이동 Ad Hoc 네트워크에서 다중경로를 통한 신뢰도 기반의 안전한 인증 기법

김재성, 송주석
연세대학교 컴퓨터학과
e-mail:{junghasea, jssong}@emerald.yonsei.ac.kr,

Multipath based Secure Authentication by Trust Level in Mobile Ad hoc Networks

JaeSung Kim, JooSeok Song
Dept of Computer Science, Yonsei University

요 약

이동 Ad Hoc 네트워크에서는 노드가 신뢰받은 인증기관을 통해 인증을 받는 형식이 아니기 때문에, 멀티홉 방식에 의해 라우팅을 수행할 경우 악의적인 중간 노드에 의해 데이터의 무결성 및 기밀성 문제가 발생할 수 있다. 따라서 이동 Ad Hoc 네트워크에서 안전하게 통신하기 위해서는 네트워크에 참여한 노드 중 악의적 중간 노드를 찾아내 격리시키고, 서로 신뢰할 수 있는 노드만이 네트워크에 참여할 수 있도록 하는 방안이 필요하다. 본 논문에서는 신뢰받는 인증기관이 없는 이동 Ad Hoc 네트워크에서 신뢰도 측정을 바탕으로 노드간 상호 인증할 수 있는 새로운 방안을 제시한다.

1. 서론

이동 Ad Hoc 네트워크는 기간망이 붕괴되거나 형성되어 있지 않은 상황에서 이웃 노드들 간의 통신을 목적으로 사용 된다. 이동 Ad Hoc 네트워크에서는 위상은 빠르면서 예측할 수 없게 변하고, 무선 인터페이스를 사용하기 때문에 고정된 유선 네트워크에 비해 보안에 취약하다.[1] 기본적으로 이동 Ad Hoc 네트워크의 보안 요구조건은 다른 통신 네트워크에서 요구되는 것과 동일하지만, 이동 Ad Hoc 네트워크에서는 노드가 신뢰받은 인증기관을 통해 인증을 받는 형식이 아니기 때문에 노드의 신분이 서로에게 불확실한 경우가 많으며, 멀티홉 방식에 의해 라우팅을 수행할 경우 악의적인 중간 노드에 의해 데이터의 무결성 및 기밀성 문제가 발생할 수 있다. 특히 매체를 신뢰할 수 없는 상황에서 암호를 사용하므로 암호 키에 크게 의존하게 된다. 따라서 키 사이에 신뢰할 수 있는 관계를 형성하고, 이를 이동 Ad Hoc 네트워크 전반에 분배하는 것이 주요 과제이다. [1][2]

본 논문에서는 신뢰받는 인증기관이 없는 Mobile Ad Hoc 네트워크에서 주변의 이웃노드가 측정한 신뢰도를 기반으로 다중경로를 통해 이웃노드 인증서를 제공하여 노드간 상호 인증할 수 있는 방안을 제안하였다. 제안된 인증 기법을 통하여 네트워크에 참여한 노드 중 악의적 중간 노드를 찾아 격리시킴으로 서로 신뢰할 수 있는 노드만 네트워크에 참여하도록 한다.

이 논문은 2008년도 정부(과학기술부)의 재원으로 한국과학재단의 지원을 받아 수행된 연구임(No. R01-2006-000-10614-0).

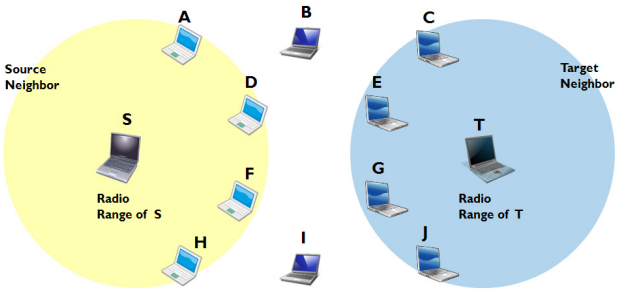
본 논문의 구성은 2장에서는 다중경로를 통한 신뢰도 기반의 인증 인증서비스를 기술하고 3장에서는 결론을 맺도록 하겠다.

