비인증서 공개키를 사용하는 보안키 생성 및 장비인증 메커니즘

허 준○, 조응준, 홍충선
경희대학교 컴퓨터공학과
{joon○, ejcho}@networking.khu.ac.kr, cshong@khu.ac.kr

A Secure Key Generation and Device Authentication Mechanism Using Certificateless Public Keys

Joon Heo○, Eing Jun Cho, Choong Seon Hong
Department of Computer Engineering, Kyung Hee University

요 약

IP 네트워크(공중망)에 새로운 네트워크 기술들의 결합, 예를 들면 IP-USN, IP-Mesh, IP-PLC 등의 이종 네트워크가 생겨나면서 이러한 네트워크를 안전하게 관리하기 위한 보안 기술의 개발이 요구되고 있다. 기존 IP 네트워크가 가지는 다양하고 견고한 보안 기술들이 이종 네트워크에 그대로 사용될 수 없으면서 생겨나는 문제 중 PKI 기반 인프라를 적용할 수 없다는 것이 가장 현실적이고 중요한 문제로 여겨지고 있다. 이러한 문제로 인해, 새로운 네트워크 기술들은 주로 내부에서 사용하는 대칭키 방식의 암호화, 복호화만을 정의하고 있다. 공개키 방식을 사용할 수 없는 가장 큰 이유는 인증기관에서 발급되는 인증서 중심의 인프라를 사용할 수 없기 때문이다. 본 논문에서는 이러한 문제를 해결하기 위해서, 이종 네트워크 환경에서 비인증서 기반의 공개키를 활용하는 보안키 관리 메커니즘을 제안한다. 제안하는 방식은 신원기반 공개키 개념을 도입하여 적용하였으며, 디바이스간 인증을 위한 인증 티켓 방식 및 보안키의 유효범위를 정하고 이를 활용하여 보다 안전한 네트워크 환경을 구축할 수 있는 방안들을 제시하였다.

1. 서 론

최근 데이터 전달 매체의 특징과 사용자 환경을 고려한 새로운 네트워크 기술들이 개발되고 상용화를 위한 노력이 진행되고 있다. 예를 들면, USN (Ubiquitous Sensor Network), 전력선통신 (Power Line Network)[1][2], 무선 메쉬 네트워크 (Wireless Mesh Network) 등의 분야에서 각각의 특징을 가지고 상용화를 위한 연구와 기술개발이 이루어지고 있으며, 국내외 표준화를 위한 노력도 함께 진행되고 있다. 이러한 신기술 네트워크들은 개발 초기 자체 환경에서의 활용에 초점을 맞추어 연구가 진행되었으나, 어느 정도 기술개발이 완성되고 있는 최근의 상황에서는 기존 상용네트워크(IP Network, Mobile Network)와의 연동과 이를 활용한 서비스 개발을 위한 노력이 진행되고 있다.

정보의 다양성과 중요성이 증가하면서, 보안 기술의 적용을 통해 안전한 통신망을 구축하는 것이 네트워크 운용에 있어 기본적인 요구사항이 되었다. 이는 이종 네트워크와 같은 기술 간의 융합에 있어서도 중요한 요소라고 할 수 있다. 그러나 이종 네트워크는 이를 구성하는 기술들의 특징으로 인해, IP네트워크에서 사용되는 보안 기술의 적용이 불가능하다. 네트워크의 확장에 따른 관리 개체의 증가에도 효율적으로 디바이스를 관리할 수 있고, 안전한 통신망 구축을 위해 필수적인 보안키 관리 메커니즘의 개발이 필요하다고 할 수 있다. 따라서 본 논문에서는 이러한 이종 네트워크의 제약조건을 고려할 때, 기존 PKI 인프라를 활용할 수 없는 환경에서 공개키를 활용한 보안키 관리 메커니즘에 관하여 기술한다. 인증기관의 부재에도 불구하고, 이종 네트워크에서 공개키 방식의 사용이 요구되어진다. IP 네트워크와의 연동을 통한 범위의 확대와 사용 디바이스의 개체가 급격하게 증가하게 되는 상황에서, 공개키 방식의 사용은 꼭 필요한 조건이라고 할 수 있다. 따라서 본 논문에서는 비인증서 기반의 공개키 활용을 위해 신원기반 암호화 기술[3][4]의 개념을 활용하였다. 신원기반 암호화 기술은 인증기관 및 인증서의 부재시에도 공개키 방식을 사용하기 위해 제안되었다.

