중소기업융합학회 논문지 제4권 제4호 pp. 1-6, 2014 ISSN 2234-4438

무선 센서 네트워크 보안 위협 및 대응책 연구

홍성혁[1*]
[1]백석대학교 정보통신학부

Research on Wireless Sensor Networks Security Attack and Countermeasures: Survey

Sunghyuck Hong[1*]
1Division of Information and Communication, Baekseok University

요 약 무선 센서 네트워크는 여러 지역에 퍼져 있는 다수의 센서 노드들이 무선 방식으로 연결 되어있는 그물망으로 전 세계에서 연구되고 있는 기술 중 하나이다. 그러나 자원의 제약성, 무선 통신 사용 등, 네트워크 자체적인 특성으로 인해 일반 네트워크에 비해서 보안이 매우 취약하다. 무선 센서 네트워크의 공격법은 크게 도청기반 공격, 위조기반 공격, 서비스 거부 기반 공격으로 나누어지며, 보안법으로 대개의 Sensor Network Application은 전송되는 정보의 도청 또는 수정, 잘못된 정보의 삽입 등 여러가지 공격으로부터 방어를 해야 할 필요가 있다. 이를 위한 기본적인 방법은 암호화 방법, 스위칭 기법 등을 서술 한다.

키워드 : 무선 센서 네트워크 보안, 센서 노드, 무선네트워크 보안, 사이버 공격, 사이버 보안

Abstract A wireless sensor network is being actively researched around the world that are connected to the mesh are a plurality of sensor nodes in a wireless manner that span different regions of the techniques. However, wireless communications use the limitation of resources, so it is very weak due to the properties of the network itself secure in comparison to the normal network. Wireless sensor network is divided into tapped-based attacks, forgery based attacks, denial of service attacks based largely by securities laws must defend against various attacks such as insertion of the wrong information being sent eavesdropping or modification of information, which is usually sensor network applications need to do. The countermeasure of sensor network attack is described in this research, and it will contribute to establish a secure sensor network communication.

Key Words : Wireless sensor networks security, Sensor node, Wireless networks security, cyber attack, cyber security

1. 서론

무선 센서 네트워크(Wireless Sensor Network, WSN)는 다수의 소형 센서 노드를 무선으로 연결한 통신망을 일컬으며 최근 인간 중심 지향적이면서 장소에 얽매이지 않고 언제 어느 곳 에서나 컴퓨팅 환경에 접속할 수 있는 Ubiquitous 패러다임이 확장되면서 전 세계에서 적극적으로 연구되고 있는 기술 중의 하나이다 [1][2].

본 연구 구성은 2장에서 무선 센서 네트워크 그리고 무선 센서 네트워크 운용시에 발생 하는 공격과 취약점에 관하여 기술 하고 3장에서는 2장에서 기술한 것에 대한 대응 방안을 기술 하였다. 마지막으로 4장에서는 결론

Received 2014-10-10 Revised 2014-10-24 Accepted 2014-11-15
*Corresponding author : Sunghyuck Hong (shong@bu.ac.kr)

을 서술함으로 본 연구의 마무리를 맺는다.

2. 무선 센서 네트워크

2.1 무선 센서 네트워크

무선 센서 네트워크(WSN)란 센서로 센싱이 가능하며 수집된 정보를 가공하는 프로세서가 달려 있다 [3][4]. 또한 센서 노드들 간에 형성된 무선 네트워크를 이용하여 정보를 얻어, 그 환경을 모니터링 하고 통제할 수 있게 해주는 기술이며, 기존의 네트워크와는 달리 의사소통의 수단이 아니라 자동화된 원격 정보의 수집을 기본 목적으로 해, 과학적·의학적·군사적·상업적 용도 등 여러 응용 개발에 널리 활용되고 있다 [9].

