Path Selection Method for Reliable Data Transmission in Sensor Networks using GA

Chung Il Sun[†] and Tae Ho Cho[††],

School of Information and Communication Engineering, Sungkyunkwan University

Summary
The wireless sensor networks are subjected to threats and highly vulnerable to various attacks due to the sensor characteristics, such as the openness of wireless communication channels, lack of infrastructure, and physical discloser. Sensor networks are highly susceptible to denial of service (DoS) attacks due to their inherent characteristics. Sinkhole attack is well-known routing attack in which a malicious node prevents sensed data from forwarding toward the base station. In this paper, we propose a method that can avoid the sinkhole attack for safe data transmission in sensor networks that uses optimal path selection using genetic algorithm based routing. The proposed method selects the optimal paths to transmit the sensed data and guarantees reliable data transmission. In simulation, our proposed method is compared with GRAM. The simulation results show that the proposed method is efficient in both the energy consumption and success ratio of the delivery.

Key words:
Reliable data transmission, routing path, genetic algorithm, sensor network,

1. Introduction

Recent advances in low-power electronic technology and wireless communications have led to the development of small multi-modal sensing devices [1]. A wireless sensor network is composed of a large number of sensors that have constrained battery life, limited computation, and narrow bandwidth. These sensor nodes are deployed in large numbers in a variety of environments, such as battlefields, hostile areas, and civil environments [2]. Sensor nodes have the ability to communicate either among each other or to a base station directly [3]. Sensor nodes continuously monitor their surrounding areas and collect sensing data to forward to the base station [4].The sensor networks are subjected to threats and highly vulnerable to various attacks due to the sensor characteristics, such as the openness of wireless communication channels, lack of infrastructure, and physical discloser. Sensor networks are highly susceptible to denial of service (DoS) attacks due to their inherent characteristics, such as low computational power, limited memory, and narrow communication bandwidth. Many-to-one, which is a well-known communication approach that is vulnerable to sinkhole attack, where an attacker attracts its surrounding nodes with unfaithful routing information, and then changes the data flow passing through it.

The sinkhole attack can be easily launched by a bogus node in the network. The bogus node advertises itself as a very attractive route to the data sink [5].The surrounding nodes choose the bogus node as the next hop for message forwarding, considering it a high quality route and propagate this route to other nodes. Almost all traffic is thus attracted to the bogus node. Moreover, it can either drop the data or selectively forward it based on some security routing mechanism. This bogus node thus forms a sink hole with itself at the center [5]. This can cause energy consumption of the nodes involved around the bogus node. If it then performs selective forwarding attack, it can seriously damage the routing operation.

A number of routing protocols [6-8] have been developed to secure the sensor network against these attacks.

In this paper, we propose a method that can avoid the sinkhole attack for safe data transmission in sensor networks that uses optimal path selection using genetic algorithm based routing. The proposed method selects the optimal paths to transmit the sensed data and guarantees reliable data transmission. In the proposed method, each node chooses the next forwarding node and delivers the routing table through a simple operation. The remainder of the paper is organized as follows. Section 2 discusses related work. Section 3 describes the proposed method. Section 4 presents simulation results. Finally, Section 5 concludes our work.

2. Related work

2.1 Sinkhole attack

Sinkhole attack prevents sensed data from forwarding toward the base station. In this attack, an adversary's goal is to lure nearly all the data flow from a particular area through malicious nodes. This attack feigns that the malicious node is located on the routing path that proceeds to an important node or destination node, such as the sink. It can exert a negative impact to the network, even if there is just one malicious node [5]. This attack can enable

Manuscript received February 5, 2011
Manuscript revised February 20, 2011

many other attacks, such as selective forwarding attack or Sybil attack.
Sinkhole attack typically operates by making a malicious node look attractive to surrounding nodes. Therefore, the surrounding nodes delude it that a malicious node is the next forwarding node for delivering the sensed data. Thus, the malicious nodes can either selectively forward data or drop the packet.

2.2 Selective forwarding attack

Selective forwarding attack is a well-known attack in which a malicious node in the forwarding path initiates a selective forwarding attack, the malicious node will refuse to forward the sensed data or drops packets randomly. When the malicious node is in the path of data flow, it can be typically the most effective and hard to detect. If this attack can be launched with the black hole attack or sinkhole attack, then it can do serious damage to the network.

