USN 환경에서 비인증서 공개키를 사용하는 보안키 관리 프레임워크

(Secure Key Management Framework in USN Environment using Certificateless Public Keys)

허 준 † 홍 충 선 ††
(Joon Heo) (Choong Seon Hong)

요 약 본 논문에서는 USN과 기존 네트워크간 연동을 위한 보안키 관리 프레임워크를 제안한다. USN과 기존 네트워크간 연동은 다양하고 많은 디바이스로 구성되기 때문에, 인증기관(Certificate Authority, CA)의 부재에도 불구하고 공개키 기반의 암호기술이 사용되어야 한다. 제안된 메커니즘은 IP 네트워크의 PKI 시스템의 지원을 받지 못하는 상황에서의 공개키/개인키 관리와 디바이스간 인증에 초점을 두고 있으며, 인증기관 부재의 문제를 해결하기 위해 신원기반 암호화 개념을 도입하였다. 또한, 실제 네트워크에서의 적용가능성 검증에 초점을 두어 USN과 IP 네트워크 그리고 PLC네트워크를 연동하여 테스트베드를 구축하고, 제안 메커니즘을 적용하여 테스트하였다. 이러한 테스트를 통해 보안키 생성, 업데이트 과정에서 대칭키 기반 알고리즘과 유사한 성능을 확인하였고, 네트워크연동 및 장비인증이 가능함을 확인하였다.

키워드 : 비인증서 공개키, USN, 보안키 관리, 장비인증

Abstract In this paper, we propose the secure key management framework to connect USN with different network. Although connected USN with different network has no CA (Certificate Authority), it is important to use public key based cryptography system because this network consists of numerous devices. The proposed mechanisms focus on device authentication and public/private key management without existing PKI system of IP network. To solve no CA and certificate problems, the IBC (Identity Based Cryptography) concept is adopted in our proposed mechanism. To verify the possibility of realization, we make an effort to implement the proposed mechanisms to real system. In the test bed, both USN and PLC network are connected to IP network; and proposed mechanisms are implemented to PLC and sensor devices. Through this test using the proposed mechanism, we met the similar performance with symmetric algorithms on key generation and update process. Also, we confirmed possibility of connection between different network and device authentication.

Key words : Certificateless Public Keys, USN, Key Management, Device Authentication

· This work was supported by the IT R&D program of MKE/KEIT. [2009-S-014-01, On the development of Sensing based Emotive Service Mobile Handheld Devices].

† 정 회 원 : NTT Information Sharing Platform Laboratories
heo.joon@lab.ntt.co.jp
†† 종신회원 : 경희대학교 전자정보대학 교수
cshong@khu.ac.kr
(Corresponding author임)

논문접수 : 2009년 3월 2일
심사완료 : 2009년 10월 7일

정보과학회논문지 : 정보통신 제36권 제6호(2009.12)

1. 서 론

유비쿼터스 센서 네트워크(USN)가 IP 네트워크 또는 전력선통신(PLC) 네트워크 등 기존의 인프라와 연동되면 다양한 서비스가 가능해져 그 활용가치가 높아진다고 할 수 있다[1]. 그러나, 이렇게 연결된 네트워크는 물리적 통신매체의 다양성과 활용분야의 상이성이 존재하기 때문에 기존의 IP 네트워크에서 사용되었던 보안 기술들을 그대로 적용하기 어려운 부분이 있다. 특히, 전체적인 보안키 관리 프레임워크 관점에서 볼 때, IP 네트워크는 단계별로 그 기능과 역할이 잘 정의되고 운용되어지는 인증기관(CA, Certificate Authority)

과 인증서 기반의 PKI 인프라를 통해 사용자 중심의 공개키 기반 시스템을 운용하고 있지만, USN 환경의 연동된 네트워크를 구성하는 디바이스들은 이러한 인증서 기반의 공개키 방식을 사용할 수 없다[2,3]. 센서 네트워크와 전력선 통신 기술[4]이 대칭키 중심의 암호화 방식을 사용하는 것은 디바이스의 물리적 한계뿐만 아니라, 이러한 인증기관을 포함하는 인프라의 부재 때문이라고 할 수 있다. 본 논문에서는 USN 기반의 연동된 네트워크를 구성하는 많은 수의 디바이스 보안키 관리를 위해 신원기반 암호기술의 개념을 적용하여 비인증서 기반의 보안키 관리 프레임워크를 제안한다. 또한, 디바이스간 인증을 위한 인증 티켓의 사용 및 보안키의 유효범위 설정과 키 갱신 절차를 정의하였다. 본 논문은 다음과 같이 구성되었다. 2장에서는 관련연구로써 신원기반 암호기술의 개념과 보안프레임워크의 목적에 관해 설명한다. 3장에서는 논문에서 제안하는 보안키 생성과 갱신 그리고 디바이스 인증절차에 관하여 설명한다. 4장에서는 제안하는 메커니즘의 성능과 적용가능성을 검증하기 위하여 IP 네트워크, USN, PLC로 연동되는 테스트베드를 구축하여 실험한 결과들을 설명하고, 기존 기술들과 비교한다. 마지막으로 결론부분에서는 본 논문의 의의와 향후 연구과제에 관하여 기술한다.

