센서 네트워크의 키 관리 기법에 대한 연구

김정식, 최경호, 임을규
한양대학교 정보통신학과

Study of Sensor Network Key Management Method

Jung-Sik Kim, Kyoung-Ho Choi, Eul-Gyu Im
Department of Information Communications, Hanyang Univ.

요 약

유비쿼터스 컴퓨팅에서는 센서 네트워크가 중요한 위치를 가진다. 센서 네트워킹의 기술이 발전하며 보안의 중요성이 떠오르고 있는데 키 관리 기법은 중요한 보안 이슈 중 하나이다. 센서 네트워크에서의 키 관리 기법은 센서 노드의 한계로 세션키, 마스터키 등을 이용하는 대칭키 방식을 사용하고 있다. 본 논문에서는 기존에 사용하는 키 관리법과 시간에 따른 신뢰도를 주는 방법을 합쳐 기존의 단점을 없애기 위한 새로운 키 관리법을 제시하였다.

I. 서론

유비쿼터스 컴퓨팅(Ubiquitous Computing)이 주목을 받으면서 이에 대한 연구가 활발해졌다. 이로 인한 기술의 비약적인 발전은 실제로 유비쿼터스 컴퓨팅을 가능해지도록 해주고 있는데 이 유비쿼터스 컴[1]퓨팅의 핵심 기술 중의 하나가 무선 센서 네트워크이다.

무선 센서 네트워크란 센서가 있어 센싱이 가능하고, 수집된 정보를 처리하고, 무선으로 전송을 할 수 있는 센서 노드로 구성된 네트워크를 말한다.

센서 노드는 센서 네트워크의 특성으로 저가, 저전력, 소형화, 메모리 제약, 제한된 계산 능력 등과 같은 성질을 가지고 있는데 지금까지는 이런 성질들을 만족시키며 성능을 높이기 위한 연구가 중심이 되어 왔다. 하지만 점차 기술의 향상과 더불어 센서 네트워크 기반의 서비스가 구체화 되면서 보안에 대한 관심이 증가하였고 그에 따라 많은 연구가 이어지고 있다.

센서 네트워크 보안은 crypto algorithm, key management, routing security, privacy 등과 같은 연구 분야가 있는데 본 논문에서는 이 중 기존의 방법을 이용한 키 관리 기법을 제시해 보았다.

본 논문의 구성은 다음과 같다. 2장은 관련 연구로서 기존의 키 관리 기법에 대해 알아보고, 3장에서는 제안하는 키 관리 기법에 대해 설명한다. 그리고 4장에서 결론 및 향후 과제를 제시한다.

II. 키 관리 기법

센서 네트워크는 센서 노드들이 설치된 이후에 안전한 네트워크 구축하고 이후에 여러 보안 프로토콜에서 사용할 키를 생성해서 분배해

1) 본 연구는 한국과학재단 특정기초연구(R01-2006-000-11196-0)지원으로 수행되었음.

주어야 한다. 하지만 센서 노드들이 처음 설치되면 신뢰할 수 없는 상태이기 때문에 키 관리 기법은 어렵고도 중요한 부분이다. 본 장에서는 센서 네트워크에서 키 관리를 위한 기법에 대해 알아보도록 한다.[1]

2.1 Key infection

Anderson, Chan, Perrig는 센서 네트워크의 최초의 키 교환을 평문상태로 교환 하는 방법을 제시하였다.[2] 이 방법은 보안이 극도로 민감하지 않은 센서 네트워크에 효율성을 위하여 사용할 수 있는 방법이다.

