A Secure Routing Protocol Based on Reputation Mechanism

Yanhui Lv, Kexin Liu, Deyu Zhang, and Zhuo Miao
(Corresponding author: Yanhui Lv)

College of Information Science and Engineering, Shenyang Ligong University
6 Nanping Middle Rd, Hunnan Qu, Shenyang 110168, China
(Email: yanhuilv@126.com)

(Received May 4, 2017; revised and accepted Aug. 28, 2017)

Abstract

The wireless sensor network is often deployed in harsh and unattended environment and is easily attacked and interfered due to its vulnerability. Most of routing protocols for wireless sensor network were initially designed for saving energy and had less consideration on security. In view of this, a secure routing protocol based on reputation mechanism is proposed. Firstly, considering at the problems of trust mechanism including complex computation of trust value and excessive energy consumption, a binomial distribution reputation mechanism (BDRM) is presented. On this basis, aiming at the deficiency of current routing protocol in security defense, a secure routing protocol ST-GEAR is designed. This protocol has a better ability to defend against attacks by introducing the secure bootstrap model and the BDRM in the routing. The simulation results show that the ST-GEAR routing can improve the transmission rate of packet and reduce the loss rate of packet and energy consumption.

Keywords: Reputation Mechanism; Secure Bootstrap Model; Secure Routing; Wireless Sensor Network

1 Introduction

The wireless sensor network (WSN) is a distributed network formed by a lot of randomly distributed sensor nodes with perception, computing and processing ability of data by self- organization [4]. The nodes can send the received information after being gathered and integrated to specific nodes in order to play a role of the real- time perception and monitoring to the target region.

WSN was mainly applied in military field at first, while its application has expanded to traffic management, environmental monitoring, smart home, medical care, manufacturing industry and other fields with the continuous development of network technology. WSN can solve some issues that cannot be achieved by traditional network, and this is also an important reason why WSN is highly valued and studied deeply.

Comparing with traditional network, WSN has a larger amount of nodes, and the energy of each node is limited. By the self- organization, the nodes form a network whose topological structure has dynamic changes. These features of WSN itself result in limited defense ability of sensor nodes and vulnerable network which is easily attacked. The nodes in the network adopt the wireless communication transmission, which will easily influence the normal network communication once the transmission is interfered. Besides, WSN is often deployed in harsh and unattended environment, which make it face serious security issues. Only when the security of WSN is guaranteed, can it be applied in corresponding fields to exert its advantages. In order to effectively solve the security issues of WSN, researches are mainly carried out from the perspective of key management, intrusion detection, secure routing and secure data fusion.

In WSN, each node has a possibility to become a routing node. The network layer routing protocol is responsible for processing the received data by nodes and transmitting the data to the target nodes along the set routes. If there are attackers in the node communication process in network, attackers can use some methods to break the normal packet transmission between nodes or intercept some useful information in network, which will have an impact to the network and even lead to network paralysis. To guarantee the data transmission security in WSN, it is necessary to study the secure routing protocol for wireless sensor network [19].

Currently, there are many routing protocols of wireless sensor network being proposed, and most of them are initially designed for saving node energy and extending network lifetime, such as LEACH [5], GEAR [17], and other routing protocols [14]. However, these routing protocols are rarely considerate the security of routing protocol and it is easy to make them not work anymore if they are attacked by attackers in certain ways.

Aiming at defense methods to attacks by analyzing the attack type that routing protocol easily suffers, a secure routing protocol based on reputation mechanism is proposed in this paper. Firstly, a binomial distribution reputation mechanism (BDRM) based on Beta distribution is proposed. The BDRM calculates the node trust value by the node energy and communication process, and simplifies the computation complexity. Then, a secure bootstrap model is given, which can ensure that the information transmitted between nodes is encrypted so that the security of data transmitted in the network can be improved. On this basis, a security trust - geographical and energy aware routing protocol (ST-GEAR) is presented combining the BDRM, secure bootstrap model and GEAR to improve the security of GEAR routing protocol. When ST-GEAR protocol selects the next hop forwarding node, it will consider the following aspects including node energy, distance and node trust value, and select the node with minimum comprehensive cost.

The rest of the paper is organized as follows. Section 2 introduces the research status. Section 3 describes the proposed binomial distribution reputation mechanism (BDRM) in detail. On this basis, Section 4 presents a security trust geographical and energy aware routing (ST-GEAR). Section 5 reports the simulation results. Concluding remarks and future directions are given in Section 6.

2 Research Status

In 2003, Karlof and Wagner initiated to study the secure routing issues of WSN, analyzed the situation that existing routing protocols are easily attacked in details and also studied the security measures for defending attacks [6].

Reference [1] explains the ways that the WSN routing protocols are easily attacked in details and also concludes the defense mechanism of each attack. Reference [18] summarizes the data security standard. The data security index mainly includes data acknowledgement, data authorization, data integrity and data update. The reference also proposes SNEP (Secure Network Encryption Protocol) and TESLA (Micro Timed Efficient Streaming Loss-tolerant Authentication Protocol). SNEP can realize data confidentiality, usability, integrity and timeliness; TESLA applies delay to send keys one by one to achieve the digital signature and further realizes the data acknowledgement. Reference [2] introduces 4 security mechanisms based on symmetric key technology in details. The introduction of security mechanism into routing protocol can effectively protect routing protocol from attacks to improve network security.

