IEEE 802.15.3 WPAN 환경에서 분산 인증키 관리 방법

송지은*, 박승민**, 조기환*
*전북대학교 컴퓨터정보학과 **전자통신연구원
jeusong, smpark, ghcho@dcs.chonbuk.ac.kr

A Distributed Certificate Key Management Method in IEEE 802.15.3 WPAN Environment

Ji-Eun Song*, Seung-Min Park**, Gi-Hwan Cho*
*Dept of Computer Information Statistics, Chonbuk University
**Electronics and Telecommunications Research Institute

요 약

IEEE 802.15.3 고속률 WPAN(Wireless Personal Area Networks)은 네트워크 구성 시 인증을 받은 노드들에게만 통신 권한을 부여함으로써 보안성을 높였다. 그러나 IEEE 802.15.3 WPAN에서 제안한 인증 방법은 사전에 각 노드들이 중앙 집중적인 키 관리자로부터 오프라인 상으로 인증키를 분배 받는 것을 가정으로 하고 있다. 이 같은 가정은 WPAN이 무선 Ad Hoc 네트워크로서 중앙 관리 노드가 부재하고 위상 변화가 유동적인 특성을 고려하지 못한 것으로 WPAN의 확장성을 감소시킨다. 따라서 본 논문에서는 WPAN의 노드들이 온라인을 통해 협력적으로 인증키를 생성하는 분산 인증키 관리 방법을 제안한다. 이 방법은 WPAN 네트워크에 확장성을 제공할 뿐 아니라 마스터 노드에 대한 보안 의존성을 감소시켜 인증 서비스의 가용성을 증대시킨다.

1. 서론

WPAN은 비교적 짧은 거리 내에서 적은 사용자 간에 정보를 전달하며, 주변 장치간 케이블 없이 직접 통신할 수 있도록 하는 기술이다. 특히 IEEE 802.15.3[1] 고속률 WPAN은 반경 10m 이내에서 통신이 가능하며 최대 54Mbps의 고속률을 지원한다. 따라서 고속률 WPAN은 홈 네트워킹뿐만 아니라, 4세대 이동통신에서 끊김 없는 서비스를 제공하기 위한 개인망 영역의 무선통신 기술로 응용이 확대될 것이다.

IEEE 802.15.3 워킹 그룹에서는 고속 데이터율과 QoS(Quality of Service, Ad Hoc 네트워킹 기술, 보안, 저전력 소모, 저비용 등을 이슈로 표준화가 진행되고 있다. 특히, WPAN은 무선 네트워크에서 보안에 대한 위협에 대응하기 위해 WPAN에 접속하고자 하는 디바이스는 coordinator와 인증 절차를 거쳐 다른 디바이스와 통신할 수 있도록 제한하였다.

그런데 IEEE 802.15.3 WPAN은 Ad Hoc 무선 네트워크[2] 방식으로 유선 네트워크에서와 같은 중앙 관리 노드가 부재 한다. 또한 구성 노드들의 이동성으로 위상 변화가 유동적이다. 따라서 WPAN에서의 인증 방법은 중앙 집중적인 인증기관(Certification Authority)에 의존하지 않고 능동적으로 노드 인증을 수행 할 수 있도록 확장성(scalability)이 보장되어야 한다. 따라서 본 논문에서는 확장성을 지원할 수 있는 분산 인증키 관리 방법을 제안하였다. 즉, 네트워크 구성 초기에 WPAN 노드들은 키 관리자로부터 부분 비밀키를 사전에 분배받을 필요 없이 온라인 상으로 인증서 서명에 사용될 마스터 비밀키를 동적으로 생성하고 재구축 할 수 있는 방법이다.