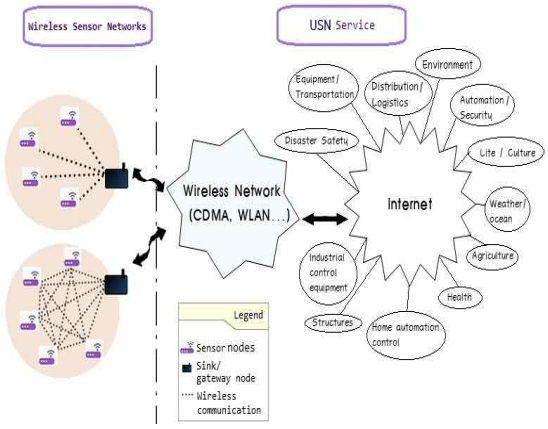

Fig. 1. 무선센서네트워크의 구조

2.1.1 WSN의 구성

1. 센서(Sensor) 노드 : 환경에 관한 정보를 수집해서, 센싱 정보, 데이터 센싱을 디지털 신호로 변형하기 위한 ADC(Analog to Digital Convertor), 프로세스, 메모리, 배터리와 데이터 송·수신을 위한 무선 트랜시버 등으로 구성이 되어 있다 [11].

2. 싱크(Sink) 노드 : 센서노드들의 데이터를 수집해, 인터넷 등의 네트워크를 통해서 사용자에게 제공하고, 센서 노드의 제어를 한다.

2.1.2 WSN의 주요 특징

기존의 통신 인프라 없이 현장에서 즉시 구축할 수 있어야 하며, 토폴로지가 동적이며, 노드의 특성상 컴퓨팅 파워가 한정되 에너지 효율성이 매우 중요하다는 특징을 가지고 있다 [12].

1) 장애 내성

센서노드들은 전력의 부족이나 물리적 손상, 환경적인 방해 요소들로 인한 동작 멈춤의 경우가 나타난다. 그러나 몇몇의 센서 노드들의 고정이 전체 센서네트워크에 영향을 주면 안 된다 [5][6].

2) 확장성

요구되는 노드의 수가 ad hoc 네트워크와는 다르게 어플리케이션에 따라서 수백에서 수천, 수만에 이르기까지 매우 많아질 수 있다. 그러므로 센서 네트워크 프로토콜은 이러한 네트워크 규모와는 관련 없이 잘 동작할 수 있어야 한다 [7].

3) 저가격

매우 많은 수의 센서 노드가 사용이 되므로 노드의 가격은 매우 저렴해야 한다. 그러므로 센서 네트워크 설계 시 가격에 영향을 미치는 고기능 고 사양을 요청하는 설계는 지양하도록 해야 한다 [8].

4) 저전력 소모

무선 센서 노드는 제한되어있는 에너지 공급원을 가지고 있으므로 네트워크 토폴로지의 변형이나 다른 요인들로 인하여 네트워크의 재구성, 패킷의 재전송을 수행하는 데에 있어 에너지 사용을 최소화해야 한다. (여기에서 에너지는 대부분 Sensing, RF통신, 데이터처리에 사용이 된다 [10].

5) 강인한 구조의 동작 환경

센서 네트워크는 유저의 접근이 쉽지 않은 곳 즉 지역적으로 먼 곳에 설치돼 동작될 수 있으며, 자연에 그대로 드러난 상태로 동작하기 때문에 센서 네트워크는 이런 열약한 동작 환경을 고려하여 설계되야 한다.[2]

2.2 WSN운용시 발생하는 취약점

2.2.1 에너지(Energy)

불법 노드로 의한 강권된 데이터 수집·전송·처리로 인하여 특별히 지정한 지역의 정상 노드의 에너지

소비를 강권하고 공갈시키는 공격에 취약하며, 해당 지역 센싱을 할 수 있는 정상 노드가 없는 현상(센싱 홀)이 나타난다.

2.2.2 구성(Topology)

센서 네트워크의 연결 형태, 구성에 따라 각 노드(싱크, 센서, 게이트웨이)에 대한 보안 취약 지점이 판이하게 발생한다.

