Wireless Sensor Network, 2015, 7, 137-148
Published Online November 2015 in SciRes. http://www.scirp.org/journal/wsn
http://dx.doi.org/10.4236/wsn.2015.711012

A Secure and Energy-Balanced Routing Scheme for Mobile Wireless Sensor Network

Bei Liu, Yuanming Wu

School of Optoelectronic Information, University of Electronic Science and Technology, Chengdu, China
Email: liubeis@163.com, ymwu@uestc.edu.cn

Received 29 August 2015; accepted 8 November 2015; published 11 November 2015

Abstract

Mobile wireless sensor network (MWSN) has the features of self-organization, multiple-hop and limited energy resources. It is vulnerable to a wide set of security attacks, including those targeting the routing protocol functionality. In this paper, the existing security problems and solutions in MWSN are summarized, and then a trust management system based on neighbor monitoring is proposed. In the trust management system, the trust value is calculated by the neighbor monitoring mechanism, and the direct trust value and the indirect trust value are combined to establish the distributed trust model to detect the malicious nodes. The consistency check algorithm is capable of defending against the attacks on the trust model. In addition, because of the limited energy of the sensor nodes, the energy-balanced algorithm is introduced to prolong the lifespan of MWSN. The residual energy and energy density are considered in the routing decision. Finally, the simulation experiments show that the proposed algorithm can detect the malicious nodes effectively and achieve the energy-balanced goal to prolong the lifespan of MWSN.

Keywords

Mobile Wireless Sensor Network, Network Security, Trust Model, Energy-Balanced

1. Introduction

Mobile wireless sensor network consists of a large number of micro sensor nodes deployed in the monitoring area, and forms a self-organized network system by the wireless multi-hop communication. Mobile wireless sensor network does not require a fixed infrastructure support, and is widely used in military reconnaissance, medical surveillance, environmental monitoring, agricultural breeding and other commercial areas [1]. Wireless sensor network has the following characteristics: 1) limited hardware resources; 2) limited power capacity; 3) no center; 4) self-organization; 5) multi-hop routing; 6) dynamic topology; 7) a large number of nodes and dense

How to cite this paper: Liu, B. and Wu, Y.M. (2015) A Secure and Energy-Balanced Routing Scheme for Mobile Wireless Sensor Network. *Wireless Sensor Network*, **7**, 137-148. http://dx.doi.org/10.4236/wsn.2015.711012

distribution. Based on the above characteristics, the design of mobile wireless sensor network which is a special network is challenging.

In data-centric MWSN, because of interference, collision and bad wireless channel, data in the transmission process may make mistakes or miss, resulting in being not correctly sent to the SINK node. The classic encryption and authentication mechanism can resist external attacks such as tapping data and breaking network communication, but can't solve the problem of internal attack. When the normal sensor node is captured and cracked by the enemy, it becomes a malicious node, attacks the network, and damages the normal function of the network. **Table 1** lists common types of malicious node attacks.

Mobile wireless sensor network faces various threats. In [2], a lightweight secure routing protocol is proposed, which can resist the known attacks that break the basic structure of the route. A protocol based on secure routing feedback is proposed [3]. Feedbacks from the neighbor nodes and base station provide the dynamic information of the current network. The secure multicast routing protocol is proposed in [4]. The trust model based on neighbor node monitoring is widely studied in recent years. A node evaluates its neighbor nodes and calculates the trust values as the decision parameters of the routing selection stage [5]. The method of obtaining trust information and calculating the trust value of each node is called trust model that can be classified by the different monitoring behaviors [6]. According to the distribution of trust decision-making mechanism, trust model can be divided into centralized [7], hierarchical [8] or fully distributed [5]. There are a series of behaviors needing to be monitored. Each behavior corresponds to a trust metric. The trust metrics should be comprehensive, including data forwarding [5], location verification [9], data packet integrity and authenticity [8], etc. The various communication behaviors need to be turned into trust values or varying levels of trust. Trust exchange mechanism is proposed [10] [11] to improve the reliability of trust information effectively. However, these mechanisms not only increase the resource consumption, but also make the trust model itself easily attacked. For example, a malicious node deceives the trust exchange mechanism through exchanging false trust information [12]. In the trust model based on direct observation [6] [7] [13], the data that the node itself monitors are not entirely accurate. So the combination of the direct trust values and the indirect trust values obtained by the third party nodes is proposed [14]. This paper proposes a trust management approach from the human social relations to defend against malicious attacks. A node monitors the behaviors of its neighbor nodes to evaluate their trust values and then considers these trust values when the node selects the next hop forwarding node. The trust values can be directly obtained by the node, and can also be provided by other neighbor nodes.

