Hindawi Publishing Corporation
Journal of Sensors
Volume 2015, Article ID 716468, 10 pages
http://dx.doi.org/10.1155/2015/716468

Research Article

Trust-Aware and Low Energy Consumption Security Topology Protocol of Wireless Sensor Network

Zuo Chen,[1,2] Min He,[1] Wei Liang,[3] and Kai Chen[1]

[1] *College of Computer Science and Electronic Engineering, Hunan University, Changsha, Hunan 410082, China*
[2] *Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China*
[3] *School of Computer Science and Engineering, Hunan University of Science and Technology, Xiangtan 411201, China*

Correspondence should be addressed to Wei Liang; idlink@163.com

Received 18 August 2014; Accepted 8 October 2014

Academic Editor: Fei Yu

Wireless sensor network (WSN) is a kind of distributed and self-organizing networks, in which the sensor nodes have limited communication bandwidth, memory, and limited energy. The topology construction of this network is usually vulnerable when attacked by malicious nodes. Besides, excessive energy consumption is a problem that can not be ignored. Therefore, this paper proposes a secure topology protocol of WSN which is trust-aware and of low energy consumption, called TLES. The TLES considers the trust value as an important factor affecting the behavior of node. In detail, the TLES would take trust value, residual energy of the nodes, and node density into consideration when selecting cluster head nodes. Then, TLES constructs these cluster head nodes by choosing the next hop node according to distance to base station (BS), nodes' degrees, and residual energy, so as to establish a safe, reliable, and energy saving network. Experimental results show that the algorithm can effectively isolate the malicious node in the network and reduce the consumption of energy of the whole network.

1. Introduction

With the development of wireless communications, electronics, and sensing technology, the wireless sensor networks (WSN) [1] have attracted much attention. WSN consist of many wireless sensors which have sensing, data processing, and short distance wireless communication function. These embedded sensors could be self-organizing and work together to sense and collect all kinds of interesting environment data. Moreover, they also analyze and process the original data to obtain accurate information under various environmental conditions [2]. The excellent characteristics of WSN make it have a broad application prospect in military defense, environmental monitoring, biological, medical, disaster relief, and commercial applications, and so forth [3–5].

In general, the WSN nodes are equipped with independent battery and usually deployed of large numbers in the wild places where people almost could not reach. It is an impossible mission to recharge or replace the sensor battery. In order to reduce the energy consumption, the communication radius of node is strictly limited. The topology protocols of WSN commonly focus on how to separate the whole network into clusters and how to make multihops construction among these cluster heads for transferring sensor data to base station by self-organization. In the open, distributed, and dynamic environment, the construction of network topology is vulnerable, which may lead entire network to be unsafe. For WSN, how to ensure the security of the communication is an important issue in the process of constructing network topology [6, 7].

In recent years, people have put forward different security routing protocols. Most of these are based on the traditional security mechanisms of the cryptosystems, which need much more memory and energy consumption. The wireless sensor network is composed of many small sensor nodes with limited bandwidth and stringent node constraints in terms of power and memory. What is more, the cryptosystems can only resist external attack; once internal nodes have mutations or attacks, they will not be able to be identified. So the traditional cryptosystems of traditional security mechanisms are not fully applicable to wireless sensor networks [8].

To solve the above problems, researchers have proposed the trust management mechanism. Trust is defined as the binary relation occurring in subject and object. The trust management mechanism depends on the history record of object behavior or interaction behavior. The record is used to calculate a trust value. The trust value provides a prediction of future behavior and determines the object's next step. The evaluation of the trust value includes node trust, link trust, and service trust. This strategy makes the trust management mechanism effective in improving the security of the network in an open environment.

This paper tries to take node trust into consideration when building a network topology, so as to ensure the security of the network communication. The TLES algorithm is based on the analysis of node behavior. It develops a variety of trust factors and then performs comprehensive analysis with direct information and recommended information. This working principle can dynamically reflect changes in the trust value between the nodes. TLES combines trust value, residual energy, and density together. This algorithm uses the local optimum principle to choose the cluster head node. Cluster head selects the next hop based on the residual energy, distance to BS, and degree of other cluster heads. As a result, it can effectively eliminate the malicious nodes in network and achieve safe, rational node communication. Besides, the energy consumption of the network is reduced.

The rest of this paper organization is as follows: the second part is a brief review of the related research work; the third part presents the system model and the problem description; the fourth part shows the details of the topology algorithm; the fifth part is about simulation results and the analysis; the last part is conclusions for summary and future work.

2. Related Work

There have been many researches on WSN trust models. Zhan et al. proposed a plane routing protocol based on trust, which is called TARF. The TARF uses the trust value and energy cost to decide the routing path. This protocol can prevent malicious nodes from tampering with routing information and misleading network traffic [9]. Raje and Sakhare [10] proposed a mechanism of cluster head election. This mechanism is based on trust model and uses a certain probability to choose cluster head. Other ordinary nodes would join a cluster head after analyzing energy and the cluster head's trust values. If no node joins a cluster head, the cluster head would become a common node. Repeating the above process until all common nodes have found their cluster heads, which is complex calculation process that would bring network too much burden and energy cost, Crosby et al. proposed a cluster head election algorithm based on trust value. In this algorithm, neighbor nodes monitor data packets and control packets forwarding information, calculate the trust value, and select the neighbor node with the highest trust value as the cluster head. This algorithm combines challenge response with redundancy strategy to reduce the possibility of malicious nodes becoming cluster head [11]. In [12], Safa et al. proposed a hierarchical routing algorithm which is called CBTRP. For the CBTRP, neighbor nodes self-organize into a cluster structure according to the corresponding trust value. To ensure the safety of data transmission, the CBTRP would send data to trust cluster head directly and apply directed diffusion. Heinzelman et al. proposed an improved LEACH algorithm [13] based on trust value, that is, LEACH-TM [14]. The LEACH-TM algorithm uses trust value to optimize the selection of cluster head and the formation of the cluster structure. In this way, the LEACH-TM can identify the malicious nodes, reduce data packet loss, and enhance network security. There is a TARP [15] protocol which applies a trust-based routing scheme responsible for routing messages from the different nodes to the base station. It is based on idea of node cooperation which forwards the neighbor messages. It uses the concept of cooperation in terms of routing reputation. TARP achieves significant improvements in terms of energy consumption and scalability. This protocol exploits nodes' past routing behavior and link quality to determine efficient paths, but it does not offer protection against the identity deception through replaying routing information.

