Ad-Hoc 네트워크의 노드 인증을 위한 효과적인 그룹 키 관리기법

이풍호°, 한인성, 주현규, 김진묵, 유황빈
광운대학교 컴퓨터과학과
e-mail : aiki@kw.ac.kr

A Effective Group Key Management for Ad Hoc Network Nodes

Pung-ho Lee°, Insung-Han, Hyeon-Kyu Joo°, Jinmook-Kim°, Hwangbin-Ryou°
Department of Computers Engineering, Kwangwoon University

요 약

에드 혹 네트워크는 불규칙한 이동성을 지닌 다수의 노드들에 의해 자율적으로 구성되는 네트워크이다. 그러나 에드 혹 네트워크는 저 전력, 낮은 프로세싱 능력, 무선채널이라는 에드 혹 네트워크만의 특징으로 인해 패킷 드롭, 재전송 공격, 서비스 거부 공격, 비잔틴 공격, 신원사칭과 같은 보안상 여러 가지 공격에 취약하다는 문제점을 안고 있다. 때문에 이러한 취약점을 개선하려는 방안으로 노드 간에 인증, 기밀성, 무결성을 비롯한 여러 가지 요소를 충족시키기 위한 보안기법이 연구되어 왔다, 그러나 Ad Hoc 네트워크는 기존의 회선을 사용하는 정적인 형태의 네트워크가 아닌 시간에 동적으로 네트워크 구조가 변화하며, 네트워크에서 불규칙한 이동성을 지닌 노드들은 적은양의 자원을 소유하는 원인으로 인해 기존의 보안기법은 효과적이지 못하다.

본 논문에서는 신뢰성이 확보된 이웃 노드 간에 그룹을 형성하고, 그룹멤버의 안전성을 입증하는 그룹 인증서를 생성하여 그룹에 접근하는 단일노드 혹은 또 다른 그룹간의 인증을 수행하는 기법을 제안한다. 또한 그룹 멤버 간에 그룹 키를 생성하여 데이터 유출에 대한 위험성 문제를 해결하고, 인증과 기밀성 유지로 인한 자원소비를 감소시킬 수 있도록 하였다.

1. 서론

초기 군사용으로 개발된 에드 혹 네트워크는 AP, 기지국이나 기타 네트워크 인프라 시스템을 지원받지 못하는 각각의 노드들이 호스트와 라우터 역할을 겸함으로써 자체적인 통신을 수행 할 수 있도록 되었다. 이렇게 이러한 특징은 단순히 전쟁터 같은 특수 상황이 아닌 개인용으로 PDA, 휴대전화, 노트북 등의 기기에 이러한 기능을 수행 할 수 있는 장치를 장착함으로써 네트워크망이 구축되지 않은 야외환경에서도 망을 구성하여 통신을 수행할 수 있는 이점을 가지고 있으며, 센서네트워크의 한 분야로 연구되고 있다[2,7]. 그러나 에드 혹 네트워크는 그 특성으로 인해 여러 가지 보안상의 취약점으로 인해 네트워크가 정상적인 작동을 하지 못하고 붕괴되는 위험성까지 안고 있다. 따라서 이렇게 동적인 변화를 가진 에드 혹 네트워크에 적합한 키 분배와 무결성 인증 기술이 요구된다[4].

이 같은 보안을 위해 사용되는 기법으로 공개키 알고리즘을 이용한 서명 및 인증서를 예로 들 수 있다. 암호/복호화에 동일한 키를 사용하는 대칭키 방식과 달리 공개키 알고리즘의 경우에는 암호화 용도인 공개키와 복호화 용도인 개인키로 이루어져 있다. 이러한 공개키 알고리즘은 단순히 기밀성을 위한 암호화뿐만 아니라. 전자인증이나 사용자의 신원을 보증할 수 있는 장점을 가지고 있으나 대칭 키 알고리즘에 비하여 많은 양의 자원을 소비하는 문제점이 있다. 본 논문에서는 Ad Hoc 네트워크의 노드 간에 그룹 인증서를 사용하여 단일 혹은 다수의 노드간에 효과적인 인증을 할 수 있는 기법을 제안한다. 제안하는 방법은 인증이 완료된 이웃노드에 대

