ISSN : 1226-7244 (Print)
ISSN : 2288-243X (Online)
논문번호 19-02-11
64

j.inst.Korean.electr.electron.eng.Vol.23,No.2,413~418,June 2019
http://dx.doi.org/10.7471/ikeee.2019.23.2.413

WSN의 네트워크 계층에서의 공격과 탐지 및 대응 방안

Attacks, Detection, and Countermeasures in WSN Network Layer

이 다 은, 이 유 진*★

Daeun Lee, Eugene Rhee*★

Abstract

Attacks on existing sensor networks include sniffing, flooding, and spoofing attacks. The basic countermeasures include encryption and authentication methods and switching methods. Wormhole attack, HELLO flood attack, Sybil attack, sinkhole attack, and selective delivery attack are the attacks on the network layer in wireless sensor network (WSN). These attacks may not be defended by the basic countmeasures mentioned above. In this paper, new countermeasures against these attacks include periodic key changes and regular network monitoring. Moreover, we present various threats (attacks) in the network layer of wireless sensor networks and new countermeasures accordingly.

요 약

기존의 센서 네트워크 상의 공격에는 Sniffing(도청) 공격, Flood 공격, Spoofing(위조)공격 등이 있고, 이에 대한 기본적인 대응 방법에는 암호화 및 인증 방법, 스위칭 방법 등이 있다. 무선 센서 네트워크(WSN)에서 네트워크 계층에서의 공격에는 Wormhole 공격, HELLO Flood 공격, Sybil 공격, 싱크홀 공격, 선택적 전달 공격 등이 있다. 이러한 공격들은 앞서 말한 기본적인 대응방안으로 방어 되지 않는 경우가 있다. 이러한 공격들에 대한 새로운 대응방안에는 정기적인 키 변경, 정기적인 네트워크 모니터링 등의 여러 가지 방안들이 있다. 본 논문에서는 무선 센서 네트워크의 네트워크 계층의 여러 가지 위협(공격)들과 그에 따른 새로운 대응방안들에 대해 제시한다.

Key words : WSN(Wireless Sensor Network), Network Layer, Security, Threat, Solution

Ⅰ. 서론

무선 센서 네트워크는 유비쿼터스 시대를 맞이하여 전 세계적으로 활발하게 연구되고 있는, 장소에 구애받지 않고 언제 어디서나 컴퓨팅환경에 접속할 수 있는 인간 중심 지향적인 기술 중 하나이다. 무선 센서 네트워크는 기존의 네트워크와 다르게 의사소통 수단이 아닌 자동화된 원격 정보 수집을 기본 목적으로 하며, 과학적, 의학적, 군사적, 상업적용도 등 다양한 응용 개발에 활용되는 기술이다. 하지만 다양한 활용에도 불구하고 이를 사용하는데 있어서 다양한 보안 위협(공격)들이 존재한다.

* Dept. of Electronic Engineering, Sangmyung University
★ Corresponding author
E-mail : eugenerhee@smu.ac.kr, Tel : +82-41-550-5413
※ Acknowledgment
Manuscript received Jun. 4, 2019; revised Jun. 10, 2019; accepted Jun. 11, 2019.

기존의 센서 네트워크 공격에는 Sniffing(도청)공격, Flood 공격, Spoofing(위조)공격 등이 있고, 이에 대한 기본적인 대응방안에는 암호화 및 인증 방법, 스위칭 방법 등이 있다. WSN에서 네트워크 계층의 공격에는 Wormhole 공격, HELLO Flood 공격, Sybil 공격, 싱크홀 공격, 선택적 전달 공격이 있는데, 이 공격들에 대해서는 기본적인 대응방안이 통하지 않는다.

본 논문에서는 기존의 대응방안으로 대응되지 않는 WSN에서 네트워크 계층에서의 공격의 종류들에 대해 알아보고, 이에 대한 새로운 대응방안에 대해 알아본 후 결론을 맺도록 한다.

