A security routing protocol based on convergence degree and trust

Ling Chen
School of Information Engineering, Chang’an University, Xi’an 710064, China
Email: lchen@chu.edu.cn

Xiaogang Qi*
School of Mathematics and Statistics, Xidian University, Xi’an 710071, China
Email: xgqi@xidian.edu.cn
*Corresponding author

Lifang Liu
School of Computer Science and Technology, Xidian University, Xi’an 710071, China
Email: llflu@mail.xidian.edu.cn

Gengzhong Zheng
Department of Computer Science and Engineering, Hanshan Normal University, Chaozhou 521041, China
Email: zgengz@126.com

Abstract: Wireless sensor networks are commonly used for critical security tasks such as intrusion or tamper detection, so they must be protected. Based on previous research, in this paper, we present a kind of routing protocol based on node convergence degree and the trust value which is named BCDTV. We focus on the security routing algorithm design and work process, including the election of cluster head and the establishment of cluster, the collection and transmission of the sensing information of wireless sensor networks. Simulation results show that the protocol can prevent some malicious behaviour of malicious nodes effectively.

Keywords: wireless sensor networks; convergence degree; trust value; security routing.


Biographical notes: Ling Chen is a Lecturer at Chang’an University, and also a PhD candidate in XJTU. Her main research interests are computational intelligence.

Xiaogang Qi is Professor and member of CCF, ACM. His research interests include graph theory and combinatorial optimisation, network optimisation theory and method and routing and switching.

Lifang Liu is a Professor, and her research interests include algorithm design and analysis, machine learning and pattern recognition in data processing.

Gengzhong Zheng is a Professor and his research interests include wireless sensor networks and topology control, data collection and performance optimisation.
1 Introduction

In recent years, there has been a huge interest in wireless sensor networks (WSNs). With the advancement in technology, many real applications have been deployed and new application areas have rapidly emerged. The sensor networks are composed of numerous resource constrained sensor nodes depending on the application, with a few base stations acting as a gateway to the outside network, such as the internet. Wireless sensor networks are intelligent networks deployed in the monitoring area by a large number of low-cost sensor nodes. Those nodes are organised automatically and collect the information through cooperation (Yang et al., 2015). They have been widely used in various fields, such as military, environmental monitoring, intelligent household and building condition monitoring and so on. Wireless sensor networks work in some special applications, such as monitoring of electroplating of the enemy, detecting the position of incoming attacks in military application, monitoring of bridges or other important buildings, and traffic control.

Large-scale sensor networks usually generate large amounts of data and real-time stream in many cases, and the sensing data may be converted to another format and must be prevented from identification by an unauthorised person. What’s more, most of the wireless sensor networks are deployed in open, not protected areas, so may be affected by a variety of attacks. If we don’t consider the safety problem, the network may have all sorts of problems, such as selective forwarding, and replay attack. It also can import or transmit false messages in the network. At present, due to the stringent constraints of energy supply and computing capability on sensor nodes, the expensive cryptographic operations are unsuitable for tiny sensor devices. What’s more, based on key establishment strategy a network can resist only the external attack. If one node captured by the enemy, the confidentiality, security and integrity of the whole network will be threatened. By introducing node trust value, as pheromone distribution strategy, in the routing protocol, we can solve problems of internal attack and establish safe and reliable data transmission relationship, because the low trust value node can be removed from the network.

As discussed above, the security provisioning for such networks is crucial to route data from source nodes to the destination node, which is also called sink node. However, there are lot of constraints in incorporating security into a wireless sensor network such as limitations in date, communication, and energy capabilities. Therefore, the design of a secure data collection protocol requires consideration of such limitations and achieving acceptable performance levels to meet the needs of specific applications of wireless sensor networks. In this paper, with the existing knowledge, we present a multi-angle and gradual security routing protocol based on the convergence degree and the trust value. In addition, we introduce the definition of the trust value, the convergence degree and the method for calculating the above value. Finally, we discuss our protocol in details, including the election of cluster head and the establishment of cluster of wireless sensor networks, the collection and the transmission of the sensing information from the sensor nodes. Furthermore, we compare our protocol with LEACH under the cluster construction rounds (Du and Wang, 2006) and the node distribution of the topology of the wireless sensor networks. Our protocol can solve the internal security problem of the wireless sensor networks effectively. Also, we provide related figures associated with the two protocols, and LEACH protocol is commonly discussed in the existing related works. Moreover, we so that the proposed protocol can prevent some malicious behaviours initiated by the malicious nodes effectively (He et al., 2014).

