무선 메쉬 네트워크의 보안

김종택 | 박세웅
서울대학교

요 약

무선 메쉬 네트워크의 보안 이슈는 노드의 오동작, 라우팅, 그리고 인증으로 구분할 수 있다. 이러한 문제는 무선 애드혹 네트워크에서 많이 다루어져 왔지만 무선 메쉬 네트워크에서는 메쉬 라우터 (MR) 들이 고정적이고, 전력 제한이 없다는 특성을 이용하면 보다 성능 좋은 해법을 제안할 수 있다. 본 고에서는 무선 메쉬 네트워크의 보안에 대한 최근 연구들을 살펴 보고, 무선 메쉬 네트워크를 대상으로 한 최초의 분산 인증 기관인 MeCA (Mesh Certification Authority)를 제안한다. MeCA에서는 무선 메쉬 네트워크의 특성을 이용하여 분산 인증 기관의 보안성과 효율성을 향상시켰다. 이를 위해 우리는 향상된 임계치 암호화 방법과 멀티캐스팅을 도입하였다. 모의 실험을 통해 MeCA가 기존의 무선 애드혹 네트워크에서 제안된 방법들에 비해 적은 오버헤드를 일으키며 더 강한 공격에도 비밀키를 노출하지 않는 것이 확인되었다.

I. 서 론

무선 메쉬 네트워크는 무선 채널을 이용해 독립적인 네트워크를 구성하거나 인터넷 연결을 위한 중계망을 형성하는 데 효과적인 기술로 주목받고 있다 [1]. 그러나 무선 메쉬 네트워크의 보안 기술에 대한 연구는 아직 큰 관심을 받지 못하고 있는 상황이다. 물론 기존의 무선 애드혹 네트워크에서 제안되었던 보안 관련 기술들이 무선 메쉬 네트워크에도 동일하게 적용될 수 있을 것이다. 하지만 무선 애드혹 네트워크와는 달리 무선 메쉬 네트워크의 메쉬 라우터 (MR)들은 이동성이 낮고 전력을 계속 공급받는다. 따라서 이에 적합한 새로운 보안 기술들이 요구된다. 무선 메쉬 네트워크는 자가조직적인 특징을 가지고 있다. 즉, 무선 메쉬 네트워크를 구성하는 MR들은 관리자의 설정 없이도 주변 MR들과 정보를 교환하여 하나의 네트워크를 구성하게 된다. 따라서 MR이 공격자에 의해 조작되어 악의적인 동작을 수행할 가능성이 있다. 또 이런 MR이 자신을 경유하는 패킷을 도청할 수도 있다. 이러한 문제를 해결하는 데에는 우선 MR과 MR, 메쉬 클라이언트 (MC)와 MR 간의 인증이 해결되어야 한다. 일반적인 공개키 기반 구조에서는 인증 기관 (Certification Authority, CA)을 모든 노드가 신뢰하므로 이를 통해 노드 상호 간의 인증을 수행할 수 있다. 그러나 무선 메쉬 네트워크와 같은 자가조직적인 네트워크에서는 이러한 신뢰받는 제 3자 (Trusted Third Party)가 존재하지 않는다. 따라서 CA 기능을 MR들이 (n, m) 임계치 암호화 방법을 이용해 분담하게 된다. 즉, CA 비밀키 k의 부분비밀을 n명이 나누어 갖고 있으며, 이 중 m명 이상의 부분비밀을 알아야 비밀 k를 재구성할 수 있다. 기존의 무선 애드혹 네트워크에서는 Mobile Certification Authority (MOCA) [2], Secure and Efficient Key Management (SEKM) [3]와 같이 임계치 암호화 방법을 이용한 분산 CA가 이미 제안되어 있다. 이러한 방법에서는 무선 애드혹 네트워크의 노드 중 비교적 성능이 높은 노드가 분산 CA 기능을 담당하게 된다. 그러나 무선 메쉬 네트워크의 MR들은 전력 제한이 없고, 모두 성능이 높기 때문에 모든

노드가 CA 기능 분산에 참여할 수 있고, 주기적으로 CA 기능을 담당하는 노드를 바꿔 주는 것도 가능하다. 무선 애드혹 네트워크의 노드들은 이동성이 높기 때문에 MOCA와 SEKM에서는 라우팅 방법으로 유니캐스팅과 브로드캐스팅을 사용하고 있다. 그러나 무선 메쉬 네트워크에서는 MR들이 거의 이동하지 않는다는 특성을 이용하면 효율적인 멀티캐스팅 방법을 적용할 수 있다. 본 고에서 우리는 무선 메쉬 네트워크에 최적화된 분산 인증 기관인 Mesh Certification Authority (MeCA) 를 제안한다. MeCA의 보안성 향상을 위해 Fast Verifiable Secret Redistribution (FVSR) 방법을 개발하고, 효율성 향상을 위해 Ruiz 트리 [4]를 이용한 멀티캐스팅을 도입한다. CA는 인증서 갱신, 폐기 및 상태 확인의 기능을 갖고 있어야 한다. MeCA에서는 부분 인증서 방법을 사용하여 인증서 갱신을 구현한다. 인증서 폐기와 상태 확인은 인증서 폐기 목록 (Certificate Revocation List, CRL) 방법을 이용한다. MeCA는 FVSR 방법을 적용하고 멀티캐스팅을 도입하여 보다 안전하고 효율적으로 이러한 CA 기능을 수행할 수 있다. 본 고는 다음과 같이 구성되어 있다. 2장에서는 무선 메쉬 네트워크의 보안에 관련된 연구들에 대해 알아본다. 3장에서는 임계치 암호화 방법에 대해 간단히 살펴본다. 4장과 5장에서 MeCA 의 구체적인 아키텍처를 설계하고, 그 성능을 평가한다. 6장에서 결론을 맺는다.

