교량 감시를 위한 센서 네트워크 보안

임화정° 전진순 이헌길
강원대학교 컴퓨터정보통신공학과
{hjlim°, doore96, hklee}@kangwon.ac.kr

Sensor Network Security for Monitoring the State of Bridge

HwaJung Lim° JinSoon Chen, HeonGuil Lee
Dept. of Computer Information and Communications Engineering, Kangwon National University

요 약

센서 네트워크는 많은 수의 센서 노드들로 구성된 네트워크로 센서를 통해 주변 정보를 감지하고 감지된 정보를 수집하고 처리한다. 센서 네트워크는 그 적용 분야가 광범위하여, 그에 따른 보안요구사항 또한 다양하다. 교량 감시에 사용되는 센서들의 특징은 교량에 일정한 간격으로 고정되어 위치하여 센서이동이 거의 없는 고정된 센서 네트워크를 형성하게 된다. 따라서, 이러한 특징을 고려한 보안프로토콜의 개발이 필요하다. 본 논문에서는 교량 감시에 사용되는 센서 네트워크와 같이 고정된 센서들로 이루어진 네트워크상에서의 보안 요구사항을 분석하고 이를 만족시킬 수 있는 보안 프로토콜을 제시한다.

1. 서 론

무선 센서 네트워크는 분산 컴퓨터와 임베디드 시스템의 새로운 연구영역이다[1].

디지털회로기술의 개선으로 자료처리와 무선 통신이 가능한 단일 칩으로 구성된 센서가 등장하였다. 소형 배터리로 작동하는 센서 노드는 언제 어디서나 저가로 실생활에 배치할 수 있고, 분산된 센서 네트워크를 구축하여 주변의 환경에 대해서 정보를 수집하고 그 결과를 편하게 모니터링 할 수 있도록 하여, 군사 목적이나 일상생활 전반에 활용되고 있다[2].

특히 센서는 위험한 지역이나 접근이 힘든 지역에 값싼 비용으로 감시 체제를 구축할 수 있어 교량의 상태를 감지하고 위험요소를 바로 발견해서 안전성을 유지하는 등의 환경 감시 장치에 많이 이용된다.

그러나, 적은 메모리, 배터리 용량의 제한, 컴퓨팅 성능의 제약 등 제한적인 하드웨어 자원을 가지고 있는 센서들은 센서 정보의 도청이나 비정상적인 패킷의 유통, 메시지의 재 사용 등 데이터 위·변조 문제와 네트워크 전체를 마비시킬 수 있는 서비스 거부 공격(Denial of Service)과 각종 물리적인 공격에 쉽게 노출된다[3]. 반면 일반적인 센서 노드와 달리 교량의 안정성 및 환경을 감시하는 센서 네트워크의 경우 센서 노드가 고정될 수 있는 특성이 있기 때문에 이에 맞는 보안 기술이 요구된다.

본 논문에서는 일반적인 센서 네트워크와 달리 교량용과 같이 센서의 위치가 변하지 않고, 한 곳에 고정된 센서 네트워크의 보안요구사항을 분석하고 이를 만족하기 위한 보안프로토콜을 제시한다.

2. 일반 센서 네트워크의 특징 및 보안 요구사항

센서 네트워크는 제한적인 하드웨어 자원을 가지고 있는 대량의 센서 노드들이 좁은 영역에 조밀하게 분포한다[4].

하나의 센서 노드가 통신하는 노드 수가 하나가 아닌 다대다 통신인 그물망 통신으로 이뤄지는 센서 네트워크는 브로드캐스트 통신 방식을 사용하기 때문에 주위의 노드들이 믿을 수 있는 상태인지에 대한 판단이 어렵고, 통신 반경이 짧아 통신시 노드들의 동작이 항상 성공적이지 못하다는 특징을 지닌다.

따라서, 센서 정보를 목적지까지 전달하기 위한 경로 설정이나 유지를 위한 노드 간의 상호 인증과 제한된 센서 자원을 이용하여 인증과 암호화에 사용될 암호 키 관리의 문제가 주요 이슈 중의 하나이다[5].

일반적인 센서 네트워크의 보안 요구사항은 다음과 같다. 첫째, 경량화된 암호 및 인증으로 라우팅 시에 보안기능을 제공하여야 한다. 둘째, 센서와 센서, 센서와 베이스 스테이션간에 사용될 암호 키 관리기능을 제공하여야 한다. 셋째, 센서의 이탈 및 고장 등으로 인한 서비스 거부공격에 강한 구조이어야 한다. 넷째, 사용자의 위치정보와 센서 노드의 집합정보에 대한 암호 기능을 제공하여 외부 공격에 대비하여 센서 노드의 노출을 방지하는 등의 보안 기능이 요구된다.