본 논문의 구성은 다음과 같다. 2장에서는 본 논문에서 제안하는 비인증서 공개키를 사용하는 보안키 생성 메커니즘에 관해 설명한다. 세부 내용으로 설계목표, 사용되는 용어의 정의, 겹선형 파라미터의 생성, 신원기반 공개키/개인키의 생성에 관해 설명한다. 보안키의 생성은 안전한 채널이 존재하는 경우와 안전한 채널을 확보할 수 없는 경우로 나누어서 제안한다. 또한, 유효범위의 개념을 도입하여 현재 유효 상태 값을 보안키 생성에 적용한다. 3장에서는 생성된 보안키를 활용한 디바이스 인증에 관해 설명한다. 디바이스인증은 등록과정과 인증과정

*"본 연구는 지식경제부 및 정보통신연구진흥원의 대학IT연구센터 지원사업의 연구결과로 수행되었음"(IITA-2008-(C1090-0801-0016))

으로 나누어 각각의 절차를 설명한다. 또한, 인증티켓을 활용하는 장비 간 인증에 관하여 설명한다. 4장에서는 연산비용 및 효율성의 관점에서의 시뮬레이션 결과에 대하여 설명한다. 마지막으로 결론부분에서는 본 논문의 의의와 향후 연구과제에 관하여 기술한다.

2. 비인증서 공개키를 사용하는 보안키 관리

본 논문에서 제안하는 보안키 관리 메커니즘을 이종 네트워크에 적용하기 위한 보안 관점에서의 설계 목표는 다음과 같다.

- 이종 네트워크의 구조적 특징에 맞도록 설계되어야 한다.
- 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 장비 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.

2.1 용어 및 시스템 파라미터 생성

본 논문에서는 인증서 부재의 한계를 가지고 있는 이종 네트워크 환경을 위해 신원 기반 암호 알고리즘의 개념을 도입하였다. 따라서 생성되는 개인키, 공개키는 PKG (Public Key Generator)에 의해 생성된 후 분배되어야 한다.[5][6]

[표 1] 용어 정의

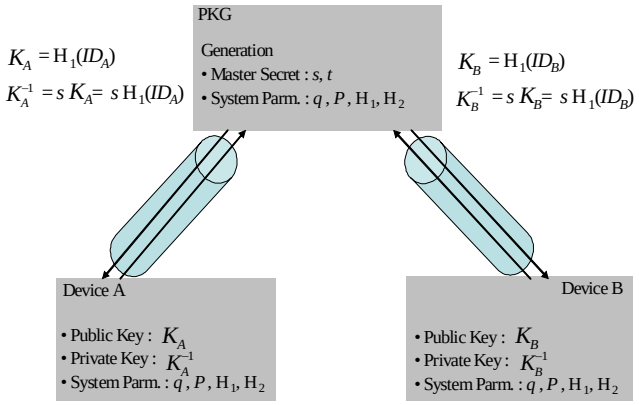
q	Large prime number
G_1, G_2	Cyclic group of order q
P	Generator of G_1
$\hat{e}$	Paring $\hat{e}$: $G_1 \times G_1 \rightarrow G_2$
s, t	Network master secret
H_1, H_2	Hash functions
K_A	Initial Public key of A
K_A^{-1}	Initial Private key of A
$K_{A,v}$	Public key of A in period i
$K_{A,v}^{-1}$	Private 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
S_{AB}	Session key of A and B
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

본 논문에서는 보안키의 유효범위를 지정하여, 해당 범위 기간 안에서만 보안키가 유효할 수 있도록 제안한다. 또한, 디바이스 간 인증이 필요할 때 관리서버에 문의하지 않고, 등록과정에서 발급 받은 인증티켓을 활용하는 방식을 제안한다. 이러한 방식들은 기본적으로 신원기반 보안키 개념을 따르고 있다. 표 1은 본 논문에서 사용되는 용어와 그 의미를 나타내고 있다.

