DOI: 10.3745/KIPSTC.2009.16-C.4.439

저속 무전 통신 환경에 적용 가능한 키 관리 방식

김 송 이[†] · 이 광 우[††] · 정 한 재[†††] · 조 영 준[†] · 차 욱 재[†] ·
김 승 주[††††] · 원 동 호[†††††]

요 약

무선 통신 기술의 발달은 기존 유선 통신 사용자에게 이동성과 접근 편리성을 제공하였다. 무선 센서 네트워크 기술은 대표적인 무선 통신 기술의 하나로, 센서 노드간의 통신에 에러가 빈번하고 통신 속도가 느린 저속 환경이며, 노드의 자원 제약 및 컴퓨팅 능력의 한계로 인해 유선 네트워크 환경에서 설계된 보안 메커니즘을 그대로 적용하는 것이 어렵다. 이러한 무선 센서 네트워크의 환경적인 제약사항이 무전 통신 환경과 유사함에 착안하여 무선 센서 네트워크 기술을 참고하여, 무전 통신 환경에 적용 가능한 효율적인 키 관리 기법을 제안하고자 한다. 본 논문에서 제안하는 방식은 일대일 통신에서 사용될 pair-wise key 설정 및 갱신, 일대다 통신에 사용될 그룹키 설정 및 갱신을 제공하며, 그룹 단위의 무전기 추가가 가능하다는 장점을 갖는다. 제안하는 master key 기반의 키 관리 방식은 군(軍)에서의 특수한 작전 수행 및 비밀 통신이 요구되는 무전 통신 환경에 활용될 수 있다.

키워드 : 무선 센서 네트워크, 키 관리, 마스터 키, 키 갱신

A Key Management Scheme for Radio Frequency Communication Environment

Songyi Kim[†] · Kwangwoo Lee[††] · Hanjae Jeong[†††] · Youngjun Cho[†] ·
Wookjae Cha[†] · Seungjoo Kim[††††] · Dongho Won[†††††]

ABSTRACT

The development of wireless communications provides mobility and accessibility to the wire communication users. Wireless sensor network is one of the leading wireless communication techniques. The security mechanism for wired network communication cannot be applied to wireless sensor network because of the limited resource and computing capability of nodes. Furthermore, communication errors frequently occur and the speed is low. Thus, efficient key management scheme is required in low-speed environment. In this paper, we proposed an efficient and secured master key-based scheme compared to the existing scheme. The advantage of our scheme is that establishing and renewing the pair-wise key is possible. In addition, it provides functions such as establishing group keys and renewing it. Furthermore, adding nodes is enabled through our scheme. The master key-based scheme can be applied to military operations and to radio communications for confidential communications.

Keywords : Wireless Sensor Network, Key Management, Master Key, Pair-Wise Key, Key Update

1. 서 론

유선 통신 환경은 유선으로 서로 연결된 통신 장비를 통해서만 통신이 가능하였기 때문에, 장소에 대한 제약이 있었다. 무선 통신 기술의 발달은 기존 유선 통신 사용자에게 장소에 상관없는 통신 환경을 제공하여 이동성과 접근 편리성을 제공하였다. 하지만 센서 네트워크의 경우 통신 에러가 빈번하고 통신 속도가 느린 저속 환경이며, 센서 노드는 제한된 자원과 컴퓨팅 능력을 갖는다. 뿐만 아니라, 무선 센서 네트워크 환경에서는 센서 노드의 배터리 소모와 추가적인 센서 노드의 배치를 고려하여 동적인 센서의 추가 및 제거가 가능해야 한다. 따라서 기존 유선 통신 환경에서 기밀성과 무결성을 제공하기 위해 제안되었던 키 관리 기법을 그대로 적용하기에는 어려움이 있어서 이러한 요구사항을 반영하여 센서 네트워크의 키 관리 방식이 제안되었다[1-5].

무전 통신 환경 역시 저속 환경으로, 무전기의 배터리는 충전 또는 교체가 필요하다는 점에서 배터리 제한이 있으며,

※ 본 연구는 지식경제부 및 정보통신연구진흥원의 대학IT연구센터 지원사업의 연구결과로 수행되었음 (IITA-2009-(C1090-0902-0016)).
† 준 회 원 : 성균관대학교 전자전기컴퓨터공학과 석사과정
†† 준 회 원 : 성균관대학교 전자전기컴퓨터공학과 박사과정
††† 준 회 원 : 성균관대학교 휴대폰학과 박사과정
†††† 종신회원 : 성균관대학교 정보통신공학부 교수
††††† 종신회원 : 성균관대학교 정보통신공학부 교수(교신저자)
논문접수 : 2009년 4월 30일
수 정 일 : 1차 2009년 6월 22일, 2차 2009년 7월 7일
심사완료 : 2009년 7월 9일

계산 능력의 한계, 낮은 대역폭과 긴 지연 시간, 무전기의 추가 및 제거관점에서 유사성을 갖는다. 센서 네트워크와 무전 통신 환경을 비교를 해보면 다음과 같다.

〈표 1〉 센서 네트워크와 무전 통신 환경의 비교

	무선 센서 네트워크	무전 통신 환경
통신 방법	무선	무선
통신 범위	근거리	근거리
통신 주체	센서	사람
통신 목적	정보수집	통신
통신 에러	빈번	빈번
배터리	제한적	제한적
추가 및 제거	필요	필요
기밀성 및 무결성	필요	필요

무선 센서 네트워크와 무전 통신 환경은 일부 통신 주체와 목적에서 차별성을 갖는다. 이러한 무선 센서 네트워크와 무전 통신 환경의 유사한 점을 바탕으로 무전 통신 환경에 무선 센서 네트워크의 키 관리 기법 적용을 고려해보았다.

현재 무전 통신 환경의 경우 주파수와 주파수 변조 방식을 동일하게 설정할 경우, 제 3자에 의해 도청이 가능할 수 있다는 문제점을 가지고 있다. 특히, 무전기를 이용하여 중요 기밀 정보를 전달하는 경우에는, 전파를 통해 송수신되는 데이터에 대한 기밀성과 무결성이 보장되어야 한다. 하지만, 무전기를 이용한 무전 통신 환경에서 기밀성과 무결성을 보장하기 위한 키 관리 기법은 현재까지 제안된 바 없다.