2. 관련연구 및 보안프레임워크 정의

본 논문에서는 다른 네트워크와 연동된 USN을 위한 공개키 관리 프레임워크에서 인증기관 부재의 문제를 해결하기 위해 신원기반 암호기술의 개념을 적용하였다. 본 장에서는 신원기반 암호기술의 개념과 설계목표에 관해 설명한다.

2.1 신원기반 암호기술

ID 기반 공개키 암호시스템은 A. Shamir에 의해 처음 소개되었으며[5], 그 특징은 다음과 같다[6].

- 사용자의 잘 알려진 신원정보로부터 해당 사용자의 공개키를 유도한다.
- 사용자는 자신의 개인키를 직접 만들 수 없고, 개인키 생성기관(PKG, Public Key Generator)을 통해서 발급 받아야만 한다.
- 사용자들은 다른 사용자의 공개키를 직접 그 사용자의 신원정보로부터 생성할 수 있다.
- 기존 공개키 시스템과 달리 공개키와 사용자를 묶어주는 인증서가 필요 없다.
- 시스템 복잡도를 낮추며, 공개키 프레임워크 확립 및 관리와 관련된 비용절감 효과가 있다.

2001년 D. Boneh와 M. Franklin은 타원곡선의 겹선형쌍(bilinear pairing)을 이용하여 실용적인 ID 기반 암호 알고리즘을 제안[7]하였으며, 이 후 다양한 암호 프로토콜 분야에 ID 기반 암호시스템이 적용되어 많은 연구결과가 발표되었다[8-10].

2.2 설계 목표

본 논문에서 제안하는 보안키 관리 프레임워크를 다른 네트워크와 연동된 USN에 적용하기 위한 보안 관점에서의 설계 목표는 다음과 같다.

- 보안키를 관리하기 위한 디바이스의 저장 공간, 연산 오버헤드, 통신 오버헤드 등의 요소 관점에서 효율적이어야 한다.
- 키 갱신을 통한 안전한 네트워크 유지가 가능해야 한다.
- 사용자의 보안 정보 입력 없이 디바이스 인증이 자체적으로 수행될 수 있어야 한다.

또한, 본 논문에서는 모든 디바이스가 동기화 되지는 않는다고 가정한다. 모든 디바이스의 동기화는 시스템 부하를 크게 증가시킬 뿐 만 아니라, 해당 네트워크의 어플리케이션에 따라 데이터 통신 빈도가 각각 다양할 수 있기 때문이다. 따라서, 제안되는 방식은 디바이스들의 비동기 상태에서도 효율적이고 안전하게 관리될 수 있어야 한다.

3. 제안 사항

3.1 신원기반 보안키 생성

본 논문에서는 인증서 부재의 한계를 가지고 있는 USN 기반 연동 네트워크 환경을 위해 신원 기반 암호 알고리즘의 개념을 도입하였다. 또한, 사용자 중심의 보안키 관리가 아닌 디바이스 중심의 보안키 관리 및 상호인증에 초점을 두었다. 따라서, 각 디바이스를 위한 개인키 뿐만 아니라 공개키도 PKG에 의해 생성된 후 분배하도록 제안하였으며, 각 디바이스는 새롭게 통신하기를 원하는 디바아스의 공개키를 PKG에서 받아 사용할 수 있도록 하였다. 이는 사용자 중심의 인증인 경우 이메일 주소 및 주민등록번호와 같은 정보를 공개키로 활용할 수 있으나, 디바이스의 경우 이러한 정보를 활용할 수 없기 때문이다.

따라서, 생성되는 개인키, 공개키는 PKG에 의해 생성된 후 분배되어야 한다. 그리고, 보안키의 유효범위를 설정하여, 해당 범위 기간 안에서만 보안키가 유효할 수 있도록 제안한다. 또한, 디바이스간 인증이 필요할 때 관리서버에 문의하지 않고, 등록과정에서 발급 받은 인증티켓을 활용하는 방식을 제안하였다. 표 1은 본 논문에서 사용되는 용어와 그 의미를 설명하고 있다. 공개키/개인키의 생성에 있어서는 신원기반 암호 시스템에서 일반적으로 사용되는 타원곡선의 겹선형 쌍(bilinear pairing) 기법을 활용한다.

