International Journal of Security and Its Applications
Vol.9, No.10 (2015), pp.381-394
http://dx.doi.org/10.14257/ijsia.2015.9.10.35

Coverage Balancing Based Trust Evaluation Method for Wireless Sensor Networks

Shen Haibo, Dong Shengjie, Xu Jian and Zhang Hong

School of Computer Science and Engineering, Nanjing University of Science & Technology, Nanjing, China
Email: hbshen29@163.com, dsjgeek@gmail.com, dolphin.xu@163.com, zhhong@mail.njust.edu.cn

Abstract

Uneven distribution of nodes will lead to information redundancy, and inadequate coverage density will cause false information when evaluate trust of nodes for wireless sensor networks. A coverage balancing based trust evaluation method for wireless sensor networks is proposed in this paper to solve this problem. First, nodes update the trust value of its neighbors by the neighbors' behaviors, and then we update working nodes through sleep mechanism to ensure the uniform distribution and the coverage density. Simulation results show that the proposed method can effectively improve nodes' lifetime, and it has higher detection rate and lower false alert rate compared with other trust evaluation methods, so it can ensure the network run safely.

Keywords: *Wireless sensor networks；Coverage balancing；Sleep mechanism；Trust evaluation*

1. Introduction

As the development of Wireless Sensor Networks (WSNs), WSNs has been widely applied to many aspects of people's lives, such as remote health monitoring [1], intelligent transportation [2] and environmental monitoring [3], et al. WSNs are usually deployed in unattended monitoring area randomly for monitoring events information and forward to the base station through a radio channel. Traditional cryptography security methods are not applicable to WSNs, because they consume too much energy of network nodes, however sensor node only has limited energy. To protect the security of information transmission between sensor nodes, we generally detect the malicious nodes by evaluating the trust value of sensor nodes.

In [4] Reputation-Based Framework for High Integrity Sensor Networks (RFSN) is proposed. This method records the interaction between nodes and revises the current trust evaluation through direct and indirect reputation, so the trust value of nodes is objective and true. In [5] Group-Based Trust Management Scheme for Clustered Wireless Sensor Networks (GMTS) is proposed. This method uses distributed trust management within the cluster and centralized trust management across clusters, so that it could reduce interaction spending between nodes. Since the GMTS does not focus on trust evaluation of a single node, it requires less memory to store the trust records compared with other trust evaluation model. In [6] Secure Trust Establishment Scheme in Wireless Sensor Networks (STES) is proposed. This method only considers misbehavior of nodes, since lawful behavior will artificially increase the trust value of the node. Besides, [7-9] proposed trust evaluation of WSNs based on cluster, in which the cluster members layer and the cluster heads layer use different methods to calculate trust values; [10-11] evaluate the trust value of nodes through aggregating direct and indirect trust.

ISSN: 1738-9976 IJSIA

These trust evaluation model for WSNs mainly aim at the accuracy of trust evaluation. Generally, the more neighbors a node has, the more accurate when evaluate its trust. However, it is difficult to ensure the uniform distribution of nodes due to random deployment and energy depletion, et al. It will lead to two extreme cases: the information for evaluating the trust of nodes in intensive area is excessively redundant, yet in sparse area is too deficient. The former case will waste energy and the latter will not evaluate the trust of nodes accurately. This paper proposed a coverage balancing based trust evaluation method for wireless sensor networks, which ensures the uniform distribution and coverage density of nodes though coverage balancing strategy. Simulation results show that the proposed method can effectively improve nodes' lifetime. Though it takes longer time on detection of malicious nodes, it has higher detection rate and lower false alert rate compared with some trust evaluation methods, so it can ensure the network run safely.

2. Coverage Balancing Strategy

The purpose of traditional coverage algorithm for WSNs is using the minimal number of nodes to ensure complete coverage of the monitoring area on the premise of full connectivity [12-14]. These strategies are impossible to adopt trust evaluation for they do not meet the nodes coverage requirements: uniform distribution and coverage density. A coverage balancing strategy is proposed in this paper to achieve that each position of monitoring area is covered by at least three nodes. It can either ensure full connectivity or meet the requirements of uniform distribution and coverage density.

2.1. Assumptions

Sensor nodes are randomly deployed in a square monitoring area whose area is S. The base station is located in regional centers. Sensor nodes have same sensing radius and communication radius, both are R_c . This paper proposed following assumptions:

1) R_c is much smaller than the side length of the monitoring area, so we can ignore the boundary factor;

2) Node *i* can only sense and receive event information in a circle area whose center is the position of node *i* and radius is R_c , i.e., we use Boolean perceptual model;

3) The base station stores location information of all nodes;

4) The communication protocol between nodes is the same communication protocol which is used when nodes send message to the base station, named Protocol I. Protocol I is different with the communication protocol which is used when the base station sends message to nodes, named Protocol II. Protocol II has a higher transmit power so that the base station can send message directly to every node;

5) The sleeping nodes use Protocol II to communicate, so that they can not receive the message sent by the neighbors, but the wake-up message from the base station.

