교량 감시를 위한 센서 네트워크 브로드캐스트 인증기법

임화정*, 이헌길*
*강원대학교 컴퓨터정보통신공학과
e-mail : {hjlim, hglee}@kangwon.ac.kr

Sensor Network Broadcast Authentication for Bridge State Monitoring

Hwa-Jung Lim*, Heon-Guil Lee*
* Dept. of Computer Information and Communications Engineering, Kangwon National University

요 약

센서 네트워크는 자원의 제약을 지닌 수 많은 센서들로 구성되어있어 보안에 취약하다. 따라서 데이터를 안전하기 전달하기 위해 센서 노드와 노드, 노드와 베이스스테이션 사이에 인증을 요구하게 된다. 본 논문에서는 센서 노드와 베이스스테이션 사이에 집합 노드 (aggregate node)들을 두어 집합 노드와 베이스스테이션 사이에 강력한 시간동기화를 요구하지 않는 TESLA 기법과 집합 노드와 센서 노드 사이에 μTESLA 기법을 적용하여 교량 환경에 보다 효율적인 브로드캐스트 인증기법 방안을 제시한다.

1. 서론

무선 네트워크와 소형전기기계시스템(micro-electro-mechanical systems)들로 구성된 센서 네트워크는 새로운 컴퓨터 분야로서 작은 애드-혹 네트워크로 불리며 다양한 응용에 사용되고 있다[1]. 이러한 센서 네트워크는 군사 목적 이외에 의료 및 산업 분야, 환경 분야 및 인공 구조물 관리 감시 분야 등 다양한 분야의 제어 및 감시를 위해 활발히 연구가 진행되고 있다.

무선 센서 네트워크는 수백 내지 수천 개의 작은 센서들로 구성되어있어 에너지 효율성 및 확장 가능성 및 각종 공격에 대비한 강력한 보안 서비스를 포함한 기밀성, 무결성을 요구하며, 센서 데이터와 라우팅 제어 트래픽의 그룹 레벨 인증을 필요로 하고 있다[2].

무선 센서 네트워크에서 제시된 대부분의 보안 문제는 애드-혹 네트워크에서의 제기된 보안 문제와 거의 유사하다[3]. 그러나, 무선 애드-혹 네트워크와 달리 무선 센서 네트워크를 구성하는 센서 노드들은 적은 메모리, 배터리 용량의 제한, 컴퓨팅 성능의 제약 등 제한적인 하드웨어 자원을 가지고 있다.

위와 같은 이유로 센서들은 노드들의 키 정보 및 센싱된 데이터의 도청, 비정상적인 패킷의 유통, 메시지의 재 사용 등 데이터의 위조 및 변조 문제와 네트워크 전체를 마비 시킬 수 있는 서비스 거부 공격(Denial of Service) 등 각종 물리적인 공격에 쉽게 노출된다[4].

따라서 센서 네트워크에서는 센서 데이터 및 키의 인증을 위한 경량화된 인증 프로토콜 및 키 관리기법을 요구하게 되고, 이에 대한 연구가 활발히 진행되어왔다.

본 논문에서는 교량과 같은 인공구조물을 위한 브로드캐스트 인증기법으로 베이스스테이션과 aggregator 노드 사이에 강력한 시간동기화를 요구하지 않는 TESLA 인증 기법과 aggregator 노드와 센서 노드 사이의 인증을 위한 μTESLA 기법을 제안한다.

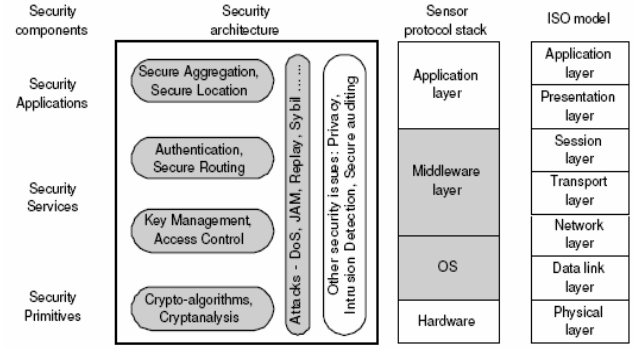
2 장에서는 센서 네트워크의 보안 요구사항을 살펴보고, 3 장은 인증 기법 관련 연구, 4 장에서는 제안하는 인증 기법을 제시한 후 5 장에서 결론 및 향후 연구에 대해 말하기로 한다.

