論 文

홈 네트워크에서의 USN 보안 고려 사항 분석

USN Security Considerations in Home Network

박우출*, 박현문**, 이명수***, 윤명현***
Woo Chool Park*, Hyun Mun Park**, Myung Soo Lee***, Myung Hyun Yoon***

Abstract - Because sensor networks use wireless communication, they are vulnerable to attacks which are more difficult launch in the wired domain. Many wired networks benefit from their inherent physical security properties. It is unlikely that an adversary will dig up the Internet backbone and splice into the line. However, wireless communications are difficult to protect; they are by nature a broadcast medium. In a broadcast medium, adversaries can easily eavesdrop on, intercept, inject, and alter transmitted data. In addition, adversaries are not restricted to using sensor network hardware. We have analyzed the IEEE 802.15.4, ZigBee specification which includes a number of security provisions and options. In this paper, we highlight places where USN security considerations and home network attack scenarios.

Key Words : Smart Home, Security, IEEE 802.15.4., ZigBee

1. 장 서 론

센서 네트워크는 유비쿼터스(ubiquitous) 컴퓨팅 구현을 위한 기반 네트워크로 초경량, 저전력의 많은 센서들로 구성된 무선 네트워크이다. 이는 특히 네트워크를 구성하는 센서의 수가 매우 많고 각 센서 노드들은 제한된 전력과 컴퓨팅 능력을 가지며, 빈번한 센서 노드들의 삽입과 제거에 의해 센서 네트워크의 토폴로지가 쉽게 변화될 수 있다는 특성을 갖는다. 이러한 센서 네트워크는 센서를 통한 정보 감지 및 감지된 정보를 처리하는 기능을 수행함으로써 우리의 삶을 자동화시키고 편리함을 제공하지만 일상 생활의 시스템에의 의존도가 높아질수록 이로 인한 위험성 또한 높아질 수 밖에 없다[1].

그러므로 센서 네트워크를 통해 제공되는 정보들을 신뢰하고 동시에 개인의 프라이버시를 보장 받을 수 있도록 하기 위한 보안 연구가 반드시 병행되어야 한다. 즉, 보다 현실적이고 안전한 유비쿼터스 컴퓨팅 환경을 구현하기 위해서는 센서 네트워크의 활용 방안 및 센서 기술 개발과 함께 감지된 정보를 안전하게 처리하고 관리할 수 있는 센서 네트워크상에서의 보안 메커니즘 개발이 반드시 함께 연구되어 적용되어야 한다. 본 논문에서는 디지털 홈 네트워크에서 발생할 수 있는 무선 센서네트워크상의 보안 문제점 분석을 하였으며, 주로 IEEE 802.15.4 스펙의 문제점들을 분석하였다.

2. 센서 네트워크 특성 및 보안상의 취약성

센서 네트워크는 일반적으로 특정 지역에 수없이 많은 센서들이 무작위로 뿌려져서 대상에 대해 감지하고 감지된 데이터를 중앙의 베이스 스테이션으로 전송하는 구조를 갖는다. 각 센서 노드가 다른 노드의 데이터를 중계해주는 기능을 한다는 점에서 기존의 모바일 애드혹 네트워크의 한 특수한 형태로 인식하는 경우도 있지만 센서 노드는 일회성을 갖는 경우가 많아 가격도 매우 저렴하고 크기도 작아야 하며 작은 기억 공간, 제한된 계산 능력 등을 특성으로 하므로 사실상 애드혹 네트워크보다도 훨씬 제약 사항이 많다[2].

센서 네트워크는 수많은 노드들이 감지된 정보를 베이스 스테이션에게 보내야 하므로 중복된 데이터도 많고 베이스 스테이션이 각각의 데이터를 일일이 취합하기에 어려움이 많을 뿐 아니라 불필요한 트래픽의 증가로 이를 중계해야 하는 노드들에게 부담이 되어 수명을 줄이는 결과를 가져올 수 있으므로 중간에 aggregator(또는 게이트웨이)를 두는 구조를 취하는 형태가 대부분이다. 즉, 제한된 능력을 갖는 일반 센서 노드들과 이 센서 노드들로부터 데이터를 전송 받아 취합하여 베이스 스테이션으로 보내거나 베이스 스테이션으로부터의 쿼리를 센서 노드로 전달하는 aggregator 노드, 각 aggregator로부터 데이터를 받아 이를 취합하여 다음 기능을 수행하거나 필요 시 데이터 쿼리를 각 aggregator로 전달하는 베이스 스테이션으로 구성된 형태를 갖는다.