2.2. Definitions

Before we propose the coverage balancing strategy, some conceptions should be defined as follows.

Definition 1. Main neighbor. For any node *i*, its main neighbor set is defined as follows: $MN(i) = \left\{ j \in N(i) \mid \frac{\sqrt{2}}{2} R_c \le d(i, j) \le R_c \right\}$, where, $N(i)$ denotes the neighbor set of node *i*, $d(i, j)$ denotes the distance between node *i* and its neighbor *j*.

Definition 2. Minor neighbor. For any node *i*, its minor neighbor set is defined as follows:

$IN(i)=\left\{ j\in N(i)\,|\,d(i,j)<\frac{\sqrt{2}}{2}R_c \right\}$, where, $N(i)$ denotes the neighbor set of node *i*, $d(i,j)$ denotes the distance between node *i* and its neighbor *j*.

Definition 3. Triple coverage. A position in monitoring area is at least within the sensing range of three nodes, then the position is triple covered.

Definition 4. Sensing triangle status. For any three nodes A, B and C, they are within the sensing range of each other, these three nodes form the sensing triangle status, denoted ST (A, B, C).

Definition 5. Communication triangle status. For any three nodes A, B and C, they are main neighbors of each other, these three nodes form the communication triangle status, denoted CT (A, B, C).

Obviously, communication triangle status is a special status of sensing triangle status. Furthermore, for CT (A, B, C), triangle △ABC is not obtuse triangle, and only when three sides are $\frac{\sqrt{2}}{2}R_c$, $\frac{\sqrt{2}}{2}R_c$ and R_c respectively, △ABC is right-angled triangle.

Corollary 1: For CT (A, B, C), any position *p* in the range of triangle △ABC, the maximal distance between *p* and any side of △ABC is $\frac{\sqrt{2}}{2}R_c$, and the minimal distance is $\frac{1}{2}R_c$.

Obviously, for CT (A, B, C), when △ABC is right-angled triangle, we get the maximal distance which is the right-angle side, and the minimal distance which is the distance between right-angle and hypotenuse. So, the maximal distance is $\frac{\sqrt{2}}{2}R_c$, and the minimal distance is $\frac{1}{2}R_c$.

Definition 6. For communication triangle status CT (A, B, C) and CT(A',B',C'), if △ ABC and △A'B'C' do not have any overlap region, it is defined that CT (A, B, C) does not contain CT(A',B',C') completely.

Corollary 2: CT (A, B, C) does not contain CT(A,B,C') completely iff $d(C,C')\geq R_c$, where, $d(C,C')$ denotes the distance between node C and C'.

Proof: First, we prove the sufficient condition. CT (A, B, C) does not contain CT(A,B,C') completely, so node C and C' lie different sides of side AB. Obviously, $d(C,C')\geq d(\mathrm{C,AB})+d(\mathrm{C',AB})$, where, $d(\mathrm{C,AB})$ and $d(\mathrm{C',AB})$ denote the distance between node C and side AB and the distance between node C' and side AB respectively. According to Corollary 1, $d(\mathrm{C,AB})\geq\frac{1}{2}R_c$ and $d(\mathrm{C',AB})\geq\frac{1}{2}R_c$, so $d(C,C')\geq R_c$.

Second, we use reductio ad absurdum to prove the necessary condition. We assume that node C and C' lie same side of side AB. For $d(C,C')\geq R_c$, $d(A,C')\leq R_c$ and $d(B,C)\leq R_c$, we get $\angle CAC'\geq\angle ACC'$ and $\angle CBC'\geq\angle BC'C$. The sum of four angles in quadrilateral □ ABC'C is 2π, but $\angle CAB\leq\pi/2$ and $\angle ABC'\leq\pi/2$, so $\angle ACC'\geq\pi/2$ or $\angle BC'C\geq\pi/2$. May assume that $\angle ACC'\geq\pi/2$, then $\angle ACC'>\angle CAC'$. Here we find the contradiction, so node C and C' lie different sides of side AB, i.e., CT (A, B, C) does not contain CT(A,B,C') completely.

Corollary 3: If node B and C are main neighbors of node A, and any communication triangle status with side AB does not contain any communication triangle status with side

AC completely, then the minimal distance between node B and C is $1.41R_c$, and the maximal distance is $1.87R_c$.

Proof: For a communication triangle status with side AB, CT(A,B,D), if the length of side AD is $\frac{\sqrt{2}}{2}R_c$ and side BD is R_c, $\angle BAD$ increase to the maximal coverage angle. For a communication triangle status with side AC, CT(A,C,D'), if the length of side AD' is $\frac{\sqrt{2}}{2}R_c$ and side CD' is R_c, $\angle CAD'$ increase to the maximal coverage angle. Fig. 1 is the critical state of that CT(A,B,D) does not contains CT(A,C,D') completely. Node D and D' are coincident in Fig. 1, and *x* and *y* denote the length of side AB and AC respectively.

