Ad hoc에서의 인증 프로토콜에 관한 연구

이근호° 이송희 이상근 황종선

고려대학교 컴퓨터학과

(root1004°, pine, yalphy)@korea.ac.kr, hwang@disys.korea.ac.kr

A Study on Authentication Protocol in Ad Hoc Network

Keun-Ho Lee° Song-Hee Yi Sang-Keun Lee, Chong-Sun Hwang

Dept. of Computer Science and Engineering, Korea University

요 약

최근에 유.무선 환경에서의 통합적인 망 구성이 이루어지고 있다. 최근 무선 환경에서의 단말기간의 라우팅 기능을 제공하는 Ad Hoc 네트워크에 대한 관심이 고조되고 있으며 이에 대한 많은 연구가 수행되고 있다. 본 연구에서는 Ad Hoc 네트워크에서의 라우팅 관련 문제들을 살펴보고, 문제를 해결하기 위한 방안으로 ARAN 프로토콜을 이용하여 이동 노드에서 상호간의 인증에 필요한 보안 프로토콜을 연구하였다.

1. 서 론

최근 인터넷의 확장과 단말기의 하드웨어, 무선통신 기술개발이 이루어짐에 따라 시·공간상의 제한 없이 인터넷을 사용하고자 하는 연구가 활발히 진행중이다. 이러한 연구분야의 한 분야가 무선 매체를 이용하는 Ad Hoc 통신망이다. Ad Hoc 통신망은 기존의 기지국이 유선 통신망에 연결된 형태의 통신 인프라 기반과는 달리 모든 단말기가 이동하는 환경에서 서로 직접적인 무선 전송 범위에 위치하지 않은 노드간의 원활한 데이터 전송을 위해 다중 홉 무선 링크로 구성되어 여러 개의 중간 단말기들의 데이터 전달(Forwarding)과 경로설정(Routing)에 의존하게 되는 새로운 형태의 통신망이다. 군대의 통신망과 긴급 구조 상황, 대규모 무선회의, 센서 통신망 등을 예로 들 수 있다. 신속하게 통신망을 구성할 수 있고 기존 통신 인프라에 의존하지 않으며 단말기 이동에 빨리 적응을 할 수 있는 장점을 가진 통신망이라 할 수 있다. Ad Hoc 통신망에서의 이동 호스트 계층은 일시적으로 고정 망의 라우터 또는 고정 라우터에 접속하는 호스트들로 이루어진다. 이러한 호스트들은 논리적으로 고정된 라우터로부터 하나의 전달 거리(hop)에 있고, 그들의 연결은 유선 또는 무선이 될 수 있다. 이러한 기술에 의해 처리되는 기본적인 기능은 위치와 주소 관리이다. 이동 라우터 계층은 고정망에 대응되는 이동 인프라 구조를 형성하기 때문에 고정망으로부터 라우팅에 관련된 지원을 요구하지 않는다. 이동 라우터 계층은 기존의 고정 네트워크 계층에 대한 대안으로 볼 수 있다. 고정 라우터는 고정 망으로의 게이트웨이를 형성하며, 이동 IP를 통한 고정 망과의 상호 운용을 가능하게 한다. 이러한 작동이 가능하려면 분산된 동작 체제 운영이 필요한데, Ad-Hoc 통신망의 노드는 보안 및 라우팅 기능 지원을 백그라운드 네트워크에 의존할 수 없다. Ad Hoc 통신망에 관한 연구는 활발한 편이지만 아직 Ad Hoc 보안 연구는 아직 미흡하다. 무선링크를 사용하는 무선 네트워크는 고정 네트워크에 비해서 취약한 보안 문제에 직면해 있다. Ad Hoc 통신망은 이동단말기의 이동성 문제로 인하여 보안에서 심각한 문제를 가지고 있는데 아직까지 제안된 Ad Hoc 통신망 프로토콜에는 충분한 보안에 관한 해결방안을 제시되지 못하고 있는 실정이다. 따라서 본 연구에서는 현재 제안된 Ad Hoc 네트워크의 라우팅 프로토콜과 보안을 접목하여 Ad Hoc 통신망에서의 보안 취약점을 분석한 후 이를 해결할 수 있는 보안 프로토콜을 제안한다.