표 1 용어 정의

q	Large prime number
P	Generator of cyclic group
s, t	Network master secret
H_1, H_2	Hash functions
K_A	Initial Public key of A
K_A^{-1}	Initial Private key of A
$K_{A,i}$	Public key of A in period i
$K_{A,i}^{-1}$	Private key of A in period i
$TK_{A,B}$	Symmetric Temporary key between A and B
K_i^T	Ticket key in period i
f_{TK}	Temporary key Generation Function
I_A	Index information for Temporary key of A
exp	Key expired period
$V_{exp\,i}^A$	Remaining Duration of A in period i
Π_A	Registered unique device information of A
T_{PKG}^A	Authenticated Ticket of A is issued by PKG
$\{W\}_K$	Encrypted W using the key K
$[W]_K$	Signature W using the key K

3.1.1 안전한 채널을 통한 공개키/개인키 생성

PKG와 디바이스간 안전한 채널이 존재하는 경우의 공개키/개인키 생성 및 분배 메커니즘의 개념은 그림 1과 같으며, 생성 조건 및 과정은 그림 2와 같다.

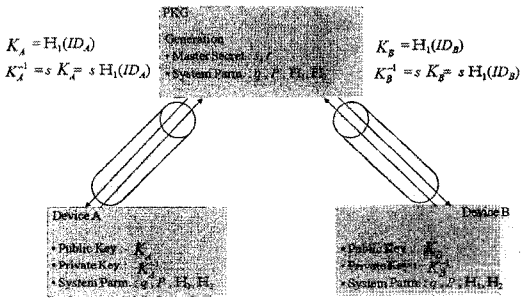

그림 1 안전한 채널을 통한 보안키 생성 및 분배

Condition : There are existing secure channel between and device. PKG decides s, t as master secret and generates q, P, H_1, H_2 as system parameters.
Step 1
1. Device A requests Public key, Private key and system parameters to PKG
2. PKG → A : K_{PKG}
Step 2
1. A generates random value R_A and $auth\_value = f(ID_A \| R_A)$
2. A encrypts $auth\_value$ and R_A using the K_{PKG}
3. A → PKG : ID_A, $\{auth\_value, R_A\}\,K_{PKG}$
Step 3
1. PKG decrypts $\{auth\_value, R_A\}\,K_{PKG}$
2. PKG verifies $auth\_value$
3. PKG generates $K_A = H_1(ID_A)$, $K_A^{-1} = s\,K_A = sH_1(ID_A)$
Step 4
1. PKG → A : K_A, K_A^{-1}, q, P, H_1, H_2
2. A get K_A, K_A^{-1}, q, P, H_1, H_2

그림 2 안전한 채널에서 보안키 생성 조건 및 과정

안전한 채널이 존재한다는 의미는 무선랜에서 사용하는 SSID와 같이 디바이스가 네트워크에 조인하기 위해 기본적인 보안 정보를 만족해야 한다는 의미이다. 먼저 PKG는 마스터 보안 정보인 s, t를 생성한다. 이 마스터 정보는 오직 PKG에 의해서만 생성되고 유출되지 않도록 안전하게 관리되어야 한다. PKG는 생성한 마스터 정보를 활용해 시스템 파라미터 값 q, P, H_1, H_2를 생성하고 디바이스의 요청에 따라 디바이스의 공개키 K_A와 개인키 K_A^{-1}을 생성한 후 안전한 채널을 사용해 디바이스에게 전달한다. 이 때, 시스템 파라미터 값인 q, P, H_1, H_2도 함께 전달된다. 디바이스는 MAC주소와 같이 유일한 값을 ID_A로 PKG에 전송하며, PKG는 이 값을 키 생성에 활용한다.

3.1.2 임시키를 사용한 공개키/개인키 생성

PKG와 디바이스 사이에 안전한 채널이 존재하지 않는 경우의 공개키/개인키 생성 및 분배 메커니즘의 개념은 그림 3과 같으며, 생성 조건 및 과정은 그림 4와 같다.