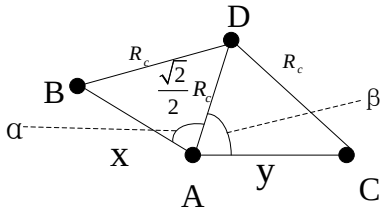


Figure 1. The Critical State of Two Communication Triangle Statuses Does Not Contain Each Other Completely

According to cosine theorem, we get three formulas as follows:

$$BD^2 = AB^2 + AD^2 - 2AB \cdot AD \cdot \cos\alpha \quad (1)$$

$$CD^2 = AC^2 + AD^2 - 2AC \cdot AD \cdot \cos\beta \quad (2)$$

$$BC^2 = AB^2 + AC^2 - 2AB \cdot AC \cdot \cos(\alpha + \beta) \quad (3)$$

We substitute the length of sides in Fig. 1 and $\cos(\alpha+\beta)=\cos\alpha\cos\beta-\sin\alpha\sin\beta$ into the above three formulas:

$$R_c^2 = x^2 + \left(\frac{\sqrt{2}}{2}R_c\right)^2 - 2x\cdot\frac{\sqrt{2}}{2}R_c\cdot\cos\alpha \quad (4)$$

$$R_c^2 = y^2 + \left(\frac{\sqrt{2}}{2}R_c\right)^2 - 2y\cdot\frac{\sqrt{2}}{2}R_c\cdot\cos\beta \quad (5)$$

$$BC^2 = x^2 + y^2 - 2xy\cos\alpha\cos\beta + 2xy\sin\alpha\sin\beta \quad (6)$$

So we get expression about the distance between node B and C:

$$BC^2 = 2R_c^2 - \frac{\left(3R_c^2 - 2x^2\right)\left(3R_c^2 - 2y^2\right)}{4R_c^2} + \frac{\sqrt{\left[8R_c^4 - \left(3R_c^2 - 2x^2\right)^2\right]\left[8R_c^4 - \left(3R_c^2 - 2y^2\right)^2\right]}}{4R_c^2} \quad (7)$$

Obviously, the distance between node B and C is monotonically increasing with *x* and *y* in interval $x \in \left[\frac{\sqrt{2}}{2}R_c, R_c\right]$ and $y \in \left[\frac{\sqrt{2}}{2}R_c, R_c\right]$. So when $x = \frac{\sqrt{2}}{2}R_c$ and $y = \frac{\sqrt{2}}{2}R_c$, the distance between node B and C is minimal and the result is $1.41R_c$; when $x = R_c$ and $y = R_c$, the distance between node B and C is maximal and the result is $1.87R_c$.

2.3. Sleep Scheduling of Coverage Balancing

We use sleep scheduling to achieve coverage balancing. The nodes who are selected to be working nodes should ensure triple coverage in local area of these nodes. Fig. 2 shows that the minimal number of communication triangle statuses to coverage the whole around of a node is four. So when working nodes update, if the number of trust main neighbors of a working node is not more than four, then these trust main neighbors join the working nodes set WS.

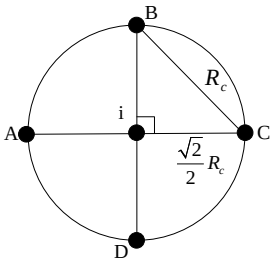


Figure 2. Minimal Number of Communication Triangle Statuses to Coverage the Whole Around of a Node

When sleep node j wakes up and is allowed to join the network, there are two steps before updating working nodes in the local area of node j:

1) The base station finds out neighbor nodes of node *j* and wake up the neighbors who are sleeping;

2) All neighbors of node *j* form candidate nodes set, and part of them will become working nodes.

The algorithm of updating working nodes is shown in Figure 3.

```
Set_Working_Nodes(x,y){
   MCxy = Select_Common_MN(x,y, MCx);
            d(m,n) = Max_Distance(MCxy);
            If   (d(m,n)>=Rc)
                  Wm=1,Wn=1;
                  Set_Sleep(MCxy,m_ID,n_ID);
            Else   If (|MCxy|>=1)
                              m                              =
Select_Max_Energy(MCxy);
                              Wm=1;
                              Set_Sleep(MCxy,m_ID);
}

MCj = Select_Trust_MN(j);
If   (|MCj|>4)
     d(i,k) = Max_Distance(MCj);
     If   (d(i,k)>=L)
            Wi=1,Wk=1;
            Set_Working_Nodes(j,i)
            Set_Working_Nodes(j,k)
     Else
          i = Select_Max_Energy(MCj);
          Wi=1;
          Set_Working_Nodes(j,i)
Else
     Set_Sleep(NCj, MCj);
```

Figure 3. The Algorithm of Updating Working Nodes

NCj in the algorithm denotes the candidate neighbor nodes set. MCj denotes the trust candidate main neighbor nodes set. MCxy denotes the set of nodes who are common candidate main neighbors of node *y* and node *x* in MCx. We set the value of *L* to be the average of minimal distance and maximal distance in Corollary 3, so $L = 1.64R_c$.

