Koinonia 고속 WPAN에서 보안을 위한 대칭/비대칭 비밀 키 교환 방법

정회원 임 순 빈*, 준회원 정 쌍 봉*, 종신회원 이 태 진*,
정회원 전 선 도**, 준회원 이 현 석***, 정회원 권 대 길***, 조 진 웅***

Generation and Distribution of Symmetric/Asymmetric Secret Keys for Secure Communications in Koinonia High-rate WPAN

Soon-Bin Yim* ***Regular Member***, Ssang-Bong Jung* ***Associate Member***,
Tae-Jin Lee*, ***Lifelong Member***, Sun-Do June** ***Regular Member***, Hyeon-Seok Lee* ***Associate Member***,
Tai-Gil Kwon**, Jin-Woong Cho** ***Regular Members***

요 약

무선 개인 네트워크(Wireless Personal Area Network: WPAN)에서 보안은 최근 무선 환경이 가지고 있는 기본적인 단점들을 극복하기 위한 중요한 이슈 중 하나이다. IEEE 802.15 등 WPAN 표준들에는 몇몇 보안 관련 기본 메커니즘이 정의 되어 있지만 아직 해결해야 할 문제들이 남아있다. 고속 WPAN 기술 중 하나인 Koinonia는 무선으로 근거리 디바이스들을 연결하여 10Mbps 정도의 고속 통신을 하기 위해 개발되었다. Koinonia WPAN의 피코넷(piconet)은 하나의 마스터(Master)와 하나 이상의 슬레이브(Slave)로 구성되며, 이와 같이 구성된 피코넷에서 기기 간 안전한 데이터 전송을 보장하기위한 보안 관련 내용은 정의되어 있지 않다. 따라서 본 연구에서는 Koinonia의 피코넷 내 기기 간 통신시 안전한 데이터 통신을 위한 대칭/비대칭 키 기반의 키 생성 및 분배, 인증 및 보안방법을 제안하고 성능을 분석한다. 보안 요구 분석을 기반으로 Koinonia WPAN의 보안 요구에 만족함을 알 수 있다.

Key Words : KOINONIA, WPAN, security, symmetric key, asymmetric key, key management

ABSTRACT

Security in WPAN is one of the most fundamental issues to overcome the barrier of wireless environment. Although piconet security mechanisms have been defined in the WPAN standards, many remains open and are left for implementation. Koinonia is a high-rate Wireless Personal Area Network (WPAN) technology, and is developed for multimedia traffic transmission in personal area. In Koinonia WPAN, a piconet consists of one master and more than one slave, and piconet security mechanisms is not defined at all. Therefore, we propose a robust piconet security mechanism for secure communications between slaves in a piconet. Based on security requirements analysis, our proposed protocols are shown to meet the security needs for Koinonia high-rate WPAN.

※ 본 연구는 정보통신부 지원 Electro-0580사업의 "복합위상 신호를 적용한 다중접속 칩셋 개발과제"로 수행되었습니다.
* 성균관대학교 정보통신공학부 네트워크시스템연구실 ({jssbong, sbyim, tjlee}@ece.skku.ac.kr)
** 경기공업대학교 전자통신과 (jsd@kinst.ac.kr), *** 전자부품연구원 통신네트워크센터 ({hslee75, tgkwon, chojw}@keti.re.kr)
논문번호 : KICS2005-12-515, 접수일자 : 2005년 12월 30일, 최종논문접수일자 : 2006년 6월 12일

Ⅰ. 서 론

WPAN(Wireless Personal Area Networks)은 단거리(10m이내)에 놓여 있는 컴퓨터와 주변기기, 이동단말기, 가전기기 등을 무선 네트워크로 연결하여 기기 간 양방향 통신을 이루어 다양한 응용분야를 지원하는 기술이다. 또한 WPAN은 소형 저가격, 저전력으로 구현이 가능하며, 기반시설과 거의 상관이 없으므로 다양한 장치에 구현할 수 있다. 이와 같은 WPAN은 컴퓨터, 노트북, PDA, 휴대폰, 프린터, 마이크, 스피커, 헤드셋, 디스플레이, 센서, 제어기기 등과 같은 기기에 주로 휴대용으로 사용할 수 있다. 현재 대표적인 WPAN 기술로는 IEEE 802.15.1 (Bluetooth)[1], IEEE 802.15.3[2, 4], IEEE 802.15.4 (ZigBee)[3] 등이 있다.

IEEE 802.15.1[1]과 IEEE 802.15.4[3]는 20kbps~1Mbps 정도의 전송률을 지원하기 때문에 MP3플레이어나 디지털 카메라 등과 같이 수백 Kbps~수십 Mbps의 데이터 전송이 요구되는 고속 WPAN 환경에는 적합하지 않다. 이러한 고속 멀티미디어와 데이터 전송을 위한 WPAN 기술로 IEEE 802.15.3[2, 4]표준이 있다. IEEE 802.15.3은 2.4GHz에서 작동하고 최대 55Mbps의 속도를 지원하는 고속 WPAN 표준이다. 그리고 IEEE 802.15.3 WPAN과 같이 2.4GHz에서 동작하고 최대 12.4Mbps의 속도를 지원하는 Koinonia 기술이 있다[5-7]. Koinonia에서 위상 변조 방식과 멀티 코드 대역 확산 기술을 이용한 물리 계층은 강한 내 잡음성과 자유롭게 조정이 가능한 대역폭을 제공해 주며, 트래픽 특성에 맞는 서비스 품질을 보장해 주므로, 단순 데이터 뿐 아니라 음성, 비디오와 같은 멀티미디어 서비스를 지원하는데 효과적이다.