The rest of the paper is organised as follows. In Section 2 we highlight the selected related research initiatives. In Section 3, we define the network architecture and describe our novel protocol. We present our solution in Section 4. We then present the performance analysis of our scheme and conclude our paper in Section 5.

2 Background and related work

In the related works, a number of trust-based models have been proposed. We can classify the variation of these models into four categories: the mathematics-based models, the punishment-based models, the probabilistic-based models, and the miscellaneous models (Lopez and Roman, 2010). In recent years, the node trust value assessment schemes of wireless sensor network are generally proposed by Wang and Zheng (2010), Poolsappasit, (2011), and Wu and Zhou (2012) and which are based on the node communication capability, the communication failure or success ratio. Yang et al. (2011) put forward three kinds of solutions, in which the trust value of node is calculated according to the success or failure ratio of the communication, if the communication successes, the trust value increase a constant, otherwise it will be reduce a large number. The trust value accumulation is difficult and slow (each only additive constant c), but its decline is faster. Along with the continuous increase of the number of mistakes, the trust value attenuation abides by the exponential growth. So, this trust value adjustment belongs to a kind of punish-based mechanism. However, this kind of mechanism only considers the transmission, namely the communications trust factors, while it does not consider the trust of relevant data.

Dong and Guo (2009) put forward a multi-parameter trust model based on communication transmission, the data amount and the energy consumption, it becomes more convenient to calculation the trust value of the node, and the model based on multi-parameter trust can judge the credibility of a node more simply and accurately. But the identity of the node in the network is different from each other, so the calculation method of the trust value varies according to the node’s characteristics. Larrea and Martin (2007) propose a gradation fault-tolerant data aggregation method and it considers the different identity characteristics of each node.
Srinivasan et al. (2006) propose a distributed security-based data collection protocol in which the beacon nodes can monitor and provide information, so that sensor nodes can choose which node can be trusted. The reputation of node \( i \) from the trust reputation of node \( k \), and which is evaluated by the changing average value shown as follows:

\[
R_{i,k} = \mu \times R_{i,k} + (1 - \mu) \times \tau
\]  
(1)

where \( \tau \) is the Bernoulli variable. \( \tau = 1 \) if node \( k \) believes node \( i \) is truthful and 0 if otherwise. \( \mu \in [0,1] \) is the weight factor which represents the observer’s preference weight on the past experience of \( i \).

Sun and Yang (2008) put forward a dynamic hierarchical routing protocol which is based on the degree of convergence, this protocol is a very good solution to solve the network node clustering problems and it can also be a very good solution to solve the problem of the node degree of overlap. But this is only a kind of method for solving the routing problem in wireless sensor networks, which does not consider the safety of nodes.

Based on the existing knowledge, we propose a multi-parameter and the gradual security routing protocol based on the convergence degree and the trust value to solve the above problems, and this protocol is named BCDTV, which is based on Convergence Degree and Trust Value. The simulation results show that our protocol can prevent some malicious behaviour of malicious nodes effectively.

3 Trust value and convergence degree

In this section, we introduce the definitions of the trust value and the convergence degree, and the method for calculating them. Then, we describe our novel protocol in details.

3.1 Trust value in WSN

No matter what kind of trust models are employed in the existing schemes, two types of evaluations are available, which are the direct trust value and the indirect trust value. The direct trust value is the information obtained from its neighbours easily. While the indirect trust value is the information obtained from the nodes which are equal to or more than 2 hops. Recommendation mechanism is an important factor in any trust evaluation schemes in which the trust value is obtained from a trustworthy third-party or a recommending way. However, the effectiveness of the recommendation mechanism is closely related to the communication routing overhead, node mobility factor, and so on. Therefore, the inferred trust may incur the additional communication cost (e.g., causing routing congestion) for trust information exchange. Moreover, the routing protocols should be simple and with the minimal communication cost, especially in mobile and resource-limited networks. Owing to the stringent constraints of energy supply and computing capability on sensor nodes, the recommendation trust schemes are not considered in this paper. At the same time, the trust calculation depends on the observations of the subject (the evaluation node) to the object (the node to be evaluated), and it will change with the behaviour of the object. Owing to the characteristics of the self-organising and the multiple-hop in wireless sensor network, we aim to build a trust evaluation mechanism without a core node and without monitoring their behaviour with each other between neighbour nodes.