II. 본론

1. 무선 센서 네트워크(WSN)

무선 센서 네트워크(Wireless Sensor Network; WSN)는 센서로 감지가 가능하고 수집된 정보를 가공하는 프로세서가 달려 있으며, 이를 전송하는 소형 무선 송수신 장치가 달린 네트워크 시스템으로, 센서 노드(Sensor Node)와 이를 수집하여 외부로 보내는 싱크 노드(Sink Node)로 구성되어 있다. 국내에서는 유비쿼터스란 개념을 포함해 USN (Ubiquitous Sensor Network)으로 불리기도 하지만 국제적으로는 WSN으로 많이 불린다[1].

가. WSN의 구조

무선 센서 네트워크(WSN)는 센서 노드, 싱크 노드(또는 게이트웨이), 소프트웨어로 구성되어 있다.

(1) 센서 노드

센서 노드는 무선 센서 네트워크를 구성하는 기본 요소이며, 물리적인 현상을 관측하고 수집하는 센싱과 그 값을 가공해 전송하는 통신 기능을 가지고 있는 일종의 작은 장치로, 온도, 기압 등과 같은 물리, 환경 조건을 측정하기 위하여 분산, 배포된 노드이다.

(2) 싱크 노드

싱크 노드는 무선을 통해 센서 노드로부터 데이터를 수집하여 이를 중앙서비스로 전달하는 노드이다. 각각의 센서 노드에서 감지한 데이터는 싱크 노드에 의해 수집되어 인터넷 등의 외부 네트워크를 통해 사용자에게 제공되어 데이터를 활용할 수 있도록 한다.

(3) 소프트웨어

소프트웨어는 측정 및 수집된 데이터를 저장, 관리, 분석, 활용하기 위한 사용자 인터페이스이다.

나. WSN의 보안 특징

무선 센서 네트워크의 안전한 보호를 위해, WSN은 다음과 같은 보안 특징을 가진다.

(1) 기밀성

기밀성은 인가된 사용자만이 정보에 접근할 수 있는 것으로, WSN에서는 수집된 데이터가 인접 네트워크로 누출되어서는 안 된다. 노드는 매우 민감한 데이터를 전달하기 때문에 WSN에서의 보안 채널은 매우 중요하다.

(2) 무결성

무결성은 적절한 권한을 가진 사용자에 의해 인가된 방법으로만 정보를 변경할 수 있도록 하는 것으로, 한 노드에서 다른 노드로 전송된 메시지가 악의적인 중간 노드에 의해 수정되지 않도록 한다.

(3) 가용성

가용성은 네트워크 시스템에서 데이터에 대해 적절한 시간에 접근이 가능하도록 한 것으로, 시스템이 지체 없이 동작하도록 하고, 사용자가 서비스 사용을 거절당하지 않도록 한다.

2. 네트워크 OSI 계층

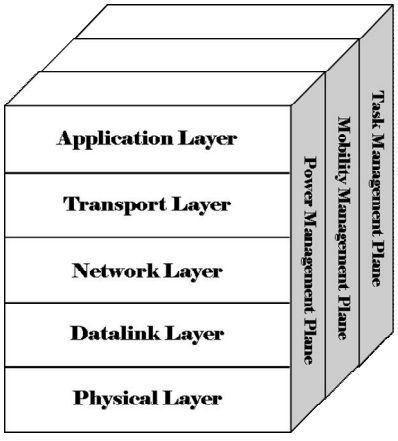

Fig. 1. Protocol Stack.
그림 1. 프로토콜 스택

네트워크를 통해 데이터를 주고 받기 위해서는 프로토콜이 필요하다. 복잡한 네트워크에서 프로토콜의 역할을 분담하기 위해 계층을 나누었으며, 이 계층화된 구조의 프로토콜 집합을 프로토콜 스택이라고 한다. 센서 네트워크에서의 프로토콜 스택은 Application Layer, Transport Layer, Network Layer, Datalink Layer, Physical Layer과 같이 기존의 프로토콜 스택과 매우 유사하며, 그림 1과 같다[2].

가. Application Layer(응용 계층)

응용 계층은 주기적으로 데이터를 수집하며 센서 네트워크의 기능을 정의한다. 구현한 것에 따라 표준 서비스 및 인터페이스 기본 요소들을 정의한다.

나. Transport Layer(전송 계층)

전송 계층은 센서 네트워크 application에 필요한 경우 데이터를 목적지까지 손실 없이 전달하는데 도움이 된다.

