韓國SI學會誌
第3卷 第2號
2004年 11月

이동 Ad Hoc 네트워킹에서 Threshold Cryptography를 적용한 클러스터 기반의 인증서 생성 및 관리 모델연구

박배효* · 이재일* · 한진백** · 양대헌***

Research on the Issuing and Management Model of Certificates based on Clustering Using Threshold Cryptography in Mobile Ad Hoc Networking

Bae Hyo Park* · Jae-il Lee* · Gene Beck Hahn** · Dae Hun Nyang***

■ Abstract ■

A mobile ad hoc network(MANET) is a network where a set of mobile devices communicate among themselves using wireless transmission without the support of a fixed network infrastructure. The use of wireless links makes MANET susceptible to attack. Eavesdroppers can access secret information, violating network confidentiality, and compromised nodes can launch attack from within a network. Therefore, the security for MANET depends on using the cryptographic key, which can make the network reliable. In addition, because MANET has a lot of mobile devices, the authentication scheme utilizing only the symmetric key cryptography can not support a wide range of device authentication. Thereby, PKI based device authentication technique in the Ad Hoc network is essential and the paper will utilize the concept of PKI. Especially, this paper is focused on the key management technique of PKI technologies that can offer the advantage of the key distribution, authentication, and non-reputation, and the issuing and managing technique of certificates based on clustering using Threshold Cryptography for secure communication in MANET.

Keyword : MANET, PKI, Threshold Cryptography, Certificate, Authentication, Clustering

* 한국정보보호진흥원(KISA) 전자거래보호단
** 연세대학교 컴퓨터과학과
*** 인하대학교 정보통신대학원

1. 서 론

정보통신 기술의 발달은 무선 네트워킹 기능을 수행하기 위한 네트워크 센서나 소형 디바이스의 성능향상을 가능하게 하였고, 무선망을 통한 네트워크에 접속하여 다양한 디바이스를 통해 원하는 서비스를 받을 수 있게 되었다. 현재까지 디바이스를 통한 혹은 디바이스 상호간의 통신을 위한 다양한 통신 프로토콜이 정의되어 있지만, 인증이나 보안기능에 대해서는 충분하게 고려하지 않고 있다. 특히, 중앙 집중적인 기반 없이 스스로 조직되는 무선 네트워크인 이동 Ad Hoc network(이하 MANET)에서는 노드들의 잦은 이동성으로 인해 토폴로지 변화가 매우 극심한데, 이러한 환경에서는 각 노드들 상호간에 안전성 및 신뢰성를 효율적으로 유지하기 위하여 보안에 필수적인 요구사항들이 존재한다.

한편, PKI는 키 분배의 용이성과 인증, 무결성 및 부인봉쇄의 기능을 제공할 수 있으며, PKI가 구축된 상황에서 인증서의 생성 및 분배를 통하여 임의의 노드들 상호간의 인증을 가능하게 한다. 하지만, 이러한 장점에도 불구하고, MANET과 같이 고정된 기반구조에 의존하지 않고, 분산된 구조로 동작하는 환경에서는 하나의 신뢰받는 CA의 존재가 개념적으로 불가능하고, 만약 존재한다고 하더라도, 그 CA가 망 전체의 유일한 취약점이 될 수 있고, PKI 연산 자체가 많은 컴퓨팅 파워를 요구하기 때문에, MANET에서 기존의 고정된 PKI 기반 인증기술은 많은 주목을 받지 못했다. 그러나, 유비쿼터스 환경에서 센서 네트워크 발전과 무선 네트워크 디바이스의 확산으로 복잡해진 네트워크를 통해 중앙 집중적 관리가 불가능하고, 언제 어디에서나 접속 가능한 개방성으로 인해 기존의 대칭키만으로는 디바이스의 인증을 수용할 수 없게 됨에 따라 현 시점에서 PKI 기반의 키 관리 기술 연구는 반드시 필요하다고 할 수 있다[1].

이에 따라, 본 논문에서는 MANET에서의 필수 보안 요구사항과 연구분야를 살펴보고, PKI 기반의 키 관리 기술연구 및 인증서 생성 방안, 인증서 관리를 위한 기본 모델을 제공하고자 한다.