2.3 Previous work

Kim and Cho [6] proposed a routing path generation method based on a genetic algorithm for reliable data transmission against the jamming zone. The base station creates the optimal path in the proposed method to avoid the jamming zone in the network. Thus, it can guarantee safe data transmission by considering the balanced energy depletion of the sensor nodes and the entire network. Moreover, it uses the genetic algorithm to find an efficient routing path by considering the radio-jamming zone, and energy consumption needed for data transmission.
Choi and Kim [7] proposed a detection scheme for sinkhole attacks in sensor networks. The proposed method can detect a sinkhole attack that uses LQI based routing and several detecting nodes. General nodes collect minimum link cost between neighborhood node and detecting nodes compute the minimum path cost with surrounding detector nodes in the proposed method. It can detect an abnormally strong signal from the actions of the malicious node by referring to the minimum link cost table.
Huijan et al. [9] proposed a scheme of secure data transmission that can forward data safely, and detect the selective forwarding attack. In the proposed method, the trust value of each node is used to select a secure path and then determine the malicious nodes that are suspected of launching selective forwarding nodes using a watermark based technique.

2.4 Motivation

In a sinkhole attack, the malicious node attracts its surrounding nodes with defective route information. Then, surrounding nodes mistake the attack node for the next forwarding node or sink node; thus, disturbing data transmission. Moreover, if a sinkhole attack is launched with another attack, such as a selective forwarding attack, then the network can be seriously damaged.

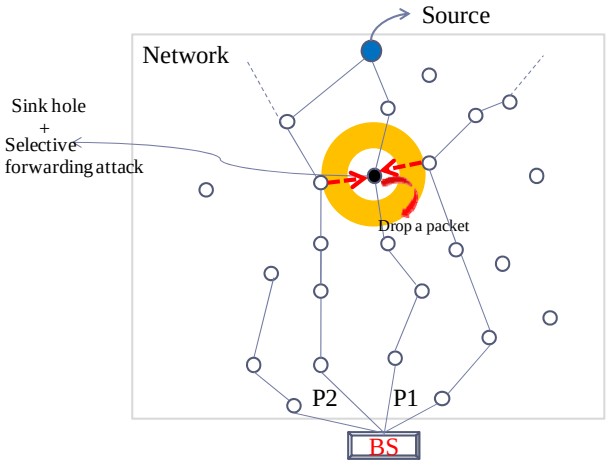

Fig. 1 a sinkhole attack performing along with a selective forwarding attack

Fig. 1 shows a sinkhole attack performing along with a selective forwarding attack. The sensed data that the source node transmits toward the base station may be not forwarded due to the interruption of both attacks. This can lead to not only false decision making by the users but also unwanted consumption of limited energy resources in the battery powered networks. Therefore, there it is necessary to avoid the threat to a route that can provide both reliable data transmission and over-all energy saving. In this paper, we propose a path selection method to provide data transmission to avoid simultaneous attacks in the network using finding the optimal path mechanism based on the GA algorithm.

3. Proposed Method

3.1 Assumption

A sensor network is composed of a large number of sensor nodes and one base station. Each sensor node has an identification that proves the broadcast message sent from the base station. We assume that sensor nodes form a number of clusters after initial deployment. Furthermore, each sensor node has a clustering mechanism that organizes a cluster automatically but there is no cluster head. One cluster node is elected to be the target node that receives the request packet from the base station. Each cluster node creates a list table containing neighbor nodes that eavesdrop the request packet.

3.2 Overview

In the proposed method, routing paths are established using a Genetic Algorithm (GA) to guarantee reliable data transmission when a sinkhole attack and selective forwarding attack multiply occur. The sink node considers the energy level of each forwarding node in establishing the routing path. In addition, once malicious nodes are detected, such nodes are not selected as forwarding nodes in every routing path. The information of the routing path generated by the sink node is broadcast to the target area. Then, all the nodes that received the message of the routing path can verify the received message through simple bit computation. Moreover, the detection of the aforementioned attacks is performed by comparing the routing message delivered by the sink node and the detection message.

3.3 Genetic algorithm

The Genetic algorithm provides an efficient approach to search for the optimum solution. A chromosome represents a routing path. Each gene in the chromosome is represented by an integer and corresponds to a sensor node. In addition, each locus of the chromosome represents the order of a forwarding node in the path.

3.4 Routing selection method

The base station forwards the request message to the represented node in each cluster and collects the sensed data periodically. Whenever the base station requests the sensing data, the routing paths change every time. Each node in the cluster area broadcasts the request message to generate the neighbor nodes list and then forwards it to the base station. After initial deployment, the base station individually generates the routing path table corresponding to each cluster area using the received neighbor node lists. Each routing table contains optimal paths, as well as candidate paths. The optimal path is chosen by a GA that decides the qualification as the path that is both reliable and energy conserving, based on the fitness of the node, path length, and path energy level. The base station preferentially selects the optimal path to request the sensing data. The base station may choose the second best path to request the sensing data when the malicious node is on the optimal path and disturbs the data transmission. The request message sent by the base station contains the list of forwarding nodes on the path based on respective identification of the forwarding nodes. Once an optimal routing path is confirmed by the base station the flooding routing message starts. We use a simple bit calculation technique to provide energy efficiency. Fig. 2 depicts an example form of the list of bits attached in the message.

