j}^{v} \rangle$, $\langle \vec{m}_{i,j}^{u}, \vec{m}_{i,j}^{v} \rangle$ is the inner product of $\vec{m}_{i,j}^{u}$ and $\vec{m}_{i,j}^{v}$.

The difference between two recommended trust pieces of evidence increases with the reduction of consistent intensity. The lower the consistent intensity is, the more probably false trust recommendation may occur.

Furthermore, the matrix of consistent intensity which is composed of all the recommended trust values is defined as

$$I_{sxs} = \begin{bmatrix} 1 & I_{1,2} & \cdots & I_{1,s} \\ I_{2,1} & 1 & \cdots & I_{2,s} \\ \vdots & \vdots & \ddots & \vdots \\ I_{s,1} & I_{s,2} & \cdots & 1 \end{bmatrix}.$$

Through summation in row and normalization, the totally consistent intensity of recommended trust $RT^{u}_{i,j}$, which is equal to the average weight $I_{u,v}$, is computed by

$$I_{u} = \frac{\sum_{v=1,v \neq u}^{s} I_{u,v}}{\text{Max} \left( \sum_{v=1,v \neq u}^{s} I_{u,v} \right)}.$$  

Then, the basic reliability function $m(e)$ of every recommended trust evidence is amended by $I_{u}$ as follows:

$$m^{u}_{i,j} (\{T\}) = I_{u} \times m^{u}_{i,j} (\{T\}),$$

$$m^{u}_{i,j} (\{-T\}) = I_{u} \times m^{u}_{i,j} (\{-T\}),$$

$$m^{u}_{i,j} (\{T,-T\}) = 1 - m^{u}_{i,j} (\{T\}) - m^{u}_{i,j} (\{-T\}),$$

$$u = 1,2, \ldots, s.$$
Above all, the recommended trust can be modified as
\[ RT_{i,j}^u = (m_{i,j}^u ([T]), m_{i,j}^u ([T, -T]), m_{i,j}^u ([T, -T]), m_{i,j}^u ([T, -T]), m_{i,j}^u ([T, -T])) \],
\[ u = 1, 2, \ldots, s. \]

Finally, we can get the consistent recommended trust
\[ RT_{i,j} = (m_{i,j}' ([T]), m_{i,j}' ([T, -T]), m_{i,j}' ([T, -T])) \] as follows:
\[ m_{i,j}' ([A]) = \sum_{u=1}^{s} m_{i,j}^u ([A]) \]
\[ A = \{T\}, \quad A = \{-T, T\}, \quad A = \{-T\}. \]

3.5. Synthesis of Overall Trust Value. The recommendation trust is useful to get a more accurate trust value, but calculating it will consume more energy. Thus there is a need for a good trust-energy consumption balance in the trust management system. To solve this problem, we calculate the overall trust value for a flexible synthesis method which works as follows: only when \( n_i \) does not have direct evidence on \( n_j \), the recommendation trust is taken into account. Hence, the overall trust value \( OT_{i,j} \) is

\[ OT_{i,j} = \begin{cases} DT_{i,j} \quad \text{while node } i \text{ has direct evidence on node } j \\ RT_{i,j} \quad \text{else} \end{cases} \]
\[ OT_{i,j} = (m ([T]), m ([T, -T]), m ([T, -T])). \] (17)

If the decision model satisfies
\[ m_{i,j} ([T]) - m_{i,j} ([T, -T]) > \varepsilon, \]
\[ m_{i,j} ([T, -T]) < \theta, \]
\[ m_{i,j} ([T]) > m_{i,j} ([T, -T]). \] (18)

Then subject \( n_i \) regards \( n_j \) as “Trust,” and adds \( n_j \) into its trustworthiness list. In like manner, \( n_j \) can be marked “Uncertain” or “Distrust.”

4. Simulation Results

In this section, we use Matlab platform to show TMS has better performance than NBBTE and BRSN in terms of ability to defeat some attacks (on-off attack, bad mouthing attack), detection of malicious nodes, and energy consumption.

4.1. Defense of Attacks

4.1.1. On-Off Attack. Trust is a dynamic event. A good entity may be captured by attackers and turns into compromise node. On the other side, an incompetent entity can redeem the way that its neighbors regard it and become competent due to environmental changes. Because of the nodes’ resource limitation, some trust schemes adopted trust compensation mechanism. However, a smart attacker can capitalize on this feature of the trust schemes and create on-off attacks in which malicious entities behave well and badly alternatively [6]. To address this issue, we adopt the adaptive time factor \( \beta \) which is introduced in Section 3.2. \( \beta \) depends on specific situations. Here, we can choose \( \beta_1 = 0.3, \beta_2 = 0.8 \). In order to prevent the malicious node registering as a new user, the pessimistic initialization strategy of trust value is accepted. Suppose that malicious nodes cooperate well with neighbor nodes to get good trust records at the beginning of the simulation but behave badly after 40 rounds. The simulation results are shown in Figures 4 and 5.