2. MANET의 개요 및 보안 요구사항

MANET은 1970년대 초 Mobile Packet Radio라 불리는 무선기반의 네트워크 기술이 제안된 이후로 무선 네트워크의 다양한 연구 분야 중의 하나로 발전하고 있는 기술이다. 기존의 인프라(기지국, Access Point)가 존재하지 않는 곳에서 디바이스 상호간의 라우팅으로 데이터의 송·수신 등의 통신기능을 수행하고, 디바이스 자신들이 라우터, 서버의 역할 등 다중적인 기능을 담당한다. 즉, MANET은 인프라가 필요하지 않는 특성으로 인하여 임시적으로 구성되는 네트워크나 지진, 태풍, 테러에 의한 재해/재난지역과 전쟁터와 같은 환경에서 적용 가능하도록 연구되었으며, 특히 전쟁에서 실전사용을 위한 군사용 망을 중심으로 기술 개발이 이루어졌다. 그러나 최근에는 인터넷의 급속한 성장을 배경으로 MANET은 초기의 원거리망에서 근거리 지역망, 일반 대중의 가정 내 개인용 디바이스간 통신망 등 상업적으로 주목받기 시작하였다[2]. MANET의 주요특징은 크게 네가지로 나눌 수 있는데, 첫째 개별 노드들의 이동성으로 각기 컴퓨팅 기능을 가진 호스트이자 라우팅 기능을 가진 라우터로써 동작한다. 둘째, 동적인 네트워크 토폴로지를 가지고 있어서 경로 설정 및 유지가 힘들고, 기존의 라우팅 프로토콜을 적용하기 힘들다. 셋째, MANET은 분산운영 기능을 가지고 고정된 백본 네트워크에 의존하지 않고, 보안 및 라우팅 기능을 스스로 지원해야 한다. 이에 따라 여러 노드간의 협력에 의해 기능들이 분산되어 운영된다. 마지막으로, MANET은 무선 네트워크 사용으로 전송거리와 전송 대역폭에 제약을 받고, 전파간섭 및 다중링크 등 무선환경에서 발생되는 보안문제를 안고 있다[3].

이와 같은 주요 특징으로 인하여, MANET의 보안은 고정 네트워크와는 전혀 다른 양상을 보인다. MANET의 보안 요구사항은 여러 가지가 존재하지만, 대체로 다섯 가지 정도로 요약할 수 있다. 첫 번째로, 가용성(Availability) 측면인데, 이는 공격자에 의한 DOS 공격에도 불구하고, 네트워크 서비스의 생존성이 보장되어야 한다는 것을 의미한다. 두 번째는 어떤 정보도 인증되지 않은 노드들에게 노출되지 않는 것을 보장하는 것으로 '신뢰성(Confidentiality)'이 중요한 보안 요구사항이라고 할 수 있다. 이는 특히 군사적인 부분에서 많이 요구된다. 세 번째는 전송된 메시지가 훼손되지 않았음을 보장하는 무결성(Integrity)이며, 네 번째는 인증(Authentication)으로서, 이는 노드로 하여금 통신에 관여하고 있는 상대노드의 신원을 확신하게 하는 것을 의미한다. 마지막으로, 부인방지(Non-Repudiation)가 요구되는데, 이는 메시지를 보낸 곳에서 메시지를 보낸 사실을 부정하지 못하도록 하는 것이다[4]. 특히, 통신에 필요한 라우팅을 수행할 경우, 악의적인 중간노드에 의해 데이터의 무결성 및 기밀성 문제가 발생할 수 있기 때문에 상대노드와의 신뢰관계 형성 및 암호화 기법을 고려해야만 한다. 또한, MANET 환경은 모든 노드들이 분산되어 있고, 어떠한 고정된 기반구조도 없으며, 모든 노드가 공평하게 역할을 나눠 갖는다는 특징을 갖고 있으므로, 이에 합당한 인증 프로토콜이 필요하다. 한편, 보안문제가 확실히 해결되다 보면, 컴퓨팅 문제가 발생되어, 노드와 네트워크 전체에 심각한 부하를 주게 되므로, 이러한 장단점(Trade-off)을 고려한 MANET에 적합하게 구현된 알고리즘, 키 분배 및 인증 프로토콜의 개발이 현실적으로 가장 필요하다. 즉, 키 사이에 신뢰할 수 있는 관계를 형성하고, 이를 MANET 전반에 분배하는 것이 주요과제가 된다. 이러한 보안요구 사항을 만족하기 위하여 기밀성, 무결성 및 부인방지를 효율적으로 제공하는 PKI 구조를 기반으로 한 키 관리에 대하여 기술하고자 한다.