좀 더 자세히 살펴보면 네트워크의 최초 설치 시 각 노드들은 각자 랜덤한 세션키를 생성하게 된다. 이 세션키를 인접한 노드끼리 교환하게 되는데 이 때 키를 평문으로 전달하게 된다. 이때 공격자가 이 키를 도청할 수 있지만 최초의 대규모 노드들이 동시에 키를 교환하게 되면 공격자는 전체의 노드들 중 일부분만을 도청할 수 있다는 것이다. 그렇기 때문에 공격자가 전체 노드들 중 일부분의 키는 도청하여 노드의 제어권을 가질 수 있지만 나머지 대부분의 안전하게 키를 교환할 수 있게 된다. 공격자가 획득한 노드를 통한 다른 종류의 공격이 가능하기 때문에 네트워크의 보안 레벨은 높지 않지만 현실적으로 그리 큰 보안 레벨이 필요하지 않고 효율성이 중요한 분야에서는 의외로 큰 효과를 낼 수 있는 방법이다.

2.2 Network-wide shared key

네트워크의 모든 센서 노드들이 하나의 공용키를 갖도록 하는 방법이다. 센서 노드들이 설치되기 전에 미리 정해진 공용키를 입력받아 설치 후 이 키를 사용하는 방법을 말한다.

TinySec[3]에서 제안하는 키 관리 기법 중 하나로 이 방법을 사용할 수 있다. TinySec의 키 관리 기법은 특정 기법에 제한되지 않지만 가장 간단한 키 관리가 필요할 경우 이 방법을 사용하여 키를 관리하게 된다.

이 방법을 사용하는 다른 프로토콜로는 LEAP(Efficient Security Mechanisms for Large-Scale Distributed Sensor Networks)[4]이 존재한다. LEAP은 S.Zhu, S.Setia, S.Jajodia가 제안한 키 관리 프로토콜로 각 센서 노드를 위해 individual key, pairwise key, cluster key, group key를 제시하였다. 이 중 group key 같은 경우는 노드가 설치되기 전에 각 노드에게 할당되는 키이다.

하지만 이렇게 모두 하나의 공용키를 사용하게 되면, 하나의 노드라도 공격자에 의해 노출이 된다면 전체 네트워크의 보안이 위험해지는 상황에 놓이게 된다. 그렇기 때문에 보안성을 유지하기 위해서 주기적으로 공용키를 교환해 주는 re-keying protocol이 필요하게 된다.

Network-wide shared key 방법은 단독으로 사용하기에는 큰 위험이 존재하지만 초기에 센서 노드를 설치할 때만 이 공용키를 사용하고 실제 네트워크가 구성이 되면 다른 키 관리법에서 사용할 키를 생성하여 전달한 뒤에 이 공용 키를 폐기하면 좀 더 나은 보안성을 가지게 된다.

2.3 Base station-node pairwise key

센서 네트워크의 대부분은 게이트웨이의 역할을 해주는 베이스 스테이션을 가지고 있다.

네트워크가 신뢰할 수 있는 베이스 스테이션을 가지고 있다면, 그리고 각 센서 노드들이 베이스 스테이션과 공유하는 마스터키를 미리 가지고 있다면, 베이스 스테이션을 KDC(Key Distribution Center)로 사용하는 프로토콜을 구성할 수 있게 된다. 이 방법으로 프로토콜을 구성하게 되면 마스터키를 이용한 베이스 스테이션과의 통신을 통해 다른 노드와의 세션키를 안전하게 공유할 수 있게 된다. SPINS (Security Protocols for Sensor Networks)[5]이 이 방법을 사용하여 키를 교환하는 대표적인 방법이다.

SPINS는 데이터 기밀성, 무결성, re-play attack 방지 등의 서비스를 제공하는 SNEP과 브로드 캐스팅에서의 데이터 인증을 제공하는 μTESLA, 두 프로토콜로 구성된 보안 프로토콜이다. 여기서 데이터 암호 알고리즘을 위한 키가 필요하게 되는데 이때 안전한 베이스 스테

이션이 존재하고, 센서 노드들은 이 베이스 스테이션과 공유하는 하나의 마스터키를 사전에 분배받는다고 가정을 한다.

이 방법은 Network-wide shared key에 비하여 높은 보안성을 보장하지만 베이스 스테이션이 single-point of failure이 되고, 키 관리가 KDC와 같은 형식으로 작동하기 때문에 세션키 교환과 같은 작업을 수행하면서 상당한 네트워크 자원을 사용하게 된다. 그래서 여러 개의 베이스 스테이션을 활용하거나 세션 키의 교환 주기 설정과 같은 방법을 사용한다면 네트워크 전체의 부담을 조금 완화시킬 수 있다.