In addition to the security threat caused by malicious node attacks, mobile wireless sensor network needs to consider the problem of limited node energy. The energy factor is considered in the routing algorithm to prolong the lifespan of the network. MDD (Multipath Directed Diffusion) routing algorithm expands the DD (Directed Diffusion) routing algorithm, and establishes multiple paths from the source node to the destination node to balance the energy consumption of each node [15]. The routing algorithm with multiple SINK nodes can reduce the paths of data transmission and save node energy [16]. In [17], LEACH (Low Energy Adaptive Clustering Hierarchy) is proposed which adopts a hierarchical structure and selects cluster heads periodically. Since each node

Table 1. Malicious attacks.

Attack type	Attacker behavior
Selective forwarding, black-hole, grey-hole	A malicious node discards part or all packets
Sinkhole attack	A malicious node tries to attract traffic advertising and fake routing information, and then it does not forward it
Replay attack	A malicious node continues to send the same data repeatedly
Link spoofing attack	A malicious node can deceive the link layer verification mechanism, so that the sender of the packet thinks that the packet has been forwarded successfully
Modification attack	A malicious node modifies the data packets that it forwards
Sybil attack	An attacker presents multiple identities
Collusion attack	Many powerful attackers work in collusion to implement attacks
Flooding attack	A malicious node sends a large number of packets to overwhelm the normal nodes
Bad mouthing attack	A malicious node provides dishonest recommendations

has the same opportunity to be chosen as the cluster head, the algorithm can balance the energy consumption of all nodes. In [18], the EBRP (Energy-Balanced Routing Protocol) routing algorithm is proposed, which can achieve the energy-balanced effect based on the depth, residual energy and energy density. The routing algorithm in this paper considers the energy factor that includes the remaining energy and energy density to prolong the lifespan of the network.

In the rest of the paper, the related work is summarized in Section 2, while in Section 3 a secure and energy-balanced routing scheme is proposed in detail. In Section 4, the simulation experiments for the algorithm are carried out. Finally, conclusions are drawn in Section 5.

2. Problem Formulation

2.1. Security Problem

In the mobile wireless sensor network, all nodes randomly move, the neighbor node set of each node is not fixed. A node monitors its neighbor nodes and evaluates their communication behaviors. When the node detects a malicious node from the neighbor nodes of the node, the node removes the malicious node from the neighbor nodes and no longer communicates with the malicious node. But the malicious node is able to move to a new location to continue to implement the attacks. So, after the node detects the malicious node, the node needs to notify the entire network of the ID of the malicious node. Considering a more complex situation, after the malicious node is detected, the malicious node changes its ID, and then moves to a new location to implement attacks. Because the ID of the malicious node is new, other nodes think that the malicious node is a normal node. As shown in **Figure 1**, this brings serious problems to the monitoring of malicious nodes. In this paper, the tracing technique through neighbor nodes is introduced to defend against this attack.

2.2. Limited Energy Problem

The weighted average of the depth, residual energy and energy density is introduced as the path decision criteria in EBRP. The algorithm can achieve energy-balanced effect in immobile wireless sensor network, but there are some problems in mobile wireless sensor network. In EBRP, the formula for calculating energy density is:

$$ED(i) = \sum_j \frac{E(j)}{S(i)} \tag{1}$$

The j means the neighbor node of the node i, $E(j)$ is the residual energy of the node j, $S(i)$ is the communication coverage area of the node i.

Due to node mobility, the neighbor nodes of the node i change constantly, if every time the neighbor nodes change, all values in Formula (1) are calculated again for a sum operation, this calculation is complex. Because

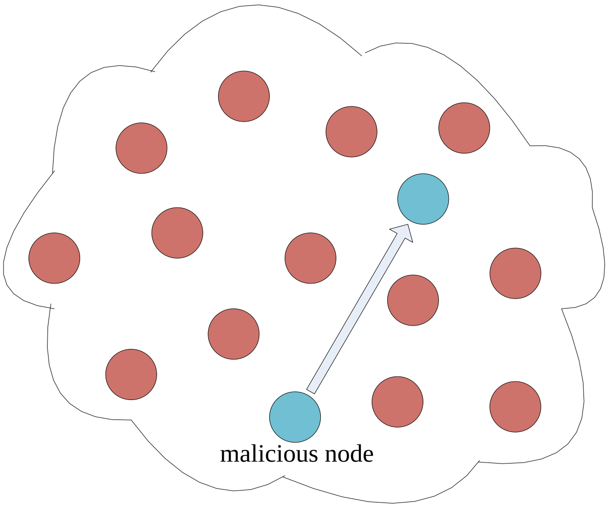

Figure 1. The malicious node moves and changes its ID.

every time the neighbor nodes change, the neighbor node set either adds a new node or reduces an old node. So the energy density only needs to add the value of the new node or subtract the value of the old node. The detailed formula is given in Chapter 3.4.

In addition, Formula (1) for calculating energy density is problematic. When the node *j* selects the next hop node for forwarding, it selects the forwarding node from the nodes that their depths are less than or equal to the depth of the node *j*. These nodes are the parent nodes or sibling nodes of the node *j*. So the node *j* should not consider all the neighbor nodes in Formula (1), but only the parent nodes and sibling nodes.