In monitoring stage, we believe that it can mainly consider three parameters to evaluate the trust of the node: the credibility of the data, the credibility of the communication and the credibility of the energy. We will briefly introduce the above three aspects as follows.

3.1.1 The credibility of the data

According to the sensing data, the factors used to determine whether the node is believable or not can be divided into two parts. The first part is the freshness of sensing data, the assessment is made by its neighbour nodes or monitoring nodes, if the neighbour nodes send the same data over and over again, we can judge that it execute a replay attack. The formula to calculate the freshness of data shown as follows:

\[
FN_{i,k}(t) = \frac{D_{\text{new}}}{D_{\text{new}} + D_{\text{repeat}}}
\]  
(2)

Here, \( D_{\text{new}} \) is the number of the fresh data packets, and \( D_{\text{repeat}} \) is the number of the repeat data packets. The second one is the data consistency between the sensing data. In the local area of a node in wireless sensor network, the sensing data of the neighbour nodes are highly related to each other. We need evaluate the sensing data from the monitoring node with the sensing data from its neighbour nodes, and also compare with their own sensing data with that in the different period. If error occurs in a certain range, we can judge that sensing data is consistent with the data from its neighbour nodes. The formula to calculate the consistency of data shown as follows:

\[
FC_{i,k}(t) = \frac{D_{\text{consistency}}}{D_{\text{consistency}} + D_{\text{inconsistency}}}
\]  
(3)

where \( D_{\text{consistency}} \) means the number of the coincident data packets, and \( D_{\text{inconsistency}} \) is the number of the inconsistent data packets. By the above two aspects, we can define the credibility of the data as follow:

\[
DT = \omega_1 FN_{i,k}(t) + \omega_2 FC_{i,k}(t)
\]  
(4)

where \( \omega_1 \) is the weight of the freshness of data while \( \omega_2 \) is the weight of the consistence of data, \( \omega_1, \omega_2 \in [0,1] \). If we want to find the replay attack, the value of \( \omega_1 \) can be little increased, if we aim to prevent the node’ forged packet, the value of \( \omega_2 \) can be little increased.

3.1.2 The credibility of the communication

In terms of communication, we mainly consider the forwarding rate of the node to judge whether this node
is credible or not. We can evaluate node \( i \) by monitoring its neighbour nodes. If a node receives data only, and does not pass data to outside frequently, we can conclude that this node launches selectively the forwarding attack or the black hole attack etc. We assume that when a forwarding packet is received, the receiving node will send a feedback-information to its neighbour nodes. The calculation of data forwarding rate is as follows:

\[
FF_i(t) = \frac{D_{\text{forward}}}{D_{\text{feedback}}} \tag{5}
\]

where \( D_{\text{forward}} \), as we mentioned before, means the number of forwarding packets, and \( D_{\text{feedback}} \) is the number of feedback information. So, we define the credibility of the communication:

\[
CT = FF_i(t) = \frac{D_{\text{forward}}}{D_{\text{feedback}}} \tag{6}
\]

3.1.3 The credibility of the energy

In the life-time of a wireless sensor network, the network is closely related to the energy of nodes. Node’s energy is mainly used to receive and send data, collect and process data in the process of gathering the sensing information from the sensors. So, it is very important to use the energy reasonably. If some nodes excessively consume the energy of sensor nodes, this reduces the lifetime of the network. So the energy is also an important reference factor to measure the credibility of the nodes. Here, credibility refers to the node’s residual energy, whether below a given threshold or not. So we can judge whether the node can finish the new communications and data processing tasks or not. If the node residual energy is below the threshold, the node energy credibility is zero, if the rest of the node energy is higher than the threshold, the credibility of energy can be calculated as follows.

\[
FE_i = \frac{E_s + E_{sp}}{E_{\text{residual}}} \tag{7}
\]

where \( E_s \) means the consumed energy when a node is receiving and sending packets, and \( E_{sp} \) is the cost of the energy when a node is collecting and processing packets. \( E_{\text{residual}} \) is the node’s residual energy at present. The formula to calculate the credibility of the energy is as follows:

\[
ET = \begin{cases} 
0 & E_{\text{residual}} \leq \varepsilon; \\
FE_i & E_{\text{residual}} > \varepsilon; 
\end{cases} \tag{8}
\]

