MANET에서 Threshold Secret Sharing과 CGA를 이용한 인증 메커니즘

조신영*, 임헌정*, 정태명**
*성균관대학교 전자전기컴퓨터공학과
**성균관대학교 정보통신공학부
{sycho, hjlim99}@imtl.skku.ac.kr, tmchung@ece.skku.ac.kr

Authentication Mechanism using Threshold Secret Sharing and CGA in MANET

Shin-Young Cho*, Hun-Jung Lim*,
Tai-Myoung Chung**
*Dept. of Electrical and Computer Engineering, Sungkyunkwan Univ.
**School of Information Communication Engineering, Sungkyunkwan Univ

요 약

안전한 통신을 위해 단말기 간에 인증이 제공되어야 하는데 MANET 환경에서는 무선 환경이라는 특징으로 보안상 취약하고, 중앙단말기의 부재로 인해 인증을 제공하는 것에 어려움이 있다. 이러한 어려움을 해결하기 위한 많은 기법 중에 단말기 간의 구조를 Local로 나누어 인증 서비스를 제공하는 Localized Certification Service가 있다. 본 논문에서는 Localized Certification Service을 상에서 Threshold Secret Sharing을 이용한 인증 메커니즘을 제안한다. 또한 제안한 메커니즘은 CGA의 재생성 후 재발급 문제 역시 해결하게 된다. 본 논문에 결론에서는 제안한 방식을 다양한 위협 시나리오에 적용하여 위협에도 안전한 인증을 제공함을 보였다.

1. 서론

MANET(Mobile Ad hoc Networks)에서 단말기는 무선 환경에서 이동성을 가지며 통신의 주체가 된다. MANET은 홍수, 지진으로 인한 자연재해 현장 등에서 통신 인프라 망이 파괴되어 이용할 수 없을 때 신속하게 네트워크를 형성하여 통신이 가능하게 한다.

MANET에서 보안 시스템을 구축하는 데에 있어서 우선적으로 고려해야 할 것은 안전한 인증 서비스를 제공하는 것이다. 인프라 기반의 네트워크에서는 인증서 발급기관(Certification Authority:CA)이 존재하였지만 MANET에서는 중앙 단말기의 부재로 CA를 지정할 수 없어 인증서를 발급하는 데에 어려움이 있다. 이러한 문제를 해결하기 위해 MANET 상에서 인증서를 발급하고 인증서비스를 제공하기 위한 Localized Certification Service가 연구되고 있다[2][3]. 본 논문에서는 Localized Certification Service 상에서 Threshold Secret Sharing을 이용한 인증 메커니즘을 제안한다. 제안한 메커니즘은 CGA의 재생성 후 재발급 문제 역시 해결하여 안전한 통신이 가능하다.

본 논문은 다음과 같이 구성된다. 2장에서는 관련연구로 Threshold Secret Sharing, Localized Certification Service, SEND에 대해 살펴보고, 3장에서는 MANET에서의 인증 메커니즘을 제안한다. 4장에서는 시나리오를 통해 인증 메커니즘을 평가하고, 5장에서 결론 및 추후 연구에 대해 설명하였다.

2. 관련연구

2.1 Threshold Secret Sharing

Threshold Secret Sharing은 비밀정보를 한 곳에 집중시키지 않고, 분산시키므로 안전하게 관리할 수 있도록 하는 기법이다[1]. “(t, n) Threshold Secret Sharing”이라고도 표현되며 참가자가 n명이라 할 때, 비밀정보 분배자가 특정 비밀정보를 n개의 분할된 비밀정보로 분할하여 참가자 n명에게 분배하고, 참가자 중 t명이 모여야 원래의 비밀정보로 복원되도록 하는 방식이다.

분할된 비밀정보는 아래와 같은 임의의 t-1차 다항식으로 구해진다.

$$f(x) = k + a_{t-1}x^{t-1} + \ldots + ax \bmod p$$

- k : 비밀정보
- a : 무작위로 선정된 값
- p : 임의의 소수 (단, p > k, n)

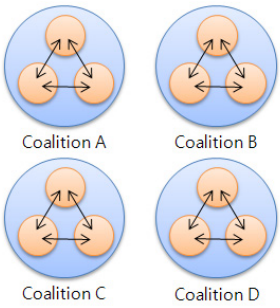
비밀정보 분배자는 x(x=1,2,..,n)에게 분할된 정보인 f(x)를 분배한다. (t, n) Threshold Secret Sharing는 비밀정보 k가 고정되어 있을 때, 다른 분할된 비밀정보 f(x)에 영향을 주지 않고도 동적으로 비밀정보를 추가하거나 바꿀 수 있고, 원래의 비밀정보 k를 바꾸지 않아서 분할된 비밀정보 f(x)들을 바꿀 수 있다. 또한 분할된 비밀정보 f(x)를 등급에 따라 다른 개수로 배포하는 것도 가능하다.