2.2 안전한 채널을 사용한 공개키/개인키 생성

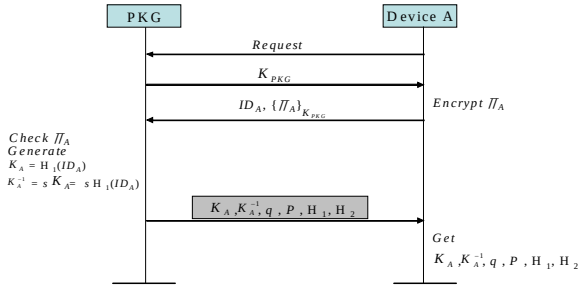
PKG에 의한 신원 기반 공개키 분배과정 중 PKG와 디바이스간 안전한 채널이 존재하는 경우의 분배 메커니즘은 그림 1과 같다. 안전한 채널이 존재한다는 의미는 무선랜에서 사용하는 SSID와 같이 디바이스가 네트워크에 조인하기 위해 기본적인 보안 정보를 만족해야 한다는 의미이다.

PKG는 마스터 보안 정보인 s, t를 생성하고, 시스템에서 사용될 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. 따라서, 디바이스는 초기 분배과정을 통해 자신이 사용할 공개키(K_A), 개인키(K_A^{-1}), 시스템 파라미터(q, P, H_1, H_2)값을 획득하게 된다.



[그림 1] 안전한 채널을 사용한 신원기반 보안키 분배

그림 2는 그림 1에서 설명하고 있는 공개키(K_A), 개인키(K_A^{-1}), 시스템 파라미터(q, P, H_1, H_2) 분배과정의 구체적인 과정을 설명하고 있다.

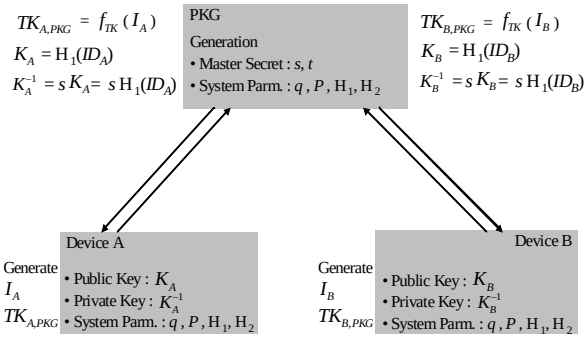


[그림 2] 안전한 채널을 사용한 보안키 분배 과정

2.3 임시키를 사용한 공개키/개인키 생성

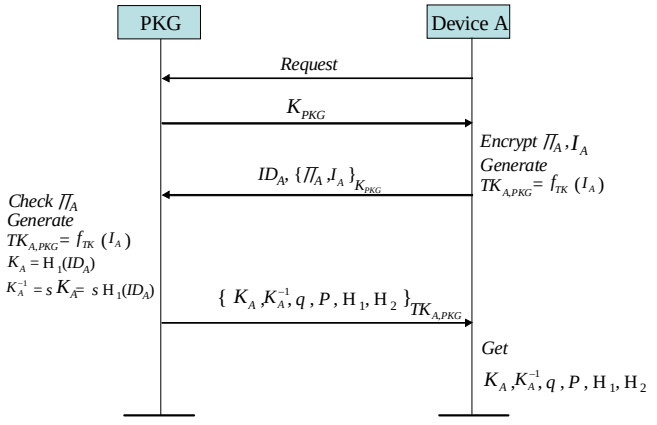
PKG에 의한 신원 기반 공개키 분배과정 중 PKG와 디바이스 사이에 안전한 채널이 존재하지 않는 경우의 분배 메커니즘은 그림 3과 같다. 안전한 채널이 존재하지 않는 경우 PKG와 디바이스는 임시키를 생성할 인덱스 정보를 교환하고, 공유하고 있는 임시키 생성 함수를 사용해 디바이스에서 사용될 공개키와 개인키, 그리고 시스템 파라미터 값을 전달한다. 임시키는 이러한 기능을 위해 한번만 사용된다.

