# 센서 네트워크에서의 공격에 대한 라우팅 프로토콜의 안전성 평가에 관한 연구

김영한*, 한영주*, 정태명**
* 성균관대학교 컴퓨터 공학과
** 성균관대학교 정보통신공학부
e-mail : {yhkim, yjhan}@imtl.skku.ac.kr
tmchung@ece.skku.ac.kr

# A Study on Safety Evaluation of Routing Protocol against Attacks in Wireless Sensor Networks

Young-han Kim *, Young-ju Han * and Tai-myoung Chung**
*Dept. of Computer Engineering, Sungkyunkwan University
** School of Information and Communication Engineering, Sungkyunkwan University

**요 약**

자원의 제한을 가지는 센서로 구성된 무선 센서 네트워크에 적용하기 위하여 in-networking 프로세싱과 에너지 효율성을 제공하는 다양한 방식의 라우팅 프로토콜들이 제안되고 있다. 반면, 무선 센서 네트워크를 대상으로 하는 다양한 공격 형태들 또한 등장하고 있다. 무선 센서 네트워크 상에서의 라우팅 프로토콜은 기존의 라우팅 방식과 달리 in-networking 프로세싱을 제공하기 때문에 라우팅 프로토콜에 대한 안전성 평가는 매우 중요하다. 본 논문에서는 현재 무선 센서 네트워크상에서 제안된 라우팅 프로토콜과 공격에 대하여 살펴보고 각각의 공격에 대한 각 라우팅 프로토콜의 안전성을 평가한다. 이는 무선 센서 네트워크를 위한 새로운 라우팅 프로토콜 제안 시 보안 취약점을 효과적으로 해결할 수 있는 방향을 제시 할 수 있다.

## 1. 서론

기존의 무선 ad-hoc 네트워크를 위해 제안된 라우팅 프로토콜은 센서 노드들의 제한된 자원(전력, 연산 능력, 메모리)과 자가 구성 능력 등의 차이가 있기 때문에 센서 네트워크에 적용하기 어렵다. 따라서, 센서 네트워크에 알맞은 다양한 방식의 라우팅 프로토콜이 제안되고 있다[1],[3-4],[7-9].

센서 네트워크에서의 라우팅은 기존의 주소 체계인 IP 주소를 사용하기에는 센서 노드의 수나 데이터 처리 능력을 감안할 때 사용하기 어렵다. 그래서 브로드캐스팅 방식을 사용하여 최소한의 자원 소모와 보안적 요구 사항을 만족하기 위한 연구가 진행되고 있고 데이터 전송에 따른 전력 소모를 줄이기 위해 멀티홉 라우팅을 통하여 산재해 있는 센서간의 통신으로 취득한 데이터를 취합하여 한 번만 보내거나 중복 데이터를 삭제하여 보내는 등의 데이터 통합 기법이 연구되고 있다.

그러나 각 노드에서의 브로드캐스팅은 공격자의 도청이나 재사용 공격에 매우 취약하다. 또한, 데이터 취합 역시 악의 있는 노드에 의해 대량의 데이터를 발생시켜 네트워크를 무력화 시키는 공격이나 오차 범위 내의 데이터를 임의로 주입하여 센싱 정보에 대한 위·변조하는 공격에 취약하다[10].

따라서, 라우팅 프로토콜을 제안함에 있어 보안적인 측면을 고려하여야 하고 공격에 대한 안전성 평가도 이루어져야 한다.

센서 네트워크에 대한 보안은 라우팅 프로토콜만으로 보안 취약성을 해결하기에는 한계가 있기 때문에 다양한 보안 기법들이 결합되어 있는 형태로 이루어

본 연구는 정보통신부 및 정보통신연구진흥원의 대학 IT 연구센터 육성·지원사업의 연구결과로 수행되었음

져 있다. 그러므로 라우팅 프로토콜의 안전성 평가는 다른 보안 기법을 포함하여 이루어져야 하지만 기존의 논문들은 라우팅 프로토콜 자체만으로 공격에 대한 안전성이 평가되었다[1].

본 논문에서는 현재 제안된 라우팅 프로토콜과 센서 네트워크에서 가능한 공격을 알아보고 다른 보안 기법을 포함한 라우팅 프로토콜에 대한 안전성 평가를 하고자 한다.