Besides, there are also some representative secure routing protocols as follows.

The trust routing TRANS [15] based on location establishes the trust routing according to geographical location of nodes and isolates the malicious nodes in the network. The protocol judges whether a node is safe or not by the node trust value. The nodes with large trust value are safer and therefore such nodes should be chosen when routing and the nodes with small trust value should be isolated. The TRANS protocol uses the loose time synchronization mechanism in the process of authentication requests between nodes and most of operations are completed by base station.

The secure routing LKHW [12] based on logical key hierarchy is proposed for solving security issues of DD routing protocol. The logical key hierarchy LKH is applied in order to improve the security of DD protocol in multicast. The key that each node obtains in the network is allocated by base station one by one. Logically, the keys obtained by all nodes can be considered as a tree with the base state as the root. Only two nodes that are the child nodes under the same root node have the same key to communicate with each other.

The SEEM [10] called secure and energy-efficient multipath routing protocol selects the routing by the base station that will choose the path with most optimal energy as the next hop forwarding path. In this protocol, each node only needs to know its own routing information to the base station, which can reduce the energy consumption and avoid being attacked.

A two-layer authentication protocol with anonymous routing TAPAR for wireless ad hoc networks is proposed in [7]. A novel solution is introduced without resorting to PKI operations to achieve anonymity between two communication entities over insecure networks.

Aiming at the security issues that LEACH routing protocol is easily attacked by Hello Flood and so on, reference [16] introduces security mechanism and frame of SPINS into the LEACH, proposes the secure low- consumption self- adaptive SLEACH routing protocol and applies the encryption method to guarantee the security of routing protocol. Moreover, other typical algorithms can reference [8, 11, 13].

However, the existing routing protocols at present still have some disadvantages in security defense. For this reason, aiming at the ways that network layer routing protocol are easily attacked, this paper designs a secure routine protocol to improve the network security.

3 BDRM

Considering the problem that routing protocols easily suffer insider attack, a binomial distribution reputation mechanism (BDRM) is presented. The node trust value is calculated by the energy and the communication process of the node. The comprehensive node trust value can be used as a basis for identifying a malicious node and will be applied to the routing in the next section.

3.1 Energy Trust Value

In the trust mechanism, if the trust value of a node is large, the number that the nodes participate the routing will increase and then will increase the energy consumption of the nodes. This can cause these nodes to fail prematurely. In order to avoid this problem, the node residual energy as well as other factors is considered when computing the node trust value in BDRM. For the sending node i and receiving node j, the calculation formula of node energy trust value ER_{ij} of node i against node j is shown in Equations (1) and (2).

$$ER_{ij} = \begin{cases} \frac{E_j}{E} & ET_{ij} \geq \theta \\ 0 & ET_{ij} < \theta \end{cases} \quad (1)$$

$$ET_{\mathrm{ij}} = \frac{E_j}{(E_{tx} + E_{rx})} \quad (2)$$

Where, E represents the initial energy of node; E_j represents the current residual energy of node j; E_{tx} represents the energy consumption of node i by transmitting the message; E_{rx} represents the energy consumption of node j by receiving the message; ET_{ij} represents the energy trust evaluation parameter of node i against node j; represents the setting threshold of node energy.

When ET_{ij} is greater than or equal to the threshold, it represents that node j can be trusted. At this time, the energy trust value of node j can be calculated. Otherwise, it represents the energy of node j cannot be trusted.

3.2 Calculation of Direct Trust Value

A node has two basic communication processes for forwarding the packet. One is that the node forwards the packet normally, and the other is that the node forwards the packet abnormally. This packet forwarding interaction can be simulated by the binomial distribution, and the direct trust value of node can be calculated.

Suppose the times of packet forwarding between two nodes is m, where, the times of normal packet forwarding is denoted by a, and the times of abnormal packet forwarding is denoted by b. At the same time, the probability of normal packet forwarding is assumed as p. Then, the probability distribution of p can be obtained by the binomial distribution as shown in Equation (3).

$$f(p) = \frac{(a+b)!}{a!b!} p^a (1-p)^b \quad (3)$$

Because $f(p)$ is the probability distribution function, the maximum value of the function can be used to present the value of p. Set

$$f'(p) = [\frac{(a+b)!}{a!b!} p^a (1-p)^b]' = 0 \quad (4)$$

By solving Equations (4), the value of p can be obtained as follows.

$$p = \frac{a}{a+b} \quad (5)$$

Assume that the trust value of node i against node j is represented by TD_{ij}, then the value of p is the value of TD_{ij} that obeys the binomial distribution B $(a+b,\, a)$, i.e. $TD_{ij} \sim$ B $(a+b,\, a)$. Thus, Equation (6) is gotten.

$$TD_{ij} = \frac{a}{a+b} \quad (6)$$

Within the communication range, a node judges whether its neighbor node normally receives the packet by a way of single- hop acknowledgement. The specific description is shown as follows.