From Figure 4 we can see that \( m([T]) \) increases slowly and \( m([-T]) \) decreases slowly in the trust compensation stage (0–40 rounds). Once the malicious nodes behave badly, \( m([-T]) \) falls off sharply while \( m([-T]) \) rises up. In other words, the time for trust accumulation is much longer than that for trust collapse. It is because \( \beta_2 = 0.8 \) which means that history information affects the trust value heavily in the trust compensation stage and \( \beta_2 = 0.3 \) which means current information bulks large when attacks happen.

Figure 5 compares the trust value calculated by different methods under on-off attack. The trust value calculated by BFSN increases the fastest in the trust compensation stage (0–40 rounds). Once the malicious nodes behave badly, \( m([T]) \) falls off sharply while \( m([-T]) \) rises up. In other words, the time for trust accumulation is much longer than that for trust collapse. The reason is that for trust collapse, \( \beta_2 = 0.8 \) which means that history information affects the trust value heavily in the trust compensation stage and \( \beta_2 = 0.3 \) which means current information bulks large when attacks happen.

From Figure 4 we can see that \( m([T]) \) increases slowly and \( m([-T]) \) decreases slowly in the trust compensation stage (0–40 rounds). Once the malicious nodes behave badly, \( m([-T]) \) falls off sharply while \( m([-T]) \) rises up. In other words, the time for trust accumulation is much longer than that for trust collapse. It is because \( \beta_2 = 0.8 \) which means that history information affects the trust value heavily in the trust compensation stage and \( \beta_2 = 0.3 \) which means current information bulks large when attacks happen.

4.1.2. Bad Mouthing Attack. Once recommendations are taken into consideration, we take the risk of receiving
dishonest recommendations which aim at framing good parties or boosting trust values of malicious peers [6]. This attack, referred to as the bad mouthing attack, is the most straightforward attack. Because of our flexible synthesis method, bad mouthing attack happens only when \( n_i \) has no direct evidence on \( n_j \). To defeat this attack, we introduce the revised D-S rule that includes the average weight \( I_u \) to combine recommendation pieces of evidence.

Suppose \( n_i \) receives twenty recommendation pieces of evidence of credible \( n_j \) and \( RT^1, RT^2, RT^9, RT^{11}, RT^{14}, RT^{18} \) are false recommendation information. Refer to Table 1 for detailed information.

Combining those twenty pieces of evidence by our method, we can obtain \( RT^i_{i,j} = [0.7327, 0.2288, 0.0385] \). The average weight \( I = (0.9997, 0.9893, 0.9805, 0.8772, 0.8630, 0.9968, 0.9788, 1.0000, 0.8657, 0.9806, 0.8374, 0.9921, 0.9942, 0.8408, 0.9968, 0.9895, 0.9900, 0.9007, 0.9783, 0.9842) \). It is obvious to see that \( I_4, I_5, I_9, I_{11}, I_{14}, I_{18} \) are smaller than others. Without the average weight, \( n_i \) would mistake \( n_j \) for unbelievable node.

To further explain TMS’s ability to defeat against bad mouthing attack, we compare it with NBBTE and BFSN under two conditions: framing good parties and boosting trust values of malicious peers. The results are shown in Figures 6 and 7.

When a malicious node launches the bad mouthing attack which aims at framing good parties, BFSN performs excellent as it only propagates good reputation information about other nodes. However, it cannot prevent malicious nodes from boosting trust values of malicious peer, as shown in Figure 7. No matter which condition it is, TMS performs better than NBBTE. Considering that BFSN is incapable of dealing with the second condition, we can come to the conclusion that TMS defends against bad mouthing attack most effectively.

4.2. Analysis of Network Security. To evaluate the network security, we compare our method with NBBTE and BRSN on the aspect of detecting malicious nodes. The proportions of
The proportion of malicious nodes is shown in Figure 7.

It is obvious to see that TMS does better at detecting malicious nodes than BRSN. This results from two aspects. First, by using D-S theory, TMS takes subject uncertainty into consideration and avoids considering prior distribution, and consequently the accuracy of trust evaluation is improved. Second, we adopt the corresponding average weight of recommended trust, which increases the robustness of trust mechanism. The proportions of detected malicious nodes of TMS are little lower than that of NBBTE, because TMS uses recommended trust conditionally while BRSN considers both direct and recommended trust.

