무선 센서 네트워크에서의 라우팅 보안 기법 비교 분석+

*김영기 **이화성 ***김용호 ****이동훈

고려대학교 정보경영공학전문대학원

*persound@hanmail.net

A Study on Routing Security in Wireless Sensor Networks

*Young Ki Kim **Hwaseong Lee ***Yong Ho Kim ****Dong Hoon Lee

Graduate School of Information Management & Security, Korea University

요약

무선 센서 네트워크란 물리적, 환경적 현상을 감지하기 위해 센서를 사용하는 수백 개에서 수천 개의 센서 노드로 구성된 네트워크를 말한다. 이러한 무선 센서 네트워크에서 라우팅 보안은 중요하다. 센싱된 데이터가 사용자에게 전달되지 않는다면 네트워크는 그 기능을 제대로 수행한다고 할 수 없기 때문이다. 따라서 무선 센서 네트워크에서 데이터가 목적지에 안전하게 도달하도록 하는 라우팅 보안 기법은 필수적이다. 최근의 라우팅 보안은 암호학적 기법, 네트워크·컴퓨터 알고리즘을 이용한 기법 등 다양한 접근 방법으로 연구가 이루어지고 있다. 본 논문에서는 최근의 무선 센서 네트워크 라우팅 보안 기법의 동향을 살펴보고 이들을 비교 분석한다.

1. 서론

무선 센서 네트워크는 데이터를 수집하고자 하는 지역에 배치되는 수백 개에서 수천 개의 센서 노드로 구성된다. 센서 노드는 가격이 낮은 특성을 가지는데, 따라서 그 계산 능력, 저장 공간, 통신 능력 등이 제약되어 있다. 특히 통신 반경이 제한되어 있기 때문에 한 노드에서 목적 노드까지 메시지를 직접 전송하기 어렵다. 그러므로 무선 센서 네트워크는 적절한 라우팅 기법을 제공해야 한다.

라우팅이란 네트워크에서 메시지나 트래픽을 전송할 경로를 선택하는 과정을 말한다. 즉, 라우팅은 소스 노드로부터 최종 목적 노드까지 패킷이 전송되는 경로를 관리한다. 무선 센서 네트워크에서 라우팅 보안은 필수적이다. 네트워크에서 메시지의 암호화와 인증이 이루어지더라도 결국 그 메시지가 목적 노드까지 도달하지 않는다면 그 네트워크는 아무런 소용이 없을 것이다. 그러므로 무선 센서 네트워크는 메시지가 의도된 목적 노드까지 전달되도록 해야 한다. 그러나 기존의 많은 무선 센서 네트워크 라우팅 기법은 보안 상 취약점을 가지고 있다.

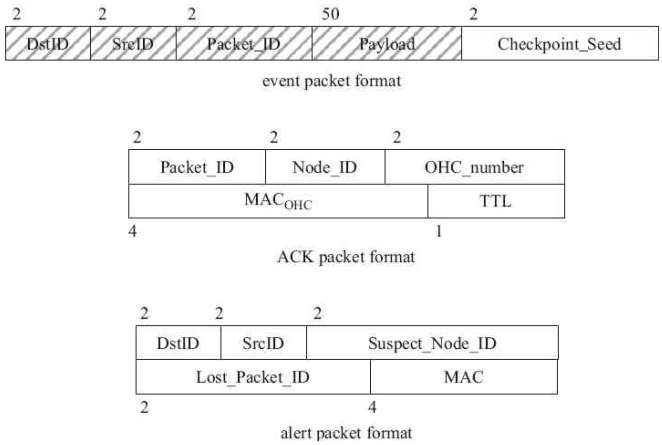
한편 무선 센서 네트워크에는 Ad-hoc 네트워크의 라우팅 기법을 적용하는 것이 적절하지 않다. 그 이유는 무선 센서 네트워크는 Ad-hoc 네트워크와 구별되는 몇 가지 특징이 있기 때문이다. 일반적으로 센서 노드는 저전력의 특성을 지니며 관리자가 직접 모니터할 수 없는 지역에 배치되는 경우가 많기 때문의 전력의 소모나 공격자의 물리적인 공격으로 인해 센서 노드가 손실되는 경우가 많다. 따라서 네트워크 토폴로지의 변화가 심하며 잦은 노드의 손실 및 추가가 이루어질 수 있어야한다. 그리고 센서 노드는 자원이 매우 제약되어 있기 때문에 기존의 라우팅 기법이 적용되기 힘들다.