이에 본 논문에서는 무전 통신 환경에 적합한 키 관리 기법을 제안하고자 한다. 본 논문에서는 무전 통신 환경의 특성상 대역폭이 적고, 에러가 빈번하게 발생할 수 있으며 무전기의 저장 공간을 고려하여, 키 설정 과정에서 master key를 기반으로 하는 키 관리 방식을 제안한다.

기존에 제안된 무선 센서 네트워크의 키 관리 방식 중 master key를 기반으로 하는 방식에는 2002년 Bocheng 등에 의해 제안된 BROSK 방식[1], 2003년 Zhu 등에 의해 제안된 LEAP 방식[2], LEAP+ 방식[3], 2004년 Dutertre 등에 의해 제안된 Lightweight 방식[4], 그리고 2005년 Lim이 제안한 LEAP++ 방식[5]이 있다.

무선 센서 네트워크의 키 관리 기법을 살펴본 결과, 무선 센서 네트워크의 경우 규모를 알 수 없는 센서간의 통신을 위해 다수의 키가 필요하거나 키 설정까지의 통신에서 무결성만 제공되고 기밀성이 보장되지 않았다. 제안하고자 하는 무전 통신 환경에서의 키 관리 기법은 불특정 다수의 센서간 통신과 다르게 일대일 통신에 필요한 pair-wise key와 일대다 그룹통신에 필요한 그룹키만이 필요하였으며, 군에서 비밀 통신의 특수 상황에 적용을 위해 키 설정 과정 또한 기밀성이 요구되었다. 또한 매 통신과정에 pair-wise key는 갱신되어야 하므로, 본 논문에서는 기존의 무선 센서네트워크의 키 관리 기법을 분석하여 통신 개체 익명성을 제공하는 무전 통신 환경에 효율적이고 안전한 키 관리 방식을 제안한다. 본 논문에서 제안하는 방식은 pair-wise key와 그룹키의 설정 및 갱신을 제공하며, 그룹 단위의 무전기 추가가 가능하다는 장점을 갖는다.

본 논문의 구성은 다음과 같다. 2장에서는 기존에 제안된 센서 네트워크에서의 키 관리 기법을 살펴보고, 3장에서는 무전 통신 환경에서의 키 관리 요구사항을 분석한다. 4장에서는 무선 센서 네트워크의 키 관리 기법에 기반하여 무전 통신 환경에 적합한 master key 기반의 키 관리 방식을 제안하고, 5장에서는 본 논문에서 제안한 키 관리 기법에 대한 안전성 및 효율성 분석한다. 마지막으로 6장에서 결론을 맺는다.

2. 관련연구

기존에 제안된 센서 네트워크 키 관리 기법에는 master key 방식, 키 풀 방식, 랜덤 키 방식 등이 있다. 이 중 master key를 기반으로 pair-wise key를 설정하는 방식에는 2002년 Bocheng 등에 의해 제안된 BROSK 방식, 2003년 Zhu 등에 의해 제안된 LEAP 방식, LEAP+ 방식, 2004년 Dutertre 등에 의해 제안된 Lightweight 방식, 그리고 2005년 Lim이 제안한 LEAP++ 방식이 있다[1-5]. master key를 기반으로 키를 설정하는 방식들은 master key가 유출될 경우, 전체 네트워크에 영향을 미칠 수 있다는 문제점을 가지고 있다. 하지만 키 설정을 위해 필요한 키 저장 공간이 작고, 센서 노드 당 키 설정에 필요한 연산량을 줄일 수 있다는 장점을 갖는다.

2.1 BROSK 방식

2002년 Bocheng 등은 master key를 기반으로 pair-wise key를 설정하는 BROSK(Broadcast session key negotiation protocol) 방식을 제안하였다[1]. BROSK 방식에서는 송신자가 매 세션마다 송신자의 식별자, 난수, 그리고 master key로 계산한 메시지 인증 코드(Message Authentication Code, MAC)를 주변 노드에 브로드캐스트한다. 수신자는 master key를 이용하여 메시지 인증 코드를 검증하여 정당한 노드로부터 온 메시지임을 확인한 후, 자신의 식별자, 난수, 그리고 master key로 계산한 메시지 인증 코드를 송신자에게 전송하여 통신에 사용할 pair-wise key를 생성한다. 이 때 pair-wise key는 송신자와 수신자가 주고받은 난수를 연접한 후 master key를 이용하여 생성한다. 이 방식은 네트워크의 생명 주기 동안 하나의 master key만을 사용하므로 네트워크의 확장성 측면에서는 효율적이지만, 동일한 master key를 사용하므로 master key가 유출될 경우에는 전체 네트

워크의 보안이 취약해 질 수 있다는 문제점을 가지고 있다.

2.2 LEAP 방식

2003년, Zhu 등은 LEAP(Localized Encryption and Authentication Protocol) 방식을 제안하였다[2]. LEAP 방식에서는 master key가 유출되기 전에 키가 설정되는 것을 가정하고 있으며, pair-wise key 설정 후에는 master key를 삭제함으로써 master key가 유출되는 것을 방지하고 있다. LEAP 방식은 pair-wise key 설정을 하기 전에 각 노드별 개인키(individual key)를 생성한다. 개인키는 K_{IN}을 키로 갖는 pseudo-random 함수 f에 자신의 식별자를 입력하여 생성한다. pair-wise key를 설정하고자 하는 노드가 자신의 식별자를 브로드캐스트하면, 수신한 노드들은 자신의 식별자, 그리고 상대방의 식별자와 자신의 식별자를 연접하여 자신의 개인키로 생성한 메시지 인증 코드를 상대방에게 전송한다. 두 번의 메시지 교환 후, 키 설정을 요청한 노드 U는 master key K_{IN}과 수신한 V의 식별자를 이용해서 V의 개인키 K_v를 생성할 수 있다. 이 후 키 설정을 요청받은 노드의 개인키를 키로 하는 f함수에 키 설정을 요청한 노드의 식별자를 입력 값으로 하여 pair-wise key를 설정한다. 모든 노드 간의 pair-wise key 설정이 완료되면, master key K_{IN}은 삭제한다.