본 논문의 2장에서는 라우팅 프로토콜과 공격에 대한 설명과 관계를 알아보고, 3장에서는 다른 보안 기법을 포함한 라우팅 프로토콜에 대한 안전성을 평가한다. 마지막으로 4장에서는 논문의 결론 및 앞으로 진행되어야 할 연구 계획을 제시한다.

## 2. 관련 연구

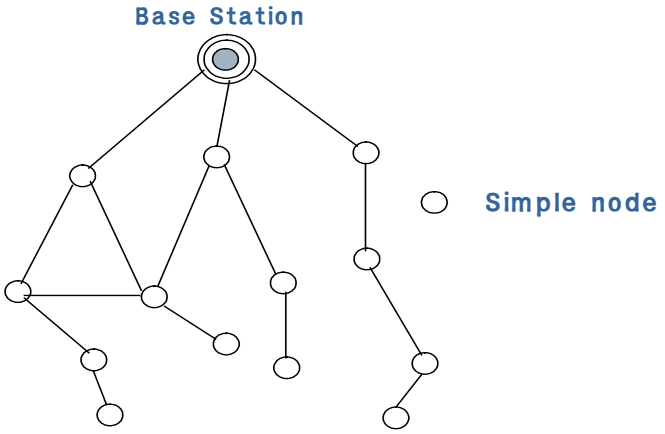
센서 네트워크 라우팅 프로토콜과 공격 가능한 유형에 대해 간략히 살펴보고 라우팅 프로토콜에 대해 어떤 공격이 가능하지 알아본다.

### 2.1 라우팅 프로토콜

센서 네트워크에서 현재 제안된 대표적인 라우팅 프로토콜은 평면 라우팅 프로토콜, 계층적 라우팅 프로토콜, 지리적 라우팅 프로토콜이 있다.

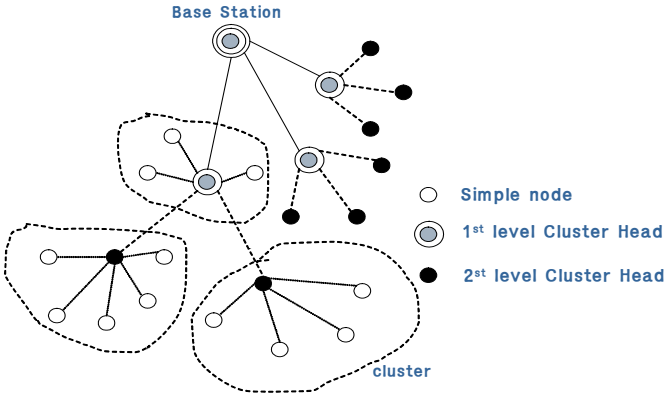
각각의 라우팅 프로토콜에 대해 살펴보면 아래와 같다.

- 평면 라우팅 프로토콜: 네트워크 전체를 하나의 영역으로 간주하여 모든 센서 노드들이 동등하게 라우팅에 참여할 수 있고 멀티홉 라우팅을 할 수 있는 특징이 있다. 대표적인 라우팅 기법으로는 Direct-diffusion, SPIN(Sensor Protocol for Information in Negotiation) 등이 있다[4],[8].



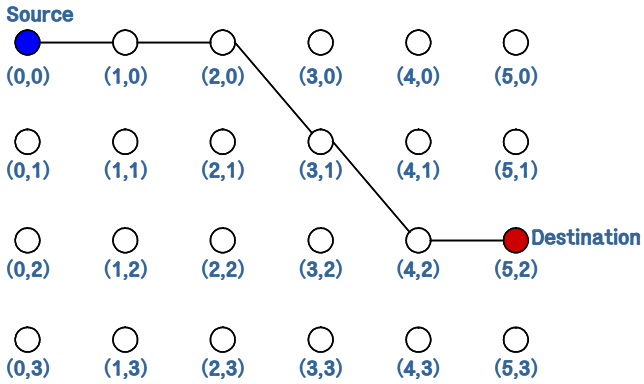

[그림 1] 평면 라우팅

- 계층적 라우팅 프로토콜: 네트워크를 클러스터링을 기반으로 한 다수의 영역으로 분할하여 각각의 특정 노드에 헤드의 역할을 부여하여 라우팅을 수행한다. 대표적인 라우팅 기법으로는 LEACH(Low Energy Adaptive Clustering Hierarchy), TEEN(Threshold sensitive Energy Efficient sensor Networks) 등이 있다[1],[7].