II. 무선 메쉬 네트워크의 보안 이슈

무선 메쉬 네트워크에서 MR들은 건물의 옥상과 같은 곳에 설치되므로 유선망의 라우터에 비해 물리적으로 외부 공격에 쉽게 노출된다. 더욱이 새로 설치된 MR은 스스로 주변의 MR들과 통신하여 메쉬 네트워크를 구성하게 된다. 따라서 무선 메쉬 네트워크에서는 MR들이 공격자에 의해 조작되어 악의적인 기능을 수행할 가능성이 있다. 또한 무선 메쉬 네트워크는 멀티홉 무선 통신을 기반으로 하기 때문에 트래픽이 도청당하거나 방해 전파 (jamming) 에 의해 훼손될 가능성이 존재한다 [5]. 본 장에서는 이러한 문제들을 해결하기 위한 기술로 어떤 것이 있는지 살펴본다. 그리고 보안을 위해 가장 근본적인 문제인 노드 간의 인증과 키 관리 문제를 해결하는 방법에 대해서도 알아보도록 한다.

1. 오동작 노드의 처리

공격자는 설치된 MR을 물리적으로 제거하거나 다른 MR로 교체할 수 있다. 이렇게 하여 메쉬 네트워크의 토폴로지를 변화시킴으로써 일부 MR을 고립시키거나 특정 MR에 과부하를 일으키는 등 공격자가 원하는 목적을 달성할 수 있다. 그러나 이러한 형태의 공격은 탐지해내기가 매우 어렵다. 무선 메쉬 네트워크의 자가조직적인 특성상 MR의 설치와 제거만으로는 그것이 악의적인 공격인지 판단할 수 없기 때문이다. 따라서 무선 메쉬 네트워크의 관리자가 주기적으로 MR의 상태를 점검할 필요가 있다. 한편 기존의 MR에 대한 관리 권한을 획득한 공격자는 MR의 설정을 변경하여 그 MR에 의해 라우팅되는 트래픽을 모두 도청하거나 그 트래픽의 라우팅을 거부할 수 있다. 이 경우 무선 메쉬 네트워크를 이용하는 MC의 익명성이 보장되지 않거나 메쉬 네트워크가 무선 백본망으로서의 역할을 수행할 수 없게 된다. 이러한 공격을 탐지하기 위해서는 [6]과 같은 방법을 사용하여 MPP (Mesh Portal)가 MR의 설정 변경 여부를 판단하도록 한다. 최근에는 다중채널을 사용하는 무선 메쉬 네트워크에서 채널을 할당할 때 공격자가 잘못된 정보를 전달하여 효율적인 채널할당을 방해하는 문제를 해결하는 방법이 제안되었다 [7]. 공격자는 자신이 보낸 채널정보의 유효성을 다른 노드가 확인하지 않는다는 점을 이용해 우선 순위가 높은 채널을 할당받아 메쉬 네트워크 전체의 성능을 열화시킬 수 있다. 이러한 문제를 해결하기 위해 [7]에서는 한 노드의 동작을 이웃 노드들이 계속 감시하고 오동작이 임계치 이상으로 발견됐을 시에는 그 노드를 신뢰하지 않도록 하고 있다.

2. 라우팅 보안

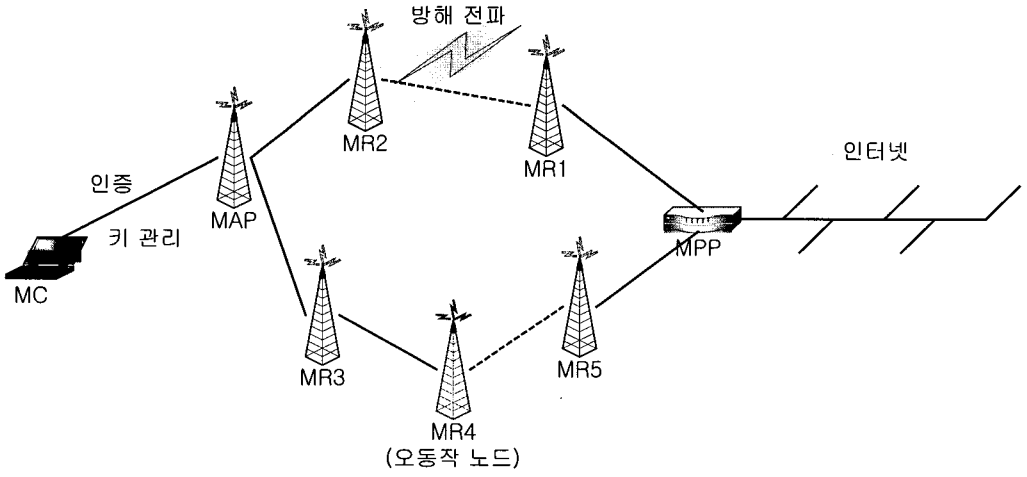
라우팅 메시지가 암호화되지 않은 경우 공격자는 이를 위조하거나 변조하여 트래픽이 특정 MR을 통과하도록 하거나 최적이 아닌 경로를 통해 MPP에 전달되도록 할 수 있다. 이러한 문제는 기존의 무선 애드혹 네트워크에서 제안되었던 안전한 라우팅 알고리즘을 적용함으로써 해결될 수 있다 [8]. 방해 전파를 이용한 DoS (Denial of Service) 공격은 라우팅에 대한 가장 간단하고 강력한 공격 방법이 된다. 방해 전파에 의해 어떤 MR이 이웃 MR과 연결이 끊기게 되면 그 MR

은 전체 메쉬 네트워크에서 고립되거나 최적이 아닌 우회 경로를 통해 MPP에 연결되게 된다. 방해 전파를 송신하는 노드를 탐지하고 [9] 가능하다면 그 노드를 제거함으로써 이러한 문제를 해결할 수 있다.