3. MANET에서의 키 관리 기술

MANET과 같이 인증기관이나 특정 서버(Central Entities)도 없는 분산된 구조를 지닌 환경에서는 다양한 공격이 가능하기 때문에 보다 높은 생존성을 보장하기 위하여 키 관리 및 인증모델로서 공개키 기반 구조의 보안 메카니즘에 대한 연구가 관심을 끌고 있다. 본 고에서는 PKI 구조를 기반으로 한 키 관리에 대하여 기술한다[5].

3.1 키 전달과 키 협상

MANET에 있어서 가장 핵심적이고 복잡한 문제는 '키 설정(Key Establishment)' 이며, 이는 키 전달(Key Transport)과 키 협상(Key Agreement)에서 분명히 보여진다. 먼저, 키 전달이란 노드가 자신이 직접 비밀키 값을 만들거나 아니면 다른 곳에서 가져와서 안전하게 전송을 해야하는 부분이며, 키 협상이란 분배된 키는 어떤 부분도 결과값을 미리 결정할 수 없게 하는 방법으로, 둘 혹은 그 이상의 제공된 정보기능으로부터 획득되게 하는 방법론을 의미한다. 이러한 접근방법은 대개 대칭키, 공개키 기술에 기초한다. 특히, 공개키 기술에서 인증기관의 존재유무는 MANET과 기타 네트워크를 구분하는 중요한 잣대로 설정된다.

3.2 인증기관의 존재

MANET에 적절한지 아닌 지의 여부는 몇 가지 특징들이 제대로 구현되어있는지 아닌 지의 여부에 달려있는데, 이는 대개 다음과 같이 구분해 볼 수 있다. 먼저 관리자(Authority)의 존재여부로써, 관리자가 존재한다면, 그곳에 몇 개의 관리자 영역(Domain)이 존재하는지도 생각해야 할 문제이며, 만일 관리자가 있다면, 초기단계에서 관리자들의 역할이 무엇인지도 중요하게 검토되어야 할 부분이다. 또한, 여러 개의 관리자 영역이 존재한다면, 그들간의 신뢰수준은 어느 정도이고, 어떠한 방법으로 그들간의 신뢰관계를 형성할 것인가도 중요

한 고려대상이다. 신뢰관계가 존재하는 경우에는 과연 그것이 온라인 상에서 접근이 가능한지도 중요하며, 여러 사용자들 중에서 상위영역의 존재여부도 보안구현을 위해서 고려해야 할 부분이다.

한편, 키 운용에 있어서 공개적으로 알려지고 이용 가능한 신뢰관계의 존재여부와 키의 주기, 즉 키의 생성, 교환은 물론 폐지시한이 고려되었는지 아닌 지의 여부도 검토되어야 할 중요한 보안관련 특징들이다. 앞서 언급한 키 방식 중 온라인 신뢰서버(On-Line Trusted Server)는 필요하지 않으므로, 어떤 신뢰기관이나 고정된 서버가 없는 경우, 대개 비대칭 암호가 적절한 개념이라고 볼 수 있다. 즉, MANET에서 유일한 인증기관(Single CA : Certificate Authority)을 사용하는 것은 키 관리 서비스를 제공하는데 있어서 문제가 된다. 왜냐하면, 네트워크의 전체 보안에 대해 책임이 있는 인증기관은 네트워크의 가장 큰 취약점이 될 수 있기 때문이다. 만일 CA를 사용할 수 없다면, 노드들은 다른 노드들의 현재 공개키를 획득할 수 없게 되어, 다른 노드들과 안전하게 통신할 수 없게 된다. 또한, 만일 CA가 적에게 공격당하여, 공격자에게 개인키가 노출되면, 공격자는 노출된 개인키를 가지고 어떤 노드를 가장하거나, 어떤 인증서를 폐지하기 위해 인증서에 잘못된 서명을 할 수 있게 되는 위험을 가져올 수 있다. 이를 위해 현재 MANET에서 중앙 집중화된 인증기관을 제거하려는 연구가 진행중이며 이는 완전히 분산된 방안으로 노드들이 적절한 상황을 설정하여 서로를 인증하게 하는 것으로, 각 노드들 상호간에 서로를 인증하고 신뢰하는 방법이다.