이 방식은 전체 네트워크 생명 주기 동안에 하나의 master key를 사용함으로써 발생하는 문제점을 키 설정 이후 master key를 삭제하는 것으로 개선하고자 하였다. 하지만, 노드 추가 시 동일한 master key를 계속적으로 사용하기 때문에 여전히 문제가 될 수 있으며, 한번 설정한 pair-wise key에 대한 갱신 과정이 없어 매 통신마다 새로운 키를 요구하는 무전 통신 환경의 키 관리에 적합하지 않다.

2.3 LEAP+ 방식

2003년, Zhu 등은 LEAP 방식을 개선하여 LEAP+ 방식을 제안하였다[3]. 기존의 LEAP 방식은 새로운 노드를 추가하고자 할 때, 기존에 배포된 노드들 간의 키 설정에 사용한 것과 동일한 master key를 사용하여 pair-wise key를 설정해야 한다. 이 때 동일한 master key를 사용함으로써 발생할 수 있는 문제점을 개선하고자, LEAP+ 방식은 네트워크의 생명 주기를 i개의 시간으로 분할한 후, 각 시간 간격별로 서로 다른 master key를 사용하도록 제안되었다.

두 노드 U와 V는 LEAP 방식과 유사한 방식으로 pair-wise key를 설정하며, 각 시간대에 따라 다른 master key를 사용하기 위해 시점 i가 추가되었다. 노드 U는 자신의 식별자와 자신이 추가되는 시점 i를 브로드캐스트한다. 수신한 노드 V는 자신의 식별자 v, 그리고 키 설정을 요청한 노드의 식별자와 자신의 식별자를 연접한 후 자신의 개인키 K_v^i로 계산한 메시지 인증 코드를 U에게 전송한다. 두 번의 메시지 교환 후, 키 설정을 요청한 노드 U는 master key K_{IN}^i와 수신한 V의 식별자를 이용하여, i 시점에서 V가 사용하는 개인키 K_v^i를 생성할 수 있다. 이 후 키 설정을 요청받은 노드 V의 개인키를 키로 하는 f함수에 키 설정을 요청한 노드의 식별자를 입력값으로 하여 pair-wise key K_{UV}를 설정한다.

이 방식은 특정 시간대에 다수의 노드 추가가 이루어지는 경우 LEAP 방식과 마찬가지로 동일한 master key를 사용하여 키를 설정하게 된다. LEAP+ 방식은 시간 간격 별로 서로 다른 master key를 사용하는 방식이므로 특정 유효기간에만 사용 가능한 키 관리 기법이다. 따라서 무전 통신 환경에서의 키 관리 방식에 적합하지 않다.

2.4 Lightweight 방식

2004년 Dutertre 등은 무선 센서 네트워크 환경에 적합한 경량화된 키 관리 방식을 제안하였다[4]. 이 방식은 그룹 인증키 bk_1과 키 생성 키 bk_2를 master key로 하여 pair-wise key를 설정한다.

송신 노드 A는 *Hello* 메시지, 자신의 식별자 I_A, 난수 N_A, 그리고 그룹 인증키 bk_1으로 계산한 메시지 인증 코드를 주변 노드에 브로드캐스트한다. 이를 수신한 노드는 Ack 메시지, 송신 노드의 식별자 I_A, 자신의 식별자 I_B, 자신이 생성한 난수 N_B, 그리고 bk_1을 키로 계산한 메시지 인증 코드를 키 설정을 요청한 노드에게 전송한다. 두 번의 메시지 교환을 통해 공유한 난수 N_A, N_B를 연접한 후, bk_2를 키로 이용하는 one-way hash 함수 G에 입력하여 pair-wise key를 설정한다. 모든 노드가 pair-wise key를 설정한 후에는 master key가 유출되는 것을 방지하기 위하여 bk_1과 bk_2를 삭제한다. 이 방식은 초기 노드가 배포된 후, 그룹 단위로 j번 노드가 추가를 되는 것을 고려하여 설계되었다.

2.5 LEAP++ 방식

최근 2008년 Lim은 LEAP 방식과 LEAP+ 방식에서 동일한 master key를 사용하는 시간대에 다수의 노드가 추가될 경우 master key가 유출될 수 있으며 비 인증된 Hello 메시지로 인해 DoS 공격이 가능할 수 있음을 지적하였다. 그리고 이러한 문제점을 개선하기 위해 LEAP++ 방식을 제안하였다[5]. LEAP++ 방식에서는 짧은 시간 간격 동안 단 한 번씩만 사용하는 one-time master key와 인증된 노드만이 pair-wise key를 설정할 수 있도록 사전에 계산된 pre-authenticator를 사용하는 방식을 제안하였다.

노드 U는 자신의 식별자 ID_u, 배포 식별자 j, master key의 상태 정보 s_u, 그리고 인증 요소 K_A^{2j-1}, A_u^j, R_u^j를 전송한다. 요청 메시지를 수신한 노드 V는 인증 요소를 이용하여 $K_A^{j-1} = F(K_A^j, j-1)$ 과 $F(K_A^{2j-1}, A_u^j, R_u^j) = 0 \bmod 2^L$이 만족되는지를 확인한다. 정당한 메시지로 판별될 경우, 자신의 식별자 ID_V, master key의 상태 정보 s_v, 인증 요소 중 A_v^j, R_v^j, 그리고 V 노드의 상태에 따른 키 K_x를 생

성하여 계산한 메시지 인증 코드를 전송한다. 두 번째 메시지를 수신한 요청 노드는 자신의 식별자 ID_u, 그리고 교환한 난수를 입력값으로 K_{UV}를 키로 사용하여 계산한 메시지 인증 코드를 V 노드에게 전송한다.

이 방식에서 노드 U와 V는 총 세 번의 메시지 교환을 통하여 pair-wise key 설정과 키 확인(key conformation) 과정을 수행한다. 또한 pair-wise key 설정 요청 메시지를 통해 인증을 수행하고, 인증되었을 경우에만 pair-wise key 설정이 가능하도록 함으로써 DoS 공격을 경감시키고자 하였다. LEAP 방식과 LEAP++ 방식을 비교하면, LEAP++ 방식은 LEAP 방식에 비해 메시지의 교환 횟수 및 연산량이 증가하는 단점이 존재하나, LEAP 방식에서 제공하지 않았던 키 확인 과정이 제공된다는 장점이 있다. 하지만 특정 시간 간격 동안 단 한번씩만 사용되는 one-time master key의 경우, 시간 간격을 작게 할수록 보안은 향상되나, 저장 공간이 늘어난다는 문제점이 있다. 이 방식도 LEAP+ 방식과 마찬가지로 특정 유효기간에만 사용가능한 키 관리 방식이라는 점에서 무전 통신 환경에 부적합하다고 고려되었다.