3. 인증과 키 관리

무선 메쉬 네트워크에는 다른 모든 노드로부터 신뢰받는 단일 노드가 존재하지 않는다. 따라서 노드 사이의 인증과 키 관리는 분산된 형태로 구현되어야 한다. 분산 키 관리 방법은 기존의 무선 애드혹 네트워크에서 많이 연구되어 왔다. Capkun et al. [10] 은 Pretty Good Privacy (PGP) 와 유사한 형태의 키 관리 방법을 제안하였다. 각 노드는 자신의 인증서를 스스로 생성하여 이웃에 전달하며, 받은 이웃의 인증서는 저장해 둔다. 다른 노드의 인증서를 인증하기 위해서는 두 노드간의 인증 고리를 찾는다. Yi et al. [2] 은 중앙집중적인 신뢰 모델과 분산된 신뢰 모델을 결합하여 두 모델의 장점을 모두 획득하였다. 이 시스템에서는 '신뢰도' 라는 개념을 도입하여 두 모델을 결합하였으나 이 신뢰도를 어떻게 설정하는지가 여전히 문제로 남아있다. Zhou et al. [11] 은 무선 애드혹 네트워크에서의 임계치 암호화 방법을 이용한 키 관리 방법을 처음으로 제안하였다. 그러나 아이디어의 제시에 그쳤을 뿐, 구체적인 디자인은 보여주지 못했다. Yi et al. [12] 은 이 아이디어를 보다 구체화하여 MOCA를 디자인하였다. MOCA 에서는 비교적 성능이 높고 보안성이 뛰어난 노드가 인증 기능을 나눠 갖는다. 인증 서비스를 필요로 하는 노드는 여러 개의 MOCA 노드에 요청 패킷을 보내야 하므로 이를 효율적으로 전송하는 방법을 제안하였다. Wu et al. [3] 은 비밀 재분배를 이용하여 보안성을 강화시킨 SEKM을 개발하였다. SEKM에서는 비밀 재분배 방법을 이용하여 주기적으로 부분비밀이 업데이트되며, 인증 요청 패킷의 전송을 위해 티켓 방법을 제안하였다. 무선 메쉬 네트워크를 대상으로 설계된 인증 및 키 관리 시스템으로는 현재까지 ARSA (Attack-Resilient Security Architecture) [13]가 유일하다. ARSA에 도입된 중개인이라는 개념은 실제 생활에서 은행과 같은 기능을 한다. 중개인은 MC를 인증하고 ID 기반 암호화 방법을 이용하여 'pass' 라는 인증서를 발급한다. MC가 다른 메쉬 네트워크로 이동할 때 이 pass를 이용하면 인증이 신속하게 완료된다.

(그림 1)은 지금까지 설명한 무선 메쉬 네트워크의 보안 이슈들을 하나의 시나리오로 나타낸 것이다. MC가 무선 메쉬 네트워크에 접속하기 위해서는 우선 인접한 MAP (Mesh Access Point)로부터 인증을 받고 키를 공유해야 한다. MC가 다른 네트워크로 패킷을 전송하는 경우 이 패킷은 MAP에서 MR2를 거쳐 MPP로 전달되는 것이 최적의 경로이다. 그러나 공격자가 MR1과 MR2 사이에 방해 전파를 이용하여 DoS 공격을 일으키면 MAP는 우회 경로를 선택하고 패킷을 MR3로 전달한다. 그러나 이번에는 MR4가 공격자에 의해 조작되어 패킷을 MR5로 전달해 주지 않는다. 그러면 MC는 패



(그림 1) 무선 메쉬 네트워크의 보안 이슈

킷을 MPP까지 보낼 수 없고 결국 이 무선 메쉬 네트워크로부터 아무런 서비스도 받지 못하게 된다.

III. 임계치 암호화 방법

1. Shamir의 비밀 공유 방법

비밀 공유 방법은 Shamir와 Blakley에 의해 처음 제안되었다. (n, m) 비밀 공유 방법에서는 다항식 또는 벡터 공간을 이용하여 비밀에 대한 n개의 부분비밀을 생성하고, 이 중 m개 이상의 부분비밀을 알면 그 비밀을 만들어낼 수 있다. 임계치 암호화 방법은 비밀 공유 방법을 통해 분배된 부분비밀만을 이용해 전자 서명과 같은 암호화 작업을 수행하는 것을 말한다. Shamir의 비밀 공유 방법 [14]에는 비밀 k를 공유하기 위해 다항식 $f(i)=k+a_1i+a_2i^2+\cdots+a_{m-1}i^{m-1}$ 이 사용된다. $f(0) = k$가 되고, 노드 i의 부분 비밀 $s_i = f(i)$ 로 계산된다.

