클러스트링 라우팅 환경의 MANET에서 자율적인 공개키 인증 모델에 관한 연구*

조강희*, 정수진**, 한영주**, 정태명*
*성균관대학교 정보통신학부
**성균관대학교 컴퓨터공학
e-mail : {khcho, sjjung, yjhan}@imtl.skku.ac.kr and tmchung@ece.skku.ac.kr

A Study on Self-issued Public Key Authentication Model based on Clustering Routing in MANET*

Kang-Hee Cho*, Soo-Jin Jung**, Young-Ju Han**, Tai-Myoung Chung*
*Dept. of Information Communication, Sungkyunwan University
**Dept. of Computer Engineering, Sungkyunwan University

요 약

MANET 에서 노드들은 스스로 네트워크를 관리 해야하기 때문에 노드간의 협동과 신뢰관계가 필수적이다. 여기서 보안은 MANET 에서의 중요한 이슈중 하나이고 키인증는 보안에 핵심요소 이다. 하지만 동적인 토폴로지, 자원의 제약, 고정된 인프라의 부재는 MANET 에서의 키인증를 어렵게 하는 요인이 된다. 이러한 MANET 에 PKI 를 적용하기 위하여 클러스터 라우팅 기반의 자율분배 키인증 모델을 제안한다. 이 모델은 공개키 링 테이블에 형성된 노드와는 CA 없이 언제든지 신뢰된 통신을 할 수 있어 다른 노드에 적게 의존함으로 해서 DoS 공격과 같은 특정 노드를 무력화 시키는 공격에 효율적으로 동작한다.

1. 서론

Mobile Ad-hoc network(MANET)은 고정된 인프라 없이 자율적으로 구성되는 네트워크로 전쟁과 재난과 같은 임시적인 상황을 고려하여 연구되었으나 최근 유비쿼터스에 대한 관심이 늘면서 Bluetooth 와 홈네트워크와 같이 실생활에 적용할 수 있는 다양한 응용분야로 그 범위가 확대 되고 있다.[1]

MANET 은 고정된 인프라가 없기 때문에 노드들 스스로 네트워크관리를 해야 하는데 원활한 네트워크관리를 위해서는 노드들 사이에 협동과 신뢰관계가 중요하게 된다. 하지만 노드들의 동적인 변화는 서로 신뢰관계를 유지하거나 생성하는 것을 어렵게 하며 다양한 공격에 노출되는 원인이 된다.[2][3] 따라서 키 관리를 통해 보안적 요구사항과 노드간의 신뢰관계를 형성하는 것이 무엇보다 중요하다. 키 관리에는 대칭키 방식과 PKI(Public Key Infrastructure)방식이 있는데 PKI 방식이 크고 복잡한 네트워크에 적용하기에 대칭키 방식보다 용이하고, 유출에 대한 문제가 적다는 장점을 가진다.

하지만 PKI 는 많은 계산능력이 요구되며 계층적인 신뢰센터(CA: Certification Authority)가 있어야 하는 단점을 가지고 있으므로 그것에 대한 해결책 모색이 필요하다. 특히, 고정된 인프라가 없는 MANET 에서의 CA 문제는 많은 논의를 불러왔으며 CA 를 분산하는 방법을 통한 해결방안들이 연구되어 왔다. 그 방법은 분산 CA 방식과 자율 CA 방식으로 나눌 수 있는데, 본 논문에서는 클러스트 라우팅 기반의 자율 CA 방식의 키 인증 방법을 제안한다.

2. 관련연구

2.1 Clustering routing Schemes

Clustering routing 은 하나의 노드를 중심으로 1 홉거

* 본 연구는 정보통신부 및 정보통신연구진흥원의 대학 IT연구센터 육성・지원사업의 연구결과로 수행되었음.

리에 있는 노드들의 단위들을 클러스트로 구성하는 라우팅 모델로 클러스터마다 크러스터 헤드를 선출하고 두개 이상의 클러스터와 접하고 있는 노드를 게이트웨이로 정한다. 클러스트 내의 일반노드들은 클러스트 헤드와 게이트웨이에 의해 관리, 통신된다.

클러스터링 기법은 MANET 에서 여러 장점을 갖는다.[4] 첫번째 클러스터 헤드와 게이트웨이가 가상적인 백본망 역할[5]을 하기 때문에 라우팅이 효과적으로 이루어진다. 두번째 각 노드들 관점에서 네트워크가 보다 간단하고 안정적인 모습을 하게 된다. 마지막으로 노드들에게 각각의 일을 부여함으로해서 각 노드가 효율적으로 동작하도록 만든다.