PKG는 마스터 보안 정보인 s, t를 생성하고, 시스템에서 사용될 시스템 파라미터 값 q, P, H_1, H_2를 생성하고 디바이스의 요청에 따라 디바이스의 공개키 K_A와 개인키 K_A^{-1}을 생성한 후 임시키를 사용하여 디바이스에 전달한다. 이 때, 시스템 파라미터 값인 q, P, H_1, H_2도 함께 전달된다. 따라서, 디바이스는 초기 분배과정을 통해 자신이 사용할 공개키(K_A), 개인키(K_A^{-1}), 시스템 파라미터(q, P, H_1, H_2)값을 획득하게 된다.



[그림 3] 임시키를 사용한 신원기반 보안키 분배

그림 4는 그림 3에서 설명하고 있는 공개키(K_A), 개인키(K_A^{-1}), 시스템 파라미터(q, P, H_1, H_2) 분배과정의 구체적인 과정을 설명하고 있다.

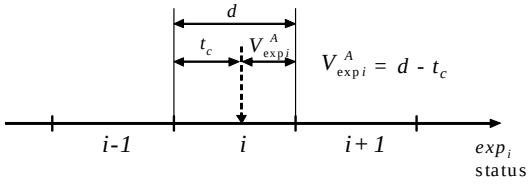


[그림 4] 임시키를 사용한 신원기반 보안키 분배 과정

3. 디바이스 인증

디바이스인증은 사용자 인증보다 많은 제약사항이 따른다. 무엇보다 디바이스 자체의 정보 유지 및 절차에 따라 인증이 이루어져야 한다는 것이다. 본 논문에서는 디바이스 인증을 등록과정과 디바이스 사이의 인증과정으로 나누어 제안한다.

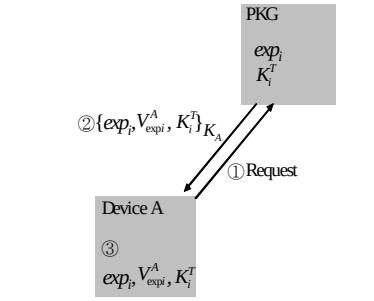
그림 5는 PKG에 의한 유효범위 개념 및 관리 방법에 관하여 설명하고 있다. PKG는 보안키의 유효범위를 설정하기 위해 exp_i 값을 사용한다. i-1, i, i+1은 PKG가 현재 사용하고 있는 유효범위를 나타낸다. 각 범위의 기간(d)은 PKG의 정책에 따른다. 디바이스 A가 등록 절차를 수행하는 시기가 i 범위에서 일정시간(t_c) 지난 상태라면 디바이스 A의 남아 있는 유효범위 기간($V_{\exp i}^A$)은 $d-t_c$라고 할 수 있다.



[그림 5] PKG에 의한 유효범위

3.1 등록 과정

앞 절에서 설명한 것과 같이 각 디바이스는 신원기반 기본 공개키(K_A), 기본 개인키(K_A^{-1}), 시스템 파라미터를 안전한 채널을 사용하거나 임시키를 사용하여 PKG로부터 부여 받는다. 그러나, 이러한 키를 계속 사용하는 것은 시스템에 심각한 위협요소로 작용할 수 있다. 따라서, 본 논문에서는 앞서 설명한 PKG의 유효범위 정책에 따라 exp_i를 수신하여 유효범위 i 상태 동안 유효한 공개키, 개인키를 생성하여 사용하도록 한다. 인증 티켓 역시 i상태 동안 유효하도록 exp_i를 사용하여 생성하도록 한다. 그림 6은 이러한 개념에 따른 디바이스의 등록 절차를 설명하고 있다.