3. Secure and Energy-Balanced Routing Algorithm

In this chapter, combining the distributed trust model and the energy-balanced algorithm, a novel, easy to deploy, safe and effective mobile wireless sensor network routing algorithm is proposed. Based on the mechanism of neighbor monitoring and trust exchange, the trust model combines direct trust value with indirect trust value to detect malicious nodes. In addition, the residual energy and energy density of the nodes are considered in the routing decision to make the energy consumption balanced and prolong the lifespan of the network.

3.1. Network Topology

A large number of sensor nodes are distributed in a region randomly and uniformly to collect and forward data, which constitute a dynamic self-organizing network. The SINK node is located in the network to collect data and coordinate network.

3.2. Initialization and Update of the Depth

The SINK node broadcasts routing initialization message that includes message type and depth. The initial depth of each node is infinite. When a node receives the initialization message, if the depth of the message is greater than the depth of the node itself, the node updates the depth of the node itself and increases the depth of the message by 1, and then forwards the message. Eventually, each node has the correct depth, such as **Figure 2**.

Since the nodes are moving, the initial depths change in real time. There are 2 ways to update the depths. One is to update the depths by the SINK node in the global range like the process of route initialization. Because the depths of all nodes are updated, the energy consumption is great. The other one is that the nodes automatically update the depths. In the practical application, the moving distances of the nodes are limited in a short time, and the depths of most nodes are unchanged. When a node moves to a new location, the depth information can be obtained from neighbor nodes of the node. The node takes minimum depth from all depths of its neighbor nodes,

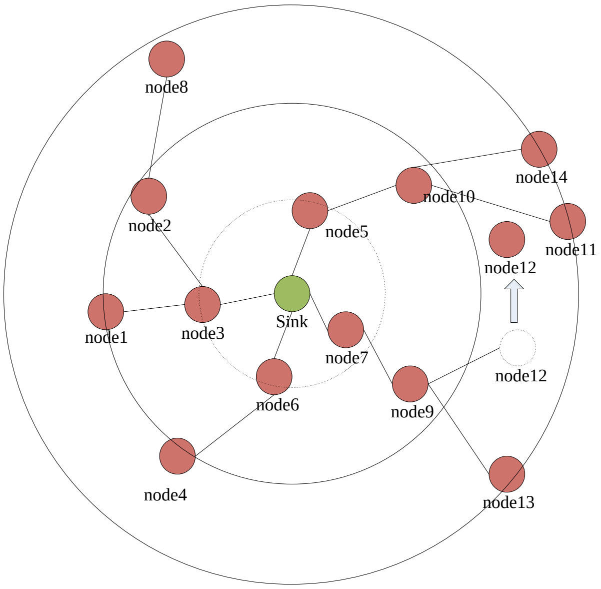

Figure 2. The depths of the nodes.

and then increases the minimum depth by 1 as the depth of the node itself. As shown in **Figure 2**, the node 12 moves to a new place, and updates its depth.

3.3. The Distributed Trust Model

The trust model consists of two modules that are the abnormal behavior detection module and the trust evaluation module. The abnormal behavior detection module establishes a series of abnormal behavior detection rules according to a variety of attack behavior features, and updates the statistics of normal and abnormal behaviors of the node according to the detection results. The trust evaluation module calculates the trust values according to the statistics, and judges whether the node is a malicious node or not. **Table 2** is some symbol descriptions of this paper.

In the trust model, a set of behaviors for node detection are defined. **Table 3** lists the trust metrics, each trust metric corresponding to one or a certain class of malicious attacks.

Specific detection methods are as follows:

1) Data forward: When the node *i* sends packets to the next hop node *j*, the node *i* is in promiscuous mode to overhear the wireless medium to ensure that whether the node *j* forwards the packets. In addition to the node *i*, the common neighbor nodes of the node *i* and the node *j* also monitor the node *j*.

2) ACK confirm: After the node *i* sends packets to the node *j*, the node *i* waits for the ACK from the node *j*. Considering the instability of the wireless communication channel, data retransmission mechanism is necessary, if the node *i* does not receive the ACK from the node *j* in a short time, the node *i* retransmits the packets. After trying the finite number of times, the node *i* gives up.

3) Data integrity: After the node *i* sends packets to the node *j*, the node *i* does not immediately delete the storage data of the packets, but monitors the node *j* and compares the forwarding packets of the node *j* with the storage packets of the node *i*.

4) Data flooding: If the number of packets received by the node *i* from the node *j* exceeds a certain threshold in a period of time, the behavior of the node *j* is considered abnormal.

Table 2. Symbol description.