2. Desmedt와 Jajodia의 비밀 재분배 방법

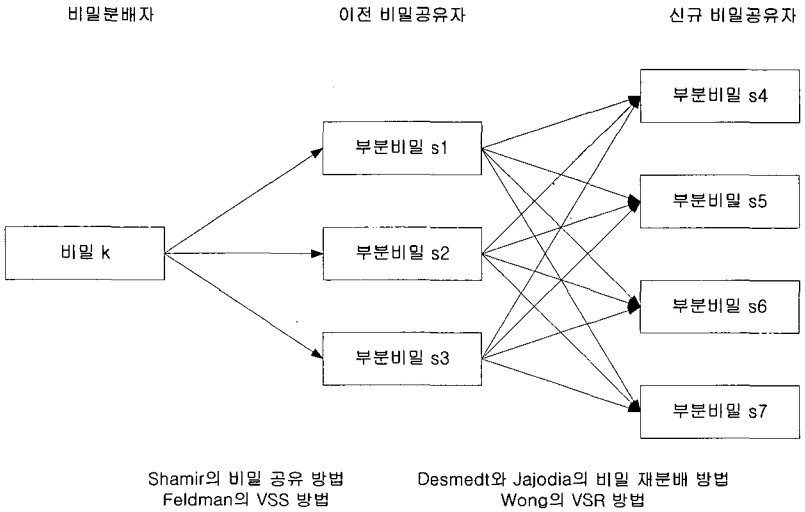
이미 분배된 부분비밀을 업데이트하거나 부분비밀을 소유하는 노드를 변경하고, 임계치를 바꾸기 위해 사용되는 것이 Desmedt와 Jojodia의 비밀 재분배 방법 [15]이다. 이 방법을 사용하여 (n, m) 비밀 공유 방법으로 분배되었던 k가 (n', m') 비밀 공유 형식으로 재분배 가능하며 이때 중간에 k를 재구성할 필요가 없다는 것이 장점이다. 이를 위해 이전 비밀공유자 i는 자신의 부분비밀 s_i에 대해 Shamir의 (n', m') 비밀 공유 방법을 이용하여 준부분비밀 $\hat{s}_{ij}$ 를 만들고 이를 분배한다.

3. Feldman의 Verifiable Secret Sharing (VSS) 방법

Shamir의 비밀 공유 방법을 사용할 때 비밀공유자는 비밀분배자로부터 받은 부분비밀이 유효한지를 확인할 수 없다. 이를 확인할 수 있도록 비밀분배자는 부분비밀에 대한 인증정보를 함께 넘겨준다 [16]. $f(i)=k+a_1i+a_2i^2+\cdots+a_{m-1}i^{m-1}$ 을 이용해 부분비밀을 생성하는 경우 적당한 상수 g를 이용해 인증정보 $g^k, g^{a_1}, \cdots, g^{a_{m-1}}$을 계산해서 비밀공유자 모두에게 브로드캐스팅한다. 비밀공유자는 이 인증정보를 이용해 자신이 받은 부분비밀의 유효성을 확인할 수 있다.

4. Wong의 Verifiable Secret Redistribution (VSR) 방법

이러한 연구를 바탕으로 Wong et al. [17]은 Verifiable Secret Redistribution (VSR) 방법을 제안하였다. VSR 방법은 비밀 재분배의 과정에서 생성된 준부분비밀이 유효한 부분비밀로부터 생성된 것인지를 확인하는 방법이다. Desmedt



(그림 2) 임계치 암호화 방법

와 Jajodia의 비밀 재분배 방법에서는 비밀 재분배 과정에서 이전 비밀공유자 i가 신규 비밀공유자 j에 대해 자신의 부분비밀 s_i의 유효한 준부분비밀 $\hat{s}_{ij}$를 생성했는지를 Feldman의 VSS를 이용하여 확인하고 있다. 그러나 i가 부분비밀 s_i자체를 조작하여 다른 값으로 재분배를 수행했을 때에는 이를 판별해낼 수 없다. VSR 방법은 비밀공유자들이 최초 비밀분배시에 계산했던 g^k를 계속해서 보관하고 신규 비밀공유자에 전달한다. 그리고 비밀 재분배 과정에서 전달되는 g^{s_i} 값을 이용해 이전 비밀공유자 i가 유효하지 않은 s_i를 보냈는지 확인할 수 있다.

(그림 2)에 이러한 임계치 암호화 방법의 요소 기술들이 언제 사용되는지 도시하였다.

IV. MeCA 아키텍처

1. MeCA 개요

N개의 MR이 모여 무선 백본망을 구성하는 무선 메쉬 네트워크가 있다고 하자. 그 N개의 MR 중 $n(n \le N)$개의 노드가 MeCA 노드가 된다. 이 n개의 MeCA 노드에는 CA의 비밀키 k가 Shamir의 비밀 공유 방법으로 분배되어 있다.

이 n개의 MeCA 노드 중 임계치 $m(\left\lfloor \frac{n+1}{2} \right\rfloor \le m \le n)$개 이상이 모이면 비밀키 k를 재구성할 수 있다. 또한 이를 이용해 MeCA 인증서를 갱신, 폐기하거나 상태 조회할 수 있다.

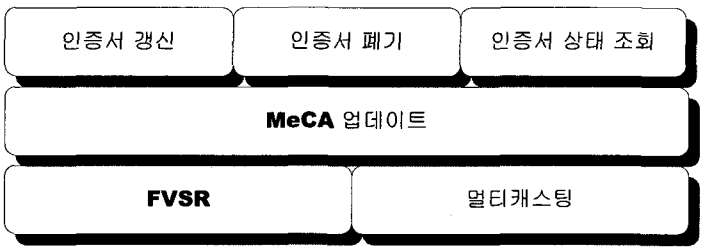
주기적으로 혹은 필요에 의해 이 MeCA 노드들은 자신이 갖고 있는 부분비밀을 갱신하거나 MeCA 기능을 다른 노드에 이전한다. 이렇게 함으로써 부분비밀이 공격자에게 일부 노출되더라도 MeCA 비밀키 k까지 노출되는 일이 없도록 한다. 이러한 MeCA 노드의 업데이트를 안전하고 빠르게 수행하기 위해 VSR을 개량한 FVSR 방법을 사용한다. 보안 위협이 커지는 경우, FVSR 방법은 MeCA 노드 수 n을 늘리거나 임계치 m을 증가시켜 MeCA의 보안 성능을 향상시킬 수 있다.

