USN에서 보안 프로토콜에 관한 연구

박익수° 오병균
목포대학교 정보공학부
{upark°, obk}@mokpo.ac.kr

A Study on Security Protocols In USN

Ik-Su Park°, Byeong-Kyun Oh
Division of Information Engineering, Mokpo National University

요 약

USN은 유비쿼터스 컴퓨팅 구현을 위한 기반 네트워크로 초경량, 저전력의 많은 센서들로 구성된 무선 네트워크이다. USN환경에서 센서 노드들이 사용 가능한 자원은 제한적이기 때문에 센서 노드들 사이에 안전한 통신 서비스를 제공하는 보안 프로토콜의 설계가 쉽지 않고, 무선통신으로 데이터를 교환하기 때문에 공격자들에게 다양한 공격들을 시도할 수 있는 기회를 제공한다. 본 논문에서는 기존에 제안된 USN에서 센서 노드간 안전한 키 설립 방법들에 관하여 살펴본다. 향후 USN 환경을 위한 센서 네트워크 기반 안전한 키 분배 보안 프로토콜을 제안하고자 한다.

1. 서 론

유비쿼터스 센서 네트워크(Ubiquitous Sensor Network: USN)는 유비쿼터스 컴퓨팅 구현을 위한 기반 네트워크로 초경량, 저전력의 많은 센서들로 구성된 무선 네트워크이다[1].

센서 네트워크는 수 많은 센서노드들로 구성되며, 센서를 통한 정보 감지 및 감지된 정보를 처리하는 기능을 수행한다. 일반적으로 센서 네트워크는 일반 PC 컴퓨팅 환경과 비교해서 제안된 CPU, 저장 공간, 대역폭, 전원 등의 제약 사항을 갖는다. 그러나 보안 요구사항은 일반적인 인터넷 환경에서 요구되어지는 수준을 만족해야 함으로 이에 적합한 연구가 이루어져야한다[2].

센서 네트워크 보안 프로토콜은 센서 노드간에 안전한 통신을 위해 키를 생성하고 분배하고 갱신하는 키 관리 연구 분야가 있다[3].

USN 키 관리 연구는 제한된 능력의 센서 노드들로 구성된 다양한 센서 네트워크 환경에 적합한 안전하고 효율적인 키 설립 방법을 설계하는 것이다. 기존에 제안된 USN 프로토콜은 신뢰하는 베이스 스테이션을 가정하고 베이스 스테이션을 경유하여 통신 가능한 이웃 센서 노드와 키를 교환하는 방식을 사용하는 SPINS(Security Protocol for Sensor Networks)[4], 같은 시간동안 노드의 노출을 근접 이웃 노드까지 노출시키는 위협을 최소화시키기 위하여 In-network processing 하는 LEAP[5], 보안 메커니즘을 데이터 별로 다양한 보안 레벨에 따라 다르게 적용함으로써 효율적인 자원관리를 수행할 수 있으며 위치 기반 스킴을 적용함으로서 네트워크의 일부에 문제가 생기는 경우에도 나머지 부분이 정상적으로 작동하는 보안 레벨 구조[6] 등이 제안되었다[3]. 최근 제안된 프로토콜은 다량의 랜덤 키를 생성하여 이를 키 풀에 저장하고 키 풀에서 무작위로 임의의 키 셋을 선택하여 각 센서 노드에게 분배하는 랜덤 키 분배방법[7]과 센서 노드간 pairwise key 설정 프로토콜로서 실제 키 값을 센서 노드들에게 할당하는 것이 아니라 키를 유도할 수 있는 다항식을 생성하여 분배하는 방법[8]들이 제안되고 있다[3].

본 논문에서는 유비쿼터스 컴퓨팅 구현을 위해 기존에 제안된 센서 노드간에 안전한 통신을 위해 키를 생성하고 분배하고 갱신하는 키 관리 프로토콜들을 살펴본다. 향후 USN 환경을 위한 센서 네트워크 기반 안전한 키 분배 보안 프로토콜을 제안하고자 한다. 본 논문의 구성은 2장에서 관련연구, 3장에서는 센서 네트워크 보안 프로토콜들을 살펴본다.