2.2 PKI 키 관리

PKI 는 CA 를 통하여 공개키를 관리하는 구조를 말하며 계층적인 CA 를 통해서 사용자의 공개키를 관리해준다. MANET 에서는 그 특성상 고정적인 CA 가 불가능하므로 고전적인 PKI 의 변형인 분산 CA 구조와 자율 CA 구조가 사용된다.

2.2.1 분산 CA 구조 [6][7]

Threshold Cryptography 는 공개키/개인키 쌍에서 개인키를 K 조각으로 나눈후 n 개의 노드에게 분산시키는 방법이다. 따라서 n 개의 노드에 분산된 K 개의 조각키를 모아야만 공개키로 암호화된 내용을 알 수 있다. Threshold Cryptography 를 이용하면 실제적으로 K 개로 분산된 CA 의 효과를 갖게 되는데 이는 K 개의 조각키를 모으지 않으면 CA 의 역할(키인증, 서명, 갱신)을 할 수 없기 때문이다. 하지만 분산 CA 구조는 한 클러스터에 K 개 이하의 노드가 존재할 경우 사용할 수 없으며 키관리를 위하여 많은 통신횟수를 요구하게 된다.

2.2.2 자율 CA 구조 [8]

자율 CA 구조는 각 노드들이 공개키를 PGP 방식[9]을통해 상호 보관 함으로 해서 이루어진다. 공개키를 상호 보관하기 위해서 노드들은 동등한 구조를 갖으며 Web of trust 를 기반으로 KeyRing 이 결정된다.

2.2.3 Key Ring

모든 키는 사용자가 효과적으로 사용할 수 있도록 체계적인 방법으로 관리, 저장될 필요가 있으며 이를 위해 PGP 에서는 해당노드가 소유하는 공개키/개인키 쌍과 다른노드의 공개키들을 저장하기 위한 자료 구조를 가지고 있다. 그 자료구조는 개인키 링 테이블과, 공개키 링 테이블로 나눌 수 있으며 개인키 링 테이블은 Key ID 나 User ID 로 색인되고 보안을 위해 IDEA(International Data Encryption Algorithm)를 이용하여 암호화 되어 해당노드에만 저장되어 있다. 공개키 링 테이블 또한 Key ID 나 User ID 로 색인 되어 있으며 다른노드의 공개키, 신뢰도 등을 기록하여 CA 없이 노드들을 인증하게 된다.

Timestamp	Key ID	Public key	Encrypted Private key	User ID
…	…	…	…	…
T_A	PK_A mod 2^{64}	PK_A	SK_A	ID_A
…	…	…	…	…

[표 1] 개인키 링 테이블

Timestamp	Key ID	Public Key	Owner Trust	User ID
…	…	PK_A	Trust	ID_A
…	…	PK_B	User defined	ID_B
…	…	PK_C	Trust	ID_C

Key legitimacy	Signature(s)	Signature Trust(s)
Trust	…	…
Trust	C의 서명	Trust
…	…	…

[표 2] 공개키 링 테이블

2.2.4 Web of Trust

노드간의 신뢰를 결정하는 방식으로 노드 A 자신이 새로운 키를 만들면 Owner Trust 와 Key legitimacy 필드를 Complete Trusted 로 채우고 인증되지 않는 노드 B 로부터 공개키를 받았을 때 Owner Trust 와 Key legitimacy 는 노드 A 자신의 정책에 맞게 결정하게 된다. 한 예로 [표 2]와 같이 노드 A 가 노드 C 로부터 서명을 받고 Signature Trust 가 Trust 인 노드 B 의 Key legitimacy 를 결정하기 위하여 자기 자신 노드 A 의 공개키 링 테이블을 살펴 보고 테이블 네에 노드 C 의 Key legitimacy 가 Trust 상태 였다면 노드 A 는 노드 B 의 Key legitimacy 를 Trust 와 같이 설정할 수 있다.

3. 자율 키관리 모델

표기법	설 명
CH	클러스터 헤드
N	일반 노드
GW	게이트웨이 노드
AN	CH, N, GW 를 포함한 전체노드
PK	공개키
SK	개인키
E_{PK}	PK 를 사용하여 암호화
E_{SK}	SK 를 사용하여 암호화
RV	임의의 수
neig	이웃 노드
PKR	PK 링 테이블
SKR	SK 링 테이블