Symbol	Description
i, j, k	Sensor node
A_m	Attack type, corresponding trust metric
R_{ij}	The distribution of the communication behavior of the node *i* about the node *j*, is a random variable
C_{ij}	The trust value of node *i* for node *j*, mathematical expectation for R_{ij}
R_{ij}^{Am}	For trust metric Am, the distribution of the communication behavior of the node *i* about the node *j*
C_{ij}^{Am}	For trust metric Am, the trust value of node *i* for node *j*, mathematical expectation for R_{ij}^{Am}
α_{ij}^{Am}	For trust metric Am, the number of nodes *j* normal communication behavior by node *j* monitor
β_{ij}^{Am}	For trust metric Am, the number of nodes *j* abnormal communication behavior by node *j* monitor

Table 3. Trust metrics for different malicious behaviors.

	Trust metric	Malicious behavior
1	Data forward	All types of packet loss attacks (black hole, gray hole, selective forwarding)
2	ACK confirm	The node does not confirm the ACK
3	Data integrity	Data tampering attack
4	Data flooding	Forward a large amount of data in a period of time
5	Data duplication	Delivery the same data repeatedly to the same node
6	Trust value response	In the trust exchange, the trust value is not returned to the requesting node
7	Trust value verification	“Badmouth” attack

5) Data duplication: If the number of the times that the node *i* receives same packet from the node *j* in a period of time exceeds a certain threshold, the behavior of the node *j* is considered abnormal.

6) Trust value response: The node *i* request trust information from the neighbor node *j*, if the neighbor node j responds the trust information to the node *i*, the number of successful times is increased by 1; otherwise the number of failed times is increased by 1.

7) Trust value verification: The trust values provided by the neighbor nodes need to be judged. This part will be given in the trust model.

The abnormal behavior detection module stores the detected results classified by the trust metrics. For a certain trust metric, if the behavior is normal, the α_{ij}^{Am} is increased by 1, otherwise the β_{ij}^{Am} is increased by 1.

There is a special case to consider: a malicious node performs well at the beginning to obtain the high trust value, and then implements attacks. The forgetting factor is introduced to detect the malicious node quickly. The trust value is calculated once every time period Δ*t*, the formulas are as follows:

$$\alpha_{ij}^{Am} = \mu_1 \alpha_{ij}^{Am} + \alpha_{ij}^{Am}(\Delta t) \tag{2}$$

$$\beta_{ij}^{Am} = \mu_2 \beta_{ij}^{Am} + \beta_{ij}^{Am}(\Delta t) \tag{3}$$

$$\mu_1 < \mu_2 \tag{4}$$

μ_1 and μ_2 are the forgetting factor.

For the trust metric *Am*, the direct trust value is:

$$C_{ij}^{Am}\_direct = E\left(R_{ij}^{Am}\right) = E\left(Beta\left(\alpha_{ij}^{Am}+1, \beta_{ij}^{Am}+1\right)\right) = \frac{\alpha_{ij}^{Am}+1}{\alpha_{ij}^{Am}+\beta_{ij}^{Am}+1} \tag{5}$$

For all trust metric, the direct trust value is:

$$C_{ij}\_direct = \frac{1}{n}\left(C_{ij}^{A1} + \gamma C_{ij}^{A2} + \gamma^2 C_{ij}^{A3} + \cdots + \gamma^n C_{ij}^{An}\right) \tag{6}$$

The γ in the Formula (6) indicates the penalty coefficient for multiple attacks. Due to the penalty coefficient, when a malicious node launches a variety of attacks simultaneously, even though the n kinds of trust values are high, the comprehensive trust value is very low.

When $C_{ij}^{Am}\_total$ is below the trust threshold value θ^{Am} or C_{ij}_total is below the trust threshold value θ, the node *i* considers the node *j* as malicious node. The node *i* sends the information about the malicious node *j* to the SINK node and then the SINK node broadcasts the information to all nodes of the network.

After the malicious node is detected, the malicious node may change its ID, and then moves to a new location to implement attacks. The tracing technique through neighbor nodes is required to defend against this attack. In mobile wireless sensor network, the moving path of a node is continuous. A node will not suddenly appear in a new place. Based on the neighbor exchange mechanism, each node broadcasts the neighbor table to its neighbor nodes. In **Figure 3**, the node 3 moves to a new location, before and after the node 3 moves, the node 4 and 5 have always been the neighbors of the node 3. The node 4 and 5 are able to trace the mobile path of node 3 and then provide tracking information to the node 1 and 2. In this way, the node 3 is identified as a normal mobile node according to the neighbor node tracking information. If the node 3 is a malicious node, after it is detected, it changes the ID, and then moves to the new location. All neighbor nodes of the node 3 have no trace information about the node 3. So the neighbor nodes consider the node 3 as a malicious node.

3.4. Energy Factor

The node needs to consider the energy factor when making the routing decision. The energy factor includes the residual energy and energy density.

The detail energy model is shown in **Figure 4**.