4. Threshold Cryptography

보안시스템에 공개키 암호체계를 운용함에 있어서, 가장 중요한 문제는 각 사용자의 공개키를 다른 사람에게 믿을 수 있다는 것을 보장하기 위한 공개키를 만드는 것이다. MANET에서 이러한 문제는 집중화된 서비스와 가능한 네트워크 분할이 없기 때문에 해결하기 곤란한 문제가 된다. 이를 위해, 현재 공개키 측면에서 연구된 중요한 이론으로는 Threshold Cryptography가 있고, 이를 보다 안전하게 하기 위해 Share Refreshing을 사용하고 있으며, 라우팅 정보와 데이터 트래픽을 보호하기 위해서 전자서명과 같은 암호구조를 고려한다. 대개 그러한 구조를 사용할 경우, '키 관리 서비스'를 요구하게 되는데, 키 분배, 무결성과 부인방지를 위해 PKI가 탁월하므로, 이와 관련된 연구들이 진행되고 있다.

4.1 Threshold Cryptography

MANET에서는 노드의 신분이 서로에게 불확실하며, 악의적인 중간노드에 의해 라우팅에 보안 문제가 발생할 수 있다. 이를 막기 위한 방법으로써, 올바른 노드들이 충분히 존재하기만 하면, 라우팅 프로토콜은 훼손된 노드들 주변을 우회할 수 있는 경로를 찾을 수 있을 것이다. 이를 위해, Threshold Cryptography라는 개념이 제안되었다. Shamir가 비밀공유 기법[6]을 제안한 후, Threshold Crypto-system이 발전하였다. Threshold Crypto-system은 공개키와 비밀키 쌍을 이용하는데, 공개키(K)는 한 개만 존재하는 반면에 비밀키(k)는 n개의 노드로 이루어진 그룹에 의해 비밀정보가 일부분씩 공유된다. 임계값 t이하의 노드는 비밀키를 얻을 수 없으므로, 원문을 복구해 내지 못하고, t+1 이상의 노드가 모여야만 비밀키를 얻어낼 수 있다[4]. 이 시스템에서는 송신자가 메시지를 수신자에게 전송하고자 하는 경우, n개 그룹의 공개키를 가지고 원문을 암호화하여 전송한다. 수신자는 각자가 가지고 있는 비밀정보를 믿을 수 있는 노드(Trusted Party)에게 안전한 채널을 통해 전송한다. 신뢰된 노드는 t+1 이상의 비밀정보를 모아서 비밀키를 만들어낸 후, 원문을 구하여 각각의 수신자에게 데이터를 전송한다.

4.2 Share Refreshing(비밀키 갱신)[4]

'Share Refreshing'을 통하여 이동하는 공격자에 대해 쉽게 대응하고, 네트워크 구성의 변화에 적

절히 적응할 수 있다. 이동하는 공격자들(Mobile adversaries)이란 일시적으로 한 서버를 공격하고, 바로 이어서 또 다른 희생자를 찾아 이동하는 특징을 가진 노드로써, 네트워크 내의 바이러스 같은 대상을 의미한다. 이러한 이동하는 적은 긴 시간동안 모든 서버를 대상으로 공격할 수도 있는데, 만약 공격당한 서버가 이 공격자들을 탐지하고, 그 노드를 배제하더라도, 그 공격자는 다른 시간들 동안 개인키 획득을 위해 t보다 많은 수의 서버를 공격할 것이다. 이러한 과정을 통해 공격자는 개인키를 획득하여 유효한 인증서를 만들 수 있는데, 이를 방지하기 위한 방법이 'Share Refreshing'이다. 'Share Refreshing'은 서버들로 하여금 이전의 Share들로부터 새로운 Share들을 계산해 낼 수 있게 하는 것으로, 새로운 Share는 개인키의 새로운 't+1' Share를 구성한다. share들을 갱신(Refreshing)한 다음, 서버는 이전 Share들을 지우고 새로운 Share를 사용하여 부분서명(Partial Signature)들을 만든다. 새로운 Share들이 이전 것과는 독립적이기 때문에, 공격자는 개인키를 얻기 위해 새로운 Shares들과 이전 Share들을 조합하려고 할 것이고, 이런 식으로 공격자는 정기적인 Refreshing 사이에서 't+1' 서버들을 공격하려고 시도할 것이다. 하지만 이러한 과정을 통해 비밀키를 생성하는 것은 거의 불가능하다. 참고로, Share Refreshing은 이체동형(Homomorphic Property) 특징에 의존한다.