[표 3] 표기법 정의

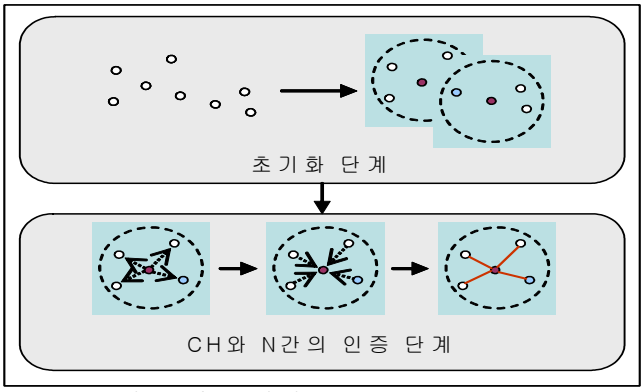
3.1 개요

본 논문에서 이야기하는 자율 키인증 모델은 클러스터링 라우팅 기반에서 자율적으로 PK 를 관리 할 수 있는 모델로 다음과 같은 특징을 갖는다. 첫번째로 CH 는 자신이 관리하는 클러스터 내의 N 들과 CH_neig 들의 PK 를 모두 가지고 있지만 다른 클러스터의 N 들의 PK 는 가지고 있지 않는다. 두번째로 각 N 들은 자신과 통신한 모든 클러스터의 N 들의 PK 를 공개키 링 테이블에 신뢰정도와 함께 기록하며 저장

소의 크기에 따라 사용하지 않는 PK 는 삭제한다. 마지막으로 각 N 들은 자신의 정책에 따라서 공개키 링 테이블 내에 신뢰도를 조절 할 수 있으며 최고의 보안을 위해서 적외선 포트나 직접 전달 받은 공개키만을 Trusted 상태로 놓을 수도 있다.

단, 기본인증과정에서 악의적인 노드가 없다고 가정하고 라우팅 상에서 CH 들이 각 노드로의 라우팅 정보를 알 수 있다고 가정한다.

[그림 2, 3, 4]에서 노드 사이의 검은 선은 신뢰관계가 형성되어 있음을 의미하며 빨간 선은 공개키 교환을 통해 새롭게 신뢰관계가 형성되었음을 의미한다.



[그림 2] 기본 인증 과정

3.2 동작과정

동작과정은 크게 기본인증과정과 상호인증과정으로 나누어 볼 수 있다. 기본인증과정은 GW, N 과 CH 간에 신뢰관계를 형성하는 과정이고, 상호인증과정은 실제 통신이 이루어지는 N 간에 실뢰를 형성하는 과정이다. 즉, 기본인증과정은 처음 네트워크가 형성되었을 때와 토폴로지가 변하였을 경우에만 사용되며 이후 필요에 의해서 상호인증과정을 수행하여 자율적으로 PK 를 교환하게 된다. PKR 에 기록된 PK 가 있는경우 상호인증과정이 필요없이 두 노드간에 신뢰가능한 통신이 가능하게 된다.

3.2.1 기본인증과정

기본인증과정에서는 CH 와 N 간에 무결성, 기밀성, 부인방지를 제공하기 위하여 RV 와 ID 를 이용하여 4 번에 통신횟수를 거쳐 인증을 한다.

3.2.1.1 초기화 단계

1. 노드들을 클러스트 단위로 묶고 CH 와 GW 그리고 N 을 구분한다.
2. 모든 노드들은 자신의 PK/SK 쌍을 만든 후 SKR 에 기록한다.

3.2.1.2 CH 와 N 간의 인증 단계

1. CH 가 클러스터 내에 자신의 PK 를 알린다.
2. 클러스터 내의 N_i는 $E_{PK_{CH}}(ID_i \| RV_i \| PK_i)$ 값을 CH에게 보낸다.
3. CH 는 $E_{PK_i}(E_{SK_{CH}}(ID_{CH} \| RV_i \| RV_{CH}))$ 를 전송한다.
4. N_i는 도착한RV_i자신이 보낸 RV_i와 비교하여 맞으면 자신의 PKR에 PK_{CH}와 ID_{CH}를 기록하고 $E_{PK_{CH}}(E_{SK_i}(RV_{CH}))$을 CH에게 보낸다.
5. CH는 RV_{CH}가 처음 보낸 것과 일치 하며는 자신의 PKR에 PK_i와 ID_i를 기록한다.

3.2.2 상호인증과정

실제 통신을 하려는 N 간에 PK 를 교환하기 위하여 CH 를 통해 통신하고자하는 N 의 PK 를 획득하여 PKR 에 기록하는 과정으로 N 들은 자신의 정책에 따라서 각기 다른 PKR 을 구성하게 된다. 통신하려는 노드가 [그림 4]와 같이 같은 클러스터에 있다면 상호 PKR 을 기록하기 위해 다음과 같은 단계를 거친다.