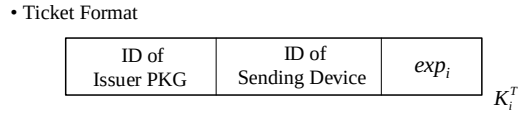
[그림 6] 등록과정

3.2 인증 과정

본 논문에서는 디바이스 사이의 인증을 위해 등록과정

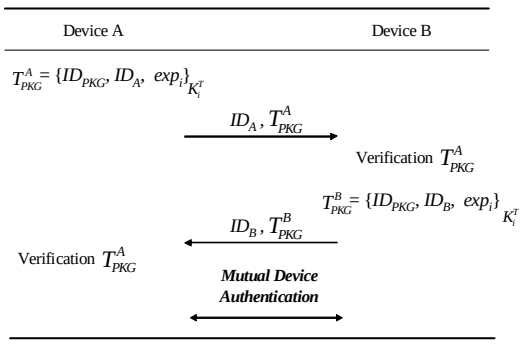
에서 발급받은 인증 티켓을 사용한다. 인증 티켓은 i 상태 동안 사용 가능하며, 각 디바이스는 상대 디바이스를 인증하기 위해 관리서버에 인증여부를 확인하는 것이 아니라, 인증 티켓을 사용해 자체적으로 수행한다. 인증 티켓의 형식은 그림7과 같으며, 각 필드의 설명은 아래와 같다.

- 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

이러한 인증 티켓을 사용한 디바이스 간 인증 과정은 그림 8과 같다.



[그림 8] 인증 과정

4. 성능평가

먼저 본 논문에서 제안된 신원 기반 키 생성 방식과 기존의 RSA, DSA의 알고리즘에서의 공개키 및 개인키 생성 소요시간을 측정하여 비교하였다. 생성되는 키의 길이는 각각 256bits, 512bits, 1024bits 이며, 측정결과는 표 2와 같다. 결과에서 알 수 있듯이 제안된 메커니즘은 RAS 알고리즘과 유사한 결과로 측정되었으나, RSA를 기존의 PKI에서 사용한다고 가정할 때, 공개키를 바인딩하기 위한 인증서 확인 과정을 거쳐야 하므로, 이러한 과정에서의 오버헤드를 고려하면 제안된 메커니즘을 키 생성 소요시간이 가장 적게 될 것이다.

[표 2] 공개키 / 개인키 생성 소요시간 (단위 ms)

key length(bits)	Proposed	RSA	DSA
256	26.40	19.80	167.50
512	51.20	28.00	198.67
1024	64.00	113.00	583.67

향후 인증서 바인딩 과정을 추가하여 좀 더 정확한 결과값을 도출할 예정이다. DSA는 제안된 방식이나 RSA 알고리즘보다 월등히 긴 시간이 소요됨을 확인할 수 있다.

두 번째로, 제안된 방식에서의 신원기반 키 생성 과정과 키 갱신 과정의 소요시간을 비교하였으며, 키 갱신 과정은 디바이스에 의한 요청 모델을 사용하였다. 키 갱신 과정은 초기 키 생성 과정과 비교했을 때, 1/3 정도의 시간이 소요됨을 알 수 있다. 이는 시스템 파라미터 분배 과정이나 초기 인증과정이 생략되는 결과로 해석할 수 있을 것이다. 또한, 생성되는 키의 길이가 증가할수록 소요시간의 증가량도 일정한 비례적으로 증가하고 있음을 확인할 수 있다.(표3)

[표 3] 키생성과 키갱신 과정의 소요시간 (단위 ms)

key length(bits)	Generation	Update
256	26.40	6.40
512	51.20	15.20
1024	64.00	24.80

5. 결론

본 논문에서는 비인증서 기반의 공개키 활용을 위해 신원기반 암호화 기술의 개념을 활용하였다. 이러한 개념을 기반으로 안전한 채널을 사용한 공개키/개인키 생성, 임시키를 사용한 공개키/개인키 생성, 등록과정 인증과정 등을 제안하였다. 또한, 디바이스 인증을 등록과정과 디바이스 간 인증과정으로 나누어 제안하였다.

제안된 메커니즘을 구현하고, 다양한 분석을 통해 성능을 검증하여 실제 시스템에 적용될 수 있는지 판단하는 노력이 더욱 필요하며, 이러한 관점에서의 향후 연구가 진행되어야 할 것이다.

참고문헌

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

[2] Richard Newman, Larry Yonge, Sherman Gavette and Ross Anderson, "HomePlug AV Security Mechanisms," In proceedings of IEEE ISPLC 2007, pp. 366-371, March 2007.

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

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

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

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