Sensors & Transducers, Vol. 22, Special Issue, June 2013, pp. 97-103

Sensors & Transducers

http://www.sensorsportal.com

A Reputation-based Mechanism to Stimulate Cooperation in Wireless Sensor Networks

[1, 2] Li Fengyun, [2] Gao Fuxiang, [2] Yao Lan, and [2] Li Peng

[1] Computing Center, Northeastern University, Shenyang 110819, P. R. China
[2] School of Information Science and Engineering, Northeastern University, Shenyang 110819, P. R. China
E-mail: lifengyun@cc.neu.edu.cn, gaofuxiang@ise.neu.edu.cn

Received: 15 April 2013 /Accepted: 20 June 2013 /Published: 28 June 2013

Abstract: In wireless sensor networks, the sensor nodes need to collaborate with each other to transmit packets to the destination. However, some malicious nodes are not cooperative. The paper introduces a new reputation-based mechanism to stimulate nodes to forward packets for other nodes and enforce the security of the networks. All nodes are encouraged to maintain a good reputation so that their packets can be forwarded by other nodes, and a node will be isolated and punished if it acts maliciously. The impact of collisions and interference on nodes' reputation is reduced, and nodes can have chance to restore cooperation after being mistaken for the selfish ones. The low competitive nodes that do not have enough energy to help other nodes can also be treated well. While searching a route to the destination, the factors of reputation, remaining energy and the distance to the destination are taken into consideration. Simulation results show that our strategy can achieve relatively high throughput even when there are malicious nodes in the networks. *Copyright © 2013 IFSA.*

Keywords: Wireless sensor networks, Reputation mechanism, Cooperation, Collision, Security.

1. Introduction

In recent years, as an important part of the Internet of Things, wireless sensor networks (WSN) have gained great attention for its unique characteristics and novel applications. A typical WSN is composed of a large number of power-constrained, tiny sensor nodes [1]. These sensor nodes are deployed in various fields like military, disaster management, industry environmental monitoring, agriculture farming, etc. Because of the power-limited nature of the sensor nodes and the possible hostile application environments in WSN, we have to solve some important problems, including efficient energy management and the security [2].

With the widely applications of WSN, the requirement of security becomes more complexly. Since the wireless sensor networks are often deployed in hostile environments, sensor nodes can easily be captured by the attacker. The traditional security mechanisms which are based on cryptography can only resist external attacks, and are unable to resist the internal nodes which are captured by the attacker [3-5]. Therefore, an effective security mechanism is needed to identify the captured sensor nodes, and take corresponding measures to reduce the losses. As an effective supplement of the cryptography measures, trust management has already become an effective mechanism to protect the security of WSN.

As the sensor nodes have limited resources and the network application is relatively single, the way of using of authentication in trust management is not suitable for WSN. Therefore, the researches on trust management in WSN mainly focus on the sensor node

trust value evaluation methods to enhance the security of the network [6]. During the process of trust evaluation, the incompleteness of information will lead to the deviation of the evaluation results and even mistake a cooperation node for a selfish node. In order to ensure the accuracy of the trust value, the indirect trust evaluation value from its neighbors is often used by a node to fix its own direct trust evaluation value, and this is the basic idea of the reputation based trust mechanism. Reputation mechanism is a kind of effective method in evaluating trust value, and this paper is based on reputation mechanism to evaluate whether a node can be trusted or not.

In WSN, due to the limitation in energy resources and communication range of the sensor nodes, each node is the potential routing node and ought to forward the incoming packets for other nodes [7-8]. However, some misbehavior nodes will not be cooperative, and will not properly execute the operation like routing, forwarding, etc. The misbehavior nodes can be divided into selfish nodes, malicious nodes and low competitive nodes.

Selfish nodes do not cooperate, saving battery life for their own communication, but they do not damage other nodes [9].

Malicious nodes disturb the normal order of the network by dropping incoming packets deliberately, issuing error routing messages in order to misdirect the path [10].

Low competitive nodes cannot provide service for other nodes as their energy is lower.

