센서 네트워크에서의 암호학적 보안 및 한계성 분석

김정태

목원대학교

Analyses of Security for Sensor Networks with Cryptography and Its Limitations

Jung Tae Kim

Mokwon University

E-mail : jtkim3050@mokwon.ac.kr

요 약

센서 네트워크은 기존의 인프라가 없는 네트워크 망을 연결한 구조를 가지고 있으며, 네트워크가 가변성을 가져 기존의 인프라 구조와는 차별적인 특성을 가진다. 사용되는 센서는 제한된 자원으로 인하여 사용할 자원이 제한되어 전통적인 보안 메카니즘을 사용하기는 보안성에 많은 문제점을 야기시킬 수 있다. 따라서 본 논문에서는 이러한 센서 네트워크의 인프라 구조하에서의 보안 서비스 요구사항과 현재까지 연구되어지는 기술적인 동향 및 특성을 분석하고자 한다.

키워드

Sensor, Network, WSN, Security, Authentication

Ⅰ. 서 론

최근들어 기술적인 발전으로 인하여 유무선 통합 환경하에서 무선 네트워크망을 이용한 다양한 프로토콜 및 통신 기법이 발전되고 있다. 특히 이러한 기술들은 센서를 이용한 네트워크의 통신이 융합 복합화되는 추세이다. 센서 네트워크는 특성상 제한된 하드웨어적 자원, 무선 환경에서 비밀성이 보장되지 못하며, 물리적 보안에도 취약성을 가지고 있다. 따라서 현재의 연구 동향으로는 센서네트워크에 대한 보안성 강화를 위하여 주로 통신 망에서의 문제, 분산 서비스 시스템에서의 문제, 제한된 센서 노드에 대한 물리적인 수명 등의 문제에 대하여 주로 연구를 진행하고 있다 [1,2]. 센서 네트워크는 많은 수의 센서 노드들로 구성된 네트워크로 센서를 통한 주변 정보 감지 및 감지된 정보를 처리하는 기능을 수행한다. 최근 유비쿼터스 컴퓨팅 개념의 도입과 함께 이를 실생활에 구현하기위한 기반 기술의 하나로 센서 네트워크가 큰 관심을 모으고 있다. 그러나 유비쿼터스 컴퓨팅을 통한삶의 편리성을 추구함과 동시에 네트워킹을 통해 제공되는 정보를 신뢰할 수 있어야 하며 개인의 프라이버시 또한 보장되어야 함은 기본적인 요구 사항이다. 따라서 본 논문에서는 이러한 연구 동향을 분석하여 기술적인 관점에 대하여 문제를 해결 제시하고자 한다.

Ⅱ. 보안성의 제약 조건

2.1 보안성 문제

보안성 문제를 해결하기 전에 해결해야 할 사항은 다음과 같다[3].

1) 복잡한 키 분배를 재제하고 키 유지 관리가 편리하여야 한다.

2) 암호화 모듈이 하드웨어적으로 소형에 구현되어야 한다. 따라서 제한된 전력 및 메모리의 조합이 요구되어지며, 공개키 알고리즘의 적용이 불가능하다.

3) 패킷의 오버해드를 최소화하기 위한 기법들이 필요하다.

4) 혼합 모드의 통신망을 제공해야 한다.

5) 종간 암호화 모듈이 설정되어 통신 보안성을 높여야 한다.

6) DoS(Denial of Service) 등의 해킹에 취약하지 않아야 한다.

2.2 보안성 제약 조건

다음은 통신 보안을 위하여 왜 암호화 기능의

제한적인 요소가 발생하는 지에 대한 설명이다 [4].

1) 트래픽 분석을 막을 수 없다.
2) 재전송의 패킷을 방지할 수 없다.
3) 재응답 공격을 방지할 수 없다.
4) 재밍된 패킷을 방지할 수 없다.
5) 악의적인 침입자 및 선택된 노드를 방지할 수 없다.

이러한 이유로 무선 환경하에서는 기존의 관용적인 암호화 알고리즘을 통하여 안전성이 보장되는 서비스 모델의 통신 프로토콜을 실현할 수 없다. 다음의 표는 일반적으로 센서 네트워크 프로토콜에서 발생할 수 있는 공격에 대한 예이다.