[그림 2] 계층적 라우팅

- 지리적 라우팅 프로토콜: 지리적인 위치와 에너지 상황을 이용해 이웃 노드들을 선택하여 최종 노드로 가는 경로를 설정한다. 대표적인 라우팅 기법으로는 GEAR(Geographical and Energy Aware Routing, GPSR(Greedy Perimeter Stateless Routing) 등이 있다[3],[9].




[그림 3] 지리적 라우팅

### 2.2 라우팅 공격

센서 네트워크 라우팅 프로토콜에 대한 공격으로는 크게 Sinkholes, Sybil, HELLO flood, Wormholes, Selective forwarding 등으로 나뉠 수 있다.

각각의 라우팅 공격에 대해 살펴보면 아래와 같다.

- Sinkholes: 모든 패킷의 최종 목적지는 Base Station(Sink)이므로 라우팅 정보를 변경하여 특정 지역의 모든 트래픽이 공격자의 노드를 지나가도록 조작한다.
- Sybil: 하나의 악의적인 노드가 다른 노드에게 여러 개의 식별자를 인식하도록 하여 하나의 노드가 여러 곳에 있는 것처럼 하여 분산된 환경이나 Multi-path 라우팅의 효과를 줄이는 공격이다.
- HELLO floods: 공격자의 노드는 충분한 파워로 HELLO 패킷을 브로드캐스팅 해서 멀리 있는 노드에게 자신이 가까운 위치에 있는 것처럼 인식하도록 하여 가까운 곳에 위치하지 않은 공격 노드에게 패킷을 보내도록 유도하여 패킷을 손실되게 하는 공격이다.

- Wormholes: Station에서 멀리 떨어져 있으며 노드간에 연결이 존재하지 않는 노드에 대해 가까이 위치하고 있는 것처럼 인식하게 하는 공격이다.
- Selective forwarding: 멀티 홉 네트워크에서 데이터 흐름을 목적으로 하여 특정 메시지나 노드에 대해 전달을 하지 않거나 메시지를 수정 또는 노드를 선택하여 전달하는 공격이다.

### 2.3 라우팅 프로토콜과 공격의 관계

센서 네트워크 라우팅 프로토콜에 대해 가능한 공격 유형을 알아보면 아래의 <표 1>과 같다[1].

<표 1> 센서 네트워크 라우팅 프로토콜에 대한 공격

| 프로토콜 | 관련 공격 |
|---|---|
| 평면 라우팅 | Sinkholes, Sybil, Wormholes, HELLO floods , Selective forwarding |
| 계층적 라우팅 | Sinkholes, Sybil, Wormholes, Hello floods, Selective forwarding |
| 지리적 라우팅 | Selective forwarding, Sybil |

평면 라우팅 프로토콜과 계층적 라우팅 프로토콜은 이웃 노드 간에 정보를 교환하지 않는 반면 지리적 라우팅 프로토콜은 지역 간에 정보를 교환하여 라우팅 경로를 설정하기 때문에 Sinkholes 공격, Sybil 공격에 안전하다. 또한 지리적 라우팅 프로토콜은 다른 라우팅 프로토콜과 달리 Hello 패킷을 보내지 않기 때문에 Hello flood 공격에도 안전하다.

## 3. 라우팅 프로토콜에 대한 안전성 평가

### 3.1 보안 요소

센서 네트워크의 대표적인 보안 기법으로는 인증 기법과 암호 기법이 있다.

공격자는 쉽게 메시지를 삽입하거나 위 변조 할 수 있기 때문에 수신자는 데이터가 원래 작성자로부터 온 것인지, 위·변조가 있었는지 확인해야 하므로 인증을 통해 데이터 무결성을 보장해야 한다.

또한 데이터 암호화를 통해 허가된 노드 이외에 데이터를 볼 수 없도록 데이터의 기밀성을 지원해야 한다.

센서 네트워크에서 대표적인 보안 프로토콜로는 SPINS(Security Protocols for Sensor Networks), LEAP(Localized Encryption and Authentication Protocol)등이 있다[2],[6].

SPINS는 데이터 기밀성, 양단간 데이터 인증, 무결성 등을 제공하는 SNEP과 데이터 브로드캐스팅에서의 인증을 제공하는 μTESLA로 구성되어 있고 LEAP는 하나의 키 매커니즘으로 대량의 센서 네트워크에 대해 안전한 키 매커니즘 설계가 어렵다는 판단으로 4개의 암호 키와 키 설정 프로토콜을 가진다.