These above methods mainly focus on single network security threats without considering trust value across the board; thus it may ignore security and performance defects of the trust routing itself. For example, the computation of trust value is too complex, malicious nodes are difficult to identify, and key nodes are vulnerable. Therefore, this paper proposes a secure routing algorithm based on trust for wireless sensor network (TLES). The TLES synthesizes direct and recommended information for trust calculation. So it can dynamically reflect the change of trust value between nodes. Besides, it takes trust value, energy cost, and node density into consideration. The nodes compete and select a cluster head. The cluster head node chooses the next-hop node according to energy cost, distance, and degree. Using this strategy, the TLES can effectively eliminate the malicious nodes in the network. It can also ensure security and rationality of node communication effectively, as well as reducing network energy cost.

3. System Model and Problem Description

This paper proposes TLES, which lets node construct the topology structure of the whole network according to the neighbor node's trust value, residual energy, and distance to base station. Models and problems of TLES topology construction are described as follows.

3.1. Network Model. Supposing N sensor nodes are randomly distributed in the $M * M$ region, the main characteristics of sensor nodes are as follows:

(1) all sensor nodes have the same initial trust value, energy value, and status;

(2) there is only one BS node in the WSN, and the BS node's energy is infinite;

(3) once a sensor node has been deployed, it cannot be moved;

(4) node is not equipped with GPS, but each node can know the location information of the current node;

(5) a sensor node has many energy levels, so the sensor nodes can dynamically adjust the model of the energy according to the transmission distance.

The first to fourth are the basic properties of wireless sensor networks, and the fifth property is defined energy levels for the communication within the cluster and the communication between clusters; the two communication modes have different energy consumption.

3.2. Wireless Communication Model. This paper uses the same wireless communication model in [16]. How to calculate d_o is shown in (1). If $d \le d_o$, the node energy consumption is proportional to the square of the communication distance; if $d > d_o$, the node energy consumption is proportional to the biquadrate of the communication distance. The above two models are called the free space model (free space) and multipath fading model (multipath fading), respectively. In order to realize that nodes' energy consumption have proportional relationship to the square of the distance, the broadcast distance of the nodes and the communication distance R were set to d_o in this paper. The energy consumption of sending k-bits data is as shown in formula (2). Consider

$$d_o = \sqrt{\frac{E_{\text{fs}}}{E_{\text{mp}}}} \tag{1}$$

$$E_{\text{tr}}(k) = E_{\text{elc}}(k) + E_{\text{amp}}(k, d) = \begin{cases} k \times E_{\text{elc}} + k \times E_{\text{fs}} \times d^2; & \text{if } d \le d_o \\ k \times E_{\text{elc}} + k \times E_{\text{mp}} \times d^4; & \text{if } d > d_o. \end{cases} \tag{2}$$

The energy consumption of sensor nodes receiving k-bits data is as shown in

$$E_{\text{rx}}(k) = k \times E_{\text{elc}}. \tag{3}$$

E_{elc} stands for the energy consumption when receiving and sending 1 bit data, E_{amp} represents the energy consumption when node fuse 1 bit data, E_{fs} stands for the consumption of energy when sending 1 bit data in the free space model, and E_{mp} represents the consumption of energy of sending 1 bit data in the multipath fading model.

3.3. Problem Description. In order to solve these weaknesses existing in the previous studies, TLES protocol needs to meet the conditions as follows:

(1) the network node communication radius is less than or equal to the d_o; therefore all the nodes in the network could meet the free space model which can effectively reduce the energy consumption;

(2) it is difficult for nodes to obtain global information, with the increasing scale of WSN; the node should construct the whole network topology only by local neighbor nodes' information;

(3) the node's trust value is dynamic, the changes of which should be able to accurately reflect the node security;

(4) in TLES algorithm, all nodes try their best to deliver packets to their next node, integrating a variety of trust mechanisms to select a neighbor node with the highest trust value as the cluster head node;

(5) communication between cluster head nodes should try to satisfy the free space model; the communication radius is less than or equal to the d_o.

4. Details of TLES

TLES algorithm consists of two parts. The first part is to calculate the trust value of nodes and select cluster head nodes according to the trust value, residual energy, and the density of nodes. If the ordinary node's trust value is less than a certain threshold, it could not be allowed to join any cluster heads. The second part is to build a weighted tree. All the cluster head nodes select the next-hop nodes, according to the node information including the value of residual energy, the distance between cluster and BS, and the value of clusters' degree, so as to construct the whole network topology and transmit the information to the BS node finally.

4.1. The Calculation of Trust Value. Trust depends on the subject's (evaluating node) assessment to the object (evaluated node) and the recommendation of other nodes, and the value will change according to object's behavior. Considering the characteristic of self-organizing and multiple hops in wireless sensor network, the trust evaluation mechanism should be set up with no core node. Nodes monitor each other's behavior between neighbors, and use the direct and indirect trust value to get comprehensive trust values.

(1) Sending Rate Factor $\text{SF}_{i,j}(t)$. Evaluating node i monitors the quantity sending of the evaluated node j. If the number is lower than the lower limit threshold T_L, the node can be regarded as a selfish node. If the number is more than the upper limit threshold T_H, the node may have performed attack as behavior of denial of service. The sending rate factor's formula is shown as follows:

$$\text{SF}_{i,j}(t) = \begin{cases} \dfrac{\text{SP}_{i,j}(t) - T_L}{\text{ES}_{i,j}(t) - T_L} & \text{SF}_{i,j}(t) \le \text{ES}_{i,j}(t) \\ \dfrac{T_H - \text{SP}_{i,j}(t)}{T_H - \text{ES}_{i,j}(t)} & \text{SF}_{i,j}(t) > \text{ES}_{i,j}(t). \end{cases} \tag{4}$$

In formula (4), $\text{SP}_{i,j}(t)$ stands for the quantity sending of the period t and $\text{ES}_{i,j}(t)$ represents the expected value of the quantity sending of the period t. When $T_L = 300$, $T_H = 700$, and $\text{ES}_{i,j}(t) = 500$, the changes of $\text{SF}_{i,j}(t)$ are shown in Figure 1.

