센서 네트워크의 다층형 데이터 보안 방법

박수용° 김성수
아주대학교 정보통신전문대학원
{cslab03°, sskim}@ajou.ac.kr

A Multi-tiered Data Security Scheme for Sensor Network Environments

Suyong Park° Sungsoo Kim
Graduate School of Information and Communication, Ajou University

요 약

센서 네트워크는 계산 용량과 에너지가 제한적이라는 특성을 가지며 그 결과 시스템의 보안관련 요구를 만족시키기 위해 기존 네트워크의 방식을 적용할 수 없다. 본 논문에서는 센서 네트워크의 보안을 위하여 기존 다층화된 보안구조에서 사용되는 키 분배 방식을 개선함으로써 에너지 소모를 크게 증가시키지 않으며 전체 네트워크의 신뢰도를 개선할 수 있는 방법을 제안한다. 랜덤 그래프의 성질을 이용한 키 분배 방식으로 이를 이용하여 비교적 낮은 에너지 소모와 개선된 신뢰성을 적절히 제공할 수 있다.

1. 서 론

센서 네트워크는 무선(유선)의 센서 노드들로 이루어진 네트워크를 의미하며 각각의 노드들은 자신의 처리능력을 내부 연산과 외부로의 데이터 전송을 위해 사용한다. 센서 네트워크와 관련하여 현재 이루어지고 있는 많은 연구들로 인해 네트워크의 저전력 동작, 빠른 노드 배치, 자가 구성, 오작동 방지와 같은 성질들이 개선되고 있다. 아래에 나와있는 센서 네트워크의 특징들은 일반적으로 연구되고 있는 기존 Ad-hoc 네트워크 환경과 구분되는 특징들로, 전체 네트워크의 보안 구조에 영향을 미치게 된다[1,2].

- 노드들은 밀집된 형태로 배치된다.
- 노드들은 실패하려는 경향을 가진다.
- 전체 네트워크의 형태가 빈번하게 변한다.
- 각 노드들이 센싱을 통해 획득한 데이터를 이웃 노드로 전송하기 위하여 브로드캐스트를 한다.
- 기존 네트워크에 비하여 센서 노드들은 전력 및 계산능력에 한계를 가진다.

2. 관 련 연 구

현재 대표적인 센서 네트워크의 보안관련 위협들은 아래의 4 가지를 들 수 있다.

- 각 센서 노드에서 실행되는 프로그램의 위/변조
- 군사용/보안용으로 쓰이는 시스템이나 고가의 센서 노드를 사용하는 시스템에서 노드 위치 정보의 발각
- 각 노드간 데이터 전송은 브로드캐스트 방식이므로 전송 데이터의 내용이 공격자에게 보여질 수 있다.
- 노드간 전송이나 노드와 기지국(base station)간에 데이터를 전송할 때 악의적인 공격자에 의해 위/변조가 발생할 수 있다.

센서 네트워크 환경에서 요구되는 보안 요소로는 데이터 무결성 및 노드 간 인증이 있으며, 이런 요소를 보장하며 4가지 주요한 보안 위협을 센서 네트워크의 한계 내에서 해결하기 위하여 기존의 시스템에서 사용되는 방법인 전송 메시지

This work is supported in the 21st Century Frontier Research and Development (R&D) Program " National Center of Excellence in Ubiquitous Computing and Network" from the Ministry of Science and Technology (MOST).
이 논문은 2004년도 두뇌한국21 사업에 의하여 지원되었음

를 암호화하여 수신시 복호화하는 방법을 고려할 수 있다. 이를 위해 사용할 수 있는 방식으로 공개키 기반 방식과 비밀키 기반 방식이 있다. 이 중 일반적으로 센서 네트워크 환경에서는 비밀키 기반 방식을 사용하게 되는데, 공개키 기반 방식의 전자 서명은 동작시 센서의 에너지와 컴퓨팅 용량을 허용 범위 이상으로 소모하기 때문이다.

그러나 비밀키 기반 방식은 통신을 위한 키를 관리하기 위한 구조가 복잡해진다는 문제점을 가진다. 또한 공개키 방식에 비해선 전력 소모가 적지만 메시지 전송시마다 암호화하게 된다면 센서 노드의 전력 한계로 인해 수명이 줄어들게 된다. 센서 네트워크의 신뢰성을 위해선 이를 개선하여 에너지의 소모를 최소화한 채로 암호화 및 복호화를 제공할 수 있는 기법이 요구된다.

