Advanced Engineering Forum
ISSN: 2234-991X, Vols. 2-3, pp 599-603
doi:10.4028/www.scientific.net/AEF.2-3.599
© 2012 The Author(s). Published by Trans Tech Publications Ltd, Switzerland.

Online: 2011-12-22

A Game Theory based Approach for Routing in Wireless Sensor Networks

Fengyun Li[1,2,a], Fuxiang Gao[2,b], Lan Yao[2,c], Guiran Chang[1,d]

[1] Computing Center, Northeastern University, Shenyang 110819, China

[2] School of Information Science and Engineering, Northeastern University, Shenyang 110819, China

[a]lifengyun@cc.neu.edu.cn, [b]gaofuxiang@ise.neu.edu.cn, [c]yaolan@ise.neu.edu.cn, [d]chang@neu.edu.cn

Keywords: Game theory, Reputation, Routing, Wireless Sensor Networks

Abstract. Aiming at the limited resources and the security issues in wireless sensor networks, a routing approach is proposed. In this approach, the factors of reputation, remaining energy, and the distance to the destination are taken into considered while searching a routing path from an original sender node to the destination. A reputation-based mechanism is also proposed, and a node's reputation depends on its behaviors. The malicious behaviors nodes will be punished and isolated, and the cooperative ones will be rewarded. Simulation results show that our proposed routing scheme can prolong the lifetime of the network and can offers a relatively high throughput than other routing protocols even when there are malicious nodes in the networks.

Introduction

Wireless sensor networks (WSN) are gaining increasingly impact in our day to day lives. They are finding a wide range of applications in various domains, including military, health-care, assisted and enhanced-living scenarios, industrial and production monitoring, control networks, and many other fields [1]. In future, WSN are expected to be integrated into the "Internet of Things", where sensor nodes join the Internet dynamically, and use it to collaborate and accomplish their tasks.

A typical WSN are composed of small, low-cost, resource-limited (battery, CPU, memory, bandwidth) nodes that communicate wirelessly and cooperate to forward data in a multi-hop fashion. Thus, they are especially attractive in scenarios where it is infeasible or expensive to deploy a significant networking infrastructure [2]. However, due to the open nature of the wireless communication, the lack of infrastructure, and the hostile deployment environments, WSN are vulnerable to many types of attacks such as Sybil attacks, Wormhole attacks, Sinkhole attacks, Denial of Service (DoS) attacks, and Selective forwarding attacks et al. One of the most dangerous attacks is Selective forwarding attacks, in which malicious nodes drop the packets transferring through them randomly and the packets may include sensitive data. Together with these security problems, WSN are subject to unique challenges for efficient power management to prolong network lifetime [3].

In WSN, the sensor nodes need to collaborate with each other in order to transfer data packets to the destination, and each node is the potential routing node. As the malicious node may drop the packets deliberately, how to find a secure, energy-efficient routing becomes an important issue to be solved. Game theory has been applied in WSN to solve the problems of energy efficiency and security [4]. Game theory is a discipline aims at modeling the situations in which decision makers have to make specific actions that have mutual conflicting or consequences. A reliable query routing scheme has been proposed in [5], the sensors are modeled as rational and intelligent agents cooperate to find optimal network architectures that maximize their payoffs in a sensor game. Two economics approaches were proposed to resist DoS attacks, they are secure auction based routing (SAR) and non cooperative non zero-sum two-player game [6]. In the SAR protocol, nodes must compete against each other in order to participate in forwarding incoming packets and gaining reputation in the networks. The competition is based on auction theory. Some reputation-based mechanisms have been proposed to detect and isolate the misbehavior nodes and ensure the security of WSN [7, 8, 9]. A new framework to detect malicious nodes was proposed using Zero-Sum game approach and selective node acknowledgements in the forward data path [10]. However, the existing routing protocols could not get a well balance between the above issues of energy efficiency and security.

In this paper, we propose a new reputation-based game model for routing in WSN. The nodes' reputation, remaining energy and the distance to the destination are both taken into considered while searching a routing path to the destination. A node will be punished if it drops the incoming packets deliberately, and its reputation will be decreased exponentially. The nodes will low reputation will be isolated by all the other nodes, and only the nodes with relatively high reputation, more energy, and is nearer to the destination will be selected as one hop in a routing path.

The rest of the paper is organized as follows. Section 2 gives a detail description of our proposed routing protocol. Simulation results are presented and analyzed in section 3. Finally, conclusions of our work are drawn in section 4.