It is clear that the range of $\text{SF}_{i,j}(t)$ is from 0 to 1. If the value of $\text{SP}_{i,j}(t)$ is closer to $\text{ES}_{i,j}(t)$, the value of $\text{SF}_{i,j}(t)$ is closer to 1, which means that the node gets a relatively higher trust value.

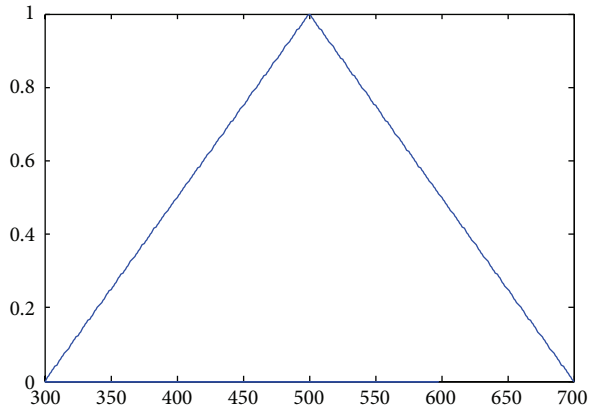

Figure 1: The variation of sending rate factor.

(2) Consistency Factor $\mathrm{CF}_{i,j}(t)$. To prevent malicious nodes forged packets, we need to compare the data of node collecting by itself with the data collecting by neighbor nodes, which is called the analysis of spatial coherence. The data gathered from different nodes in the same local area of local networks generally shows a high degree of correlation. The evaluating node i monitors the packet of evaluated node j, compared with its acquisition data. The evaluating node i monitors the packet of evaluated node j, and i compares the data collecting by itself with the data collecting by j. If the difference between the two data is within a certain range, the evaluating node i and evaluated node j have a consistent opinion about the monitored environment. Consider

$$\mathrm{CF}_{i,j}(t) = \frac{\mathrm{CP}_{i,j}(t)}{\mathrm{CP}_{i,j}(t) + \mathrm{NCP}_{i,j}(t)}. \tag{5}$$

In formula (5), $\mathrm{CP}_{i,j}(t)$ stands for the number of nodes having the same packet with evaluated node j and $\mathrm{NCP}_{i,j}(t)$ stands for the number of inconsistent packet. $\mathrm{CP}_{i,j}(t) + \mathrm{NCP}_{i,j}(t)$ is the number of all the packet that i received from its surrounding nodes.

(3) Packet Loss Rate Factor $\mathrm{DF}_{i,j}(t)$. Because the energy of node is limited in WSN, some nodes cannot communicate with the base station (BS) directly and need other nodes as relay node to forward information to the BS by a multiple-hop topology. The packet drop is likely to exist in the process of transmission, which leads to the loss of information. The formula of packet loss rate factor is shown in

$$\mathrm{DF}_{i,j}(t) = \frac{T(t)}{R(t)}. \tag{6}$$

In formula (6), $T(t)$ is the amount of all the packets sent by all the nodes, in the period t. $R(t)$ is the amount of packet received by all the nodes times, at the same time. Obviously, the range of $\mathrm{DF}_{i,j}(t)$ is also from 0 to 1.

Suppose that nodes i and j are neighbor nodes. When node i assesses node j, considering the attack of malicious nodes and selfish node, we need to combine all trust factors mentioned previously. Firstly, calculating nodes' direct trust value and then calculating the indirect trust value through other node k which is connecting both nodes i and j, the computation formula of direct trust value is as follows:

$$\begin{aligned}\mathrm{Td}_{i,j}(t) = {} & (1-\alpha) * \mathrm{SF}_{i,j}(t) * \mathrm{CF}_{i,j}(t) * \mathrm{DF}_{i,j}(t) \\ & + \alpha * \mathrm{Td}_{i,j}(t-1).\end{aligned} \tag{7}$$

In formula (7), $\mathrm{SF}_{i,j}(t)$ is sending rate factor, $\mathrm{CF}_{i,j}(t)$ is consistency factor, $\mathrm{DF}_{i,j}(t)$ is packet loss rate factor, α is a constant coefficient, and the range is from 0 to 1. The range of $\mathrm{Td}_{i,j}(t)$ is from 0 to 1. $\mathrm{Td}_{i,j}(t)$ is 0, representing that the node is abnormal node, and the node is untrusted, while 1 stands for the fact that the node is normal completely, and the node is trusted. The greater the trust value is, the more credible the node is.

When selecting the next-hop node, each node is subjective to judge whether the next-hop node could be trusted by calculating the trust of the next-hop node. In order to reduce deviation, the indirect trust value also should be considered, and formula is as follows:

$$\mathrm{Tid}_{i,j}(t) = f_t\left(\mathrm{Td}_{i,j}(t), \mathrm{Td}_{k,j}(t)\right). \tag{8}$$

In formula (8), $\mathrm{Td}_{i,j}(t)$ is the direct trust value of evaluated node j by i and $\mathrm{Td}_{k,j}(t)$ is the direct trust value of evaluated node j by k, connected simultaneously with node i and node j. $f_t[\cdot]$ can be determined according to the needs of actual network. It can be set into linear, such that $\alpha * \mathrm{Td}_{i,j}(t) + \beta * \mathrm{Td}_{k,j}(t)$, and $\alpha + \beta = 1$. The value of α and β can be determined according to the actual needs. If we want to pay more attention to trust value of the other nodes, we can set the β value higher. However, if the node trust value judgment by own is more important, α could be higher.