The node i sends packet to node j and require node j to return to it an Ack after receiving the packet. Node i compares the copy it saves with the received Ack. If they are the same, it proves that node j normally receives the packet from node i; otherwise, it means the node j does not receive the packet.

In addition, a node uses the two- hop acknowledgement to judge whether its neighbor node normally forwards the received packet. The specific description is shown as follows.

After the node i has confirmed the node j normally receives the packet, node j should further forward the received packet. Suppose the forwarding node is node k, after node k receives the packet, it needs to send two Acks. One is for node j to let the node j know that node k normally receives the packet. The other is for node i, and node i will also compare the Ack with the copy after receiving the Ack form node k. If they are the same, it proves that node j is normally forwarding the packet of node i; otherwise, it indicates that node j does not normally forward the packet of node i. There may be something wrong with node j; perhaps, the node j itself is a problematical node.

3.3 Calculation of Indirect Trust Value

For the node i and node j, they may have some common neighbor nodes. If node i is able to ensure the credibility of these neighbors, it evaluates the node j by these neighbors, which is the indirect trust value of node i against node j. Let node N_1 is one of the common neighbor nodes of node i and node j, next, we use an example to illustrate the computing process of the indirect trust value.

Firstly, node i sends a request packet to node N_1 for calculating the indirect trust value of node j. After N_1 receives the request packet, it will send a response packet to node i, which includes the latest trust parameter value $(a_{N_{1j}}, b_{N_{1j}})$ on the evaluated node j.

According to the trust parameter value of node j sent by N1, node i calculates the indirect trust value $TD_{N_{1j}}$ against node j, and the calculation formula is shown in Equation (7).

$$TD_{N_{1j}} = \frac{a_{N_{1j}}}{a_{N_{1j}} + b_{N_{1j}}} \quad (7)$$

If node i receives n valid indirect trust values from neighbors, and they are TD_{1j}, TD_{2j}, TD_{3j}, $\cdots$, TD_{nj}, respectively. Take the average value of these values as the indirect trust value TI_{ij} of node i against the evaluated node j, and the calculation formula is shown in Equation (8).

$$TI_{ij} = \overline{TD_{Nkj}} = \frac{\sum_{k=1}^{n} TD_{Nkj}}{n} \tag{8}$$

3.4 Calculation of Comprehensive Trust Value of Nodes

From Equations (1), (6) and (8), we can obtain the node energy trust value ER_{ij}, direct trust value TD_{ij} and indirect trust value TI_{ij} respectively, and the direct and indirect trust value are actually the trust value of node in the communication process. So, the trust value in the communication process is the integration of the value TD_{ij} and TI_{ij} and is represented by TC_{ij}. The calculation formula is shown in Equation (9).

$$TC_{ij} = \alpha TD_{ij} + \beta TI_{ij} \tag{9}$$

Where, α and β represent the weights of TD_{ij} and TI_{ij}, respectively, and they satisfy the equation α+β=1, α>0, β>0.

The choice of weights of and will influence the trust value of node in the communication process. When α>0.5, it signifies the node has more trust in TD_{ij} and less consideration to TI_{ij}. While, the result will be opposite if β selects a larger value.

Oh this basis, the comprehensive trust value T_{ij} of node is calculated based on the energy and the communication process of node. It is the integration of the trust values of TC_{ij} and ER_{ij} and the calculation formula is shown in Equation (10).

$$T_{ij} = \omega TC_{ij} + \gamma ER_{ij} \tag{10}$$

Where, ω and γ denote the weights of TC_{ij} and ER_{ij}, and they satisfy the equation ω+γ=1, ω >0, γ >0.

3.5 Update of Node Trust Value

Each transmission of the trust value between nodes will consume some energy of the nodes. Considering the energy consumption of node itself, the BDRM uses periodic updates to update the node trust value. Each node is to update its trust value according to its own trust update period (TUP), and the calculation method of TUP is shown in Equation (11).

$$TUP = 3 \times (b\text{int} + drate \times b\text{int}) \tag{11}$$

Where, *bint* denotes the time interval of communication between nodes, and *drate* denotes the number of the packets sent per second.

Within the TUP of node, the communication process and energy of node will have some changes and therefore, the comprehensive trust value of node will also change. The following example will have a specific explanation.

For the node i and node j, suppose that the two nodes have m $(m = a + b)$ communication process, after that, they interacts w times again. Among the w times, the times of normal and abnormal packet forwarding are r and s respectively, i.e. w=r+s. The latest direct trust value TD_{ij}^{new} of node i against node j within the TUP also obeys the binomial distribution B(m+w, a+r), i.e. $TD_{ij}^{new} \sim$ B $(m+w, a+r)$ that is shown in Equation (12).

$$TD_{if}^{new} = \frac{a+r}{m+w} = \frac{a+r}{a+b+s+r} \tag{12}$$

Correspondingly, the energy trust value and indirect trust value of node i against node j will change, and the updated value T_{new} will be obtained.