Forwarding a k-bit message consumes energy as follows:

$$E_{Tx} = E_{Tx_{elec}}(k) + E_{Tx_{amp}}(k,d) = \begin{cases} kE_{elec} + k\varepsilon_{fs}d^2, & d < d_0 \\ kE_{elec} + k\varepsilon_{mp}d^4, & d \ge d_0 \end{cases} \tag{12}$$

To receive a k-bit message, the energy consumption is computed by:

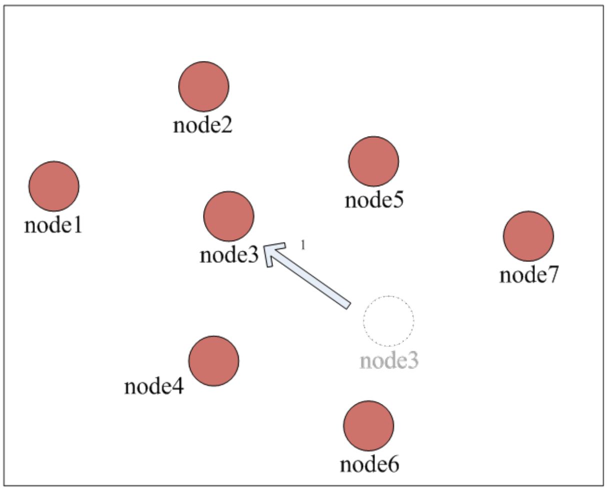

Figure 3. Tracing technique through neighbor nodes.

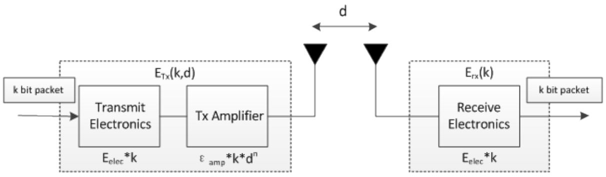

Figure 4. Energy model.

$$E_{Rx} = E_{Rx_{elec}}(k) = kE_{elec} \tag{13}$$

In WSN, energy consumption is caused by communication and calculation, but communication energy consumption is the main. Therefore, Formula (12) and (13) will be used in simulation experiments to estimate the energy consumption of sensor nodes.

Formula (14) is to calculate the energy density of the node:

$$ED(i) = \sum_j \frac{E(j)}{S(i)} \tag{14}$$

j means the parent nodes and sibling nodes that their depths are less than or equal to the depth of the node *j*, *E*(*j*) is the residual energy of the node *j*, *S*(*i*) is the communication coverage area of the node *i*.

When the neighbor nodes of the node *i* change, the neighbor node set either adds a new node or reduces an old node. The energy density only needs to add the value of the new node *k* or subtract the value of the old node *k* in Formula (15).

$$ED(i)\_new = ED(i)\_old \pm \frac{E(k)}{S(i)} \tag{15}$$

The energy factor *EE* is calculated:

$$EE(j) = \alpha * E(j) + \beta * ED(j) \tag{16}$$

$EE(j)$ represents the energy factor of the node *j*. The coefficient α and β mean the proportion of the residual energy and energy density. The Chapter 3.5 will introduce the energy factor in detail in secure and energy-balanced routing algorithm.

3.5. Secure and Energy-Balanced Routing Algorithm

The proposed routing algorithm includes the depth update stage and the data transmission stage. The depth update stage is introduced in detailed in Chapter 3.2. In the data transmission stage the node makes the routing decision to choose the next hop node for forwarding data. When the node *i* forwards data, the routing decision is made according to the following steps:

Step 1: according to the trust model, the neighbor nodes of the node *i* are judged and the malicious nodes are removed.

Step 2: select the nodes that their depths are less than the depth of the node *i*.

Step 3: select the node that has the largest energy factor EE from the nodes that have been selected in the step 2. The selected node becomes the next hop forwarding node of the node *i*.

4. Simulation and Analysis

The experiments of this paper are carried on the simulation platform MATLAB. 200 nodes are randomly deployed in 400 m*400 m rectangular space, and the SINK node is in the center.

4.1. Initialization and Update of the Depth

The **Figure 5** is the depth map after the initialization of the network, the circle represents the sensor node, and the square represents the SINK node. Some nodes are marked with a number that represents the depth of the node.

When a node moves randomly showed in **Figure 6**, the depth of the node is updated periodically showed in **Figure 7**. The depth of the node can be updated correctly and the change of the depth within a period is not more than 1.

