제21회 한국정보처리학회 춘계학술발표대회 논문집 제11권 제1호 (2004. 5)

분산 PKI 메커니즘을 고려한 안전한 클러스터 기반 라우팅 프로토콜에 관한 연구

한진백*, 양대헌**, 김신규***, 서성훈*, 송주석*
*연세대학교 컴퓨터과학과 정보통신 연구실
**인하대학교 정보통신 대학원 정보보호 연구실
***국가보안 기술연구소
e-mail : gbhahn@emerald.yonsei.ac.kr

A Study on Secure Cluster Based Routing Protocol considering Distributed PKI Mechanisms

Gene-Beck Hahn*, Dae-Hun Nyang**, Sin-Kyu Kim***, Sung-Hoon Seo*, Joo-Seok Song*
*Computer & Communication Lab, Dept. of Computer Science, Yonsei University
**Security Research Lab, Graduate School of Information Technology and Telecommunication, Inha Univ.
***National Security Research Institute

요 약

본 연구에서는 MANET(Mobile Ad Hoc Network)에서 분산 PKI(Public Key Infrastructure) 메커니즘을 라우팅 프로토콜에 적용하기 위한 방법을 제안한다. 이를 위해 MANET 이 사용하는 라우팅 프로토콜로 CBRP(Cluster Based Routing Protocol)를 고려한다. 제안하는 프로토콜은 CBRP 의 기능과 분산 PKI 메커니즘을 활용하여 효율적으로 인증서 체인을 찾을 수 있고, 이를 통해 통신노드 상호간의 세션키 설정과 송수신하고자 하는 데이터에 대한 암호화를 지원한다. 또한, 라우팅 프로토콜의 안전한 동작을 위해 제안하는 프로토콜은 전자서명된 HELLO 메시지를 교환하여 악의적인 공격자들에 대해 신뢰성을 제공하고, 안전한 라우팅을 가능하게 한다.

1. 서론

최근 이동 Ad Hoc 망에 대한 연구가 활발하게 진행되고 있다. MANET 에서의 통신은 공유된 무선매체를 통한 이동노드들의 협력에 의존하며, 이러한 관점에서 현재까지의 연구는 주로 라우팅에 초점이 맞추어져 왔고, IETF 에 의해 MANET 을 위한 라우팅 프로토콜들이 제안되었다[1, 3, 4, 5, 7]. MANET 은 라우터나 스위칭 장비 등의 고정된 기반구조를 고려하지 않으며, 이는 MANET 이 중앙화된 보안 솔루션에 의존하지 않는다는 것을 의미한다. 따라서, 많은 보안상의 공격들이 라우팅 프로토콜을 붕괴시키고, 통신을 무력하게 할 수 있다. 이를 막기 위해 각 노드는 악의적인 노드들로부터의 예기치 않은 다양한 공격에 대해 항상 대비해야 한다. 현재 MANET 을 위한 안전한 라우팅 프로토콜들이 제안되어 있으며[2, 8, 9], PKI 를 MANET 에 적용한 방안들이 제시되어 있다[6, 11].

본 연구에서는 CBRP 에 분산 PKI 메커니즘을 적용하기 위한 방법론을 기술한다. 제안하는 프로토콜은 HELLO 메시지를 전자서명하여 해당 노드의 인증서와 함께 인접노드들로 브로드캐스트한다. 한편, 제안하는 프로토콜은 분산된 형태로 키 관리 서비스를 제공하기 위해 Threshold Cryptography 를 사용하며, 성공적으로 분산 PKI 가 형성된 후, 인증서 체인을 탐색하기 위한 방법을 제공한다. 본 논문의 구성은 다음과 같다. 먼저 2 장에서는 CBRP 의 동작과 중요한 특징들에 대해 살펴보고, 3 장에서는 제안하는 프로토콜에 대해 자세히 기술한다. NS-2 기반의 시뮬레이션을 통해 4 장에서는 제안한 프로토콜의 성능을 보인다. 마지막으로, 결론을 제시하고, 향후 연구방향에 대해 언급한다.