4 Design of ST-GEAR Secure Routing Protocol

Among the geographical location based routing protocols, comparing with other routing protocols, the GEAR protocol has more advantages, and that is why this paper takes GEAR protocol as a research object. Aiming at the deficiencies in the defense of GEAR protocol, a security trust - geographical and energy aware routing (ST-GEAR) protocol is proposed to improve the security of GEAR. The BDRM and the secure bootstrap model are introduced in the ST-GEAR, which makes it have a better ability to resist attacks.

4.1 Design of Secure Bootstrap Model

The secure bootstrap model is the protection mechanism of wireless sensor network. The nodes in the network form a secure communication network based on identity authentication, encryption key and authentication key, and among them the core is to establish the key. After confirming the key between nodes, the packet transmitted between nodes is the encrypted packet. Only after decrypting the packet with decryption key, can the nodes obtain the original data, which improves the security of information transmission between nodes.

In WSN, there are many key management schemes. The simplest one is the pre- shared key scheme which means that only one symmetric key is shared among all nodes in the network, but this way is too dependent on the sink node. In fact, the random key pre- distribution scheme is more widely used. There is a large key pool in the random key pre- distribution scheme. Each node has a portion of keys in the key pool, and only the nodes with the same pair of key can establish a connection to form a secure transmission path. In the random key predistribution scheme, a node just needs to store a portion of keys of the key pool, which can reduce the key storage space. For each sensor node In WSN, the storage capacity and computing power is limited, so it is feasible to choose the random key pre- distribution scheme. Considering that the performance of the random key pre- distribution scheme can be improved to some extent by combining it with the geographic location of node, a random key predistribution scheme based on grid deployment model is proposed in this paper.

Suppose there are n sensor nodes being randomly deployed in WSN, and each node can store m keys. The location information of each node can be known in advance, so we will consider it as the ID of node in order to distinguish each node, showing as $ID_i (i = 1, 2, 3, \cdots, n)$.

1) Initialization Phase of Key
In the network initialization, each node should be allocated with key. Each node IDi randomly selects m nodes from other nodes around it and generates m node pairs. Each node pair (IDi, IDj) is allocated with corresponding key. Thus, an n×m common matrix P can be created according to the node number n and node number m being randomly selected.

   Meanwhile, the sink nodes in the network can build a random n×n symmetric matrix S which is only known by the sink nodes themselves and confidential to others. Thus, the matrix $A = (SP)^T$ can be calculated. Next, store the element of i^{th} row of A and the i^{th} column of P in node i; store the element of j^{th} row of A and the j^{th} column of P in node j. When the shared key for communication between node i and node j is needed to be established, they should exchange their own information, and take the product of the i^{th} row of A and the j^{th} column of P as the key k^{ij} of node i and consider the product of the j^{th} row of A and the i^{th} column of P as the key k^{ji} of node j. because S is symmetric, it is easy to get the Equation (13).

$$\begin{aligned} K &= (SP)^T P = P^T S^T P \\ &= P^T SP = (AP)^T = K^T \end{aligned} \quad (13)$$

   Therefore, the node pair (IDi, IDj) takes k_{ij}=k_{ji} as the shared key.

2) Grid Deployment Model
In WSN, the communication range of sensor node is round, so there must be certain overlapping parts within the communication range between nodes. To reduce the overlapping parts, the grid deployment model is used. The grid deployment model is to deploy several virtual regular polygons in WSN, making them cover the whole network as much as possible. By comparing regular polygons including square, equilateral triangle and regular hexagon, we can know that the overlapping area of regular hexagon is smaller than that of both. Therefore, we choose the regular hexagon to be as the deployment model [9].

3) Key Establishment
The next phase is to establish the key. Firstly, each node should broadcast its own location information to the nodes around itself. According to the location information, it is easy to know whether there is a shared key between the two nodes.

   In addition, each regular hexagon unit uniquely shares a common matrix with its adjacent unit. Thus in the key establishment phase, each node in a unit and the node in adjacent unit can exchange their ID in the network to confirm the key pair. The key pair is unique to each node pair.

   After finishing the key establishment, each node pair with shared key has a connection line. According to the connection lines, the whole network forms a connection graph. Further, based on each connection line in the connection graph, each node in the network can find the node with the shared key one by one, and the connection path composed by these nodes is safe.

4.2 Design of ST-GEAR Secure Routing

When a node selects a neighbor node as the next hop forwarding node, it needs to consider the following factors including the location, residual energy and trust value of the node, and chooses the node with minimum comprehensive cost value from the neighbor node to the target node. For a forwarding node j, the calculation formula of comprehensive cost Cc (j, D) from the node j to target node D is shown in Equation (14).

$$Cc = \alpha \times (\beta d(j, D) + (1 - \beta)E_j) + (1 - \alpha)(1 - T_{ij}). \quad (14)$$

Where, d $(j,$ $D)$ denotes the distance from the node j to node D; α and β are the adjustable ratio parameters between 0 and 1.