2.2.3 이동성(Mobility)

노드(센서, 싱크 등) 이동에 의한 센서 네트워크 구성 및 노드 인증 에 취약하며, 핑퐁(ping-pong) 현상에도 취약하다.(노드 에너지 고갈 발생)

2.2.4 연결성(Connectivity)

노드(센서, 싱크)의 이동에 따른 핑퐁 현상에 취약하고, 불법적 노드 침입 및 접속을 유발하는 공격에도 취약하다 [14][15].

2.2.5 위치 및 영역(Deployment)

노드의 데이터 수집과 전송 영역이 매우 클 경우 내부 정보(네트워크의 위치 및 센서노드)의 유출에 취약하고, 사용자 거부나 노드 물리적 도난, 해킹 및 불법적 위치 추적 에 취약하다.

2.2.6 기능 및 매체(Heterogeneity)

전파방해(jamming) 및 전파차단 등의 물리적 공격과 정보 수집의 정확성에 대해서 취약하다.

2.3 WSN공격

2.3.1 센서 네트워크 공격 유형 용어

도청(Sniffing) 공격
- 센서네트워크 상에서 전송되는 시호를 도청

플러드(Flood) 공격
- 센서 네트워크에 필요하지 않은 반복적인 신호를 전송함

스캔(Scan) 공격
- 센서 네트워크에 필요 없는 신호를 전송하며 그 응답 신호를 활용하여 공격함

보충하자면 응답신호에는 노드 및 센서 네트워크 정보(키 노드, 노드 ID, 네트워크 등) 포함된다.

죽음의 핑(Ping of death) 공격
- 센서 네트워크에 허용범위 이상의 크기 신호를 반복 전송하여 공격한다.

위조(Spoofing) 공격
- 정상적인 노드를 가장하여 센서 네트워크를 공격함

랜드(Land) 공격
- 도청, 위조 공격을 활용해서 센서 네트워크를 공격함

서비스 거부(Dos) / 분산 서비스 거부(DDos)
- 센서 네트워크에 불법적 대량의 신호를 전송하여 센서 네트워크를 공격함

세션 하이재킹(Session Hijacking) &MITM 공격
- 도청, 위조 공격을 활용하여 센서 네트워크르르 공격함

Fake Access Point 공격
- 불법적인 노드(싱크/게이트웨이 역할) 주입을 통해 센서 네트워크 공격

물리적인 노드 공격
- 노드에 대한 물리적 파괴 및 절취, 전파방해 등의 방법을 통해 공격

Table 1. 단일 공격 유형

Single attack type
Taps
Forged
Flood
Scan
Ping of Death
Land
Rejected (distributed) service
MITM / session hijacking
Camouflage access point
Physics

이렇게 10가지의 단일 공격 유형이 있으며 이를 복합적으로 분류하여 네 가지의 복합 공격 유형으로 만든 것이 Table 2 이다 [13].

Table 2. 복합 공격 유형

Composite attack type	
Taps	Scan
	Session Hijacking
Forged	MITM
	Camouflage access point
(Distributed) Denial of Service	Flood
	Ping of Death
	Land
Physics	Jamming / blocking, cut, Damaged, the cable connection

2.3.2 도청기반(Sniffing) 공격

도청기반 공격이란, 네트웍 트래픽을 모니터링하여 중요한 정보를 찾아내는 것을 말한다.

대부분의 루트킷(rootkit)에는 스니퍼(sniffer)가 들어있고 스니핑 방법은 다음과 같다.

이전 : 허브에 연결해 네트워크 인터페이스 카드를 promiscuous 모드로 변경

최근 : 스위치 활용으로 인하여 promiscuous 모드 스니핑이 불가능

2.3.3 위조(Spoofing)기반 공격

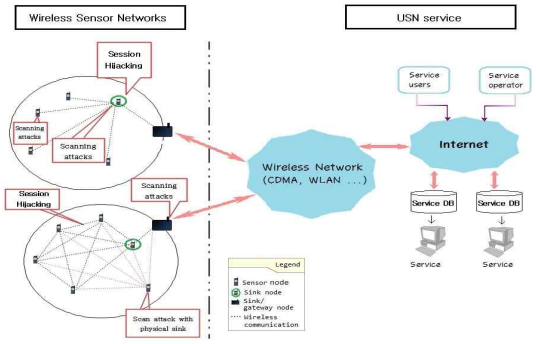

Fig. 2. 도청기반 공격

위조기반 공격이란, 주체를 속이는 것이며, 주체 검사 단계에 대한 능동적 공격을 말한다. 또한, 통신의 모든 계층에서 가능하고, 항상 고의적며 배신과는 다르고, 반드시 악의적인 것이 아니며, 새로운 것도 아니다.