3. 무전 통신 환경에서의 키 관리 요구사항

무전 통신 환경에서의 키 관리 기법이 만족해야 하는 요구사항은 <표 2>와 같다.

무전 통신 환경에서의 키 관리 기법에 대하여 가능한 공격 방법은 <표 3>과 같다.

무전 통신 환경에서의 키 관리 방식은 <표 2>에서 분석된 키 관리 요구사항을 만족해야 하며, <표 3>에 열거된 공격 방법으로부터 안전하게 설계되어야 한다.

4. 제안하는 키 관리 방식

기존의 센서 네트워크의 키 관리 방식을 조사한 결과 BROSK 방식은 동일한 master key의 사용에 따른 문제점이 존재하였으며, LEAP 방식은 동일한 master key 사용으로 인한 문제와 pair-wise key에 대한 갱신 과정이 없으므로 매 통신마다 새로운 pair-wise key를 요구하는 무전 통신 환경의 키 관리에 적합하지 않다. 또한 LEAP+와

〈표 2〉 무전 통신 환경에서의 키 관리 요구사항

키 관리 요구사항	정의
인증 (Authenticity)	무전 통신 환경에서의 키 관리 기술은 네트워크 내에서 통신하는 무전기들이 서로를 인증할 수 있어야 한다.
기밀성 (Confidentiality)	무전 통신 환경에서의 키 관리 기술은 인증되지 않은 제 3자의 도청으로부터 통신되는 데이터를 보호해야 한다.
익명성 (Anonymity)	무전 통신 환경에서의 키 관리 기술은 인증되지 않은 제 3자의 도청으로부터 통신 개체가 드러나서는 안된다.
무결성 (Integrity)	무전 통신 환경에서의 키 관리 기술은 오직 네트워크 안에 있는 무전기만이 키에 접근할 수 있고, 통신되는 메시지들은 비인가된 변조로부터 안전해야 한다.
유연성 (Flexibility)	무전 통신 환경에서의 키 관리 기술은 무전기의 배치에 상관없이 정상적으로 동작해야 하며, 무전기의 추가나 폐기 시에도 정상적으로 동작해야 한다.
확장성 (Scalability)	무전 통신 환경에서의 키 관리 기술은 네트워크의 규모에 상관없이 높은 보안을 제공해야 하며, 저장해야 하는 값에 변화가 없어야 한다.
키 갱신 (Key update)	무전 통신 환경에서의 키 관리 기술은 주기적인 키 갱신을 통해 키를 항상 최신 상태로 유지함으로써 공격자로부터 네트워크를 보호해야 한다.
키 확인 (Key confirmation)	무전 통신 환경에서의 키 관리 기술은 통신 상호간에 같은 키를 가졌다는 확인이 이루어져야 한다.

〈표 3〉 무전 통신 환경에 대한 공격 방법

가능한 공격	정의
Replay attack	공격자가 정당한 사용자로 가장하기 위하여 이전에 사용되었던 메시지를 재사용하는 공격 방법이다.[6]
Parsing ambiguity attack	메시지 요소의 정확한 bit 수를 정의하지 않음에 따라 수신한 메시지의 분석과정에서 일어날 수 있는 모호함을 이용하는 공격 방법이다[7].
Known key attack	현재의 세션키를 구할 때 과거의 세션키를 이용하는 경우, 과거의 세션키를 아는 공격자가 현재의 세션키를 구할 수 있는 공격 방법이다[12].
Man-in-the-middle attack	공격자가 통신 참여자 사이에 위치하여 모든 통신을 가로채는 공격 방법이다[13].
Cloning attack	네트워크에 노드가 배포되는 시간동안 새로운 노드 또는 기존 노드로 위장하는 복제 노드를 주입하는 공격 방법이다[3].

LEAP++ 방식은 새로운 그룹의 추가를 위해 시간 간격 별로 서로 다른 master key를 사용하는 방식이므로 특정 유효 기간에만 사용 가능한 키 관리 방식이므로 무전 통신 환경의 키 관리 방식으로 적합하지 않았다.

본 절에서는 무전 통신 환경에 적용 가능한 키 관리 기법을 제안하고자 한다. 본 논문에서 제안하는 방식은 암호화 통신으로 통신 개체의 익명성 보장 및 초기 키 설정 이후 새로운 무전기 그룹이 추가되는 경우도 고려하였다. 또한 매 세션마다 난수를 기반으로 생성한 세션키를 사용함으로써 안전한 통신이 가능하도록 설계하였다.

4.1 제안하는 키 관리 방식에서의 표기법

제안하는 키 관리 방식에서 사용될 표기법은 <표 4>와 같다.

〈표 4〉 제안하는 키 관리 방식에서 사용하는 표기법

표기법	정의
I_X	X의 식별자
R_X	X가 생성하는 랜덤한 수
K_g	그룹키
$G_k()$	pair-wise key 생성에 사용되는 키 k를 사용하는 one-way hash function
$H_k()$	pair-wise key 갱신 및 세션키 생성에 사용되는 키 k를 사용하는 one-way hash function
mk_1	그룹 인증 master key
mk_2	키 생성 master key
gk_j	j번째 추가 무전기들의 master key
K_{XY}	X와 Y의 pair-wise key
$\{P\}_k$	키 k를 사용하여 평문 P를 암호화
SK_{AB}	무전기 A와 B가 공유하는 세션키
Hello	초기 배포 무전기의 pair-wise key 설정 요청 메시지 헤더
Ack	초기 배포 무전기의 pair-wise key 설정 요청 응답 메시지 헤더
AckCom	초기 배포 무전기의 pair-wise key 설정 과정의 키확인을 위한 메시지 헤더
AddHello	추가되는 무전기 그룹의 pair-wise key 설정 요청 메시지 헤더
AddAck	추가되는 무전기 그룹의 pair-wise key 설정 요청 응답 메시지 헤더
AddCom	추가되는 무전기 그룹의 pair-wise key 설정의 키확인 메시지 헤더
GKey	대표 무전기의 그룹키 설정 요청 메시지 헤더
GHello	새로운 그룹 무전기간의 pair-wise key 설정 요청 메시지 헤더
GAck	새로운 그룹 무전기간의 pair-wise key 설정 요청 응답 메시지 헤더
GAckCom	새로운 그룹 무전기간의 pair-wise key 설정 키확인 메시지 헤더