For a node i, when it needs to select a neighbor node as the next hop forwarding node, the specific description of routing algorithm is shown as follows.

1) The node i needs to confirm whether it has neighbor nodes or not.

2) If the node i has neighbor nodes, it needs to choose a node such as node j. Next, to judge whether the energy of node j satisfies the energy threshold set in the network. If it does, go to step (3); if not, the node i needs to broadcast the message that the node j is with less energy.

3) In the case that the energy of node j satisfies the requirement, the node i needs to further determine whether the node j is reliable by its trust value. If the trust value of node j is smaller than the trust threshold set in the network, the node i needs to broadcast the message that the node j is with small trust value.

4) Only when the energy and trust value of node j are greater than corresponding threshold, can the comprehensive cost of node j be calculated. For node i, there may be multiple neighbor nodes satisfy above requirements. The node i will select the node with minimum comprehensive cost as the next hop forwarding node.

In addition, the data transmitted between nodes is the encrypted packet. Only after decrypting the packet with decryption key, can the nodes obtain the original data. In ST-GEAR protocol, the sink node will query data in target region to obtain the corresponding information. According to the location of target region, the sink node will send the query command to the target region. This process will be divided into two parts: the first is that the sink node sends query commands to target region, and the second is that the query command is transmitted in target region.

When the sink node sends a query command to target region, it selects the next hop node to forward the message. The message sent by sink node is encrypted, and only the selected next hop node can decrypt the encrypted message, can the node send the message continuously. For node j, when it receives the message sent by node j, it needs to decrypt the message with the shared key k_{ij} to get the location information of the target node. Repeat this process until the target node is found. After a query command sent by the sink node arrives in the target region, it can be transmitted using different strategies according to the distribution of nodes in target region. Firstly, set a threshold for the number of nodes according to the node distribution in target region. If the number of nodes is greater than the threshold, the recursion method to transmit the message can be used. Otherwise, the flooding method can be used to broadcast the message directly.

5 Simulation Experiment and Analysis

In this section, the simulation environment and performance index will be given firstly. Then, the simulation results of ST-GEAR protocol are presented.

5.1 Simulation Environment and Performance Index

The simulation scenario is set to a square monitoring region that the side length is 100 m. There are 100 wireless sensor nodes are deployed randomly. The specific simulation parameters are shown in Table 1.

5.2 Analysis on Simulation Results

There are many ways to attack the routing protocol. In this simulation experiment, the selective forwarding attack is adopted that means a node will not forward the packet after receiving. The specific simulation results and analysis are shown as below.

- Simulation analysis of the BDRM

Figure 1 shows the trust value simulation results of normal and abnormal nodes. The initial trust value of node is set to 0.5. After a number of packet transmission, the trust value of a normal node tends to 0.9, while the trust value of an abnormal node tends to 0.1. If the node trust value is small, this node can be considered as a malicious node that will not be chosen in the routing.

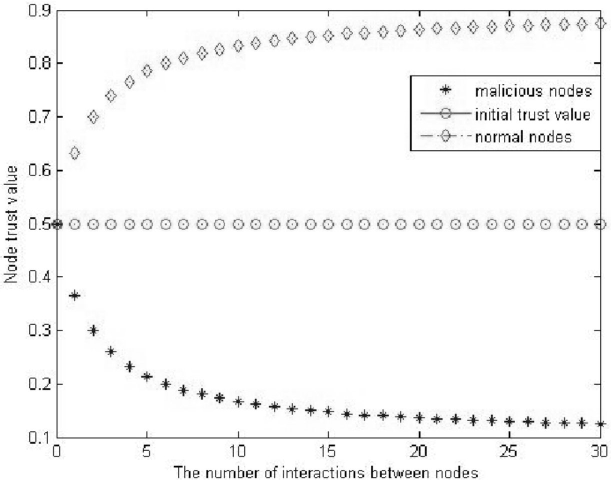

Figure 1: Node trust value

Next, make a simulation comparison between BDRM proposed in this paper with classic BRSN [3], and the results are shown in Figure 2 and Figure 3. The node trust value is an important basis for routing algorithm and the node can be judged whether it can be trusted by the node trust value. In BDRM, the node trust value is calculated based on the node energy and communication process; while in BRSN, it does not take into account the energy factor. From Figure 2, we can see that there are some difference between node trust value calculated by BDRM and BRSN. The trust value of BRSN obeys Beta distribution, while the BDRM obeys binomial distribution. The uptrend of normal node trust value calculated by BDRM is more stable than that of node trust value calculated by BRSN.