4.3 RSA Threshold Cryptography[7]

RSA Threshold Cryptography를 통하여 하나의 그룹 내에 개별적으로 존재하는 노드들이 Secret Share을 공유하는 방법을 살펴보면, Secret Share 공유는 비밀 다항식(Secret Polynomial) $f(x)$에 의해 이루어진다. 즉, 비밀 다항식 $f(x)$의 차수가 K-1인 경우, 한 집단 내 K개의 노드들이 Lagrange Interpolation을 통해 완전한 비밀(Secret)이 복구될 수 있다. 반면, 해당 집단 내의 노드들의 수가 K이하인 경우, 완전한 비밀(Secret)에 대한 정보는 얻을 수 없다. 이것이 K-Threshold Secret Sharing이다. 집단이 형성되면, 그 집단은 RSA 비밀키 SK = <d, n>을 얻고, 임의로 차수가 K-1인 다항식 $f(x)$를 선택한다. $f(x)$는 다음과 같이 표현될 수 있다.

$$f(x) = d + f_1 * x + f_2 * x^2 + \ldots + f_{k-1} * x^{k-1} \quad (1)$$

여기서, Shared Secret $f(0)$ = d 이다. 구체적으로, 집단 C에 존재하는 노드 i는 Secret Share P_{C_i} =($f(C_i) \bmod n$)을 소유하고, 동일한 집단 C내에 존재하는 K개 노드들의 협력에 의해 Lagrange Interpolation은 다음의 식 (1)을 만족시킨다.

$$d \equiv \sum_{i=1}^{K} (P_{C_i} * l_{C_i}(0) \bmod n) \equiv \sum_{i=1}^{K} SK_i \pmod n \quad (2)$$

여기서, $l_{C_i}(0)$는 Lagrange 계수를 의미하며, K개 이상의 노드들이 집단에서 자신들의 Secret Share를 사용하여 SK_i를 생성할 수 있다. Lagrange Interpolation에 의해, SK는 전술한 다항식 d로부터 복구될 수 있다. 즉, (1)에서, Lagrange Interpolation의 합은 다음과 같이 표현될 수 있다.

$$d \equiv \sum_{i=1}^{K} (P_{C_i} * \ l_{C_i} \bmod n) = t * n + d \quad (3)$$

그러나, 어떠한 수학적인 증명도 다음의 식 (4)를 보장하지 않는다[7].

$$M^{t*n+d} \equiv M^{t*n} * M^d \neq 1 * M^d \equiv M^d \pmod n \quad (4)$$

(3)에서 각 $(P_{C_i} * l_{C_i} \bmod n)$은 모듈러 연산(Modular

Arithmetic)에 따라 0과 n-1 사이의 값을 가지므로, t는 $0 \leq t \leq K$를 만족시킨다. 그러므로, K-Bounded Coalition Offsetting 알고리즘을 사용함에 의해 원래의 메시지 M을 사용하여 M^d를 복구할 수 있으며, M은 시스템의 공개키 $<e, n>$이다. 여기서 Threshold K는 각 집단 내에 존재하는 복수의 노드들을 의미하며, 반드시 큰 수일 필요는 없다. 이는 K-Bounded Coalition Offsetting 알고리즘이 허용가능한 시간 내에서 종료될 수 있음을 의미한다.

5. Threshold Cryptography를 적용한 클러스터 기반의 인증서 생성 및 관리 모델

MANET은 토폴로지와 구성원이 수시로 변하는 동적인 구성을 가지고 있어서 어떤 노드가 훼손되었을 때, 노드들의 신뢰관계도 변하게 되어 다른 무선 네트워크와는 다르게 노드들이 동적으로 관리 도메인(Administrative Domains)에 가입하고 탈퇴한다. 따라서 빈번한 변화에 즉각적으로 적응할 수 있는 시스템이 필요하므로, 본 논문은 앞 장에서 제시하는 Threshold Cryptography를 적용하고 도메인 기반으로 수많은 노드들을 그룹화하기 위하여 클러스터 기반의 인증서 생성 및 관리 모델[1]을 검토하고 클러스터간의 신뢰관계 구축방안을 제안하고자 한다.