The main idea of algorithm is: first, we select two nodes *i* and *k* whose distance is not less than *L* to become working nodes; second, we select two nodes in MCji to become working nodes, and these two nodes must lie different side of side *ji*; third, we select two nodes in MCjk to become working nodes, and these two nodes must lie different side of side *jk*; finally, the nodes who do not become working nodes in MCj and the nodes in NCj but not in MCj will sleep.

For selecting a new working node in every side of side *ji* as much as possible, the coverage density of nodes should be big enough. The shadow in Fig. 4 is one side of the area that nodes in MCji may lie in. The area of the shadow is nearly twice of the area of triangle △ABC in Fig. 4, so:

$$S_{shadow} \approx \frac{R_c^2}{4l}\left(\sqrt{R_c^2 - \frac{l^2}{4}} - \sqrt{\frac{R_c^2}{2} - \frac{l^2}{4}}\right) \quad (8)$$

Formula (8) shows that S_{shadow} is monotonically decreasing with l in interval $l \in \left[\frac{\sqrt{2}}{2}R_c, R_c\right]$, and when $l = R_c$, S_{shadow} get the minimal result $0.092R_c^2$. So the coverage density of nodes should at least be $\frac{10.87}{R_c^2}$. If the area of monitoring area is S, we need at least deploy $\frac{10.87S}{R_c^2}$ nodes.

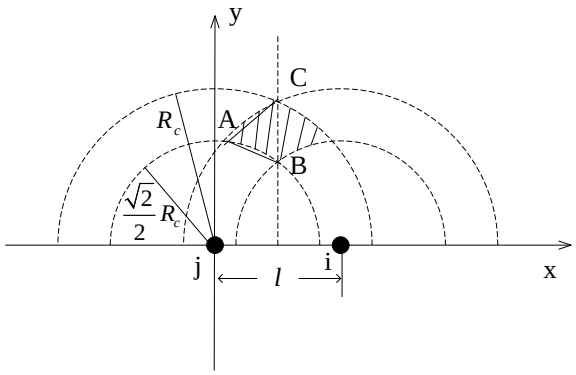


Figure 4. One Side Area of MCji

3. Coverage Balancing Based Trust Evaluation Method

Every node keeps an about its neighbors, and the table structure is shown in Table 1:

Table 1. Information Table of Neighbors

IDj	Xj	Yj	Ej	T(i,j)	MNj	Wj

In this table, IDj denotes neighbor's ID; Xj and Yj denote neighbor's coordinate; Ej denotes neighbor's energy; T(i,j) denotes neighbor's trust value which is evaluated by itself ; MNj denotes the neighbor is main neighbor or not; Wj denotes the neighbor is working node or not.

After all nodes are deployed in monitoring area, every node broadcasts its location, then all nodes establish their own information table of neighbors according to the broadcast message they received. In the beginning, T(i,j) in every node's information table is initialized as 100. The coverage balancing based trust evaluation method includes three steps as follows:

1) Select initial working nodes. All nodes update Ej and Wj in their information table. The nodes that are not selected to be working nodes sleep;

2) The working nodes have two tasks, one is sensing event and sending it to the base station, another is updating Ej and T(i,j) in their information table;

3) Once a sleep node wakes up, we will update the working nodes in local area of this node according to coverage balancing strategy which is mentioned in section 2, and at the same time, the base station updates the trust of the node who wakes up just now.

3.1. Select Initial Working Nodes

If three nodes are distributed as Figure 5(a), the shadow area in Figure 5(a) where is triple covered by these three nodes is maximal. Then we can calculate the average area covered by one node when all nodes are distributed the most sparsely like Fig. 5(b). Obviously, every node covers a regular hexagon area whose side length is $R_c / \sqrt{3}$. So the maximal average area covered by one node is $S_{\max} = \frac{\sqrt{3}}{2} R_c^2$, and we need at least $S / S_{\max}$ working nodes, i.e., $N_{\min} = \frac{2S}{\sqrt{3} R_c^2}$.

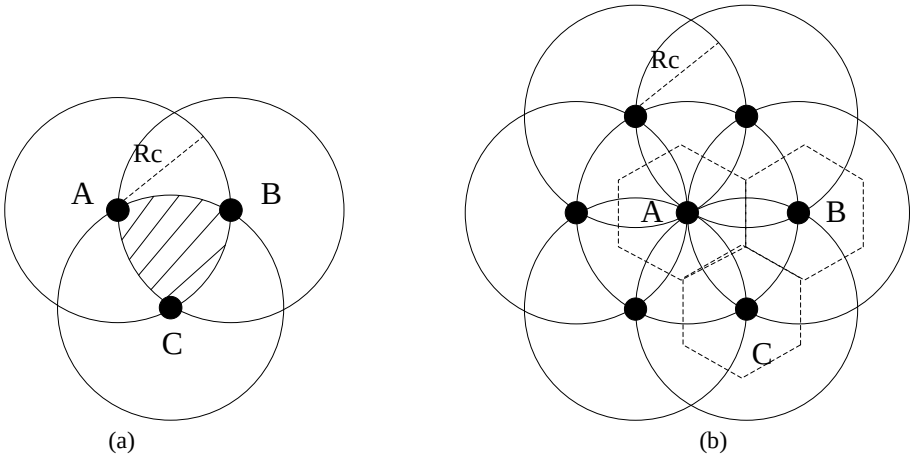


Figure 5. Working Nodes are Distributed the Most Sparsely

We select $N_{\min}$ nodes as initial working nodes to add into working nodes set WS. All nodes in WS broadcast the message that they are working nodes. Nodes who received the message update Ej and Wj in their information table. Finally, nodes who are not selected to be working nodes sleep.