이와 같이 WPAN에서 데이터 전송의 고속화와 편이성에 의해 무선의 효용성이 증가 되면서 무선 환경에서 안전한 데이터 통신을 위해 보안이 중요한 이슈가 된다. Bluetooth에서는 키 생성 및 암호화에 관련한 보안 알고리즘이 제안되어 있고, IEEE 802.15.3와 IEEE 802. 15.4 표준에서는 데이터 암호화를 위하여 CCM (CTR+ CBC-MAC)방식을 이용하는 방법이 정의되어 있지만 키 분배 방법 등이 정의되어 있지 않아 아직 해결해야 할 부분들이 남아있다. 이와 같은 부분을 해결하기 위해 관련 연구가 진행 중이다. 논문[7, 8]은 WPAN의 개인인증기관(Personal Certificate Authority: PCA)라는 개념을 도입하여 기기 간 인증과 인증서 관리에 관한 방법

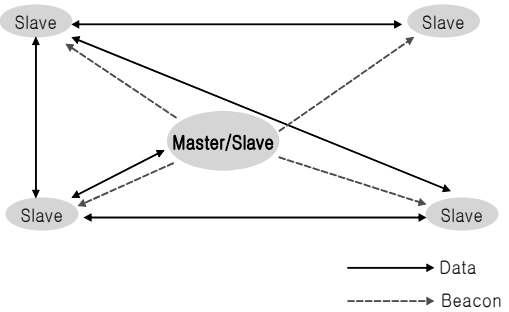

그림 1. Koinonia 피코넷 구조

을 제안한다. 또한 IEEE 802.15.3 WPAN 기반으로 기기 간의 인증 및 키 전송, 그리고 인증서 관리 방법도 연구되고 있다[10]. Koinonia WPAN 표준에서는 보안에 관련한 사항은 정의되지 않고 있다. 따라서 Koinonia의 피코넷 내 기기 간 안전한 데이터 통신을 위한 보안에 관한 정의가 필요하다. 따라서 본 논문에서는 Koinonia 고속 WPAN의 보안을 위해 필요한 대칭 기반 암호 키의 안전한 전송을 위한 키 생성 및 분배 방법을 제안한다.

본 논문의 구성은 다음과 같다. 2장에서는 Koinonia의 표준에 대해 설명하고 3장에서는 기존 보안 방법에 관한 연구와 IEEE 802.15.3 WPAN의 보안 개요에 대해 설명한다. 4장에서는 암호키 전송을 위해 대칭키 및 비 대칭키 분배 방법에 대하여 살펴보고, 5장에서는 생성된 키의 관리에 대하여 살펴본다. 6장에서는 제안한 키 분배 방식에 관한 성능분석을 다루고 마지막으로 7장에서 결론을 맺는다.

Ⅱ. KOINONIA 고속 WPAN

데이터 전송을 위한 채널 타임의 할당 등의 정보를 슬레이브에게 제공하고 CTA의 스케줄링, 슬레이브의 결합, 분리와 전력소비 모드의 관리 등 피코넷의 전반적인 사항을 관리한다. 비콘과 관리 프레임은 마스터와 슬레이브 사이에서만 전송되지만 실제 데이터 프레임은 마스터를 통하지 않고 peer-to-peer 전송이 가능하다.

Koinonia 피코넷에서는 마스터가 비콘 프레임을 슬레이브들에 전송하는데 비콘 프레임은 네트워크에 대한 기준 정보를 가지고 있으며, Koinonia 네트워크내의 모든 슬레이브들은 비콘 프레임내의 기준 정보들을 사용하여 네트워크 동기를 맞춘다. Koinonia의 슈퍼 프레임은 그림 2처럼 크게 3부분으로 구성되며, 각 구간의 길이는 가변적이다. 비콘 구간은

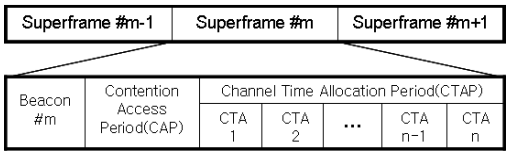

그림 2. Koinonia 슈퍼프레임 구조

마스터가 슬레이브들에게 네트워크 기준정보를 가지고 있는 비콘 프레임을 전송한다. 경쟁 구간(CAP : Contention Access Period)에서는 슬레이브와 마스터가 네트워크 합류요청/분리요청/허용, 자원할당 요청/허용, 연결 요청/허용, 인증 요청/허용 등의 명령 패킷을 임의 접근 방식으로 전송한다. 채널타임 할당구간(CTAP : Channel Time Allocation Period)은 여러 개의 시간 슬롯으로 나누어지고, 각각의 디바이스에게 시간 슬롯단위로 할당된다. 시간 슬롯을 할당 받은 디바이스는 해당 슬롯동안 동기/비동기 데이터와 명령 패킷을 전송한다.

Koinonia 표준에서 피코넷 내 기기 간 보안에 관련한 기술은 아직 정의되어 있지 않으므로, 본 논문에서는 Koinonia 기술과 유사한 IEEE 802.15.3 WPAN에 정의된 보안 방법을 살펴보고, 이를 바탕으로 Koinonia 표준에 적합한 키 생성 및 전송 방법을 제안한다.데이터 전송을 위한 채널 타임의 할당 등의 정보를 슬레이브에게 제공하고 CTA의 스케줄링, 슬레이브의 결합, 분리와 전력소비 모드의 관리 등 피코넷의 전반적인 사항을 관리한다. 비콘과 관리 프레임은 마스터와 슬레이브 사이에서만 전송되지만 실제 데이터 프레임은 마스터를 통하지 않고 peer-to-peer 전송이 가능하다.

Koinonia 피코넷에서는 마스터가 비콘 프레임을 슬레이브들에 전송하는데 비콘 프레임은 네트워크에 대한 기준 정보를 가지고 있으며, Koinonia 네트워크내의 모든 슬레이브들은 비콘 프레임내의 기준 정보들을 사용하여 네트워크 동기를 맞춘다. Koinonia의 슈퍼 프레임은 그림 2처럼 크게 3부분으로 구성되며, 각 구간의 길이는 가변적이다. 비콘 구간은 마스터가 슬레이브들에게 네트워크 기준정보를 가지고 있는 비콘 프레임을 전송한다. 경쟁 구간(CAP : Contention Access Period)에서는 슬레이브와 마스터가 네트워크 합류요청/분리요청/허용, 자원할당 요청/허용, 연결 요청/허용, 인증 요청/허용 등의 명령 패킷을 임의 접근 방식으로 전송한다. 채널타임 할당구간(CTAP : Channel Time Allocation Period)은 여러 개의 시간 슬롯으로 나누어지고, 각각의 디바이스에게 시간 슬롯단위로 할당된다. 시간 슬롯을 할당 받은 디바이스는 해당 슬롯동안 동기/비동기 데이터와 명령 패킷을 전송한다.