5.1 클러스터 개요

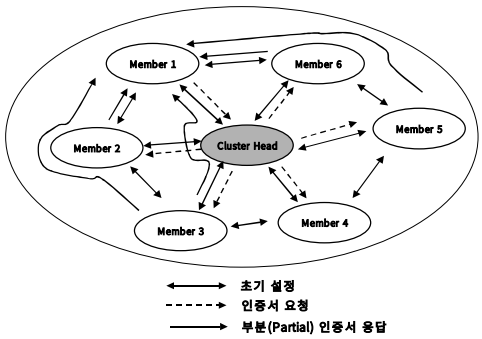
클러스터란 MANET 라우팅 프로토콜 중의 하나인 CBRP(Cluster Based Routing Protocol : 클러스터 기반 라우팅 프로토콜)에서 정의하는 하나의 개념으로, 일련의 노드(node)들이 모인 그룹을 의미한다. CBRP에서는 2 Hop의 지름을 갖는 클러스터의 형태로 네트워크 토폴로지가 형성한다. 한 클러스터 내의 개별 노드는 위조될 수 없는 특정 ID를 가지고 유일하게 식별되며, 다른 클러스터에 속할 수도 있고, 그렇지 않을 수도 있다. 클러스터를 대표하는 클러스터 헤드(Cluster Head)는 클러스터 멤버쉽(Cluster Membership) 정보를 유지하며, 클러스터간 경로는 클러스터 멤버쉽 정보를 참조함에 의해 동적으로 탐색되고 유지된다. 게이트웨이 노드는 클러스터 헤드가 인접 클러스터와 통신하기 위해 반드시 거쳐야 하는 노드이다. 노드들을 클러스터 단위로 구성함에 의해 CBRP는 경로 탐색을 위한 트래픽을 플러딩(Flooding)하는 오버헤드를 감소시킬 수 있는 장점을 가진다.

5.2 인증서 발급 및 관리

5.2.1 인증서 발급

클러스터 기반의 인증서 발급은 초기화 단계를 통한 클러스터 생성이 이루어지고, 클러스터 헤드와 클러스터 멤버간의 관계가 형성된 후에 시작된다. 하나의 노드가 특정 클러스터의 멤버가 되면, Threshold Cryptography를 사용하여 클러스터 내의 k노드들을 통해 인증서를 발급 받는다.

Threshold Cryptography을 통한 인증서의 발급 과정을 기술하면, 먼저, 클러스터의 공개키는 클러스터 내의 모든 멤버노드들에게 알려진다. 클러스터 내의 멤버노드가 새로운 인증서를 요청하면, 클러스터의 개인키가 분할되어 클러스터 내 (k개)노드로 분배된다. 즉, 클러스터의 개인키는 인증서 서명키로써의 역할을 수행하며, 새로운 인증서의 발급은 (k개) 클러스터 멤버들의 협력(Coalition)에



[그림 4] 인증서 발급

의해 이루어진다. 해당 클러스터 멤버들은 Partial 인증서들을 생성하며, 이 값들을 클러스터 헤드를 통해 해당 노드로 전송한다. 인증서 발급을 요청한 노드는 (k개의) Partial 인증서들을 합하여 완전한 인증서를 생성한다.

5.2.2 클러스터간 상호인증(Cross-Certificate)

상호인증이란 서로 다른 두 영역의 PKI를 가진 인증기관이 서로의 신뢰관계를 기반으로 상호연동을 위하여 교차인증을 하는 방법으로, 이 과정을 통하여 개별 클러스터간에는 신뢰관계를 구축할 수 있다. 클러스터에 대한 상호인증 인증서는 해당 인접 클러스터를 탐색할 때 생성되는데, 인접 클러스터의 공개키가 클러스터 헤드에게 전해지면, 클러스터 헤드는 새로운 Cross-Certificate를 생성하기 위하여, 인증서 발급과 동일한 방법으로 클러스터의 개인키가 분할하고 클러스터 내 (k개)노드로 분배된다. 즉, 클러스터의 개인키는 인증서 서명키로써의 역할을 수행하며, 새로운 인증서의 발급은 (k개) 클러스터 멤버들의 협력에 의해 이루어진다. 해당 클러스터 멤버들은 Cross-Certificate을 위한 Partial 인증서들을 생성하며, 이 값들을 클러스터 헤드를 통해 게이트웨이 노드로 전송한다. 이것은 해당 클러스터의 신뢰관계를 확인하기 위하여 인증서 검증시 게이트웨이 노드에 의하여 사용된다.