Some incentive mechanisms have been proposed to detect and isolate the misbehavior nodes and ensure the security of WSN [11-14]. Incentive mechanisms can be divided into credit-based systems and reputation-based systems [15]. In credit-based systems, each time a node acts as a relay and forwards a packet, it will receive payments, and such credit can later be used by this node to encourage other nodes to be cooperative. If a node has no credit to pay, it will be isolated and none of the nodes will help it to forward packets. In reputation-based strategies [16-18], the behavior of a node is measured by other nodes in the network, and the misbehavior nodes will be isolated by the network.

At present, the evaluations of a node's reputation in WSN are mainly from the communication angle. A generally used reputation-based system is the RFSN model which is proposed by Ganeriw and Srivastava, and this system uses the watchdog mechanism to evaluate a node's reputation [19]. The reputation is composed of direct reputation $(R_{ij})_D$ and indirect reputation $(R_{ij})_{ID}$, that is $R_{ij}=(R_{ij})_D+(R_{ij})_{ID}$. In RFSN scheme, the Beta probability function is used to compute the trust value of a node, that is

$$T_{ij} = E(R_{ij}) = E(Beta\{\alpha_{j+1}, \beta_{j+1}\}) = \frac{\alpha_j + 1}{\alpha_j + \beta_j + 1}, \quad (1)$$

where R_{ij} is the reputation of node j which is maintained by node i, α_j and β_j means the communication between node i and node j. TRANS (trust routing for location-aware sensor networks) is a secure mechanism based on the trust mechanism, and can make sure that packets can be transmitted to the destination through a secure route which is composed of trusted nodes [20]. Each sensor node computes the trust value of its neighbor nodes and does not select the lower reputation nodes as its relay nodes.

These reputation-based schemes only consider the factors in communication, and ignore other factors. One problem is that refusing to forward the incoming packets is a normal behavior when the energy of a node is decreased to a certain threshold, and saving energy to transmit its own data later is more important than acting as a relay. But if a node does that, it will be isolated and punished in the traditional reputation systems. Another problem is that it is not always possible to perfectly estimate how a node behaves due to interference and collisions, so sometimes the cooperative nodes may be mistaken for the selfish ones. These situations may cause the cooperative nodes be isolated in error, and the connectivity and throughput of the network decrease accordingly.

In this paper, a reputation-based mechanism is proposed to stimulate cooperation (RBMSC for short) among nodes and punish the non-cooperative behavior. The reputation, remaining energy and the distance to the destination are both taken into consideration in our routing scheme. A relay node can decide whether to help the sending node to forward packets according to the reputation of the sending node, and the reputation depends on the behaviors of the sending node in the previous time slot. In our scheme, a node can have chance to restore its reputation after being perceived as a selfish node falsely, and the low competitive nodes can get help from the other nodes in the networks.

The rest of this paper is organized as follows. Section 2 introduces the network model and our proposed reputation model. Section 3 gives a detailed description of our reputation-based routing algorithm and discusses its performance. Section 4 presents the simulation results of our approach. Finally, we give the conclusions in Section 5.

2. Model Definition

2.1. Network Model

(1) The network is a connected graph and consists of N sensor nodes.

(2) All the sensor nodes including the Sink node are stationary, and each node has unique ID value.

(3) The sensor nodes in the network include cooperative nodes and non-cooperative nodes. The non-cooperative nodes are malicious nodes. These nodes drop the arriving packets deliberately, but do not attack other nodes actively.

(4) All the nodes are rational, and their main target is to maximize their payoff value.

(5) The time is divided into slots, and the nodes can transmit several packets during one time slot.

2.2. Reputation Model

In WSN, as the nodes need to collaborate with each other to transmit data to the destination, the credibility of the nodes is an important measurement for the security of the networks. In our model, each node uses a watchdog mechanism to monitor the behavior of its neighbors, and evaluates their reputation based on the monitoring results. We assume that the misbehavior nodes drop the incoming packets deliberately, but they do not damage other nodes.