2.2 Localized Certification Service

단말기가 인증서비스에 참여하려면 제 3의 신뢰할 수 있는 기관으로부터 인증서를 발급받아야 한다. MANET상에서 CA가 구성되는 방식에 따라 세 가지로 구분할 수 있다.

- 중앙 집중식 방식(Centralized Certification Service)
- 계층적인 방식(Hierarchical Certification Service)
- 지역적인 방식(Localized Certification Service)

중앙 집중적/계층적인 방식은 상위의 CA가 공격당했을 때, 해당 CA와 관련된 단말기들은 인증서비스가 중단되는 문제가 있다. 지역적인 방식은 지역으로 단말기들을 구분지어 한 지역 안에 단말기들은 각각이 CA의 역할을 할 수 있는 방식이다. MANET에서는 단말기들이 이동성을 가지므로 특정한 단말기를 CA로 정하는 데에 어려움이 있어 지역적 방식에 대한 연구가 활발히 진행 중이다. (그림 1)은 지역적인 방식에 대한 설명이다.



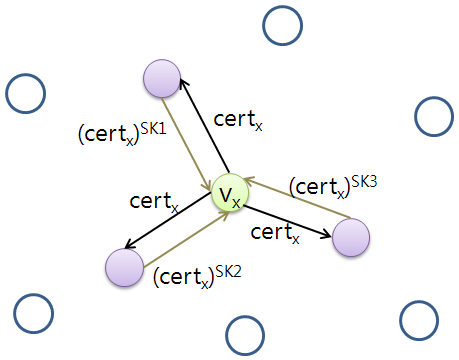
(그림 1) Architecture of Localized Certification Service

[2]에서는 지역적인 방식에서 Threshold Secret Sharing 방식을 적용한 인증 기법을 제안하였다. 시스템 부팅 시 각 단말기 v_i는 인증서$cert_i$ 와 비밀정보 Pv_i를 가지게 된다. $cert_i$는 $[v_i \| pk_i \| T_{sign} \| T_{expire}]$ 의 구조로 이루어져 있다. 분할된 비밀정보 Pv_i는 시스템의 공개키 {SK, PK} 중 비밀키 SK를 분할한 정보로 $Pv_i = f(v_i) \bmod n$으로 구해지고, 숨겨지는 비밀정보는 $f(0) = SK$ 이다. 분할된 정보 P_{v_i}에서부터 완전한 시스템 비밀키 SK를 구하기 위한 공식은 다음과 같다.

$$SK \equiv \sum_{j=1}^{k} (Pv_i \bullet lv_i(0) \bmod n) \equiv \sum_{j=1}^{k} SK_j \bmod n$$

새로운 단말기 v_x가 다른 단말기들과 안전한 통신을 하기 위해 인증서비스에 참여하도록 인증서를 발급하는 과정은 위 (그림 2)와 같다. 단말기 v_x가 참여하고자 하는 Coalition의 모든 단말기들에게 인증서 요청 메시지는 브로드캐스트 한다. 인증서 요청을 받은 해당 Coalition에 속한 단말기들은 단말기 v_x가 믿을만한 단말기인지 아닌지를 확인한다. 믿을만한 단말기일 경우 분할된 인증서를 계산하여 단말기 v_x에게 전송한다. 단말기 v_x를 신뢰 할 수 없는 경우에는 인증서 요청을 버리고 무시한다. 단말기 v_x가 Coalition으로부터 k개 이상의 분할된 인증서를 얻게 되면 muti-signature protocol의 방식 을 이용하여 시스템 개인키로 서명한 새로운 완전한 인증서를 발급받게 된다. multi- signature protocol의 공식은 다음과 같다.

$$X^{sk_1} \bullet X^{sk_2} \bullet \ldots \bullet X^{sk_k} = X^{sk_1 + sk_2 + \ldots + sk_k}$$