4.2. The Distributed Trust Model

Combining direct trust value with indirect trust value, the trust model is simulated. 50 nodes are randomly selected from the network to send 6 packets to the SINK node per second. After 10 seconds 3 malicious nodes are randomly selected to implement selective forward attack. The packet loss rates respectively are 30%, 40% and 50%. After the node with 30% packet loss rate is detected, it changes the ID and moves to a new location to implement selective forward attack again. In **Figure 8**, the data arrival rate is lower than 100% from 11 seconds, which shows that there is packet loss attack in the network. **Figure 9** shows the number of times of malicious node attack. Because from 11 seconds the malicious nodes start to implement selective forwarding attack, the number of times begins adding. After 31 seconds, the numbers of attacks do not increase, it shows that the mali-

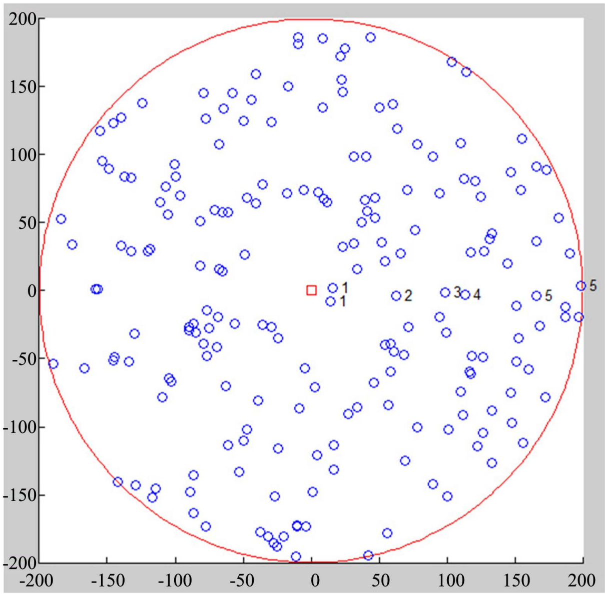

Figure 5. Initialization of the network.

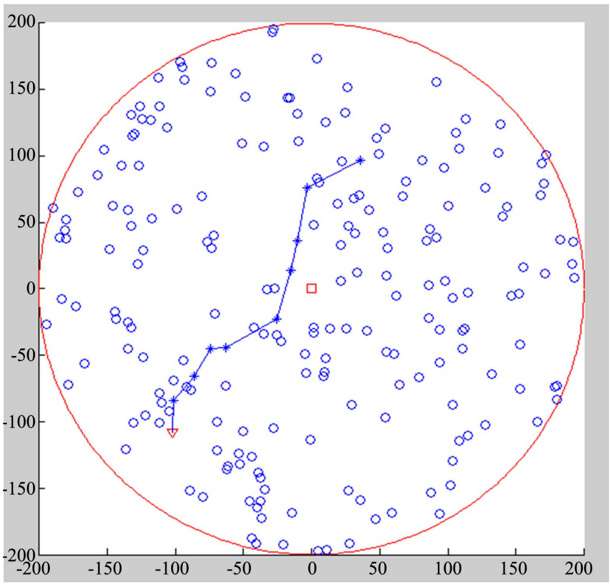

Figure 6. A node moves randomly.

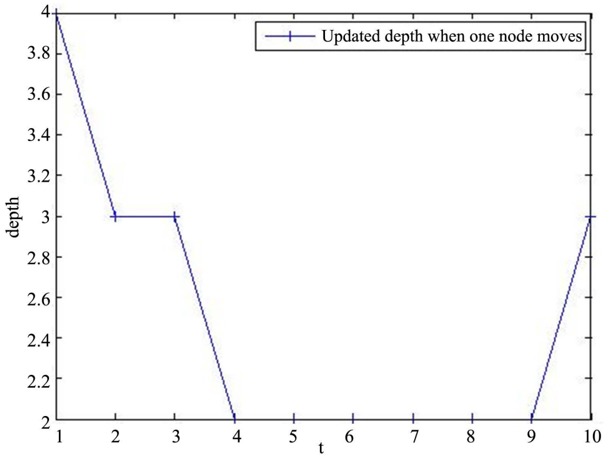

Figure 7. The depth of the node is updated.

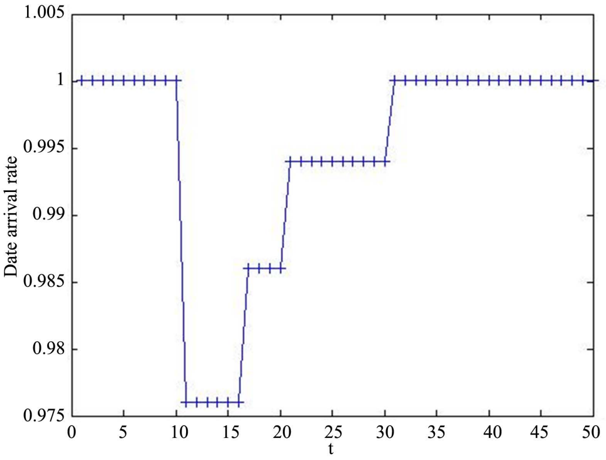

Figure 8. Packet arrival rate.

cious node changes the ID and moves to a new location, the malicious node is still identified as malicious node. **Figure 10** shows the failure rate for malicious node detection. The first malicious node is detected in 17 seconds and second in 21 seconds and third in 31 seconds. When all malicious nodes are detected, the probability of miss is 0. The simulation results show that the trust model can detect the malicious nodes effectively.