In our model, we use the packets forwarding ratio to evaluate the reputation of a node. Each node has a reputation list that stores the reputation of its neighbors. At the end of a time slot, each node computes the packets forwarding ratio of its neighbors that it has observed during this time slot and sends the value to its other neighbors. Here, we suppose node *j* is the sending node, and node *i* is the receiver. We let N_i^k be the set of neighbors that node *i* has discovered in time interval *k*. S_{ij}^k is the number of packets sent to *j* in time slot *k* (*k*≥0), and F_{ij}^k means the number of packets *j* actually forwarded in time slot *k*. At the ends of the time slot *k*, node *i* computes the packet forwarding ratio [21].

$$(p_{ij})_D^k = \frac{F_{ij}^k}{S_{ij}^k} \tag{2}$$

and proceeds to send this value to its neighbors. With the values gathered from all the neighbors, node *i* computes the average indirect packet forwarding ratio

$$(p_{ij})_{ID}^k = \frac{\sum_{m \in N_i^k, m \neq j} (p_{im})_D^k \times (p_{mj})_D^k}{\sum_{m \in N_i^k, m \neq j} (p_{im})_D^k} \tag{3}$$

In Eq. (3), $(p_{mj})_D^k$ is the packet forwarding ratio of node *j* that is perceived by node *m*, and the average value is weighted with the perceived packet forwarding ratio that node *i* measured from node *m*. Using this method, even if a node spreads a false value to improve a selfish node's reputation, it will have a small impact on the average since the other nodes give low value. This method can help to avoid Sybil attacks.

Using the direct observation value $(p_{ij})_D^k$ and the indirect observation value $(p_{ij})_{ID}^k$, the forwarding ratio of node *j* at time slot *k* can be computed as

$$p_j^k = \alpha (p_{ij})_D^k + \beta (p_{ij})_{ID}^k \tag{4}$$

where $\alpha, \beta \in [0,1]$, $\alpha + \beta = 1$. It must be stressed that if there is no incoming packet arriving at node *j* during time interval *k*, node *i* will not execute the above computation, and just using the previous transmitting history to evaluate the reputation of node *j*, that is $p_j^k = p_j^{k-1}$.

In WSN, due to collisions and interference, it is not always possible to detect whether a node forwards a packet or not. Meanwhile, it is hard to measure the probability that a packet has been forwarded but is not overheard by its neighbors. In order to stimulate cooperation, we adopt a strategy that can efficiently punish the non-cooperative nodes, and the nodes that have made a mistake unintentionally can get back in good standing by cooperation in the next stage. Based on the packets forwarding ratio of node *j* which is computed by node *i* at the end of time slot *k*−1, the reputation of node *j* at time slot *k* can be expressed as

$$R_j^k = \begin{cases} f(p_j^{k-1} - p_{j,RBMSC}^{k-1}), & k \geq 0 \\ 0, & k = -1 \end{cases}, \tag{5}$$

where p_j^{k-1} is the average packet forwarding ratio of node *j* which is perceived by its neighbors, $p_{j,RBMSC}^{k-1}$ is the packet forwarding ratio under RBMSC. If $p_j^{k-1} > p_{j,RBMSC}^{k-1}$, it means node *j* is perceived to forwarding more packets than it should under RBSMC, the reputation value of node *j* will be above zero. Here, we define the function

$$f(x) = \begin{cases} 1, & x \geq 1 \\ x, & 0 < x < 1 \\ 0, & x \leq 0 \end{cases} \tag{6}$$