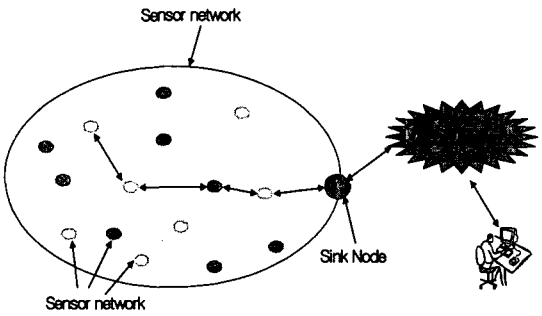
2. 관련연구

센서 네트워크는 현실적인 유비쿼터스 환경을 제공해 줄 수 있는 주요 이슈로 부각되고 있으며, 센서 네트워크의 활용 방안 및 센서 기술 개발과 함께 감지된 정보를 안전하게 처리하고 관리할 수 있는 센서 네트워크 상에서의 보안 기술들이 제안되고 있다.

2.1 센서 네트워크

센서 네트워크는 물리공간의 상태인 빛, 소리, 온도, 움직임 같은 물리적인 데이터를 센서노드에서 감지하고 측정하여 베이스 스테이션으로 전달하는 센서 노드들로

구성되는 네트워크이므로 멀티 홉 무선 네트워크 형태의 다수의 분산 센서 노드들로 구성된다. 센서 네트워크가 기존의 네트워크와 구분되는 점은 기본 목적이 상호간의 정보 전달보다는 자동화된 원격 정보의 수집에 있다. 센서 네트워크의 장점은 낮은 사양의 하드웨어를 이용하여 무선 Ad-Hoc 네트워크를 구성할 수 있다. 기존의 블루투스, 무선랜등은 반드시 컴퓨터, PDA같은 고급 컴퓨팅 장치를 필요로 하는데 센서 네트워크 노드는 독자적으로 네트워크를 구성한다. 센서 네트워크 내의 각각의 센서 노드에서 센싱된 데이터는 싱크 노트에 의하여 수집되어 인터넷 등의 외부 네트워크를 통하여 사용자에게 제공된다. 그림 1은 이런 센서 네트워크의 기본적인 구성을 보여주고 있다[9].



(그림 1) 센서 네트워크의 기본 구성도

센서 네트워크의 주요 네트워크 구조 및 특징은 센서 노드의 제한된 자원 등으로 인해 대부분의 경우에 1홉(hop)간의 통신이 아니라 멀티 홉 라우팅을 통하여 산재해 있는 센서들 간 통신이 이루어지게 되고 최종적으로 싱크 노드를 통해 센서로부터 취득한 데이터를 취합하게 된다[10].

2.2 센서 네트워크 보안 요구 사항

현재까지의 보안 프로토콜들은 제한된 자원들 사이의 절충을 통해 설계되고 있으나 기존의 네트워크에서의 보안 서비스만큼 안전성을 제공하지 못하고 있다. 센서 노드들 사이에 안전한 통신서비스를 제공하기 위해서는 기존의 네트워크에서 고려하지 않았던 추가적인 보안 요구사항이 필요하다[1].

- 센서 네트워크 환경은 수많은 센서 노드들로 구성되며, 공격자에 의한 센서 노드의 손실이나 배터리 소모와 같은 다른 물리적인 원인에 의한 센서 노드의 손실과 그에 다른 센서 노드 추가 등에 고려하여 설계되어야 한다.
- 센서 노드들은 센서 필드에 배치되기 전에 노드들 사이에 서로 인증을 할 수 있는 정보를 가지고 있어 필드에 배치된 후 이 인증정보를 가지고 메인 서버나 중간 매개체를 거치지 않고 자신의 이웃 노드들에 대한 정보를 얻을 수 있는 자가 구성 능력을 갖추고 있어야 한다.
- 공격자에게 센서 노드가 노출되었을 때 노출된 센서 노드를 탐지할 수 있는 보안 프로토콜을 설계해야한다.

3. 센서 네트워크 보안 프로토콜

센서 네트워크 보안 프로토콜에 관한 연구는 센서 노드간에 안전한 통신을 위해 키를 생성하고 분배하고 갱신하는 키 관리로 제안되고 있다.