MeCA의 효율적인 동작을 위해 MeCA 노드들을 수신자로 하는 효율적인 멀티캐스팅 방법이 필요하다. 이는 MeCA 업데이트 시 MeCA 노드 i가 부분비밀 인증정보 혹은 의심 메시지, 인증서 폐기 메시지를 다른 MeCA 노드에 전송할 때와 MAP가 MeCA 노드에 인증서 갱신 또는 상태 요청을 할 때 사용된다. 이를 구현하기 위해 우리는 Ruiz 트리를 이용한다. 각각의 MeCA 노드와 MAP에 대해 Ruiz 트리를 만드는 것이 최적이지만, 이는 트리 생성에 많은 오버헤드를 일으킨다. 따라서 우리는 MeCA 노드들 사이에 하나의 Ruiz 트리를 생성하고 이를 이용해 모든 MeCA 노드들과 MAP들이 멀티캐스팅을 수행하도록 한다.

(그림 3)에 MeCA의 아키텍처를 간단히 도시하였다.

2. FVSR 방법

VSR 방법은 두 가지 문제를 가지고 있다. 첫째, 신규 비밀공유자는 모두 선의의 노드여야 한다는 것이다. 하나라도 악의의 노드가 포함된 경우, 이 노드가 계속해서 abort 메시지를 브로드캐스팅하면 비밀 재분배 과정이 완료되지 못한다. 둘째, 이전 비밀공유자 중에 악의의 노드가 있을 경우 비밀 재분배 과정이 완료될 때까지 기하급수적인 시간이 걸린다는 것이다. 일부 노드가 유효하지 않은 인증정보를 보낸 경우 VSR은 그것이 정확히 어느 노드인지를 구별할 수 없



(그림 3) MeCA 아키텍처

다. 이 경우 VSR은 이전 비밀공유자 중 무작위로 m개씩 선택해 보는 작업을 모두가 유효한 인증정보를 보낼 때까지 계속한다.

이 문제를 해결하기 위해 우리는 VSR을 다음과 같이 수정하였다. 첫째, 유효성 확인을 위해 비밀공유자가 g^k만 저장하던 것을 $g^k, g^{a_1}, \cdots, g^{a_{m-1}}$을 저장하는 것으로 수정하였다. 여기서 $a_1, \cdots, a_{m-1}$은 현재의 부분비밀을 생성하는 다항함수의 계수에 해당하며 $g^{a_1}, \cdots, g^{a_{m-1}}$은 비밀 재분배가 일어날 때마다 갱신된다. 둘째, 비밀 재분배에 참여하는 이전 비밀공유자가 임의의 m개 노드였던 것을 모든 이전 비밀공유자가 참여하는 것으로 바꾸었다.

FVSR에서는 신규 비밀공유자에 악의의 노드가 존재하더라도 그 개수가 m'보다 작으면 비밀 재분배를 성공적으로 완료할 수 있다. 또한 이전 비밀공유자에 악의의 노드가 존재할 때 이 노드가 보낸 유효하지 않은 부분비밀을 배제하기 위해 VSR이 최악의 경우 $\binom{n}{m}-\binom{n-m+1}{m}$회의 반복이 필요했던 데 비해, FVSR은 한번에 유효하지 않은 부분비밀을 걸러낼 수 있다. 더불어 유효하지 않은 부분비밀을 보낸 노드와 잘못된 인증정보를 보낸 노드를 알아낼 수 있다. 이 노드에 대한 정보는 어떤 노드가 악의의 노드인지 파악하는 데 사용될 수 있다.

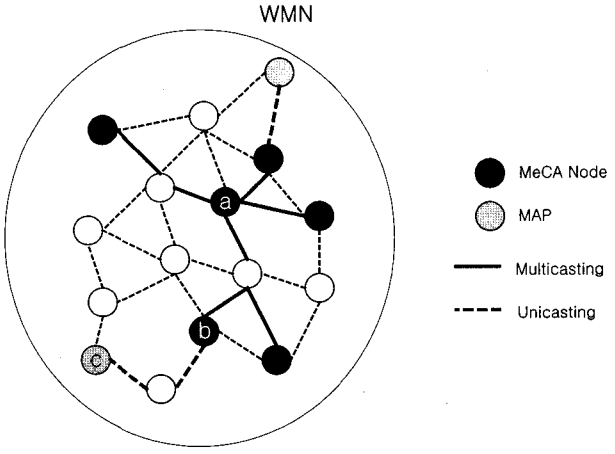
3. 멀티캐스팅

무선 통신의 특성상 어느 한 노드가 이웃 노드에 패킷을 전송하면 이 패킷은 그 노드의 전송 범위 안에 있는 모든 노드에 자동으로 전달된다. 이러한 특성을 이용하면 무선망에서 멀티캐스팅을 수행할 때 전체 전송 횟수를 크게 줄일 수 있다. 이 아이디어를 무선 메쉬 네트워크에 적용한 것이 Ruiz 트리이다.

그러나 Ruiz 트리는 송신자 하나에 대한 최적의 해이므로 여러 MeCA 노드가 멀티캐스트 송신자이면서 동시에 수신자인 MeCA에 그대로 적용할 수는 없다. 각각의 MeCA 노드에 대해 Ruiz 트리를 생성하는 것이 전송 횟수를 최소화하는 측면에서 가장 효과적이나 이 경우 Ruiz 트리 생성에 많은 컨트롤 오버헤드가 발생한다.

따라서 우리는 MeCA 노드들 모두를 연결하는 하나의 멀티캐스트 트리 t^*를 생성하고 모든 MeCA 노드가 멀티캐스트 메시지를 보낼 때 이 트리를 이용하도록 한다. 한편 이전 MeCA 노드 또는 MAP가 송신자가 되고 새로운 MeCA 노드가 수신자가 되는 경우도 있다. 이 경우 역시 t^*를 이용하여 멀티캐스팅을 수행하는 것이 효과적이다.

