논문 2010-2-21

GEOP : 보안 인식 다중경로 라우팅 프로토콜

GEOP : A Security Aware Multipath Routing Protocol

공형윤*

Hyung-yun Kong

요 약 MEMS(Micro Electro-Mechanical Systems) 분야의 급격한 발전은 저비용의 정보 처리 센싱 능력을 갖춘 센서의 발전에 박차를 가했다. 이러한 기술의 흐름은 강력하고 높은 확장성을 가지는 WSNs(Wireless Sensor Networks)을 위하여 더 많은 센서 간 연결을 위한 연구가 진행되고 있는 실정이다. WSNs의 자원부족, Ad-hoc 배치방법, 보다 광대해지는 규모는 센서 간 통신에서 안전성을 보다 중요한 문제로 인식하게 하고 있다. 센서 네트워크의 주요 고려사항은 에너지 효율이기 때문에, 보안 기술은 통신에서의 보안 특징과 그것을 수행하기 위해 계산해야하는 오버헤드 간 균형을 맞춰야한다. 본 논문에서는 새로운 보안 인식 다중경로 위치기반 라우팅 프로토콜을 개발하기 위하여 위치정보와 전송확률을 결합한다. 네트워크 시뮬레이터(ns-2)를 실행한 결과 보다 나은 성능을 얻을 수 있음을 알 수 있다.

Abstract Rapid technological advances in the area of micro electro-mechanical systems (MEMS) have spurred the development of small inexpensive sensors capable of intelligent sensing. A significant amount of research has been done in the area of connecting large numbers of these sensors to create robust and scalable Wireless Sensor Networks (WSNs). The resource scarcity, ad-hoc deployment, and immense scale of WSNs make secure communication a particularly challenging problem. Since the primary consideration for sensor networks is energy efficiency, security schemes must balance their security features against the communication and computational overhead required to implement them. In this paper, we combine location information and probability to create a new security aware multipath geographic routing protocol. The implemented result in network simulator (ns-2) showed that our protocol has a better performance under attacks.

Key Words : multipath, geographic routing

Ⅰ. Introduction

Advances in micromechanical and computer engineering technology facilitate the development of low cost, low power, multifunctional sensor devices. It is feasible to deploy these small sensor nodes in large numbers, and without pre-existing infrastructure. Therefore sensor networks, with their flexible and scalable nature, have great potential for a variety of applications such as battlefield surveillance, monitoring wildlife habitats, tracking vehicles, health monitoring, etc[1-4]. The utilization of sensors in critical systems such as airports, hospitals and plants, requires the authenticity and confidentiality. However, this is very difficult in WSNs environments, due to the limitation of resources and their physical insecurity.

The research challenge is to secure the routing infrastructure against threats such as tampering, denial-of-service (DOS) attacks[5-7]. Some attacks in routing protocols include bogus routing information, selective forwarding, sinkhole attacks, wormholes, HELLO flood attacks, acknowledgement spoofing[7].

*정회원, 울산대학교/전기전자정보시스템공학부
접수일자 2010.03.15, 수정일자 2010.4.9

Prior work in securing WSNs focuses on symmetric key-based techniques for achieving authenticity and confidentiality of the transmitted data. Examples of security protocols in WSNs can also be found such as SPINS suite of security building blocks[8], fault tolerant routing, securing of TinyOS routing[9], directed diffusion[7], and the INSENS secure routing system[10]. Although, these protocols give a considerable improvement their implementation is difficult and there are still unresolved security issues. Most of them cannot protect against the attacks from internal nodes.

In this paper we develop a secure routing protocol based on location information and probability for sensor networks. Our goal is to design multi-path routing algorithms with high delivery rate and low communication overhead, achieved by restricted flooding approach. In addition, our protocol must be security aware. The proposed protocol has implemented by using ns-2[11].

This paper is organized as follows. The detail of our protocol is described in Section 2. Experiment results are given in section 3. Section 4 concludes the paper.

Ⅱ. GEOP

1. Assumptions

In this subsection, we describe our assumptions throughout the paper. Firstly, each node in the network is aware of its (x, y) coordinates in the plane. The node can either be equipped with a GPS device, or use some other localization scheme, such as the signal-strength based localization. Secondly, the source which attempts to transmit the packet to the destination, needs to know the location of the destination.