3.2. Update Trust of Nodes

The trust of nodes is divided into two parts: the trust between nodes and the trust calculated by the base station. The former is used to select the next hop when nodes forward data packets and judge that neighbors are allowed to join the network or not when they wake up. The latter is the basis of judging whether the node is malicious node. When node *j* wakes up and requests to join the network, its neighbors will send an allowed message (AM) or a refused message (RM) to the base station. AM denotes the message

that neighbor *i* allows node *j* to be working node, RM denotes the message that neighbor *i* refuses node *j* to be working node. Some smart malicious nodes perform lawfully in peacetime, however, attack the network when there are nodes wake up and request to join the network. To find out these malicious nodes quickly, the behavior of nodes when sending message is divided into two categories: one is that whether nodes have sent false AM or RM message, denoted as behavior A, and all other behavior is denoted as behavior B. The behavior that legitimate nodes do not forward AM or RM message for network congestion and malicious nodes refuse to forward AM or RM message does not belong to behavior A , but belong to behavior B.

When node *x* updates its neighbors' trust, node *x* will get neighbors' recent behavior by time window mechanism. Then we calculate the trust value ($T_{x,y}$) of node *y* at node *x*:

$$T_{x,y} = \left[100 \left(\frac{BS_{x,y} + AS_{x,y}}{BS_{x,y} + AS_{x,y} + BU_{x,y} + AU_{x,y}} \right) \left(1 - \frac{1}{BS_{x,y} + AS_{x,y} + 1} \right) \left(\frac{1}{AU_{x,y} + 1} \right) \right] \quad (9)$$

Where, $[\cdot]$ is the nearest integer function. $AS_{x,y}$ and $BS_{x,y}$ denote the correct times of behavior A and behavior B monitored by node *x* about node *y*, respectively. $AU_{x,y}$ and $BU_{x,y}$ denote the incorrect times of behavior A and behavior B monitored by node *x* about node *y*, respectively. The previous two expressions in formula (9) is same with the trust evaluating formula at the node level in [5], and the last expression is used to reduce $T_{x,y}$ rapidly with an increase in $AU_{x,y}$. Node x will update T(i,j) in its information table of neighbors according to $T_{x,y}$.

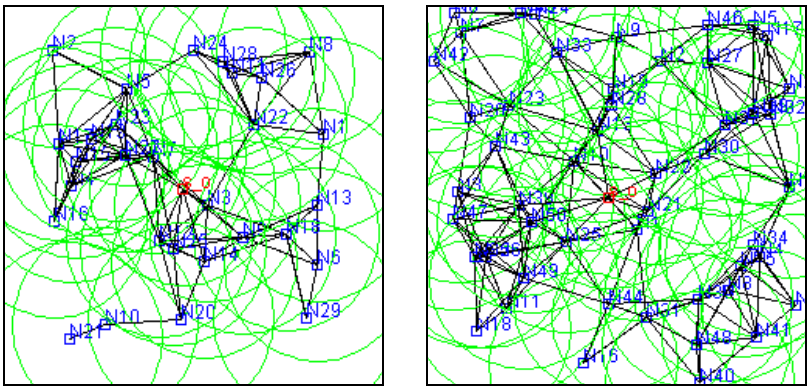
The base station updates the trust of nodes only when these nodes wake up. When node *j* wakes up, its neighbor *i* allows it to be working node or not according to T(i,j) in information table of neighbor *i*. If T(i,j) is larger than T_w, neighbor *i* sends message AM to the base station, otherwise neighbor *i* sends message RM to the base station. T_w denotes the trust threshold that a node is allowed to be working node. The initial trust of all nodes at the base station is 100. If the number of AM about node *j* is less than the number of RM, the trust of node *j* at base station minus 1. When the trust of node *j* at base station is lower than T_m, the base station judges node *j* to be malicious node, and removes it from network.

3.3. Update Working Nodes

When node *j* wakes up, the base station judges whether node *j* is allowed to join the network according to the number of message AM and RM. If node *j* is not allowed to be working node, the base station will notice it to sleep again. Else the base station will notice node *j* to be working node and update working nodes in the local area of node *j* according to the coverage balancing strategy which is mentioned in section 2.

4. Simulation Experiments and Analysis

We compare the proposed method with RFSN and GTMS in the nodes' lifetime, the detection rate and false alert rate of malicious nodes through simulation experiments. In simulation environment, we design a $100 \times 100 m^2$ square monitoring area, and the sensing radius and communication radius of sensor nodes are both 20m. The initial energy of sensor nodes is 1J, and the energy consumption of sending and receiving data package are both 100nJ/b. The node size of proposed method cannot be designed the same with RFSN and GTMS, which is discussed in below.