4.3. Analysis of Energy Consumption. To evaluate the performance of the flexible synthesis method proposed in Section 3.5, we make experiments on the energy consumption under different circumstances. The radio energy model proposed in [24] is used for our simulation. The simulation parameters are listed in Table 2 and the simulation results are shown in Table 3 and Figure 9.

Circumstance 1 is a special situation, where \( n_i \) has no neighbor. Compare circumstance 2 and circumstance 3, we can see that the more neighbors \( n_i \) has, the longer it will survive. It is because computing direct trust just needs one interaction while computing recommended trust needs two. Circumstance 3 and circumstance 4 tell us that the decreasing of average recommended pieces of evidence can increase \( n_i \)'s lifetime. The reason is that decreasing one piece of average recommended evidence can reduce \( 2 \times (100 - a) \) interactions in a word, the simulation results demonstrate that the flexible synthesis method saves energy greatly, especially when the number of average recommended pieces of evidence is small.

To further show how long \( n_i \) can survive by the flexible synthesis method of TMS comparing with NBBTE and BRSN, we count rounds that \( n_i \) can survive under different number of average recommended pieces of evidence. In this experiment, we set the number of \( n_i \)'s neighbor nodes 30 and the number

**Table 2: Simulation parameters.**

| Parameters                                   | Corresponding value |
|----------------------------------------------|---------------------|
| Simulation field                             | \( 100 \text{ m} \times 100 \text{ m} \) |
| Number of nodes                              | 100                 |
| Transmission radius                          | 15 m                |
| Number of \( n_i \)'s neighbor nodes        | \( a \)             |
| Number of average recommended pieces of evidence | \( b \)        |
| Initial energy per node                      | 0.5 J               |
| Energy consumption of transmitter and receiver \( (E_{elec}) \) | 50 nJ/bit           |
| Transmit Amplifier \( (E_{amp}) \)           | 100 pJ/bit/m\(^2\)  |
| Message bits sent per round per node         | 4000 bit            |

**Table 3: Round of \( n_i \) dies with different parameter values.**

|                     | \( a \) | \( b \) | Round of \( n_i \) dies |
|---------------------|---------|---------|-------------------------|
| Circumstance 1      | 0       | 30      | 101                     |
| Circumstance 2      | 10      | 20      | 124                     |
| Circumstance 3      | 30      | 20      | 137                     |
| Circumstance 4      | 30      | 10      | 184                     |
of average recommended pieces of evidence 10, 20, and 30, respectively. The results are shown in Figure 10. It is obvious to see that \( n_i \) can survive the longest by using TMS.

5. Conclusions

In this paper, a trust management scheme (TMS) based on revised D-S evidence theory is proposed. It provides vector forms to express subjective trust opinions. On this basis, direct trust value on each neighbor node is calculated by considering trust factors which are defined according to node behaviors in order to detect malicious attacks. At the same time, recommended trust value from common neighbor nodes of subject and object nodes is obtained through conditional transitivity and the weight of each recommendation is obtained by revised D-S evidence theory. Afterwards, we use a flexible synthesis method to calculate the overall trust. Furthermore, the Matlab platform is used to test the performance of TMS, and simulation results show that the proposed algorithm can effectively resist vulnerabilities such as on-off attack and bad mouthing attack, reasonably evaluate trust levels of sensor nodes, and improve the network robustness and security. In addition, the flexible synthesis method saves energy greatly and, hence, prolongs the lifetime of WSNs.

Acknowledgments

The authors are grateful to the anonymous reviewers for their insightful comments. This work is supported by the National Natural Science Foundation of China under Grant no. 61201317 and no. 61001138.

References

[1] W. T. Zhu, J. Zhou, R. H. Deng, and F. Bao, “Detecting node replication attacks in wireless sensor networks: a survey,” Journal of Network and Computer Applications, vol. 35, no. 3, pp. 1022–1034, 2012.

[2] M. Saleem, G. A. Di Caro, and M. Farooq, “Swarm intelligence based routing protocol for wireless sensor networks: survey and future directions,” Information Sciences, vol. 181, no. 20, pp. 4597–4624, 2011.

[3] T. A. Zia, “Reputation-based trust management in wireless sensor networks,” in Proceedings of the International Conference on Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP ’08), pp. 163–166, December 2008.

[4] P. Trakadas, S. Maniatis, P. Karkazis, T. Zahariadis, H. C. Leligou, and S. Voulitis, “A novel flexible trust management system for heterogeneous wireless sensor networks,” in Proceedings of the International Symposium on Autonomous Decentralized Systems (ISADS ’09), pp. 369–374, March 2009.

[5] Y. Yu, K. Li, W. Zhou, and P. Li, “Trust mechanisms in wireless sensor networks: attack analysis and countermeasures,” Journal of Network and Computer Applications, vol. 35, no. 3, pp. 867–880, 2012.