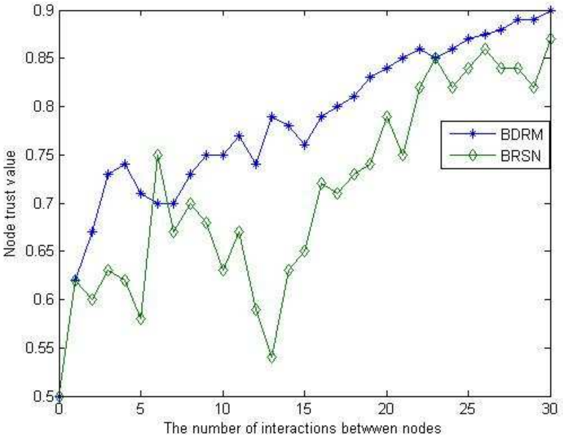

Figure 2: Trust value of normal node

Table 1: Specific parameters of simulation

Simulation Parameters	**Values**
number of nodes	100
communication radius of node	50m
initial energy of node	2J
energy consumed by sending or receiving a packet	0.001J
packet length	36bit

On the contrary, when there are malicious nodes in the network, the BDRM and BRSN can recognize the malicious node by the node trust value. As can be seen from Figure 3, the trust value of malicious node calculated by BDRM is on a downward trend from the initial trust value of 0.5. Comparing with BRSN, the trust value of malicious node in BDRM changes significantly, this can improve the probability of identifying the malicious nodes in the network.

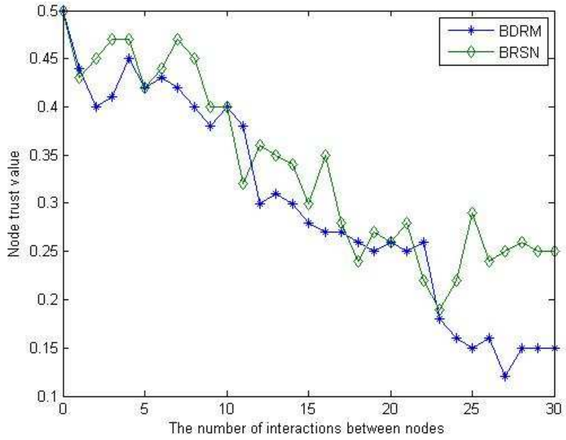

Figure 3: Trust value of malicious node

- Simulation analysis of ST-GEAR protocol.

The simulation results of routing, transmission rate of packet, loss rate of packet and energy consumption rate are given as follows.

1) Routing Simulation from Source Node to Target Node
Set a source node and a destination node randomly. Define the source node as the current node and calculate the distance from the current node to destination node.

Normally, when the network is not attacked, the selected path from current node to destination node is shown in Figure 4. The node will choose the path with the minimum cost according to the distance to target node and the residual energy of node.

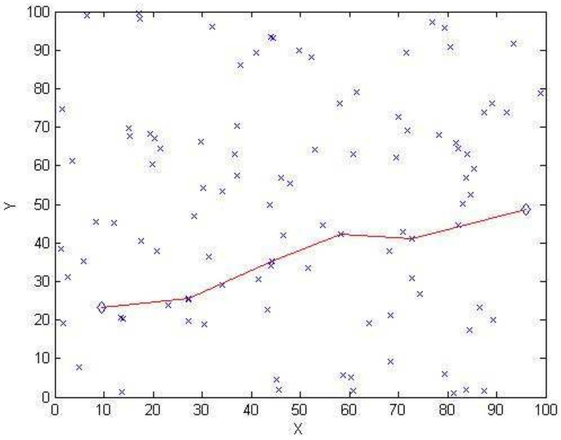

Figure 4: Normal routing

When the network is attacked which means there are some malicious nodes in the network, the nodes with small trust value can be found based on BDRM. In the routing process, the node will choose the path with the minimum cost according to the node trust value as well as the distance and the residual energy of nodes. The node with small trust value can not participate in the routing process. The simulation result is shown in Figure 5.

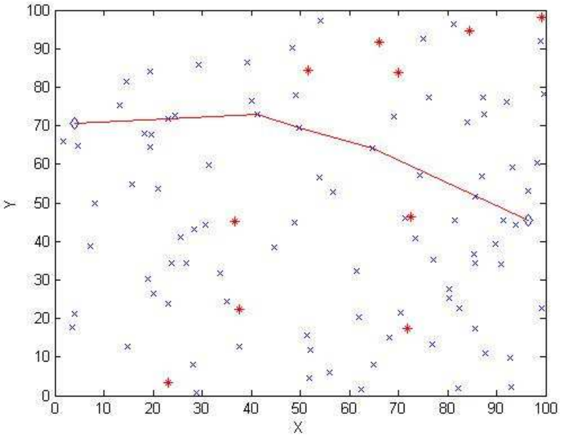

Figure 5: Routing with malicious nodes

2) Transmission Rate of Packet

When there are attacking nodes in the network, the transmission rate of packet in ST-GEAR, E-GEAR and GEAR are shown in Figure 6.