다. Network Layer(네트워크 계층)

네트워크 계층은 네트워크에서 데이터를 목적지까지 전송하기 위한 중간 경로를 탐색 및 지시하는 역할을 한다.

라. Datalink Layer(링크 계층)

링크 계층은 이웃한 센서 노드에게 데이터를 전달하는 역할을 하며, 신뢰성 있는 전송을 보장한다.

마. Physical Layer(물리 계층)

물리 계층은 주파수 선택, 신호 탐지, 변조 및 데이터 암호화를 담당하고, 무선 채널을 통해 데이터를 전송한다.

3. WSN에서의 네트워크 계층의 공격

제한된 노드를 사용하는 무선 센서 네트워크는 여러 가지 공격에 대해 매우 취약하다. 무선 센서 네트워크에서의 네트워크 계층에서의 공격의 종류는 다음과 같다[3].

가. Wormhole 공격

Wormhole 공격은 데이터를 전달하는 기존의 두 노드 사이에 공격자가 포획한 다른 한 노드를 통해 데이터가 전송되게 함으로써 공격자가 데이터를 도청, 위조, 손실 등을 하게 되는 공격법이다. 공격자가 노드에 대해 경로를 더 짧게 하는 방식으로 설득을 해서 네트워크를 중단시킬 수 있는 공격방법으로, 그림 2와 같다.

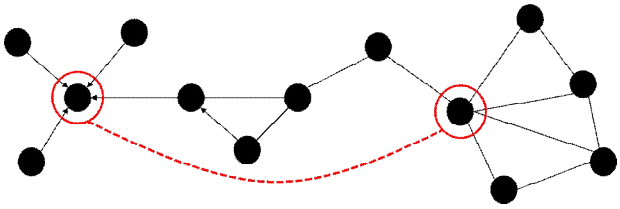

Fig. 2. Wormhole Attack.
그림 2. Wormhole 공격

나. HELLO Flood 공격

많은 프로토콜은 인접 네트워크에 HELLO 패킷을 브로드캐스팅 하기 위해 노드를 필요로 한다. HELLO 패킷을 수신하는 노드는 송신자의 정상적인 무선 범위 내에 있다고 가정할 수 있지만, 이 가정은 거짓일 수 있다. 노트북(Laptop)급 공격자가 충분한 전송 전력으로 라우팅이나 기타 정보를 브로드캐스팅 하면 네트워크의 모든 노드가 상대방이 이웃이라는 사실을 알고 정보를 교환할 수 있는데, 이것이 HELLO Flood 공격이고, 그림 3과 같다.

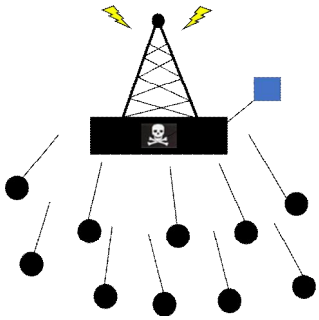

Fig. 3. HELLO Flood Attack.
그림 3. HELLO Flood 공격

다. Sybil 공격

Sybil 공격은 공격자가 어떤 특수한 목적을 이루기 위해 한 사람의 행위를 여러 사람의 행위인 것으로 속여 네트워크를 공격하는 방법으로, 그림 4와 같다. 단일 노드가 네트워크의 다른 노드에 여러 ID를 제공하므로 결함 허용(Fault Tolerant)제도의 효율성을 크게 저하시킬 수 있기 때문에 공격자가 한 번에 여러 위치에 있을 수 있다.

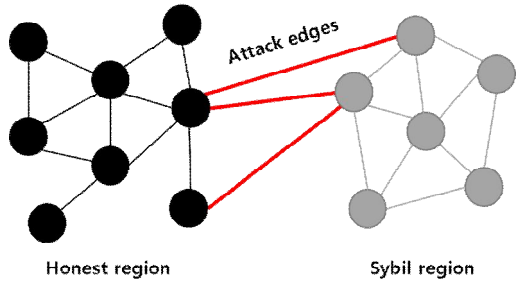

Fig. 4. Sybil Attack.
그림 4. Sybil 공격

라. 싱크홀 공격

싱크홀 공격은 공격자가 주위의 노드 중 특정 손상된 노드를 통해 공격자를 중심으로 싱크홀을 만들어 트래픽을 유인하는 공격으로, 그림 5와 같다. 근처에 있는 노드는 응용 프로그램 데이터를 조작할 기회가 많기 때문에 싱크홀 공격은 패킷이 따르는 경로 상에서 선택적 포워딩 공격 같은 다른 많은 공격을 할 수 있다.