To reduce the impact of collisions and interference on the reputation of a node, the receiving node *i* compares its reputation with that of the sending node *j*, and will punish the sending node if its reputation is higher than the sending node. The punishment can be expressed as

$$q_{i,RBMSC}^k = f(R_i^k - R_j^k), \quad k \geq 0, \tag{7}$$

where $q_{i,RBMSC}^k$ is the dropping probability of node *i* to the incoming packets from node *j*. That is to say, node *i* can punish node *j* if it has higher reputation than node *j* at the time interval *k*. Then, under our proposed approach RBMSC, aiming at the incoming packets that are from node *j*, node *i* should adopt the packet forwarding ratio

$$p_{i,RBMSC}^k = 1 - q_{i,RBMSC}^k, \quad k \geq 0 \tag{8}$$

3. The Reputation-based Secure Routing Algorithm

3.1. Algorithm Description

While searching a route to the destination, each hop is a game between a sending node and a relay

node. When a routing request message is arriving, a node can decide whether to drop or forward packets for the sending node according to its residual energy and the reputation of the sending node. The sending node can select the suitable node as its next hop relay according to its payoff value. The pseudo code description of the relay node selection process can be seen in algorithm 1, and the detailed steps of the reputation-based routing algorithm are as follows:

Step 1: A sensor node *j* has packets to send at time slot *k*. It will send packets to the destination directly if the destination is within its communication range (Line 1-7). Otherwise, the sending node sends a route request message to its neighbors (Line 8).

Algorithm 1: The reputation-based secure routing

j-the sending node *i*-the receiving node

BEGIN
1: //node *j* has data to be transmitted at time slot *k*
2: compute d_{sink}
3: if(d_{sink}<*R*) then
4: {
5: senddata(*sink*, *j*)
6: return
7: }//endif
8: broadcast*(req)*
9: //node *i* receive route request message from node *j*
10: if(*i* has a route to sink) then
11: { ack(*route*, *j*)
12: senddata(*route*, *j*)
13: return
14: }
15: else
16: {
17: if($E_{rem,i} \geq E_{th}$) then
18: {
19: if($E_{rem,j}$<E_{th}) then
20: ack(*j*)
21: else{
22: compute $u_i(k)$
23: if($u_i(k) \geq 0$) then
24: { compute $p^k_{i,RBMSC}$
25: send ack(*j*) with probability $p^k_{i,RBMSC}$
26: } //endif
27: } //endif
28: } //endif
29: } //endif
30: //node *j* receive some ack message
31: compute $u_j(k)$ aiming at each ack
32: *i*=max($u_j(k)$)
33: reply(*i*)
34: //node *i* receive ack message from node *j*
35: act as a sender and execute line 6-31
END

Step 2: Some nodes receive the route request message. If a receiving node *i* is the destination or it has a route to the destination, it will send a reply message including the full source route in reverse order, and go to Step 5 (Line 9-11). Otherwise, node *i* will drop the route request message if its remaining energy E_{rem} is below a given threshold E_{th}, as it is important to save energy than to gain reputation. If $E_{rem} \geq E_{th}$, the node predicts the sending node's remaining energy based on the communication history of the sending node, and will send an ACK message to the sending node when the sending node's energy is lower than E_{th}. Since it may be the aiming of saving energy for data collecting that caused the sending node to drop packets in the previous slot, and we should not isolate it for the connectivity of the network. Except for these situations, node *i* will evaluate the reputation of the sending node from the communication angle. Firstly, node *i* computes its payoff value $u_i(k)$, and will not refuse to forward packets for the sending node if the value is below zero. If $u_i(k) \geq 0$, node *i* computes the packet forwarding ratio $p^k_{i,RBMSC}$ that it should adopt, and sends an ACK message to the sending node with the probability of $p^k_{i,RBMSC}$ (Line 15-29).

Step 3: After a while, the sending node receives some ACK messages. For each ACK message, the sending node computes its payoff value. Then, the sending node selects the node that can maximize its payoff value as its next hop relay, and sends a reply message to the relay node (Line 30-33).

Step 4: When the reply message arrives at the relay node, a new game between the relay and its next hop is begun. In the new game, the relay acts as a sending node, and it will find a suitable node as its next hop. The new sending node puts its node ID into the source route and forwards the route request message to its neighbors. Then, go to Step 2 (Line 34-35).

Step 5: When the reply message arrives at the original sending node, a routing path is picked out, and the sending node can send packets along this path (Line 12-13).