한 그룹인증서를 만들고 차후 자신과 인증과정을 거친 또 다른 노드들에게 그룹 인증서를 전송함으로써, 별도의 최소한의 인증작업으로 특정 노드와 신뢰관계에 있는 다수의 노드들을 신뢰한다. 본 논문은 다음과 같다. 2장에서는 공기키 기반의 에드 혹 네트워크의 인증방식인 Certificate Chains[3][5] 기법과 Diffie-Hellman의 비밀 키 교환기법[9]을 기반인 그룹 키 교환 기법과 같은 기존의 연구기술을 살펴본다. 이어서 3장에서는 에드 혹 네트워크에서의 그룹 인증서와 그룹 키 기법에 대한 제안기법을 설명하고 마지막으로 4장에서는 본 기법에서 지원하는 보안 요구사항을 기존의 기법과 비교하고, 5장에서는 결론을 내린다.

2. 관련연구

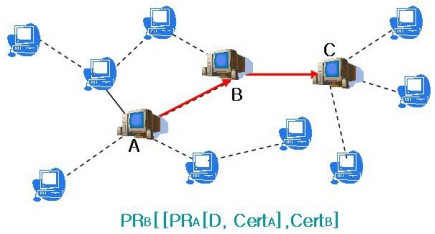
2.1 Group Key Generation

Diffie-Hellman key exchange[9]을 기반으로 둔 기법으로, 그룹멤버 간에 공통된 비밀 키를 교환할 수 있는 기법[1]으로 그룹 멤버간에 교환한 값을 기반으로 동일한 키를 생성/소유 할수 있다는 특징을 가지고 있다. 먼저 n개의 노드는 그룹 키 생성난수를 생성할 헤더 노드에게 [그림 2]와 같이 Private/ Private DH Value값인 g^{r^i}/X^i을 생성하고, Public DH Value값 g^{r^i}을 브로드캐스트 한다. 브로드캐스트를 통해 g^{r^i}값을 받은 헤더 노드는 난수 Z를 생성하고, 각각 그룹에 속해있는 노드들의 g^{r^i}로 난수 Z를 암호화($e(Z)g^{r^i}$)하여 전송한다. 후 난수 Z 값을 전송받은 각각 n개의 멤버들은 모든 그룹멤버들의 공개키인 g^{r^i}를 XOR 연산하여 또 다른 난수 F를 만들게 된다. ($F=f(g^{r^0},g^{r^1},g^{r^2}....g^{r^n})$)이와 같이 그룹멤버들은 난수 Z와 F를 계산하여 공통된 비밀 키 K를 소유하게 된다.($K=F\circ Z$)그룹 키 분배방식은 주로 그룹멤버만의 비밀정보를 보호하려는, 즉 외부공격에 대해 기밀성을 유지하려는 목적으로 사용된다. 그러나 비밀 키를 생성할 때, 모든 노드가 브로드캐스트를 통해 g^{r^i}값을 전송하기 때문에 악의적인 노드의 키 생성 개입에 대한 인증과정이 필요하다는 문제점이 있다.

2.2 Certificate Chains

보통 네트워크상에서는 인증서 발급 Server(CA)로부터 CA의 개인키로 서명되어 있는 인증서를 발급받아 사용하여 노드간 에 인증작업을 수행한다.[8] 즉 각각의 노드는 인증이 필요할 때 이 인증서를 상대 노드에게 전송하고 상대 노드는 인증서를 CA의 서명을 체크하여 해당 노드가 CA에게서 인증을 받은 안전한 노드라는 것을 확인할 수 있다. 동적으로 네트워크 구조가 변화하는 에드 혹 네트워크에서는 모든 노드가 라우터의 역할을 함께 수행하므로 단순히 출발지 노드와 목적지 노드만의 인증뿐만 아니라 패킷이 전송된 경로의 안전성 여부를 증명시킬 기술이 요구된다.