센서 네트워크는 네트워크가 갖는 근본적 특성으로 인해 일반 네트워크보다 훨씬 보안에 취약하다는 특성을 갖는다. 우선 센서 노드의 제약으로 인해 다양한 보안 스킴을 적용하기 힘들 뿐 아니라 노드가 배치된 물리적 환경이 공격에 그대로 노출되어 전송되는 정보가 쉽게 변경되거나 정당하지 않은 노드가 데이터를 전송함으로써 전체 정보의 무결성을 쉽게 무너뜨릴 수 있다. 뿐만 아니라 악의적인 노드가 센서

저자 소개
* 전자부품연구원 지능형정보시스템 연구센터 선임연구원
** 국민대학교 박사과정
***전자부품연구원 유비쿼터스컴퓨팅 연구센터 수석연구

노드로 가장하여 불필요한 정보를 계속 발생시켜 중간 노드의 자원을 소모시킴으로써 네트워크의 수명을 단축시킬 수도 있다. 이처럼 간단한 공격만으로도 네트워크 전체를 쉽게 와해시킬 수 있을 뿐 아니라 특히 센서 네트워크의 목적에 따라서는 그 위험성이 상상을 초월할 수도 있다. 이처럼 보안에 취약함에도 불구하고 센서 네트워크의 보안 연구에 관한 필요성이 간과되는 경우가 많을 뿐 아니라 기존보안 기법을 그대로 적용하기도 힘들다. 그러므로 센서 네트워크 기반 기술 연구의 초기 단계인 지금 이 센서 네트워크의 특성에 적합한 보안 기술 연구가 같이 진행되어야 하는 시점이다[3].

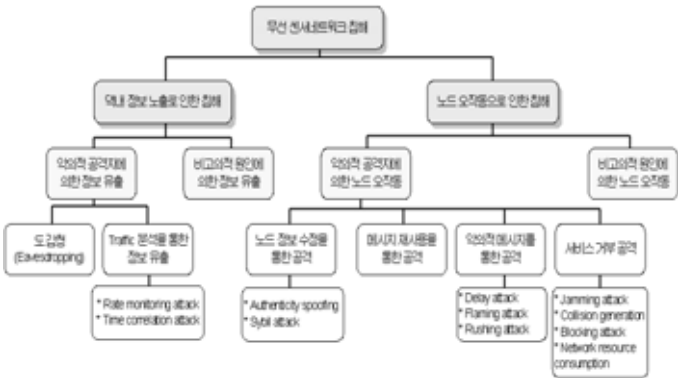

그림 1. 홈 센서 네트워크 상에서의 침해 가능 유형

3. IEEE 802.15.4 및 ZigBee 보안 위험 사항 분석

3.1 ACL 및 Nonce 관리 문제

3.1.1 Same key in multiple ACL entries

IEEE 802.15.4에는 255 ACL 항목이 있으며, 각각의 다른 키와 관련된 nonce을 가진다. 송신자가 목적지 주소에 근거한 적당한 ACL 엔트리를 선택한다. 두 가지 다른 ACL 항목에서 같은 키를 사용한다면 보안 문제점이 발생 할 수 있다. 송신자가 nonce을 우연하게 재 사용 할 가능성이 있기 때문이다. 송신자에 의한 nonce의 재사용으로 인하여 발생 할 수 있다. adversary가 두 개의 서로 다른 수신자에게 가는 암호문을 XOR 함으로써, 두개의 평문을 XOR 한 것과 같은 결과를 얻어낸다.