Our Proposed Model

Protocol Description. In our model, while searching a routing path from an original sender to the destination, each hop of the routing path is supposed to be a game between a sender and its next hop relay node. Out of the selfish nature, each of the two players will try to maximize its own payoff function. The payoff function of a sender node is related to its opponent's reputation, remaining energy and the distance between its opponent and the destination. The relay's payoff function is in proportion to the sender's reputation. Based on the payoff function, the sender will select the nodes that can maximize its payoff from all the potential relay nodes, and the relay will help the sender that are with higher reputation to forward packets if it has enough energy to forwarding packets. Each node uses a watchdog mechanism to monitor the behaviors of its neighbors, and based on the monitoring results to evaluate the reputation of its neighbors [11]. The reputation manifests the reliability of a node. Using this mechanism, the sender with higher reputation can get help from other nodes, so each of the nodes will have to help other nodes to forward packets in order to maintain a good reputation. The detail steps of our routing protocol are listed as follows:

Step 1, a sensor node has packets to send. If the destination is within its communication range, the sender will send packets to the destination directly with out executing the following route selection procedures. Otherwise, the sender sends a ROUTE REQUEST message to its neighbors.

Step 2, some nodes receives the ROUTE REQUEST message. If a node is the destination or has a route to the destination, go to Step 5. Otherwise, each node that receives the message will first check its remaining energy E_{rem}. If $E_{rem}<E_c$, the node will not forward the packet, as it is important to save energy than to gain reputation. Here, E_c represents the maximum cost of energy while forwarding a packet. If $E_{rem}\geqslant E_c$, the node will calculate its payoff value in the following. If the value is above zero, the node will send an ACK message to the sender, which means it is willing to act as a relay and will forward packets for the sender.

Step 3, after a while, the sender receives some ACK messages. Aiming at each ACK message, the sender computes its payoff value. Then, the sender selects the node that can maximize its payoff value as its next hop relay, and send a REPLY message to the relay node.

Step 4, when the REPLY message arrives at the relay node, a new game between the relay and its next hop is began. In the new game, the relay acts as a sender, and it will find a suitable node as its next hop. Firstly, the new sender puts its node ID into the source route and forwards the ROUTE REQUEST message to its neighbors. Then, go to Step 2.

Step 5, if a receiving node is the destination or has a route to the destination, it will not forward the packets, but sends a REPLY message including the full source route in reverse order.

Step 6, when the message arrives at the original sender, a routing path is picked out, and the sender could sender packets along this path.

The Reputation. Since there may be malicious nodes in the networks, and these nodes will drop the incoming packets deliberately, we adopt a reputation-based mechanism to resist the Selective forwarding attack and enforce the security of WSN. Each node has a reputation list, which stores the reputation of its neighbors [12]. In our model, the reputation represents how cooperative a node is, the reputation value of a node ranges from [0, 1], and the original reputation value is defined to be 1. Here, we define $(R_{ij})_D$ as the reputation of node j which is directly recognized by node i. If node i detects a packet is dropped deliberately by node j, it will update the reputation of node j as in (1), and then broadcasts the latest reputation value of node j to its neighbors.

$$(Rij)_D = \left\lceil \frac{(Rij)_D}{2} \right\rceil \tag{1}$$

If node j takes part in the packet forwarding actively, it will be rewarded, and its reputation will be increased as in (2).

$$(Rij)_D = (Rij)_D + 0.1 \tag{2}$$

From (1) and (2), we can see that the reputation of a node loses easily and gains hard in our mechanism. As the bad reputation node will be isolated, a rational node will not take risk to destroy its reputation.

To reduce the energy consumption of the networks, we let a node broadcast the reputation value of another node only when it detects the node's behaviors of dropping packets deliberately. Moreover, due to the collisions and interference, the direct observation value $(R_{ij})_D$ may not be precise. Thus, node i calculates the indirect observation value based on all the collected reputation information. We define $(R_{ij})_{ID}$ as the indirect observation value, $(R_{ij})_{ID}$ can be computed as

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

Here, N_i represents the set of node i's neighbors. From (3), we can see that node i gives more reliance to the information received from highly reputed node. This can increase the preciseness of the value of $(R_{ij})_{ID}$.

Using the direct observation value $(R_{ij})_D$ and indirect observation value $(R_{ij})_{ID}$, the reputation of node j at node i can be computed as

$$R_{ij} = \alpha (R_{ij})_D + \beta (R_{ij})_{ID}, \ (\alpha, \beta \in [0,1], \alpha + \beta = 1) \tag{4}$$

Then, using the reputation value R_{ij}, node i can calculate its payoff value when it receives a packet from node j. Based on the payoff value, node i will decide whether or not to forward this packet.