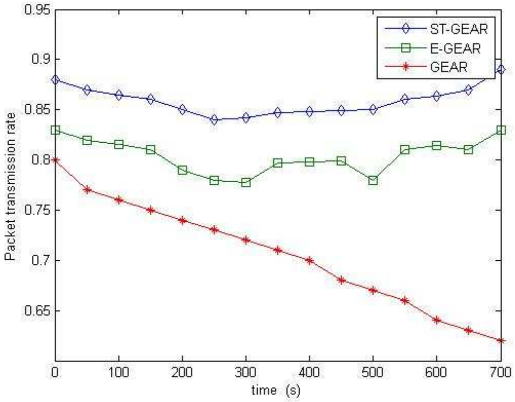

Figure 6: Transmission rate of packet

As shown in Figure 6, the transmission rate of packet in GEAR decreases gradually with time. While, the transmission rates in ST-GEAR and E-GEAR are relatively stable. This is because the node trust mechanism is introduced into the ST-GEAR and E-GEAR, and the node trust value is used as an important factor when routing. The trust value of attacking node will be reduced over time, and when a node selects the next hop, the node with small trust value will not be chosen. In addition, the transmission rate of packet in ST-GEAR is greater than that of E-GEAR, because the BDRM is used in ST-GEAR.

3) Loss Rate of Packet
The simulation result of the loss rate of packet is shown in Figure 7 when there are attacking nodes in the network. It can be seen that the loss rate of packet in ST-GEAR is small compared with other two protocols. In addition, the loss rate of packet in ST-GEAR is smaller than that of E-GEAR. This is because the node trust mechanism used in BDRM takes into account the node energy as well as the communication process of node.

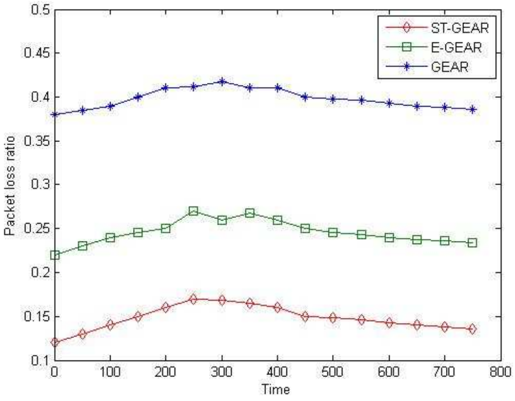

Figure 7: Loss rate of packet

4) Energy Consumption Rate
Figure 8 presents the simulation results of energy consumption rate in ST-GEAR, E-GEAR and GEAR. The energy consumption rate of GEAR is the minimal compared with two protocols. This is because the introduction of the reputation mechanism into the two other protocols consumes some energy. In addition, the energy consumption of ST-GEAR is less than that of E-GEAR. This is because the computational complexity of calculating the node trust value in BDRM is reduced, and the energy consumption is correspondingly reduced.

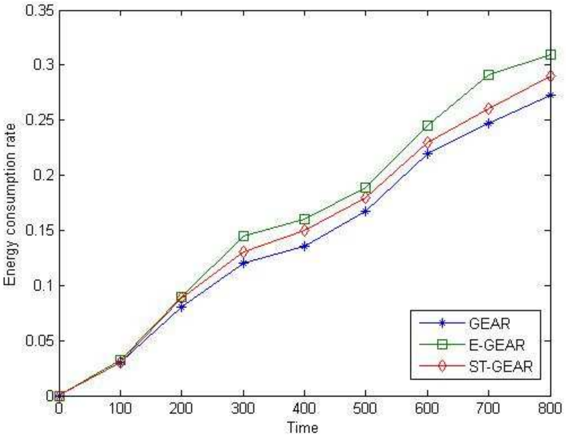

Figure 8: Energy consumption rates

6 Conclusions

This paper takes the security of wireless sensor network as the research background and proposes a ST-GEAR secure routing protocol. Firstly, aiming at the problems of complex computation of trust value and excessive energy consumption of node in current trust mechanism, a reputation mechanism BDRM based on binomial distribution is presented. The node trust value is calculated by the residual energy and the communication process, which can be taken a basis of identifying the malicious nodes in the network. Secondly, a secure bootstrap model based on regular hexagon grid deployment is given. On this basis, the ST-GEAR protocol is proposed. In the routing, the protocol selects the node with minimum cost as the next hop forwarding node considering the node energy, distance and the trust value. This protocol can ensure that the information transmitted between nodes is encrypted, which can prevent the malicious nodes in the network to attack the network and improve the security and robustness of the network. The simulation results show that the ST-GEAR protocol can improve the transmission rate of packet and reduce the loss rate of packet and energy consumption compared with GEAR and C-GEAR protocols.

The proposed ST-GEAR protocol can solve the problems including the selective forwarding, Sybil attack and false routing attack that are vulnerable to the GEAR, but there still are some disadvantages. Firstly, the introduction of reputation mechanism BDRM in the protocol has some influence on the energy consumption of the network. Secondly, the consideration of the type of malicious nodes is not very comprehensive. There are other types of malicious nodes. These will be improved in the future researches.

Acknowledgments

This work is supported by the Natural Science Foundation of Liaoning Province (CN) (20170540777). The authors also gratefully acknowledge the helpful comments and suggestions of the reviewers, which have improved the presentation.

References

[1] W. Bo and L. La-Yuan, "Secure routing algorithm based on power-efficient for wireless sensor networks," in *Pacific-Asia Conference on Circuits, Communications and System*, pp. 35–38, 2009.