2. CBRP 개요

CBRP 는 분산된 방식으로 MANET 노드들을 중복되거나 겹치지 않는 지름이 2 홉인 클러스터들로 분할한다. 각 클러스터마다 하나의 클러스터 헤드가 선택되어 해당 클러스터의 대표로써, 모든 노드들에 대한 클러스터 멤버쉽 정보를 유지한다. CBRP 는 클러스터 구조에 기반을 두고, 클러스터 멤버쉽 정보를 사용하여 통신을 위한 경로를 탐색한다. CBRP 의 중요한 특징은 경로탐색을 위한 플러딩 트래픽을 줄인다는 것과 이 절차를 빠르게 수행한다는 것이다[1].

2.1 데이터베이스 구조

CBRP 는 기본적으로 3 가지 데이터베이스를 포함하며, 이는 인접노드 테이블, 인접 클러스터 테이블, 2 홉 토폴로지 데이터베이스이다. 인접노드 테이블은 링크나 연결감지, 클러스터 생성을 위해 사용되며, 인접 클러스터 테이블은 인접 클러스터 탐색절차에 의해 갱신되는 인접 클러스터들에 대한 정보를 유지한다. 마지막으로, 2 홉 토폴로지 데이터베이스는 자신으로부터 최대 2 홉 떨어진 네트워크 토폴로지에 대한 정보를 유지한다[1].

2.2 클러스터 생성

클러스터 생성의 목적은 어떤 구조를 형성하여 계층적인 Ad Hoc 네트워크를 만들고자 하는 것이다. 이를 위해 변형된 “Lowest ID” 클러스터링 알고리즘이 사용되며, 각 노드는 클러스터 생성을 위해 HELLO 메시지 내의 정보를 사용한다[1].

2.3 인접 클러스터 탐색

인접 클러스터 탐색의 목적은 각 클러스터가 자신과 양방향으로 연결된 모든 인접 클러스터들을 감지하고자 하는 것이다. 이를 위해, 각 노드는 자신의 인접 클러스터 헤드들을 기록하는 CAT 를 유지한다. 인접 클러스터 탐색에는 2 가지 방법이 있는데, 하나는 HELLO 메시지를 사용하는 것이고, 다른 하나는 CAE (Cluster Adjacency Extension)를 사용하는 것이다[1].

2.4 라우팅 고려사항

CBRP 라우팅은 소스 라우팅에 기반을 둔다. 전술한 것처럼, 클러스터 계층구조는 경로탐색시의 플러딩 트래픽을 최소화하기 위해 사용되며, 이는 클러스터 헤드만이 경로탐색을 위한 RREQ(Route Request)를 플러딩함을 의미한다. 패킷을 라우팅하기 위해 소스는 RREQ 를 전송하며, 이를 위한 정보는 소스의 CAT 로부터 얻는다. 목적지는 RREQ 를 수신하면, 소스에게 응답하기 위한 패킷인 RREP(Route Response)를 전송한다. RREP 는 RREQ 로부터 복사된 클러스터 주소들에 대한 리스트를 포함한다[1].

3. 분산 PKI 메커니즘을 고려한 안전한 CBRP

이 장에서는 CBRP 에 분산 PKI 메커니즘을 적용시키기 위한 방법론을 기술한다. MANET 도메인에 하나의 CA(Certificate Authority)를 가정하는 기존의 PKI 공증서비스와 달리 클러스터 기반의 분산 PKI 를 제안하는 이유는 MANET 에 PKI 를 적용할 때, 하나의 CA 만을 고려하는 것은 MANET 고유의 특징들로 인해 많은 문제점을 야기할 수 있기 때문이다[11]. 즉, MANET 에서 인증서비스의 제공을 위해 하나의 CA 에 의존하는 것은 비효율적이고, 안전하지 못하다. 한편, MANET 과 같은 분산된 환경에서 인증서 체인을 찾기 위한 방법론은 노드들에게 PKI 보증서비스를 제공하기 위해 반드시 필요한데, 이는 여러 홉 떨어져 있는 노드와 통신하기 위해서는 통신에 관여된 노드들 상호간에 신뢰관계가 형성되어야 하며, 이를 위해서는 인증서 체인을 찾아야만 하기 때문이다. 이러한 관점에서 MANET 에서 분산 PKI 메커니즘을 형성하고, 인증서 체인을 찾기 위한 방법론을 제시하는 것은 중요하다고 할 수 있다.