(그림 4)는 MeCA 노드 a에 대한 Ruiz 트리 t_a^*를 생성하고 이를 모든 MeCA 노드가 멀티캐스팅에 공통으로 사용하는 것을 나타낸다. MAP c는 t_a^* 위의 노드 중 가장 가까운 노드



(그림 4) 멀티캐스트 트리의 생성 및 이용

b에 유니캐스팅한 뒤 t_a^*를 이용해 MeCA 노드로 멀티캐스팅한다. 이와 같은 멀티캐스팅 방법은 각 노드마다 최적의 경로를 설정하는 데 비해 트리 생성 오버헤드를 대폭 감소시킬 수 있다. 물론 이 경로가 전송 횟수 측면에서 최적의 경로는 아니지만 그 차이는 2홉을 넘지 않는다는 것을 증명할 수 있다. 자세한 증명은 지면 관계상 생략하도록 한다.

4. 인증 서비스

노드들은 자신의 인증서가 만료되기 전에 MeCA에 갱신을 요청해야 한다. 인증서 갱신을 위해서는 부분 인증서 방법이 사용된다. 또한 인증서는 만료 시점 이전에 폐기될 수 있다. 이러한 폐기 상태를 확인하기 위해 CRL 방법이 사용된다. CRL을 MeCA 노드가 직접 관리하도록 하여 CRL 전체를 매번 전송할 필요 없이 인증서 하나하나의 폐기 결정 및 상태 조회를 개별적으로 관리할 수 있다.

1) MeCA 업데이트

MeCA에 대한 공격자는 계속해서 MeCA 노드를 공격하여 그 부분비밀을 알아내려고 시도한다. MeCA 노드들은 자신의 부분비밀을 주기적으로 업데이트하거나 MeCA 기능을 다른 노드에 이전하여 이러한 공격에 대처한다. 또한 임계치를 증가시킬 수도 있다. 이러한 작업은 FVSR 방법을 이용해 수행된다. 부분비밀의 업데이트는 비교적 간단하므로 자주 일어난다. 반면에 MeCA 기능의 이전 혹은 임계치의 변화는 새로운 MeCA 노드의 선택 및 멀티캐스트 트리의 생성으로 인해 오버헤드가 높다. 따라서 이는 부분비밀의 업데이트에 비해 드물게 발생한다. MeCA 기능을 이전받을 노드는 공격자에 의해 장악되지 않았을 가능성이 높은 노드로 결정한다.

2) 인증서 갱신

MC는 자신의 인증서가 만료되기 전에 MeCA에 갱신을 요청해야 한다. 인증서 갱신을 위해서는 부분 인증서 (partial certificate) 방법이 사용된다. MC a는 자신의 공개키와 비밀키 쌍 (K_a, k_a)를 생성하여 공개키 K_a를 현재의 비밀키로 서명한 뒤, 이를 자신이 결합 (association)돼 있는 MAP b를 통해 MeCA 노드에 멀티캐스팅한다. MeCA 노드 c는 받은 공개키 K_a와 자신의 부분비밀 s_c를 이용해 부분 인증서 $Cert_c^{K_a} = K_a^{s_c}$를 생성하여 b에 보내게 된다. b는 받은 $Cert_c^{K_a}$를 인증한 뒤, 인증된 부분 인증서들을 결합하여 새로운 인증서 $Cert^{K_a}$를 생성하여 a에 전달해 준다.

3) 인증서 폐기와 상태 조회

인증서의 만료 기간이 지나지 않았더라도 그 인증서를 폐기해야 할 경우가 있다. 해당 인증서를 소유한 소유자가 신분 변화, 인증서 분실 등의 이유로 오프라인으로 폐기를 요청할 수도 있고, MeCA 노드들이 특정 노드의 비정상적인 행동을 감지하고 온라인으로 인증서의 폐기를 결정할 수도 있다. 오프라인으로 폐기가 결정된 경우 네트워크 관리자가 MeCA 노드들에 폐기되는 노드의 ID를 알려주며, 온라인의 경우 MeCA 노드 업데이트 때와 마찬가지 방법으로 MeCA 노드는 의심스러운 노드를 선택하고 이 노드의 인증서 폐기를 결정한다. 어떤 노드 a의 폐기를 결정한 MeCA 노드는 RVK_REQ 메시지에 a의 ID를 넣고 부분 서명을 한 뒤 모든 MeCA 노드들에 멀티캐스팅한다. RVK_REQ 메시지를 받은 MeCA 노드들은 부분 서명을 인증하고 a에 대해 m개 이상의 인증된 RVK_REQ 메시지가 도착하면 a의 인증서를 폐기하고 이를 CRL에 추가한다.

MeCA에서는 CRL을 관리하는 디렉토리가 따로 없으며, MeCA 노드가 CRL을 직접 관리한다. 따라서 CRL 업데이트 시 전체 CRL을 모두 전송할 필요 없이 새로 폐기되는 인증서 정보만 알려주면 된다.

MAP는 결합된 MC의 인증서 상태를 조회하기 위해 STATUS_REQ 메시지에 MC의 ID를 넣어 MeCA 노드에 전송한다. STATUS_REQ 메시지를 받은 MeCA 노드는 ID에 해당하는 인증서의 폐기 상태를 자신의 CRL에서 확인한 뒤 그 결과를 STATUS_REP 메시지에 넣고 부분 서명을 하여 요청한 MAP에 응답한다.

MAP는 m개 이상의 인증된 STATUS_REP 메시지를 받으면 이를 이용해 MC의 인증서 상태를 결정한다.

V. 성능 평가

본 장에서는 모의 실험 결과를 통해 MeCA의 성능을 평가한다. 성능 평가는 보안성과 효율성 측면에서 이루어지며

기존의 무선 애드혹 네트워크에서 제안되었던 SEKM, MOCA와 그 성능을 비교한다. 또한 MeCA에서 FVSR 또는 멀티캐스팅 기능을 제거한 경우와도 비교한다. 결과 분석에 앞서 먼저 모의 실험 환경에 대해 설명하도록 하겠다.