### 3.2 안전성 평가

라우팅 프로토콜에 대한 안전성 평가는 암호화와 인증 기법을 포함하여 2.3절에서 각각의 라우팅 프로토콜에 대해 가능했던 공격을 막을 수 있는지 여부로 평가한다.

무결성을 제공하기 위한 인증 기법과 기밀성을 제공하기 위한 암호 기법은 센서 노드와 Base Station 간의 통신과 센서 노드간의 통신, Base Station과 모든 노드간의(브로드캐스팅) 통신에서 사용된다고 가정한다.

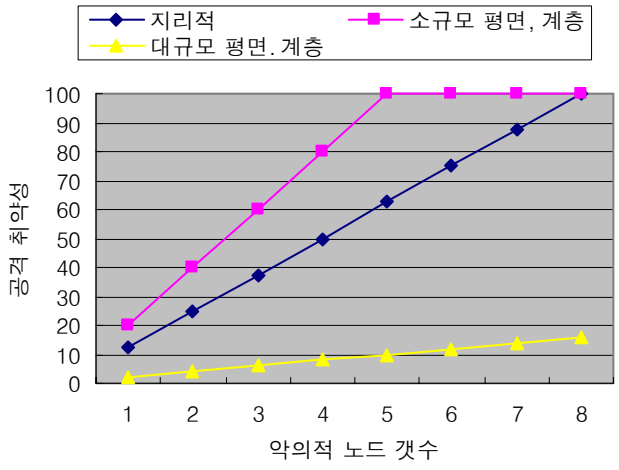
인증과 암호화에 사용할 비밀키는 Base Station에서 브로드캐스팅을 통해 모든 노드들과 공유하게 된다.

센서 네트워크 라우팅 프로토콜에서 가능했던 Sybil 공격은 비밀 키를 이용한 노드간 상호 인증으로 막을 수 있다. 또한 HELLO 패킷을 브로드캐스팅 해서 멀리 있는 악의적인 노드를 가까운 위치에 있는 것처럼 믿게 하는 HELLO floods 공격에 대해서도 패킷을 암호화하여 보내면 안전하다.

Selective forwarding 공격은 인증이나 암호화 기법을 포함하여도 막기가 어렵다. 그러나 다중 경로 라우팅의 경우 다음 경로를 동적으로 선택하도록 설계하면 막을 수 있다.

지리적 라우팅 프로토콜은 가까운 두개의 노드간의 거리는 1이고 각각의 노드는 8개의 이웃 노드들에게 패킷을 전달할 수 있다고 가정하고 있다. 따라서 Selective forwarding 공격을 막기 위해 다음 경로를 동적으로 선택하여도 하나의 노드에 대해 8개의 악의적인 노드가 존재하면 Selective forwarding 공격을 막을 수 없다. 그러나 평면 라우팅 프로토콜이나 계층적 라우팅 프로토콜의 경우 하나의 노드에 연결된 이웃 노드의 수가 증가할수록 Selective forwarding 공격에 대해 안전하다.

다음의 [그림 4]를 보면 평면 라우팅 프로토콜이나 계층적 라우팅 프로토콜은 소규모(하나의 노드에 5개의 이웃 노드가 연결되었다고 가정) 네트워크의 경우 지리적 라우팅 프로토콜 보다 Selective forwarding 공격에 취약하나 대규모(하나의 노드에 50개의 이웃 노드가 연결되었다고 가정) 네트워크의 경우 지리적 라우팅 프로토콜 보다 Selective forwarding 공격을 막기가 쉽다.




[그림 4] Selective forwarding 공격 취약성

평면 라우팅 프로토콜이나 계층적 라우팅 프로토콜

은 인증이나 암호화 기법을 포함하여도 Wormholes 공격이나 Sinkholes 공격에는 안전하지 않다.

Wormhole 공격은 감추어진 주파수 채널을 사용하므로 탐지가 어렵고 Sinkholes 공격은 남아있는 에너지나 라우팅 경로의 신뢰성에 관한 정보 등에 대해 확인하기가 어렵기 때문이다. 또한 Wormhole 공격과 Sinkholes 공격을 결합하여 공격하는 경우 막기가 더 어렵다.

지리적 라우팅 프로토콜은 지역간의 정보를 서로 교환하여 지리적인 위치와 에너지 상황에 대한 정보를 기반으로 경로를 구성하며 이웃 노드 간에 무선 주파수의 도달 거리를 알려주기 때문에 공격자의 위조된 연결의 탐지가 쉽다. 즉, Wormhole이나 Sinkhole 공격을 막을 수 있다.