PRi	i의 개인키
Certi	i의 인증서
D	Date



[그림 1] Certificate Chains의 구조

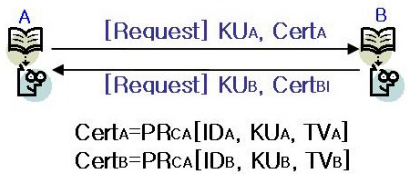
[그림 1]에서 보는 바와 같이 Certificate Chain[3,5] 기법에서는 경유노드들이 패킷에 전자서명과 인증서를 포함시켜, 최종적으로 패킷을 전송받은 목적지 노드가 전자서명과 인증서를 체크하여 패킷이 어느 경로를 통해서 전송되었고, 신뢰할만한 경로인지 확인할 수 있는 방법을 제안하였다. 그러나 연속적인 서명과 인증서가 요구되므로 거리의 증가에 따라 자원소모 또한 증가한다는 문제점이 있다.

3. 제안된 기법

3.1 인증(Authenticate)

안전성이 입증된 CA로부터 이미 인증서를 발급을 받는다고 가정할 때[8], 이 인증서는 CA의 개인키로 서명되어 있어 CA의 공개키로 인증서를 체크 할 수 있다. 먼저 상호간의 인증작업은 [그림 3]과 같이 공개키 기반의 인증방법과 같다[6].

Certi	i의 공개 키 인증서
IDi	i의 ID
KUi	i의 공개 키
PRi	i의 개인 키
TVi	인증서의 유효기간



CertA=PRCA[IDA, KUA, TVA]
CertB=PRCA[IDB, KUB, TVB]

[그림 2]Ad Hoc에서의 Node간 인증방법

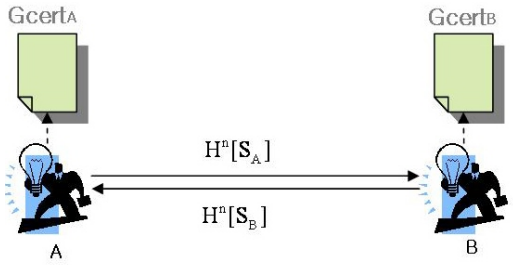
에드 혹 네트워크 노드인 A와 B는 [그림 3]과 같이 인증서를 사용한 인증작업을 수행한다. 이렇게 A와 B는 CA의 서명을 체크하여 상대노드가 CA와 인증과정을 거쳤는지 판단할 수 있다.

3.2 그룹 인증서 생성

인증이 완료된 노드 A와 B는 이후부터 그룹 G의 그룹멤버로 분류되며, 그룹멤버는 차후 이 그룹에 노드 혹은 그룹이 참여하게 될 때, 그룹에 대한 대해 안전성을 입증 시킬 수 있는 그룹 인증서를 생성한다. 인증과정을 거친 그룹멤버는 각각 유일한 난수 Si를 생성하고 n번만큼의 Hash작업(H)을 수행하여 Hash-Chain값을 생성한다.

즉, $H^n[S_i] = H[H[H[...H[S_i]...]]]$ (n Times)

Hash-Chain에서 n번째 Hash-Value인 $H^n[S_i]$을 상대노드에게 전송한 후, [그림 4] 와 같이 유일한 값인 $H^n[S_i]$와 노드의 ID, 노드의 공개키를 포함한 그룹인증서를 생성한다.



[그림 3] hash-Value 교환과 그룹인증서 생성

이때, 그룹 인증서는 아래와 같은 신뢰관계로 나타낼 수 있다.

① $Cert_A = PR_{CA}[ID_A, KU_A, TV_A]$ 이므로, CA는 A를 신뢰한다.

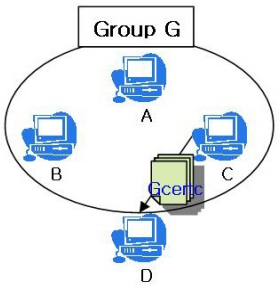
② $Gcert_A = PR_A[ID_B, KU_B, H^n[S_B]]$ 이므로 A의 그룹인증서인 또한 안전하다.