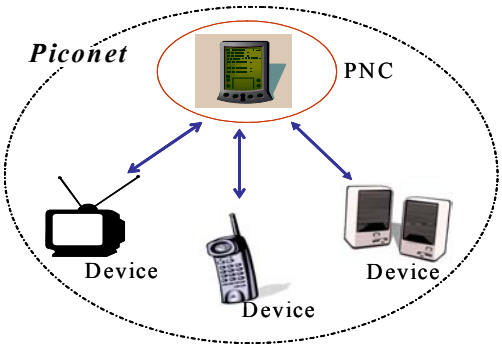
본 논문의 구성은 다음과 같다. 2장에서는 IEEE 802.15.3 WPAN 인증 방법과 Ad Hoc 네트워크의 분산 인증 방법에 대해 살펴본다. 이어 3장에서는 본 논문에서 제안하는 협력적인 WPAN 분산 인증키 생성 및 공유 방법을 기술한다. 마지막으로 4장

에서는 결론을 내리고 향후 연구 과제를 살펴본다.

2. 관련연구

2.1. IEEE 802.15.3 WPAN 인증[1]

IEEE 802.15.3의 보안 모델은 크게 세 가지 모드로 분류될 수 있다. 첫째로, 보안 멤버쉽을 전혀 요구하지 않는 개방형 인증 모드이다. 이 모드에서는 인증 및 데이터 기밀성 유지도 전혀 지원하지 않는다. 둘째로, 보안 멤버쉽을 가진 디바이스만이 인증을 통해 네트워크에 참여할 수 있도록 하는 폐쇄형 인증 모드이다. 이 경우, 데이터 기밀성 지원은 수행되지 않는다. 마지막 보안 모드는 폐쇄형 인증 및 데이터 기밀성을 지원하는 방법으로 인증을 성공적으로 수행한 디바이스에 대해 데이터 기밀성과 무결성을 보장하는 대칭키를 생성하여 분배하는 구조로 되어있다. [그림 1]과 같이 네트워크에 참여하고자 하는 디바이스는 PNC(PicoNet Coordinator)로 선출된 노드에게 인증을 받아야 한다. 성공적으로 인증을 수행하고 난 후, PNC는 데이터 각 디바이스에게 데이터 기밀성과 무결성을 위해 대칭키를 분배한다.

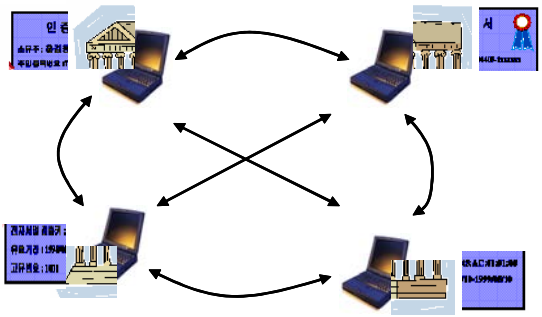


[그림 1] WPAN 인증

그런데 IEEE 802.15.3 WPAN 보안 메커니즘은 사전에 보안 멤버쉽과 인증키가 분배되어 있다고 가정하고 있다. 이와 같은 가정은 임의의 노드가 동적으로 네트워크를 구성하는 WPAN Ad Hoc 특성상 확장성을 감소시키는 가정이다.

2.2 Ad Hoc 네트워크의 분산 인증 기법

유선 네트워크에서 공개키 기반 암호화를 사용하기 위해서는, 신뢰 가능한 제 3의 기관인 키 분배 센터나 인증기관을 이용하였다. 그러나 일반적인 Ad Hoc 네트워크에서는 충분히 신뢰 가능한 제 3의 기관(Trusted Third Party)이 존재한다고 보장할 수 없다. 따라서 대부분의 Ad Hoc 네트워크에서 인증키 관리에 관한 연구들은 (k, n) 임계치 암호화 방식[3][4]을 사용하여 [그림 2]와 같이 신뢰기관의 기능을 각 노드에게 할당하는 형태로 수행되고 있다.



[그림 2] Ad Hoc 네트워크 분산 인증

이 경우 최대 k-1개의 노드에 대한 신뢰성이 손상되더라도, 신뢰 가능한 기관의 비밀키의 노출을 방지할 수 있다. 부분 서명키가 모든 Ad Hoc 노드들에게 분배되어 있는 지 혹은 네트워크상에 임의의 특정 노드에게 분배되어 있는지에 따라 완전 분산 인증기관[5]과 부분 분산 인증기관 구조[6]로 분류된다.