2. 관련 연구

2.1 Ad hoc 통신망 기반구조

Ad Hoc 통신망은 기반구조가 없는 네트워크이다. 전통적인 네트워크와는 달리 기반구조를 미리 배치시키지 않고, 중앙관리 라우터 혹은 중단간 라우팅을 지원하기 위한 엄격한 정책을 따르고 있다. 노드들은 자신의 라우팅 패킷에 의존하고 있으며, 노드들은 노드들간의 라우팅 패킷에 의존한다. 움직이는 노드는 다른 노드의 무선범위와 직접적으로 통신할 수 있으나, 노드들이 멀리 떨어져 있는 경우는, 중간노드의 라우트 메시지에 의존하여 통신한다[4].

2.2 Ad Hoc 라우팅에 관한 보안 문제

- 인접한 노드간의 함축적인 신뢰 관계

현행 Ad Hoc 라우팅 프로토콜의 모든 관련은 선천적으로 신뢰할 만하다. 대부분의 Ad Hoc 라우팅 프로토콜은 라우트 패킷에 의한 이웃노드에 의해 협동적인 특성이 있다. 순수한 신뢰적인 모델은 Ad Hoc 네트워크를 마비시키는 악의적인 노드에 의한 잘못된 라우팅 업데이트를 삽입하거나, 낡은 정보를 재생시키거나 라우팅 업데이트를 바꾸거나 혹은 잘못된 라우팅 정보를 광고하는데 있다. 이러한 공격방법은 고정된 네트웍에서도 또한 같으며, Ad Hoc 환경은 더욱 크게 확대되며 이러한 악의적인 노드를 발견하기는 어렵다[1].

- 처리량

Ad Hoc네트워크의 최대 네트워크 처리량은 라우팅과 포워딩을 위한 사용 가능한 모든 노드들에 의한다. 노드의 과부하와 이기적 악의적 혹은 깨짐에 의한 이유로 포워드 패킷과 실패한 패킷의 동의에 의해 불량노드가 될 수 있다. 불량 노드는 문제가 될 수 있다. 불량 노드에 처리량에는 평균 손실량이 높지 않고 최악의 경우는 매우 높다.

- 프로토콜 필드의 변화에 따른 메시지 공격

현재 라우팅 프로토콜은 노드들 간에 지나가는 메시지 프로토콜들의 변경될 수 없음을 가정하고 있다. 라우팅 프로토콜 패킷들은 Ad Hoc네트워크에서 데이터전송의 일들이 관리되고 중요한 관리 정보를 운반하고 있다. 전통적인 Ad Hoc네트워크에서 신뢰의 레벨은 측정되거나 혹은 강화되지 않았다. 악의적인 노드는 네트웍 트래픽과 DOS공격의 방향전환을 이런 필드의 변경을 쉽게 할 수 있기 때문이다. 그림 1에서 네트워크를

설명하고 있다. 악의를 가진 노드 M은 도착점 X까지 도달하는 네트워크에서 노드 B는 X가 더욱 가까움을 알고 X를 유지하고 C는 다시 M으로부터 광고를 받게 된다. 공격은 원거리 방향을 변경하는 공격방법과 서비스를 부정하는 공격방법으로 구분된다. 다음을 살펴보자.

· 경로 순서 변경의 원거리 redirection

원격 전송 공격은 블랙홀 공격이라고도 하며, 이 공격법에는 악의를 가진 노드는 라우팅프로토콜을 사용한다. 프로토콜은 AODV의 예와 라우터의 유지에서 특정한 목적지를 향한 라우트에 의한 순서를 증가 시키고 할당한다. AODV에서 어떠한 노드는 스스로를 통해 트래픽 방향 전환을 할 수 있는데, 인증값보다 목적지 순서 값이 더 클 경우의 노드는 라우트 된다. 그림 1의 예는 Ad Hoc 통신망이다. 악의적인 노드의 제안, 노드 M, 라우트 발견에 의한 원래 노드 S, 목적지 노드 X에 의한 RREQ 메시지를 받은 후 B의 경로 발견을 위한 redirection을 하게 된다.

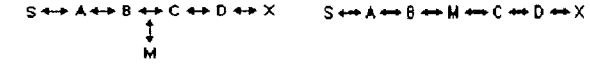

그림 1 라우팅 실패에 따른 노드에 의한 처리량 문제

· 홉 카운트 변경의 redirection(AODV)

Redirection 공격은 경로 발견 메시지에서 홉 카운트 필드의 변경에 의한, AODV 프로토콜에서 가능하다. 라우팅 결정이 다른 측정 기준에 의해 만들어지지 않는다. AODV는 최단경로를 결정하기 위해 홉 카운트 필드를 사용한다. AODV에 있어서 악의를 가진 노드는 0까지 RREP의 홉 카운트 필드를 재설정하고, 관심 있는 노드로 향하게 된다. 비슷하게 무한대로 RREP의 홉 카운트 필드를 설정하게 되면, 경로는 새롭게 생성하게 되고 악의적인 노드는 포함되지 않는다.

