보안을 고려한 센서 네트워크 분류기준에 관한 연구

임휘빈*, 박상진*, 김미주**, 신용태*, 최종원***
*숭실대학교 컴퓨터학과
**한국인터넷진흥원 정보보호본부
***숙명여자대학교 컴퓨터과학과
e-mail:hblim@cherry.ssu.ac.kr

A Study on The Sensor Network Classification with Security

Hui-Bin Lim*, Sang-Jin Park*, Mi-Joo Kim**,
Yong-Tae Shin*, Jong-Won Choe***
*Dept of Computing, Soong-Sil University
**Korea Information & Security Agency
***Dept of Computer Science, Sook-Myung Women's University

요 약

현재 센서 네트워크의 보안 기술 연구는 센서 네트워크 내의 정보전달 및 처리과정에서의 정보 보호 및 중요 센서 노드의 보호를 위한 정보인증, 노드인증, 보안 라우팅, 키 관리, 도처, 위조 방지 등에 중점을 두고 진행되고 있다. 그러나 대부분의 연구는 USN 응용 서비스 유형에 종속되는 단점을 가진다. 즉, 특정 서비스에만 유용한 보안 기술 연구가 대부분이라 하겠다.

따라서, 특정 USN 응용 서비스에 국한되지 않는 다양한 USN 응용 서비스를 지원할 수 있는 정보보호 기술이 개발이 이루어져야 하며, 이를 위해서는 다양한 USN 응용 서비스를 지원할 수 있도록 보안을 고려한 센서 네트워크의 구성에 대한 연구가 선행되어야 한다.

이에 본 논문에서는 현재 개발된 다양한 USN 응용 서비스를 분석하여 공통적인 센서 네트워크의 구성 요소를 도출하였으며, 이를 토대로 보안을 고려한 센서 네트워크 분류기준을 제시하였다.

1. 서론

USN(Ubiquitous Sensor Network)은 적은 메모리, 저용량의 배터리, 제한적인 컴퓨팅 성능 등 제한된 하드웨어 자원을 가진 수많은 센서 노드들이 무선 통신으로 연결된 네트워크이다. 이러한 센서 네트워크는 다양한 주변 상황을 인식하고 파악하여 기상/해양 관측, 재해/재난 관측, 수자원관리, 생태관리, 농작물 관리 등의 환경, 건설, 건강, 국방 분야 등에 활용된다.

센서 네트워크는 무선 통신 방식으로, 정형화된 네트워크 토폴로지를 가지지 않음으로 인해 유선 네트워크에 비해 매우 다양한 보안 취약성을 가진다. 이를 보완하기 위한 연구하고 있는 많은 보안 기술들은 특정 서비스만을 고려하여 개발되어 다양한 USN 응용 서비스들을 지원하지 않는다.

따라서 어느 특정 USN 응용 서비스에 국한되지 않고, 다양한 USN 응용 서비스를 지원하기 위해서는 보안을 고려한 센서 네트워크의 구성에 대한 연구가 필요하다.

이에 본 논문에서는 현재 개발된 다양한 USN 응용 서비스를 조사・분석하여 공통적인 센서 네트워크의 구성 요소를 도출하고, 이를 토대로 보안을 고려한 센서 네트워크 분류기준을 제시하였다.

본 연구는 정보통신기술협회의 정보통신표준기술력향상 사업의 일환으로 수행하였음. [2009-P1-32-08J46]

2. 센서 네트워크 분류기준 요구사항

현재 센서 네트워크의 분류는 센서 네트워크가 지원하는 USN 응용 서비스별 또는 센서 네트워크에서 사용되는 프로토콜에 따라 분류[1]되고 있다. 그러나 이러한 분류는 특정 응용 서비스 및 프로토콜에 종속되어 공통적인 분류기준을 찾기 힘들며 확장성이 떨어지는 단점을 가지고 있다. 이러한 단점을 보완하고자 일부 연구에서는 각각의 응용 서비스를 분석하여 공통적인 구성요소를 찾기 위한 연구가 이루어졌다[2].

따라서 센서 네트워크 분류기준은 센서 네트워크를 물리적/논리적으로 분류할 수 있어야 하며 특정 서비스에 독립적이고, 다양한 USN 응용 서비스에 적용될 수 있어야 한다.

이에 본 논문에서는 이러한 요구사항을 만족할 수 있는 분류기준으로 센서 네트워크 구성의 관점의 분류기준을 제안하였으며, <표 1>에서 기존의 연구와 제안한 분류기준의 장・단점을 비교하였다.