Koinonia 표준에서 피코넷 내 기기 간 보안에 관련한 기술은 아직 정의되어 있지 않으므로, 본 논문에서는 Koinonia 기술과 유사한 IEEE 802.15.3 WPAN에 정의된 보안 방법을 살펴보고, 이를 바탕으로 Koinonia 표준에 적합한 키 생성 및 전송 방법을 제안한다.

Ⅲ. 기존 보안 연구 및 IEEE 802.15.3 WPAN 표준 보안 개요 분석

3.1 기존 보안 연구

Wireless PAN을 기반으로 제안하는 여러 가지 보안 방법들은 대부분 비대칭 키 분배 방법을 이용하고 있다[8-11]. 논문[8-10]은 WPAN의 개인인증기관(Personal Certificate Authority: PCA)이라는 개념을 도입하여 기기 간 인증과 인증서 관리에 관한 방법을 제안하였으며, 논문[8, 9]는 비대칭 키 쌍이 각 디바이스에 이미 존재하는 것으로 가정하고 디바이스 간 인증 및 인증서 관리에 관한 방법을 제안하였다.

논문[10]은 IEEE 802.15.3 WPAN 기반으로 비대칭 키 전송을 위한 인증방법 및 인증서 관리 등 전반적인 부분에 대해 기술하고 있다. WPAN은 PCA와 일반 디바이스로 피코넷이 구성되며, 보안동작을 위해 구성요소의 초기화 과정이 이루어진다. PCA는 키 발생기로써 키 쌍을 생성해야하며, 디스플레이가 가능한 디바이스이어야 한다. 일반 디바이스는 Diffie-Hellman 프로토콜을 이용하여 PCA와 인증 절차를 거친다. 이와 같은 인증 절차를 거쳐 PCA와 일반 디바이스 간 비밀키를 생성하게 되고 생성된 비밀키를 이용하여 키 쌍과 인증서를 분배한다. 여기서 인증을 위해 PCA는 임의의 키 값 K와 Diffie-Hellman 프로토콜을 이용할 때 사용되는 파라미터를 이용하여 확인 값(check value)을 계산하고 K와 확인 값을 디스플레이 한다. 디바이스는 디스플레이 된 키 값인 K와 확인 값을 직접 입력하여 인증을 하게 된다. 논문 [11]에서는 여러 키 교환방법들을 비교하였으며 일부는 논문[8, 9]와 마찬가지로 비대칭 키 쌍의 교환에 관련한 방법은 제시되어 있지 않고 인증서를 바탕으로 한 인증 방법들이 제안되어 있다. 인증하는 과정에서 키를 생성하는 방법들도 제안되어 있는데 키를 생성하기 위해서는 키 생성에 필요한 파라미터를 전송하는 과정이 필요하다. 그러

나 이러한 과정을 통하여 파라미터가 외부에 노출되며, 키 생성에 필요한 파라미터의 노출은 키 노출의 위험성을 가지고 있다. 이와 같이 키 교환을 위해 Diffie-Hellman 프로토콜을 대부분 많이 사용하지만, Diffie-Hellman 프로토콜의 취약점인 man-in-the-middle attack 문제를 극복하기 위해 인증 방법의 강화 등의 방법[11]이 제안되어 있다. 본 논문에서는 비대칭 비밀키/대칭 비밀키 생성 및 분배하는 방법을 제안한다.

3.2 IEEE 802.15.3 WPAN 표준 보안 개요

IEEE 802.15.3 WPAN 표준은 고속 데이터 전송을 보장하기 위하여 몇 가지 보안 방법을 표준화하고 있다. 표준에서는 보안 모드를 0과 1로 분리하여 모드 0일 경우 보안 동작을 수행하지 않게 되며, 모드 1에서는 기기 간 보안관계를 설정하여 안전한 데이터 전송을 보장한다. 이와 같이 모드 1에서는 사용되는 방법은 CCM 방법으로 비콘, 커맨드(command), 데이터(data) 프레임을 보호하기 위해 CCM 방법을 사용한다. CCM 방법에서 CBC-MAC 방법은 데이터 인증에 사용되며, 데이터의 암호화는 CTR 방법을 이용한다. CCM 방법에서 사용되는 암호화 알고리즘은 128-bit AES (Advanced Encryption Standard)알고리즘을 사용한다. 또한 PNC (Piconet Coordinator) 간의 핸드오버, 키 분배, 그리고 멤버쉽 업데이트 같은 몇 가지 보안 관련 프로토콜이 IEEE 802.15.3 표준에 정의 되어 있다. 그러나 기기 간 보안 관계 설정 및 키 교환과 관련한 구체적 프로토콜 부분은 표준에 제시되어 있지 않다. 논문[8]에서는 이를 보완하고자 Diffie- Hellman 프로토콜을 이용하여 인증 절차를 거친 후, 비대칭 키 전송에 필요한 비밀키를 생성하는 방법을 제안하고 있다.