2. 다중경로를 통한 신뢰도 기반 인증

다중경로를 통한 신뢰도 기반 인증은 주변의 이웃노드들을 통하여 목적지노드까지 다중의 경로로 자신의 공개키를 전달하는 방식이다. 소스노드와 주변 이웃노드는 관찰을 통해 측정한 신뢰도를 기반으로 상호인증을 하고, 인증서를 발행한다. 이 인증서는 목적지노드에게 송신자의 신원을 밝혀주는데 사용된다. 따라서 네트워크에 참여하는 모든 노드는 자신이 직접 공개키를 전달하는 것이 아닌 주변의 이웃노드가 전달하고 신원을 보장해주는 방식의 인증을 수행한다.

2.1 네트워크 환경

신뢰할 수 있는 인증기관이 없는 이동 Ad Hoc 네트워크에서 노드간 인증을 하기 위한 가정 사항으로 새로운 노드가 네트워크에 참여하기 위한 기본은 이웃노드의 공개키를 요청함과 동시에 자신의 공개키를 주변 이웃노드에게 전달하는 것이다. 자신의 ID와 공개키는 노드 인증 시 사용되며, 자신이 공개한 공개키에 대한 인증은 전자서명 방식을 이용한다.[4] 각 노드는 이웃노드의 감시 하에 신뢰도를 쌓기 위하여 네트워크에 적극적으로 참여하게 된다.



Path 1	S - A - B - C - T
Path 2	S - D - E - T
Path 3	S - F - G - T
Path 4	S - H - I - J - T

(그림 1) 기본 네트워크 구성

통신을 위한 경로탐색 시 On-Demand 방식의 노드가 겹치지 않는 AOMDV(Ad hoc On-demand Multipath Distance Vector) 등의 라우팅 알고리즘을 통한다.[5][6] 또한 네트워크에는 악의적 노드가 일정 수 존재하고 Man-in-the-Middle Attack, Packet Drop 등의 공격을 수행한다.

2.2 인증처리

소스노드는 통신을 하기 위해서 먼저 자신의 주변노드와(한홉이내) 상호인증서 교환을 해야 한다. 이것은 통신을 위한 기본 조건으로서 상호 감시를 통하여 신뢰도를 측정하고[7] 일정 신뢰도 이상인 경우에 한하여 교환하도록 한다. [7]의 방법을 이용하여 본 논문에서는 (1)과 같이 노드간 상호인증서를(C_{XY}) 정의한다. 인증서는 인증하는 노드의 개인키로 인증받고자 하는 노드의 ID와 공개키, 유효기간을 서명한 값이다.

$$C_{XY} = KPV_X\langle ID_Y, KPU_Y, VP\rangle \quad (1)$$

소스노드는 인증서 교환이 완료된 자신의 이웃노드들의 공개키 테이블 $TKPU_S$를 생성한다. 그 다음 임의의 랜덤 값을 생성하여 자신과 목적지노드의 ID, RREQ의 Sequence Number를 자신의 개인키로 서명한 후, $TKPU_S$와 함께 RREQ 메시지를 네트워크로 브로드캐스트 한다.

S→A: RREQ, $TKPU_S$, $KPV_S\langle ID_S, ID_T, SN, N_S\rangle$ (2)

RREQ를 전달 받은 소스노드의 이웃노드들은 소스노드에 대한 인증서를 패킷에 추가하여 중간노드로 포워딩한다.

A→B: RREQ, $TKPU_S$, $KPV_S\langle ID_S, ID_T, SN, N_S\rangle$, C_{AS} (3)

중간노드는 전달 받은 RREQ를 변경없이 목적지 노드까지 포워딩한다.