The Payoff. The payoff function of each node is the sum of its virtual utility and physical utility. We suppose node i receives a ROUTE REQUEST from node j. Then, a new game between node i and node j is started. In this game, node i acts as a receiver, and node j is the sender. The payoff of the receiver node i can be expressed as

$$U_i = \zeta R_{ij} - \eta E_c, \ (\zeta, \eta \in [0,1], \zeta + \eta = 1) \tag{5}$$

In (5), R_{ij} is the reputation of node j, and E_c is the maximum energy cost of forwarding a packet. As the value E_c is a constant, the value U_i is in proportion to the sender's reputation. When $U_i>0$, node i will send a ACK message to node j.

To enforce the security, energy efficiency and balance of the networks, the payoff function of the sender j is defined as

$$U_j = \zeta R_{ji} - \eta E_{dest} E_{tot}/E_{rem}, \ (\zeta, \eta \in [0,1], \zeta + \eta = 1) \tag{6}$$

where R_{ji} is the reputation of node i which is recognized by node j, E_{dest} is the evaluation of node i's energy cost when it sends a packet to the destination directly. E_{tot} is the initial energy of a node, and E_{rem} represents the remaining energy of node i. Using (6), we can make sure that the node has relatively higher reputation, more remaining energy and is nearer to the destination will be selected as the next hop of node j.

Performance Analysis. In our proposed routing mechanism, all nodes in each hop of a routing path can make decision according to their payoff values, and this is in accord with their selfish nature. Meanwhile, the reputation-based mechanism can make the malicious nodes be punished and isolated, and can enforce the security of the networks. Moreover, at each hop of a routing path, the sender selects the node that has relatively higher reputation, more energy and is nearer to the destination node as its next hop relay according to its payoff value. At last, by using the backward induction method, the distance from the original sender to the destination node will be the shorter one. Then, it will cost less energy of the sensor networks than the other path while sending packets through the routing path, and the problem of energy cost unbalanced can also be solved, so our proposed scheme is an energy-efficient routing algorithm and this is very important in wireless sensor network.

Simulation

In this paper, the simulation is implemented on OMNet++. One hundred of sensor nodes are scattered in an area of 100m × 100m, and each battery has the same initial energy in the beginning, the initial energy E_{tot} is set to be 1J. Two sensor nodes are able to communicate with each other if they are within the transmission range. In order to evaluate the performance of our algorithm, we use a simple radio model for radio energy consumption, where the transmitter consumes energy for radio electronics and power amplifier, and the receiver consumes energy for radio electronics [13]. In this paper, we set the communication radius of a sensor node to 50m, and within this distance the energy cost follows the free space propagation mode. In this mode, the energy cost of a sensor node when transmitting a message with l-bit over a distance d is:

$$E_{Tx}(l,d) = E_{Tx-elec}(l) + E_{Tx-amp}(l,d) = lE_{elec} + l\varepsilon_{fs}d^2 \tag{7}$$

And the formula for receiving an l-bit message is:

$$E_{Rx}(l) = E_{Tx-elec}(l) + E_{Tx-amp}(l,d) = lE_{elec} \tag{8}$$

Fig. 1 shows compares our proposed game theory based routing approach (GBRA for short) with LEACH protocol in the numbers of existing nodes of the networks versus time. In this experiment, we suppose there is no malicious node in the network. The results show that our proposed scheme can prolong the lifetime of the networks when compares with LEACH protocol. In LEACH protocol, each node is selected as cluster head with equal probability, and it doesn't consider the node's remaining energy and distance to the destination while selecting the cluster heads. This cause some nodes waste more energy and will die earlier. In our proposed scheme, the two factors are taken into consideration, the energy cost of all nodes can get well balanced and the lifetime of the networks are prolonged accordingly.