Ⅳ. 제안하는 Koinonia 고속 WPAN 보안

WPAN에서 데이터를 안전하게 전송하기 위해서는 데이터를 암호화하여 전송하여야 하며, 암호화에 사용되는 암호키 또한 안전하게 전송되어야 한다. 암호키를 안전하게 전송하기 위하여 본 논문에서는 대칭 비밀키(symmetric secret key) 생성 및 전송 방법과 비대칭 비밀키(asymmetric secret key)를 이용한 방법을 제안한다. 대칭 비밀키의 생성 및 전송을 위해서는 세션키(session key)를 이용하여야 하는데, 여기서 세션키란 피코넷에서 모든 일반 디바이스들을 컨트롤 하는 마스터와 통신을 원하는 일반 슬레이브 간에 생성되는 일시적인 비밀 키이다. 이와 같이 세션키는 피코넷에서 마스터-슬레이브 간이 아닌 슬레이브들 간 peer-to-peer의 보안 통신을 가능하게 하기 위해서 필요한 대칭 비밀키를 생성 및 전송할 수 있게 하는 역할을 한다. 대칭 비밀키를 이용하는 이유는 암호키를 전송하여 슬레이브들 간 안전한 통신을 하기 위함이므로, 마스터라 하여도 슬레이브들 각각의 암호키를 알 수 없게 해야 하기 때문이다. 따라서 생성된 세션키를 이용하여 바로 암호키를 전송하지 못하며, 암호키 전송을 위해서는 대칭 비밀키를 이용하여야 한다. 대칭 비밀키를 이용하여 암호키를 전송할 경우 마스터는 세션키를 이용하여 슬레이브간의 대칭 비밀키를 생성할 수 있게 한다. 비대칭 비밀키를 이용할 경우에는 각 슬레이브가 키 쌍(공개키/개별키)를 생성하여 공개키를 공개하면 마스터 즉, PCA는 기기와 보안 관계 설정을 위하여 인증서를 발급한다. 이와 같이 대칭/비대칭 비밀키를 이용하여 암호키(encryption key)를 분배, 데이터를 암호화한다.

제안하는 프로토콜의 안전성을 분석하기 위하여 필요한 보안 요구 사항들은 다음과 같다.

1. 개체 인증: 키 교환 방법에 참여한 상대방의 신원을 확인한다.
2. 키 확인: 키 교환 방법에 참여한 사용자가 상대방과 동일한 세션키를 실제로 공유하고 있는지 확인한다.
3. 묵시적 키 인증: 세션키의 소유 여부를 모르더라도 키 교환에 참여한 사용자 이외의 제 3자가 세션키 계산이 불가능함을 확인한다.
4. 키 신규성: 세션마다 새로운 키 설정을 확인한다.
5. 제 3자의 위장 공격(active impersonation attack) 불가: 공격자가 임의의 다른 사용자로 위장하여 키 교환 프로토콜에 참여하여도 정당한 사용자와의 키 교환이 어려움을 확인한다.
6. 기밀성 및 무결성: 통신 내용을 제 3자가 알지 못하고 통신 내용이 제 3자에 의해 변경되지 않음을 확인한다.
7. 알려진 키에 대한 보안: 과거 세션키가 노출되어도 현재 세션키의 안전성에는 아무런 영향을 미치지 않음을 확인한다.

4.1 제안 대칭 비밀키 교환방법

4.1.1 세션키 생성 및 인증방법

대칭 비밀키 전송을 위해 사용되는 세션키 생성을 위하여 먼저 슬레이브 기기와 마스터 기기는 미리 정해진 패스워드(W_{M_i,S_j})를 공유하고 있다고 가정한다. 공유된 패스워드는 생성된 세션키의 인증 과정에 사용된다. 본 논문에서 제안하는 세션키 생성 방법은 Diffie-Hellman 프로토콜에 기반 한다. 따라서 man-in-the- middle attack 문제가 발생할 수 있다. 이와 같은 문제를 보완하기 위한 인증 방법을 제시하고 이를 통하여 세션키를 생성하는 방법을 제안한다. 세션키 생성방법은 그림 3과 ㅌ같다.

우선 마스터 *i*-슬레이브 *j*의 세션키 생성을 위해 마스터 *i*가 랜덤변수 x를 생성하고 $g^x \bmod p$를 계산하여 슬레이브 *j*에게 전송하고, 이를 수신한 슬레이브 *j*는 랜덤 변수 y를 생성, $g^y \bmod p$를 계산하여 마스터 *i*에게 전송한다. 이와 같은 과정을 통하여 마스터 *i*와 슬레이브 *j*는 두개의 같은 파라미터를 공유하게 되고 이 공유된 파라미터를 이용하여 세션키 K_{M_i,S_j}를 생성한다. 이와 같이 생성된 세션키를 사용하기 전에 마스터 *i*-슬레이브 *j* 간에 공유하는 패스워드 W_{M_i,S_j}를 이용하여 인증 과정을 거치게 된다. 즉, 마스터 *i*는 공유하는 세션키로 마스터 *i*-슬레이브 *j* 사이에 공유하는 모든 파라미터(W_{M_i,S_j} 포함)를 암호화하여 전송하고 수신한 슬레이브 *j*는 복호화 후 소유하고 있는 자신의 파라미터와 비교한다. 이와 같은 인증 과정을 거친 후, 최종 세션 키 $K_{M_i,S_j} = g^{xy} \bmod p$를 공유하게 된다.

4.1.2 대칭 비밀키 교환 방법

데이터의 암호화를 위한 암호키의 안전한 전송을 위해 대칭 비밀키 이용 방법을 제안한다. 즉, 위에서 생성한 세션키를 이용하여 통신을 원하는 슬레이브 간 대칭 비밀키를 생성하고 분배하는 방법에 대하여 살펴본다. 피코넷에서 마스터는 KDC(Key Distribution Center)로 키를 생성하고 분배하는 역할을 수행한다. 피코넷에서의 통신은 두 슬레이브 간 peer-to-peer통신 방식이 가능하므로 슬레이브 간 비밀 통신을 하기 위해서는 이들만의 대칭 비밀키를 공유해야 한다. 이는 비밀 통신에 사용되는 데이터 암호키를 안전하게 전송하기 위해 필요한 키이다. 이와 같은 대칭 비밀키 생성과정은 그림 4와