2. Neighbor Management

Due to the routing decision based on the information of one hop neighbors, it is very important to guarantee that this information is correct and up to date. Each sensor node broadcasts the HELLO message to its neighbors periodically. To avoid collision of the HELLO messages from two neighbors, the sensor node adds a random delay (within the selected range) before broadcasting. The HELLO message includes the identifier of node (ID), location of node and a sequence number. The purpose of the sequence number is to ensure freshness of an HELLO message.

Upon receiving HELLO message from node B, node A checks to see if node B is in its neighbor table. If so, node A will update new lifetime for node B's entry. Otherwise, node A will add a new entry for node B.

The information in neighbor table has become less accurate as one of neighbors may leave out or a new sensor node enters radio range. If a node does not receive a HELLO message from a neighbor after a period of time, it will delete that neighbor from its Neighbor Table and make the appropriate changes to its Gradient Table.

The Neighbor Table includes following fields:

- Neighbor addresses (NodeID) - The identifier of neighbor node.
- Lifetime - The interval that a node does not receive anything from a neighbor and it considers that the link is unavailable.
- Sequence Number (SeqNo) - The number of the last packet received from that neighbor. This field is used to acknowledge a transmission of a neighbor and to identify packets that are out of sequence.
- Location - Geographic position of the node.
- Penalty - The value that indicates the trust of neighbor node.

3. GEOP Algorithm

Most wireless routing protocols often use one or many metrics (e.g. hop count, shortest distance etc…) to decide to which the data packet should be forwarded if it cannot be delivered directly. It is difficult to secure these protocols because malicious node can change or spoof routing information to make itself look especially

attractive to other nodes with respect to the routing algorithm. The cryptographic algorithms can be used to achieve availability, confidentiality, integrity, and authentication of routing information but they cannot protect against the attacks from internal nodes.

In our protocol, instead of choosing one or several nodes to forward packet, each node will forward the packet with a probability p < a given threshold. The value of this threshold is a challenging problem. If it is too small, it can result in low delivery rate and if it is too large, the redundant data will increase. Moreover the topology of sensor networks changes very frequently due to node sleeps or node failures. Therefore it is difficult to define a fixed threshold for optimizing the performance of system. Furthermore, generating the probability p is also not simple. If we generate p randomly we cannot take advantage of local information at each node. We solved these problems by creating a variable threshold and defining the probability p as a function of local information.

We divided the Neighbor Set into 3 subset S1, S2, S3 as illustrated in Fig. 1. Each subset has a forwarding probability correspondingly P1, P2, P3 in which P1 is the highest (approximately equal to 1).

● The Forwarding Candidate Set of Node i :

$FSi(Destination) = \{node \in NSi \mid L - L\,next >$

in which

- ○ L : distance from node i to the destination
- ○ $L\ next$: distance from the next hop forwarding candidate to the destination.

● $S1 = \{node \in NSi \mid r_{ij} < \theta\}$

in which

- ○ r_{ij} : the ratio between the distance from node i to destination and the distance from node j to destination. Node j is the node that forwarded packet to node i.
- ○ θ : included in packet header

● $S2 = FSi \setminus S1,\ S3 = NSi \setminus (S1 \cap S2)$

To evaluate the trust of neighbor nodes, each time a node forwards packet, it will increase penalty of neighbors belong to S1. If node detects the forwarding direction is legal, it will decrease penalty of the neighbor before dropping packet.

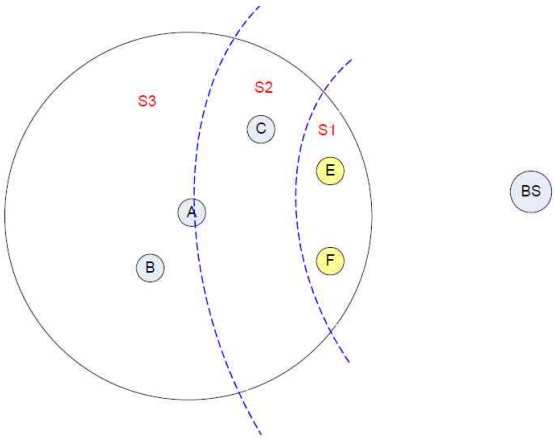

Fig. 1. Three forwarding subset
그림 1. 세 개의 전달 집합

Next, we analyze how GEOP detects the malicious actions.