최근 무선 센서 네트워크에 적합한 라우팅 보안 기법의 연구가 이루어지고 있다. 본 논문에서는 다양한 라우팅 보안에 관한 최근의 연구를 비교 분석하고 앞으로의 연구 방향을 살펴본다.

2. 여러 가지 라우팅 공격

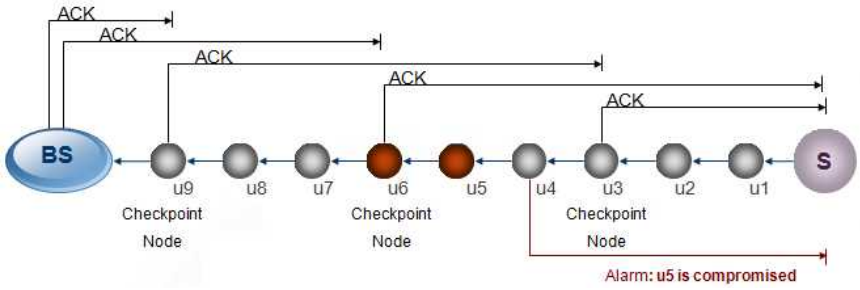
네트워크 계층에서의 공격은 다음과 같이 분류된다[1].

·라우팅 정보의 조작 및 변경
·선택적 포워딩(Selective forwarding) 공격
·싱크홀(Sinkhole) 공격
·시빌(Sybil) 공격
·웜홀(Wormhole) 공격
·DoS 공격
·ACK 조작 공격



<그림 1> CHEMAS의 패킷 형식

+ "본 연구는 정보통신부 및 정보통신연구진흥원의 대학 IT연구센터 지원사업의 연구결과로 수행되었음" (IITA-2008-(C1090-0801-0025))



<그림 2> CHEMAS: 포획된 노드 탐지

본 논문에서는 이 중 선택적 포워딩 공격과 싱크홀 공격을 중점적으로 살펴본다. 선택적 포워딩 공격이란 메시지가 전송되는 경로의 한 노드가 일부 패킷을 다음 노드에 전달하지 않고 삭제해 버리는 것을 말한다. 이렇게 공격자가 선택적으로 일부의 패킷만 삭제할 때는 전체 패킷을 삭제할 때에 비하여 그 공격을 탐지하기가 어려워진다.

싱크홀 공격에서 공격자의 목표는 포획된 노드로 주위의 대부분의 트래픽을 유도함으로써 싱크홀을 만드는 것이다. 공격자는 주변의 트래픽을 끌어옴으로써 보다 많은 데이터에 접근할 기회가 생기며 따라서 선택적 포워딩 공격을 포함한 다양한 형태의 공격을 시도할 수 있게 된다[1].

3. 선택적 포워딩 공격에 대한 보안 기법

Xiao와 Yu, Gao는 무선 센서 네트워크에서 선택적 포워딩 공격을 탐지하는 보안 기법 CHEMAS을 제안하였다[5]. 이 기법에서 사용하는 패킷 형식은 <그림 1>과 같다. 이 기법에서는 패킷이 전달되는 경로의 일부 노드들을 임의로 체크포인트(Checkpoint) 노드로 선택한다. 체크포인트 노드는 패킷을 전달받을 때 ACK 패킷을 발생시켜 이를 데이터 패킷이 전송되는 반대 방향으로 k 세그먼트(Segment)까지 전달한다. 패킷이 정상적으로 전달되었다면 그 경로의 모든 노드들은 k 개의 ACK 패킷을 받아야 하며, 만일 어떤 노드가 k개 미만의 ACK 패킷을 전송받으면 그 노드는 패킷이 삭제되었다고 판단하고 경고 패킷을 발생시켜 이를 알린다.