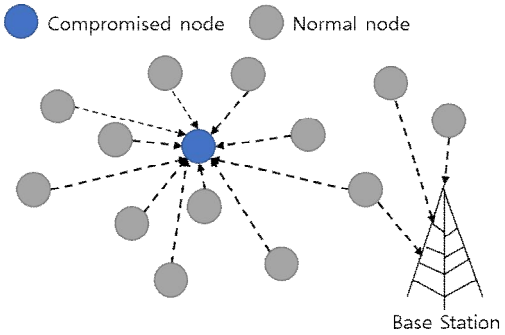

Fig. 5. Sinkhole Attack.
그림 5. 싱크홀 공격

마. 선택적 전달 공격

선택적 전달 공격은 블랙홀처럼 행동하고, 특정 메시지를 전달하지 않고 간단히 삭제하여 더 이상 전파되지 않도록 하는 공격으로, 블랙홀 공격이라고 부르기도 하며, 그림 6과 같다. 공격자는 인접한 노드가 실패했다고 판단하여 다른 경로를 찾는데 따르는 위험을 감수해야 한다. 이 공격의 파악하기 어려운 형태는 상대방이 선택적으로 패킷을 전달할 때 발생한다. 일부의 선택된 노드에서 시작된 패킷을 억제하는데 관심이 있는 상대방은 나머지 트래픽을 안정적으로 전달함으로써 잘못된 행동에 대한 의혹을 제한할 수 있다.

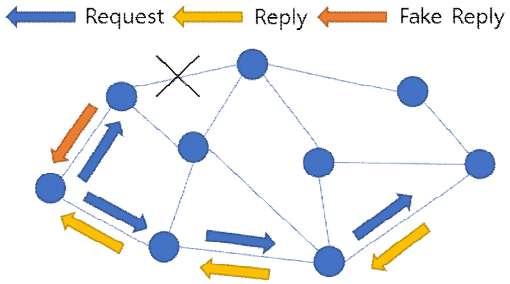

Fig. 6. Selective Forwarding.
그림 6. 선택적 전달 공격

4. 공격에 대한 대응방안

대부분의 외부 공격은 암호화 및 인증을 통해 대응할 수 있다. 하지만 앞의 내용과 같은 네트워크 계층에서의 공격들, 특히 Wormhole 공격과 HELLO Flood 공격에 대해서는 암호화 및 인증과 같은 기본적인 대응방안들로는 대응이 되지 않으며, 이에 대한 새로운 대응방안들이 존재한다. 본 논문에서 제안하는 새로운 대응방안은 다음과 같다.

가. Wormhole 공격에 대한 방안

Wormhole 공격은 필드 장치의 물리적 모니터링 및 소스 라우팅(송신 경로 지정)을 이용한 네트워크의 정기적인 모니터링을 통해 방어할 수 있으며, 모니터링 시스템은 패킷 침출 기술(패킷을 걸러내는 기술)을 사용할 수 있다. Wormhole 공격은 싱크홀 공격과 조합하여 사용되는 경우 방어하기가 어렵고, 기본 센서 네트워크에 보이지 않는 사설 대역 외 채널을 사용하기 때문에 탐지하기가 어렵다. Wormhole 공격을 막는 일반적인 접근 방법은 합법적인 노드가 패킷을 보낸 시점부터 수신자가 패킷을 수신한 지점까지의 시간인 패킷 전파 지연을 측정하고 지나치게 멀리 이동한 패킷을 사용하는 것이다. 하지만 이것은 엄격한 시간 동기화가 필요하기 때문에 대부분의 센서 네트워크에서는 실행이 불가능하다. 이러한 공격에 대해 기존의 프로토콜을 바꾸는 것은 어렵기 때문에 웜홀과 싱크홀이 의미가 없는 라우팅 프로토콜을 주의하여 설계하는 것이 좋다[4].