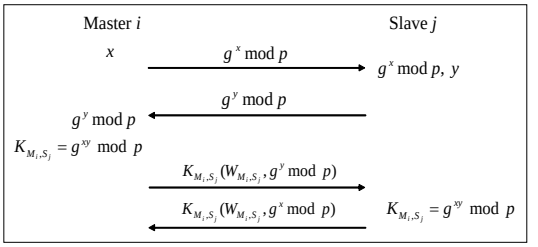

그림 3. 제안하는 세션키(K_{M_i,S_j}) 생성 및 인증과정

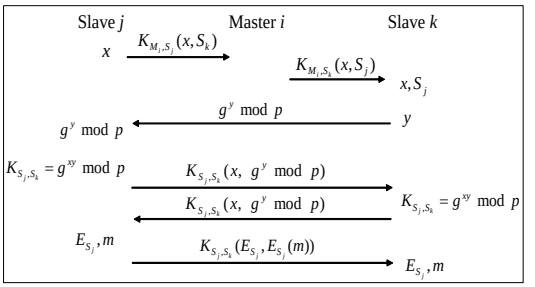

그림 4. 제안하는 대칭 비밀키(K_{S_j,S_k}) 생성, 분배 및 인증과정

같다. 그림 4에서 보는 바와 같이 슬레이브 *j*가 슬레이브 *k*와 통신을 원할 경우, 슬레이브 *j*는 마스터 *i*에게 슬레이브 *k*와 통신을 원한다는 메시지를 마스터 *i*-슬레이브 *j* 간의 세션키(K_{M_i,S_j})를 이용하여 암호화해서 보낸다. 이와 같은 요청 메시지를 전송할 때, 슬레이브 *j*는 랜덤변수 x를 생성하여 함께 전송한다. 이 랜덤 변수는 슬레이브 *j*와 슬레이브 *k*의 대칭 비밀키 생성을 위해 사용된다. 메시지를 받은 마스터 *i*는 생성된 랜덤 변수 x를 마스터 *i*-슬레이브 *k* 간의 세션키(K_{M_i,S_k})를 이용하여 암호화 시킨 후, 슬레이브 *k*에게 전송한다. 슬레이브 *k*는 세션키(K_{M_i,S_k})로 이를 복호화하여 슬레이브 *j*에 의해 생성된 랜덤 변수 x를 소유하게 된다. 이 과정이 끝나면 슬레이브 간 세션키는 소멸되고 비밀 관계 설정을 위한 두 슬레이브 간 대칭 비밀키 생성과정에 들어간다. 생성 방법은 Diffie- Hellman 프로토콜을 이용한다. 슬레이브 *k*는 랜덤변수 y를 생성하여 $g^y \bmod p$를 계산, 슬레이브 *j*에게 전송한다. 그리고 각 슬레이브는 랜덤 변수 x를 이용하여 슬레이브 *j*-*k*간 대칭 비밀키 $K_{S_j,S_k} = g^{xy} \bmod p$를 계산할 수 있다. 슬레이브 *j*와 *k*는 랜덤 변수 x와 $g^y \bmod p$를 서로 비교하는 인증 과정을 거친 후, 같을 경우 $K_{S_j,S_k} = g^{xy} \bmod p$를 두 슬레이브 간 대

칭 비밀키로 사용한다. 이와 같이 슬레이브 *j*와 슬레이브 *k* 간 생성된 대칭 비밀키를 이용하여 슬레이브 *j*는 실제 데이터 암호에 사용되는 암호키 E_{S_j}를 슬레이브 *k*에게 전송한다. 이때 슬레이브 *j*는 슬레이브 *k*에게 전송할 메시지 m을 암호키 E_{S_j}로 암호화하여 암호키 E_{S_j}와 함께 전송한다. 슬레이브 *k*는 대칭 비밀키 K_{S_j,S_k}로 암호키 E_{S_j}와 메시지 m을 수신하게 된다.

4.2 제안 비대칭 비밀키 교환 방법

본 절에서는 앞 절과 마찬가지로 암호키의 안전한 전송을 위하여 비대칭 비밀키 교환방법을 제안한다. 피코넷에서 마스터 *i*는 PCA (Personal Certificate Authority) 역할을 수행한다. 마스터 *i*는 먼저 보안 관계를 설정하기 위해 키 쌍(공개키/개별키)을 생성한 슬레이브들은 마스터 *i*에게 자신의 공개키를 전송하고, 마스터 *i*로부터 인증서를 발급 받는다. 인증서는 마스터 *i*가 각 슬레이브들을 인증하기 위한 것으로 각 슬레이브의 공개키(P_{S_j},P_{S_k})와 식별자(ID_{S_j},ID_{S_k})를 마스터 *i*의 비밀키(R_{M_i})로 서명하여 인증서를 생성하여 분배한다.

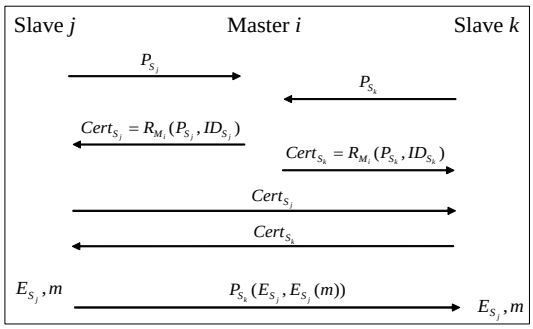

그림 5. 제안하는 비대칭 비밀키를 이용한 암호키(E_{S_j})전송 과정

비대칭 비밀키를 이용한 암호키 분배과정은 그림 5와 같다. 그림 5에서 보는 바와 같이 슬레이브 *j*와 슬레이브 *k*는 각각 마스터 *i*에게 자신의 공개키를 전송하고 인증서를 발급받는다. 슬레이브 *k*와 통신하고자하는 슬레이브 *j*는 슬레이브 *k*에게 인증서를 보내고, 슬레이브 *k*도 인증서를 슬레이브 *j*에게 보낸다. 슬레이브 *k*의 인증서를 수신한 슬레이브 *j*는 마스터 *i*의 공개키를 이용하여 슬레이브 *k*의 공개키와 식별자를 확인한다. 마찬가지로 슬레이브 *k* 또한 슬레이브 *i*의 식별자와 공개키를 획득하여 상호 간 인증을 확인할 수 있다. 슬레이브 *j*는 수신한 슬레이브 *k*의 공개키를 이용하여 자신의 암호키 E_{S_j}를 슬레이브 *k*에게 전송한다. 이때 슬레이브 *j*는 슬레이브 *k*에게 전송할 메시지 *m*을 암호키 E_{S_j}로 암호화하여 함께 전송한다. 슬레이브 *k*는 자신의 개별키로 복호화하여 암호키 E_{S_j} 와 암호화 된 메시지 *m*을 수신한다.