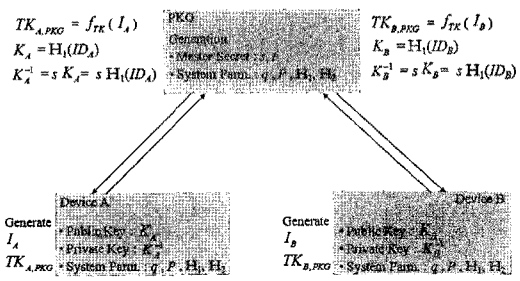

그림 3 임시키를 사용한 보안키 생성 및 분배

Condition : There are no existing secure channel between PKG and device. However, PKG and device share common data table and generation function to generate temporary key. PKG decides s, t as master secret and generates q, P, H_1, H_2 as system parameters.
Step 1
1. Device A requests Public key, Private key and system parameters to PKG
2. PKG → A : K_{PKG}
Step 2
1. A generates I_A, random value R_A and $auth\_value = f(ID_A \| R_A)$, $TK_{A,PKG} = f_{TK}(I_A)$
2. A encrypts R_A, $auth\_value$ and I_A using K_{PKG}
3. A → PKG : ID_A, $\{auth\_value, R_A, I_A\}\,K_{PKG}$
Step 3
1. PKG decrypts $\{auth\_value, R_A, I_A\}\,K_{PKG}$
2. PKG verifies $auth\_value$
3. PKG generates $TK_{A,PKG} = f_{TK}(I_A)$ $K_A = H_1(ID_A)$, $K_A^{-1} = s\,K_A = sH_1(ID_A)$
Step 4
1. PKG→A:$\{K_A, K_A^{-1}, q, P, H_1, H_2\}\,TK_{A,PKG}$
2. A decrypts $\{K_A, K_A^{-1}, q, P, H_1, H_2\}$ using the $TK_{A,PKG}$
3. A gets K_A, K_A^{-1}, q, P, H_1, H_2

그림 4 임시키를 사용한 보안키 생성 조건 및 과정

안전한 채널이 존재하지 않는 경우 PKG와 디바이스는 임시키를 생성할 인덱스 정보를 교환하고, 공유하고 있는 임시키 생성 함수를 사용해 디바이스에서 사용될 공개키와 개인키, 그리고 시스템 파라미터 값을 전달한다. 임시키는 이러한 기능을 위해 일회만 사용된다. 이를 위해 PKG와 인가된 장비는 인덱스와 그에 해당하는 값으로 구성된 인덱스 테이블과, 임시키 생성 함수를 공유하고 있어야 한다.

3.2 디바이스 인증

디바이스 인증은 사용자 인증보다 많은 제약사항이 따른다. 예를 들면, 사용자 인터페이스가 부족하거나 존재하지 않는 상황, 보안 정보의 관리가 어려운 상황, 사용자에 의한 입력에 의존하는 것이 아니라 디바이스 자체의 특징 및 관리 서버에 저장되어 있는 인증 정보에 따르는 상황 등을 이유로 들 수 있다. 무엇보다 디바이스 자체의 정보 유지 및 절차에 따라 인증이 이루어져야 한다는 것이다. 본 논문에서는 디바이스 인증을 등록과정과 디바이스 사이의 인증과정으로 나누어 제안한다. 그림 5는 PKG에 의한 유효범위 개념 및 관리 방법에 관하여 설명하고 있다. PKG는 보안키의 유효범위를 설정하기 위해 exp_i 값을 사용한다. i-1, i, i+1 는 PKG가 현재 사용하고 있는 유효범위를 나타낸다. 각 범위의 기간(d)은 PKG의 정책에 따른다. 디바이스 A가 등록 절차를 수행하는 시기가 i 범위에서 일정시간(t_c) 지난 상태라면 디바이스 A의 남아 있는 유효범위 기간($V^{A}_{\exp i}$)은 d-t_c라고 할 수 있다.

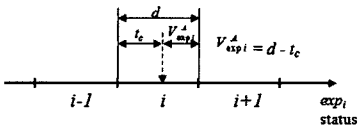

그림 5 PKG에 의한 유효범위 개념

3.2.1 등록 과정

앞 절에서 설명한 것처럼 각 디바이스는 신원기반 기본공개키(K_A), 기본개인키(K_A^{-1}), 시스템 파라미터를 안전한 채널을 사용하거나 임시키를 사용하여 PKG로부터 분배 받는다. 그러나, 이러한 키를 계속 사용하는 것은 시스템에 심각한 위협요소로 작용할 수 있다.

따라서, 본 논문에서는 PKG의 유효범위 정책에 따라 exp_i 를 수신하여 유효범위 i 상태 동안 유효한 공개키/개인키 쌍을 생성하여 사용한다. 이 키 쌍은 유효공개키($K_{A,v}$)와 유효개인키($K_{A,v}^{-1}$)이며 각 디바이스에서 PKG로부터 발급 받은 K_A, K_A^{-1}와 시스템 파라미터를 사용하여 생성한다. 디바이스간 인증에 사용되는 인증 티켓 역시 i 상태 동안 유효하도록 exp_i 를 사용하여 생성하도록 한다. 그림 6은 이러한 개념에 따른 디바이스의 등록 절차를 설명하고 있다.