4.2 배포 전 무전기 설정

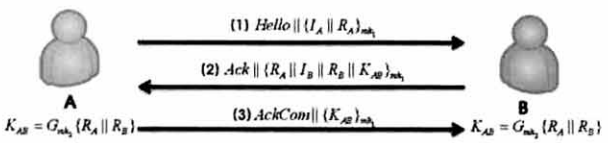
초기 배포되는 무전기들은 자신의 식별자 I_X, 그룹 인증 master key mk_1, 키 생성 master key mk_2, 최대 j번째 그룹까지의 추가를 고려한 j와 gk_j의 쌍을 저장하여 배포된다. 추가되는 그룹의 무전기에는 그룹 master key gk_j와 그 이후의 무전기 그룹 추가를 위한 j와 gk_j의 쌍을 저장하여 배포된다.

4.3 pair-wise key 설정 및 갱신 과정

비밀 통신이라는 특수 상황에의 적용을 위해서 통신에 사용될 pair-wise key 설정 과정 역시 기밀성이 유지되어야 한다. 또한 통신 개체의 익명성을 보장하기 위하여 암호화를 사용하는 방식을 제안한다.

4.3.1 초기 배포 무전기 간의 pair-wise key 설정 과정

무전기 A는 pair-wise key 설정을 위해 요청 메시지를 네트워크 전체에 있는 무전기들에게 브로드캐스트 한다. 메시지를 수신한 무전기 중 B와의 pair-wise key 설정 과정은 다음과 같다.



(그림 1) 초기 배포 무전기 간의 pair-wise key 설정 과정

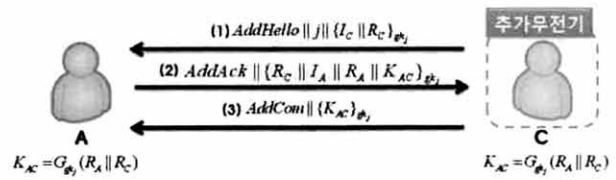
무전기 A는 $Hello$ 메시지, 자신의 식별자 I_A와 자신이 생성한 랜덤한 수 R_A를 그룹 인증 master key mk_1로 암호화한 $Hello \| \{I_A \| R_A\}_{mk_1}$를 브로드캐스트한다. 이를 수신한 B는 mk_1로 메시지를 복호화하여 얻은 랜덤값 R_A와 자신이 생성한 랜덤한 수 R_B로 pair-wise key K_{AB}를 생성한다. B는 수신 확인 Ack와 A에게 수신한 R_A, 자신의 식별자 I_B, 생성한 랜덤값 R_B, 계산하여 얻은 pair-wise key K_{AB}를 mk_1으로 암호화하여 다시 A에게 전송한다. A는 2번 메시지를 통해 B가 그룹 인증 master key mk_1을 가지고 있는 정당한 참여자임을 확인하며, 수신한 랜덤값 R_B로 pair-wise key K_{AB}를 생성한다. 생성한 K_{AB}를 B로부터 수신한 키와의 비교를 통해 키확인을 할 수 있다. 확인 과정을 거친 후, B에게 자신이 생성한 K_{AB}를 다시 암호화하여 전송함으로써, 무전기 B도 키 확인 및 무전기 A의 인증을 하게 된다. 무전기 A와 B의 pair-wise key K_{AB}의 생성 방법은 다음과 같다.

$$K_{AB} = G_{mk_2}(R_A \| R_B)$$

무전기 A와 B 사이의 초기 pair-wise key는 키 생성 master key mk_2를 키로 사용하는 G함수에 통신과정에서 주고받은 A와 B가 각각 생성한 랜덤한 수 R_A, R_B를 입력 값으로 사용하여 생성된다. 이 때, G함수의 입력 값인 랜덤한 수 R_A, R_B는 생성한 식별자의 알파벳 순서를 따른다. 본 논문에서 제안하는 방식은 무전기가 포획될 경우 master key가 유출되는 것을 방지하기 위하여 초기 pair-wise key 설정 및 그룹키 설정이 완료되면, 그룹 인증 master key mk_1과 키 생성 master key mk_2를 메모리에서 삭제한다. 이 때, 초기 배포 무전기 간의 pair-wise key 설정 시간이 오래 걸릴수록 무전기가 포획되었을 때 master key가 유출될 수 있는 가능성이 높아지므로, 초기 배포 그룹의 수는 가급적 소규모로 제한하고, 신속하게 초기 pair-wise key를 설정하도록 하는 것이 바람직하다.

4.3.2 무전기 추가 과정

무전 통신 환경에서는 초기 배포된 무전기들의 pair-wise key 설정 과정 이후에 새로운 그룹의 무전기 추가 상황도 고려해야 한다. 무전기 추가 과정은 추가되는 무전기의 통신 요청으로 시작되며, 무전기 추가 과정은 다음과 같다.

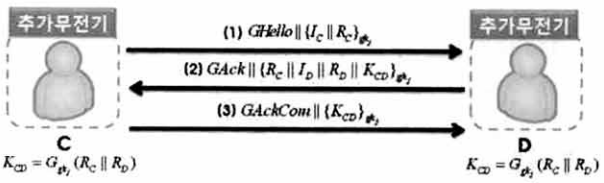


(그림 2) 무전기 추가 과정

초기 배포 그룹의 무전기 A는 추가될 그룹의 무전기 C로부터 전송받은 j를 이용하여 배포 전 메모리에 저장된 gk_j를 검색한다. A는 gk_j로 복호화하여, C가 생성한 랜덤 값을 획득한다. A는 수신 확인 메시지인 $AddAck$와 자신의 식별자 I_A, 수신한 랜덤값 R_C와 자신이 생성한 랜덤값 R_A 그리고 계산하여 획득한 K_{AC}를 gk_j로 암호화하여 다시 C에게 전송한다. C는 자신의 그룹키 gk_j로 복호화 하여 얻은 결과값과 생성한 K_{AC}의 비교를 통하여 키확인 과정을 수행한다. 이 후, 무전기 C는 무전기 A에게 설정한 pair-wise key K_{AC}를 확인시켜주기 위해 다시 $AddCom$ 메시지를 그룹키 gk_j로 암호화한 K_{AC}와 함께 A에게 전송한다. 이와 같은 방법으로 j번째 추가되는 그룹 무전기의 인증 및 pair-wise key 확인이 수행된다.