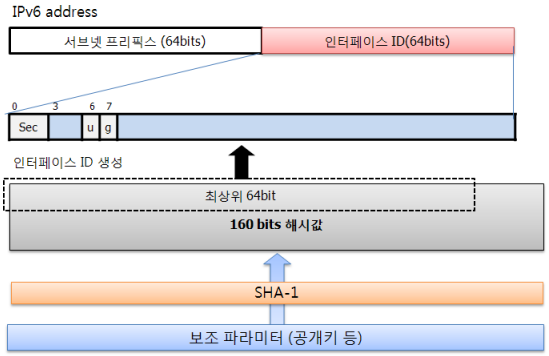


(그림 2) Localized Certification Service

2.3 SEcure Neighbor Discovery(SEND)

SEND은 이웃 탐색(Neighbor Discovery) 메시지의 송신자 주소가 실제 메시지 송신자의 주소와 일치하는 지를 증명해주고, 디지털 서명을 통한 송신자 인증과 메시지의 무결성을 제공하는 것이다[5]. SEND를 통해 공격자가 특정 단말기를 사칭하여 이웃탐색 메시지 보내지 못하도록 한다. 재전송 공격(Relay Attack)을 방지하기 위해, Redirect와 같은 단방향 메시지에는 타임스탬프(Time Stamp) 값을 이용하고, Solicitation/Advertisement와 같은 양방향 메시지에는 임의의 수를 이용한다. SEND는 디지털 서명(Digital Signature)과 CGA(Cryptographically Generated Address)[4]를 기반 기술로 하고 있다.

SEND에서는 IKE(Internet Key Exchange)에 의한 키 분배를 사용하지 않고, 각 단말기들이 직접 공개키를 교환한다. CGA는 각 단말기들이 직접 키를 교환할 수 있도록 한다. CGA의 주소 형식은 다음 (그림 3)과 같다.



(그림 3) CGA의 주소 형식

CGA는 공개키 서명방식과 IPv6 주소를 결합하는 방식으로 IPv6에 인터페이스 ID에 해당하는 주소가 되고, CGA

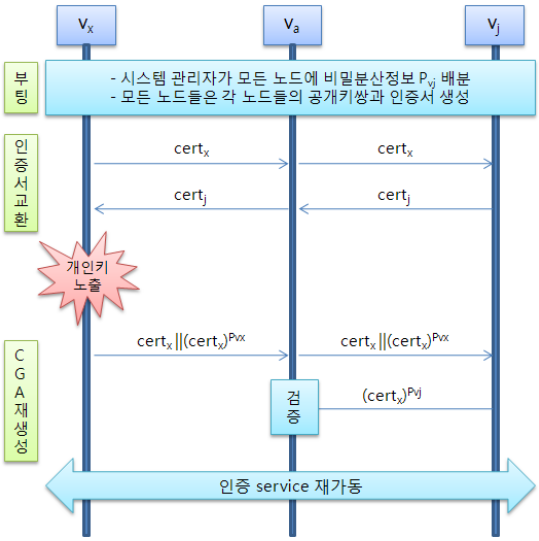
주소 값은 메시지 생성자의 공개키와 보조 파라미터를 일방향 해시 함수로 암호화하여 연산함으로 구할 수 있다. IPv6 주소에서 처음 64bit는 서브넷 프리픽스 값을 설정하고, 주소에 나머지 64bit에는 인터페이스 ID 대신에 공개키와 보조 파라미터를 해시 함수로 연산하여 나온 160 bit 길이의 해시 값에 처음 64bit 사용하여 주소를 생성하여 설정한다. 이때 Sec은 전사공격(brute-force attacks)를 방지하기 위한 요소이다.

검증은 수신 받은 상대방이 CGA주소를 생성할 때에 사용 했던 공개키와 보조 파라미터를 가지고 해시값을 재계산하여 인터페이스 ID 부분과 비교하는 과정을 통해 이루어진다.

CGA 주소 검증을 한 후에 이웃 탐색 프로토콜 옵션인 CGA 옵션에 포함된 공개키를 이용하여 RSA Signature 옵션에 포함된 디지털 서명을 검증한다. 공격자가 자신이 생성한 개인키와 공개키로 서명한 경우에도 CGA주소에 인터페이스 ID와 해시 값을 비교하면 검증이 가능하다. 이 과정을 통해 송신 단말기에 대한 인증이 이뤄지고, 전송된 메시지가 인증된다.

3. 제안방식

하나의 Coalition에 참여하는 단말기들 간에 신뢰성 있는 통신을 위해서는 인증이 제공되어야 한다. 본 논문에서는 SEND기법과 Threshold Secret Sharing기법을 적용하며 제안 방식의 전체적인 구조는 (그림 4)와 같다.



(그림 4) 제안 방식

SEND는 각 단말기의 공개키가 실제로 그 단말기의 공개키인지 아니면 다른 단말기로 가장한 악의적인 단말기의 공개키인지를 판별해 줄 수 있다. 기능을 제공을 위해 SEND에서는 CGA를 사용한다. CGA를 생성하는 요소 중에 각 단말기의 공개키 값이 포함된다.