3. 센서 네트워크 보안 구조

본 논문에서는 다층화된 보안구조[1]의 키 분배 방식을 개선하고자 기존의 단일 마스터 키 방식이 아닌 랜덤 그래프의 성질을 이용한 키 분배 방식을 적용한다. 다층화된 보안구조는 시스템 데이터의 보안 중요도(Security level)에 따라 암호화/복호화의 깊이(depth)에 변화를 줌으로서 에너지의 소모를 감소시킬 수 있으며 또한 랜덤 그래프의 성질을 이용한 키 분배 방식에서 키 조합의 공유 키에 의한 암호화는 중요한 데이터에 대해서 제한적인 출처 노드의 인증도 가능하게 된다.

현재 센서 네트워크의 보안을 가장 효율적으로 보장하기 위한 기법은 각 데이터의 중요성에 따라 보안 단계를 설정하여 비밀키 기반 암호화 정도에 변화를 주어 시스템의 부담을 줄이는 다층화된 보안구조 방식이다. 이 방식은 데이터의 중요성에 따라 보안 단계를 변화시켜 전력 소모를 차별화 할 수 있으며 각 응용 시스템의 목적에 따라 보안 단계의 계층 구조를 재구성할 수 있으므로 매우 효율적인 보안 구조이다.

이러한 구조에서 각 노드간 통신을 위해 사용된 비밀키 구조는 그림 1과 같이 센서 노드가 실제 서비스를 위해 배치되기 전에 전체 노드를 위한 단일 마스터 키를 생성하여 각각의 노드에 입력한 후, 노드의 배치가 이루어지고 이 마스터 키에서 의사 난수 발생기(Pseudo Random Number Generator)를 이용하여 동일한 주기로 통신용 키를 도출하여 암호화 및 복호화에 사용하게 된다. 이런 구조는 실제 적용시에 몇 가지 취약성을 가지게 되는데, 그 중 가장 심각한 문제는 외부 공격자가 전체 시스템 중 단 하나의 센서 노드라도 공격에 성공하게 된다면 전체 네트워크 시스템의 마스터 키와 의사 난수 발생기가 공개되므로 전체 시스템의 실패가 쉽게 일어나게 되는 것이다. 일반적으로 센서 노드들은 무작위로 필드상에 밀집되어 배치되기 때문에 노드가 공격자의 손에 들어갈 확률은 매우 높으며 결과적으로 공격자의 노드 획득 및 공격 성공에 대한 대비는 필수적으로 이루어져야 한다.

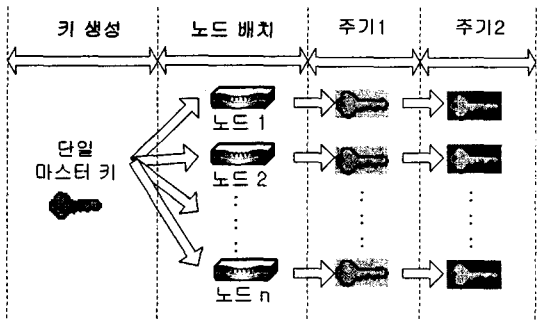

그림 1. 단일 마스터 키 기반 키 분배

이러한 단일 마스터 키 방식의 약점을 해결하기 위하여 그림 2 와 같이 랜덤 그래프의 성질을 이용한 키 분배 방식을 사용한다. 이 방식에 따르면 2^{17} 개 정도의 매우 많은 키 집합(Key pool)을 생성한 후, 시스템 상의 전체 노드들의 수 n 에 대하여 n 회씩 k 개의 키를 무작위로 선택하여 키 조합(Key ring)을 구성한 후 이를 각 노드들에 분배하는 것이다. 이후 배치된 후에 각 키 조합에 따라 인근 노드들과 키 조합내 공유 키를 설정하여 통신하게 된다.

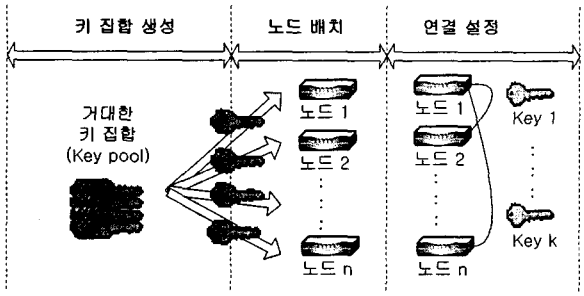

그림 2. 키 집합(key pool) 기반 키 분배

4. 성능 시뮬레이션 및 분석

제안 구조의 성능 평가를 위해 가정한 파라미터들은 표 1 과 같으며 이를 도출하기 위하여 센서 노드별로 암호화 알고리즘을 적용해 소모 에너지를 측정한 기존 논문의 결과값을 이용하였다[4].