1. 모의 실험 환경

모의 실험은 자체 제작한 이벤트-기반 시뮬레이터로 이루어졌다. 1km×1km의 공간에 100 개의 MR이 무선 메쉬 네트워크를 구성하는 경우를 가정하였다. 모든 MR의 통신 반경은 250m로 동일하게 하였다. MR의 위치는 임의로 결정되며 각각의 모의 실험 결과는 서로 다른 토폴로지 100 개에 대해 실험한 뒤 평균을 구한 것이다.

네트워크 관리자는 복구 주기 T_r마다 주기적으로 MR의 운영체제, 디바이스 드라이버를 업데이트하고, 비밀 번호를 변경하는 등 관리 작업을 수행하여 공격자에 의해 조작된 노드를 1개씩 복구할 수 있다고 가정한다. 이러한 공격으로 인해 공격자가 같은 시간에 m개 이상의 부분비밀을 알게 되면 MeCA의 비밀키가 공격자에 노출되어 MeCA는 CA로서의 기능을 상실하게 된다. MC가 MAP에 결합을 요청할 때, 그 MAP는 항상 MeCA에 그 STA의 인증서 상태를 조회한다고 가정한다. 하나의 MAP에서 인증서 상태 요청이 발생하는 주기를 T_a로 나타낸다. 따로 언급이 없으면 모든 모의 실험에는 〈표 1〉의 파라미터들이 사용된다.

〈표 1〉 모의 실험 파라미터

Parameter	Value
number of MeCA nodes n	30
threshold m	15
number of MAPs	5
secret share update interval T_u	3 days
MeCA function transfer interval T_t	15 days
exposure attack success interval T_e	1 day
compromise attack success interval T_c	5 days
recovery interval T_r	5 days
sassociation request interval T_a	30 minutes

2. 모의 실험 결과

(그림 5.(a))는 분산 인증 기관의 노드 개수 n을 10개에서 50개까지 변화시켜 가면서 비밀키 노출 시간을 도시한 것이다. 모의 실험 기간은 1000일이므로 결과값이 1000일이면 모의 실험 동안에 비밀키가 노출되지 않았음을 의미한다. 4가지 방법 모두 n이 클수록 노출 시간이 커지는 경향을 보여준다. 공격자가 알아내야 할 부분비밀의 개수가 더 많아지기 때문이다.

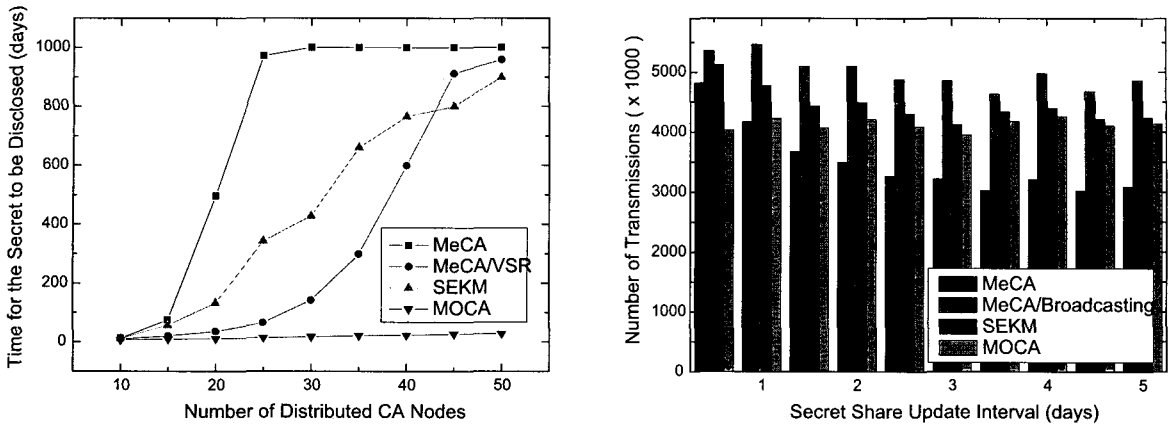
MeCA에서는 n이 30 이상이면 비밀키가 노출되지 않았다. n이 30보다 작을 때에는 공격자의 공격이 순간적으로 집중되는 경우에 노출된 부분비밀의 개수가 임계치를 넘어설 수 있는 것이다. MeCA/VSR은 MeCA에서 FVSR 대신 VSR 방법을 사용한 경우이다. 이 경우 n이 증가함에 따라 비밀키 노출에 걸리는 시간이 커지긴 하지만 n이 50이 되어도 비밀키가 결국 노출된다. 따라서 FVSR이 보안성을 강화하는 데 중요한 역할을 함을 알 수 있다. SEKM과 MOCA 역시 1000일 이내에 비밀키가 노출되었다.

(그림 5.(b))에 부분비밀 업데이트 주기 T_u를 0.5일에서 5일로 바꿔 가며 100일 동안의 전체 오버헤드를 도시해 보았다. 효율성 측정을 위한 실험에서는 공격자의 공격이 전혀 없다고 가정한다. 실험 결과 T_u= 0.5일일 때만 MOCA의 오버헤드가 가장 작았고, T_u= 1일부터는 MeCA의 오버헤드가 가장 낮았다. MeCA는 부분비밀 업데이트와 MeCA 기능 이전, Ruiz 트리 생성으로 컨트롤 오버헤드가 높지만, 인증서 상태 요청시 멀티캐스팅을 이용하므로 데이터 오버헤드를 대폭 감소시켜 전체적인 오버헤드도 가장 낮았다. 반면 MOCA는 컨트롤 오버헤드는 없지만 인증서 상태 요청을 유니캐스팅으로 하기 때문에 데이터 오버헤드가 높다.