Ⅴ. 세션키, 대칭/비대칭 비밀키 관리

위와 같이 암호키 전송을 위해 마스터와 슬레이브가 생성하여 소유하고 있어야 할 키의 관리가 필요하다. 세션키는 마스터-슬레이브 간 생성된 키로써 마스터가 모든 슬레이브들의 세션키를 소유하고 있으므로 마스터가 관리하여야 한다. 대칭 비밀키를 이용하여 암호키를 전송 할 경우 각 슬레이브들은 슬레이브 간에 필요한 대칭 비밀키를 관리하여 야 하며, 비대칭 비밀키를 이용할 경우는 마스터가 모든 슬레이브에게 비대칭 비밀키를 생성하여 분배하므로 모든 슬레이브의 인증서를 관리하여야 한다.

따라서 본 절에서는 앞서 살펴 본 세션키 관리 방법과 세션키를 이용하여 생성된 대칭 비밀키, 비대칭 비밀키 관리 방법에 대하여 기술한다.

5.1 세션키 관리

마스터는 모든 슬레이브와 세션키를 생성하므로 세션키 목록(SKL: Session Key List)을 작성하여 관리해야 한다. 세션키 목록은 슬레이브 아이디와 해당 슬레이브의 세션 키, 한 쌍으로 형성되며, 각 슬레이브의 세션키 업데이트와 폐기에 관하여 관리한다. 슬레이브가 마스터와 보안 관계를 설정하고자 한다면 마스터는 슬레이브와 세션키를 생성하고 해당 슬레이브 아이디와 생성된 세션키를 세션키 목록에 추가한다. 반대로 슬레이브가 마스터와 보안 관계 설정 해제를 원하면 마스터는 해당 슬레이브에 관한 부분을 세션키 목록에서 삭제하게 된다. 마스터-슬레이브 간에 생성된 세션키는 대칭/비대칭 비밀키를 교환한 후 자동적으로 세션키 목록에서 삭제된다. 또한 현재 마스터가 다른 슬레이브로 마스터의 역할을 이동할 경우 기존의 피코넷 망은 유지되므로 세션키 목록을 새로운 마스터에게 양도한다.

5.2 대칭 비밀 키 관리

세션 키를 이용하여 생성된 대칭 비밀 키는 앞 절에서 보는 바와 같이 마스터-슬레이브 간 생성되는 것이 아니라 슬레이브-슬레이브 간에 생성되는 키이다. 따라서 피코넷의 마스터가 아닌 각 슬레이브에서 대칭 비밀키를 관리하며, 슬레이브가 관리해야 할 대칭 비밀키는 최대 피코넷의 슬레이브 수만큼 생성될 수 있다. 따라서 각 슬레이브는 효율적으로 대칭 비밀키를 관리해야 한다.

각 슬레이브는 대칭 비밀키 목록(SSKL: Symmetric Secret Key List)을 작성하여 관리해야 한다. 대칭 비밀키 목록은 슬레이브 아이디와 해당 슬레이브의 대칭 비밀 키, 한 쌍으로 형성되며, 각 슬레이브의 대칭 비밀키 업데이트와 폐기에 관하여 관리한다. 한번 생성된 슬레이브 간 대칭 비밀키는 슬레이브가 피코넷의 멤버에서 제외될 때까지 유지된다. 피코넷에 어떤 슬레이브가 새롭게 추가된 경우, 그 슬레이브와 통신을 원하는 슬레이브는 세션키를 통하여 슬레이브 간 대칭 비밀키를 생성하여 슬레이브 각각이 자신의 SSKL에 대칭 비밀키 정보를 추가한다. 반대로 통신하는 슬레이브가 현재 속해있는 피코넷에서 해제될 경우 각 슬레이브는 해제된 슬레이브의 아이디와 대칭 비밀키를 자신의 대칭 비밀키 목록에서 삭제한다.

5.3 비대칭 비밀 키 관리

비대칭 비밀키는 앞서 살펴봤던 대칭 비밀키와는 다르게 마스터가 개별인증기관(PCA)이 된다. 인증기관은 피코넷의 슬레이브들에게 인증서를 발급한다. 인증기관에서 비대칭 비밀키 관리는 많은 방법이 있지만 가장 많이 다루어지는 관리방법은 인증서 관리 목록(CRL: Certificate Revocation List) 방법이다. 이와 같이 생성된 각 슬레이브들의 인증서는 PCA가 관리하고 있으며, 슬레이브가 새로운 인증서를 원할 때, 또는 현재 키 쌍에 대한 인증서가 만료되었을 경우 마스터는 인증서를 업데이트해야 한다. 또한 피코넷에서 마스터가 다른 슬레이브에게 마스터의 기능을 핸드오버 할 경우 기존의 마스터는 자신이 관리하던 인증서 관리 목록을 핸드오버 된 슬레이브에게 전송한다. 인증서 관리 목록은 각 슬레이브들에게도 분배되어 슬레이브 간 통신에서 발생하는 인증서 관리 목록의 업데이트된 정보를 슬레이브 간에 서로 공유하며, 이를 마스터에게 전송하면 마스터는 이를 통하여 또한 최신 인증서 관리 목록을 유지하게 된다.

Ⅵ. 성능 분석

제안한 프로토콜은 앞서 요구한 7가지 조건에 충족하는지 분석하여야 한다.