그러나 기존의 분산 인증 기법은 키 관리 기반 시설을 필요로 할 뿐 아니라 새로운 Ad Hoc 네트워크가 구성 될 때마다 오프라인 상으로 사전에 키 정보를 분배받는 형태는 네트워크 구성 및 서비스 수행의 지연을 초래할 수 있다. 따라서 네트워크 구성 초기에 분산 인증 노드들은 키 관리자로부터 부분 비밀키를 사전에 분배받을 필요 없이 온라인 상으로 서로 인증서 서명에 사용될 마스터 비밀키를 동적으로 생성하고 재구축 할 수 있는 방법이 필요하다.

3. 제안 방법론

본 논문이 제안하는 WPAN 환경의 분산 인증키 구축 방법은 기본적으로 '신뢰 기관을 이용하지 않는 임계치 암호화 기법' [7]을 응용하였다. '신뢰 기관을 사용하지 않는 임계치 암호화 기법'은 통신에 참여하는 멤버들이 각각 발생시킨 난수를 기반으로 즉석에서 공개키와 분산된 비밀 공유키를 생성하도록 지원하는 암호학 방법이다. 또한 본 논문은 다음과 같은 사항을 가정으로 삼고 있다.

- 하나의 스캐터넷(Scatternet)은 단일 도메인을 구성한다.
- 각 Ad Hoc 노드들은 임의의 곱셈그룹 Z^*_p의 생성자 g를 알고 있다.
- 악의적인 내부 공격의 가능성을 배제한다.

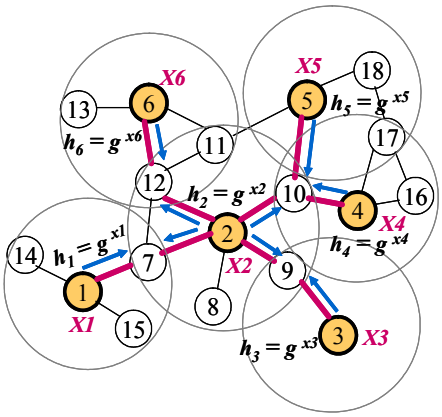
3.1. 1단계 : 공개키와 검증 가능한 부분 비밀키 생성

PNC를 중심으로 구성된 피코넷(Piconet)이 child 피코넷과 parent 피코넷의 관계에 의해 확장된 스캐터넷 구조를 단일 도메인으로 간주한다. 1단계에서는 도메인 공개키와 인증서 서명 비밀키 쌍을 생성 및 구축을 수행한다. 대표적으로 PNC 노드들이 CA로서 각자 생성한 임의의 난수를 이용하여 도메인 인증 공개키와 검증 가능한 부분 비밀키를 생성하여 분배한다.

가. CA 공개키 생성

(1) 부분 공개키 분배

다음 [그림 3]과 같이 각 CA는 임의의 난수 X_i를 발생시키고 부분 공개키 값인 h_i를 생성하여 다른 피코넷의 PNC 즉, CA 들에게 유니캐스트 한다.



[그림 3] 부분 CA 공개키 생성

(2) 공개키 획득

부분 공개키 분배가 완료되면 CA들은 각각 6(각 피코넷의 PNC 수가 6일때)개의 부분 공개키 $h_i(1 \le i \le 6)$를 획득하게 된다. 각 CA 노드는 연산에 의해 도메인 공개키를 생성하여 보유한다.