MeCA/Broadcasting은 MeCA에서 멀티캐스팅을 제거하고 MeCA와 MAP이 멀티캐스팅하던 것을 각각 브로드캐스팅과 유니캐스팅으로 바꾼 것이다. MeCA/Broadcasting은 모든 경우에 오버헤드가 가장 높아, MeCA에서 멀티캐스팅이 오버헤드를 얼마나 많이 감소시켜 주는지 잘 나타내 준다. SEKM은 MeCA와 같은 CA 기능 이전 과정이 없으므로 MeCA/Broadcasting에 비해 오버헤드가 약간 감소한다.

VI. 결 론

본 고에서 우리는 무선 메쉬 네트워크의 보안 이슈를 노드의 오동작, 라우팅, 그리고 인증으로 나누어 살펴 보았다. 그리고 인증 문제를 해결하기 위한 방법으로 무선 메쉬 네트워크를 위한 최초의 분산 인증 기관인 MeCA를 제안하였다.



(그림 5) (a) 분산 인증 기관의 노드 개수 에 따른 부분 비밀 노출 시간, (b) 부분비밀 업데이트 주기에 따른 전송 횟수

MeCA의 FVSR과 멀티캐스팅은 무선 메쉬 네트워크의 MR들이 전력에 제한이 없어 모두 CA 기능을 분담할 수 있는 능력이 되며, 비교적 고정적이어서 멀티캐스팅의 효과가 크다는 점을 이용한 것이다. 모의 실험 결과 MeCA는 기존의 무선 애드혹 네트워크에서 제안된 분산 인증 기관에 비해 효율성은 떨어뜨리지 않으면서 보안성은 대폭 강화함을 확인할 수 있었다.

[1] I. F. Akyildiz, X. Wang, and W. Wang, "Wireless mesh networks: a survey," Computer Networks, 47(4):445-487, 2005.

[2] S. Yi and R. Kravets, "MOCA: mobile certificate authority for wireless ad hoc networks," The 2nd Annual PKI Research Workshop (PKI' 03).

[3] B. Wu, J. Wu, E. Fernandez, and S. Magliveras, "Secure and efficient key management in mobile ad hoc wireless networks," Proceedings of the 19th IEEE international parallel and distributed symposium (IPDPS 2005). The first international workshop on security in systems and networks (SSN 2005), p.288, 2005.

[4] P. M. Ruiz and A. F. Gomez-Skarmeta, "Heuristic algorithms for minimum bandwidth consumption multicast routing in wireless mesh networks," Proceedings of ADHOC-NOW, pp. 258-270, 2005.

[5] N. Ben Salem and J.-P. Hubaux, "Securing Wireless Mesh Networks," IEEE Wireless Communications, 13(2):50-55, Apr. 2006.

[6] A. Seshadri, A. Perrig, L. van Doorn, and P. Khosla, "SWATT: SoftWare-based Attestation for Embedded Devices", Proceedings of IEEE Symposim on Security and Privacy, 2004.

[7] A. Haq, A. Naveed, and S. S. Kanhere, "Securing Channel Assignment in Multi-Radio Multi-Channel Wireless Mesh Networks," UNSW-CSE-TR-0622, 2006.

[8] Y.-Ch. Hu and A.Perrig, "A Survey of Secure Wireless Ad Hoc Routing," IEEE Security and Privacy, special issue on Making Wireless Work, vol 2, no. 3, 2004.

[9] W. Xu, W. Trappe, Y.Zhang, and T. Wood, "The Feasibility of Launching and Detecting Jamming Attacks in Wireless. Networks," Proceedings of MobiHoc, 2005.

[10] S. Capkun, L. Buttyan, and J.-P. Hubaux, "Self-organized public-key management for mobile ad hoc networks,". IEEE Transactions on Mobile Computing, 2(1), 2003.

[11] L. Zhou and Z. Haas, "Securing ad hoc networks," IEEE Network Magazine, 13(6):24?30, 1999.

[12] S. Yi and R. Kravets, "Composite Key Management for Ad Hoc Networks," Proceedings of MobiQuitous, 2004.

[13] Y. Zhang and Y. Fang, "ARSA: An Attack-Resilient Security Architecture for Multihop Wireless Mesh Networks," IEEE Journal on Selected Areas in Communications, vol. 24, no. 10, 2006.

[14] A. Shamir, "How to share a secret," Communications of the ACM, 22(11):612-613, Nov. 1979.

[15] Y. Desmedt and S. Jajodia, "Redistributing secret shares to new access structures and its applications," Technical Report ISSE TR-97-01, George Mason University, 1997.

[16] P. Feldman, "A practical scheme for non-interactive verifiable secret sharing," Proceedings of the 28th IEEE Annual Symposium on Foundations of Computer Science, pp. 427-437, Oct. 1987.

[17] T. M. Wong, C. Wang, and J. M. Wing, "Verifiable secret redistribution for archive systems," Proceedings of the First International IEEE Security in Storage Workshop (SISW 2002), Greenbelt, MD, Nov. 2002.

약 력

김 종 택

2002년 서울대학교 전기 · 컴퓨터공학부 학사
2002년 ~ 현재 서울대학교 전기 · 컴퓨터공학부 석박사 통합과정
관심분야 : 네트워크 보안, 암호학

박 세 웅

1984년 서울대학교 전기공학과 학사
1986년 서울대학교 전기공학과 석사
1991년 University of Pennsylvania 박사
1991년 ~ 1994년 AT&T Bell Lab.
1994년 ~ 현재 서울대학교 전기 · 컴퓨터공학부 교수
관심분야 : 차세대 무선 네트워크, 네트워크 보안