표 1. 각각의 프로토콜에 대한 공격의 예

Protocol	Relevant attacks
TinyOS beaconing	Bogus routing information, selective forwarding, sinkholes, Sybil, wormholes, HELLO floods
Directed diffusion and multipath variant	Bogus routing information, selective forwarding, sinkholes, Sybil, wormholes, HELLO floods
Geographic routing (GPSR,GEAR)	Bogus routing information, selective forwarding, Sybil
Minimum cost forwarding	Bogus routing information, selective forwarding, sinkholes, wormholes, HELLO floods
Clustering based protocols (LEACH,TEEN,PEGASIS)	Selective forwarding, HELLO floods
Rumor routing	Bogus routing information, selective forwarding, sinkholes, Sybil, wormholes
Energy conserving topology maintenance	Bogus routing information, Sybil, HELLO floods

2.3 해결해야 할 문제

1) 통신 보안 문제

실제적인 트래픽을 제어할 수 있는 제어 능력 및 하드웨어적 구현으로 구현 시 보안성 비도의 적절성 문제

2) 분산 프로토콜에서의 암호화학적인 프로토콜의 접근 방법 문제

3) 각각의 노드에 대한 하드웨어적인 보안 모듈 탑제 시의 안정성 문제

4) 강화된 암호알고리즘의 설계 및 구현

2.4 센서 노드

(그림1)은 대표적인 센서 모듈에 대한 기본적인 개념이다. 센서 노드 소프트웨어 플랫폼은 크게 운영체계, 데이터베이스, 미들웨어 등으로 구분할 수 있다. 현재 세계적으로 많이 사용되는 것은 미국 버컬리 대학의 TinyOS와 국내의 ETRI 기술인 NanoOs 이다. 그리고 이러한 센서 노드는 스마트 센싱, 데이터 프로세싱, 무선 통신 등의 기능을 갖추고 있어야 한다. 또한 저전력 소모, 안정성 운여, 네트웍 접속 기능, 분산 처리, 자원을 효율적으로 관리할 수 있는 인터페이스 기술등을 제공하여야 한다. 또한 센서네트워크는 다양한 요소기술이 유연하게 통합하여 하나의 솔루션으로 개발되므로 표준화를 정하기는 어려움을 가지고 있으며, 현재는 센서 모듈에 보안성 강화를 위한 보안 모듈을 내장한 방향으로 기술적인 발전을 기하고 있다.[5].

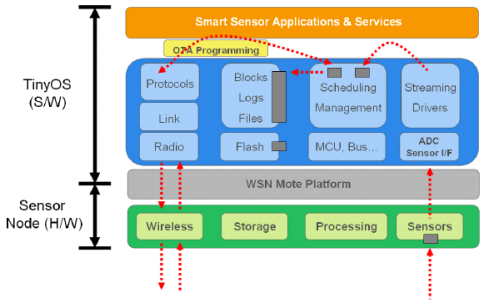

그림 1. 센서 모듈의 블록도

III. 결 론

본 논문에서는 센서 네트워크의 구현에서 발생할 수 있는 여러 종류의 문제를 보안성 측면에서 해석하였다. 보안성의 접근 방법은 현재의 응용 기술면에서는 기존의 방법을 사용하여 모든 문제는 해결할 수 없지만 그 대안적인 방법들이 많이 연구되고 있다. 추후의 연구 방향으로는 각각의 센서 노드에 구현 가능한 암호학적 알고리즘의 개발 및 여러 종류에 응용 가능한 프로토콜을 해석할 예정이다.

Acknowledgement

This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology (grant number: 2010-0024133

참고문헌

[1] X.L. Jia, Q.Y. Feng, C.Z. Ma, “An efficient anti-collision protocol for RFID tag identification,” IEEE Communications Letters, vol.14, no.11, pp.1014-1016, 2010.

[2] L. Atzori, A. Iera, and G. Morabito, “The Internet of Things: A survey,”Computer Netw., vol. 54, no. 15, pp. 2787.2805, 2010.

[3] M. Zorzi, A. Gluhak, S. Lange, and A. Bassi, “From today’s INTRAnet of things to a future INTERnet of things: A wireless- and mobilityrelated view,”IEEE Wireless Commun., vol. 17, no. 6, pp. 44.51, 2010.

[4] G. Wu, S. Talwar, K. Johnsson, N. Himayat, and K. D. Johnson, “M2M: From mobile to embedded Internet,” IEEE Commun. Mag., vol. 49, no.4, pp. 36 - 43, Apr. 2011.

[5] 김석우, “센서네트워크 연구개발 및 상용화 사례”, 주간기술동향 통권 1325호 2007.12.5.