3.2. The Payoff

In WSN, all the sensor nodes want to maximize their own payoff. Therefore, the routing selection process can be taken as the game between sending nodes and relay nodes. Here, we assume that node *j* is the sending node and node *i* is the receiver. Each node is a rational user and wants to maximize its own payoff. The payoff function of each node is the sum of the virtual utility value and physical utility value. Therefore, when it acts as a relay at time slot *k*, the payoff of the node *i* can be expressed as

$$u_i(k) = \varsigma u_{v,i}(k) + \eta u_{c,i}(k), \quad (9)$$

where $u_{v,i}(k)$ is the virtual utility of node *i* and $u_{c,i}(k)$ is the physical utility, ς and η are the weight parameters, and $\varsigma + \eta = 1$.

Here, the reward that a relay node receives is equal to the reputation of the sending node, which means if a relay node helps a higher reputation node it will get

more virtual utility $u_{v,i}(k)$. As forwarding a packet consumes energy, we define the physical utility of a relay node $u_{c,i}(k)$ to be in proportion to the energy consumption of transmitting a packet. To facilitate the calculation, we use the maximum energy consumption of transmitting a packet, which is E_{maxc}. Then, according to the radio energy dissipation model, the value of E_{maxc} can be compute by Eq. (10).

$$E_{maxc}(l,d) = \begin{cases} lE_{elec} + l\varepsilon_{fs}R^2 & R < d_0 \\ lE_{elec} + l\varepsilon_{amp}R^4 & R \geq d_0 \end{cases} \quad (10)$$

Thus, if node i forwards packets for node j at time slot k, its payoff function can be express as

$$u_i(k) = \varsigma R_j^k - \frac{1000\eta E_{maxc}}{e}, \quad (11)$$

where R_j^k is the reputation of node j that is computed by node i, and the value of e is 1J. As the value of E_{maxc} is very small, for example, when the length of the packet is 4000 bit and the communication radius is 50 m, by computing Eq. (10), the value of E_{maxc} is equal to 0.0003J. Therefore, we set 1000 as the accommodation coefficient so as to balance the ratio of physical utility value and virtual utility value.

To enhance the energy efficiency and security of the networks, the payoff function of the sending node j is defined as

$$u_j(k) = \varsigma R_i^k - \frac{1000\eta E_{dest,i}E_{tot}}{eE_{rem,i}}, \quad (12)$$

where R_i^k is the reputation of node i which is evaluated by node j, $E_{dest,i}$ is the evaluation of the energy cost of node i if it sends a packet to the destination directly. E_{tot} is the initial energy of a node, and $E_{rem,i}$ represents the remaining energy of node i. Using Eq. (12), we can make sure that the node which has relatively high reputation, more remaining energy and is close to the destination will be selected as the next hop of node j.

3.3. Performance Analysis

In our proposed reputation-based model, we can see from Eqs. (7) and Eqs. (8), the packet forwarding ratio $p_{i,RBMSC}^k$ that node i adopts in time slot k is consistent with the reputation of node j, that is R_j^k. We can also conclude from Eqs. (5) and Eqs. (6) that the reputation of node j is decided by its packets forwarding ratio in time slot $k-1$, that is p_j^{k-1}. Therefore, when node i receives a packet from node j at time slot k, the packet forwarding ratio $p_{i,RBMSC}^k$ is decided by the forwarding behavior of node j during time slot $k-1$. In other words, if node j behaves well, its packets will be treated well in the next time slot. Otherwise, if node j does not follow the packet forwarding ratio $p_{i,RBMSC}^k$ that it should adopt in time slot $k-1$, it will be punished and no node will help it to forward packets. According to the sending node's payoff function (Eqs. (12)), the lower reputation node will also not be selected as the relay node.

Since no node can have more gain if it does not follow our proposed scheme, as a rational node, each node will be cooperative and forward packets for its neighbors with higher probability. So we can conclude that no node can gain by deviating from the expected behavior in RBMSC. When both nodes use RBMSC, the full cooperation is achieved, that is $p_i^k = p_j^k = 1$, for all $k \geq 0$.