2.4 Random key pre-distribution

Random key pre-distribution 키 관리법은 network-wide shared key와 같이 센서 노드가 설치하기 전에 센서 노드에 임의의 키 값들(key ring)을 넣어주는 방법이다. 이 키 값들은 key pool이라 불리우는 키의 집합 S에서 미리 생성되어 있는 키 값을 사용하게 된다. 이 키 링의 크기는 확률 p에 의해서 결정되는데 두 개의 키 링을 추출 했을 때 최소한 하나의 공통키가 있을 확률이 p가 될 때의 크기가 키 링의 크기가 된다.

이렇게 키 링을 가지는 각 노드들이 설치되면 이웃한 센서 노드와 공통이 되는 키 값을 찾아내거나 만약 공통키가 없을 경우에는 이웃 노드를 경유하여 키를 찾아내는 방식이다. 이 방법은 확률을 사용하기 때문에 낮은 확률이지만 네트워크가 완전히 구성되지 않을 수도 있다. 또 한 센서 노드가 키 링이라 불리우는 키의 집합을 가지고 있으므로 하나의 노드가 공격자에게 넘어가면 다른 노드들이 쓰고 있을 확률이 높은 키의 집합 전체가 공격자에게 노출되고 만다.

2.5 Random pairwise key

Random key pre-distribution의 단점을 보완할 수 있는 방법이다. 키 링을 사용하는 방법으로는 같은 키를 가진 노드가 발생할 수 있고, 이 경우 다른 노드가 같은 키를 가진 노드들을 구분 할 수 없게 된다. 그리고 키 링의 유출로 인한 연쇄적인 공격도 있게 되는데 random pairwise key 방법은 random key pre-distribution과 비슷하게 사용가능 하지만 각 노드들이 고유의 키를 할당받는 방식을 사용하게 된다. 이로써 노드간의 인식과 연쇄적인 공격에 대한 대비를 할 수 있게 되었다.

2.6 Public Key Technique

지금까지의 키 관리 기법은 대칭키를 사용하는 방법이었다. 이는 공개키 방식의 키 교환은 연산이 복잡하기 때문에 제한된 능력의 센서 노드에서는 사용하기가 힘들었다. 하지만 계속적인 연구들로 인해서 공개키 방법을 센서 네트워크에서 사용할 수도 있다는 연구결과가 나오고 있는데 이것이 가능해 진다면 대칭키 방법의 근본적인 문제를 해결 할 수 있게 된다.

III. 제안하는 방법

공개키 방식을 제외하고는 기존의 키 관리 기법은 단독으로 사용하기에는 문제점들이 존재한다. 본 논문에서는 기존의 키 교환방법을 효율적으로 사용하는 방법을 제안해 본다.

3.1 개요

앞에서 살펴본 키 관리 기법들은 각각의 장단점을 가지고 있다. 여기서 제안하는 방법은 2.2, 2.3의 키 관리법을 사용하는 방법이다. 2.2의 장점은 간단한 사용법으로 빠른 처리를 해준다는 것이고, 2.3의 장점은 KDC의 역할을 하는 베이스 스테이션이 신뢰할 수 있다면 높은 보안성을 보장해 준다는 것이다.

시간의 흐름에 따라 신뢰도를 조절한다는 말은 노드들을 wide shared key를 사용하는 일정 그룹 단위로 나누어 놓은 다음 시간의 경과에 따라 그룹의 신뢰도를 높여주며 같은 신뢰도를 가진 그룹끼리 유지를 하는 방법이다.

3.2 세부 내용

어떤 센서 네트워크가 베이스 스테이션 B와 센서 노드 n1, ..., nN으로 구성되어 있다고 가정하자. 각 센서 노드는 B와 통신을 할 수 있

는 pairwise key를 미리 가지고 있다.