이 기법에서 ACK 패킷의 인증은 단방향 키 체인을 이용한다. 각 노드는 마지막 키 K_n을 임의로 선택하고 단방향 함수 F를 이용하여 $K_i = f(K_{i+1})$ 형태로 나머지 모든 키를 만든다. 이 때 K_0는 초기키로서 상호공유키(Pair-wise key)로 암호화되어 패킷 전달 경로의 노드들에게 전송됨으로써 인증을 가능하게 한다.

4. 싱크홀 공격에 대한 보안 기법

가. A secure alternate path routing in sensor networks

Lee와 Choi이 제안한 기법[2]은 암호학적 기법을 이용한 싱크홀 공격에 안전한 라우팅 기법이다. 이 기법은 일종의 멀티패스(Multipath) 기법으로 각 노드는 여러 개의 베이스 스테이션까지의 경로를 저장하여 라운드 로빈(Round robin) 형태로 각 메시지를 다른 경로를 통해 전송함으로써 라우팅 공격에 대한 피해를 최소화한다.

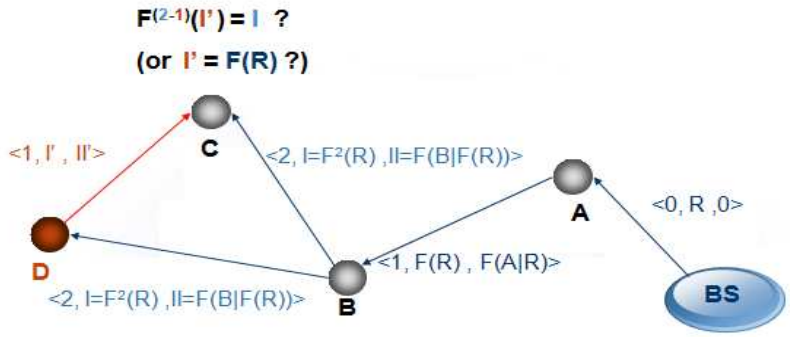
그리고 싱크홀 공격 등의 라우팅 공격을 막기 위해 Neighbor Report System을 사용한다. 이 기법에서 라우팅 업데이트 메시지는 *<Hop count, Hopping #-I, Hopping #-II>*로 구성된다. 먼저 베이스 스테이션은 임의의 수 R을 선택하고 *<0, R, 0>*를 주위 노드에 전송함으로써 라우팅 업데이트를 시작한다. 라우팅 메시지 *<h, I, II>*를 전송받은 각 노드는 *<h+1, F(I), F(ID/I)>*를 이웃 노드에게 다시 전송한다. 이때 F는 단방향 해시 함수이다. 이웃 노드 N으로부터 라우팅 메시지 *<h′, I′, II′>*을 받은 노드는 이전에 받은 메시지 *<h, I, II>*를 이용하여 다음과 같은 검사를 한다.

- $h' \le E$ (E는 지나치게 큰 h'을 막기 위해 사전 정의된 수)
- $F^{(h-h')}(I') = I$
- $F(N/I') = II$

검사한 라우팅 메시지가 위의 세 항목에 해당하지 않으면 노드는 이 메시지를 보낸 노드를 포획된 노드로 판단하고 이를 베이스 스테이션에 보고한다. 그런데 포획된 노드가 거짓된 보고를 보낼 수도 있으므로 베이스 스테이션은 보고를 받으면 해당 노드의 이웃 노드들에게 라우팅 메시지를 요청하고 이 중 다수에 해당하는 라우팅 메시지를 가지고 다음의 검사를 수행한다.

- $h' \le E$
- $F^{h'}(R) = I'$
- $F(N/F^{h'-1}(R)) = II'$

이 검사를 통과하면 잘못된 보고를 한 노드를 포획된 노드로, 통과하지 못하면 보고된 노드를 포획된 노드로 판단하여 네트워크에서 삭



<그림 3 > A secure alternate path routing in sensor networks에서의 싱크홀 노드 탐지

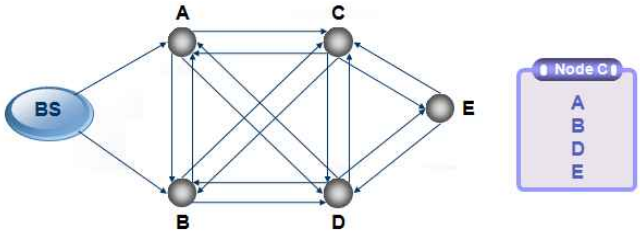
제한다.