Meike Keao : 시스템과 서비스에 접근하기 위해서 주체에 대한 그릇된 정보를 제공하는 것이며, TCP/IP 프로토콜의 구조적 결함, 다시말해 TCP 시퀀스 번호, 소스 어드레스, 소스 라우팅을 이용한 인증 메커니즘 등을 이용한 방법이며, 인증 기능을 지니고 있는 시스템에 침입하기 위해서 침입자가 이용하는 시스템을 신뢰성 있는 호스트로 가장하는 방법이다.

2.3.4 서비스 거부 기반 공격

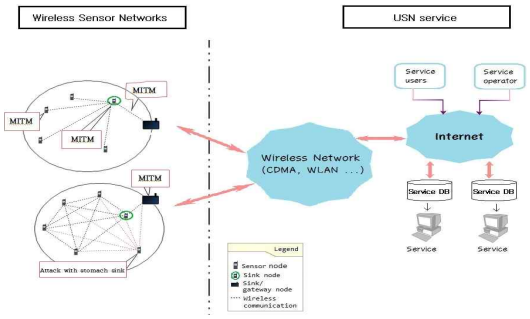

Fig. 3. 위조기반 공격

서비스 거부 기반 공격이란, 공격자가 호스트의 Hardware나 Software 등을 무력하게 만들어 호스트에서 법규에 맞는 사용자의 서비스 요청을 거부하도록 만드는 일련의 행위로 공격의 원인 및 원천지를 찾기 힘드며, 공격 방법이 아주 다양하고, 단순한 공격 방법이 많아서 누구나 쉽게 이용가능하다. 또한 뚜렷한 방지 대책이 없고, 근래 네트워크를 이용한 원격 DOS 공격 급격히 증가하고 있다 [7].

DoS 공격의 형태로는 디스크 채우기, 프로세스 만들기, 메일폭탄, 메모리 고갈 - anonmail, Buffer Overflow, kabomb,, Ping Flooding, SYN Flooding, 등이 있다. DoS 공격 도구로는 Blood Lust, Bitch Slap, Click, Cyber가 있다.[3]

3. 무선 센서 네트워크 보안

3.1 도청(Sniffing) 기반 공격 보안

3.1.1 암호화 방법

(Secure Shell, SSH)은 네트워크 상에서 다른 컴퓨터에 로그인 또는 원격 시스템에서 명령을 실행해 다른 시스템으로 파일을 복사할 수 있게 해 주는 응용프로그램이며, 막강한 인증 방법 또는 안전하지 못한 네트워크에

서 안전하게 통신 할 수 있는 기능을 제공한다.

(Secure Socket Layer, SSL)은 전자상거래 등의 보안을 위해 개발 하였다.

SSL은 특히 전송계층 (Transport Layer)의 암호화 방식이기 때문에 HTTP, FTP등 응용계층 프로토콜의 종류에 상관없이 사용할 수 있어 보안에 용이하다.

PGP, S/MIME SMTP 상으로 보내지는 메일은 기본적으로 암호화가 되지 않기 때문에 Sniffing해서 그 내용을 쉽게 얻을 수가 있다. PGP, S/MIME 등을 이용해서 메일에 대해 암호화 기능을 한다.