나. HELLO Flood 공격에 대한 방안

HELLO Flood 공격은 링크를 통해 수신된 메시지를 기반으로 적당한 조치를 취하기 전에 링크의 양방향성을 확인함으로써 방어할 수 있다. 신원 확

인 프로토콜은 HELLO Flood 공격을 막기에 충분하다. 두 노드 사이의 양방향 링크를 확인할 뿐만 아니라, 공격자가 민감한 수신자를 가지고 있거나 네트워크의 여러 위치에 웜홀이 있는 경우에도 각 노드에 대해 인접한 노드의 수를 제한하는 신뢰할 수 있는 기지국은 적은 수의 노드가 훼손된 경우 네트워크의 큰 부분에서 HELLO Flood 공격을 막을 수 있다.

다. Sybil 공격에 대한 방안

Sybil 공격은 장치 재설정 및 세션 키 변경을 통해 방어할 수 있다. 공격자가 네트워크에 참여하는 것을 막을 수 없지만, 손상된 노드의 ID를 사용하여 막을 수 있어야 한다. 전역적으로 공유되는 키를 사용하면 공격자가 임의의 노드로 가장할 수 있고, 심지어는 존재하지 않는 노드로 가장할 수 있다. 따라서 신원이 반드시 확인되어야 한다. 기존의 설정에서 이것은 공개 키 암호화를 통해 해결될 수 있지만, 디지털 서명을 생성하고 확인하는 것은 센서 노드의 기능을 넘어선다. 한 가지 해결책은 모든 노드가 신뢰할 수 있는 기지국과 암호화와 복호화에 같은 암호를 사용하는 방식인 고유한 대칭 키를 공유하도록 하는 것이다. 그 다음 두 노드는 대칭 키와 인증 서버의 개념을 사용하여 제안한 키 교환 프로토콜인 Needham-Schroeder 프로토콜을 사용하여 서로의 신원을 확인하고 공유 키를 설정할 수 있다. 한 쌍의 인접 노드는 결과 키를 사용하여 두 노드 사이의 인증된 암호화 링크를 구현할 수 있다. 공격자가 고정된 네트워크 주변을 배회하고 네트워크의 모든 노드와 공유 키를 설정하는 것을 방지하기 위해 기지국은 노드가 허용하는 인접 노드의 수를 합리적으로 제한하고 노드가 이것을 초과하게 되면 오류 메시지를 보낼 수 있다. 따라서 노드가 손상된 경우에는 검증된 인접 노드와만 소통할 수 있도록 제한된다. 이것은 노드가 여러 개의 홉으로 떨어져 있는 기지국이나 집적 지점으로 메시지를 보내는 것이 금지된 것은 아니지만, 확인된 인접 노드가 아닌 다른 노드를 사용하여 메시지를 보내는 것은 제한된다. 그리고 공격자가 웜홀을 이용하여 두 노드 사이에 인공적인 링크를 만들어 이웃 노드라고 확신시킬 수 있지만, 공격자는 그 사이에서 도청하거나 수정할 수 없다[5].

라. 싱크홀 공격에 대한 방안

싱크홀 공격에 대해서는 센서 네트워크의 링크 품질 지표에 기초한 감지 방법이 있다. 이 방법은 링크 품질에 기반한 라우팅인 LQI(Link Quality Indicator) 기본 라우팅과 몇몇 탐지 노드를 사용하여 싱크홀 공격을 탐지할 수 있다. 싱크홀 공격에서는 홉 수를 사용하여 악의적인 노드를 탐지할 수 있으며, 이 방법은 기지국과의 협상이 없이도 악의적인 노드를 탐지할 수 있다[6-8].

마. 선택적 전달 공격에 대한 방안

선택적 전달 공격은 소스 라우팅을 이용한 정기적인 네트워크 모니터링 기술을 통해 방어할 수 있다. 싱크홀, 웜홀, Sybil 공격에 완전히 거부된 프로토콜의 경우에도 손상된 노드는 소스 또는 기지국 근처에 위치한 경우 데이터 흐름에 자체를 포함하여 선택적 전달 공격을 시작할 가능성이 크다. 다중 경로 라우팅은 이러한 유형의 공격에 대응할 수 있다. 노드와 완전히 분리된 경로를 통해 전달된 메시지는 손상된 노드와 관련된 선택적 전달 공격으로부터 완전히 보호되며, 노드가 손상될 때마다 잠재적인 보호 기능을 제공한다. 하지만 완전히 분리 된 경로를 만드는 것은 어려우며, 꼬여진 경로는 공동으로 노드를 가지고 있지만 공동의 링크는 없다. 이 꼬인 경로는 공동으로 2개가 연속된 노드가 없다. 다중 편조 경로의 사용은 선택적 전달 공격에 대해 확률적인 보호를 제공하고, 오직 지역화된 정보만을 사용할 수 있다[9, 10].