4.2. The Selection of Cluster Head. Before the first choice of cluster, base station nodes globally broadcasted, each node receives the base station's information and calculates the distance between itself and base stations. Then, each node broadcasts information of itself in local area within the range of distance d_o. When other cluster head nodes receive a message, then they will send a confirmation message to the sending node. After each node calculates the p_{ch}, each node will broadcast the p_{ch} of itself, and the range is d_o. Consider

$$p_{\mathrm{ch}} = f_p\left(E_{\mathrm{current}}, T_{\mathrm{ch}}, S_d\right) \tag{9}$$

where E_{current} represents the residual energy of node, T_{ch} represents the trust value of nodes, and S_d is the number of neighbor nodes within a radius of $d_o/4$. $f_p[\cdot]$ is the function to computing nodes' p_{ch}. p_{ch} of node is related to residual energy, the trust value, and the density of the node. We hope that the greater the residual energy of nodes, the greater the trust value, and the greater the density of nodes, the higher the probability of cluster head nodes.

Figure 2 is a schematic diagram of a WSN that consisted of five nodes, and the p_{ch} of node 5 is the biggest. By the following steps, the competition of cluster heads will be completed.

```
(1) if round=1
(2)    Bs_str = Receive_Str(msg form BS) //radio strength from BS
(3) endif
(4) if (S(i).energy > 0 && S(i).type! = "U")
(5)    S(i).state = "N";
(6)    broadcast N_MSG within range d_o;
(7)    Receive (confirmation message of neighbor node within the range of d_o);
(8)    calculate p_ch;
(9)    broadcast PCH_MSG within range d_o;
(10)   receive PCH_MSG from others
(11)   p = max(p_ch received, p_ch own)
(12) endif
(13) if (S((i). p_ch == p)
(14)   S(i).state = "C";
(15) endif
(16) if (S(i).state == "C")
(17)   broadcast MC_MSG within range d_o;
(18)   waitfor JOIN_MC_MSG;
(19) endif
```

Algorithm 1: The pseudocode of elected cluster head.

(1) all nodes broadcast their information within the scope of the d_o and receive the other nodes' information within the same scope;

(2) all the nodes calculate their own p_{ch} according to the received information and then broadcast their p_{ch} information, within the scope of d_o; all nodes receive p_{ch} of other nodes in this scope; as shown in Figure 2, the node 5 got the p_{ch} value of itself and the other nodes 1, 2, 3, and 4;

(3) compare its own p_{ch} and other p_{ch} values, if its own p_{ch} is the maximum one; the node will become cluster head; as shown in Figure 2, comparing with the value of node 5 by its own and other values of 1, 2, 3, and 4 nodes, node 5 finds that own value is the biggest, so node 5 becomes a cluster head node by competition.

Algorithm 1 is the pseudocode of clusters:

(1) BS node broadcast information of base station;

(2) all the nodes are not isolated and the energy is greater than zero; broadcast their information with range of d_o; at the same time, all the nodes receive the information of the other nodes within the range of d_o, calculating their p_{ch}; at last, compare their own P_{ch} and the received neighbor node P_{ch};

(3) the node with the maximum P_{ch} becomes cluster head node;

(4) cluster head nodes wait for the join massages from other nodes.

4.3. Weighted Spanning Tree Generation. In this section, we want to set up a multihop topology among all the cluster head nodes by generating a weighted spanning tree construction. For convenience of discussion, all the nodes mentioned in this section represent cluster head nodes.

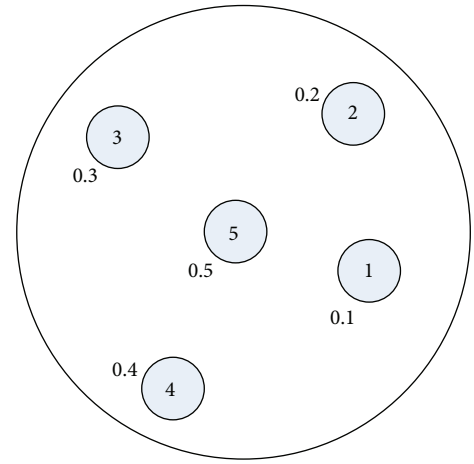

Figure 2: The competition of cluster head.

Cluster head selects the next hop from other cluster head nodes, considering the residual energy, the distance between BS and the next node, and degree of the next node. In this paper, the concept of the degree is not just the number of nodes connected directly. For example, the degree of node A is the number of all the nodes, which take the node A as a root node and need node A to forward their information. In TLES, each cluster node broadcasts its information, and the radius of broadcast is d_o. When other cluster nodes have received the message, they will send an acknowledgement message to the node that has broadcasted the message, the acknowledgement message (Message1) and the detail format of the acknowledgement message as shown in Table 2. An acknowledgement message includes the residual energy of the current node, the location of the node, the distance between the node and BS, and the degree of node. When the node has received the acknowledgement message (Message1)

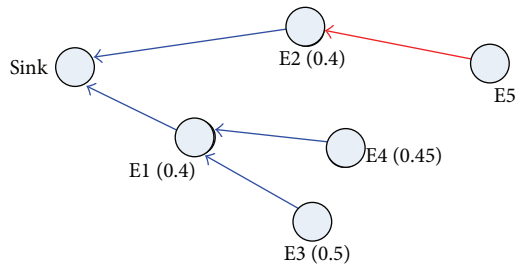

Figure 3: Select the next-hop node.

from its neighboring nodes, it will select the next hop from the neighboring nodes.

How to select the next-hop method is as follows.

(1) Node selects the node whose distance with BS node is less than the distance between the current node and BS node to join the set V from the nodes that have sent Message1 to the current node.

(2) Select the next-hop node in the set V according to formula (10).

(3) If node has received the Message1 from the BS node, its next hop is the BS node. Consider

$$\text{Nextnode}\ (i,j) = a * \frac{\text{distance}\ (i,j)}{d_o} + b * \frac{E_{\text{current}}}{E_o} + c * \frac{\text{max degree} - \text{degree}}{\text{max\_degree}}. \quad (10)$$

In formula (10), i represents the current node, j represents the neighbor node, and Nextnode (i, j) represents the link weights between the current node i and node j. distance (i, j) represents the distance between node i and node j. E_{current} stands for the residual energy of node j. E_o stands for the initial energy. max_degree represents the biggest degree of the previous round of the network. degree represents the degree of j. a, b, and c are constant coefficients, and $a + b + c = 1$. Finally, nodes will select the largest Nextnode as the next hop.