2. 센서 네트워크의 보안 요구사항

일반 사용자에게 보다 편리한 하나의 센서 노드는 다수의 센서 노드와 브로드캐스트 방식으로 통신한다. 따라서 주위의 노드를 신뢰하기가 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].

센서 네트워크의 보안 요구사항 및 해결 방법을 살펴보면 첫째, 데이터의 기밀성(Confidentiality) 보장을 위한 암호화(Encryption)수행 둘째, 인증(Authenticity)을 위해 메시지 인증 코드(MAC)를 이용하여 각 노드 및 베이스스테이션에 대한 인증 셋째, 데이터 재사용 방지(Freshness)를 위한 일회성(Nonce)키 사용 넷째, 데이터의 무결성(Integrity)을 위해 단 방향 해쉬 함수를 이용 다섯 번째, 메시지 거부 및 부인 봉쇄(Non repudiation)를 위해 서명(Signature)을 한다[6].

위의 보안 요구 사항을 기준으로 센서 네트워크에서 필요로 하는 보안 기능은 암호 알고리즘, 키 관리 및 보안 프로토콜, 인증 및 보안 라우팅, 보안 데이터 aggregate 등으로 아래 그림 1 과 같다.



(그림 1) 센서 네트워크 보안구조

3. 센서 네트워크의 브로드캐스트 인증기법

일반적으로 두 노드 사이의 안전한 통신을 위해서는 별도의 복잡한 키 관리를 필요로 하지 않는 공개키 방식을 많이 사용하고 있으나, 제약사항이 많은 센서 네트워크 키 관리 및 보안 프로토콜에서는 대부분 대칭 키 방식의 암호 기법을 이용하는 방법이 제안되고 있다.

센서 네트워크에서 인증은 보안을 위한 가장 기본적인 단계로서, 멀티 캐스트 통신에서 각 패킷 인증에 주로 사용되는 스킴은 TESLA(Timed Efficient Stream Loss-tolerant Authentication)이다[7]. TESLA 는 지연 키 노출 방법을 사용하여 각 패킷의 인증을 수행한다. 인증키는 단 방향 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 SPINS(Security Protocols for Sensor Networks)는 센서 노드들이 베이스 스테이션과 공유하는 하나의 마스터 키를 사전에 분배하는 방식을 이용한다[6].

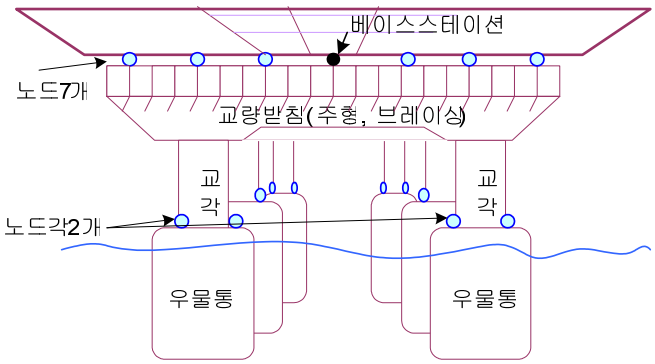
SPINS 는 센서 노드와 노드 사이에 전달되는 데이터의 기밀성 제공을 위한 SNEP(Secure Network Encryption Protocol) 구조와 베이스 스테이션으로부터 노드로 브로드캐스팅 되는 데이터의 인증을 제공하기 위한 시간 간격과 순차 번호를 이용한 μTESLA 스킴으로 구성된다.