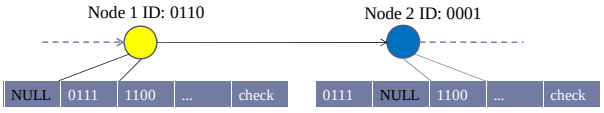

Fig. 2 The example form of the list of bits

The routing message consists of a list of 4-bits that is used to find the next node's ID and check bit. The length of the routing message is the number of nodes on the path. The first and last index of the list attached in the first instance of the message is NULL and check bit respectively. If there is a NULL in the first bit of the list, this message is sent from base station. When a node receives the first instance of a routing message, it computes the XOR operation with the first path bit in the list using its own identification to determine the next forwarding node. Then, it updates the list attached in the message, in such a way that the node shifts the value of NULL to the next position in the list. For example, if there are n nodes on the path, then the list length is n+2. A nodei that is the first received message computes the XOR operation with i+1 value of the list. As shown in Fig. 2, the identification of node 1 and 2 are 0110(2) and 0001(2) respectively. Node 1, the first receiving node in the routing path, can find the ID of the next forwarding node using the second index following the value of NULL. The value 0001(2) is generated by the XOR operation between 0110(2) and the second index 0111(2). It is possible to transmit the information of the forwarding nodes to the destination node using the aforementioned XOR operation. The destination node delivers sensing data by the bit operation based on the received route message in reverse order.

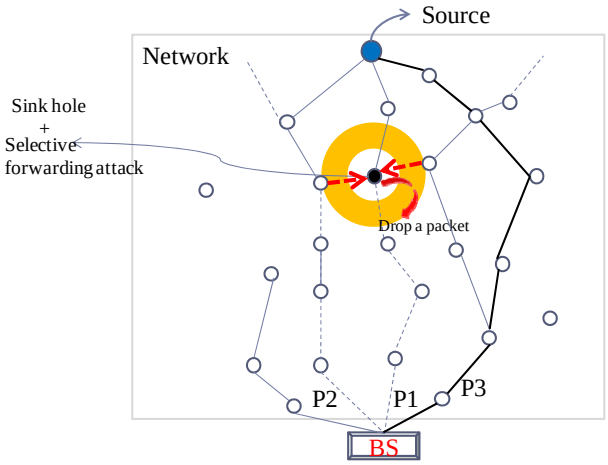

Fig.3 The optimal path for transmitting the data

Fig. 3 shows that if path P1 and P2 cannot transmit the sensing data or routing message caused by the malicious node, then the base station finds optimal path P3 that does

not include the malicious node for data transmission. The base station can determine the malicious node by comparing the node list of the routing message of both P1 and P2.

4. Simulation Results

Simulation was performed to compare the proposed method to the existing GRAM [6]. In this simulation, 1000 sensor nodes are randomly deployed in a 250 x 250 territory. The performance criterion is success rate of data transmission and energy consumption of nodes. The network contains three malicious nodes. Each node consumes 16.56uJ /12.5uJ to transmit/receive a byte. The packet size is 32bytes.

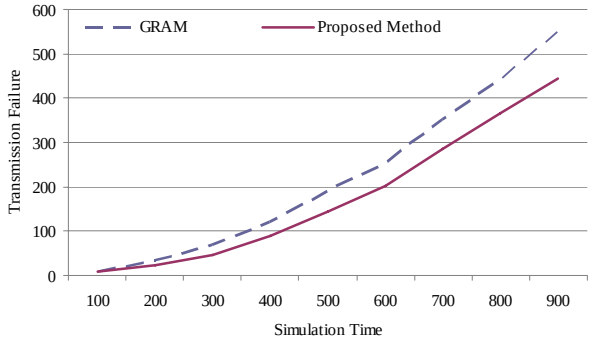

Fig. 3 The data transmission failures cased by the multiple attacks

Fig. 3 shows the simulation results of the transmission failures caused by the multiple attacks. Since the proposed method selects the optimal routing path by considering the remaining energy of nodes, the number of the data transmission failures in the proposed method is less than GRAM.