3.1 센서 네트워크 제안 모델 및 Trust Setup 인증 구조

- SPINS[4]는 A. Perrign, R. Szewczyk, V. Wen, D. Culler, J. D. Tygar가 제안하였으며, 신뢰하는 베이스 스테이션을 가정하고 베이스 스테이션을 경유하여 통시 가능한 이웃 센서 노드와 키를 교환하는 방식을 사용하고 있다. 그러나 각 노드들은 키 교환을 위해 베이스 스테이션과 통신을 해야 하기 때문에 베이스 스테이션 주위의 노드들의 급격한 에너지 소모가 발생하므로 대규모 센서 네트워크 환경에 적합하지 않다.
- LEAP[11] Sencun Zhu, Sanjeev Setia, Sushil Jajodia가 제안하였으며, 같은 시간동안 노드의 노출이 근접 이웃 노드까지 노출시키는 위협을 최소화시키기 위하여 In-network processing 하는 센서 네트워크를 위한 키 관리 프로토콜이다.
- 계층적 보안 구조[12]는 Jing deng, Richard Han, Shivakant Mishra 가 제안하였으며, 네트워크 내부에 aggregator를 두어 중간에 데이터를 취합하여 base station에 보내고 base station으로부터의 데이터를 말단의 센서 노드에게 분배하기 위한 안전한 메커니즘이다.
- 보안 레벨 구조[13]은 Sasha slijepcevic, Miodrag Potkonjak, vlasios Tsiatsis, Scott Zimbeck, Mani B. Srivastava가 제안하였으며, 보안 메커니즘을 데이터 별로 다양한 보안 레벨에 따라 다르게 적용함으로써 효율적인 자원관리를 수행할 수 있으며 위치 기반 스킴을 적용함으로써 네트워크의 일부에 문제가 생기는 경우에도 나머지 부분이 정상적으로 작동할 수 있도록 하였다.

3.2 센서 네트워크에서의 키 관리 기법

센서 네트워크에서의 키 관리는 센서 노드간에 안전한 통신을 위해 키를 생성하고 분배하고 갱신에 관한 프로토콜들이 제안되고 있다.

- 랜덤 키 설정 기법

이 프로토콜들은 랜덤 그래프 $G(n, p)$를 기반으로 한다.

a. 랜덤 키 사전 분배는 L. Eschenauer, V. Gligor가 제안하였으며, 선택적인 키 분배와 폐기 및 부가적인 통신

이 필요하지 않은 키의 재설정에 관한 문제를 다루고 있다. 이는 랜덤 그래프 이론에 바탕을 둔 센서 노드간의 확률적 키 공유 방법을 이용하여 간단한 프로토콜을 제안함으로써 해결하였고, 공통키 설정과 키의 폐기, 키의 재설정 등을 가능하도록 하였다. 단일키를 사용한 키 설정과 Pair-wise 키를 사용한 키 설정 방법의 문제점을 보안하기 위해 제안되었다[1,2,3,7].

b. q-composite 키 분배는 H. Chan, A. Perrig, D. Song가 제안하였으며, 센서 네트워크에서의 키 설정을 위한 노드 사이에 q개의 키를 공유한다. 해쉬 함수나 XOR 방식을 통한 새로운 키 생성 방식으로 기본의 노드간의 통신을 위한 키 분배 방식 보다 노드가 공격을 당했을 때의 통신 채널의 보안성을 높였다[1,2,3,11].

c. 오버랩 키 공유를 이용한 키 분배는 Lai, Hwang, Kim. Verbauwhede가 제안하였으며, 랜덤 키 사전 분배 방법의 공용 키 풀의 구조를 키 스트링 풀로 변형하여 사용하는 방법이다[1,2,3,15].