③그룹 인증서 $Gcert_A$에는 B의 안전성을 입증하는 내용을 포함하고 있다.($ID_B, KU_B, H^n[S_B]$)

④따라서 CA가 신뢰하는 A는 B와 신뢰관계에 있으므로 B는 안전하다.

위 신뢰관계에서 알 수 있듯이 각각의 그룹멤버들은 그룹 인증서를 사용하여, 그룹멤버들에 대한 인증작업을 일괄적으로 대신 수행 할 수 있다.

3.3 사용 및 인증



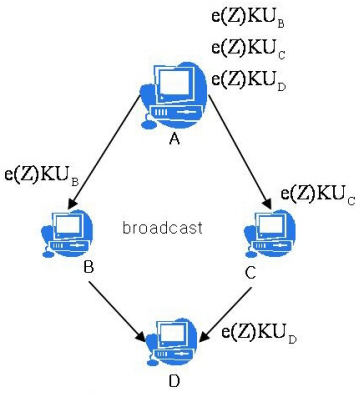
$Gcert_C = PR_C[|ID_A, KU_A, H^n[S_A]||ID_B, KU_B, H^n[S_B]|]$

[그림 4] 그룹 인증서를 통한 인증방법

상호간에 인증된 A, B, C 로 구성된 그룹 G가 있고, 그룹에 참여하려는 외부노드 D가 그룹멤버 C와 신뢰관계에 있다고 가정한다면, C는 [그림 4]와 같이 그룹 G의 그룹 인증서를 D에게 전송한다. C의 개인키로 서명된 그룹인증서를 전송받은 D는 C와 신뢰관계에 있으므로 D는 C의 그룹멤버인 A와 B를 신뢰할 수 있다. 또한 C는 새로운 그룹 인증서를 그룹멤버에게 전송 하여 그룹 멤버에 대한 정보를 갱신할 수 있다. 또한 제안된 기법에서는 에드 혹 네트워크의 동적변화에 대한 주기적인 인증 및 확인작업을 수행한다. 시간별 인증/확인을 하기위해 그룹멤버는 3.2장의 Hash-chain을 사용하는데, 여기서 각각의 그룹멤버들은 일정주기마다 다음과 같은 공식에 해당되는 Hash-Value를 브로드캐스트한다.

즉, 일정 주기마다 $C = C + 1$, $H^{n-C}[Si]$을 전송받은 그룹멤버노드들은 전송받은$H^{n-C}[Si]$를 Hash한 값과 자신이 소유하던 기존의 $H^n[S_i]$값을 비교하여, 차후 각각의 노드들은 인증서가 아닌 Hash-Chain 값으로 인증작업을 실행함으로써 공개키 인증서 사용으로 인한 오버헤드와 자원소모 문제를 해결할 수 있다.

3.4 그룹 키 생성



[그림 5] 추가적인 그룹 키 생성법

외부공격에 대한 기말성 유지를 위한 목적으로그룹 키 교환기법을 통해 그룹 멤버노드들은 동일한 비밀키를 소유한다. 여기서 이미 그룹 키 K를 생성하기 위한 Private/Public DH Value값(g^n/X^i)는 그룹 멤버의 Private/Public Key(KU_{i+}/PR_{i+})로 사용하고 A가 헤더노드로 선발 되었다고 가정한다. 노드 A는 위 [그림 7]와 같이 그룹 키 생성난수 **Z**를 그룹멤버의 개인키로 암호화하여 전송한다. 자신의 개인키를 통해 암호문을 복호화한 그룹멤버들은 그룹 키 분배기법[1]과 같이 다른 그룹 멤버들의 공개키를 계산하여 또 다른 난수 **F**를 생성하고, 이 **Z**와 **F** 값을 사용하여 동일한 그룹 키인 **K**를 생성할 수 있다.