B~T: RREQ, $TKPU_S$, $KPV_S\langle ID_S, ID_T, SN, N_S\rangle$, C_{AS} (4)

<표1> Notation

KPV_A	Private key of node A
KPU_A	Pubic key of node A
$TKPU_A$	Neighbor Public key table of node A
C_{AB}	Certificate of node B from node A
ID_A	Identity of node A
N_A	nonce of node A
SN	Sequence Number
VP	Validity Period
$KPV_A\langle D\rangle$	Digital Signature of data D with KPV_A

목적지노드는 각 경로를 통하여 RREQ 값을 수신하고 3개 이상이 되었을 때 소스노드에 대한 인증절차를 시작한다. 첫 번째 단계는 각각의 경로를 통해 전달받은 소스 이웃노드들의 공개키 값을($TKPU_S$) 검사한다. 만일 이 과정에서 $TKPU_S$가 다른 것이 있다면 악의적노드에 의한 패킷의 변경이라 판단하고 경로에서 배제한다. 두 번째 단계는 이웃노드가 보낸 인증서를 검증한다. 이웃노드가 보낸 인증서는 수신한 $TKPU_S$로부터 검증할 수 있다. 만일 이웃노드의 공개키로부터 소스노드의 ID 및 공개키를 추출할 수 없다면 경로에서 배제하고 다른 경로를 검증한다. 마지막 단계는 인증서를 통하여 추출한 소스의 공개키를 가지고 각각의 경로를 통하여 전달받은 소스노드가 서명하여 보낸 임의의 변수 값을 상호 비교한다. 만일 임의의 변수 값이 다르다면 해당 경로는 배제한다.

응답과정은 경로탐색과정과 유사하다. 목적지노드는 RREQ를 수신하여 소스노드가 생성한 임의의 랜덤 변수 N_S와 목적지노드의 임의의 랜덤 변수 N_T를 개인키로 서명하여 각각의 경로로 $TKPU_T$ 및 RREP와 함께 보낸다. 목적지 노드는 RREQ를 통하여 각 경로 상에 있는 이웃노드를 알 수 있지만 악의적 중간노드에 의해 목적지노드에 대한 인증서가 안전하지 못하기 때문에 전체 이웃노드의 공개키 테이블인 $TKPU_T$를 단일 경로로 전달하고, 소스노드가 모든 RREP를 수신하였을 때 $TKPU_T$를 비교하여 목적지 노드에 대한 1차 인증을 할 수 있도록 한다.

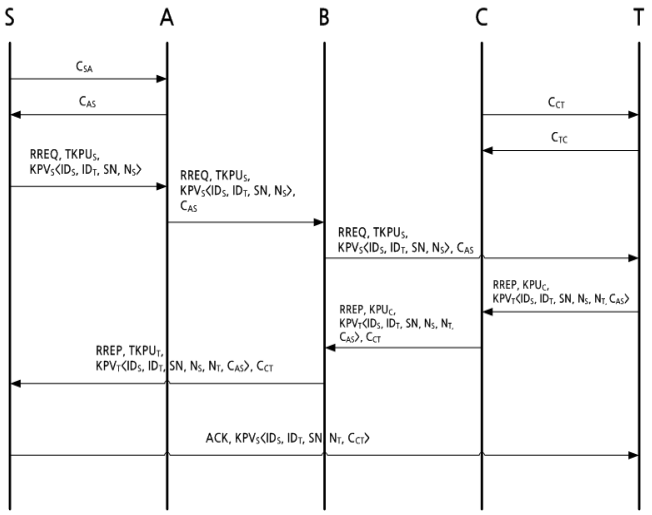
T→C: RREP, $TKPU_T$, $KPV_T\langle ID_S, ID_T, SN, N_S, N_T\rangle$ (5)

RREP를 전달 받은 목적지노드의 이웃노드들은 목적지노드에 대한 인증서를 RREP에 추가하여 중간노드로 전송한다.

C→B: RREP, $TKPU_T$, $KPV_T\langle ID_S, ID_T, SN, N_S, N_T\rangle$, C_{CT} (6)

중간노드는 전달 받은 RREP를 변경없이 소스노드까지 전달한다.