3.1 개요

제안하는 프로토콜은 기본적으로 CBRP 의 동작을 계승하며, 분산 PKI 메커니즘을 사용하여 통신노드 상호간에 신뢰관계 형성을 위한 인증서 체인탐색을 지원하도록 수정되었다. 구체적으로, 제안하는 프로토콜은 노드들에게 분산된 형태로 키 관리 서비스를 제공하기 위해 Threshold Cryptography 를 사용한다. 또한, 각 노드가 HELLO 메시지를 전자서명하여 자신의 인증서와 함께 브로드캐스트함에 의해 HELLO 메시지의 안전한 전달을 가능하게 하며, 신뢰할 수 있는 네트워크 토폴로지 정보를 교환하도록 한다. 마지막으로, 제안하는 프로토콜은 통신노드 상호간의 신뢰관계 형성을 위한 인증서 체인탐색 절차를 제공한다. MANET 에서는 노드의 신분이 서로에게 불확실한 경우가 많으므로, 다중 홉 방식에 의해 라우팅을 수행하는 경우, 악의적인 중간노드들에 의해 통신이 붕괴되거나 프로토콜이 정상적으로 동작하지 않을 수 있기 때문에 제안하는 프로토콜은 이에 대한 해결책을 제시할 수 있다. 제안하는 프로토콜에서 각 클러스터에 존재하는 노드는 자신의 고유한 공개키/비밀키 쌍을 보유하며, 자신의 클러스터에 대응되는 공개키와 부분적인 비밀키를 보유한다. 이는 클러스터의 비밀키가 복수의 Secret Share 들로 분할되어 동일 클러스터의 노드들에게 분배된 값이다.

3.2 데이터베이스 구조

CBRP 의 데이터베이스 구조 외에, 제안하는 프로토콜은 2 가지 추가적인 데이터베이스를 필요로 하는데, 이는 인증서 캐쉬와 CRL(Certificate Revocation List) 테이블이다. 먼저, 인증서 캐쉬는 자신과 통신하고자 하는 노드의 인증서를 저장하기 위해 사용되며, 한 노드가 저장하고 있는 다른 노드의 인증서가 만료될 때, 그 인증서는 해당 노드의 인증서 캐쉬로부터 삭제된다. 한편, CRL 테이블은 폐지된 인증서를 가진 노드에 대한 정보를 저장한다. CRL 테이블에 포함된 인증서들은 유효하지 않은 동시에 만료되지 않은 인증서들이며, 이는 한 노드가 유효하지 않고, 만료된 인증서들을 유지할 필요가 없음을 의미한다.

3.3 공개키 교환

제안하는 프로토콜에서는 각 노드의 비밀키로 전자서명된 HELLO 패킷에 해당 노드의 인증서와 현재 클러스터의 공개키가 첨가되어 인접노드들로 전달된다. 이를 통해, 한 노드는 자신의 인증서를 동일 클러스터 내의 노드들에게 알릴 수 있고, 인접 클러스터로 자신의 클러스터의 공개키를 알릴 수 있다. 이는 HELLO 패킷이 하나 이상의 게이트웨이 노드들을 통해 인접 클러스터에 속하는 복수의 노드들로 전송되기 때문에, 한 클러스터는 인접 클러스터의 공개키를 얻을 수 있다는 의미이다. 또한, 이는 한 노드가 주기적으로 브로드캐스트되는 HELLO 메시지를 수신하여, 최대 2 홉 떨어진 네트워크 토폴로지를 알 수 있다는 CBRP 의 특징에 기반을 둔다. 이러한 정보를 사용하여 한 클러스터는 인접 클러스터에 의해 발급된 인증서의 타당성을 확인할 수 있으며, 전자서명된 HELLO 메시지의 전달을 통해, 제안하는 프로토콜은 라우팅 정보를 안전하게 교환하고, 신뢰할 수 있는 인접노드 탐색을 가능하게 하며, 안전한 라우팅을 지원할 수 있다. 이는 MANET 라우팅 프로토콜이 다수의 정상적으로 동작하지 않는 노드들에 의해 영향을 받을 수 있기 때문에 반드시 필요하며, 정상적인 노드가 악의적으로 변경된 HELLO 패킷을 수신하는 경우, 제안하는 프로토콜은 그러한 메시지를 버리도록 함으로써, CBRP 를 패킷누락, 수정, 변경으로부터 성공적으로 보호한다.