한편 라우팅 메시지는 로컬 브로드캐스트(Local broadcast) 메시지이므로 이웃 노드들 간에 일대 다 인증이 필요한데 이는 ARMS[3]를 이용한다.

나. SEEM: Secure and energy-efficient multipath routing protocol for wireless sensor networks

Nasser와 Chen이 제안한 기법[4]은 일반적인 암호학을 사용하지 않은 라우팅 기법이다. 이 기법은 멀티패스 기법으로 무선 센서 네트워크에서 효율성이 주요한 이슈임에 초점을 맞추어 대부분의 작업을 베이스 스테이션이 처리하도록 한 효율적인 기법이다.

먼저 네트워크 토폴로지를 구성하기 위해서 베이스 스테이션은 Neighbors Discovery 메시지를 전송한다. 메시지를 받는 각 노드는 메시지에 저장된 주소를 테이블에 저장하고 메시지의 주소를 자신의 주소로 바꾼 후 이를 다시 이웃 노드들에 전송한다. 이 작업이 완료되면 <그림 4>과 같이 각 노드의 테이블에 모든 이웃 노드들이 저장되는데 베이스 스테이션에 가까운 노드일수록 테이블의 위쪽에 저장된다.



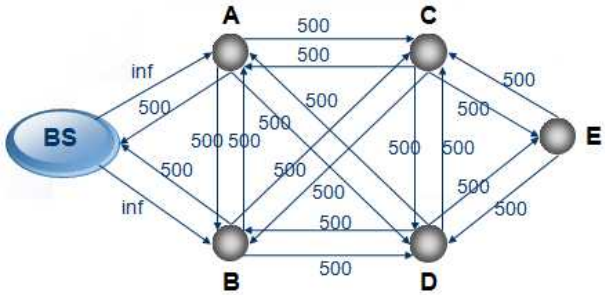
<그림 4> 이웃 노드 테이블

이와 같이 각 노드가 이웃 노드의 테이블을 저장하면 베이스 스테이션은 이 테이블을 취합한다. 베이스 스테이션은 취합한 정보로부터 전체 네트워크의 구조를 알 수 있게 되는데 이를 방향 그래프로 나타내고 각 간선의 가중치는 노드가 전달할 수 있는 총 패킷 수로 한다[그림 5].

이 기법에서 데이터의 전송은 베이스 스테이션이 요청에 따라 이루어진다. 베이스 스테이션이 요청 메시지를 전체 네트워크에 전송하면 해당 데이터를 지닌 노드는 응답 메시지를 베이스 스테이션으로 전송하는데 이 메시지는 전달 경로의 각 노드의 테이블 첫 번째 노드를 통해 전달된다. 베이스 스테이션은 응답 메시지를 보낸 노드가 데이터를 보낼 최단 경로를 그래프에서 변형된 너비우선탐색을 함으로써 결정하는데 이때 이 변형된 너비우선탐색은 기존의 너비우선탐색을 기본으로 하고 간선의 가중치, 즉 노드의 남은 에너지를 고려하여 가중치가 일정 수 이하로 낮은 간선은 선택하지 않는 방식이다. 데이터가 전송될 경로가 결정되면 그래프의 해당 간선들의 가중치를 *1*씩 감소시킨다.

이 기법은 암호학적 방법을 거의 사용하지 않음에도 불구하고 싱크홀 공격에 대하여 어느 정도의 안전성을 제공한다. 패킷이 전달되는 경로는 베이스 스테이션이 결정하며, 경로를 선택할 때 각 노드의 남은 에너지 수준을 고려하여 에너지의 균형을 맞추기 때문에 결국 네트워크의 트래픽은 전체 노드에 고르게 분산되며 싱크홀 공격은 한계를 갖게 된다.