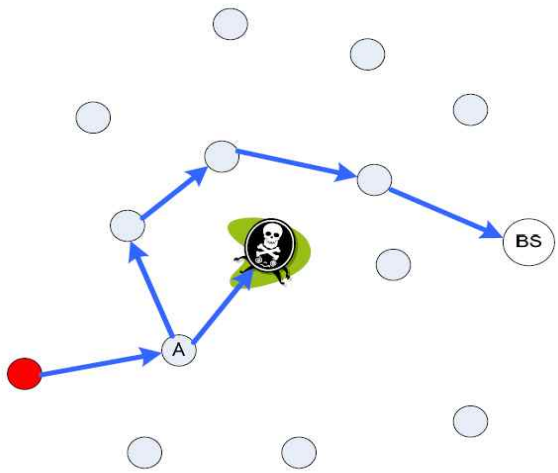

Fig. 2. How GEOP protects against selective forwarding attacks
그림 2. GEOP를 이용한 선택적 전달 공격에 대한 방어 방법

If malicious nodes M drop or misdirect received packets, node A does not receive the rebroadcast

packet from node M, the penalty of node M will be decreased. Next forwarding time, node A will change Θ. It results to other nodes will have higher forwarding probability. The packet can go through another path to destination (see Fig.2).

Ⅲ. Protocol Evaluation

Table 1. Simulation Parameters

Mac layer protocol	IEEE 802.11
Transmission radio range	250m (random scenarios) 40m (grid scenarios)
Bandwidth	2 Mbps
Data rate	2 packets/s
Simulation area	1000 x 1000m^2 (random scenarios) 200 x 200m^2 (grid scenarios)
Number of sensor nodes	100
Effective simulation time	1000 seconds
Energy model	Energy Model
Initial energy	1000 J
Rx Power	0.0522 J
Tx Power	0.0591 J
Idle Power	0.00006 J
Sleep Power	0.000003 J

The GEOP protocol is implemented in the network simulator (ns-2). We compare GEOP with GPSR which is available in ns-2.

Table 1 shows the simulation parameters we use ; unless otherwise indicated these parameters are used in the studies. We use both the grid and random deployment to simulate our algorithm. In grid deployment, we divide the covered simulation area into 10 × 10 grids covering an area of 200x200 square meters. One of the 100 sensor nodes is placed at the center of each the grid tiles. Nodes publish data at the rate of 2 packets per second in order to simulate a fairly high load traffic scenario. In random deployment, the 100 nodes are randomly placed in the simulation area while the sink is placed roughly at the center of the area.

Since GEOP does not require any MAC layer information, we use the original IEEE 802.11 with 914MHz Lucent WaveLAN DSSS radios as our MAC layer protocol.