Figure 3 is a schematic diagram of WSN composing 6 nodes. The blue lines are the original connection in the network and red line is the new one connected in this round. Obviously, when choosing the next-hop node, E5 will consider three aspects: distance, energy, and degrees. In this diagram, E1 is closest to the sink node, and E1 is furthest to E5 within the range of d_o (within the range of d_o, sending the data as far as possible regardless of the degree of E1, the E1 can be considered as the next-hop node of E5 temporarily, but, given degree of E1, the E2 has the same energy with E1 whose degree is relatively small. What is more, E2 is the farthest to E5 except for E1, so E2 becomes the next hop of node E5.

In this paper, the concept of the degree is not just the number of nodes connected directly. The degree of one node is the number of all the nodes, which take this node as a root node and need this node to forward information. After the selection of next cluster head node, the next-hop node's degree should be updated. The formula is as shown in

$$\text{degree}_j = \text{degree}_j + \text{degree}_i. \quad (11)$$

degree_j stands for the current node's degrees and degree_j represents the degree of the next-hop j. All the nodes except for j, which has connected i, need j to forward packet. So, node j should update the value of degree. After node j has updated its degree, it should broadcast the information of the new degree. Then, the next hop of j also should update the one for the change of node j's degree. This process is repeated until the node has been found, whose next hop is the BS node.

Figure 4 is a schematic diagram of a WSN composing 7 nodes. The blue lines are the original connection in the network and red line is the new one connected in this round. After the E6 has chosen E5 as the next-hop node, E5 needs to update the value of degree, and E4 also needs to update the degree. Because the next hop of E4 is BS node, so no more nodes need to update degree, in this network.

Algorithm 2 is the pseudocode of weighted spanning tree:

(1) BS node broadcasts its information;

(2) all the nodes radiobroadcast the information of themselves, and the radiodistance is d_o;

(3) nodes receive the radiomessages from the nodes whose distance with the nodes are less than d_o or equal to d_o;

(4) all surviving nodes in the network according to the neighbor node information choose the next-hop node, if the distance of node i to BS is greater than that of the node j to the BS and has the Max (Nextnode); the node j will became the next-hop node;

(5) node j and nodes, whose descendant is j, refresh their degree;

(6) node i sends its TDMA table to its child nodes, and the connected node receive TDMA.

5. Simulation

The experimental environment is as follows: the area of network is $200 * 200$ and the number of sensor nodes is 200. The initial value of trust of each node is 1. Some malicious nodes are scattered randomly. Malicious nodes may have some bad behaviors, such as packet loss, too big or too small quantity of sending packet, and sending wrong data. Simulation experiment of the initialization parameters are shown in Table 1.

The experiment can be divided into three parts. First, we analyze the detection accuracy of malicious nodes by setting different isolation threshold values. Second, we use the better threshold, gotten by the first part, we analyze the change of average sending ratio, the change of average consistency ratio, and the change of average packet delivery ratio as the change of communication round, in order to verify whether the proposed algorithm could isolate the malicious nodes effectively and improve the average sending ratio, the

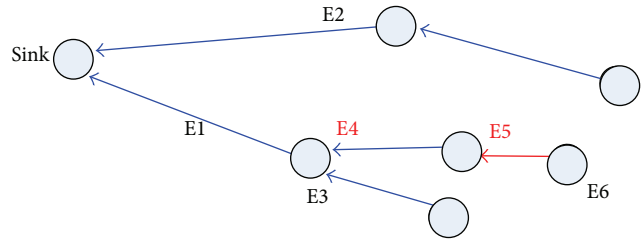

Figure 4: Update of degree.

```
(1) if round = 1
(2)    Bs_str = Receive_Str(msg form BS) //radio strength from BS
(3) endif
(4) if (S(i).energy > 0 && S(i).type! = "U")
(5)    if (S(i).distanceToSink < S(j).distanceToSink && S(i).E > 0 && S(j).type! = "U")
(6)      choose max(a* distanceij/do + b* Ecurrent/Eo + c* (max_degree − degreei)/max_degree) as next node
(7)        S(i).nextnode = j;
(8)       degree j += degreei //updated the next-hop node's degree
(9)       j broadcast N_MSG within range do;
(10)   end if;
(11) end for
(12) for (All nodes whose residual energy are greater than 0)
(13)   Node I Send TDMA table to it's connected node;
(14)   nodes have connected to the node i receives the TDMA
(15) end for
```

Algorithm 2: The pseudocode of weighted spanning tree.

Table 1: The initial value of the parameter.

Parameter	Value
Etx	$50e - 9$ J/bit
Erx	$50e - 9$ J/bit
Efs	$10e - 12$ J/bit/m2
Emp	$0.0013e - 12$ J/bit/m4
EDA	$5e - 9$ J/bit/singal
Control packet length	100 bits
Data packet length	4000 bits
SINK	(0, 0)

Table 2: The format of the Message1.

ID	Residual energy	Distance with BS	Location	Degree

average consistency ratio, and the average packet delivery ratio of the network. At last, we compare the consumption of energy of TLES with the consumption of energy of some hierarchical routing protocols including LEACH, LEACH, and LEACH_MF.