4. 비교분석

본 논문에서 제안된 기법은 인증 및 그룹 키 분배 기법이지만, 그룹 키의 사용과 각각의 노드가 소유한 Hash-chain 값를 라우팅 테이블에 포함시켜 라우팅 패킷 및 제어 패킷의 기밀성 및 무결성과 인증을 유지하는 용도로 사용할 수 있다. 따라서 [표 1]에서는 본 논문에서 제안한 방법을 라우팅에 적용시킨 부분과 기존의 보안 라우팅이 지원하는 보안성의 정도, 무결성 및 인증에 대한 지원 사항을 기존의 기법과 비교하였다

[표 1] 제안된 방법과 기존 방법의 보안성 비교

비교항목 / 보안기법	SEAD	ARAN	Secure-AODV	제안된 방법
보안요구 사항 지원	인증 무결성	인증 무결성	인증 무결성	인증 무결성 기밀성
서명 및 인증	해쉬체인 사용	비 대칭키 서명	비 대칭 키 서명	해쉬체인 그룹 키 사용
오버헤드	낮음	높음	높음	낮음

5. 결론

본 논문에서는 동적인 이동성을 가지는 노드에 의해 자율적으로 구성되는 에드 혹 네트워크 환경의 특성으로 인한 보안상 취약점을 해결하려는 방안으로 그룹 인증서와 그룹 키를 통한 인증 및 키 분배 기법을 제안하였다. 제안된 방법은 각각의 노드들은 인증된 이웃노드들 간에 그룹을 형성하고, 그룹멤버들의 안전성을 증명하는 그룹인증서를 생성한다. 이후 그룹에 단일노드 혹은 또 다른 그룹의 간의 인증작업에 사용하도록 하였다. 이렇게 그룹 인증서를 사용함으로써, 작은 양의 자원소모로 효율적인 인증을 할 수 있도록 하였으며, 멤버들만에 유일한 Hash-Chain 값을 브로드캐스트를 하여 그룹 내의 멤버들의 확인 및 인증작업을 수행하도록 하였다. 또한 그룹 키 분배방식을 적용하여 라우팅 패킷을 비롯한 제어 패킷의 기밀성을 유지할 수 있도록 하였으며, 기밀성 유지에 필요한 그룹 키 분배 시 악의적인 노드가 개입하여 생겨날 수 있는 보안상의 취약점 해결하였다.

5. 참고 문헌

[1] A. Yasinsac, V. Thakur, S. Carter, and I. Cubukcu. “A Family of Protocols for Group Key Generation in Ad Hoc Networks.” In Proc. o IASTED International Conference on Communications and Computer Networks. 2002

[2] Dirk Balfanz, D. K. Smetters, Paul Stewart and H. Chi Wong Talking To Strangers: Authentication in Ad-Hoc Wireless Networks In Symposium on Network and Distributed Systems Security (NDSS '02), San Diego, California, February 2002

[3] G. Gouda and Eunjin Jung "Certificate Dispersal in Ad-hoc Network" Mohamed in the Proceedings of IEEE ICDCS 04, March 2004

[4] L. Zhou and Z. J. Haas, "Securing Ad Hoc Networks," IEEE Network Magazine, vol. 13, no.6, November/December 1999

[5] J-P. Hubaux, L. Buttyan´and S. Capkun, "The Quest for Security in Mobile Ad Hoc Networks" In Proc. ACM MOBICOM, Oct. 2001

[6] M. Steiner, G. Tsudik and M. Waidner "Key Agreement in Dynamic Peer Groups" IEEE Transactions on Parallel and Distributed Systems, August 2000

[7] N. Asokan, Philip Ginzboorg Key agreement in ad hoc networks Computer Communications, 23:1627-1637, 2000

[8] Needham, R., and Schroeder, M. "Using Encryption for Authentication in Large Networks of Computers." Communications of the ACM, December 1978

[9] W. Diffie and M. Hellman: New directions in cryptography, IEEE Trans. Inf. Theory, IT-22, 1976, pp.644-654