■ 다항식 기반 키 분배

이 프로토콜들은 다항식을 이용한다.

a. Grid 기반 키 분배 구조는 D. Liu, P. Ning이 제안하였으며, 센서 노드간 pair-wise key 설정 프로토콜이다. 랜덤 키와 다른 점은 실제 키 값이 센서 노드들에게 할당하는 것이 아니라 키를 유도할 수 있는 다항식을 생성하여 분배한다. 임의의 두 센서 노드가 동일한 *t*차 다항식을 공유하여 두 노드는 그 다항식으로부터 서로 공통되는 키 값을 유도한다[1,2,3,8].

b. Location 기반 키 분배 구조는 D. Liu, P. Ning이 제안하였으며, pair-wise key 설정 프로토콜이다. Grid 기반처럼 다항식을 이용하여 센서 필드를 셀 단위로 나누고 그 셀과 고유한 다항식을 연관시켜 특정 셀에 위치하고자 하는 센서는 그 위치에 해당하는 다항식과 그 셀 인접 4개 셀에 해당하는 4개의 다항식이 할당되어 이웃 4개 셀에 배치된 센서와 pair-wise key를 생성한다[1,2,3,14].

4. 결론

센서 네트워크는 현실적인 유비쿼터스 환경을 제공해 줄 수 있는 주요 이슈로 부각되고 있으며, 센서 네트워크의 활용 방안 및 센서 기술 개발과 함께 감지된 정보를 안전하게 처리하고 관리할 수 있는 센서 네트워크 상에서의 보안 기술들이 제안되고 있다. 본 논문에서는 유비쿼터스 컴퓨팅 구현을 위해 기존에 제안된 센서 노드간에 안전한 통신을 위해 키를 생성하고 분배하고 갱신하는 키 관리 프로토콜들을 살펴보았다. 향후 USN 환경을 위한 센서 네트워크 기반 안전한 키 분배 보안 프로토콜을 제안하고자 한다.

참고문헌

[1] 이동훈, "USN 정보보호 기술 동향," ITFIND 주간기술동향, 1212, 2005.

[2] 서운석, 신순자, 구자동, 임진수 " 유비쿼터스 컴퓨팅 환경에서 보안 및 인증서비스 방향 연구," 한국전산원, 2004.

[3] 천은미외6, "센서 네트워크에서의 안전한 통신을 위한 클러스터 기반 키 분배 구조," 정보처리학회논문지 C, 제12-C권 제4호, 2005.

[4] A. Perring, R. Szewczyk, V. Wen, D.Culler, and J. Tygar, "SPINS: Security protocols for sensor networks," Wireless Networks journal, 2002.

[5] S. Zhu, S. Setia and S. Jajodia, "LEAP: Efficient Security Mechanisms for Large-Scale distributed sensor Networks," the 10th ACM Conference on Computer and Communication Security(CCS'03).

[6] S. Slijepcevic, M. Potkonjak, V. Tsiatsis, S. Zimbeck and M. B. Srivastava, "On Communication Secuirty in Wireless Ad-Hoc Sensor Network," Proc. of WETICE'20.

[7] L. Eschenauer and V. D. Gligor, "A Key-Management scheme for Distributed Sensor Networks," Proc. of the 9th ACM conference on computer and communications security, pp. 41-47, 2002.

[8] d. Liu and P. Ning, "Establishing Pairwise Keys in Distributed Sensor Networks," Proc. of the 10th ACM conference on Computer and communications Security(CCS), pp.52-61. 2003.

[9] 유승하, 류기열, "유비쿼터스 정보 단말," 정보과학회지 제23권 제9호 제196호 9, 2005.

[10] 남상엽, 송병훈, "무선 센서 네트워크 활용," 도서출판 상학당, 2005.

[11] H. Chan, A.Perrig, and D. Song, "Randdom Key Predistributed Schemes for Sensor Networks," IEEE Symposium on security and Privacy, pp.197-213,2003.

[12] J. D. Richard and S. Mishra, "Security Support for In-Network Processing in Wireless Sensor Network," Proc. of SASN '03.

[13] S Slijepcevic, M Potkonjak, V Tsiatsis, S Zimbeck, M B. Srivastava, "On Communications Security in Wireless Ad-Hoc Sensor Network," Proc. of WETICE'02.

[14] D. Liu, P.Ning, "Location-Based Pairwise Key Establishments for Static Sensor Networks,"SASN '03 First ACM Workshop on the Security of Ad Hoc and Sensor Networks, 2003.

[15] B. C. Lai, D. Hwang, S. Kim, and I. Verbauwhede, "Reducing radio energy consumption of key management scheme for wireless sensor networks,"Proceedings of ACM/IEEE International Symposium on Low Power Electronics and Desing(ISLPED'04), pp.351-356,2004.