3.2 Trust computation

In our opinion, the evaluation of a node must monitor a part or all trust factors, and calculate the trust value of a node by the weighted average method. Here, we assume that the previous period of history trust value is \( T(t - 1) \), in order to identify malicious nodes and improve the security of the network, the node comprehensive trust value calculation formula is presented as follows.

\[
T(t) = (1 - \delta)(\alpha DT + \beta CT + \gamma ET) + \delta T(t - 1) \tag{9}
\]

where \( \delta, \alpha, \beta, \gamma \in [0,1] \) and \( \alpha + \beta + \gamma = 1 \). We define \( \delta \) as the weight of the historical factor, that \( (1 - \delta) \) is the weight in the comprehensive trust value, if you want to reference the history trust value more, then you can set \( \delta \) larger.

However, according to the identity of the node position and the role of different nodes, we believe that the calculation method of the trust value is different from each other. Wireless sensor network is a hierarchically network and its nodes can be divided into three classes, which are common nodes, cluster head nodes and forwarding nodes.

In the first place, the importance of cluster head nodes is incomparable between any other nodes. Therefore, the trust value of the cluster head node should be higher than that of other nodes. No matter what the credibility of data, the credibility of communication, or the credibility of the energy requirements, it should be very strict. So, for the candidate cluster head nodes, all the factors are considered to calculate the trust value. The calculation process of trust value for the candidate cluster head node is described as follows: First of all, according to their previous communication between nodes, we set the candidate cluster head node \( i' \) and its neighbour nodes set \( j \). To monitor the reliability of communication and data, the credibility of energy, each node will get \( 3*|j| \) values, then the corresponding average value is set as the trust factors of node \( i' \), the trust of node \( i' \) can be obtained according to equation (9).

Secondly, we aim to evaluate the forwarding node which is mainly used in establishing routing, collecting the perception data, or forwarding to cluster head or base station after the data aggregation, its main function is to forward data to other node in wireless sensor network. Further, in order to calculate the trust value of the forwarding node, it is necessary to consider the choice of the cluster head nodes with high requirements to forwarding data. Our main concern is the trust factors. Accordingly, we make a weighted average between the reliability of communication and the energy, and then a value will be obtained as the trust value of this node.

As for the common node, the sensing data is the only factor which should be considered, so the credibility of data is employed as the trust factors to calculate the trust value of the common nodes.

3.3 The convergence degree of node

We use an undirected graph to represent a wireless sensor network \( G = (V, E) \), where \( V \) recorded as the set of sensor nodes and \( E \) recorded as the set of the communication
links. Assume that \( i \in V \) and \( N_i \) is the set of one-hop neighbour nodes. The formula to calculate the convergence degree is as follows:

\[
d_i = \frac{|e \in (u,v) \in E, u,v \in \{i\} \cup N_i|}{|N_i| + 1}
\]

Equation (10) means the ratio of the degree of the sub-graph to the number of the nodes. If the degree of convergence is much larger, this means that the nodes in the sub-graph distribute more closely.

Consider an example whose topology is shown in Figure 1. Node C has five neighbour nodes, as shown in Figure 1, which are A, B, D, E and F, those nodes all belong to set \( N_c \). There are nine sides in the sub-graph connected by node C and its five neighbour nodes, so the convergence degree of node C is 1.5 according to equation (10). In the similar way, we can calculate that of the other nodes in the network. The convergence degree of each node in the network can be obtained as shown in Table 1.

**Figure 1** Network topology

![Network topology](image)

**Table 1** Parameters of node in network

<table>
<thead>
<tr>
<th>Node</th>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
<th>E</th>
<th>F</th>
<th>G</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of neighbour</td>
<td>3</td>
<td>3</td>
<td>5</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>Convergence degree</td>
<td>1.25</td>
<td>1</td>
<td>1.5</td>
<td>1.25</td>
<td>1.25</td>
<td>1</td>
<td>0.67</td>
</tr>
</tbody>
</table>

### 3.4 Protocol design

In practice, it is not necessary to choose so many factors to be considered when the cluster head nodes should be elected. The more complicated the algorithm the more energy the network will cost. So, this paper mainly chooses the degree of polymerisation, the residual energy and the trust value as the key consideration factors in the process of cluster head nodes election.