인증서를 발급하는 데에는 Threshold Secret Sharing이 사용된다. 인증서비스를 이용하던 단말기가 만료기간 안에 인증서를 재 갱신하지 못하였거나 공격자에 의해 개인키가 노출되었을 경우 공개키 쌍을 재생성하여 이웃 단말기들에게 새로운 인증서와 공개키를 전송해야 한다. 새로운 공개키 쌍을 생성한 단말기의 주소는 CGA기법에 따라 그에 해당하는 새로운 주소를 가지게 된다. 개인키가 노출된 경우에는 공격자도 단말기 v_x의 개인키를 알고 있으므로 공격자가 자신의 공개키를 이웃단말기들 v_j에게 새로운 공개키인 듯 속여 전송할 수 있게 된다. 이때 Threshold Secret Sharing 기법에 의해 새로운 공개키가 공격자가 아닌 정당한 단말기의 것임을 증명한다.

○ 부팅

부팅 전에 시스템 관리자는 시스템의 공개키 쌍 (SK, PK)를 생성한다. 관리자는 자신의 개인키 SK를 (t, n) Threshold Secret Sharing에 다항식 f(x)로 비밀분산정보 $P_{v_j} = (f(v_j) \bmod n)$을 구한다. 모든 단말기들이 부팅되기 전에 시스템 관리자는 비밀분산 정보 P_{v_j} 를 부여하고, 부팅 시에 각 단말기들은 자신만의 공개키쌍 (sk_j, pk_j)와 인증서 $cert_j = (v_j, pk_j, T_{sign}, T_{\text{expire}})$를 생성한다.

○ 인증서 교환

각 단말기들은 자신이 생성한 인증서 $cert_j$를 SEND를 이용하여 이웃 단말기들에게 전송해주는 방식으로 서로 인증서를 교환한다. 이로 인해 공격자가 자신을 사칭하는 사태를 사전에 방지한다.

○ CGA 재생성 및 인증서 재분배

본 논문에서 제안 하는 핵심 부분으로써 단말기의 개인키가 공격자에 의해 노출 되었거나 인증서 만료기간 안에 인증서 갱신이 이루어지지 않았을 경우, 단말기는 자신의 인증서를 더 이상 사용할 수 없으며 공개키 쌍과 인증서를 재생성해야 하고 새로운 공개키에 따라 단말기의 CGA 값도 재생성하게 된다.

개인키가 노출된 경우 공격자는 단말기 v_x의 노출된 개인키를 알고 있으므로 이웃단말기들 v_j은 공격자가 자신의 주소와 공개키를 전송하면서 단말기 v_x인 듯 속일 경우 판별할 수 없다. 이러한 상황을 방지하기 위해 부팅 전에 시스템 관리자에게 부여받은 비밀분산정보를 이용한다. 비밀분산정보는 공격자에 의해 노출되는 것을 방지하기 위해 주기적으로 업데이트됨으로 비밀분산정보가 노출될 확률이 낮다고 가정한다. 단말기 v_x는 자신이 부여받은 비밀분산정보로 서명한 분할된 인증서와 인증서 원본을 이웃단말기들에게 전송한다. 인증서 원본을 받은 이웃단말기들은 자신에게 부여된 비밀분산정보로 서명을 하여 다시 이웃단말기들에게 전송한다.

이웃단말기 중 하나인 단말기 v_a는 개인키가 노출된 단말기 v_j가 전송한 분할된 인증서 $(cert_x)^{P_{vx}}$ 와 다른 이웃 단말기들이 자신들의 비밀분산정보로 서명한 인증서 중 k-1개의 인증서를 선택하여 multi-signature protocol에 따라 $X^{sk_1} \bullet X^{sk_2} \bullet \ldots \bullet X^{sk_k} = X^{sk_1+sk_2+\ldots+sk_k}$ 로 연산하여 인증서를 얻어낸다. 연산 결과가 시스템의 개인키가 서명한 인증서일 경우, 단말기v_j의 비밀분산정보가 정당한 것임이 판명되어 단말기v_j가 다시 인증 서비스에 참여 할 수 있게 된다. 복원되지 않는 경우에는 공격자로 판단하여 인증서 요청은 무시하게 된다. 이때 악의적인 단말기가 잘못된 비밀분산 정보를 보낼 수 없다고 가정한다. 이렇게 하여 시스템 개인키로 서명하는 동시에 정당한 단말기임을 증명할 수 있다.