보안 기법을 포함한 라우팅 프로토콜에 대해 가능한 공격 유형을 보면 아래의 <표 2>와 같다.

<표 2> 보안 기법을 포함한 경우에 가능한 공격

| 프로토콜 | 관련 공격 |
|---|---|
| 평면 라우팅 | Sinkholes, Wormholes, Selective forwarding |
| 계층적 라우팅 | Sinkholes, Wormholes, Selective forwarding |
| 지리적 라우팅 | Selective forwarding |

평면 라우팅 프로토콜과 계층적 라우팅 프로토콜을 기반으로 하는 라우팅 기법들은 이웃 노드간에 서로 정보를 교환하여 Wormholes 공격이나 Sinkholes 공격에 대해 안전할 수 있도록 설계되어야 한다.

지리적 라우팅 프로토콜을 기반으로 하는 라우팅 기법들은 이웃 노드가 악의적인 노드인지 판단하여 Selective forwarding 공격에 대해 안전할 수 있도록 설계되어야 한다.

## 4. 결론 및 향후 계획

센서 네트워크의 라우팅 프로토콜은 보안적 측면보다는 네트워크 오버헤드와 전력 소모를 줄이기 위한 방향으로 연구가 이루어지고 있다. 그러나 센서 네트워크는 기존 네트워크의 보안 기법을 그대로 적용하기 어렵기 때문에 보안 상 취약점을 가진다. 따라서 라우팅 프로토콜을 제안 시 안전성 평가가 이루어져야 한다.

기존의 라우팅 프로토콜에 대한 안전성 평가는 보안 기법을 포함하지 않고 안전성 평가가 이루어져 왔다. 그러나 라우팅 프로토콜에 대한 안전성 평가는 보안 기법을 포함하여 평가하는 것이 바람직하다. 따라서 본 논문에서는 대표적 보안 기법인 암호화와 인증 기법을 고려하여 평가하였다.

앞으로 새로운 라우팅 프로토콜을 제안하기 위해서는 에너지 효율적인 측면과 더불어 보안 기법을 포함한 안전성 평가를 통해 안전한 라우팅 프로토콜이 제안 되어야 할 것이다.

## 참고문헌

[1] A. Manjeshwar et al., “TEEN: A Routing Protocol for Enhanced Efficiency in Wireless Sensor Networks”, 1st Int’l Workshop Parallel and Distributed Computing Issues in Wireless Networks and Mobile Computing, April 2001.

[2] A. Perrig et al,. “SPINS: Security Protocols for Sensor Networks”, Proceeding of Seventh Annual International Conference on Mobile Computing and Networks, July 2001.

[3] B. Karp, H. T. Kung, “GPSR: Greedy Perimeter Stateless Routing for Wireless Networks”, MobiCom, 2000

[4] C. Intanagonwiwat, R. Govindan, D.Estrin, “Direct Diffusion: A Scalable and Robust Communication Paradigm for Sensor Networks”, IEEE/ACM Transactions on Networking, vol. 11, pp. 2 - 16, Feb 2003.

[5] C. Karlof, D. Wangner, “Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures”, First IEEE International Workshop on Sensor Network Protocols and Applications, May 2003.

[6] S. Zhu, S. Setia, and S. Jajodia, “LEAP: Efficient Security Mechanisms for Large-Scale Distributed Sensor Networks”, In Proc. of the 10th ACM CCS’03, Oct 2003.

[7] W. Heinzelman, A. Chandrakasan, and H. Balakrishnan, “Energy efficient Communication Protocol for Wireless Micro Sensor Networks”, in Proc. of the 33rd Annual Hawaii International Conf. on System Sciences, pp. 3005 – 3014, 2000.

[8] W. heinzelman, J. Kulik, and H. Balakrishnan, “Negotiation-based Protocols for Disseminating Information in Wireless Sensor Networks”, in Proc of the 5th Annual ACM/IEEE International Conference on Mobile Computing and Networking, 1999.

[9] Y. Yu, R. Govindan, and D. Estrin, “Geographical and Energy Aware Routing: a recursive data dissemination protocol for wireless sensor networks”, UCLA Tech. Report, 2001.

[10] 나재훈, 채기준, 정교일, “센서 네트워크 보안 연구 동향”, 전자통신동향분석, Feb, 2005.