<표 1> 분류기준 분석

분류기준	장 점	단 점
서비스 프로토콜	- 분류가 쉬움 - 센서 네트워크의 논리적 분류가 쉬움	- 서비스/프로토콜에 종속 - 분류기준의 변화 다양 : 서비스/프로토콜 수에 종속 - 센서 네트워크의 물리적 분류가 어려움
네트워크 구성	- 서비스/프로토콜에 독립 - 네트워크 설계 용이 : 표준적인 네트워크 설계 - 유지보수 용이	- 특정 서비스/프로토콜을 위한 추가적인 설계가 필요

3. 관련연구 및 제안하는 센서네트워크 분류 기준

센서 네트워크의 분류를 네트워크의 구성 관점에서 연구한 자료를 살펴보면, 유럽에서 수행된 15개의 프로젝트를 조사하고 각각의 프로젝트를 지원하기 위한 센서 네트워크 분석을 통하여 14개의 공통적인 네트워크 구성요소[2]를 도출하거나, Zigbee 기반의 WSN 개발 사례를 분석하여 센서 네트워크를 분류[3]한 연구 등이 있다. 이외에도 계층적 구조를 활용하거나 통신을 위해 전송되는 신호의 종류를 이용한 연구도 진행되었다. 하지만 이러한 연구들은 구성 기준의 도출에 있어서 보안을 고려하지 않고 있다.

따라서 본 논문에서는 센서 네트워크의 공격유형[4][5][6][7]을 <표 2>로 정리하고, 이를 고려한 구성기준인 <표 3>을 제안한다.

<표 2> 센서 네트워크 공격유형

공격유형	내용
도청 (sniffing)	노드 신호의 도청을 통한 통신 및 운영 방해
위조 (spoofing)	신호 및 노드 위조를 통한 통신 및 운영 방해
플러드 (flood)	불법신호 전송을 통한 통신 및 운영 방해
스캔 (scan)	불법신호 전송을 통한 통신 및 운영 방해
죽음의 핑 (ping of death)	불법신호 전송을 통한 통신 및 운영 방해
랜드 (land)	도청, 위조를 활용한 노드 자원의 운영 방해
서비스 거부 (denial of service)	불법신호 전송을 통한 통신 및 운영 방해
세션 가로채기 (session hijacking)	통신세션가로채기를 통한 통신 및 운영 방해
위조노드 (fake access point)	위조노드 주입을 통한 통신 및 운영 방해
물리적 (physical)	전파방해, 절취 등을 통한 물리적 파괴 및 통신방해

<표 3> 보안을 고려한 센서 네트워크 분류기준

분류기준	정의	세부타입
Energy	안전한 운영을 위한 노드 자원 보호	- 전력공급형태 - 전력공급기간
Topology	안전한 구축을 위한 물리적 구성 보호	- 인프라구조/애드혹 - 스타/트리/그래프
Mobility	이동성 관리를 통한 구성객체 보호	- 지속적/주기적 이동 - 네트워크 이동 유,무
Connectivity	연결주기 관리를 통한 노드 자원 보호	-지속적/주기적 연결
Deployment	물리적 위치 및 영역 관리를 통한 센서 네트워크 보호	- 노드살포 방법/영역 - 살포노드 개수
Heterogeneity	구성 객체의 역할 및 전송 매체 관리를 통한 노드 보호	- 노드의 역할(기능) - 물리적 전송매체 종류

4. 향후연구 방향

본 논문에서는 특정 USN 응용 서비스에 국한되지 않는 다양한 USN 응용 서비스를 지원할 수 있도록 보안을 고려한 센서 네트워크의 구성을 위한 분류기준을 제안하였다. 이에 대한 연구를 위해 USN 응용 서비스 및 센서 네트워크 구성 관련 연구 동향을 고찰하고, 관련 기술 자료를 조사·분석 하였으며, 이를 토대로 USN 응용 서비스 기반 센서 네트워크 분류기준을 도출하였다. 그리고 도출된 분류기준을 보안을 고려하여 재정의 하였으며 정의된 분류 기준에 적합한 분류타입을 도출하고 <표 3>과 같은 분류표를 제시하였다.

향후에는 이러한 분류기준에 대한 검증을 통해 타당성을 검토하고 이를 확장하여 센서 네트워크 구성에 있어 기본적인 보안 점검 가이드라인으로 활용하기 위한 연구가 필요하다.

참고문헌

[1] “Introduction to Sensor Networks,” 2006

[2] Kay Romer and Friedemann Mattern, “The Design Space of Wireless Sensor Networks,” IEEE, 2004

[3] Ilya bagrak, “Design a wireless sensor network,” EE Times-India

[4] 박준석, “USN 표준화 동향 및 전망,” 전자공학학회지, 2009

[5] 조현숙, 정교일, 최두호, 강유성, “RFID/USN 보안 기술 개발 동향,” 한국전파학회, 2008

[6] 이석준, 오경희, 김호원, 정병호, “USN 공격 기법 및 보안 기술 동향,” 한국인터넷정보학회, 2008

[7] 손승원, “USN 정보보호 기술,” 대한전자공학회지, 2005