[2] B. Chen, K. Jamieson, H. Balakrishnan, and R. Morris, "Span: An energy-efficient coordination algorithm for topology maintenance in ad hoc wireless networks," *Wireless Networks*, vol. 8, no. 5, pp. 481–494, 2002.

[3] 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, pp. 1–37, 2008.

[4] V. C. Gungor and G. P. Hancke, "Industrial wireless sensor networks: Challenges, design principles, and technical approaches," *IEEE Transactions on Industrial Electronics*, vol. 56, no. 10, pp. 4258–4265, 2009.

[5] W. B. Heinzelman, A. P. Chandrakasan, and H. Balakrishnan, "An application specific protocol architecture for wireless microsensor networks," in *IEEE Transactions on Wireless Communication*, pp. 660–670, 2002.

[6] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: Attacks and countermeasures," in *Proceedings of the First IEEE International Workshop on Sensor Network Protocols and Applications*, pp. 113–127, 2003.

[7] C. T. Li and M. S. Hwang, "A lightweight anonymous routing protocol without public key en/decryptions for wireless ad hoc networks," *Information Sciences*, vol. 181, no. 23, pp. 5333–5347, 2011.

[8] W. T. Li, T. H. Feng, and M. S. Hwang, "Distributed detecting node replication attacks in wireless sensor networks: A survey," *International Journal of Network Security*, vol. 16, no. 5, pp. 323–330, 2014.

[9] Y. Lv, Z. Miao, and X. Wei, "An energy gradient based hexagon clustering protocol for wireless sensor networks," *ICIC Express Letters Part B*, vol. 6, 2015.

[10] N. Nasser and Y. Chen, "Seem: Secure and energy-efficient multipath routing protocol for wireless sensor networks," *Computer Communications*, vol. 30, no. 11-12, pp. 2401–2412, 2007.

[11] G. R. Pathak and S. H. Patil, "Mathematical model of security framework for routing layer protocol in wireless sensor networks," *Procedia Computer Science*, vol. 78, pp. 579–586, 2016.

[12] R. D. Pietro, L. V. Mancini, Y. W. Law, and S. Etalle, "Lkhw: A directed diffusion-based secure multicast scheme for wireless sensor networks," in *Proceedings of International Conference on Parallel Processing Workshops*, pp. 397–406, 2003.

[13] S. Roy and A. K. Das, "Secure hierarchical routing protocol (SHRP) for wireless sensor network," in *International Symposium on Security in Computing and Communication*, pp 20-29, 2014.

[14] E. Stavrou and A. Pitsillides, " A survey on secure multipath routing protocols in WSNs," *Computer Networks*, vol. 54, no. 13, pp. 2215-2238, 2010.

[15] S. Tanachaiwiwat, P. Dave, R. Bhindwale, and A. Helmy, "Location-centric isolation of misbehavior and trust routing in energy-constrained sensor networks," in *IEEE International Conference on Performance, Computing, and Communications*, pp. 463–469, 2004.

[16] W. Xiao-yun, Y. Li-zhen, and C. Ke-fei, "Sleach: Secure low-energy adaptive clustering hierarchy protocol for wireless sensor networks," *Wuhan University Journal of Natural Sciences*, vol. 10, no. 1, pp. 127–131, 2005.

[17] Y. Yu, R. Govindan, and D. Estrin, "Geographical and energy aware routing: A recursive data dissemination protocol for wireless sensor networks," *Marine Pollution Bulletin*, vol. 20, no. 1, pp. 48, 2011.

[18] Y. Zhang, L. Xu, and X. Wang, "A cooperative secure routing protocol based on reputation system for ad hoc networks," *Journal of Communications*, vol. 3, no. 6, pp. 283–285, 2008.

[19] L. I. Zhi-Yuan and R. C. Wang, "A survey of secure routing in wireless sensor networks," *Journal of Nanjing University of Posts and Telecommunications*, vol. 30, no. 1, pp. 77–87, 2010.

Biography

Yanhui Lv biography. She received the master's degree in computer application technology from Shenyang Ligong University in 2005, and the Ph.D. degree in computer application technology from Northeastern University in 2010. Now, she is a professor working in the College of Information Science and Engineering, Shenyang Ligong University. Her current research interests include wireless sensor network and system simulation.

Kexin Liu biography. She received the B.E. degree in computer science and technology from Jiangxi University of Traditional Chinese Medicine in 2016. Currently, she is a master degree candidate for computer application technology at Shenyang Ligong University. Her research interests include wireless network and software engineering.

Deyu Zhang biography. He received the Ph.D. degree in computer science from Nanjing University of Science and Technology in 2005. Currently, he is a professor working in the College of Information Science and Engineering, Shenyang Ligong University. His research interests include wireless network, artificial intelligence and embedded system.

Zhuo Miao biography. She received the B.E. degree in computer science and technology from Shenyang Ligong University in 2014, and the master's degree in computer application technology from Shenyang Ligong University in 2017. Her research interests include wireless sensor network and embedded system.