3.4 인증서 발급

클러스터가 생성된 후, 클러스터 내의 노드들은 인증서를 요청할 수 있으며, 인증서의 발급은 전술한 것처럼, 동일한 클러스터 내에 존재하는 복수의 노드들의 협력에 의해 이루어진다. 즉, 각 노드는 자신의 고유한 Secret Share 를 사용함에 의해 협력적으로 CA 로써 동작하여 인증서를 생성하고, 이를 요청한 노드에게 제공할 수 있다. 구체적으로, 한 노드가 인증서를 요청하는 경우, 동일 클러스터 내의 노드들이 자신의 Secret Share 를 사용하여 부분 인증서를 생성하고, 이를 요청노드에게 전송하면, 요청노드는 그 결과들을 취합하여 완전한 인증서를 만든다. 이러한 방식으로 PKI 는 클러스터 기반으로 형성될 수 있고, 각 클러스터 내에 존재하는 노드들은 인증서를 요청한 노드에게 인증서를 발급해줄 수 있는 책임을 동일하게 공유하게 된다.. 인증서가 만료되면, 해당 인증서를 보유하고 있는 노드로 인증서가 갱신되어야 하며, 이는 인증서 발급과 유사하다.

3.5 인증서 체인 탐색

제안하는 프로토콜에서 제공되는 인증서 체인탐색은 CBRP 의 경로탐색을 사용하므로, 인증서 체인탐색을 위한 플러딩 트래픽을 줄일 수 있다. CBRP 의 경로탐색과 제안하는 프로토콜의 인증서 체인탐색의 차이점은 후자는 인증서 체인을 찾기 위해 3-Way Handshake 를 필요로 하지만, 전자는 소스경로를 찾기 위해 2-Way Handshake 를 필요로 한다는 것이다. 소스와 목적지 사이의 인증서 체인을 찾기 위해, 소스는 RREQ 를 브로드캐스트하며, 이는 CBRP 와 동일하다. 목적지가 RREQ 를 수신하면, 소스에서 목적지까지의 경로에 대한 정보를 얻게 되며, 이를 사용하여 RREP 를 서명한 후, 이를 자신의 인증서와 함께 RREP 에 추가하고, 소스에게 전송한다. 이 때, 목적지는 자신의 인증서에 대한 검증요청을 RREP 에 명시한다. 이를 위해 RREP 패킷에 몇가지 새로운 필드가 추가되며, 이는 (그림 1)에 나타난다. VQ 필드는 목적지의 인증서 검증요청을 명시하기 위해 추가된 필드이고, VR1 필드는 목적지의 인증서 검증에 대한 결과를, VR2 필드는 목적지를 제외한 중간노드가 수행하는 이전노드의 인증서 검증에 대한 결과를 명시한다.

01	Num1	G	VQ	VR1	VR2	Num2	Identification
Destination Address							
Destination Public Key							
Serial Number of Destination's Certificate							
Cluster Address [1]							
.....							
Cluster Address [Num1]							
Calculated Route [1]							
.....							
Calculated Route [Num2]							

(그림 1) RREP 응답절차

(RREP, 전자서명된 RREP, 목적지의 인증서)가 다음 노드로 전달되면, 해당 노드는 목적지가 포함된 클러스터의 공개키로 목적지의 인증서를 검증하고, 그 결과로 얻은 목적지의 공개키를 통해 서명된 RREP 를 확인한 후, 목적지의 인증서 검증결과를 RREP 에 기록한다. 그 후, 해당노드는 RREP 를 자신의 비밀키로 서명하여, 그 결과를 자신의 인증서와 함께 RREP 에 추가한 후, 인접노드로 전송한다. 이 과정은 RREP 가 소스에 도달할 때까지 계속 반복되며, 구체적인 동작은 (그림 2)에 제시되어 있다.