Under our strategy, the nodes that drop the packets deliberately will be isolated and punished. This can resist some attacks such as selective forwarding attacks. In the meanwhile, it can avoid Sybil attacks since the average value in Eq. (3) is weighted with the perceived packet forwarding ratio of node i measured from node m. Therefore, our strategy can enforce the security of the networks.

4. Simulation

In order to evaluate the performance of the proposed scheme, we deploy a network of 100 sensor nodes in an area of 100×100 meters target field. The simulation is implemented on OMNeT++ [22]. All nodes are scattered over the area randomly, and each node has the same maximum energy at the beginning. Two sensors are able to communicate with each other if they are within the transmission range. The sensor nodes perform a measurement task and periodically report to the sink node. The communication radius of a sensor node is set to be 50 meters, and within this distance the energy cost follows the free space propagation mode [23].

Fig. 1 indicates the average throughput of the networks in two cases, no malicious node and twenty percent of malicious nodes in the networks.

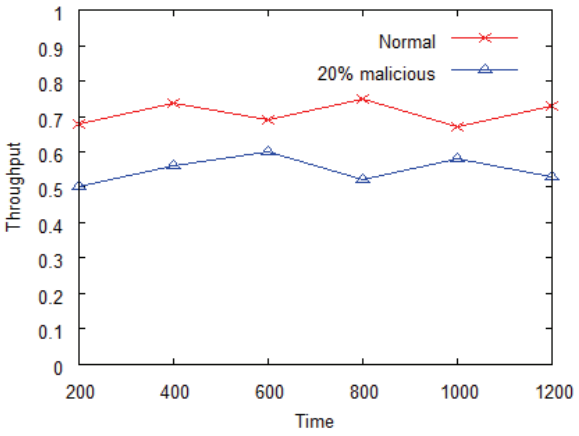

Fig. 1. Throughput vs. time.

We can see from Fig. 1 that when there are malicious nodes in the networks, the average

throughput is just a little less than that when all the nodes acts normally. The throughput keeps steady even when there are malicious nodes in the networks. The reasons behind that are no node will select the bad reputation nodes as its next hop relay, and the malicious nodes will forward other nodes' packets actively in the next time slot to restore its reputation if they are punished during one time slot.

Fig. 2 compares our strategy with two strategies in terms of throughput versus times, one is the RFSN scheme and the other one is the repeated game scheme proposed by Ref. [17].

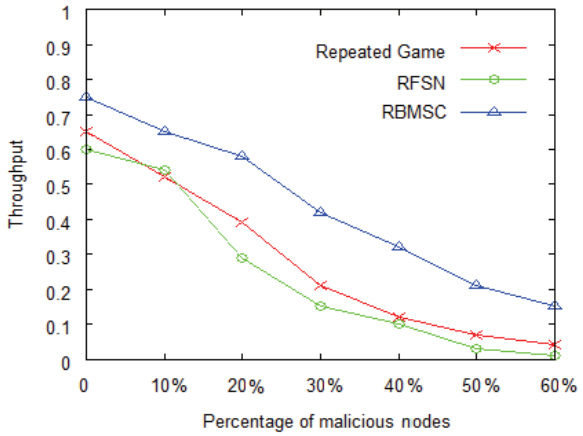

Fig. 2. Throughput vs. number of malicious nodes.

The simulation results in Fig. 2 show that the throughputs of all three approaches are decreased while more malicious nodes are introduced in the network. Our strategy RBMSC has better performance than the other two strategies. In repeated game, the intrusion detection system (IDS) evaluates the reputation of a node based on the history of all games. Therefore, if a node is mistaken for a misbehavior one in one game, this will affect it all the time, and it may be isolated forever. In RFSN model, the Beta probability function is used to predict the packet forwarding ratio of a node. The reason of lower throughput in RFSN is that it only considers the communication factor, so it may mistake a cooperative node or a low competitive node for a misbehavior node and punish the node, this will cause the decrease in throughput. In RBMSC, the collisions and interference that caused by the communication environments are considered, and the low competitive nodes can be treated well, so the throughput is higher than that of other strategies even in hostile environments.