3.1.2 Loss of ACL state due to power failure

센서노드들은 대부분 배터리를 전력으로 사용하기 때문에 효율적인 전력 관리 문제가 매우 중요하다. 파워 손실시에도 ACL 상태 관리를 효율적으로 고려해야 한다.

- Flash 메모리에 ACL state를 저장하는 것은 비효율적이며, 느림
- 카운터를 매번 플래시 메모리에 저장하지 않고 일정 블록 단위로 저장
- 파워 손실시에 카운터 값 복구 불능(통신 불가)

3.1.3 Auxiliary header does not protected

그림 2. 발생 가능한 상황의 예

헤더 정보가 평문으로 전송되므로 패킷 캡처를 통하여 카운터 정보를 획득 가능하다. 이를 통하여 nonce 정보를 생성 가능하다.

3.2 키 관리 문제

3.2.1 key capture problems

초기 디바이스 join시에 plaintext로 전송되는 네트워크 키나 마스터키의 유출가능성이 존재한다. 키 유출의 경우에는 그 사실 여부 판명이 불가능하며, 마스터 키가 유출 될 경우 위장된 코디네티어를 만들 수도 있다[4].

3.2.2 Network shared key is incompatible with Replay protection

네트워크 키의 경우에는 모든 네트워크에 존재하는 노드들을 공유해야 한다. 새로운 노드가 네트워크에 접근할 때 plaintext 형태로 전송한다. 네트워크 키의 획득 및 재사용이 용이하다. 키 카운터에 대한 동기화가 명확하지 않을 경우 특정 노드 간 통신 불가능한 경우도 발생 가능하다[5].

3.2.3 No Support for Group Keying

각 ACL 항목에는 디바이스 주소가 들어가 있으므로, 그룹 단위의 키를 설정하기 어렵다. 모든 그룹 멤버에 대해서 동일한 키를 지니는 ACL 항목들을 만들어야 하며, cost ineffective 하며, ACL 관리의 어려움이 있다. 즉 링크 키와 그룹 키의 구분이 불가능하다.

3.3 Integrity 문제

3.3.1 Unauthenticated Security Mode

시큐리티 모드에 따라서 메시지 인증이 안되는 경우가 발생 할 수 있다. Integrity check를 하지 않을 경우 다양한 공격이 가능하다. 공격이 가능한 해킹 요소로는 Sybil Attack, Delay Attack, Flaming attack, Rushing Attack등이 있다.