1. Suppose cluster head C receives RREP, signature for RREP and destination(or previous node)'s certificate. Validate the certificate of destination(or previous node) by using the corresponding public key.
   If cluster head C validates the certificate of destination(or previous node), verifies the RREP by using the public key of destination(or previous node). Record the result in RREP.
   1.1 It decrements Num1 by 1
   Cluster Address [Num1] is the neighboring cluster head that C should forward RREP to in order to reach S
   1.2 C tries to find out a gateway node X to Cluster Address [Num1] such that the Calculated Route [Num2] could reach X directly
   If it succeeds,
   C digitally signs the RREP and send it to X with RREP and (destination's and its) certificates
   Else C increments Num2 by 1 and C records itself in Calculated Route [Num2]
   Else, discard the RREP

2. Suppose member node M receives RREP, signature for RREP and destination(or previous node)'s certificate. Validate the certificate of destination(or previous node) by using the corresponding public key.
   If member node M validates the certificate of destination(or previous node), verifies the RREP by using the public key of destination(or previous node). Records the result in RREP.
   2.1. It increments Num2 by 1 and records itself in Calculated Route [Num2]
   2.2. If Cluster Address [Num1] is its Neighbor
   M digitally signs the RREP and send it to Cluster Address [Num1] with RREP and (destination's and its) certificates
   Else if Cluster Address [Num1] could be reached by X,
   M digitally signs the RREP and send it to X with RREP and (destination's and its) certificates
   Else discard the RREP
   Else, discard the RREP

(그림 2) RREP 응답절차

인증서 체인탐색을 위한 마지막 단계로써, 소스는 자신의 인증서에 대한 검증을 위해 (그림 2)과 유사한 동작을 수행한다. 이 경우, RREP 는 (그림 1)과 동일한 포맷을 가지며, 목적지에 대한 정보 대신에 소스에 대한 정보가 첨가된다.

3.6 인증서 폐지

인증서 폐지는 다음과 같은 경우에 수행된다.

- 인증서가 만료될 때
- 인증서의 재발급이 요청될 때

인증서 발급과 마찬가지로, 인증서 폐지는 각 클러스터 내 노드들의 협력에 의해 이루어지며, 이는 복수의 노드들이 협력적으로 특정 노드에 대한 인증서 폐지를 수행함을 의미한다. 구체적으로, 한 노드가 인증서 폐지요청을 브로드캐스트하면, 이를 수신한 동일 클러스터 내의 노드들은 자신의 CRL 테이블 엔트리를 갱신하고, 협력적으로 요청노드의 인증서를 폐지한다. 인증서가 폐지되면, 그 결과는 자신과 통신을 수행했던 노드들에게 전달되며, 이를 위해 제안하는 프로토콜은 경로캐쉬에 저장된 정보를 사용하고, 추가적으로, 인증서 폐지 메시지라는 제어패킷을 사용한다.

4. 시뮬레이션

본 절에서는 제안하는 프로토콜의 성능분석을 위해 범용 네트워크 시뮬레이터인 NS-2 를 사용하여 수행한 시뮬레이션을 통해 얻은 결과를 기술한다. 성능분석을 위해 고려된 기본적인 모델은 다음과 같다.

- Packet Size : 512 Byte
- Traffic Rate : 4 Packets/sec
- Simulation Period : 180 Seconds(3 Minutes)
- Field Size : 1500m * 300m
- Pause Time : 1 Second

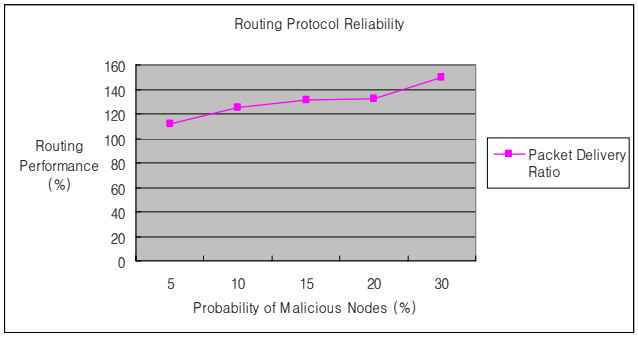
전술한 모델을 기반으로 악의적인 노드가 존재하는 경우, 안전한 라우팅 측면에서의 성능효율을 제시한다. 이를 위해 50 노드, 100 연결, 10m/s 의 이동속도가 고려되며, 악의적인 노드가 라우팅 정보를 변조하여 비정상적인 토폴로지 정보를 네트워크에 유입시킬 때 나타나는 CBRP 와 제안한 프로토콜의 라우팅 측면에서의 효율을 비교한다. 라우팅 측면에서의 효율은 다음과 같이 정의된다.