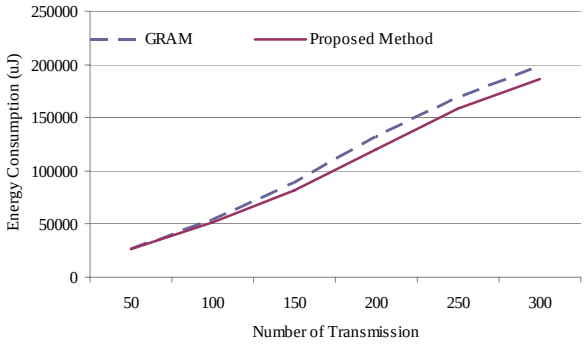

Fig. 4 The energy consumption with the number of the data transmission.

Fig. 4 illustrates the energy consumption caused by the data transmission. In the figure, the proposed method consumes less energy for forwarding message that GRAM. The proposed method guarantees the rate of success for data transmission to provide energy efficiency.

5. Conclusion

The main purpose of wireless sensor networks is to collect sensing data in target environments. It is important to guarantee that the sensing data are transmitted to the sink node. In this paper, we propose a path selection method to avoid threats to the route to provide both reliable data transmission and over-all energy conservation. In the proposed method, the routing path is generated by considering the energy required for data transmission, location information to avoid the interruption of sinkhole attack with a selective forwarding attack. Moreover, we apply the genetic algorithm to determine the optimal routing path and simple computation to conserve node energy and safe message transmission. Simulations show data transmission from target nodes to the base station is guaranteed in our proposed method. The results also show the proposed method can collect more data in the territory than can existing methods. However, the proposed method guarantees data transmission to provide energy efficiency but cannot detect a malicious node. Therefore, we will focus on the detection of the attacking node in future research.

Acknowledgments

This work was supported by National Research Foundation of Korea Grant funded by the Korean Government (No. 2010-0011188).

References

[1] K. Akkaya and M. Younis, “A Survey on Routing protocols for Wireless Sensor Networks”, Ad hoc Netw., vol. 3, no. 3, pp. 325-349, May 2005.

[2] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, “A Survey on Sensor Networks,” *IEEE Communications Magazine*, vol.40, no.8, pp.102-144, Aug. 2002.

[3] J. Al-Karaki and A. Kamal, “Routing Techniques in Wireless Sensor Networks: A Survey,” *IEEE Wirel. Commun.*, vol. 11, no. 6, Dec. 2004, pp. 6-28.

[4] Q. Jiang and D. Manivannan, “Routing Protocols for Sensor Networks,” in *Proc. of CCNC*, pp. 63-98, Jan. 2004.

[5] Edith C. H. Ngai, Jianchuan Liu, and Michael R. Lyu, "On the Intruder Detection for Sinkhole Attack in Wireless Sensor Networks," in Proc. IEEE ICC., pp. 3383-3389, June 2006.

[6] J. M. Kim and T. H. Cho, "Routing Path Generation for Reliable Transmission in Sensor Networks Using GA with Fuzzy Logic Based Fitness Function," Lecture Notes in Computer Science, vol. 4707, pp. 637-648, 2007.

[7] Byung Goo Choi, Enug Jun Cho, Jin Ho Kim, Choong Seon Hong, and Jin Hyoung Kim, "A Sinkhole Attack Detection Mechanism for LQI based Mesh Routing in WSN," in Proc. ICOIN 2009, pp. 1-5, Jan 2009.

[8] Edith C. H. Ngai, Jianchuan Liu, and Michael R. Lyu, "On the Intruder Detection for Sinkhole Attack in Wireless Sensor Networks," in Proc. IEEE ICC., pp. 3383-3389, June 2006.
[9] Huijuan Deng, Xingming Sun, Baowei Wang, and Yuanfu Cao, “Selective Forwarding Attack Detection using Wateramark in WSNs.” In Proc. ISECS 2009., pp. 109-113, 2009.

Chung Il Sun received his M.S. degree in Information and Communication Engineering from Sunkyunkwan University and B.S. degree in Computer Science from Kyungwon University, Korea, in 2009 and 2007. He is currently a graduate student in the School of Information and Communication Engineering at Sungkyunkwan University. His research interests include wireless sensor networks, and security in wireless sensor networks.

Tae Ho Cho received the Ph.D. degree in electrical and computer engineering from the University of Arizona, USA, in 1993, and the B.S. and M.S. degrees in electrical engineering from Sungkyunkwan University, Korea, and the University of Alabama, USA, respectively. He is currently a Professor in the School of Information and Communication Engineering, Sungkyunkwan University, Korea. His research interests are in the areas of wireless sensor network, intelligent system, modeling and simulation, enterprise resource planning.