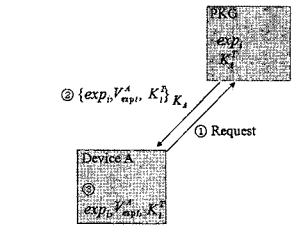

그림 6 디바이스 등록과정

3.2.2 인증 과정

본 논문에서는 디바이스간의 인증을 위해 등록과정에서 발급받은 인증 티켓을 사용한다. 인증 티켓은 i 상태 동안 사용 가능하며, 각 디바이스는 상대 디바이스를 인증하기 위해 관리서버에 인증여부를 확인하는 것이 아니라, 인증 티켓을 사용해 자체적으로 수행한다. 인증 티켓의 형식은 그림 7과 같으며, 각 필드의 설명은 아래와 같다.

- ID of Issuer PKG : 인증 티켓을 발행한 PKG의 신원정보
- ID of Sending Device : 인증을 요청하는 디바이스의 신원정보
- exp_i : 등록과정에서 발급받은 현재의 유효 상태
- K_i^T : 인증 티켓을 교환하는 과정에서 암호화하기 위해 PKG로부터 발급받은 티켓키

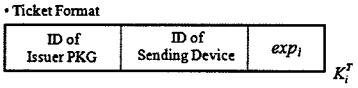

그림 7 인증 티켓의 형식

인증 티켓을 발급받은 각 디바이스는 유효기간 i 동안 인증티켓과 유효공개키/유효개인키를 사용해 상호 인증을 수행할 수 있다. 그림 8은 이러한 인증 절차를 설명하고 있다.

3.3 보안키 갱신

본 논문은 PKG로부터 발급받은 신원기반 공개키(K_A)와 개인키(K_A^{-1})를 계속적으로 사용하는 것이 아니라, 등록과정을 통해서 PKG로 발급받은 exp_i 를 사용해 유효 공개키($K_{A,v}$)와 유효 개인키($K_{A,v}^{-1}$)를 생성하여 사용하도록 정의하였다. 이러한, 방법은 시스템의 보안성을 유지하고 네트워크 변화에 적응하기 위해 꼭 필요한 방법이라고 할 수 있다. 이렇듯 키의 유효범위를 지정하여 사용하는 경우 보안키의 갱신 과정이 필요하게 된다. 본 논문에서는 보안키 갱신 과정을 디바이스

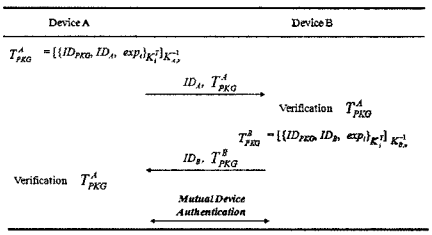

그림 8 디바이스간 인증 과정

요청에 의한 갱신 모델과 PKG에 의한 갱신 모델로 구분하여 정의하였다. 먼저, 디바이스 요청에 의한 갱신 모델의 경우 i 상태에서 $K_{A,v}$, $K_{A,v}^{-1}$, K_i^T 를 사용하던 각각의 디바이스가 $V_{\exp i}^{A} \rightarrow 0$ 이 될 때, PKG에게 새로운 유효범위 상태 (i+1)를 요구하는 것이다. 반면, PKG에 의한 갱신 모델의 경우 그룹키를 사용하는 어플리케이션처럼 특정 도메인의 디바이스들은 모두 동일한 그룹키를 사용하므로, 모든 디바이스로부터 보안키 갱신 요청을 받는 것이 아니라, 게이트웨이와 같은 연결 포인트 디바이스에게만 PKG가 갱신 정보를 전달하고, 도메인 내부의 디바이스들은 연결 포인트 디바이스에게 갱신정보를 받는 모델이다.

3.3.1 디바이스 요청에 의한 갱신 모델

각 디바이스가 서로 다른 유효 공개키와 유효 개인키를 사용하고 인증의 주체가 되는 네트워크에 사용되는 보안키 갱신 모델이다(그림 9). 디바이스 A가 i 상태에서 등록과정을 통해 PKG로부터 exp_i 와 $V_{\exp i}^{A}$를 분배받아 유효키를 생성하여 사용하던 중 $V_{\exp i}^{A} \rightarrow 0$ 의 상태가 되면 PKG에게 새로운 상태 (i+1)의 exp_i+1 과 $V_{\exp i+1}^{A}$ 값을 요청하게 된다. 그림 9는 이러한 개념을 설명하고 있다. 상태가 i 에서 i+1 가 되는 시점에서 요청을 하지 않는 이유는 앞서 설명한 것과 같이 시스템내의 모든 단말은 동기화되지 않기 때문에 각 디바이스의 시간 상태에 따라 요청시기가 달라지기 때문이다.