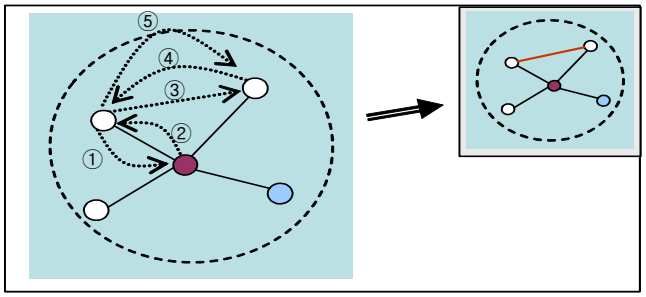
① CH에게 PK_B를 요청

② CH의 PKR에 PK_A가 있는지 확인하고 없다면 3.3.1 을 통해 N_A를 인증
존재한다면 $E_{SK_{CH}}(E_{PK_B}(PK_B))$를 보냄

③ $E_{PK_B}(ID_A \| RV_A \| PK_A))$를 N_B에게 보냄

④ $E_{PK_A}(E_{SK_B}(ID_B \| RV_A \| RV_B))$ 를N_A에게 보내면 N_A는 RV_A값을 확인하고 맞으면 PKR에 자신의 정책에 맞게 PK_B와 ID_B를 저장

⑤ N_A는 $E_{PK_B}(E_{SK_A}(RV_B))$ 를 N_B에게 보내고 받은 N_B는 자신이 보낸 RV_B와 비교하여 일치하는지 확인하고 맞으면 자신의 PKR에 자신의 정책에 맞게 PK_A와 ID_A를 저장



[그림 3] 단일 CH 에서의 N 간의 인증 과정

통신하려는 노드가 [그림 4]와 같이 다른 클러스터에 있다면 조금 더 복잡한 다음과 같은 통신과정을 거친다.

① CH에게 PK_C를 요청

② CH의 PKR에 PK_C가 있는지 확인하고 없으므로 라우팅 정보를 통해 CH_{neig}에게 PK_C를 요청

③ CH_{neig}가 PK_C를 가지고 있으므로 요청한 CH에게 PK값을 보내기 이전에 3.2.2 에서 ③④⑤와 같은 형태로 CH간에 쌍방향 인증을 한뒤에 $E_{PK_{CH}}(E_{SK_{CH_{neig}}}(ID_D \| PK_D))$를 보냄

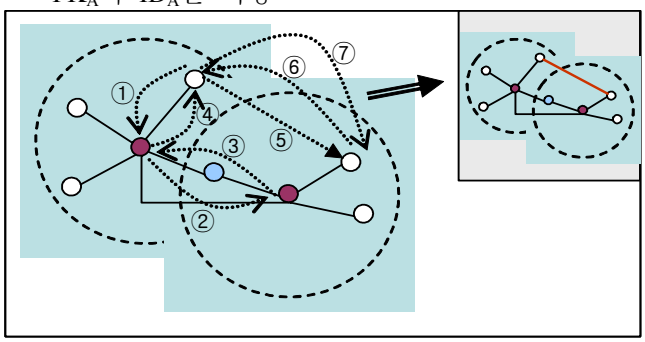
④ N_B에게 $E_{PK_B}(E_{SK_{CH}}(ID_C \| PK_C))$ 를 보냄

⑤ N_B는 N_C에게 $E_{PK_D}(ID_B \| RV_B \| PK_B)$ 를 N_C에게 보냄

⑥ $E_{PK_B}(E_{SK_C}(ID_C \| RV_B \| RV_C))$ 를N_B에게 보내면 N_B는 RV_B값을 확인하고 맞으면 PKR에 자신에 정책에 맞게 PK_C와 ID_C를 저장

⑦ N_B는 $E_{PK_C}(E_{SK_B}(RV_C))$ 를 N_C에게 보내고 받은

N_C는 자신이 보낸 RV_C와 비교하여 일치하는지 확인하고 맞으면 자신의 PKR에 자신의 정책에 맞게 PK_A와 ID_A를 저장



[그림 4] 여러 CH 에서의 N 간의 인증 과정

3.3 다른 클러스터헤드 및 노드의 이동

CH 가 클러스터 지역을 벗어나거나 사라졌을 때에 각 N 은 라우팅 과정 중에 CH 로 부터의 응답이 없다는 사실을 통해 알 수 있으며 그 클러스터 지역은 클러스터 라우팅 프로토콜에 의해 새로운 CH 를 선출하게 된다. 이후에 동작은 3.2.1 과정을 따른다. 노드가 다른 지역으로 이동하거나 사라졌을 때 각 N 간의 혹은 CH 와 N 간의 메시지를 통해서 알 수 있으며 CH 의 PKR 에서 사라진 N 의 데이터를 삭제한다. 새로 유입된 N 은 3.3.1 과 같은 과정을 따르며 PKR 은 그대로 유지하고 있으므로 각 N 끼리의 통신에서는 PKR 의 정보를 이용한다.