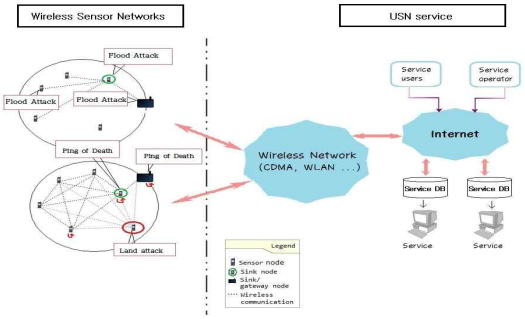

Fig. 4. 서비스거부기반 공격

3.1.2 암호화 방법스위칭 기법 사용

스위칭 기법은 기본적으로 Layer 2 헤더 정보인 MAC 주소 정보를 이용해서 패킷이 어떠한 목적지로 보내질 것인지 결정한다.

따라서 허브환경에서와는 달리 패킷은 실제 수신 대상에게만 보내지게 되고, 공격 대상이 암만 인터페이스를 Promiscuous 모드로 세팅하였다 해도 내용을 훔쳐 볼 수 없다.

3.2 위조(Spoofing) 기반 공격 보안

3.2.1 Spoofing 예방 방법

Static ARP Table으로 설정

ARP Table은 자동과 수동으로 설정이 가능하며 수동으로 설정 할 경우 ARP Cache 테이블의 정보를 변정하지 못한다, 그러나 이중 게이트웨이가 네트워크에 실존할 시에는 사용할 수 없다.

Spoofing은 예방 할 수 있지만, 불편한 방법으로는 IP로 인증하는 서비스는 사용하지 않아야한다. 암호화된 Protocol을 사용하면 Spoofing공격을 상당수 차단할 수 있지만 속도가 느려지는 단점이 있다.

3.2.2 Spoofing 보안 방법

네트워크 관리자로서 감염 대상 파악은 가장 요한 것이다. ARP Spoofing이 처음 발견되면 빠른 시간 안에 MAC 주소를 모니터링 해서 주 감염원을 찾아 네트워크 라인을 네트워크에서 제거해야한다. PC가 하나의 MAC 주소에 2개 이상의 IP를 가졌다면 해당 MAC 주소의 장비를 검사 한다. 그리고 모든 PC에 대해 최신에 백신으로 치료를 이행하고 주 감염 PC는 자료를 백업한 뒤에 O/S를 재 설치하게 해야 한다.

3.3 서비스 거부(DoS) 기반 공격 보안

공격자는 Dos공격을 통해 무선 센서 네트워크의 성능을 떨어뜨린다. 가장 단순한 Dos공격 형태는 공격자가 높은 에너지 신호를 브로드 캐스팅해서 네트워크의 동작과 기능을 마비시키거나 혼란시키는 것이다. 공격자가 802.11 매체접근제어 프로토콜을 방해해서 통신을 못하게 하는 더욱 강력한 공격도 가능하다. 이러한 공격을 방어하는 표준 중 하나는 스펙트럼 확산 통신 (spread-spectrum-communication)이다. 하지만, 이는 암호학적으로 안전하기는 하지만 상용가능한 것이 아니며, 공격자가 노드를 직접 포획하여 암호학 적인 키를 얻어낼 경우는 안전하지 않다. 스펙트럼 확산통신 이외에 센서네트워크의 속성으로 인한 새로운 방어가 가능하다. 전파방해가 단지 네트워크의 어떠한 부분에서만 영향을 미칠 경우, 전파 방해에 대해 저항력있는 네트워크는 전파 방해와 영향 받은 지역을 탐지해 그 지역 주변을 라우팅 해 방어가 가능하다.[4]

4. 결론

WSN는 센서를 네트워크로 구성한 것으로, 센서노드와 싱크노드로 구성된 네트워크이다. 또한 센서로 센싱이 가능하며 센서 노드들 간에 형성된 무선 네트워크를 이용하여 정보를 얻어, 그 환경을 모니터링 하고 통할 수 있게 해주는 기술이며, 주요 공격 방법으로는 Sniffing, Spoofing, DoS등이 있고, 이외에도 다양한 공격 법이 존재한다.