In the third group of experiment, the percentage of malicious nodes is set to 10 %, and the number of the sensor nodes that sending data simultaneously is varying from 10 to 30. From Fig. 3 we can see that when there are more sensor nodes that sending data simultaneously in the network, the throughput of the network will be decreased due to the collision of the packet. However, our proposed scheme has relatively high anti-interference ability when compared to other schemes.

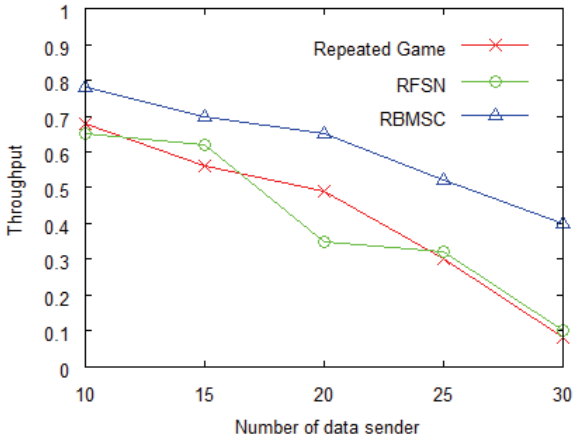

Fig. 3. Throughput vs. number of data sender.

Based on the above simulation results, we can conclude that our proposed reputation-based secure routing scheme has strong fault-tolerant ability in resisting packet collisions and environmental interference. Our scheme can stimulate "rational" selfish nodes to be cooperative so as they can gain good reputation. The low competitive nodes can get help from other nodes. The "irrational" selfish nodes will be excluded from the routing path, and will not affect the performance of the network.

6. Conclusions

In this paper, we propose a new reputation-based mechanism called RBMSC. In this approach, all nodes share the perceived packet forwarding ratio with its neighbors. The low competitive nodes can get help from other nodes. The impact of collisions and interference to the reputation of the nodes is reduced. The nodes that made a mistake unintentionally can get a chance to restore cooperation. The malicious nodes that do not follow RBMSC will be isolated and punished. Our approach can achieve full cooperation as no node can gain if it deviates from the expected behavior. Moreover, the simulation results show that RBMSC can achieve a higher throughput than the other strategies.

Acknowledgements

This work was supported by the National Natural Science Foundation of China under Grant No. 60903159.

References

[1]. J. Yick, B. Mukherjee, and D. Ghosal, Wireless sensor network survey, *Computer Networks*, Vol. 52, Issue 2, 2008, pp. 2292-2230.

[2]. I. F. Akyildiz, W. L. Su, A survey on sensor networks, *IEEE Communications Magazine*, Vol. 40, Issue 8, 2002, pp. 102-114.

[3]. M. Pugliese, F. Santucci, Pair-wise network topology authenticated hybrid cryptographic keys for wireless sensor networks using vector algebra, in *Proceedings of the 5th IEEE International Conference on Mobile Ad Hoc and Sensor Systems',* Atlanta, GA, 2008, pp. 853-859.

[4]. J. Deng, Y. S. Han, Multipath key establishment for wireless sensor networks using just-enough redundancy transmission, *IEEE Transactions on Dependable and Secure Computing*, Vol. 5, Issue 3, 2008, pp. 177-190.

[5]. S. A. Camtepe, B. Yener, Combinatorial design of key distribution mechanisms for wireless sensor networks, *IEEE/ACM Transactions on Networking*, Vol. 15, Issue 2, 2007, pp. 346-358.

[6]. Y. Yu, K. Li, W. Zhou, P. Li, Trust mechanisms in wireless sensor networks: Attack analysis and countermeasures, *Journal of Network and Computer Applications*, Vol. 35, 2012, pp. 867-880.

[7]. B. Tavli, M. B. Akgun, and K. Bicakci, Impact of limiting number of links on the lifetime of wireless sensor networks, *IEEE Communications Letters*, Vol. 15, Issue 1, 2011, pp. 43-45.