4.3. Algorithm Simulation

Malicious nodes implement attacks like Chapter 4.2. The simulation compares the lifespan of 2 algorithms. The algorithm a does not consider the energy factor in the routing decision, only choosing the secure node with minimum depth. The algorithm b is the proposed algorithm in this paper. The result in **Figure 11** shows that the algorithm b with the energy factor can significantly improve the lifespan of the network. Combined with Chapter 4.2, the proposed algorithm is secure and energy-balanced routing algorithm.

5. Secure and Energy-Balanced Routing Algorithm

In this paper, a secure and energy-balanced routing algorithm which supports mobile wireless sensor network is proposed. The proposed algorithm adopts the trust model that realizes a distributed joint detection model combining the direct trust value with the indirect trust value. Meanwhile, the energy-balanced algorithm based on nodes' residual energy and energy density is introduced to prolong the lifespan of the network. Simulation results show that the routing algorithm is capable of detecting malicious nodes successfully. The consistency check

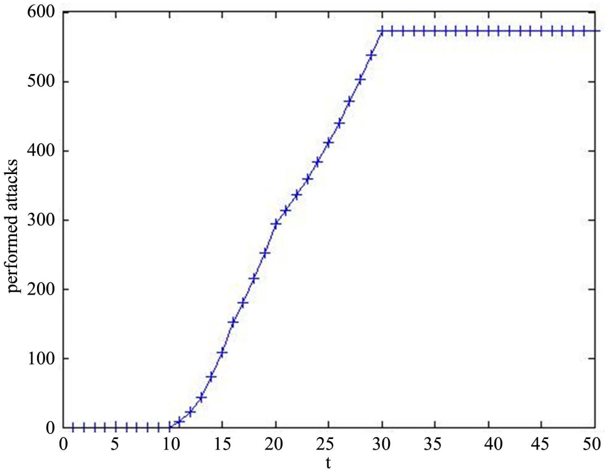

Figure 9. Total numbers of attacks.

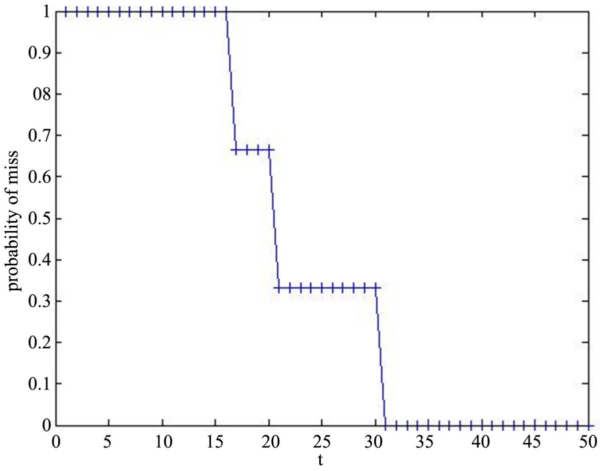

Figure 10. Probability of miss.

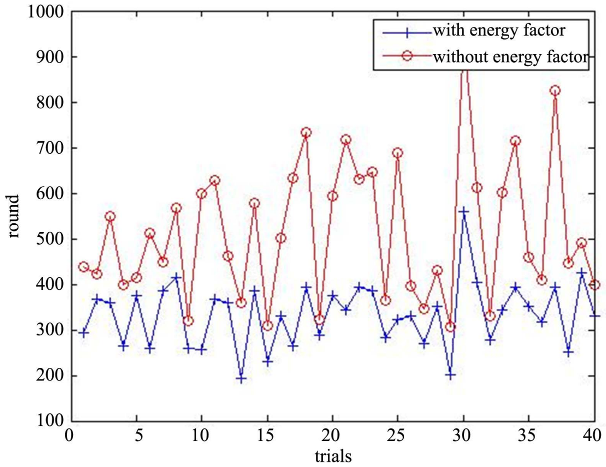

Figure 11. Lifespan of the network.

algorithm of the indirect trust values helps the network to defend against the attacks on the trust model. The algorithm also prolongs the lifespan of the network.

Acknowledgements

The authors wish to acknowledge the anonymous reviewers for their valuable comments and suggestions. We also thank MATLAB Technologies, Inc., for providing us with Wireless Modeler to validate our approaches.