(a) (b)

Figure 6. Network Topology

To compare the effectiveness of the above three methods under same nodes size, we should know the average number of working nodes (N_{work}) when the whole area is balanced covered in proposed method. Then the nodes size of RFSN and GTMS will set to be N_{work} . According to the simulation environment and the minimal coverage density mentioned in section 2.3, we deploy 272 nodes on the monitoring area randomly. At the beginning of simulation, 29 nodes are selected randomly to be working nodes, as shown in Fig. 6(a). Fig. 6(b) shows the network topology at a moment when the whole area is balanced covered, and the nodes size of other moment of coverage balancing is nearly 50 too. So $N_{work} = 50$, and the nodes size of proposed method is 5.5 times the nodes size of RFSN and GTMS. When we set malicious nodes artificially, the number of malicious nodes of proposed method is 5.5 times the number of RFSN and GTMS, too.

We set the attack of malicious nodes to be selective forwarding attacks, and the malicious nodes forward data packets correctly by 50%.

4.1. Comparison of Nodes' Lifetime

The lifetime of nodes in proposed method is the sum of working time which not including sleeping time. To compare with the other two methods in one figure, we sample 50 nodes randomly in proposed method. Figure 7 shows the comparison of the nodes' lifetime among proposed method, RFSN and GTMS under the premise of no malicious nodes. It is observed that nodes' average lifetime in proposed method is about 2100 seconds, while RFSN is about 1500 seconds and GTMS is about 1700 seconds. So the proposed method can increase nodes' lifetime effectively. One hand, the proposed method can ensure uniform distribution of working nodes during whole lifetime of network, so there is no excessively redundant information. On the other hand, there is no aggregation of trust in proposed method and nodes only send the message AM or RM to the base station, while nodes in the other two methods should send their neighbors' trust to the base station to be aggregated. Obviously, the latter data packages are much more, and they consume more energy when be sent.

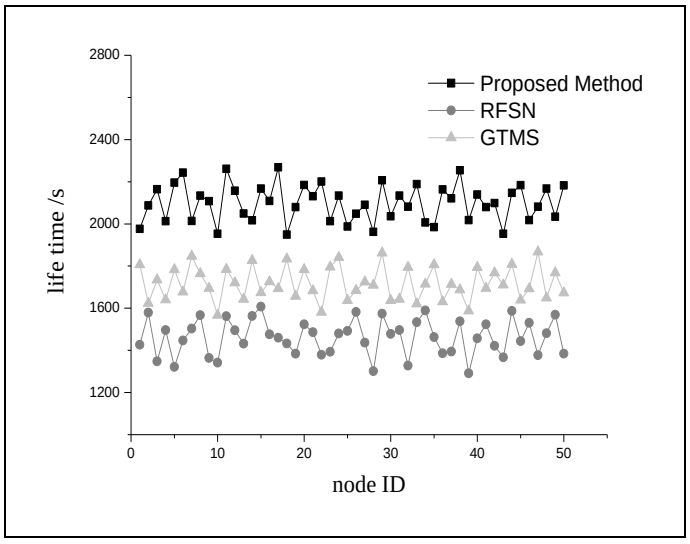


Figure 7. Comparison of Nodes' Lifetime

4.2. Comparison of Detection Rate

Figure 8 shows the variation in detection rate of proposed method, RFSN and GTMS vs. the number of malicious nodes. As we can see the detection rate of proposed method is better than the other two methods, moreover, it is above 80% when the proportion of malicious nodes is close to 40%. With the increase of malicious nodes, they will unite together to attack the network. The trust of these malicious nodes at base station will be calculated higher than the real trust, so the malicious nodes cannot be detected. However, the detection rate of proposed method does not decrease obviously when the proportion of malicious nodes is between 25% and 50%. Because when a small part of the malicious nodes unite together to attack the network, they will forward many false message AM or RM, and the trust of these malicious nodes at their neighbors will decrease quickly according to formula (9). These malicious nodes will be noticed to sleep when updating working nodes in nearby area. When they wake up, if their trusts at neighbors are low, they are not allowed to join the network. Then the trusts of them at the base station will decrease until below T_m , and finally they will be removed from network.