5. 비교 분석 및 결론



<그림 5> 네트워크 구조 방향 그래프

지금까지 살펴본 기법 중 Xiao, Yu, Gao의 기법은 기존의 보안을 고려하지 않은 라우팅 기법에 보안을 추가하는 방식이며, Lee와 Choi의 기법과 Nasser와 Chen의 기법은 새로이 설계된 보안을 고려한 라우팅 기법이다.

Xiao, Yu, Gao의 기법은 선택적 포워딩 공격에 대한 보안을 제공하나 ACK 패킷의 일대 다 인증을 위하여 μTESLA 등의 인증 기법이 각 노드에 구현됨을 가정한다. 따라서 네트워크의 각 노드가 동기화되고 단방향 키 체인을 유지해야 하는 한계를 갖는다.

싱크홀 공격에 대한 보안은 앞장에서 두 가지 기법을 살펴보았다. Lee와 Choi의 기법은 싱크홀 공격을 하는 노드를 탐지해내는 보다 적극적인 형태의 보안을 제공하는데 비하여 Nasser와 Chen은 포획된 노드를 탐지하지는 않지만 네트워크 트래픽의 균형을 맞춤으로써 싱크홀 공격의 피해를 최소화한다. 한편 효율성의 측면에서는 암호학적 기법을 사용하지 않고 베이스 스테이션이 대부분의 작업을 수행하게 한 Nasser와 Chen의 기법이 더 효율적이다. 각 기법의 장단점을 정리하면 <표 1>과 같다.

	CHEMAS	Secure alternate path routing	SEEM
특징	기존 라우팅 기법에 보안 기능 추가	Neighbor report system	암호학적 기법 사용 안함
장점	선택적 포워딩 공격 탐지의 첫 논문 중 하나	높은 안전성	높은 효율성
단점	많은 가정	상대적으로 많은 계산량	포획 노드를 탐지 안함

<표 1> 여러 라우팅 보안 기법의 장단점

일반적으로 보안을 고려하지 않은 라우팅 기법을 안전하도록 수정하는 것은 힘들다[1]. Xiao, Yu, Gao의 기법은 기존의 기법에 보안 기능을 추가하였으나 각 노드에 μTESLA가 구현되어야 함을 요구한다. 무선 센서 네트워크에서의 라우팅 보안은 처음부터 보안을 고려하여 라우팅 기법을 설계하는 것이 더욱 효율적인 해결책이 될 수 있을 것이다. 한편 Lee와 Choi의 기법과 Nasser와 Chen의 기법에서 살펴본 것과 같이 일반적인 암호학적 기법을 사용한 라우팅 기법은 보다 높은 안전성을 제공하지만 상대적으로 효율성은 떨어진다. 추후 암호학적 기법과 비암호학적 기법을 적절히 혼용함으로써 안전성과 효율성의 조화를 이루는 라우팅 보안의 연구가 유효할 것이며, 응용 환경에 따라 보다 다양한 접근 방식의 연구가 이루어질 것으로 보인다.

[참고문헌]

[1] C. Karlof and D. Wagner. “Secure routing in wireless sensor networks: Attacks and countermeasures", First IEEE International Workshop on Sensor Network Protocols and Applications, pp. 113-127, May 2003.

[2] S. Lee and Y. Choi. "A secure alternate path routing in sensor networks", Computer Communications, Vol. 30, No. 1., pp. 153-165, Dec 2006.

[3] S. Lee and Y. Choi. "ARMS: An authenticated routing message in sensor networks", Secure Mobile Ad-hoc Networks and Sensors Workshop (MADNES'05), Lecture Notes in Coputer Science, Springer, Sep 2005.

[4] N. Nasser and Y. Chen. "SEEM: Secure and energy-efficient multipath routing protocol for wireless sensor networks", Computer Communications, Vol. 30, No. 11-12., pp. 2401-2412, Sep 2007.

[5] B. Xiao, B. Yu, and C. Gao, "CHEMAS: Identify suspect nodes in selective forwarding attacks", Journal of Parallel and Distributed Computing (JPDC - Elsevier), Volume 67, Issue 11, Pages 1218-1230, Nov. 2007.