In Figure 5, the horizontal axis represents the proportion of the malicious nodes (C_p), and the vertical axis represents the percentage of correctly detected malicious nodes in total malicious nodes when the first node dies in the network. Some different curves are gotten by setting different threshold R_o. It can be seen from the diagram that all malicious nodes can be detected when the threshold R_o is 0.3. Figure 6 shows that average trust values of the malicious nodes are changing following the changing of round number. In this experiment, assuming initial trust value of each node is 1 and then calculating the node trust value according to the previous communication performance of node, we can conclude that, no matter how much the proportion of malicious nodes is, the average trust values are falling and malicious node trust value will be dropped to below 0.3. Therefore, the malicious nodes are detected by setting the isolation threshold value R_o as 0.3 under the experimental environment.s

All the nodes are fully trusted at the beginning of the experiment; that is to say, each node's trust value is 1. The average consistency ratio, the average sending ratio, and the average packet delivery ratio of the whole network are 1. At the beginning of the communication, all the nodes are fully trusted and malicious nodes have not been isolated. Because malicious nodes exist in the network, a lot of abnormal behaviors that include loss of packet, wrong packet, or node not sending packets or sending too much packets will occur, all the three trust factors will decline in the former stage. With the increased rounds of communication, the malicious node will be detected and isolated slowly, and these bad behaviors will decrease relatively, so, in the later communication stage of the entire network, all the three trust factors will increase with the increased rounds of communication.

In order to verify the changes of three trust factors, we got Figures 7, 8, and 9. In Figure 7, the horizontal axis stands

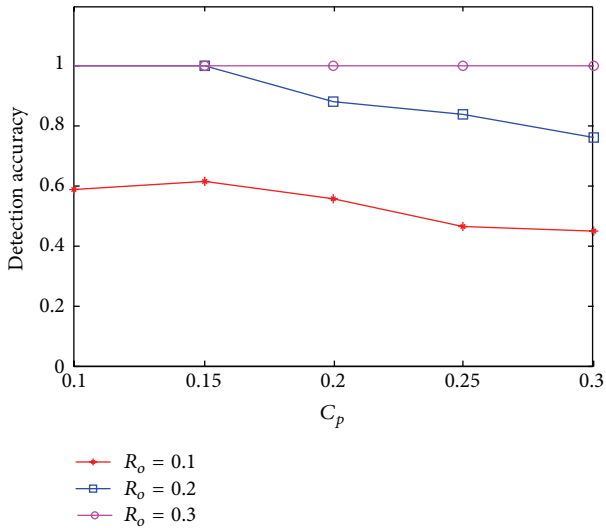

Figure 5: Proportion of malicious nodes and detection accuracy.

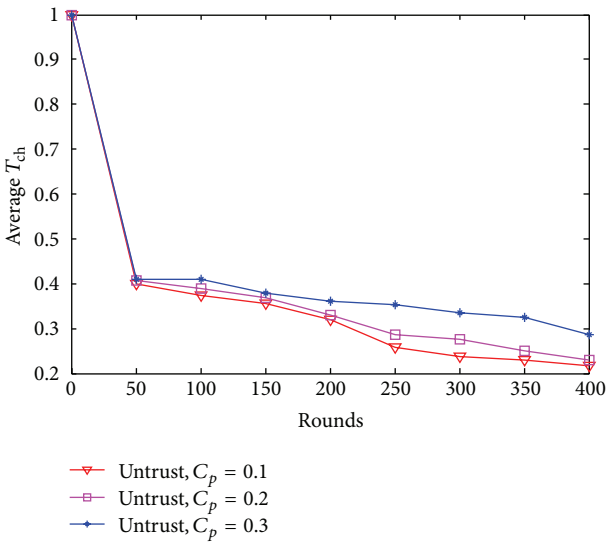

Figure 6: The average value of malicious node's trust.

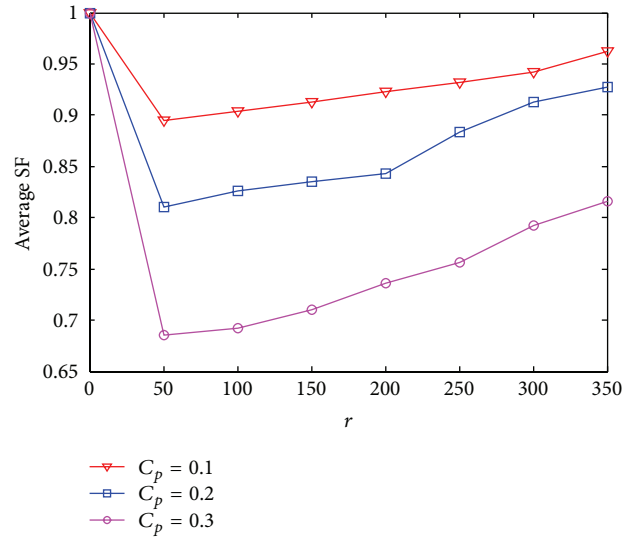

Figure 7: The average sending ratio.

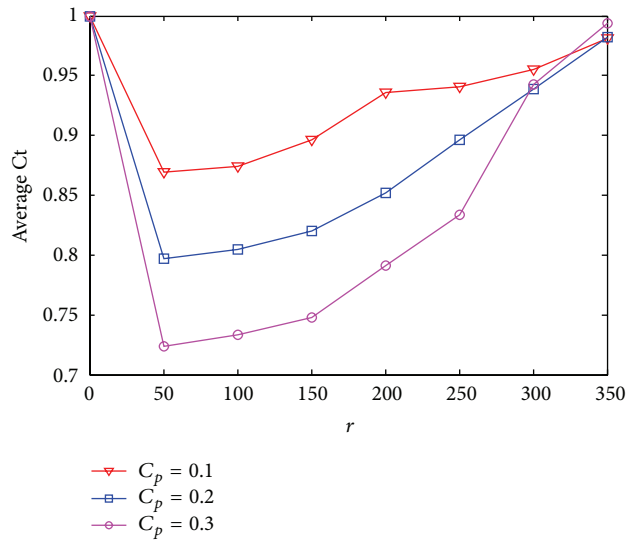

Figure 8: The average consistency ratio.

for number of communication round, and the vertical axis represents the average sending ratio. In Figure 7, no matter how much the proportion of malicious nodes is, the change of average sending ratio in the network suffers degradation in the first stage; with the increased number of communication, it will increase significantly. The greater the proportion of malicious nodes is, the faster the rate of decline is in the down phase. The horizontal axis and vertical axis represent number of communication round and the average consistency ratio respectively, in Figure 8. In Figure 9, the horizontal axis is number of communication rounds, and the vertical axis represents the average packet delivery ratio. The change of consistency ratio and average packet delivery is the same as that of the change of average sending ratio; they are all suffer a degradation in the first stage and then increase significantly, no matter how much the proportion of malicious nodes is. And they also have the characteristic; namely, the greater the proportion of malicious nodes is, the faster the rate of decline is in the down phase.