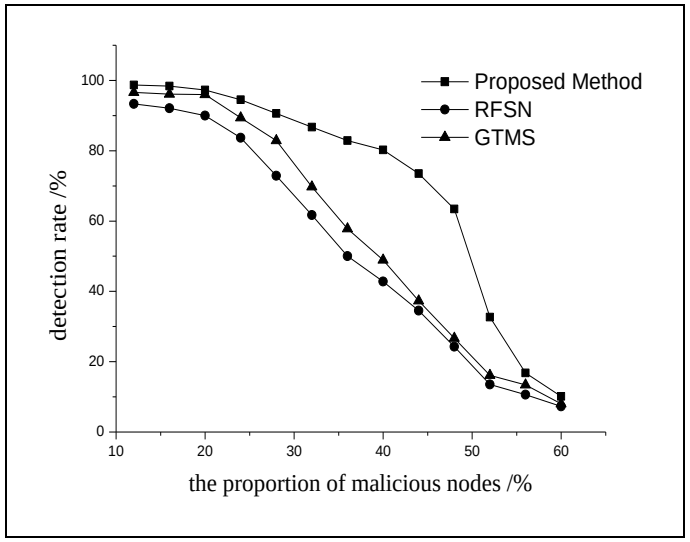


Figure 8. Comparison of Detection Rate

4.3. Comparison of Detection Efficiency

As shown in Figure 8 the detection rate of three methods are all above 90% when the proportion of malicious nodes is 20%, so the simulation experiment set the proportion of malicious nodes to be 20% to compare the detection efficiency of the three methods. Fig. 9 shows the variation in detection rate of proposed method, RFSN and GTMS vs. time. As we can see the detection efficiency of proposed method is much lower than the other two methods. GTMS only needs about 200 seconds to detect 95% malicious nodes, RFSN needs about 300 seconds to detect 90% malicious nodes. However the proposed method needs 450 seconds to detect 95% malicious nodes. The detection efficiency of proposed method is lower than half of GTMS. The reason is that even though the trust of a malicious node at its all neighbors is very low, it is still not removed from network immediately. A malicious node will constantly repeat the process of sleep, wake up and request to join the network. Finally, the base station will judge whether it is malicious node or not. Although the process is cumbersome, it can reduce the false alert rate of legitimate nodes, which we will discuss in the next section.

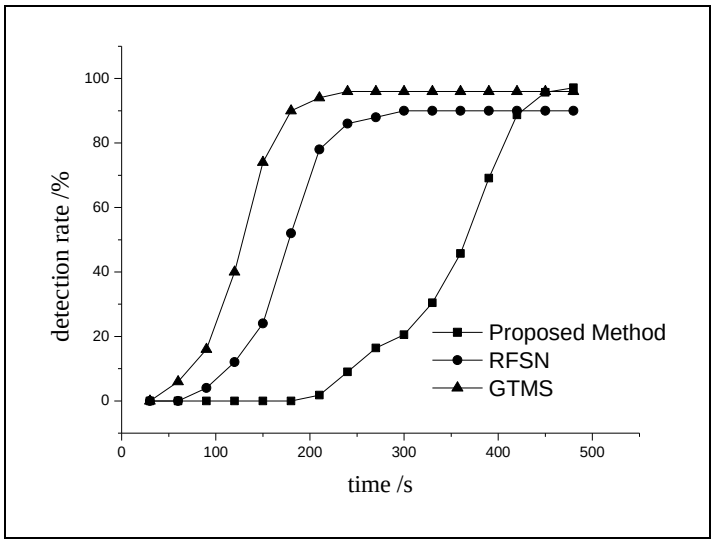


Figure 9. Comparison of Detection Efficiency

4.4. Comparison of False Alert Rate

Figure 10 shows the variation in false alert rate of proposed method, RFSN and GTMS vs. the number of malicious nodes. As we can see the false alert rate of proposed method is lower than the other two methods, moreover, it is below 10% when the proportion of malicious nodes is close to 35%. When the base station mistake a legitimate node for malicious node, there must be some malicious nodes forwarding false message AM or RM. Then their trust at neighbors will decrease quickly according to formula (9). These malicious nodes will be noticed to sleep when updating working nodes in nearby area. When they wake up, if their trusts at neighbors are low, they are not allowed to join the network. Since the malicious nodes always keep sleep and cannot attack the network continuously, the legitimate nodes will not be easily mistaken for malicious nodes.

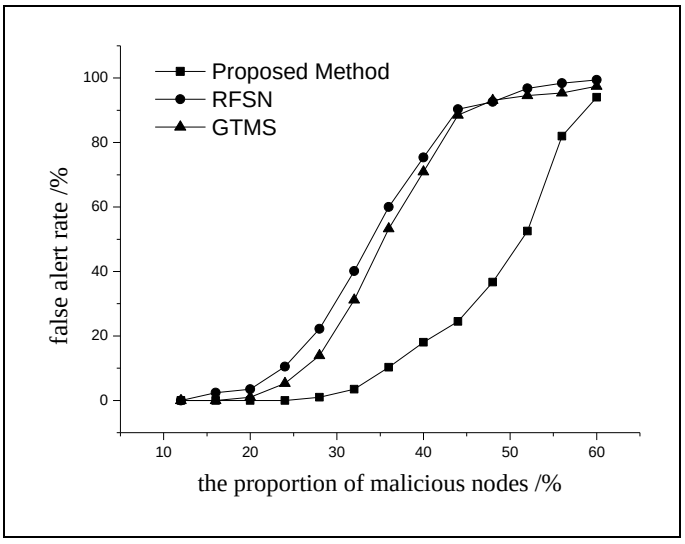


Figure 10. Comparison of False Alert Rate

5. Conclusion

When the distribution of nodes in WSNs meets certain nodes coverage requirements of uniform distribution and coverage density, the trust evaluation of nodes will not only save energy but also be accurate. For this purpose, this paper proposed a coverage balancing based trust evaluation method for WSNs. We defined and designed the coverage balancing strategy, and elaborated on the process of updating working nodes and updating the trust of nodes. Simulation results show that the proposed method can effectively improve node lifetime. Though it takes longer time on detection of malicious nodes, it has higher detection rate and lower false alert rate compared with some trust evaluation methods, so it can ensure the network run safely.