3. 센서 네트워크의 보안기법 동향

3.1 인증기법

센서 네트워크에서 인증은 보안을 위한 가장 기본 적인 단계로서, 멀티 캐스트 통신에서 각 패킷 인증에 주로 사

용되는 스킴은 TESLA(Timed Efficient Stream Loss-tolerant Authentication)이다[6,7]. 지연 키 노출 방법을 사용하여 각 패킷의 인증을 수행한다. 인증키는 단방향 키 체인(one-way key chain)을 사용하여 시간의 역방향으로 계산되므로 중간에서 임의로 생성할 수 없다. 이 방식은 패킷 손실에 강한 반면, 송·수신자간에 시간 동기화(time synch)가 필요하다.

센서 네트워크의 인증 메커니즘 중 하나인 SPINS(Security Protocols for Sensor Networks)는 센서 노드들이 베이스 스테이션과 공유하는 하나의 마스터 키를 사전에 분배하는 방식을 이용한다[8].

SPINS는 그림 1과같이 데이터의 기밀성을 제공하기 위한 SNEP(Secure Network Encryption Protocol) 구조와 브로드캐스팅되는 데이터의 인증을 제공하기 위한 μTESLA 스킴으로 구성된다.

$$A \rightarrow B: \{D\}(K_{encr}, C), MAC(K_{mac}, C|\{D\}(K_{encr}, C))$$

(D: message, K_{encr}: encryption key, C: counter)

그림 1 SNEP 구조

3.2 키 관리기법

키 관리 기법으로는 베이스 스테이션과 클러스터 구조를 중심으로 중간에 aggregator 노드를 두는 것을 기본구조로 하는 그룹 키 관리 기법과 일부 노드의 노출이 근접한 이웃 노드까지 노출시키는 위협을 최소화하기 위한 LEAP(Localized Encryption and Authentication Protocol)이 있다[9,10].

3.3 보안을 위한 센서 네트워크의 구조

센서 네트워크의 보안을 위해 제안된 여러 방식의 네트워크 구조를 살펴보면, 첫째, 베이스 스테이션을 보안 상의 제약사항을 갖지 않는 특수한 노드로 설정하는 일반적인 방식과 달리 베이스 스테이션에 대한 보안 강화를 위한 다중 베이스 스테이션을 두는 네트워크 구조가 제시되었다. 둘째, 센서 네트워크의 특성을 고려하여 비용, 공간 및 에너지 절약, 시간 효율성 등을 고려하여 네트워크를 관리영역과 비 관리 영역으로 분리하여 구성하는 분산된 네트워크 구조 및 키 관리 구조가 있다. 셋째, 센서 노드의 레벨을 기반으로 하여 계층화된 구조를 정의하고 이웃의 수와 계층 클러스터에서의 레벨을 이용하여 에너지 효율을 높이는 동시에 최단 거리 통신을 가능하도록 하는 방안을 제시하는 방법 등이 있다[11,12,13].

이 중 레벨 기반 계층화 구조방식은 타이머와 GPS 수신기를 가지고 위치가 고정된 센서 노드들로 구성된다. 고정 센서 노드는 저장공간이나 계산 능력이 일반적인 센서 노드에 비해 뛰어나며, 모든 센서 노드들에 대해 각각의 대칭키를 갖는 Sink 노드(베이스 스테이션에 해당) 가 있음을 가정한다.

라우팅 방식은 Sink 노드가 네크워크 토폴로지 파악 후 그룹 키를 생성, 각 센서 노드에게 암호화 하여 전송한다.

그룹 키 생성에 Multiparty Diffie- Hellman 프로토콜을 응용, 각 센서 노드가 말단 노드로부터 상위 노드로 자신의 부분 키를 내놓으면 부모 노드가 이를 취합하고 다시 부모 노드들이 내놓은 부분 키를 그 상단에서 취합함으로써 그룹의 가장 상단의 노드가 전체 그룹 키를 최종적으로 확정하고 이를 암호화 한 다음 각 센서 노드에게 보내는 방법을 취한다.