B~S: RREP, $TKPU_T$, $KPV_T\langle ID_S, ID_T, SN, N_S, N_T\rangle$, C_{CT} (7)



(그림 2) 인증절차

소스노드는 각 경로를 통하여 RREP 값을 수신하고 소스노드 인증과 마찬가지로 3개 이상이 되었을 때 목적지노드에 대한 인증절차를 시작한다. 인증절차는 소스노드에 대한 인증절차와 같다. 이웃노드들의 공개키 값에 대한 검사, 이웃노드가 보낸 인증서를 검증, 인증서에 포함된 목적지노드의 ID와 공개키 값을 상호 비교 절차를 마친 후, 마지막으로 자신이 생성한 전달된 임의의 변수 값과 자신이 생성한 공개키 값을 비교한다. 소스노드가 보낸 N_S와 전달받은 N_S가 다를 경우, 마찬가지로 악의적 노드에 의한 공격으로 판단하여 경로에서 배제한다.

인증의 마지막과정인 목적지노드가 생성한 임의의 변수에 대한 확인은 ACK 메시지를 통하여 전달한다. 소스노드는 목적지 노드가 생성한 임의 변수 N_T와 이웃노드 인증서를 자신의 개인키로 서명하여 목적지노드로 전송한다.

$$S \sim T\text{: ACK, } KPV_S\langle ID_S, ID_T, SN, N_T, C_{CT}\rangle \quad (8)$$

ACK 메시지를 수신한 목적지 노드는 전달받은 N_T와 자신이 생성했던 N_T를 상호 비교하여 일치할 경우 소스노드에 대한 인증을 완료한다.

3. 결론

본 논문에서는 다중경로를 통한 신뢰성 기반의 인증기법을 제안하였다. 이동 Ad Hoc 네트워크에서 신뢰할 수 있는 기관이 존재한다는 것은 현실적으로 어렵기 때문에 본 논문은 신뢰성 있는 인증기관을 대신하여 한홉 이내의 이웃노드가 신뢰도를 측정하여 서로를 인증 해주는 기법을 제안하였다. 제안된 방법의 장점은 네트워크 내에 악의적 노드가 일정 수 포함되더라도 다중경로를 통하여 인증이 가능하다. 하나의 경로만을 통하여 인증할 경우 하나의 악의적인 노드로 인증에 실패할 수 있으나 다중경로를 통할 경우 이를 방지할 수 있다. 또한 악의적 노드가 있을 것이라 판단되면 경로에서 배제하여 보다 안전한 라우팅이 가능하다. Man-in-the-Middle Attack의 경우 또한 여러 경로를 통해 받은 공개키를 상호 비교하여 적절하게 대응할 수 있다.

참고문헌

[1] Yih-Chun HU, Adrian Perrig, "A Survey of Secure Wireless Ad Hoc Routing", IEEE SECURITY & PRIVACY 2004, pp.28 - 39.

[2] D Djenouri, L Khelladi, AN Badache, "A survey of security issues in mobile ad hoc and sensor networks", Communications Surveys & Tutorials, IEEE, 2005.

[3] Xiaoqi Li, Michael R. Lyu, and Jiangchuan Liu. "A Trust Model Based Routing Protocol for Secure Ad Hoc Networks" IEEE Aerospace Conference. March 2004.

[4] Behrouz A. Forouzan "Cryptography and Network Security" International Ed. McGraw Hill

[5] D.B. Johnson, D.A. Maltz, Y. Hu, and J.G. Jetcheva, "The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks", IETF Internet Draft, draft-ietf-manet-dsr-07.txt, Work in progress, February 2002.

[6] Xuefei Li and L. Cuthbert, "On-demand node-disjoint multipath routing in wireless ad hoc networks," Local Computer Networks, 2004. 29th Annual IEEE International Conference on, pp. 419 - 20, 16-18 Nov. 2004.

[7] G. Theodorakopoulos and J.S. Baras. "On trust models and trust evaluation metrics for ad hoc networks" IEEE Journal on Selected Areas in Communications, 24(2):318-328, Feb. 2006.