Ⅲ. 결론

센서를 네트워크로 구성한 기술인 무선 센서 네트워크는 전 세계적으로 다양한 분야에서 제품 및 프로그램 개발에 활용되고 있다. 무선 센서 네트워크에서의 위협들에는 Wormhole 공격, HELLO Flood 공격, Sybil 공격, 싱크홀 공격, 선택적 전달 공격이 있다. 이 공격들은 암호화 또는 스위칭 방법 같은 기존의 네트워크 공격 대응 방안으로는 대응되지 않으며, 소스 라우팅을 이용한 정기적 네트워크 모니터링, 키 변경 방법, 또는 프로토콜의 신중한 설계와 같은 대응 방안으로 탐지 및 방어될 수 있다. 무선 센서 네트워크는 기존 네트워크에 비해 취약해 강력한 보안이 요구되며, 안전한 활용을 위해

위의 대응방안 외에도 더 새롭고 완벽한 대응방안에 대한 연구가 필요하다.

References

[1] D. Boyle and T. Newe, “Securing Wireless Sensor Networks: Security Architectures,” *Journal Of Networks*, Vol.3, No.1, pp.65-77, 2008.

[2] S. Nithya, K. VijayaLakshmi, and V. PadmaPriya, “A Review of Network Layer Attacks and Countermeasures in WSN,” *IOSR Journal of Electronics and Communication Engineering,* Vol.10, Issue.6, pp.10-15, 2015.

[3] H. K. Kalita and A. Kar, “Wireless Sensor Network Security Analysis,” *International Journal of Computer Science & Information Technology,* Vol.1, No.1, pp.1-10, 2009.

[4] N. Sharma1 and U. Singh, “Various Approaches to Detect Wormhole Attack in Wireless Sensor Networks,” *International Journal of Computer Science and Mobile Computing,* Vol.3, Issue.2, pp.29-33, 2014.

[5] A. M. Abdul and S. Umar, “Attacks of Denial-of-Service on Networks Layer of OSI Model and Maintaining of Security,” *Indonesian Journal of Electrical Engineering and Computer Science* Vol.5, No.1, pp.181-186, 2017.

[6] M. Ibrahim and M. Muntasir, “Detecting Sink Hole Attacks in WSN using Hop Count,” *Computer Networks and Information Security,* Vol.3, pp.50-56, 2015.

[7] H. Shafiei, A. Khonsari, H. Derakhshi, and P. Mousavi, “Detection and Mitigation of Sinkhole Attacks in Wireless Sensor Networks,” *Journal of Computer and System Sciences*, Vol.80, Issue.3, pp.644-653, 2014.

[8] G. W. Kibirige and C. Sanga, “A Survey on Detection of Sinkhole Attack in Wireless Sensor Network,” *International Journal of Computer Science and Information Security,* Vol.13, No.5, pp.1-9, 2015.

[9] J. Shokeen, P. Palak, and P. Devi, “A Survey on Selective Forwarding Attacks in Wireless Sensor Networks,” *International Journal of Computer Science and Mobile Computing*, Vol.5, Issue.8, pp.45 - 50, 2016.

[10] J. Singh and A. Gupta, “Different Approaches to Mitigate Selective Forwarding Attacks in WSN,” *International Journal of Innovations in Engineering and Technology*, Vol.3, pp.40-46, 2014.

BIOGRAPHY

Daeun Lee (Member)

2016~ : Information Telecommunication Engineering, Sangmyung University.

Eugene Rhee (Member)

2001 : BS degree in Electronic Engineering, Hanyang University.
2003 : MS degree in Electronic Engineering, Hanyang University.
2010 : PhD degree in Electronic Engineering, Hanyang University.
2012~present : Associate Professor, Sangmyung University.