다만 WSN는 일반 네트워크에 비해서 보안이 매우 취

약해 사용자들은 관심을 갖고 암호화, 빠른 감염대상 파악, 최신 백신 치료, 전파방해를 받은 지역을 탐지해 그 주변은 라우팅 하는 등의 방법을 이용하여 자주 점검하고, 관리해야 한다.

REFERENCES

[1] N. A. Boudriga, M. Baghdadi, and M. S. Obaidat, “A New Scheme for Mobility, Sensing, and Security Management in Wireless Ad Hoc Sensor Networks,” In Proceedings of the 39th Annual Symposium on Simulation, pp. 61 - 67, 2006.

[2] P. Barooah, H. Chenji, R. Stoleru and T. Kalm´ar – Nagy, “Cut Detection in Wireless Sensor Networks,” In IEEE Transactions on Parallel and Distributed Systems, vol. 23, no. 3, March 2012

[3] E. Sabbah, A. Majeed, K. D. Kang, K. Liu, and N. Abu-Ghazaleh, “An Application-Driven Perspective on Wireless Sensor Network Security,” In Proceedings of the 2nd ACM International Workshop on Quality of Service & Security for Wireless and Mobile Networks, pp. 1 - 8, 2006.

[4] S. Ransom, D. Pfisterer, and S. Fischer, Comprehensible Security Synthesis for Wireless Sensor Networks,” In Proceedings of the 3rd International Workshop on Middleware for Sensor Networks, pp. 19 - 24, 2008.

[5] J. Albath and S. Madria, “Practical Algorithm for Data Security (PADS) in Wireless Sensor Networks,” In Proceedings of the 6th ACM International Workshop on Data Engineering for Wireless and Mobile Access, pp. 9 - 16, 2007.

[6] W. Stallings, Cryptography and Network Security: Principles and Practice, Fifth edition, Pearson Education, 2011.

[7] IEEE, IEEE Standard 1363-2000, Standard Specifications for Public Key Cryptography, 2000.

[8] A. Perrig, J. Stankovic, and D. Wagner, “Security in Wireless Sensor Networks,” Communications of the ACM, 47(6):53 - 57, June 2004.

[9] H. Yang, F. Ye, Y. Yuan, S. Lu, and W. Arbaugh, “Toward Resilient Security in Wireless Sensor Networks,” In Proceedings of the 6th ACM International Symposium on Mobile Ad Hoc Networking and Computing, pp. 34 - 45, 2005.

[10] J. Deng, R. Han, and S. Mishra, “Security Support for In-Network Processing in Wireless Sensor Networks,” In Proceedings of the 1st ACM Workshop on Security of Ad Hoc and Sensor Networks, pp. 83 - 93, 2003.

[11] J. Paradells, J. Vilaseca, and J. Casademont, “Improving Security Applications Using Indoor Location Systems on Wireless Sensor Networks,” In Proceedings of the International Conference on Advances in Computing, Communication, and Control, pp. 689 - 695, 2009.

[12] O. Yagan and A. M. Makowski, "Connectivity in Random Graphs Induced by A Key Pre distribution Scheme - Small Key Pools," IEEE 978-1-4244-7417-2-10-2010.

[13] O. Yagan and A. M. Makowski, "Key Ring Sizes in The Random Pairwise Key Distribution Scheme," submitted for inclusion in the program of the Twenty-second Annual IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC 2011), Toronto (ON, Canada), September 2011.

[14] N. Shrivastava, S. Suri, C.D. T\oth, "Detecting Cuts in Sensor Networks," In: IPSN, pp. 210-217. IEEE, Los Alamitos (2005).

[15] Sunghyuck Hong, “Analysis of DDoS Attack and Countermeasure: Survey,” Journal of Digital Convergence, vol. 12, no. 1, pp. 423-429

저 자 소 개

홍 성 혁(Hong, Sunghyuck) [종신회원]

- 1995년 2월 : 명지대학교 컴퓨터 공학과 (공학사)
- 2007년 8월 : Texas Tech University, Computer Science (공학박사)
- 2012년 3월 ~ 현재 : 백석대학교, 정보통신학부 교수

<관심분야> : 네트워크 보안, 센서네트워크