Acknowledgments

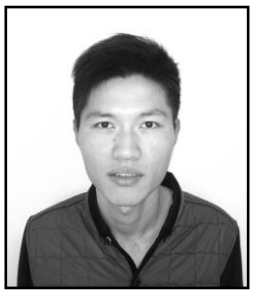
This work was supported by the national natural science foundation of China (No. 61300053), the 973 plan project foundation of Jiangsu province (No. BK2011023), and the six talent peaks project foundation of Jiangsu province (No. 2011DZXX028).

References

[1] S. H. Shah, A. Iqbal, S. S. A. Shah, "Remote health monitoring through an integration of wireless sensor networks, mobile phones & Cloud Computing technologies", IEEE Global Humanitarian Technology Conference, **(2013)**, pp.401-405.
[2] Z. YU, W. GAO, X. ZUO, "Design of Novel Intelligent Transportation System based on Wireless Sensor Network and ZigBee Technology" , J. Sensors and Transducers, vol. 156, no. 9, **(2013)**, pp. 95-102.
[3] J.G. Kolo, Li-Minn Ang, Kah Phooi Seng, S.R.S. Prabaharan, "Performance comparison of data compression algorithms for environmental monitoring wireless sensor networks", J. International Journal of Computer Applications in Technology, vol. 46, no. 1, **(2013)**, pp. 65-75.
[4] S. Ganeriwal, L. K. Balzano, M. Srivastava, "Reputation based frame-work for high integrity sensor networks", J. ACM Transactions on Sensor Networks, vol. 4, no. 3, **(2008)**, pp. 1-37.
[5] R. A. Shaikh, H. Jameel, B. J. d'Auriol, H. Lee, S. Lee, Y. J. Song, "Group-based trust management scheme for clustered wireless sensor networks", J. IEEE Transactions on Parallel and Distributed Systems, vol. 20, no. 11, **(2009)**, pp. 1698-1712.
[6] F. Ishmanov, S. W. Kim, "A secure trust establishment in wireless sensor networks", International Conference on Electrical Engineering and Informatics, **(2011)**, pp. 1-6.
[7] J. Zhang, R. Shankaran, M. A. Orgun, V. Varadharajan, A. Sattar, **"**A trust management architecture for hierarchical wireless sensor networks", IEEE 35th Conference on Local Computer Networks, **(2010)**, pp. 264-267.

[8] J. Zhang, R. Shankaran, M. A. Orgun, V. Varadharajan, A. Sattar, "A Dynamic Trust Establishment and Management Framework for Wireless Sensor Networks", IEEE/IFIP 8th International Conference on Embedded and Ubiquitous Computing, **(2010)**, pp. 484-491.
[9] V. R. S. Dhulipala, N. Karthik, R. M. Chandrasekaran, "A Novel Heuristic Approach Based Trust Worthy Architecture for Wireless Sensor Networks", J. Wireless personal communications, vol. 70, no. 1, **(2013)**, pp. 189-205.
[10] P. Trakadas, S. Maniatis, P. Karkazis, T. Zahariadis, H. C. Leligou, S. Voliotis, "A novel flexible trust management system for heterogeneous wireless sensor networks", International Symposium on Autonomous Decentralized Systems, **(2009)**, pp. 1-6.
[11] T. Zahariadis, P. Trakadas, H. C. Leligou, S. Maniatis, P. Karkazis, "A novel trust-aware geographical routing scheme for wireless sensor networks", J. Wireless personal communications, vol. 69, no. 2, **(2013)**, pp. 805-826.
[12] D. F. Luiz, C. M. S. Figueiredo, E. F. Nakamura, "A coverage-based drop-policy in wireless sensor network with disruptive connections", IEEE Symposium on Computers and Communications, **(2012)**, pp. 000394-000398.
[13] D. Wang, Q. Qin, J. Yu, "The Algorithm of Coverage Base on Probability Sensing Model in Wireless Sensor Network", 8th International Conference on Wireless Communications, Networking and Mobile Computing, **(2012)**, pp. 1-4.
[14] M. Mahdavi, M. Ismail, K. Jumari, "Load balancing in energy efficient connected coverage wireless sensor network", International Conference on Electrical Engineering and Informatics, **(2009)**, pp. 448-452.

Author



Shen Haibo, he received his B.E. degree from Nanjing University of Science and Technology (NUST), China, in 2009. Now, he is a Ph.D. candidate in NUST. His research interests include wireless sensor network and information security.