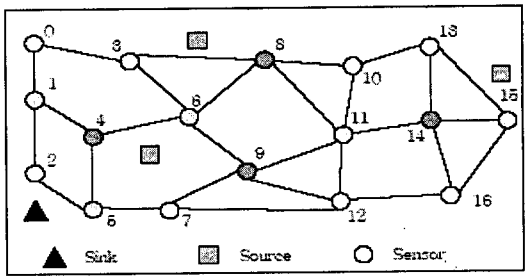

그림 2 레벨 기반 계층적 라우팅 프로토콜

그림 2에서 각 센서는 배치된 후 자신의 ID와 NBR(이웃의 수)을 브로드캐스트하여 주변에서 가장 높은 NBR을 가진 센서가 클러스터헤드가 된다. 일반센서, 클러스터헤드, 두 개 이상의 클러스터 헤드를 연결하는 root순으로 레벨 1,2,3으로 점차 높아지며, 노드의 색깔이 진해질수록 레벨이 높은 센서를 의미한다.

이러한 계층적 구조는 네트워크 트래픽을 줄여 센서들의 자원을 절약할 수 있으며, 악의적인 노드에 의한 공격이나 센서의 고장으로 인해 정보가 중간에 잃어버리는 것을 방지할 수 있지만, 상단의 노드가 베이스 스테이션과 멀리 떨어져있을 경우, 가까이 있는 센서로부터 정보가 바로 전송되지 않고 우회하여 갈 수 있다.

4. 교량 환경에 요구되는 보안 기법

교량 감시용 센서 네트워크는 센서가 교량에 고정되어 센서의 이동성이 거의 없기 때문에 이동에 따른 배터리 소모가 줄어들고, 위치가 고정되어있으므로 최단거리의 안정적인 보안을 제공할 수 있다. 또한 센서의 수명이 일반 센서보다 길기 때문에 보다 강력한 보안기술 및 키 관리 기법을 수용할 수 있다.

즉, 교량 감시용 센서 네트워크에서는 고정된 센서에 맞는 새로운 키 관리 및 보안 기법 제시가 필요하다.

4-1. 인증기법

교량 감시용 센서 네트워크에서 인증 기법은 SPINS 인증과 같이 키 생성 및 유지가 베이스 스테이션에 집중되는 것을 분산시키기 위해 3계층 구조를 응용한 TESLA 인증 방식을 사용한다[14].

교량 감시용 센서 네트워크에서는 노드가 고정되어 초기 인증서 발급 이후 인증서 재발급이 필요 없다. 즉, TESLA 방식을 사용 TTP(Trusted Third Party)로부터 발행된 초기 인증서와 새로 장착된 노드와 응용 간의 공유키만을 설립하는 2계층방식을 사용한다.

4-2. 키 관리기법

고정된 센서 네트워크에 효율적인 키 관리 기법으로 Grid 기반 키 사전분배나 위치 기반 키 사전분배방식, 에너지 효율을 고려한 게이트웨이(aggregator)와 커맨드 노드(베이스 스테이션)사이의 통신을 위한 두 개의 키를 저장하는 방식 등을 응용할 수 있다[15,16,17].

4-3. 보안을 위한 센서 네트워크의 구조

교량 감시용 센서 네트워크는 입체적인 교량 안전진단을 위해 그림 3과 같은 하이퍼 큐브 구조로 센서 노드를 장착하여 노드 위치를 기반으로 한 계층화 구조로 노드와 베이스 스테이션간의 최단거리 경로를 설정할 수 있다.

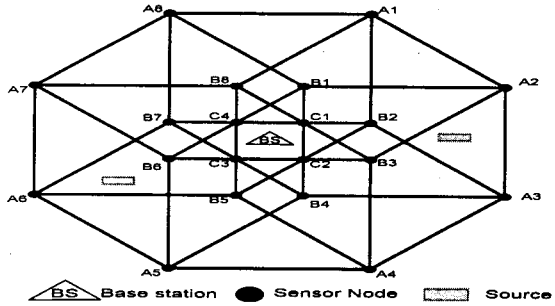

그림 3 하이퍼 큐브 구조 라우팅 프로토콜

하이퍼 큐브 구조의 라우팅 프로토콜에서 센서 노드는 이웃의 수(NBR)이 높고, 베이스 스테이션에 근접 할수록 클러스터 헤더가 된다. 그림에서와 같이 A1, A3의 클러스터 헤더는 B2가 되고, B1, B2, B3 등 두 개 이상의 root는 C1이 된다. 노드 C1은 BS(베이스 스테이션)으로 전체 그룹 키를 최종적으로 확정하고 이를 암호화한다음 각 센서 노드에게 보낸다.