$$h = \prod_{i=1}^{n} h_i \qquad \text{(h: 공개키)}$$

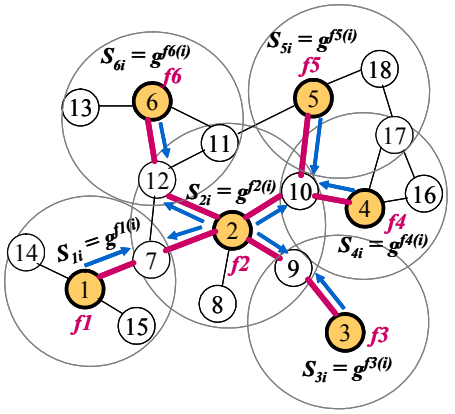
나. 검증 가능한 부분 인증서 비밀키 생성

(1) 검증 계수 교환

CA 노드 P_i는 각각 생성한 난수 X_i를 y절편으로 하는 k-1(k : 임계값)차의 임의의 다항식 f_i를 생성한다. 교환하는 부분 비밀키의 타당성 검증을 위해 다항식 f_i의 계수들 f_{ij}에 대한 정보인 $F_{ji} = g^{fji}$를 다른 PNC 노드들에게 유니캐스트 한다.

(2) 난수에 대한 부분키 전송

CA 노드 P_i는 [그림 4]와 같이 자신이 생성한 임의의 수에 대한 부분키 값인 $S_{ij} = g^{fi(j)}$를 다른 CA 노드인 P_j 들에게 유니캐스트 방식으로 전송한다.



[그림 4] 난수에 대한 부분키 전송

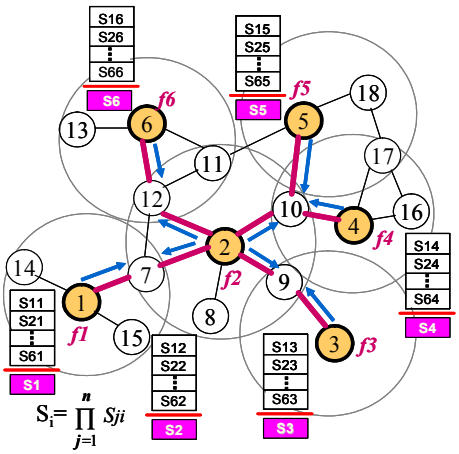
(3) 부분키 검증

검증 계수와 난수에 대한 부분키 전송이 모두 완료되면 CA 노드 P_i는 전송 받은 부분키 S_{ij}가 정당한 값인지를 검증하기 위하여 다음과 같은 계산을 수행한다. 만일 검증이 실패할 경우 'error found' 메시지를 전송하여 해당 노드에게 실패한 부분키 S_{ij}에 대한 재전송을 요청한다.

$$g^{S_{ji}} = \prod_{l=0}^{K-1} F_{jl}^{\,il}$$

(4) 부분 서명 비밀키 생성

검증 계수를 사용하여 성공적으로 전송 받은 난수에 대한 부분키의 검증이 모두 완료되면 [그림 5]와 같이 CA 노드 P_i는 서명 비밀키에 대한 부분키 Si를 생성한다.



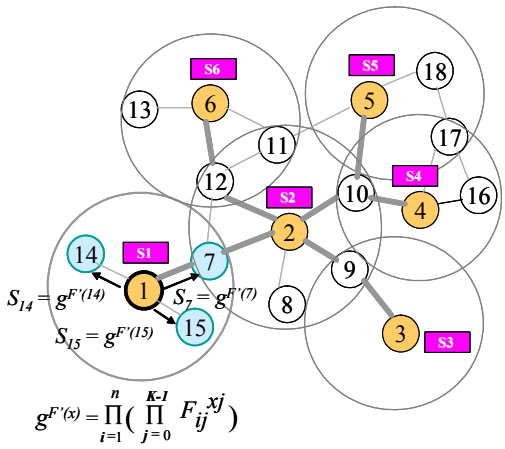
[그림 5] 부분 서명 비밀키 생성

3.2. 2단계 : 부분 비밀키의 완전 분산

WPAN은 Ad Hoc 네트워크로서 노드들이 동적으로 이동할 수 있다. 특히, 피코넷 내에서 타임 슬롯을 제공하고 인증을 수행하는 PNC가 네트워크를 이탈하거나 권한이 변조될 경우 인증키를 위임하거나 재구축 해야 하므로 인증 서비스의 지연이 발생할 수 있다. 따라서 각 피코넷의 모든 멤버 노드들에게 인증 비밀키를 분배함으로써 PNC에 대한 보안 의존성을 감소시켜 인증 서비스의 가용성을 높일 수 있다. 따라서 본 논문에서는 동일 도메인 내에 존재하는 WPAN 노드가 임계치 이상의 이웃 노드와의 협력을 통해 인증서 서비스를 제공받을 수 있는 완전 분산 인증 구조를 지원한다.