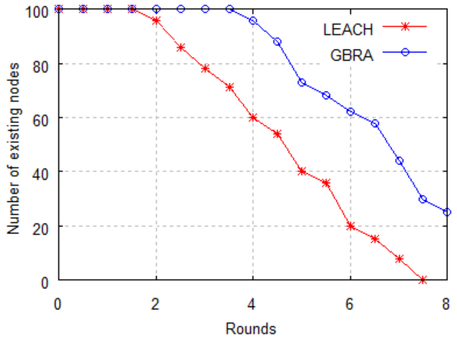

Fig. 1. The lifetime of the networks

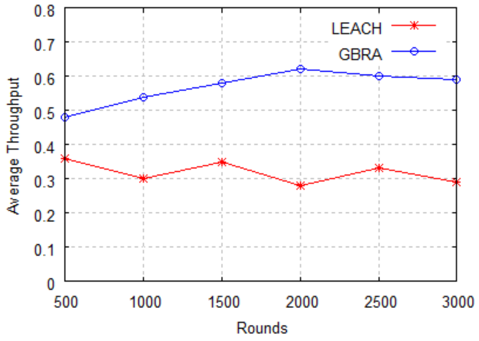

Fig. 2. The throughput versus time, 20% are malicious

Fig. 2 compares our routing scheme with LEACH protocol in terms of throughput versus times. Here, we set twenty percent of malicious nodes in the network, and the bad behaviors of a malicious node are only dropping packets deliberately. The results show that our scheme can get higher throughput than LEACH protocol even in hostile environments. The reason for that is our reputation mechanism can make the malicious nodes be punished and isolated by the other normal nodes, and the affection of the malicious nodes to the network throughput is reduced accordingly.

Summary

In this paper, we proposed a new routing approach to enforce the security of the network, and prolong its lifetime. In this approach, each node makes decision referring to the value of its payoff function. The payoff function of a sender node is designed to be associated with its opponent's reputation, remaining energy, and the distance to the destination. Only the node with higher reputation can get help from other nodes. In our reputation-based evaluation model, a node's reputation declines exponentially and increases linearly. If a node makes a mistake at time t, it must make more effort to restore its reputation. The bad reputation node will be isolated by the other nodes, so a rational node will not take risk to destroy its good reputation. Simulation results show that our routing approach can prolong the lifetime of the networks and can achieve a higher throughput even when there are malicious nodes in the networks.

References

[1] D. Christin, A. Reinhardt, P. Mogre and R. Steinmetz, Wireless sensor networks and the internet of things: selected challenges, Proceedings of the 8th GI/ITG KuVS Fachgespräch “Drahtlose Sensornetze”. (2009) 31-33.

[2] J. Yick, B. Mukherjee, and D. Ghosal, Wireless sensor network survey, Computer Networks. 52 (2008) 2292–2330.

[3] R. Machado, S. Tekinay, A survey of game-theoretic approaches in wireless sensor networks, Computer Networks. 52 (2008) 3047–3061.

[4] P. Trakadas, T. Zahariadis, H. C. Leligou, S. Voliotis, and K. Papadopoulos, AWISSENET: Setting up a Secure Wireless Sensor Network, 50th International Symposium ELMAR-2008. (2008) 519–523.

[5] R. Kannan, S.S. Iyengar, Game-theoretic models for reliable path length and energy-constrained routing with data aggregation in wireless sensor networks, IEEE Journal of Selected Areas in Communications. (2004) 1141-1150.

[6] A. Agah, K. Basu and S.K. Das, Enforcing security for prevention of DoS attack in wireless sensor networks using economical modeling, Proceedings of IEEE International Conference on Mobile Adhoc and Sensor Systems Conference. (2005) 526–535.

[7] A. Agah, S.K. Das, and K. Basu, A non-cooperative game approach for intrusion detection in sensor networks, Proceedings of 2004 IEEE 60th Vehicular Technology Conference. (2004) 2902–2906.

[8] Yenumula B. Reddy, A game theory approach to detect malicious nodes in wireless sensor networks, Proc. 2009 Third International Conference on Sensor Technologies and Applications (SENSORCOMM). (2009) 462–468.

[9] A. Agah, and S.K. Das, Preventing DoS Attacks in Wireless Sensor Networks: A Repeated Game Theory Approach, International Journal of Network Security, 5 (2007) 145–153.

[10] Yenumula B. Reddy, S. Srivathsan, Game theory model for selective forward attacks in wireless sensor networks, 17th Mediterranean Conference on Control and Automation. (2009) 458-463.

[11] S. Marti, T.J. Giuli, K. Lai and M. Baker, Mitigating routing misbehavior in mobile ad hoc networks, Proceeding of The 6th International Conference on Mobile Computing and Networking (MOBICOM). (2000) 255-265.

[12] F.Y. Li, G.R. Chang, L. Yao, F.X. Gao, Cooperative based routing approach for wireless sensor networks, International Journal of Computer Applications in Technology, in press.

[13] W. Heinzelman, A. Chandrakasan, and H. Balakrishnan, An Application-Specific Protocol Architecture for wireless microsensor networks, IEEE Transactions on Wireless Communications, 1 (2002) 660–670.