Compared with Figures 7, 8, and 9, We can see that the change of values of trust factors decreases first and then increases with the increase of the number of comunication rounds. Sending factor's change is quite gentle, and the change of consistency factor and packet loss rate factor is relatively larger. This is because that we let malicious nodes send one more packet or one less packet than normal node in each round, in this experiment. And then statistics each node's sending rate after 50 rounds. The change of nodes' sending rate is not very high, so change of sending factor is slow.

The last part experiments the energy consumption in comparison with LEACH, LEACH-MF, CMRA, and TLES.

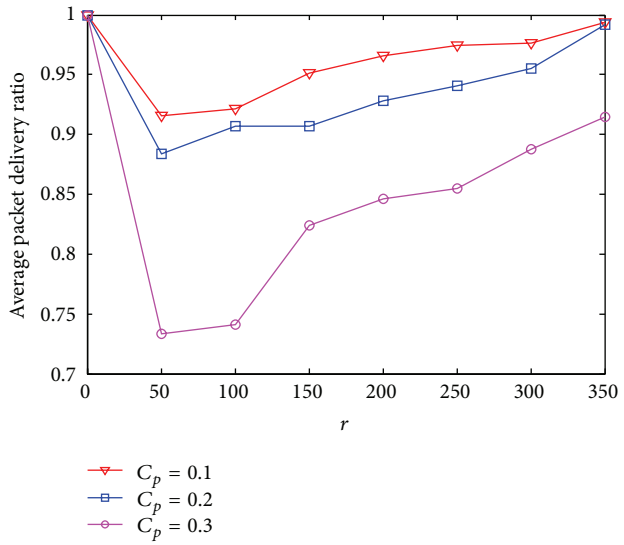

Figure 9: Average packet delivery ratio.

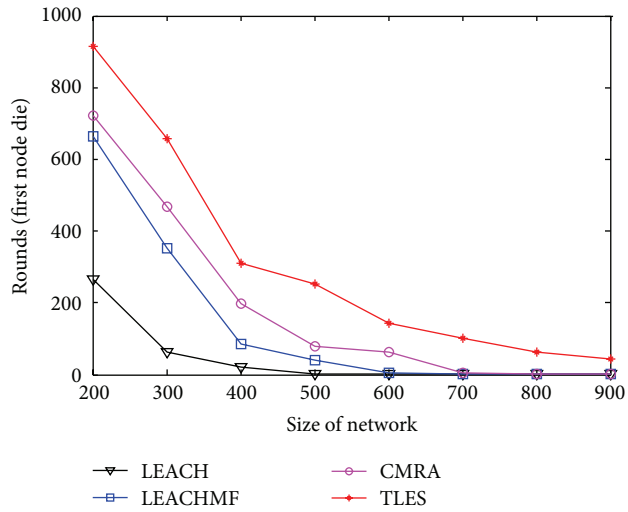

Figure 11: The relationship between the monitoring area and lifetime of network (the first node dies).

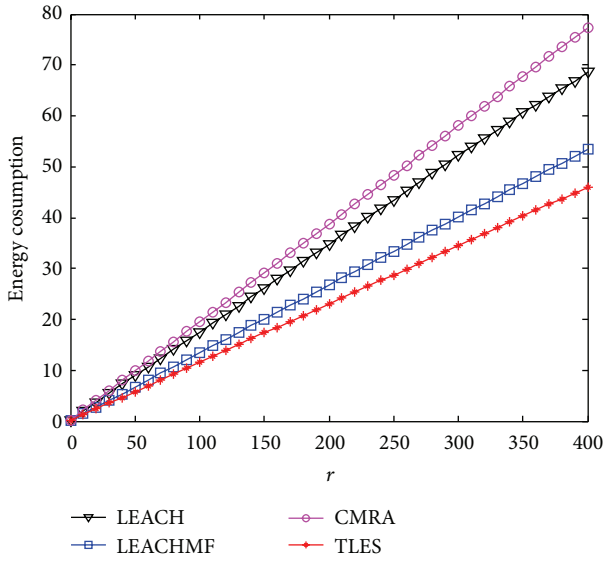

Figure 10: The comparison of energy consumption.

LEACH, LEACH_MF [17], and CMRA [18] are clustering routing protocols in WSN. Under the initial environment, we get the contrast Figure 10 of energy consumption of the four different algorithms. In Figure 10, the horizontal axis shows round number, the vertical axis represents the sum of all the network nodes' energy consumption, and the unit is J. As can be seen from Figure 10, TLES energy consumption is obviously smaller than the other three.

The number of rounds represents the lifetime of network in this simulation. The lifetime of network contains three kinds of definitions: the first node dies, half of nodes die, and the last node dies. In this experiment, we adopt the fist definition (the fist node dies) to count lifetime of network.

The comparison of energy consumption (LEACH, LEACH-MF, CMRA, and TLES) in the different scale of network is shown in Figure 11. Monitoring area is 200 ∗ 200, 300 ∗ 300, 400 ∗ 400, 500 ∗ 500, 600 ∗ 600, 700 ∗ 700, and 800 ∗ 800, respectively. Initial energy is 0.6 J. In Figure 11, the horizontal axis represents the network scale; the vertical axis represents the lifetime (first node dies). With the increase of network size, most nodes' distance to the BS will increase. According to the communication model, we know that the increase of distance is bound to bring the increase of energy consumption. From Figure 11, we can see that the lifetimes of LEACH, LEACH-MF, CMRA, and TLES all decline with the increase of network scale. Although TLES is falling with the increase of scale of network, its survival time is longer than other algorithms under every scale.

Through Figures 10 and 11, we can know that TLES compared with LEACH, LEACH-MF, and CMRA has less energy consumption in each communication round and, with the increase of network scale, has the longest lifetime in the network.