4.3.3 추가되는 무전기 간의 pair-wise key 설정 과정

초기 배포 이후에 추가되는 그룹의 무전기에 대하여, 동일한 그룹에 속해 있는 무전기 C와 D의 pair-wise key 설정은 다음과 같다.



(그림 3) 추가 무전기 간의 pair-wise key 설정 과정

위와 같은 방식으로 추가되는 모든 무전기 사이의 pair-wise key 설정과 이후의 그룹키 설정이 수행되면, gk_j를 메모리에서 삭제한다.

4.3.4 pair-wise key를 사용한 비밀 통신

모든 무전기 간의 통신은 비인가된 사용자의 도청으로부터 기밀성이 보장되어야 한다. 오랜 기간 같은 키를 사용하여 통신할 경우에는 키가 유출될 가능성이 있으므로 매 세션마다 새로운 세션키를 생성하여 통신한다. 무전기 A와 B는 데이터 통신을 수행하기 전에 랜덤한 수 R_A와 R_B를 나누어 가지며, 사전에 설정된 pair-wise key K_{AB}를 이용해서 다음과 같이 세션키를 생성한다.

$$^{New}K_{AB} = SK_{AB} = H_{K_{AB}}(R_A \| R_B)$$

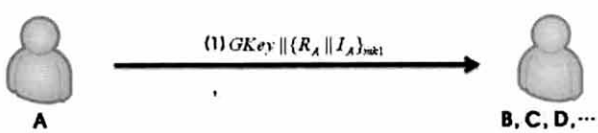
생성된 SK_{AB}로 암호화 통신을 수행하므로 제3자의 도청에 안전한 통신을 수행할 수 있으며, 사용한 세션키는 무전기 A와 B의 새로운 pair-wise key가 된다.

4.4 그룹키

무전 통신 환경에서 전체 무전기의 비밀 통신을 제공하기 위하여 그룹키가 요구되어진다. 무전 통신 환경에서 동일한 주파수를 사용하여 통신하는 경우에는 불특정 다수가 통신 내용을 도청할 수 있다는 문제점을 갖는다. 따라서 동일한 키를 가지고 있는 그룹의 참여자간의 안전한 통신을 제공하기 위하여 그룹키의 설정 및 갱신 과정을 제안한다.

4.4.1 그룹키 설정 과정

그룹키는 초기 배포 무전기들이 배포된 직 후 사전에 지정된 무전기에 의해 초기 설정이 수행되며, 설정 방식은 다음과 같다.



(그림 4) 그룹키 설정 과정

사전에 지정된 무전기 A는 배포와 동시에 그룹키 설정을 알리는 $GKey$와 그룹 인증 master key mk_1로 암호화한 자신이 생성한 랜덤값 R_A와 자신의 식별자 I_A를 브로

드캐스트한다. 이를 수신한 모든 무전기들은 다음과 같이 그룹키를 생성한다.

$$K_g = G_{mk_1}(R_A \| I_A)$$

그룹키 요청 메시지를 수신한 무전기들은 그룹 인증 master key mk_1을 통해 메시지를 복호화하여, 사전에 그룹키를 요청하기로 지정된 무전기의 식별자와 현재 그룹키 요청을 한 A의 식별자 비교를 통해 정당한 메시지인지 확인한다. 확인 후에는 수신한 요소를 이용하여 그룹키 K_g를 생성한다.

4.5 그룹키를 사용한 통신 과정

그룹키를 사용한 그룹 전체 통신은 그룹 통신의 특성 상 공지사항과 정보 전달을 목적으로 시작된다. 따라서 특정 무전기의 그룹통신 요청에 의해 그룹 세션키를 맺고 그 키를 이용하여 통신을 한다. 그룹 세션키 설정은 다음과 같다.

$$^{New}K_g = G_{K_g}(I_A \| R_A)$$

위와 같이 생성된 그룹키는 다음 그룹 통신 요청이 있을 때까지 모든 무전기가 공유하고 있으며, 새로운 그룹 통신이 있을 경우에 위와 같은 과정을 거쳐 그룹키 갱신을 수행한다.

5. 안전성 분석

이 장에서는 앞서 소개된 무전 통신 환경에서의 요구사항을 바탕으로 키설정 과정의 기밀성을 제공하기 위하여 암호화 통신을 하며, 키확인 과정을 제공하는 제안한 키 관리 방식의 안전성에 대하여 분석한다. <표 5>는 본 논문에서 제안하는 키 관리 방식과 기존에 제안된 방식들의 요구사항 만족 여부를 비교하여 나타낸 표이다.

〈표 5〉 제안하는 키 관리 방식과 기존 키 관리 방식의 요구사항 만족 여부 비교

구분	BROSK [1]	LEAP [2]	LEAP+ [3]	Light weight [4]	LEAP++ [5]	제안하는 방식
인증	O	-	-	O	O	O
기밀성	O	O	O	O	O	O
익명성	×	×	×	×	×	O
무결성	O	O	O	O	O	O
유연성	O	O	O	O	O	O
확장성	×	×	O	O	O	O
키갱신	O	-	-	-	-	O
키확인	×	×	×	×	O	O

※ O : 만족함 × : 취약함 - : 제공하지 않음

- 인증 : 제안한 키 관리 방식은 사전에 공유하고 있는 master key를 알고 있는 자만이 정당한 메시지를 생성할 수 있도록 하였다. 초기에 배포되는 무전기들은 배포 전에 master key인 mk_1과 mk_2를 포함하여 배포되며, master key를 알고 있는 무전기만이 pair-wise key를 설정할 수 있다. 또한 추가되는 무전기의 경우에도 그룹 master key인 gk_j를 알아야만 기존 그룹에 포함되어 있는 무전기들과 pair-wise key를 설정할 수 있다.

- 기밀성 : 무전기 간의 모든 통신 내용은 pair-wise key로부터 유도된 세션키를 이용하여 암호화되어 통신되기 때문에, 비인가된 사용자는 통신 내용을 볼 수 없다. 또한 그룹 통신의 경우에도 그룹키로 암호화하여 통신되기 때문에, 그룹에 속하지 않은 제 3자는 통신 내용을 볼 수 없다.