3.3.2 No Integrity on Acknowledgement Packets

공격자가 손쉽게 Ack 메시지 생성이 가능하다. Jamming

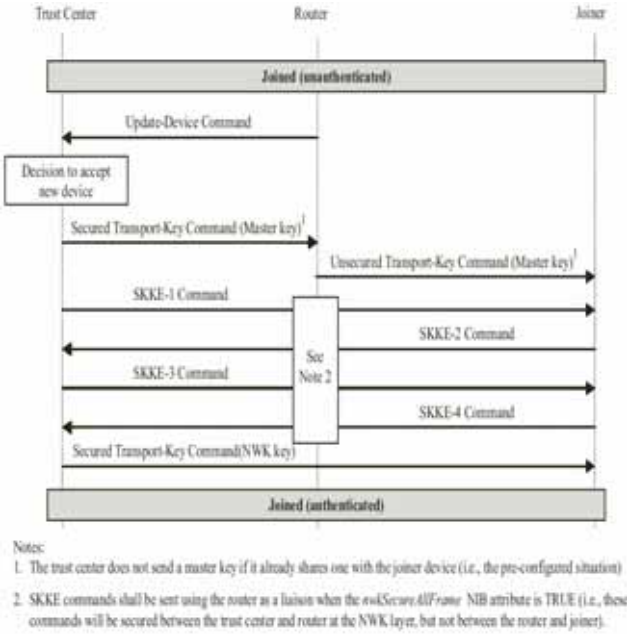

그림 3. Key Capture Problems

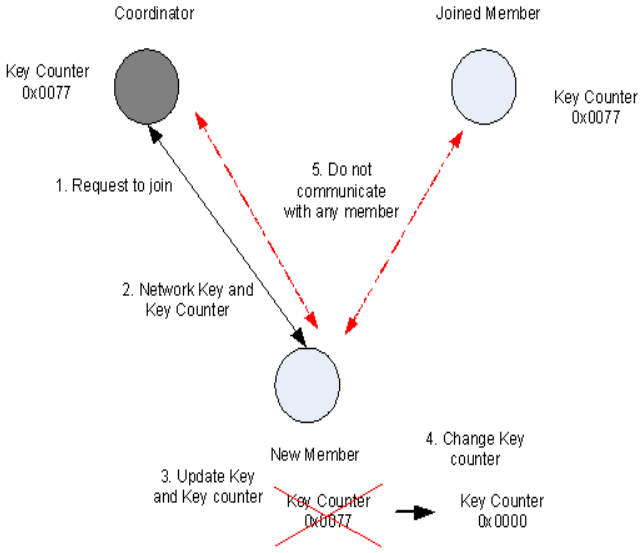

그림 4. 네트워크 키 획득 및 재사용 용이

attack과 함께하여 전송 노드가 모르게 메시지 전송을 방해할 수 있다. 예를 들면, A가 메시지를 보낼 때 jamming을 통해서 메시지가 못가게 하고, ack를 전송하여 A로 하여금 전송이 성공되었다고 믿게한다.

3.4 ZigBee 환경에서의 문제점

3.4.1 불충분한 키 관리

직비 디바이스가 이동하여 새로운 직비 네트워크를 형성할 때 마다 scan/join 키 교환 과정을 거쳐야 한다. 동적인 네트워크 형성시에는 상당한 에너지 소비 문제가 발생하여 비 효율성을 발생시킨다. 또한 매 join 과정마다 키 유출 가능성이 발생한다. ACL 상의 항목들의 관리에 대한 문제 언급이 없다.

3.4.2 No Security Policy for a New Device

새로운 장치 및 센서에 대한 인증 프로토콜에 대한 정책이 없다. 매 요청하는 모든 장치 및 센서에 대한 허용해야 한다. ZigBee 서비스 프로파일에서 시큐리티에 관련한 보안 요구 사항 및 정의 사항이 없다. 차후 프로파일에는 보안에 대한 사항을 구체적으로 명시한 프로파일이 필요하다.

4. 결 론

디지털 홈에서의 유비쿼터스 요소로서 센서네트워크에 대한 관심 및 실제 응용을 위하여 많은 연구 및 실험 테스팅등이 진행되고 있다. 본 논문에서는 유비쿼터스 홈 네트워크에서 무선 센서네트워크의 산업체 표준인 IEEE 802.15.4 및 ZigBee 보안에 대한 문제점을 위협 요소등을 분석하였다. 실제 디지털 홈 시범 사업자인 SKT, KT 컨소시엄에서의 무선 센서네트워크의 보안 위협 사항들에 지적이 중요한 문제로 대두되기도 하였다. 디지털 홈 사업의 성공적인 시행을 위하여 본 논문에서 제시된 문제점들을 해결되어야 할 것이다.

* 감사의 글

본 연구는 산업자원부 및 한국산업기술평가원의 성장동력 기술개발사업의 연구결과로 수행되었습니다.

5. 참고 문헌

1] A. Perrig, R. Szewczyk, V. Wen, D. Culler, and J.D.Tygar, "SPINS: Security Protocols for Sensor Networks,"Proc. of the 7th ACM/IEEE International Conference on MobiCom, 2001.

[2] J. Deng, R. Han, and S. Mishra, "Security Support for In-Network Processing in Wireless Sensor Networks," Proc. of the 1st ACM Workshop on the Security of Ad Hoc and Sensor Networks(SASN), 2003.

[3] S. Slijepcevic, M. Potkonjak, V. Tsiatsis, S. Zimbeck, and Mani B. Srivastava, "On Communication Security in Wireless Ad-Hoc Sensor Network," Proc. of WETICE' 02, 2002.

[4] L. Eschenauer and V. Gligor, "A Key-Management Scheme for Distributed Sensor Network," Proc. of the 9th ACM Conference on Computer and Communications Security, 2002.