3.3.2 PKG에 의한 갱신 모델

ZigBee 네트워크[11]와 전력선 통신과 같이 특정 그룹에서 동일한 보안키를 사용하는 네트워크의 경우 모든 디바이스가 PKG에게 보안키 갱신을 요청할 필요가 없으며, 만약 이렇게 될 경우 시스템에 큰 부하가 작용하게 된다.

따라서, 동일한 그룹에서 공통으로 그룹키를 사용하는 경우 상태가 i 에서 i+1 으로 바뀌는 경우 PKG에 의한 보안키 갱신이 더욱 효율적인 방법이라고 할 수 있다. 그림 10은 이러한 개념을 설명하고 있다. PKG는 상태가 i 에서 i+1 로 바뀔 때 그룹 X의 연결 포인트 디바이스인 X_0 에게 exp_i 를 exp_i+1 로 변경하여 사용할 것을 전달한다. X_0 는 PKG로부터 이와 같은 정보를 수신한 뒤 동일한 그룹 X 에 속해 있는 모든 디바이스에게 exp_i+1

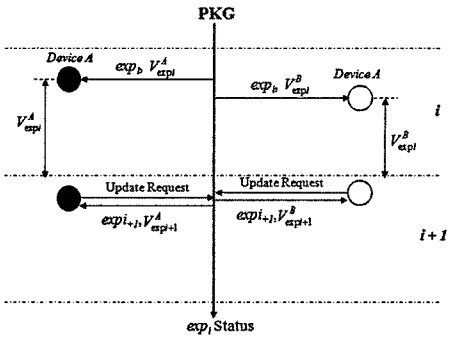

그림 9 디바이스 요청에 의한 보안 키 갱신

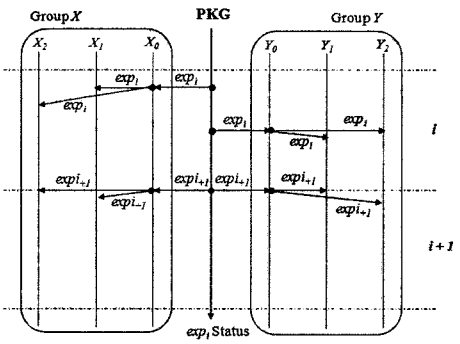

그림 10 PKG 요청에 의한 보안 키 갱신

을 전달하여, 갱신된 보안키 정보가 사용되도록 한다.

4. 성능평가

비인증서 기반 신원기반 암호시스템을 활용한 현재까지의 대부분의 연구들은 암호학적 분석이나 이론적 해석에 중점을 두고 있다. 본 논문은 제안된 보안키의 생성 및 분배 그리고 디바이스간 인증과 같은 메커니즘이 실제 네트워크를 구성하는 센서 디바이스 또는 전력선 통신 장비에 적용 가능한지를 검증하기 위하여 이러한 디바이스들을 IP 네트워크와 연동시키고 각 디바이스에 구현하여 성능을 검증하였다. 그림 11은 테스트베드의 구조와 여기에 사용된 장비들을 설명하고 있다.

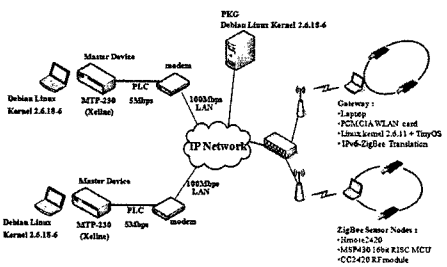

그림 11 연동 네트워크 테스트베드

4.1 IP-USN 네트워크

IP-USN 네트워크의 경우 게이트웨이를 통하여 연동된다. 테스트에 사용된 센서 디바이스의 하드웨어적 특징은 표 2와 같다. 센서네트워크 기술 중 ZigBee 네트워크는 센서간 대칭키 생성을 위하여 SKA(Symmetric Key Agreement)를 정의하고 있다[11]. 또한, 센서 네트워크에 공개키 기술을 적용하기 위해 EC-MQV와 같은 타원곡선 기반 기술[12,13]을 활용하는 연구들이 진행되고 있다.

표 2 센서 디바이스의 하드웨어적 특성

802.15.4 Transceiver	Chipcon CC2420
Frequency	2.400 GHz ~ 2.4835 GHz
Modulation and Transmission	DSSS with Q-PSK
Maximum Transmission Rate	250 Kbps
Program Flash Memory	128 Kbytes
EEPROM	4 Kbytes

표 3과 그림 12는 제안된 메커니즘과 SKA, EC-MQV에서의 공개키와 개인키의 생성과 분배 그리고 키 갱신 과정에 있어서 센서 디바이스에서의 연산 시간을 나타내고 있다.