[6] Y. L. Sun, Z. Han, and K. J. R. Liu, “Defense of trust management vulnerabilities in distributed networks,” Communications Magazine, vol. 46, no. 4, pp. 112–119, 2008.

[7] H. C. Leligou, P. Trakadas, S. Maniatis, P. Karkazis, and T. Zahariadis, “Combining trust with location information for routing in wireless sensor networks,” Wireless Communications and Mobile Computing, vol. 12, no. 12, pp. 1091–1103, 2012.

[8] H. Deng, Y. Yang, G. Jin, R. Xu, and W. Shi, “Building a trust-aware dynamic routing solution for wireless sensor networks,” in Proceedings of the IEEE Globecom Workshops (GC ’10), pp. 153–157, December 2010.
[9] N. Poolsappasit and S. Madria, “A secure data aggregation based trust management approach for dealing with untrustworthy motes in sensor network,” in Proceedings of the 40th International Conference on Parallel Processing (ICPP ’11), pp. 138–147, September 2011.

[10] R. J. Feng, S. Y. Che, and X. Wang, “A credible cluster-head election algorithm based on fuzzy logic in wireless sensor networks,” Journal of Computational Information Systems, vol. 8, no. 15, pp. 6241–6248, 2012.

[11] G. V. Crosby, N. Pissinou, and J. Gadze, “A framework for trust-based cluster head election in wireless sensor networks,” in Proceedings of the 2nd IEEE Workshop on Dependability and Security in Sensor Networks and Systems (DSSNS ’06), pp. 10–22, April 2006.

[12] W. R. Claycomb and D. Shin, “A novel node level security policy framework for wireless sensor networks,” Journal of Network and Computer Applications, vol. 34, no. 1, pp. 418–428, 2011.

[13] F. Bao, I.-R. Chen, M. Chang, and J.-H. Cho, “Hierarchical trust management for wireless sensor networks and its applications to trust-based routing and intrusion detection,” IEEE Transactions on Network and Service Management, vol. 9, no. 2, pp. 169–183, 2012.

[14] M. Moman, S. Challa, and R. Almouz, “BNWSN: bayesian network trust model for wireless sensor networks,” in Proceedings of the International Conference on Communications, Computers and Applications (MIC-CCA ’08), pp. 110–115, August 2008.

[15] R. Feng, X. Xu, X. Zhou, and J. Wan, “A trust evaluation algorithm for wireless sensor networks based on node behaviors and D-S evidence theory,” Sensors, vol. 11, no. 2, pp. 1345–1360, 2011.

[16] S. Ganeriwal, L. K. Balzano, and M. B. Srivastava, “Reputation-based framework for high integrity sensor networks,” ACM Transactions on Sensor Networks, vol. 4, no. 3, article 15, 2008.

[17] X. Gu, J. L. Qiu, and J. Wang, “Research on trust model of sensor nodes in WSNs,” Procedia Engineering, vol. 29, pp. 909–913, 2012.

[18] E. Aivaloglou and S. Gritzalis, “Hybrid trust and reputation management for sensor networks,” Wireless Networks, vol. 16, no. 5, pp. 1493–1510, 2010.

[19] M.-Z. Zhou, Y. Zhang, J. Wang, and S.-Y. Zhao, “A reputation model based on behavior trust in wireless sensor networks,” in Proceedings of the International Conference on Scalable Computing and Communications- 8th International Conference on Embedded Computing, pp. 189–194, September 2009.

[20] M. Zarei, A. M. Rahmani, A. Sasan, and M. Teshnehlab, “Fuzzy based trust estimation for congestion control in wireless sensor networks,” in Proceedings of the International Conference on Intelligent Networking and Collaborative Systems (INCoS ’09), pp. 233–236, November 2009.

[21] R. A. Shaikh, H. Jameel, B. J. d’Auriol, H. Lee, S. Lee, and Y.-J. Song, “Group-based trust management scheme for clustered wireless sensor networks,” IEEE Transactions on Parallel and Distributed Systems, vol. 20, no. 11, pp. 1698–1712, 2009.

[22] J. Lopez, R. Roman, I. Agudo, and C. Fernandez-Gago, “Trust management systems for wireless sensor networks: best practices,” Computer Communications, vol. 33, no. 9, pp. 1086–1093, 2010.

[23] C. Q. Tian and B. J. Yang, “A D-S evidence theory based fuzzy trust model in file-sharing P2P networks,” Peer-To-Peer Networking and Applications, 2012.

[24] W. R. Heinzelman and H. Balakrishnan, “Energy-efficient communication protocol for wireless microsensor networks,” in Proceedings of the 33rd Hawaii International Conference on System Sciences, pp. 3005–3014, 2000.