3.3.1 클러스터에 새로운 N 의 유입

1. N_i가 PK_{CH}를 알고 있는 경우 PK_{CH}로 메시지를 보내면 CH는 자신의 PKR을 살피고 N_i가 없으므로 RV_i와 ID_i을 요청하여 인증을 시켜준다.
2. N_i가 PK_{CH}를 모르는 경우 N_i는 CH에게 PK_{CH}요청 메시지를 보내고 받은 PK_{CH}로 RV_i와 ID_i를 보냄으로 해서 인증한다.

4. 성능평가

4.1 비교성능평가

[표 4]에서 최소 노드 개수 제한이란 인증을 하기 위해 최소한 몇 개의 노드가 있어야 하는지를 나타내며 노드간의 의존도란 인증과정에서 다른노드에게 얼마나 의존하는지를 나타낸다.

	분산 CA[7]	제안 기법
최소노드 개수 제한	K 개	X
새로운 노드 인증시 암호화 횟수	3 회	4 회
새로운 노드 인증시 통신 횟수	K+2 회	3 회
인증형태	단방향	양방향
노드간에 의존도	높음	낮음

[표 4] 분산 CA 와 제안기법의 요약

4.2 제안 기법의 장점

1. 각 노드들은 자신의 PKR 에 형성된 노드와 통신을 위해 상호인증과정이 필요없으므로 MANET 의 제 형성시 큰 비용이 들지 않는다.
2. 노드가 자신의 PKR 을 가지고 있어 다른 노드에 최대한 적게 의존하므로 DoS 공격과 같이 특정 노드를 무력화 시키는 공격에서 효율적으로 동작할 수 있다

5. 결론 및 향후 과제

본 논문에서는 토폴로지의 동적인 변화, 고정된 인프라의 부재에서 오는 MANET 에서의 보안을 위해서 PGP 방식을 활용하여 클러스트 라우팅 기반에서 동작하는 자율적인 공개키 인증 모델을 제시했다. 노드는 자기만에 PKR 을 유지 함으로 해서 자율적인 키 인증이 가능했다.

향후 시뮬레이션을 통해 다양한 관점에서의 성능평가와 경량화에 초점을 둔 연구를 할 예정이다.

참고문헌

[1] Frank Stajano, Ross Anderson, “The Resurrecting Duckling: Security Issues for Ad-hoc Wireless Networks”, In Proceedings of the 7th International Workshop on Security Protocols, 1999.

[2] Djamel Djenouri, Lyes Khelladi, “A Survey of Security Issues in Mobile Ad Hoc and Sensor Networks”, The Electronic Magazine of Original Peer-Reviewed Survey Articles, Vol.7, No.4, Fourth quarter 2005.

[3] Patroklos G. Argyroudis, Donal O’Mahony, “Secure Routing for Mobile Ad hoc Networks”, The electronic Magazine of Original Peer-Reviewed Survey Articles, Vol.7, No.3, First quarter 2005.

[4] Jane Y. Yu, Peter H.J. Chong, “A Survey of Clustering Schemes for Mobile Ad Hoc Networks”, The electronic Magazine of Original Peer-Reviewed Survey Articles, Vol.7, No.1, First quarter 2005.

[5] Wei Lou, Jie Wu, “A Cluster-Based Backbone Infrastructure for Broadcasting in MANETs”, IEEE IPDPS, 2003.

[6] GeneBeck Hahn, DaeHun Nyang, JooSeok Song, Jae-il Lee, BaeHyo Park, “Secure Cluster Based Routing Protocol Incorporating the Distrubuted PKI Mechanisms”, IEEE MELECON, 2004

[7] 이혜원, 문영성, “CGSR 기반의 이동 애드 혹 네트워크에서 신뢰성있는 통신을 위한 노드간 인증 기법”, 정보과학회논문지, 제 32 권 제 6 호, 2005

[8] Srdjan Capkun, Levente Burryan, “Self-Organized Public-Key Management for Mobile Ad Hoc Networks”, IEEE Transactions on Mobile Computing, VOL.2, NO.1, 2003.

[9] Simson Garfinkel, ‘PGP: PRETTY GOOD PRIVACY’, O’Reilly, 1998

[10] Ozkan M.Erdem, “Efficient Self-Organized Key Management for Mobile Ad Hoc Network”, IEEE Communications Society Globecom, 2004.