가. 피코넷 멤버에게 부분 비밀키 분배

각 피코넷의 PNC 노드는 도메인 CA의 공개키와 비밀키 쌍을 생성하는 과정에 대표로 참여하는 협력적인 분산 CA들이다. PNC 노드가 도메인 CA 공개키와 부분 서명 비밀키 생성을 완료하면 피코넷의 슬레이브 멤버들에게도 부분 서명 비밀키를 분배한다. 이 방법은 하나의 스캐터넷을 구성하는 모든 피코넷의 노드들에게도 CA기능을 분배하여 인증서비스의 가용성을 높일 수 있다.



[그림 6] 피코넷 멤버들에게 부분 서명키 분배

나. 서명키 생성 및 인증서 발행

생성된 부분 비밀 서명키는 서명키 생성에 이용된다. 가령, 노드 P_2가 인증서 발행을 위해 공개키 h에 대한 서명을 수행하고자 할 때, P_2는 인접하는 슬레이브 노드들에게 부분 서명키를 요청한다. 이때, P_2는 임계치 이상의 부분 서명키 S_j를 획득하면 다음과 같은 방법으로 서명키 S를 생성할 수 있다. 서명키 S를 이용하여 인증을 요청한 WPAN 노드의 공개키에 대한 인증서를 발행할 수 있다.

$$S = \prod_{j=1}^{k} S_j \quad (k : 임계값)$$

4. 결론

본 논문에서는 '신뢰 기관을 이용하지 않는 임계치 암호화 기법'을 IEEE 802.15.3 WPAN에 응용하여 협력적인 분산 인증키 구축 방법을 제안하였다. 이는 WPAN 노드들이 사전에 키 관리자를 통해 비밀키를 분배받지 않고 단일 도메인 내에서 온라인을 통해 협력적으로 인증키를 생성할 수 있도록 지원하여 확장성을 증가시킨다. 또한 인증 권한 즉, 인증서 비밀키를 모든 피코넷 노드들에게 분산시킴으로써 PNC에 대한 보안 의존성을 감소시켜 인증 서비스의 가용성을 높였다. 그러나 여전히 무선 자원의 제약으로 WPAN에서 제어 메시지를 최소화하는 노력이 요구된다. 따라서 적은 보안 제어 메시지와 연산 오버헤드로 인증키를 협의할 수 있는 방안이 계속해서 활발히 연구되어야 한다.

참고문헌

[1] IEEE Draft P802.15.3/D08, "Wireless Medium Access Control(MAC) and Physical Layer(PHY) Specifications for High Rate Wireless Personal Area Networks(WPAN^{TM})," Nov. 2001.

[2] Charles E. Perkins, "Ad Hoc Networking," *Addison Wesley Press*, Dec. 2000

[3] A. Shamir, "How to Share a Secret," *Communication of the ACM, 22(11),* pp. 612-613, 1979.

[4] Y. Frankel and Y. G. Desmedt, "Parallel Reliable Threshold Multi-signature, *Technical Report TR-92-04-02,* Univ. of Wisconsin Milwaukee, Apr. 1992.

[5] H. Luo, J. Kong, P. Zerfos, S. Lu, and L. Zhang, "Self-securing As Hoc Wireless Networks," *Proc. of the 7th IEEE Symposium on Computers and Communications (ISCC '02)*, 2002, pp. 567-574.

[6] L. Zhou and Z. J. Haas, "Securing Ad Hoc Networks," *IEEE Networks*, 13(6), pp. 24-30, 1999.

[7] T. P Pedersen, "A Threshold CryptoSystem without a Trusted Party," *In Advances in Crytology Eurocypt 91*, pp. 522-526, 1991.