$$\text{패킷 전송률} = \frac{\text{목적지에 올바로 도착하는 패킷(SE-CBRP)}}{\text{목적지에 올바로 도달하는 패킷(CBRP)}}$$

(그림 3)에 제시된 것처럼, 악의적인 노드의 존재확률이 증가할수록, CBRP 의 성공적인 전송 패킷량과 제안한 프로토콜의 성공적인 전송 패킷량의 비는 증가한다. 이는 제안한 프로토콜에 의해 제공되는 인증서비스로 인해 악의적인 노드들을 효과적으로 방어할 수 있기 때문이다.

5. 결론

본 논문에서는 MANET CBRP 에 보안성을 고려한 새로운 프로토콜을 제안하였다. 제안하는 프로토콜은 분산 PKI 를 구현하기 위해 Threshold Cryptography 를 사용하여 CA 의 역할을 각 클러스터로 분산시켰다. 또한, 제안하는 프로토콜은 분산 PKI 가 형성된 후, 인증서 체인을 탐색하기 위한 절차를 제공하며, 안전한 라우팅을 지원한다. MANET 에서는 노드들이 보안 및 라우팅 기능의 제공을 백본 네트워크에 의존할 수 없다는 문제점을 가지고 있기 때문에, 제안하는 프로토콜은 이러한 문제를 해결하기 위한 한가지 방안으로써 의미가 있다. 향후에는 MANET 고유의 문제점들을 고려하여 MANET 을 위해 제안된 다른 라우팅 프로토콜에 대해서도 제안하는 프로토콜을 적용하고자 한다.



(그림 3) 라우팅 성능효율

참고문헌

[1] Mingliang Jiang, Jinyang Li, Y. C., Cluster Based Routing Protocol(CBRP). Internet Draft, MANET Working Group, Tay, 14, August, 1999.

[2] Panagiotis Papadimitratos, Zygmunt J. Haas, Secure Link State Routing for Mobile Ad Hoc Networks, Jan. 2003.

[3] E. M. Royer, C. –K. Toh, A Review of Current Routing Protocols for Ad Hoc Mobile Wireless Networks, IEEE Personal Communications, page 46-55, Apr. 1999

[4] D. B. Johnson et al. The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks(DSR). Internet Draft, MANET Working Group, Feb. 2002.

[5] C. E. Perkins, E. M. Royer, S. R. Das, Ad Hoc On-Demand Distance Vector(AODV) Routing. IETF Draft, MANET Working Group, Jan. 2002

[6] Srdjan Capkun, Levente Buttyan, Jean Pierre Hubaux, Self Organized Public Key Management for Mobile Ad Hoc Networks, IEEE Transactions of Mobile Computing, Vol. 2, No.1, Jan-March, 2003

[7] C. E. Perkins, Ad Hoc Networking. Addison Wesley Professional, Dec. 2000

[8] L. Zhou, Z. Haas, Securing Ad Hoc Networks, IEEE Network, Vol.13, No.6, pp.24-30, Nov. /Dec. 1999

[9] Aram Khalili, Jonathan Katz, William A. Arbaugh, Toward Secure Key Distribution in Truly Ad-Hoc Networks, IEEE Proceedings of 2003 Symposium on Applications and Internet Workshops.

[10] Dept. of Computer Science, Caneigie Mellon University, Pittsburgh, PA 15213, The CMU Monarch Project's Wireless and Mobility Extensions to ns, The CMU Monarch Project, http://www.monarch.cs.emu.edu.

[11] Jiejun Kong, Petros Zerfos, Haiyun Luo, Songwe Lu, Lixia Zhang, Providing Robust and Ubiquitous Security Supports for Mobile Ad Hoc Networks, IEEE Proc. ICNP, pp.251-260, Nov. 2001