The standard of choosing a candidate node as a cluster head node defined in our algorithm is the weighted average of the convergence degree, the trust value and the residual energy of the candidate nodes. All nodes collect the information of the neighbour nodes through exchanging the control message. After the execution of these above steps repeatedly, each node will get the ID of its one-hop neighbour nodes and its degree of aggregation. Then, we select the top \( K \) nodes as the candidate cluster head nodes and calculate their comprehensive trust values respectively. By setting an energy threshold \( E_{\text{threshold}} \), the node with the largest comprehensive trust value and its own energy satisfying this threshold will be elected. If one candidate node is elected, the candidate one will send a message which declares itself as the cluster head. When the cluster head node is confirmed, all neighbour nodes of the cluster head will receive the release news and announce to join in the cluster. This process is divided into the following five steps as shown in Figure 2.

**Figure 2** Diagram of BCDTV (see online version for colours)

- **Step 1**: Judge the energy of the cluster head nodes.
  - When the cluster head nodes’ energy is less than the threshold value or the network operated after a period of time, the current cluster head releases the election information to elect a new cluster head node.

- **Step 2**: Get information of neighbour nodes.
  - Node \( i \) broadcasts its own ID and its neighbour nodes’ IDs that have been known actively in the earlier time. All one-hop neighbour nodes will receive a receipt, and then update their neighbour nodes’ list, mark the interconnection one-hop neighbour nodes, and broadcast their own ID and the known neighbour node ID to the other nodes. When all nodes sent out these messages, each node will know its one-hop neighbour nodes and their interconnection conditions.

- **Step 3**: The convergence degree computation.
  - According to the information of above steps, the convergence degree of the node \( i \) can be calculated, and it will be broadcast.
A security routing protocol based on convergence degree and trust

After a certain period of time, all nodes will get the convergence degree one by one. Because node $i$ knows the convergence degree of its each neighbour nodes, the nodes with the largest convergence degree will be selected as the candidate cluster head nodes.

**Step 4:** Cluster head election and the establishment of the cluster.

We compute the trust value of the candidate nodes respectively and broadcast it in the network. All the candidate nodes will perform the following operations. If the trust value of one node is the largest one among all candidate nodes and the residual energy is higher than the configured threshold, this node will become the cluster head node and broadcast this message to all nodes in the network. Otherwise, the trust value of one node is the largest one among all candidate nodes will be elected as the cluster head node, if and only if the residual energy is higher than the configured threshold.

**Step 5:** Transmission stage.

After the structure of the cluster is established, all nodes will enter the data transmission phase. Cluster head nodes set up a time division multiplexing scheme for the rest member nodes, and send to all members within the cluster by multicast or broadcast way. Member nodes receive the message, send their data in their respective time slot (data contains its own confidence). After all members of the cluster finish the transmission of the sensing data, the cluster head nodes will aggregate data according to the trust. If the trust value is lower than a certain value, the cluster head node will throw the data directly. It will compress into a new signal and send it to the base station or the nodes near to the base station after aggregating all data. Forwarding node selects the next node according to the trust value.

a. If two nodes in a cluster are equal to each other in the convergence degree, the trust value and energy, then the node with the minimal ID will be elected as the cluster head node.

b. If a node receives a message from a cluster head, at the same time it doesn’t belong to any cluster. Afterward it will release a message for joining in this cluster. Otherwise, it has added to another cluster, and thus no operation should be executed.

c. If a node does not receive any message from the cluster head nodes, but it receives the joining request message, then it will mark the node as crusted and set a time threshold value. After a certain time, this node will become an independent cluster head.

d. When a cluster head node receives the joining message, this state that a node request to join in the cluster, the cluster head node should insert it in the list of cluster members.

### 4 Simulation and experimental results

#### 4.1 Parameter setting

In this paper, we simulate our scheme with VC ++ 6.0. The parameters in our simulation are shown in Table 2, and the maximum communication range is 30 metres, the threshold waiting for the event set to be 30 ms. When we calculate the trust value by the weighted average, the weights are set as follows.

$$\alpha = \beta = \gamma = \frac{1}{3}.$$

<table>
<thead>
<tr>
<th>Table 2</th>
<th>Simulation parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameter</td>
<td>Values</td>
</tr>
<tr>
<td>Simulation area</td>
<td>(0,0) ~ (100,100) m</td>
</tr>
<tr>
<td>The position of sink</td>
<td>(50,50) m</td>
</tr>
<tr>
<td>$N$</td>
<td>100</td>
</tr>
<tr>
<td>Initial energy of node</td>
<td>1 J</td>
</tr>
<tr>
<td>$E_{\text{elec}}$</td>
<td>50 nJ/bit</td>
</tr>
<tr>
<td>$\varepsilon_{\text{mp}}$</td>
<td>0.0013 pJ/(bit*mb^4)</td>
</tr>
<tr>
<td>Packet size</td>
<td>1000 bit</td>
</tr>
</tbody>
</table>

The history coefficient $\delta = 0.5$, 90% of nodes are member nodes, while 10% of nodes are the malicious sensor nodes in the simulation network. The members of the malicious nodes join the nearest cluster according to the distance, send their replicated or faked packets repeatedly, or refuse to send the sensing packets, disturb the cluster head node in data transmission and fusion. Simulation structure diagram is shown in Figure 3.