[8]. Y. Y. Xu, Efficient and secure routing protocol for wireless sensor networks through optimal power control and optimal handoff-based recovery mechanism, *Computer Networks and Communications*, 2012, pp. 1-8.

[9]. A. Agah and S. K. Das, Preventing dos attacks in wireless sensor networks: A repeated game theory approach, *International Journal of Network Security*, Vol. 5, Issue 2, 2007, pp. 145-153.

[10]. H. Hu, Y. Chen, W. S. Ku, Z. Su, and C. H. Chen, Weighted trust evaluation-based malicious node detection for wireless sensor networks, *International Journal of Information and Computer Security,* Vol. 3, Issue 2, 2009, pp. 132-149.

[11]. J. Lopez, R. Roman, I. Agudo, and C. F. Gagoa, Trust management systems for wireless sensor networks: Best practice, *Computer Communication*s, Vol. 33, Issue 9, 2010, pp. 1086-1093.

[12]. R. Kannan and S. S. Iyengar, Game-theoretic models for reliable, path-length and energy-constrained routing in wireless sensor network, *IEEE Journal of Selected Areas in Communications*, Vol. 22, 2004, pp. 1141-1150.

[13]. L. Buttyan and J. Hubaux, Stimulating cooperation in self-organizing mobile ad hoc networks, *Mobile Networks and Applications*, Vol. 8, Issue 5, 2003, pp. 579-592.

[14]. F. Y. Li, G. R. Chang, F. X. Gao, L. Yao, Cooperative game-based routing approach for wireless sensor network, *International Journal of Computer Applications in Technology*, Vol. 44, No. 2, 2012, pp. 101-108.

[15]. F. Y. Li, G. R. Chang, F. X. Gao, L. Yao, A novel cooperation mechanism to enforce security in wireless sensor networks, in *Proceedings of the 5th International Conference on Genetic and Evolutionary Computing*, Kinmen Taiwan/Xiamen, China, 2011, pp. 341-344.

[16]. X. Wang, L. Ding, and S. Wang, Trust evaluation sensing for wireless sensor networks, *IEEE Transactions on Instrumentation and Measurement*, Vol. 60, Issue 6, 2011, pp. 2088-2095.

[17]. A. Agah, K. Basu, and S. K. Das, Security enforcement in wireless sensor networks: A framework based on non-cooperative games, *Pervasive and Mobile Computing Journal on Security in Wireless Mobile computing systems (PMC)*, Issue 2, 2006, pp. 137-158.

[18]. S. Ozdemir, Functional reputation based reliable data aggregation and transmission for wireless sensor networks, *Computer Communications*, Vol. 31, Issue 7, 2008, pp. 3941–3953.

[19]. S. Ganeriwal, L. K. Balzano, and M. B. Srivastava, Reputation-based framework for high integrity sensor networks, *ACM Transactions on Sensor Networks*, Vol. 4, Issue 3, 2008, pp. 1-37.

[20]. S. Tanachaiwiwat, P. Dave, R. Bhindwale, A. Helmy, Location-centric isolation of misbehavior and trust routing in energy-constrained sensor networks, in *Proceedings of IEEE Workshop on Energy-Efficient Wireless Communications and Networks*, Phoenix, 2004, pp. 463-469.

[21]. J. J. Jaramillo and R. Srikant, A game theory based reputation mechanism to incentivize cooperation in wireless ad hoc networks, *Ad Hoc Networks*, Vol. 8, Issue 4, 2010, pp. 416-429.

[22]. A. Varga and Hornig, An overview of the OMNeT++ simulation environment, in *Proceedings of the 1st International Conference on Simulation Tools and Techniques for Communications, Networks and Systems*, Marseille, France, 2008, pp. 1-10.

[23]. W. Heinzelman, A. Chandrakasan, and H. Balakrishnan, An aplication-specific protocol architecture for wireless microsensor networks, *IEEE Transactions on Wireless Communications*, Vol. 1, Issue 4, 2002, pp. 660-670.