- 익명성 : 무전 통신 환경의 비밀 통신에서는 무전기 간의 키설정 과정에서도 통신 개체의 익명성이 요구되어진다. 제안하는 방식에서는 통신 내용을 암호화하여 전송함으로써 익명성을 제공하였다.

- 무결성 : 무전기 사이에 주고받는 모든 메시지는 사전에 공유하고 있는 pair-wise key 또는 그룹키를 사용하여 암호화하여 전달하기 때문에 메시지의 무결성을 보장한다.

- 유연성 : 제안한 키 관리 방식은 무전기가 배포되기 전에 j번의 무전기 그룹이 추가되는 경우를 고려하여 j와 gk_j의 쌍을 저장하여 배포한다. 따라서 무전기의 수에 상관없이 j번의 그룹이 확장가능하다.

- 확장성 : 제안한 키 관리 기법은 그룹단위의 무전기 추가가 가능하며 무전기 추가가 기존 참여자들의 안전성에 영향을 미치지 않는다.

- 키 갱신 : 제안한 키 관리 방식은 크게 pair-wise key와 그룹키에 대한 갱신 과정을 제공한다. pair-wise key의 경우, 매 세션마다 무전기가 교환한 새로운 랜덤값을 기반으로 새로운 pair-wise key를 설정하여 통신한다. 또한 그룹키의 경우에도 통신을 요청하는 참여자의 식별자와 랜덤값으로 갱신하여 통신한다.

- 키 확인 : 제안한 키 관리 방식은 암호화 통신을 하며, 3번의 메시지 교환으로 통신의 참여자가 동일한 키를 가지고 있다는 확인과정을 수행한다.

<표 6>에서는 제안하는 키 관리 방식과 기존에 제안된 방식들에 가능한 다양한 공격에 대해 안전성을 분석한 것이다.

〈표 6〉 제안하는 키 관리 프로토콜에 대한 안전성 비교

구 분	BROSK [1]	LEAP [2]	LEAP+ [3]	Light weight [4]	LEAP++ [5]	제안하는 방식
Replay attack	○	○	○	○	○	○
Parsing ambiguity attack	○	○	○	○	○	○
Known key attack	○	-	-	-	-	○
man-in-the-middle attack	○	○	○	○	○	○
cloning (or replication) attack	×	×	×	○	○	○

※ ○ : 안전함 × : 취약함 - : 제공하지 않음

• Replay attack

본 논문에서 제안하는 방식은 pair-wise key 설정 과정에서 전송하는 메시지에 master key를 사용하여 계산한 메시지 인증 코드를 포함하고 있다. 따라서 메시지의 변조 및 재전송 공격이 불가능하고, pair-wise key 설정 과정 이후, 세션마다 서로 다른 세션키를 사용하므로 재전송 공격으로부터 안전하다.

• Parsing ambiguity attack

키 관리 프로토콜에서 메시지의 길이를 정의하지 않았을 경우 또는 이웃해 있는 메시지 요소와의 경계가 불명확한 경우, 공격자는 메시지의 일부를 변조함으로써 수신자가 메시지를 파싱하는 과정에서 정당한 프로토콜의 참여자에게 혼란을 줄 수 있다. 이 공격은 사전에 메시지 포맷 또는 길이를 고정함으로써 방어 가능하다. 본 논문에서 제안하는 키 관리 방법은 식별자는 32bit, 타임스탬프 32bit, 랜덤한 수 128bit, pair-wise key, 세션키 및 그룹키는 AES 알고리즘의 128bit 키를 사용함으로써 메시지 요소들 간의 경계가 명확하고, 모든 메시지에는 메시지 인증 코드를 포함하여 전송하므로 공격자가 파싱 과정의 모호함을 이용하는 Parsing ambiguity attack으로부터 안전하다(Appendix 1 참고).

• Known key attack

본 논문에서 제안하는 키 관리 방식에서는 이전 세션키를 이용하지 않고 매 세션마다 통신에 참여하는 노드가 새로 생성한 랜덤한 수와 pair-wise key를 바탕으로 one-way hash 함수를 이용하여 새로운 세션키를 생성하기 때문에, 이전에 사용하던 세션키가 노출되더라도, 이후 생성되는 세션키를 유추할 수 없다. 따라서 본 논문에서 제안하는 방식은 해당 공격으로부터 안전하다.

• Man-in-the-middle attack

본 공격은 통신과정에서 교환하는 값의 인증 과정이 없을 경우에 가능하다. 본 논문에서 제안한 키 관리 방식에서는 모든 메시지에 메시지 인증 코드를 포함하여 교환되는 메시지들을 인증하고 있으므로 해당 공격에 안전하다.

• Cloning attack

본 논문에서 제안한 키 관리 방식에서 노드는 배포되는 시점에서 짧은 시간 내에 키 설정을 완료한다. 초기 키 설정 동안에는 공격자가 배치 장소 및 시간에 대해 사전 정보가 없으므로 노드 포획을 통한 능동적 공격은 어렵다는 이론과 제안한 방식의 초기배포는 소규모로 할 것을 권장하고 있으므로 해당 공격에 대해 안전하다.

6. 결 론

본 논문에서는 저속 무전 통신 환경에 적용 가능한 master key 기반의 pair-wise key 설정 및 갱신 방법과 그룹키 설정 및 갱신 방법을 제안하였다. 본 논문에서 제안하는 방식은 pair-wise key 설정 이후, master key를 삭제하는 방식으로 master key 유출에 따른 문제점의 제거하고자 하였으며, pair-wise key와 난수를 바탕으로 통신에 사용될 세션키를 매 세션 생성하여 사용함으로써 안전한 통신을 고려하였다. 그룹키는 통신을 요청하는 무전기에 의하여 갱신되도록 제안하였다. 본 논문에서는 기존의 무선 센서 네트워크와 무전 통신 환경의 공통점에 기반하여 무전 통신 환경에 적합하게 개선하여 키관리를 제안하였다. 제안한 방식은 그룹 단위의 무전기 추가가 가능하며 군(軍)과 같이 특수한 작전 수행 및 비밀 통신이 요구되는 저속 무전 통신 환경에 활용될 수 있다.