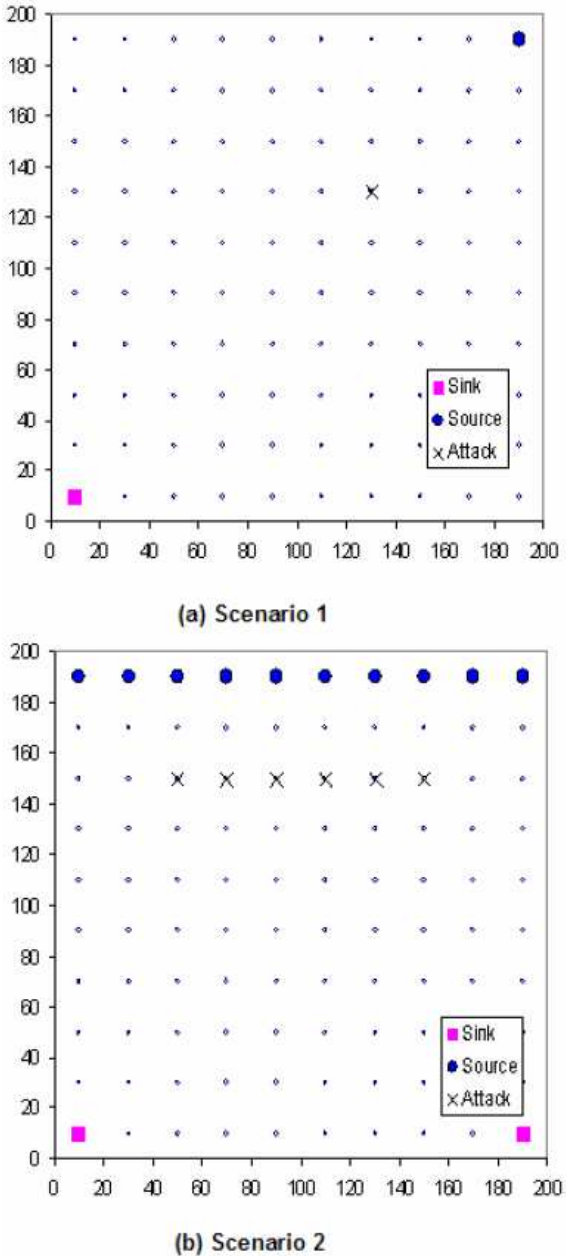

Fig. 3. Scenarios for simulation study
그림 3. 모의 실험을 위한 시나리오

The period of hello message is 5 seconds. To update the location of sink node we use a query timer. Each

sink node broadcasts a query message into network periodically. Upon receiving this query message, sensor nodes will update the location of sink node to its sink list. In our simulation, the query messages are broadcast each 10 seconds. In order to evaluate the performance of routing protocols under different attack models we use grid scenarios shown in Fig. 3.

In the scenario 1, only one attacker resides on the shortest path from the source to destination constructed by GPSR. In the scenario 2, the six attackers form a wall across the network and try to separate the source and destination.

To evaluate the performance of routing protocols in normal, we generate random scenarios in square of 1000 m^2. Nodes will mobile with velocity of 20 m/s.

In evaluating our protocol, the following metrics were used.

- Packet Delivery Success Rate : the ratio of the total over all nodes of the number of data packets received, divided by the total number of data packets sent from the sources.
- Energy usage : The amount of power used during the simulation will be monitored and used for evaluating the protocols. Batteries have a finite amount of power and nodes die once power runs out. For this reason, lower power usage is preferable to higher power usage.

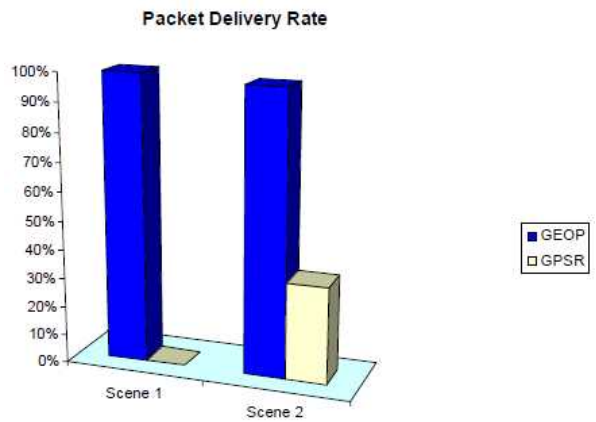

Fig. 4. Packet delivery rate
그림 4. 패킷 전송률

Fig. 4 shows the delivery ratio achieved in the different scenarios. In scenario 1, GPSR completely fails if any attacks are on the path from the source to destination. As a result, no packet is received by the destination. GEOP has high delivery ratio in both scenarios. It means that GEOP can always find the path to destination. It results to the energy usage of GEOP (Fig. 5).

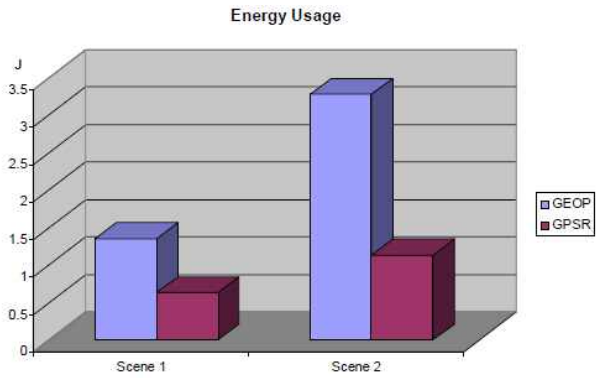

Fig. 5. Energy Usage
그림 5. 에너지 사용 비교

IV. Simulation Result

We also evaluate the performance of GEOP in mobility networks. Fig. 6 shows that GEOP has good packet delivery ratio even in mobile networks. As we known, AODV is one of best routing protocols for high mobility ad hoc network. But AODV is not appropriate to sensor networks because it uses routing table for forwarding message. Maintaining such routing table is possible for networks with few nodes but very difficult or impossible for networks with large number of nodes. Sensor networks can have thousands of nodes, so the size of routing table will be very large. Therefore the use of routing table in sensor networks is not the good choice. Our protocol does not use routing table and has packet delivery ratio approximately to AODV. So we can conclude that GEOP is a better choice for using in WSNs than AODV.