1. 개체 인증(entity authentication): 세션키 생성과정에서 마스터-슬레이브가 키 생성을 위한 파라미터 교환 후 마스터-슬레이브 만이 공유하고 있는 고유한 패스워드를 통하여 인증을 거치게 되므로 상대방의 신원은 확인된다. 또한 다중 피코넷에서 자식 마스터는 자식 피코넷에서 마스터 역할과 부모 피코넷에서 슬레이브 역할을 한다. 따라서 자식 마스터는 이미 부모 피코넷에서 인증이 확인 되었으며, 다중 피코넷에서 키 교환 시 비대칭 키를 이용하므로 다중 피코넷 보안을 위한 슬레이브 인증은 피코넷에서만 이루어지면 된다.
2. 키 확인(key confirmation): 마스터는 슬레이브로부터 인증받기 위해 생성된 세션키를 최종 사용하기 전에 인증 절차를 거친다. 이 과정에서 같은 패스워드를 공유하고 있으면 생성된 세션키를 사용한다.
3. 묵시적 키 인증(implicit key authentication): 키 생성을 위한 파라미터가 제 3자에게 노출 되었다할지라도 세션키를 생성하는 기기 간 패스워드를 알지 못하면 인증이 실패하게 되므로 세션키를 생성할 수 없다.
4. 키 신규성(key freshness): 세션키는 대칭/비대칭 비밀키 분배 후 자동 소멸된다. 합류 해제되었던 슬레이브가 피코넷에 다시 합류하여 보안 관계를 형성하고자 한다면, 마스터-슬레이브 간 새로운 세션키를 생성한다.
5. 능동적 위장 공격 불가: man-in-the-middle attack로 키 교환에 필요한 파라미터를 가로챘다 할지라도 마스터-슬레이브 간 고유한 패스워드는 알 수 없기 때문에 위장 공격은 어렵게 된다.
6. 기밀성(confidentiality) 및 무결성(integrity): 세션키를 이용하여 대칭 비밀키를 분배하고 대칭 비밀키를 이용하여 암호키를 분배한다. 전송된 암호키는 데이터 암호화에 사용되며 사용되는 CCM 방법에서 기밀성과 무결성이 보장된다.
7. 알려진 키 보안(known key security): 세션키는 대칭 비밀키를 전송하면 자동으로 소멸되므로 제 3자가 과거의 소멸된 세션키를 알고 있다

해도 현재 세션키에 아무런 영향을 미치지 않는다.

6.1 세션키 보안 분석

위에서 살펴본 바와 같이 본 논문에서는 Koinonia WPAN의 무선 환경에서 암호키를 안전하게 전송하기 위하여 대칭/비대칭 비밀키를 생성하여 분배, 인증하는 방법을 제안하였다. Koinonia WPAN 피코넷에서 각 슬레이브들은 마스터를 통하여 보안 관계를 설정하며, 슬레이브 간 비밀키를 교환한다. 따라서 비밀키 교환을 위해 마스터-슬레이브 간 일시적인 키가 필요하게 되므로 마스터는 비밀통신을 요청하는 슬레이브들과의 세션키를 각각 생성하게 된다. 이와 같이 대칭 비밀키 전송을 위해 마스터-슬레이브 간 일시적인 세션키를 생성하였다. 따라서 가장 보안에 강하게 생성되어야 할 키는 처음에 생성되는 세션키이다. 세션키가 보안에 강하게 생성되면 각 슬레이브들에게 대칭 비밀키가 안전하게 분배되며, 또한 안전하게 분배된 대칭 비밀키로 실제 데이터 암호화에 필요한 암호키를 안전하게 분배할 수 있기 때문이다.

위 4.1.1절에서 제안한 세션키 생성과정은 Diffie-Hellman 프로토콜에 기반하며, man-in-the-middle attack에 취약하다. 이를 보완하기 위해 키 생성 후 상호 인증 과정이 필요하며, 본 논문에서는 마스터-슬레이브 간에 공유하는 고유한 패스워드를 이용한다. 패스워드는 이미 두 기기가 각각 소유하고 있다고 가정하며, 인증 과정에서 마스터-슬레이브 간의 보안 관계 설정에 사용된다. 키 생성을 위한 파라미터 교환 과정에서 파라미터들이 제 3자에 의해 가로채여 키를 생성한다 할지라도 마스터-슬레이브 간 고유한 패스워드는 가로챌 수 없기 때문에 파라미터와 패스워드를 비교하는 인증 과정에서 발생할 수 있는 man-in-the-middle attack 문제를 보완할 수 있다. 따라서 이와 같이 생성된 마스터-슬레이브 간 세션키는 보안에 강인하며, 대칭 비밀키 전송에 이용된다. 대칭 비밀키 생성 시 마스터-슬레이브 간의 비밀 통신을 원할 경우, 따로 대칭 비밀 키를 이용하지 않고 제안 방법에 의해 생성된 세션키를 이용하여 암호키를 안전하게 전송할 수 있다.

6.2 대칭/비대칭 비밀키 보안 분석

생성된 세션키는 마스터-슬레이브 간에 생성된 슬레이브의 개별키라 볼 수 있다. 마스터는 모든 슬레이브의 세션키를 알고 있으며, 세션키를 이용하여 대칭 비밀키를 생성하여 분배한다.

위 4.2절에서 제안한 대칭 비밀키 생성과정은 세션키 생성과정과 마찬가지로 Diffie- Hellman 프로토콜에 기반하고, 통신을 요청한 슬레이브가 랜덤하게 생성한 변수를 통신 대상이 되는 슬레이브에게 세션키를 이용하여 안전하게 전송한다. 이렇게 생성, 전송된 랜덤 변수는 슬레이브 간 인증 과정에 사용되며, 인증 과정을 peer-to-peer 슬레이브-슬레이브 간에 한 번 더 수행하게 되므로 보안 설정을 재확인하여 보안관계가 설정된다. 또한 슬레이브-슬레이브 간의 인증 과정을 통하여 man-in-the-middle attack을 보완할 수 있다. 제안한 비대칭 비밀키 분배 방법은 공개키로 암호화 된 암호키 전송은 각자의 공개키에 대응하는 비밀키로 암호키를 전송받을 수 있으므로 보안에 강인하게 동작한다.

Ⅶ. 결 론

WPAN에서 무선으로 데이터 전송 시 데이터 보안을 위해 암호화를 하여야하며 이를 위한 암호키를 안전하게 전송하는 것이 중요하다. 특히 Koinonia WPAN에서는 보안에 관련한 어떠한 정의도 되어있지 않은 상태이기 때문에 본 논문에서는 Koinonia WPAN의 암호키 전송을 위해 슬레이브-슬레이브 간 대칭 비밀키 생성 및 분배, 마스터-슬레이브 간 비대칭 비밀키 생성 및 분배 방법을 제안하였다. 또한 이와 같은 대칭/비대칭 비밀키 생성 및 분배를 위해 마스터-슬레이브 간 세션키의 생성 및 인증과정을 제안하였다. Koinonia의 피코넷에서 통신을 하기 위해 슬레이브는 항상 마스터를 통하기 때문에 처음 피코넷 슬레이브가 합류할 경우 association과정 후 비밀 통신을 위해서는 보안 관계를 설정해야 한다. 이와 같은 초기 보안 관계 설정은 피코넷의 마스터와 슬레이브 간 세션키를 생성하여 이루어진다. 따라서 본 논문에서는 가장 처음에 생성되는 중요한 세션키를 얼마나 보안에 강하게 생성하고 분배할 것인가에 초점을 두고 그 방법을 제안하였다. 패스워드 인증 과정을 거쳐 생성된 세션키는 보안에 강하며, 생성된 세션키를 기반으로 슬레이브들의 대칭/비대칭 비밀키 또한 안전하게 생성하여 분배할 수 있다. 이와 같이 생성된 비밀키를 이용하여 실제 데이터를 암호화 시키는 데 필요한 암호키를 안전하게 전송할 수 있으며, 암호키를 이용하여 안전한 통신이 가능하게 된다.