참 고 문 헌

[1] Bocheng Lai and Sungha Kim, "Scalable Session Key Construction Protocol for Wireless Sensor Networks", IEEE Workshop on Large Scale Real-Time and Embedded Systems(LARTES), 2002.

[2] Sencun Zhu and Sanjeev Setia, "LEAP:Efficient Security Mechanisms for Large-Scale Distributed Sensor Networks", In: Proceedings of the Tenth ACM conference on Computer and Communications Security, pp.62-72, October, 2003.

[3] Sencun Zhu and Sanjeev Setia, "LEAP+: Efficient security mechanisms for large-scale distributed sensor networks", ACM Trans. on Sensor Networks, 2(4), pp.500-528, 2006 (the journal version of CCS'03 paper).

[4] Bruno Dutertre and Steven Cheung, "Lightweight Key Management in Wireless Sensor Networks by Leveraging Initial Trust", SDL Technical Report, SRI

International, SRI-SDL-04-02, April 6, 2004.
[5] Chae Hoon Lim, "LEAP++: A Robust Key Establishment Scheme for Wireless Sensor Networks", The 28th International Conference on Distributed Computing Systems Workshops, pp.376-381, 2008.
[6] YC Lee, YC Hsieh, PS You, "A New Improved Secure Password Authentication Protocol to Resist Guessing Attack in Wireless Networks", ACACOS '08, pp.160-163, 2008.
[7] Liqun Chen and Chris J. Mitchell, "Parsing ambiguities in authentication and key establishment protocols", 30th September, 2008.
[8] Chris Karlof and David Wagner, "Secure routing in wireless sensor networks: attacks and countermeasures", Proceedings of the First IEEE. 2003 IEEE International Workshop on, pp.113-127, 2003.
[9] 김용호, 이화성, 이동훈, "소모형 센서 네트워크 환경에 적합한 키 관리 스킴", 정보보호학회논문지, pp.71-80, 2006.
[10] SEYIT A. CAMTEPE and BULENT YENER, "Key Distribution Mechanisms for Wireless Sensor Networks: a Survey", IEEE/ACM Transactions on Networking (TON), Vol.15, pp.346-358, 2007.
[11] Wen-Shenq Juang and Jing-Lin Wu, "Two efficient two-factor authenticated key exchange protocols in public wireless LANs", Computers&Electrical Engineering, Vol.35, pp.33-40, 2009.
[12] Jeeyeon Kim, Seungjoo Kim, Kilsoo Chun, Jaeil Lee, Dongho Won, "Group Key Agreement Protocol Among Mobile Devices in Different Cells", LNCS, Vol.4331, pp.1090-1097, 2006.
[13] Dang Nguten Duc and Kwangjo Kim, "Securing HB+ against GRS Man-in-the-Middle Attack", SCIS 2007, 2007.
[14] 김종은, 조경산, "센서 네트워크의 노드간 세션키 생성을 위한 개선된 프로토콜", 정보처리학회논문지, Vol.13, No.2, pp.137-146, 2006.
[15] 김태연, "무선 센서 네트워크를 위한 새로운 키 사전 분배 구조", 정보처리학회논문지, Vol.16, No.2, pp.183-188, 2009.

김 송 이

e-mail : s2kim@security.re.kr
2006년 강남대학교 지식정보공학부(학사)
2008년~현 재 성균관대학교 전자전기컴퓨터공학과 석사과정
관심분야 : 네트워크 보안, 인증, 키관리, 정보보호

이 광 우

e-mail : kwlee@security.re.kr
2005년 성균관대학교 정보통신공학부(학사)
2007년 성균관대학교 전자전기컴퓨터공학과 (석사)
2007년 ~현 재 성균관대학교 전자전기컴퓨터공학과 박사과정
관심분야 : 암호이론, 정보보호, 네트워크 보안, 전자투표

정 한 재

e-mail : hjjeong@security.re.kr
2006년 성균관대학교 정보통신공학부(학사)
2008년 성균관대학교 전자전기컴퓨터공학과 (공학석사)
2008년~현 재 성균관대학교 휴대폰학과 박사과정
관심분야 : 정보보호, 보안성 평가, 무선네트워크

조 영 준

e-mail : yjcho@security.re.kr
2008년 성균관대학교 정보통신공학부 컴퓨터공학과(학사)
2008년~현 재 성균관대학교 전자전기컴퓨터공학과 석사과정
관심분야 : 네트워크 보안, 암호이론, 정보보호, 보안성 평가

차 욱 재

e-mail : wjcha@security.re.kr
2005년 서울산업대학교 컴퓨터공학과(학사)
2008년~현 재 성균관대학교 전자전기컴퓨터공학과 석사과정
관심분야 : 암호이론, 네트워크보안, IPTV, DRM, 정보보호

김 승 주

e-mail : skim@security.re.kr

1994년~1999년 성균관대학교 정보공학과 (학사, 석사, 박사)

1998년~2004년 한국정보보호진흥원(KISA) 팀장

2004년~현 재 성균관대학교 정보통신공학부 교수

2001년~현 재 한국정보보호학회, 한국인터넷정보학회, 한국정보과학회, 한국정보처리학회 논문지 및 학회지 편집위원

2002년~현 재 한국정보통신기술협회(TTA) IT 국제표준화 전문가

2005년~현 재 디지털콘텐츠유통협의체 보호기술워킹그룹 그룹장

관심분야 : 암호이론, 정보보호표준, 정보보호제품 및 스마트카드 보안성 평가, PET

원 동 호

e-mail : dhwon@security.re.kr

1976년~1988년 성균관대학교 전자공학과 (학사, 석사, 박사)

1978년~1980년 한국전자통신연구원 전임연구원

1985년~1986년 일본 동경공업대 객원연구원

1988년~2003년 성균관대학교 교학처장, 전지전자 및 컴퓨터공학부장, 정보통신대학원장, 정보통신기술연구소장, 연구처장

1996년~1998년 국무총리실 정보화추진위원회 자문위원

2002년~2003년 한국정보보호학회장

2002년~현 재 대검찰청 컴퓨터범죄수사 자문위원, 감사원 IT 감사 자문위원

2007년~현 재 성균관대학교 정보통신공학부 교수, 한국정보보호학회 명예회장

관심분야 : 암호이론, 정보이론, 정보보호