5.2.3 인접 클러스터의 탐색

인접 클러스터 탐색의 목적은 한 클러스터가 자신과 양방향으로 연결된 모든 인접 클러스터들을 발견하고 이를 신뢰하고자 하는 것이다. 이를 위해 모든 노드는 자신과 인접한 모든 클러스터 헤드들에 대한 정보를 기록한다. 인접 클러스터를 탐색할 때, 기존의 동작 외에 추가되는 부분은 링크/연결 상태 감지 메커니즘과 유사하다. 즉, 인접 클러스터 헤드가 2 Hop 떨어진 경우, 해당 노드에 대한 인증서를 통해 타당성 여부를 판단하고, 3 Hop 떨어진 경우에도, 자신의 멤버노드들로부터 브로드캐스트된 인접 클러스터 헤드가 정상적인지 아닌지의 여부를 상호인증(Cross-Certificate) 목록을 통하여 확인한다.

5.2.4 인증서 분배

클러스터가 형성되면, 클러스터 헤드와 멤버노드 상호간에 인증서가 교환되어야 한다. 이는 클러스터를 구성하는 모든 노드들이 직접 자신의 인증서를 인접노드들로 브로드캐스트함에 의해 이루어진다. 또한, 클러스터 헤드는 인접 클러스터 헤드들과 신뢰관계를 형성하기 위해 서로간에 인증서를 교환한다. 이를 통해 한 클러스터의 노드(Head, Member)는 상호인증(Cross-Certificate)을 통하여 다른 클러스터의 노드 (Head, Member)에 대한 공개키(인증서)를 신뢰할 수 있게 된다. 각 클러스터는 인접 클러스터들로 자신의 공개키를 알릴 수 있는데, 이는 개별적인 클러스터들의 공개키가 인접한 클러스터들로 전달될 수 있음을 의미한다.

인증서를 저장하기 위해 인증서 캐쉬가 요구되며, 클러스터 헤드의 인증서 캐쉬에는 원하는 인증서를 가진 목적지 노드로의 경로상에 존재하는 모든 클러스터 헤드들의 인증서가 저장된다. 즉, 원하는 인증서를 가진 목적지 노드와 그에 대응되는 클러스터 헤드, 소스노드의 클러스터 헤드로부터 목적지 클러스터 헤드 사이에 존재하는 중간 클러스터 헤드들에 대한 인증서가 포함된다. 한편, 인증서를 원하는 소스노드(클러스터 멤버)의 인증서 캐쉬에도 이와 동일한 정보가 저장된다. 다른 (클러스터의) 노드에게 전송된 인증서가 만료된 경우, 인증서에 대응되는 노드는 이를 갱신하여(해당 클러스터 내의 k 개의 노드들로부터 재발급 받아서), 해당 노드가 여전히 자신의 인증서를 필요로 하는 경우, 즉, 인증서 요청을 수신하면, 갱신된 인증서를 전송한다. 이를 수신한 노드는 자신의 인증서 캐쉬를 갱신한다.

5.2.5 인증서 폐지

인증서 폐지는 노드나 클러스터의 인증서가 만료될 때나 타당하지 않은 개인키를 폐지하고 인증서를 재발급할 때에 수행될 수 있다. 인증서 발급과 마찬가지로, 인증서의 폐지는 각 클러스터 내의

노드들의 협력에 의해 이루어질 수 있으며, 이는 복수의 노드들이 협력적으로 특정 노드에 대한 인증서 폐지를 수행함을 의미한다. 구체적으로, 한 노드는 인증서 폐지요청을 같은 클러스터 내의 노드들에게 브로드캐스트하면, 이 요청을 수신한 해당 노드들은 복수의 노드들이 협력적으로 요청노드의 인증서를 폐지하고, 요청노드의 인증서가 폐지되면, 그 결과는 자신의 인접 클러스터들과 이전에 해당 노드와 통신을 수행했던 노드들에게 전달된다. 만료된 인증서는 한 노드의 인증서 캐쉬로부터 자동적으로 삭제된다. 이는 다른 노드들의 인증서들을 저장하고 있는 노드가 해당 인증서들의 유효기간을 알고 있다는 사실에 기인한다. 또한 하나의 클러스터가 없어지거나, 새로운 공개키를 가지는 경우에도, 기존의 Cross-Certificate는 해당 클러스터의 노드들의 협력에 의하여 폐지된다.