표 1. 시뮬레이션 입력 파라미터

암호화 알고리즘	RC6
노드의 기종	Sparc 440
데이터 보안 단계	2 단계
최대 이웃 노드 수	10 개
메시지의 크기	16 byte

데이터의 중요도에 상관없이 암호화를 수행한 경우와 데이터의 중요도에 따라 다층화된 보안구조를 적용한 경우의 에너지 소모는 그림 3 과 같다. 그래프에서 보듯이 데이터에 따라 적응적으로 암호화를 하는 방식을 적용할 때 입력에 따라 전송시 에너지 소모가 감소하게 된다.

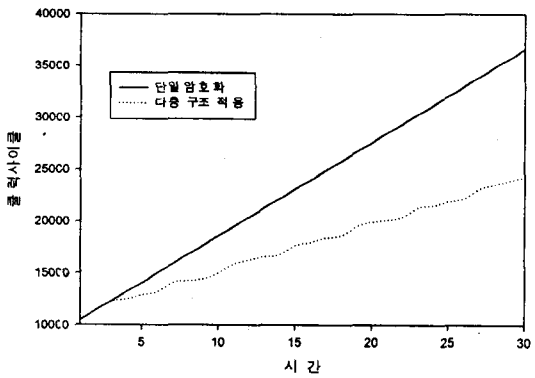

그림 3. 구조에 따른 에너지 소모 비교

또한 다층화된 보안구조 적용시 키 분배 방식에 따른 에너지 소모를 측정하기 위하여 단일 마스터 키 방식과 키 조합 방식의 에너지 소모는 그림 4 와 같다. 3 초마다 새로운 통신용 키를 도출한다고 가정했을 때 키 조합 방식의 에너지 소모가 더 크게 측정되지만 노드의 공격에 대하여 더 견고하게 동작하므로 전체 시스템의 신뢰성을 높일 수 있다.

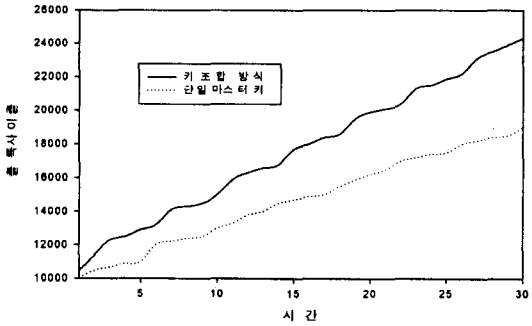

그림 4. 키 분배 방식에 따른 에너지 소모 비교

5. 결 론

본 논문에서는 에너지와 계산 용량 소모를 감소시키고 시스템의 신뢰성을 향상시키기 위하여 키 조합(Key ring) 분배 방식을 이용한 다층화된 보안구조 방식을 제안하였다. 향후 연구에서는 실제 센서 네트워크에 본 방식을 적용시 시뮬레이션에서 선택한 파라미터의 적절성과 정확성 여부를 검증하기 위한 작업이 필요하며, 또한 구조적인 취약성의 존재 여부도 조사할 필요가 있다.

6. 참 고 문 헌

[1] S. Slijepcevic, et. al., " On Communication Security in Wireless Ad-Hoc Sensor Networks," Proceedings of IEEE Workshop on Enabling Technologies: Infrastructure for Collaborative Enterprises, pp. 139-144, June 2002.

[2] J. Zhu, S. Papavassiliou, and S. Xu, " Modeling and Analyzing the Dynamics of Mobile Wireless Sensor Networking Infrastructures," Proceedings of IEEE Conference on Vehicular Technology Conference, pp. 1550-1554, Sep. 2002.

[3] L. Eschenauer and V. Gligor, " A Key-Management Scheme for Distributed Sensor Networks," Proceedings of ACM Conference on Computer and Communications Security, pp. 41-47, Nov. 2002.

[4] P. Ganesan, et. al., " Analyzing and Modeling Encryption Overhead for Sensor Network Nodes," Proceedings of ACM Workshop on Wireless Sensor Networks and Applications, pp. 151- 159, Sep. 2003.