하이퍼 큐브 구조의 라우팅 프로토콜은 기존 레벨기반 계층적 라우팅 프로토콜과는 달리 최 상위 센서 노드들이 베이스 스테이션과 인접해 있어 키 관리 및 정보전달시 최단 경로 구축이 쉽다, 또한, 하나의 베이스 스테이션 주변에 4개의 최상위 센서 노드들이 위치해있어 잘못된 정보 전달을 발견하고 차단할 수 있다.

5. 결 론

센서 네트워크는 상당히 다양한 분야에 응용되고 있으며, 교량 감시 또한 센서 네트워크가 응용되는 하나의 영역임을 안다.

본 고에서는 센서 노드의 이동성을 가정하는 일반적인 센서 네트워크의 경우와 달리 고정되 센서들로 이루어진 센서 네트워크의 경우에 요구되는 보안기법이 서로 다를 수 있다는 것에 초점을 두었다.

관련 연구들을 살펴본 결과, 이동성이 많지 않은 센서 노드 또는 한 곳에 고정된 센서 노드들로 이루어진 네트워크에서는 노드의 이동성이 희박하기에 실시간 인증이나 여러 개의 키를 생성 또는 분배하기 보다. 적은 키로 Grid 구조를 가진 네트워크구조에서 보다 효율적인 보안을 유지할 수 있을 것이라는 아이디어를 도출하였다.

앞으로 우리가 해야 할 과제는 시뮬레이션을 통해 센서 네트워크에 적용, 성능분석을 통하여 레벨기반 센서 네트워크 보안구조와 비교하여 성능향상 정도를 측정하고 보다 나은 기술에 대해 생각해 보는 것이다.

참고문헌

[1] I.F. Akyildiz,W. Su, Y. Sankarasubramaniam, and E. Cyirci. Wireless sensor networks: A survey. In *Computer Networks*, volume 38(4), pages 393- 422, 2002.

[2] T. Nieberg, S. Dulman, P. Havinga, L.v. Hoesel, and J.Wu. Collaborative algorithms for communication in wireless sensor networks. In T. Basten, M. Geilen, and H. de Groot, editors, *Ambient Intelligence:Impact on Embedded Systems Design*, pages 271- 294.Kluwer Acad. Publishers, 2003.

[3]Tieyan Li, " Security Map of Sensor Network," http://www.i2r.a-star.edu.sg/icsd/SecureSensor/papers/ security-map.pdf, Aug. 2004.

[4] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci, Wireless sensor networks: a survey Computer Networks 38 (2002) 393- 422, December 2001

[5] http://dutetvg.et.tudelft.nl/~alex/CFP/

[6]Jean-Pierre Avognon, Zhi Tang Li, " New Multicast Technology Survey and Security Concerns," Information Technology Journal 3 (1): 95-105, 2004.

[7]http://www.ietf.org/internet-drafts/draft-ietf-msec-tesla-spec-00.txt draft-ietf-msec-tesla-intro-01.txt

[8] 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.

[9] 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.

[10] Sencun Zhu, Sanjeev Setia, and Sushil Jajodia, " LEAP: Efficient Security Mechanisms for Large-Scale Distributed Sensor Networks," Proc. of the 10th ACM Conference on Computer and Communication Security (CCS), 2003.

[11] J. Deng, R. Han, and S. Mishra, " Enhancing Base Station Security in Wireless Sensor Networks," Technical Report CU-CS-951-03, Department of Computer Science, University of Colorado, Apr. 2003.

[12] Yee Wei Law, Ricardo Corin, Sandro Etalle, and Pieter H. Hartel, " A Formally Verified Decentralized Key Management Architecture for Wireless Sensor Networks," Proc. of PWC ' 03, Sep. 2003.

[13] Malik Tubaishat, Jian Yin, Biswajit Panja, and Sanjay Madria, " A Secure Hierarchical Model for Sensor Network," Proc. of SIGMOD, Mar. 2004.

[14] Mathias Bohge and Wade Trappe, " An Authentication Framework for Hierarchical Ad Hoc Sensor Networks," Proc. of WiSE ' 03, 2003.

[15] D. Liu and P. Ning, " Establishing Pairwise Keys in Distributed Sensor Networks," Proc. of the 10th ACM Conference on Computer and Communication Security (CCS), 2003.

[16] D. Liu and P. Ning, " Location-Based Pairwise Key Establishments for Static Sensor Networks," Proc. of the 1st ACM Workshop on the Security of Ad Hoc and Sensor Networks (SASN), 2003.

[17] G. Jolly, Kuscu, and P. Kokate, " A Low-energy Key Management Protocol for Wireless Sensor Networks," Proc. of the 8th IEEE International Symposium on Computers and Communications, June 2003.