네트워크가 처음 설치되게 되면 베이스 스테이션이 센서 노드의 신뢰도에 따라 노드들을 구분하여 그룹을 형성하게 한다. 그룹이 나누어 지게 되면 각 그룹은 wide shared key의 성격을 가지고 있는 그룹 키를 베이스 스테이션으로부터 받게 되는데 이 이후에는 각 그룹은 그룹 내의 노드 사이에 통신을 할 경우에는 그룹키를 이용한 network-wide shared key 방식의 키 관리법을 사용하고 그룹 외의 노드와 통신을 할 때에는 베이스 스테이션을 이용한 세션키를 사용하도록 한다.

베이스 스테이션에는 각 그룹의 신뢰도가 기록되어 있는데 일정 시간이 지나면 신뢰도가 낮은 그룹의 신뢰도를 일정만큼 향상 시켜주게 된다. 일정 이상 신뢰도가 향상된 그룹은 상위 그룹에 합쳐지게 된다. 이런 작업이 반복되어 일어나게 되면 pairwise key를 이용하는 횟수가 줄어들게 된다.

하지만 그룹이 일정이상 커지게 되면 wide shared key 방식의 문제점이 나타나게 되는데 하나의 그룹이 너무 커졌을 경우에는 그룹을 적당한 크기로 다시 나누어 주게 된다. 또, 특정 노드가 공격을 받아 신뢰도가 떨어지게 되면 현재 그룹의 전 형태의 그룹으로 다시 나누어 주게 된다. 이렇게 그룹이 나누어지게 되면 wide shared key 방법처럼 모든 노드가 노출되지는 않게 된다.

IV. 결론

본 논문에서는 시간의 흐름에 따라 신뢰도를 부여하는 키 관리법에 대해 제안을 하였다. 이 방법은 2.2, 2.3의 두 관리 기법을 같이 사용하는 방법으로 2.2, 2.3의 두 장점을 모두 가지도록 고려를 해보았다. 하지만 많은 문제점이 존재하게 되는데 우선, 베이스 스테이션의 single-point of failure 문제는 여전히 해결되지 않았다. 각 그룹의 신뢰도 측정방법도 문제가 되는데 시간이 흐름에 따라 각 그룹에 동일한 신뢰도를 부여하게 된다면 그룹은 영원히 합쳐지지 않게 된다. 또 다른 문제는 특정 노드가 공격을 당하게 되면 그룹이 다시 이전 상태로 돌아간다고 하였는데, 이를 위해서는 베이스 스테이션이 전 상태의 그룹 구성과 각 그룹이 사용하던 키 값 등을 기억을 해 두어야 한다. 이는 베이스 스테이션이 더 많은 기억공간을 필요로 하기 때문에 베이스 스테이션 자체도 제약이 걸려있는 상황에서는 사용할 수 없게 된다.

새롭게 제시한 키 관리법의 문제점을 확실히 파악하고 보안하기 위해서는 새로운 방법에서 사용하는 그룹 관리법과 신뢰도 부여법에 대한 연구가 진행된 후 성능 측정을 통한 효율성에 대한 연구가 진행 되어야 할 것이다.

[참고문헌]

[1] 임채훈, "유비쿼터스 센서 네트워크 보안", 한국통신학회지(정보통신) 제22권 8호, pp. 35-50, 2005

[2] R.Anderson, H.Chan and A.Perrig, "Key infection: Smart Trust for Smart Dust", 12th IEEE ICNP, Oct. 2004.

[3] C.Karlof, N.Sastary and D.Wagner, "TinySec: A Link Layer Security Architecture for Wireless Sensor Networks", ACM SecSys 2004, Nov. 2004.

[4] S.Zhu, S.Setia, S.Jajodia, "LEAP: Efficient Security Mechanisms for Large-Scale Distributed Sensor Networks", 10th ACM CCS, 2003.

[5] A.Perrig, R.Szewczyk, V.Wen, D.Culler and J.D.Tygar, "SPINS: Security Protocols for Sensor Networks", ACM, Sep. 2002.