**Figure 3** Schematic diagram of simulation (see online version for colours)

#### 4.2 Simulation results

First of all, we analyse the stability of the proposed scheme. Our standard is that a stable clustering protocol should have the stable number of cluster heads. Accordingly, we
compare our scheme with LEACH under this standard. By choosing 100 rounds from the process of simulation and checking the number of cluster heads generated according to the above schemes. The results are shown in Figure 4.

**Figure 4** Two protocols generated the number of cluster head nodes distribution statistics (see online version for colours)

![LEACH](image1.png)

![BCDTV](image2.png)

Owing to simplicity LEACH protocol can be used in a random scale network and a configured threshold way to elect the cluster heads, the number of cluster head fluctuation is larger than that by the other existing schemes. Our scheme can be used in the local candidate node competition, which can control the number of cluster heads. The convergence degree of each node by our scheme is lower than that by the other existing schemes. In other words, our scheme may configure some nodes into the sleep mode, and will not participate in the sensing task. For instance, if node degree of aggregation equals 0, it shows that the node has no neighbours and becomes an isolated node in the network. Based on the degree of aggregation to build cluster will be more symmetrical because the radius of node communication.

It is more symmetrical after we introduce the convergence degree into the network. Furthermore, the trust value is also used in our scheme. As we can see in the figure, it is hardly that the malicious nodes exist in the network as the cluster head node. The reason is that the trust value of this node is much lower than that of any other node, so it is difficult to have the opportunity to become a cluster head node in the network. A part of the malicious nodes will regard as the dead node to be neglected, because the trust value is also too low. The convergence degree of each individual node is too low and it will be regarded as an isolated node.

When malicious nodes join into the network, LEACH algorithm doesn’t take any measures to check the malicious nodes, the simulation of the topological structure is as shown in Figure 5. Compared with LEACH algorithm, the topological structure by BCDTV scheme shown in Figure 6 under network attacks is extremely symmetrical. It is obvious that the number of cluster head nodes by our scheme is larger than that by LEACH algorithm. The key factor leads to this result is that BCDTV scheme builds the cluster based on the convergence degree of each node in the network, the radius of the cluster is much shorter, so the number of cluster head nodes by BCDTV scheme is larger than that by LEACH.

**Figure 5** Cluster of LEACH algorithm under network attacks (see online version for colours)

**Figure 6** Cluster of BCDTV algorithm under network attacks (see online version for colours)

5 Conclusions

This paper puts forward a security routing protocol which is based on the convergence degree and the trust value of the nodes in the wireless sensor network. The core idea of this algorithm is to select a suitable cluster head node according to the credibility of the data, the credibility of the communication, the credibility of the energy and the convergence degree of each candidate node.

At the period of information transmission, the next node used to forwarding data is selected by the trust value of the candidate nodes. But every node has different roles in the
A security routing protocol based on convergence degree and trust

wireless sensor network, the method for computing it may be different. Simulation results show that the proposed protocol can prevent some malicious behaviour by malicious nodes effectively.

In the near future, wireless sensor networks are becoming a part of our everyday life. With the sensors become smaller and more capable, their potential valuation will continue to be increased. However, the security of the wireless sensor networks should be solved in many critical scenarios.

Acknowledgements

This work is partially supported by the National Natural Science Foundation of China (Grants Nos. 71271165, 61373174, 61572435), the Natural Science Foundation of Shaanxi Province (Grants Nos. 2015JZ002, 2015JM6311), the Natural Science Foundation of Zhejiang Province (Grant No. LZ16F020001), the High Level Talents in Colleges of Guangdong Province (Guangdong Finance Education [2013] No. 246), the Natural Science Foundation of Guangdong Province (Nos. 2014A030307014, 2015A010103015), and the Central University Basic Scientific Research Funding (JB140712).

References