6. Summary and Outlook

This paper proposed a secure topology protocol of WSN, that is, TLES. The trust mechanism used in TLES is introduced. Trust factors were defined by the node's historical behavior, and the trust value of each node was calculated according to the comprehensive value of direct trust and indirect trust, which are related to the trust factors. TLES uses the idea of clustering. First of all, the cluster heads were selected according to the trust value, residual energy, and density of nodes. Then, the cluster heads choose the next-hop node by the residual energy, the distance to BS, and degree of candidate node. After that, the construction of the whole network topology was built. Experimental results show that TLES can eliminate the malicious nodes in network effectively, so as to ensure the safety and rationality of node communication. At the same time, it can also reduce the energy consumption of the network.

The existing problems of this paper are focused on the following two aspects. First, this paper improves the average packet delivery ratio and increases the calculation leading to the increase of packet delay. Second, the mobile sensor network and heterogeneous network would become the new characteristics of network. It is important to figure out how to make improvement in the future.

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

Acknowledgments

This work was sponsored by the Natural Science Foundation of Hunan Province, China (13JJ3091 and 14JJ3062), National Nature Science Foundation, China (61202462 and 61300036), and the Fundamental Research Funds for the Central Universities, China.

References

[1] T. Eswari and V. Vanitha, "A novel rule based intrusion detection framework for Wireless Sensor Networks," in *Proceedings of the International Conference on Information Communication and Embedded Systems (ICICES '13)*, pp. 1019–1022, IEEE, Chennai, India, February 2013.

[2] F. Gao, H.-L. Wen, L.-F. Zhao, and Y. Chen, "Design and optimization of a cross-layer routing protocol for multi-hop wireless sensor networks," in *Proceedings of the International Conference on Sensor Network Security Technology and Privacy Communication System (SNS & PCS '13)*, pp. 5–8, Nangang, China, May 2013.

[3] Z. Li, N. Wang, A. Franzen et al., "Practical deployment of an in-field soil property wireless sensor network," *Computer Standards and Interfaces*, vol. 36, no. 2, pp. 278–287, 2014.

[4] L. Yu, N. Wang, and X. Meng, "Real-time forest fire detection with wireless sensor networks," in *Proceedings of the International Conference on Wireless Communications, Networking and Mobile Computing (WCNM '05)*, pp. 1214–1217, September 2005.

[5] X. Liu, H. Zhao, X. Yang, and X. Li, "SinkTrail: a proactive data reporting protocol for wireless sensor networks," *IEEE Transactions on Computers*, vol. 62, no. 1, pp. 151–162, 2013.

[6] J. Q. Zhang, R. Shankaran, M. A. Orgun et al., "A dynamic trust establishment and management framework for wireless sensor networks," in *Proceedings of the 8th International Conference on Embedded and Ubiquitous Computing (EUC '10)*, pp. 11–13, 2010.

[7] J. Q. Duan, D. Y. Gao, D. Yang et al., "An energy-aware trust derivation scheme with game theoretic approach in wireless sensor networks for IoT applications," *IEEE Internet of Things Journal*, vol. 1, no. 1, pp. 58–69, 2014.

[8] J. Duan, D. Yang, H. Zhu, S. Zhang, and J. Zhao, "TSRF: a trust-aware secure routing framework in wireless sensor networks," *International Journal of Distributed Sensor Networks*, vol. 2014, Article ID 209436, 14 pages, 2014.

[9] G. Zhan, W. Shi, and J. Deng, "Design and implementation of TARF: a trust-aware routing framework for WSNs," *IEEE Transactions on Dependable and Secure Computing*, vol. 9, no. 2, pp. 184–197, 2012.

[10] R. A. Raje and A. V. Sakhare, "Routing in wireless sensor network using fuzzy based trust model," in *Proceedings of the 4th International Conference on Communication Systems and Network Technologies (CSNT '14)*, pp. 7–9, 2014.

[11] G. V. Crosby, N. Pissinou, and J. Gadze, "A framework for trust-based cluster head election in wireless sensor network," in *Proceedings of the 2nd IEEE Workshop on Dependability and Security in Sensor Network and Systems(DSSNS '10)*, pp. 24–28, 2006.

[12] H. Safa, H. Artail, and D. Tabet, "A cluster-based trust-aware routing protocol for mobile ad hoc networks," *Wireless Networks*, vol. 16, no. 4, pp. 969–984, 2010.

[13] W. R. Heinzelman, A. P. Chandrakasan, and H. Balakrishnan, "Energy-efficient communication protocol for wireless microsensor networks," in *Proceedings of the 33rd International Conference on System Sciences*, pp. 1–10, Maui, Hawaii, USA, 2000.

[14] W. Wang, F. Du, and Q. Xu, "An improvement of LEACH routing protocol based on trust for wireless sensor networks," in *Proceedings of the 5th International Conference on Wireless Communications, Networking and Mobile Computing (WiCOM '09)*, pp. 1–4, Beijing, China, September 2009.

[15] A. Rezgui and M. Eltoweissy, "TARP: a trust-aware routing protocol for sensor-actuator networks," in *Proceedings of the IEEE Internatonal Conference on Mobile Adhoc and Sensor Systems (MASS '07)*, pp. 1–9, IEEE, Pisa, Italy, October 2007.

[16] W. B. Heinzelman, A. P. Chandrakasan, and H. Balakrishnan, "An application-specific protocol architecture for wireless microsensor networks," *IEEE Transactions on Wireless Communications*, vol. 1, no. 4, pp. 660–670, 2002.

[17] H. Liu, Y. Fang, X. Hao, J. Dou, H. Li, and W. Bi, "Research of inter-cluster multi-hop routing algorithm for wireless sensor networks," in *Proceedings of the 3rd International Conference on Intelligent System and Knowledge Engineering (ISKE '08)*, vol. 1, pp. 1367–1372, Xiamen, China, November 2008.

[18] W. B. Heinzelman, A. P. Chandrakasan, and H. Balakrishnan, "An application-specific protocol architecture for wireless microsensor networks," *IEEE Transactions on Wireless Communications*, vol. 1, no. 4, pp. 660–670, 2002.