6. 결 론

본 논문에서는 디바이스의 이동성과 토폴로지 변화에서 오는 MANET의 보안 요구사항을 만족하기 위하여 PKI 기반의 키 관리 기술과 인증서 생성 및 분배 모델을 검토하였다. 특히, MANET은 고정 네트워크 없이 개별 노드들의 협력에 의해 인증서를 생성 및 폐지하기 위하여 Threshold Cryptography 기법을 활용하였고, 이러한 모델을 통하여 빈번하게 변하는 네트워크 토폴로지나 멤버쉽 상태에서 잘 동작할 수 있으리라 판단된다. 결과적으로, 클러스터 기반의 인증서 생성 및 관리 모델을 통하여, MANET에서 현실 세계와 유사한 도메인 중심의 PKI 기반 구조를 구축하였으며, 이를 통하여 도메인 간, 노드 간의 암호화를 위한 키 관리와 전자서명을 위한 인증기반을 마련하였다.

다만, MANET의 주요 특징 중 하나인 컴퓨팅 파워 한계와 배터리 운용제약이 공개키 연산에 있어서 부담이 될 수 있다. 이러한 문제를 해결하기 위하여, 향후 각 노드들간의 효율적인 라우팅 프로토콜이나 암호화 알고리즘의 연구를 병행할 것이다.

참 고 문 헌

[1] G. Hahn, D. Nyang, J. Song, J. Lee, B. Park, *Securing Cluster Based Routing Protocol Incorporating the Distributed PKI Mechanisms*, Melecon2004, May 2004.

[2] 권혜연, 신재욱, 이병복, 최지혁, 남상우, "Ad Hoc 통신망 프로토콜 개발동향", 「Telecommunication Review」, 제12권, 제3호(May~June, 2002).

[3] 권혜연, 신재욱, 이병복, 최지혁, 남상우, "이동 Ad Hoc 네트워크 기술 동향", 「전자통신동향분석」, 제18권, 제2호(2003).

[4] L. Zhou and Z. Hass, *Securing ad hoc networks*, IEEE Network, 1999.

[5] M.S. Corson and J.P. Macker, *Mobile Ad hoc Networking(MANET) : Routing Protocol Performance Issues and Evaluation Considerations*, IETF RFC 2501, Jan., 1999.

[6] Adi Shamir, "How to share a secret," *Communications of the ACM*, Vol.22(1979), pp.612-613.

[7] J. Kong, P. Zerfos, H. Luo, S. Lu, L. Zhang, "Providing Robust and Ubiquitous Security Supports for Mobile Ad Hoc Networks," *IEEE Proc.* ICNP(2001), pp.251-260.

◈ 저 자 소 개 ◈

박 배 효 (parkbh@kisa.or.kr)

한국과학기술원(KAIST) 전기 및 전자공학과에서 학사, 광주과학기술원(GIST)에서 기전공학 석사학위를 취득하고, 현재 한국정보보호진흥원 암호인증기술팀에 재직중이다. 관심분야는 암호프로토콜, 통합인증기술, RFID/USN 보안기술 등이다.

이 재 일 (jilee@kisa.or.kr)

서울대학교 계산통계학과에서 학사와 석사학위를 취득하고, 1991년 1월부터 1996년 6월까지 한국 IBM에서 근무한 후, 현재 한국정보보호진흥원 전자거래보호단장으로 재직중이다. 관심분야는 정보보호, 유무선 PKI, 유비쿼터스 보안 등이다.

한 진 백 (gbhahn@emerald.yonsei.ac.kr)

고려대학교 전산학과에서 학사, 연세대학교 컴퓨터과학과 대학원에서 석사학위를 취득하고, 현재 연세대학교 컴퓨터 과학과 대학원에서 박사과정에 재학중이다. 관심분야는 이동 Ad-Hoc 네트워크, 무선 통신망, 네트워크 보안 등이다.

양 대 헌 (nyang@inha.ac.kr)

한국과학기술원 전기 및 전자공학과 학사, 연세대학교 컴퓨터과학과에서 석사와 박사학위를 취득하고, 현재 인하대학교 정보통신대학원에서 조교수로 재직 중이다. 관심분야는 암호 알고리즘, 암호 프로토콜, 네트워크 보안 프로토콜, PKI 등이다.