키 관리 기법으로는 베이스 스테이션과 클러스터 구조를 중심으로 중간에 aggregator 노드를 두는 것을 기본구조로 하는 그룹 키 관리 기법[8]과 일부 노드의 노출이 근접한 이웃 노드까지 노출시키는 위협을 최소화하기 위한 LEAP(Localized Encryption and Authentication Protocol)이 있다[9].

베이스스테이션이 감염된 노드에 의한 데이터 수정을 발견할 수 있도록 하는 Hop-by-Hop 인증 기법[10]과 메시지 인증을 end-to-end, hop-to-hop 그리고 물리적과 가상적 멀티 패스 인증으로 구분하는 인증 기법이 있다[11]. 또한 AP(Access Point)를 갖는 3 계층의 애드-혹 네트워크 토폴로지를 갖는 구조를 설정하고 이들간의 효율적 인증을 위해 TESLA 를 이용한 인증서 방식을 제안한 연구도 있다[12].

4. 교량 같은 인공 구조물을 위한 브로드캐스트 인증 기법

교량 내의 센서들의 배치는 그림 2 와 같이 하나의 베이스스테이션과 다수의 센서 노드들로 구성되어있다. 또한 각 교각의 중심에는 집합 노드가 있어 센서 노드와 베이스스테이션 사이에서 각각에 대한 인증을 한다.



(그림 2) 교량 내의 노드 들의 위치

교량 감시용 센서 네트워크의 특징은 센서가 교량에 고정되어 이동성이 거의 없기 때문에 이동에 따른 배터리 소모가 작다. 노드 배치 시 위치를 지정해주

기 때문에 각 노드 간의 거리 측정이 가능하다. 또한 센서 노드와 베이스스테이션 사이에 일정 위치에 집합 노드를 두어 베이스 스테이션과 센서 노드 간의 인증을 연계해 주어 보다 강력한 보안기술 및 키 관리 기법을 수용할 수 있다.

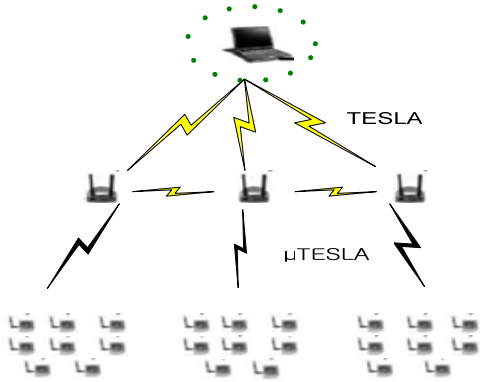
따라서 교량 감시용 센서 네트워크에서는 고정된 센서에 맞는 새로운 키 관리 및 보안 기법 제시가 필요하다.

제안하는 인증 기법은 다음과 같은 가정을 한다.

첫째, 각 그룹 별 인증방식은 그림 3 과 같다.

둘째, 베이스스테이션은 일반적인 가정을 따른다.

셋째, 집합 노드는 베이스스테이션과 센서 노드 양쪽의 인증을 담당한다.



(그림 3) 인증방식

제안하는 교량 감시용 센서 네트워크에서 인증 기법은 키 생성 및 유지가 베이스스테이션에 집중되는 것을 분산시키기 위해 베이스스테이션, 집합 노드, 센서 노드 등 3 계층 구조로 구성 한다.

각 각의 인증 방법은 아래 그림 3 와 같이 베이스스테이션과 집합 노드 사이 및 집합 노드와 집합 노드 사이에 TESLA 를 사용한다.

TESLA 는 송신자 준비, 수신자 대기, 송신자의 인증 브로드캐스트 메시지 전송, 수신자의 브로드캐스트 메시지 인증으로 구성된다[7].