참 고 문 헌

〔1〕 IEEE, “Standards for Part 15.1: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Wireless Personal Area Networks (WPANs),” Jun. 2002.

〔2〕 IEEE, “Standard for Part 15.3: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for High Rate Wireless Personal Area Networks (WPANs),” Sep. 2003.

〔3〕 IEEE, “Standard for Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (LR-WPANs),” Oct. 2003.

〔4〕 J. Karaoguz, “High-Rate Wireless Personal Area Networks,” IEEE Communications Magazine, vol. 39, no. 12, pp. 96-102, Dec. 2001.

〔5〕 KETI, Koinonia 표준규격서, 물리 계층과 데이터링크 계층 규격 버전 1.0, 5. 2003.

〔6〕 조진웅, 주민철, 서경학, 류승문, “WPAN용 Binary CDMA 기술,” 한국통신학회지, vol. 19, no. 5, pp. 136-146, 2002.

〔7〕 정쌍봉, 임순빈, 이태진, 전선도, 이현석, 권대길, 조진웅, “Koinonia 고속 WPAN의 다중 피코넷 레벨 및 용량 분석,” 한국통신학회논문지, vol. 31, no. 3B, pp. 216-223, 2006.

〔8〕 C. Gehrmann, K. Nyberg and C. J. Mitchell, “The personal CA-PKI for a Personal Area Network,” in Proc. of IST Mobile and Wireless Communications Summit, pp. 31-35, Jun. 2002.

〔9〕 R. H. Deng and F. Bao, “An Improved Personal CA for Personal Area Networks,” in Proc. of IEEE Globecom 2003, vol. 3, pp. 1486-1490, Dec. 2003.

〔10〕 Z. Tao, Z. Guo and R. Yao, “Piconet Security in IEEE 802.15.3 WPAN,” in Proc. of Wireless Communications and Networking Conference, vol. 4, pp. 2125-2130, Mar. 2005.

〔11〕 G. Horn, K. M. Martin and C. J. Mitchell, “Authentication Protocols for Mobile Network Environment Value-Added Services,” IEEE Transactions on Vehicular Technology, vol. 51, no. 2 Mar. 2002.

임 순 빈 (Soon-Bin Yim) 정회원

1998년 2월 한서대학교 전자공학과(학사)

2004년 2월 성균관대학교 전기전자컴퓨터공학과(석사)

2005년 3월~현재 성균관대학교 정보통신공학부 재학중(박사)

<관심분야> 무선 LAN/PAN, ad-hoc 네트워크, 광 네트워크

정 쌍 봉 (Ssang-Bong Jung) 준회원

2005년 2월 대구대학교 정보통신공학부 졸업(학사)

2005년 3월~현재 성균관대학교 정보통신공학부 재학중(석사)

<관심분야> WPAN, WLAN

이 태 진 (Tae-Jin Lee) 종신회원

1989년 2월 연세대학교 전자공학과 졸업 (학사)

1991년 2월 연세대학교 전자공학과 졸업 (석사)

1995년 12월 University of Michigan, Ann Arbor, EECS (M.S.E.)

1999년 5월 University of Texas, Austin, ECE (Ph.D.)

1999년 5월~2001년 2월 삼성전자 중앙연구소 책임연구원

2001년 3월~현재 성균관대학교 정보통신공학부 조교수

<관심분야> 통신 네트워크 성능 분석 및 설계, 무선 LAN/PAN, ad-hoc/센서 네트워크, 광 네트워크, 무선 통신 시스템

전 선 도 (Sun-Do June) 정회원

1993년 2월 광운대학교 전자통신공학과 졸업(학사)
1995년 2월 광운대학교 전자통신공학과 졸업(석사)
2000년 2월 광운대학교 전자통신공학과 졸업(박사)
2000년 3월~2002년 4월 삼성종합기술연구원 전문연구원
2002년 5월~2006년 2월 전자부품연구원 책임연구원
2006년 3월~현재 경기공업대학 전자통신과 조교수
<관심분야> 무선 네트워크, 통신 시스템, HCI

이 현 석 (Hyeon-Seok Lee) 준회원

2000년 2월 한양대학교 전파공학과 졸업(학사)
2002년 2월 한양대학교 전자통신공학과 졸업(석사)
2002년 1월~2003년 2월 삼성전기 주임연구원
2003년 2월~현재 전자부품 연구원 전임연구원
<관심분야> 무선 PAN 네트워크, Embedded System Software

권 대 길 (Tai-Gil Kwon) 정회원

2001년 2월 동의대학교 산업 공학과 졸업(학사)
2003년 8월 고려대학교 산업 시스템정보공학과 졸업(석사)
2003년 9월~현재 전자부품 연구원 전임연구원
<관심분야> 무선 네트워크, 멀티미디어

조 진 웅 (Jin-Woong Cho) 정회원

1986년 2월 광운대학교 전자통신공학과 졸업(학사)
1988년 2월 광운대학교 전자통신공학과 졸업(석사)
2001년 2월 광운대학교 전자통신공학과 졸업(박사)
1993년 6월~현재 전자부품연구원 통신네트워크 센터장
1999년 일본 산업기술종합연구소 STA fellow
1989년 9월~1993년 6월 동양정밀 중앙연구소
<관심분야> 무선 PAN 네트워크, 산업용/가정용 무선 네트워크