References

[1] Akyildiz, I.F., Melodia, T. and Chowdury, K.R. (2007) Wireless Multimedia Sensor Networks: A Survey. *IEEE Wireless Communications*, **14**, 32-39. http://dx.doi.org/10.1109/MWC.2007.4407225

[2] Deng, J., Han, R. and Mishra, S. (2006) INSENS: Intrusion-Tolerant Routing for Wireless Sensor Networks. *Computer Communications*, **29**, 216-230. http://dx.doi.org/10.1016/j.comcom.2005.05.018

[3] Wood, A.D., Fang, L., Stankovic, J.A., *et al.* (2006) SIGF: A Family of Configurable, Secure Routing Protocols for Wireless Sensor Networks. *Proceedings of the Fourth ACM Workshop on Security of Ad Hoc and Sensor Networks*, Alexandria, 30 October 2006. http://dx.doi.org/10.1145/1180345.1180351

[4] Dong, J., Curtmola, R. and Nita-Rotaru, C. (2011) Secure High-Throughput Multicast Routing in Wireless Mesh Networks. *IEEE Transactions on Mobile Computing*, **10**, 653-668. http://dx.doi.org/10.1109/TMC.2010.194

[5] Hur, J., Lee, Y., Yoon, H., Choi, D. and Jin, S. (2005) Trust Evaluation Model for Wireless Sensor Networks. *Proceedings of Advanced Communication Technology Conference*, *ICACT* 2005, **1**, 491-496.

[6] Ganeriwal, S., Balzano, L.K. and Srivastava, M. (2008) Reputation-Based Framework for High Integrity Sensor Networks. *ACM Transactions on Sensor Networks*, **4**, 3.

[7] Crosby, G., Pissinou, N. and Makki, K. (2006) Location-Aware, Trust-Based Detection and Isolation of Compromised Nodes in Wireless Sensor Networks. *International Journal of Network Security*, **12**, 107-117.

[8] Theodorakopoulos, G. and Baras, J.S. (2006) On Trust Models and Trust Evaluation Metrics for Ad-Hoc Networks. *IEEE Journal on Selected Areas in Communications* (*JSAC*), **24**, 318-328. http://dx.doi.org/10.1109/JSAC.2005.861390

[9] Sun, Y., Yu, W., Han, Z. and Liu, K.J.R. (2006) Information Theoretic Framework of Trust Modeling and Evaluation for Ad Hoc Networks. *IEEE JSAC Special Issue on Security in Wireless Ad Hoc Networks*, **24**, 305-317.

[10] Li, H. and Singhal, M. (2006) A Secure Routing Protocol for Wireless Ad Hoc Networks. *Proceedings of the* 39*th Hawaii International Conference on System Sciences*. http://www.computer.org/csdl/proceedings/hicss/2006/2507/09/250790225a.pdf

[11] Kang, K.D., Liu, K. and Abu-Ghazaleh, N. (2006) Securing Geographic Routing in Wireless Sensor Networks. 9*th Annual NYS Cyber Security Conference*: *Symposium on Information Assurance*, Albany, 14-15 June 2006, 38-49. http://www.albany.edu/iasymposium/proceedings/2006/kang.pdf

[12] Akyildiz, I.F., *et al.* (2002) A Survey on Sensor Networks. *IEEE Communications Magazine*, **40**, 102-114. http://dx.doi.org/10.1109/MCOM.2002.1024422

[13] Lindsey, S. and Raghavendra, C.S. (2002) PEGASIS: Power-Efficient Gathering in Sensor Information Systems. *IEEE Aerospace Conference Proceedings*, **3**, 1125-1130. http://dx.doi.org/10.1109/aero.2002.1035242

[14] Hung, K.S., Lui, K.S. and Kwok, Y.K. (2007) A Trust-Based Geographical Routing Scheme in Sensor Networks. *Proceedings of IEEE Wireless Communications and Networking Conference*, Hongkong, 11-15 March 2007, 3123-3127. http://dx.doi.org/10.1109/wcnc.2007.577

[15] Eghbali, A.N., Javan, N.T. and Dehghan, M. (2007) Load-Balancing Using Multi-Path Directed Diffusion in Wireless Sensor Networks. *Lecture Note on Computer Science*, **4864**, 44-55. http://dx.doi.org/10.1007/978-3-540-77024-4_6

[16] Cicirello, P., Mottola, L. and Picco, G.P. (2007) Efficient Routing from Multiple Sources to Multiple Sinks in Wireless Sensor Networks. *Proceedings of the* 4*th European Conference on Wireless Sensor Networks* (*EWSN* 2007), Delft, 29-31 January 2007, 34-50. http://dx.doi.org/10.1007/978-3-540-69830-2_3

[17] Heinzelman, W., Chandrakasan, A. and Balakrishnan, H. (2000) Energy-Efficient Communication Protocol for Wireless Microsensor Networks. *Proceedings of the* 33*rd Hawaii International Conference on System Sciences* (*HICSS*'00), 4-7 January 2000. http://dx.doi.org/10.1109/hicss.2000.926982

[18] Ren, F.Y., *et al*. (2011) EBRP: Energy-Balanced Routing Protocol for Data Gathering in Wireless Sensor Networks. *IEEE Transactions on Parallel and Distributed Systems*, **22**, 2108-2125. http://dx.doi.org/10.1109/TPDS.2011.40