Sender Setup

$T_1 = T_0 + T_{\text{int}}$

$F(k) = f_k(0)$

$K_i = F(K_{k+i})$

$K_i = F^{N-i}(K_N)$

Broadcast Authentication message

K_j, K_{j-1}, MAC

$F'(k) = f_k'(1)$

$P_j = \{M_j \| MAC(K_i', M_j) \| K_{i-d}\}$

Bootstrapping Receivers

T_{int}, *start time* T_i

Key disclosure delay d

$K_i \ (i < j - d)$

Authentication Receiver

P_j, K_{i-d}

$(i, M_j, MAC(K_i', M_j))$

(그림 4) TESLA 메시지 구성

또한 SPINS 와 같이 aggregator 노드와 센서 노드 사이에는 μTESLA 를 사용하여 인증한다[6].

위와 같이 제안한 인증 기법은 센서 네트워크의 구조에 따른 인증 기법으로 센서 네트워크를 3 계층으로 분할 했을 경우 aggregator 를 두어 베이스스테이션으로 집중되는 인증 키를 분산하여 분배할 수 있다.

또한 베이스스테이션과 aggregator 노드 사이에 인증기법으로 TESLA 를 사용하여 보다 견고한 보안을 유지 할 수 있도록 하였다.

반면, aggregator 노드와 센서 노드 사이에는 제시된 SPINS 의 인증을 이용하였다.

5. 성능 분석

교량과 같은 인공구조물에 설치되는 센서네트워크의 브로드캐스트 인증기법으로 TESLA 와 μTESLA 를 사용하였을 때, aggregator 노드와 베이스 스테이션 사이의 인증을 TESLA 로 강화할 수 있고, 노드 들에 의한 베이스스테이션 인증공격이 감소함을 알 수 있다.

5.1. 보안 분석

센서네트워크의 브로드캐스트 인증 기법중 μTESLA 기법은 모든 노드들이 가지고 있는 브로드캐스트된 인증을 받을 때까지의 시간을 계산하여 모든 노드가 다 받았을 시간을 기다려 인증 키를 보내어 인증을 하는 방식으로 보안을 위해서 노드와 베이스스테이션 간의 시간동기화, 베이스스테이션이 모든 노드가 메시지를 수신할 수 있을 정도의 시간을 계산하여 인증 키를 보내기 때문에 발생하는 시간 간격설정 문제 및 많은 수의 노드 들의 인증을 베이스스테이션 혼자 감당하는 부하 문제 등이 있다.

이러한 문제들로 발생하는 공격을 살펴보면 첫째 베이스스테이션과 많은 센서 노드 들의 시간동기화가 되지 않음으로써 모든 노드가 브로드캐스트 메시지를 받지 않았음에도 인증 키를 분배할 수도 있고, 노드들이 시간동기화가 맞지 않은 브로드캐스트 메시지를 받아들이지 않을 수도 있다.

둘째 베이스스테이션이 브로드캐스트 인증을 수행하기위해서는 수 많은 센서 노드의 수를 파악하고 이 노드들로 브로드캐스팅되는 시간을 계산하여 인증 키

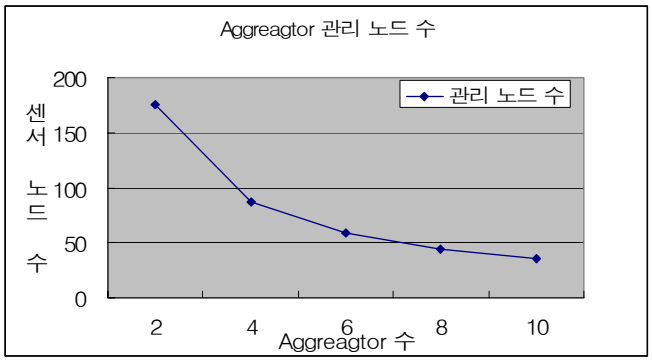
를 다시 브로드캐스팅 하므로 베이스스테이션이 관리하기엔 많은 부하가 일어날 수 있다.

5.2. 성능 분석

교량과 같이 계층적 구조를 가진 센서 네트워크에서는 이미 제시된 브로드캐스트 인증기법의 단점을 보완하기 위해 두 가지의 인증기법의 동시에 적용하여 베이스스테이션과 aggregator 노드 사이에 TESLA 기법을 사용하여 베이스스테이션이 이 모든 노드들과 시간동기화를 맞춰야 하는 부담을 각 aggregator 노드들로 분산시켰다.