테스트 결과에서 제안된 메커니즘은 키 생성 및 분배에 있어서 SKA보다 약간 많은 연산 시간을 필요한 것을 확인할 수 있다. SKA는 센서간 대칭키만을 생성하기 때문에 연산 오버헤드는 작을 수 있으나, 많은 수의 센서를 관리해야 할 경우 대칭키가 가지는 한계를 극복하지 못하는 단점이 있다. 또한, 테스트 결과의 키 갱신 과정에서 제안 메커니즘이 효율적인 것을 확인할 수 있다.

표 3 IP-USN에서의 키 생성 및 갱신 소요시간(ms)

	Proposed mechanism	EC-MQV	SKA
Key generation	597	828	316
Key update	142	685	280
Total overhead	739	1513	596

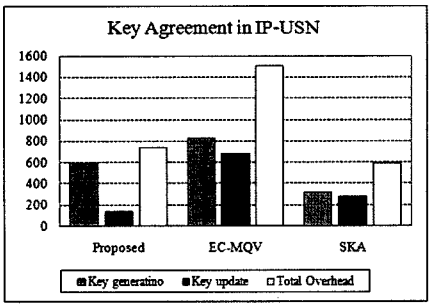

그림 12 IP-USN에서 보안키 생성 및 갱신 시간(ms)

4.2 IP-PLC 네트워크

IP-PLC 네트워크의 경우 보안 기술 개발에 있어서 제안된 메커니즘과 비교할 수 있는 기존 연구가 매우 적어 제안 메커니즘이 PLC 장비에서 어느 정도의 성능 나타내는지 보안키의 길이를 다양화하여 테스트하였다. 표 4와 그림 13은 키의 길이를 512bits, 1024bits 그리고 2048bits로 생성하는 경우의 필요한 연산시간을 나타내고 있다. 각 결과는 연산을 위한 시간과 통신 절차를 포함한 시스템적인 소요시간으로 구분하였다.

표 5는 제안된 인증 메커니즘을 통한 PLC 디바이스간 인증 소요시간을 나타내고 있다. 이 결과 또한 연산을 위한 소요시간과 통신 절차를 포함한 시스템적 소요시간으로 구분하여 나타내었다.

표 4 IP-PLC에서 개인키/대칭키 생성 소요시간(ms)

key length(bits)	Computation	System	Total Overhead
512	21.4	194.4	215.8
1024	59.6	359.2	418.8
2048	193.2	1227.6	1420.8

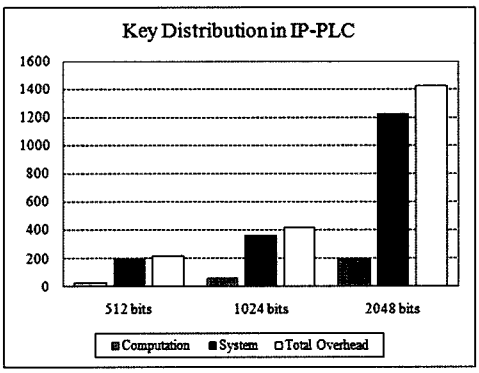

그림 13 IP-PLC 개인키/대칭키 생성 소요시간(ms)

표 5 PLC 디바이스간 인증 소요시간(ms)

key length(bits)	Computation	System	Total Overhead
512	14.2	46.1	60.3

4.3 보안성 분석

표 6은 본 논문에서 제안하고 있는 메커니즘을 다양한 공격의 관점에서 비교하였다. 제안된 메커니즘은 기밀성 및 인증과 관련된 공격에는 효과적으로 대응할 수 있으나, DoS 공격 형태에는 취약할 수 있음을 알 수 있다. 이러한 분석 결과를 통해 다양한 통신 기술들이 연동되는 환경에서 발생할 수 있는 여러 가지 공격 형태에 대한 대응 방법에 관한 연구가 추가적으로 이루어져야 함을 알 수 있다.