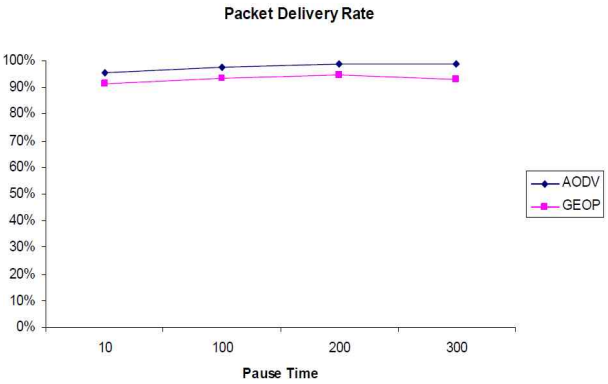

Fig. 6. Packet delivery rate in high mobility networks
그림 6. 높은 이동성의 네트워크에서 패킷 전송률

V. Conclusion

While security in WSNs has been well studied, most existing works have focused on traditional routing protocols. The nature of geographic routing makes it vulnerable to many kinds of attacks and required specialized solutions for securing them. To address the problem, we proposed a multipath geographic routing protocol which is aware security. Our protocol geographically route packet without any routing tables or topological information. We discussed the proposed approach in detail and compared our protocol to a well known geographic routing protocol. The simulation results showed that our protocol has good performance under attacks. In addition, GEOP works well in networks with high mobility. We will implement our protocol on mote and apply it in real applications.

참 고 문 헌

[1] K. Akkaya and M. Younis. A survey on routing protocols for wireless sensor networks. Elsevier Ad Hoc Network, Vol. 3/3 pages 325 - 349, 2005.

[2] Department of Computer Science York University. Sensor network routing algorithms for realistic battery models, July 2005. Workshop on Information Fusion and Dissemination in Wireless Sensor Networks, at Budapest, Hungary.

[3] Holger Karl and Andreas Willig. Protocols and Architectures for Wireless Sensor Networks. Wiley, 2005. ISBN:0470095105.

[4] I. F. Akyildiz,W. Su, Y. Sankasubramaniam, and E. Cayirci. "Wireless Sensor Networks: A Survey", Computer Networks, 38:393 - 422, 2002.

[5] Perrig, Adrian, John Stankovic, and David Wagner. Security in Wireless Sensor Networks. Communications of the ACM, Volume 47, Issue 6 (June 2004): 53-57.

[6] Karlof, Chris, Naveen Sastry, and David Wagner. TinySec: A Link Layer Security Architecture for Wireless Sensor Networks. Proceedings of the Second ACM Conference on Embedded Networked Sensor Systems (SenSys'04) (November 3 - 5, 2004).

[7] Karlof C. and D. Wagner. Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures. Proceedings of the First IEEE International Workshop on Sensor Network Protocols and Applications(SNPA'03) (11 May 2003).

[8] Perrig, Adrian, Robert Szewczyk, Victor Wen, David Culler, and J.D. Tygar. SPINS: Security protocols for sensor networks. In The Seventh Annual International Conference on Mobile Computing and Networking (MobiCom 2001), (2001).

[9] J. Staddon, D. Balfanz, G. Durfee, "Efficient Tracing of Failed Nodes in Sensor Networks", First Workshop on Sensor Networks and Applications, WSNA'02, Atlanta, Georgia, USA.

[10] J. Deng, R. Han and S. Mishra, "The Performance Evaluation of Intrusion-Tolerant Routing in Wireless Sensor Networks", to appear in IEEE 2nd International Workshop on

Information Processing in Sensor Networks (IPSN '03), Palo Alto, CA, USA, April, 2003

[11] "The network simulator - ns2" http://www.isi.edu/nsnam/ns/.

저자 소개

공 형 윤(정회원)

- 1989년 2월 : New York Institute of Technology(미국) 전자공학과 학사
- 1991년 2월 : Polytechnic University (미국) 전자 공학과 석사
- 1996년 2월 : Polytechnic University (미국) 전자 공학과 박사
- 1996년~1996년 : LG전자 PCS팀장
- 1996년~1998년 : LG 전자 회장실 전략 사업단
- 1998년~현재 : 울산대학교 전기전자정보시스템공학부 교수

<주관심분야> 모듈레이션, 채널 부호화, 검파 및 추정 기술, 협력통신, 센서네트워크