또한 aggregator 노드와 센서 노드들 사이에 브로드캐스트 인증 기법으로 μTESLA 기법을 사용하여 하위 센서 노드 들의 인증을 수행한다.

제안하는 센서 네트워크환경에서 베이스스테이션에서 인증하는 노드는 aggregator 노드로 국한되어 각 aggregator 노드와 인증에 TESLA 기법을 사용하여 공개키와 유사한 인증을 수행하여 보안을 강화하였다. 그림 5 와 같이 aggregator 노드 수 A 에 따라 브로드캐스트 인증 기법을 수행 하기 위해 기다려야 하는 시간 간격이 전체 센서 노드들 N 의 수는 N/A 로 반비례하는 것을 알 수 있다. 따라서 브로드캐스트 인증을 수행할 때 설정되는 시간도 줄어들기 때문에 인증하는 전체 시간 역시 줄어듦을 유추할 수 있다.



(그림 5) 브로드캐스트 인증 시 관리 노드 수

그림 5 의 결과에서 알 수 있듯이 많은 수의 센서 노드의 브로드캐스트는 센서네트워크의 과부하를 초래하기 때문에 중간에 aggregator 노드에게 부하를 분배하는 것이 보다 빠른 브로드캐스트 인증을 수행할 수 있음을 알 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 고정된 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 희박하기 때문에 계층적인 네트워크 구조를 설계할 수 있음을 이용하여 일반 센서 네트워크에서 사용하는 SPINS 이외에 베이스와 aggregator 노드 사이에 TESLA 인증 방법을 사용하여 보다 효과적인 보안을 유지할 수 있도록 하는 방법을 제안하였다.

앞으로 우리가 해야 할 과제는 시뮬레이션을 통해 센서 네트워크에 적용, 성능분석을 통하여 베이스스테이션만이 브로드캐스트 인증 방법을 수행 하는 것과 제안한 방식과 비교하여 성능향상 정도를 측정하고 보다 나은 기술에 대해 생각해 보는 것이다.

참고문헌

[1] Jeffery Undercoffer, Sasikanth Avancha, Anupam Joshi, John Pinkston“Security for Sensor Networks,” CADIP Research Symposium, 2002.

[2] 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.

[3] Fei Hu, Jim Ziobro, Jason Tillett, Neeraj K. Sharma, “Secure Wireless Sensor Networks: Problems and Solutions “, Volume 1 - Number 4 , Journal of Systemics, Cybernetics and Informatics, 2003

[4] Rishi pidva, “security in wireless sensor networks” Communications of the ACM, Volume 47, Pages: 53 – 57, Issue 6 June 2004.

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

[6] 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, July 2001.

[7] A. Perrig, R. Canetti, B. Brisco, D. Song, and D. Tygar, “TESLA: Multicast source authentication transform introduction,” IETF working draft, draft-ietf-msec-tesla-intro-01.txt.

[8] 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.

[9] S. Zhu, S. Setia and S. Jajodia, “LEAP: Efficient Security Mechanisms for Large-Scale Distributed Sensor Networks,” Proc. of the 10th ACM Conference on Computer and Communication Security (CCS’03), Washington D.C., October, 2003.

[10] Sencun Zhu, Sanjeev Setia, Sushil Jajodia, and Peng Ning “An Interleaved Hop-by-Hop Authentication Scheme for Filtering of Injected False Data in Sensor Networks.” In Proc. IEEE Symposium on Security and Privacy, Oakland, California, May 2004.

[11] Harald Vogt, “Exploring Message Authentication in Sensor Networks. “1st European Workshop on Security in Ad-Hoc and Sensor Networks (ESAS 2004), LNCS 3313, Heidelberg, Germany, August 6, 2004.

[12] Mathias Bohge and Wade Trappe, “An Authentication Framework for Hierarchical Ad Hoc Sensor Networks,” Proc. of WiSE’03, 2003.