4. 보안성 평가

본 논문에서 제안하고 있는 인증 메커니즘은 중앙 단말기가 없는 MANET 환경에서 중앙 단말기 없이도 시스템 관리자의 비밀키로 서명된 인증서를 발급할 수 있도록 한다. 또한 단말기가 보내는 인증서가 실제 그 단말기의 인증서임을 보장하고, 인증서를 재발급 시에도 공격자의 방해를 차단하여 안전하게 인증서를 분배할 수 있다.

제안하는 인증 메커니즘은 (t, n) Threshold Secret Sharing기법은 적용하므로 각 단말기들이 직접 인증서 발급기관의 역할을 수행하여 중앙단말기 없이도 인증서의 일부분을 발급한다. 공격자가 인증 서비스를 중단시킬 목적으로 하나의 단말기가 동작을 멈추게 할 경우, 단말기의 수가 임계치인 n개만큼만 있어도 인증 서비스 계속적으로 제공할 수 있어 어느 정도의 서비스 가용성을 보장한다. 공격자가 단말기를 공격하여 비밀분산정보를 알아냈을 경우, 임계치 n개의 비밀분산정보를 모은 것이 아니면 시스템 관리자의 개인키가 복원되지 않고 안전하다.

인증서를 생성하고 이웃단말기들에게 전송하여 이웃단말기들이 자신의 공개키를 알 수 있도록 하려고 할 때, 공격자가 정당한 단말기의 주소로 자신의 공개키를 전송하여 마치 정당한 단말기 인 것처럼 속일 수 있다. SEND기법을 적용하면, 주소와 공개키 사이에 연관성을 갖도록 하므로 특정 단말기의 주소로는 자신의 공개키만을 보낼 수 있게 되어 안전하다.

공격자가 단말기를 공격하여 그 단말기의 개인키가 노출 되면 단말기는 공개키 쌍을 새로 생성하여 이웃단말기들에게 알려주게 된다. 이때 공격자가 공격한 단말기의 개인키와 공개키를 알고 있어 공격을 당한 단말기인 것처럼 위장하여 자신의 공개키를 제공하려고 할 수 있다. 이때 공격자는 비밀분산정보를 가지고 있지 않기 때문에 공격자가 임의의 수를 정하여 인증서 발급을 시도하더라도, 공격자가 만든 분할된 인증서로는 완전한 인증서를 계산할 수 없고 정당한 사용자가 아님이 판단되어 완전한 인증서가 발급이 되지 않는다.

5. 결론 및 향후 연구방향

본 논문에서는 MANET 환경에서 Threshold Secret Sharing과 SEND를 적용한 인증 메커니즘을 제안하였다. 제안한 인증 메커니즘은 인증 요청을 보내는 단말기 자체에 대한 인증과 메시지에 대한 인증을 제공하며, CA없이도 CGA를 재 생성하여 인증서를 재발급 받을 수 있다.

추후 연구로써 새로운 인증서를 발급받는 다른 인증 메커니즘에 대한 조사와 제안하는 인증 메커니즘과 비교 분석이 이루어져야 할 것이다.

참고문헌

[1] Adi Shamir, How to share a secret, Communications of the ACM, 22(11):612-613, 1979

[2] J. Kong et al., Providing robust and ubiquitous security support for mobile ad-hoc networks, In Proc. IEEE ICNP, pp.251-260, 2001

[3] H. Al-bahadili et al., Performance evaluation of the TSS node authentication scheme in noisy MANETs, International Journal of Network Security, vol.12, No.3, PP.121-129, 2011

[4] T. Aura, "Cryptographically Generated Addresses(CGA)", IETF, RFC 3972, March, 2005

[5] Arkko, J., Ed., "SEcure Neighbor Discovery(SEND)", IETF, RFC 3971, March, 2005

<표 1> Notation

기 호	설 명
SK	개인키
PK	공개키
SK_{sys}	System 개인키
PK_{sys}	System 공개키
P_{v_j}	단말기 j(1,...,K)에게 분배한 비밀분산정보를 계산하기 위한 값
sk_j	단말기 j(1,...,K)의 개인키
pk_j	단말기 j(1,...,K)의 공개키
v_j	한 Coalition에 속하는 모든 단말기들
v_x	CGA를 재생성하는 단말기
$Coalition$	1~K개의 단말기가 구성하는 한 집합
$cert_j$	단말기 j(1,...,K)의 인증서
T_{sign}	인증서를 생성한 시간
$T_{\exp ire}$	인증서 만료 시간
SK_j	j(1,...,K)개로 나눠진 비밀분산정보