표 6 제안된 메커니즘의 보안성 분석

Possible Attacks	Security Analysis	Description
Spoofing	High	▪ Using the authentication data(auth_value) ▪ Updating the ticket key
Replay Attacks	Medium	▪ Using the term of validity ▪ Maintain the term of validity for a long time
Man-in-the-middle attack	Medium	▪ Exchanging of challenge and response value ▪ Fabricated PKG
Eavesdropping	High	▪ Data encryption ▪ Updating the keys
Denial-of-Service Attacks	Low	▪ Weakness of structural characteristic ▪ Be vulnerable to various DoS attacks
Authentication Ticket Interception	High	▪ Updating the ticket key ▪ Exchanging of signature value
Modification of Information	High	▪ Using the random value ▪ Exchanging of signature value
Service Stealing Attack	Low	▪ Limiting access of adversary ▪ Various attacks of wired and wireless network

5. 결론 및 향후 과제

본 논문에서는 USN기반 연동네트워크와 같이 기존의 인증관련 인프라를 사용할 수 없는 상황에서 비인증서 기반의 보안키 관리 프레임워크를 제안하였다. 인증기관의 부재를 해결하기 위해 신원기반의 암호개념을 도입하여, 보안키의 생성과 분배 유효기간의 사용 및 디바이스간 인증 방법을 제안하였다. 현재까지 연구된 신원기반 암호 알고리즘은 대부분 수학적 증명으로 논문의 타당성을 입증하였다. 본 논문은 증명에 의한 기존 연구와의 비교보다는 제안한 메커니즘을 실제 구현하여 시스템 적용 가능성을 평가하는데 중점을 두고 테스트하였다. 본 논문의 최종 목표는 성능 평가 후 제안된 보안키 관리 프레임워크를 USN기반 연동네트워크 디바이스에 적용하는 것이다. 따라서, 제안된 메커니즘을 구현하고, 다양한 분석을 통해 성능을 검증하여 실제 시스템에 적용될 수 있는지 판단하는 노력이 더욱 필요하며, 이러한 관점에서의 향후 연구가 진행되어야 할 것이다.

참 고 문 헌

[1] G. Mulligan, "The 6LoWPAN architecture," *Proceedings of the 4th workshop on Embedded networked sensor*, pp.78-82, 2007.

[2] L. Eschenauer and V. Gligor, "A Key-Management Scheme for Distributed Sensor Networks," *Proc. Ninth ACM Conf. Computer and Comm. Security*, 2002.

[3] H. Chan, A. Perrig, and D.Song, "Random Key Predistribution Schemes for Sensor Networks," *Proc. IEEE Symp. Security and Privacy*, May 2003.

[4] Korea Standard, "High Speed Power Line Communication MAC and PHY," KS X4600-1, 2006.

[5] A. Shamir, "Identity-based Cryptosystems and Signature Scheme," *Proceedings of CRYPTO '84, LNCS 196*, pp.47-53, Springer-Verlag, 1984.

[6] K. J. Kim, J. Kim, W. D. Yeo, "ID based Cryptography System," *2005 Tech-Issue Emerging S&T Report,* KISTI, Dec.2005. (in korean)

[7] D. Bonech and M. Franklin, "Identity-based Encryption from Weil Pairing," *Proceedings of CRYPTO 2001, LNCS 2139*, pp.213-229, Springer-Verlag, 2001.

[8] C. Cocks, "An Identity Based Encryption Scheme Based on Quadratic Residues," *Proceedings of IMA 2001, LNCS 2260*, pp.360-363, Springer-Verlag, 2001.

[9] C. Gentry and A. Silverberg, "Hierarchical ID-Based Cryptography," *Proceedings of ASIACRYPT 2002, LNCS 2501*, pp.548-566, Springer-Verlag, 2002.

[10] M. Bellare, C. Namprempre and G. Neven., "Security Proofs for identity-based identification and signature Scheme," *Proceedings of Eurocrypt 2004, LNCS 3027*, pp.268-286, Springer-Verlag, 2004.

[11] ZigBee Security Services Specification, V1.0, Dec. 2004.

[12] A. M. Fiskiran and R. B. Lee, "Workload Characterization of Elliptic Curve Cryptography and other Network Security Algorithm for Constrained Environments," *WWC-5*, pp.127-137, 2002

[13] M. Rosing, "Implementing Elliptic Curve Cryptography," MANNING, 1999.

허 준

2002년 경희대학교 컴퓨터공학과(공학사) 2004년 경희대학교 컴퓨터공학과(공학석사). 2008년 경희대학교 컴퓨터공학과(공학박사). 현재 NTT Information Sharing Laboratories Post Doc. Fellow 관심분야는 유비쿼터스 보안, VoIP서비스 보안

홍 충 선

1983년 경희대학교 전자공학과(공학사) 1985년 경희대학교 전자공학과(공학석사) 1997년 Keio University, Department of Information and Computer Science (공학박사). 1988년~1999년 한국통신 통신망 연구소 수석 연구원 / 네트워킹연구실장. 1999년~현재 경희대학교 컴퓨터공학과 교수. 관심분야는 인터넷 서비스 및 망 관리 구조, 미래인터넷, IP mobility, Sensor Networks, Network Security