3. 기존 보안 인프라를 이용한 문제해결 방안

3.1 가정

Managed-open 환경은 기존에 사용되던 방법들이 사용된다. 통신을 하고자 하는 노드들은 초기 파라미터들을 교환할 수 있다. 이것은 기존의 인프라 네트워크에서 세션키를 교환하는 방식으로 이루어질 수 있으며, 인증기관과 같은 신뢰된 제 3기관을 통해 이루어질 수도 있다.

3.2 Managed-open 환경에서의 ARAN 프로토콜

ARAN(Authenticated Routing for Ad-hoc Networks) 프로토콜은 Ad Hoc 환경에서 제 3자에 의한 악의적인 행동을 감지하고 보호한다. ARAN 프로토콜은 인증, 메시지 무결성, 부인방지를 제공한다. ARAN 프로토콜은 2단계 과정으로 이루어진다. 첫 번째 단계는 단순하지만 기존에 사용되던 Ad Hoc 프로토콜과는 다르게 각 노드에서 좀 더 추가적인 작업이 요구된다. 선택 사항인 두 번째 단계에서는 경로 설정에 보안성이 추가된다. 그러나 두 번째 단계에 참여하지 않는 노드들에게는 추가적인 비용이 든다. ARAN 프로토콜은 인증과 부인방지를 위해 암호학적 인증서를 사용한다[2].

- 단계 1

예비 인증서 단계와 필수사항으로 종단간 인증 단계를 포함한다. 간단한 단계로서 많은 자원을 요구하지 않는다.

· 예비 인증서

ARAN 프로토콜은 신뢰할 수 있는 인증 서버 T를 사용한다. Ad Hoc 네트워크에 들어가기 전에 각각의 노드들은 인증 서버 T에게 인증서를 요구한다. 노드 A의 인증서는 다음과 같다.

$$T \rightarrow A : cert_A = [IP_A, K_{A^+}, t, e]K_{T^-}$$

인증서는 노드 A의 IP 주소와 공개키, 인증서가 생성된 타임스탬프 t, 인증서 유효기간 e가 포함되어 있다. 이러한 변수들은 서버 T에 의해 서명된다. 모든 노드들은 항상 신뢰할 수 있는 서버로부터 새로운 인증서를 유지해야하며, 서버 T의 공개키를 알고 있어야 한다.

· 종단간 인증

단계 1의 주 목적은 근원지가 원하는 목적지에 도달할 수 있는지를 검증하는 것이다. 여기서 되돌아오는 경로는 목적지가 선택한다.

a) 근원지 노드

근원지 노드 A는 RDP(route discovery packet) 메시지를 자신의 이웃 노드들에게 브로드캐스트 함으로써 목적지 X에 대한 경로 설정을 시작한다. RDP 메시지는 다음과 같다.

$$A \rightarrow broadcast : [RDP, IP_X, cert_A, N_A, t]K_{A^-}$$

RDP는 패킷 유형 식별자 ("RDP"), 목적지의 IP주소 (IP_X), 노드 A의 인증서 ($cert_A$), 난수 N_A, 현재 시간 t를 포함하고 있으며, 이 모든 것이 노드 A의 개인키로 서명되어 있다. 노드 A는 경로 설정을 할 때마다 난수 값을 단순하게 증가시킨다. 그러면 노드들은 가장 최근의 난수 값을 타임스탬프와 함께 저장한다.

b) RDP를 처리하는 중간 노드

각각의 노드들은 자신이 어느 이웃 노드로부터 메시지를 받았는지 기록한다. 그 다음 받은 메시지를 자신의 개인키로 서명해 자신의 이웃 노드들에게 전송한다. 이러한 서명을 함으로써 경로를 변경하거나 루프(loop)를 생성하는 spoofing 공격을 막을 수 있다. 노드 A의 이웃 노드를 B라고 했을 때, 메시지는 다음과 같다.

$$B \rightarrow broadcast : [[RDP, IP_X, cert_A, N_A, t]K_{A^-}]K_{B^-}, cert_B$$

노드들은 (N_A, IP_A)쌍을 비교하여 예전에 이미 받았던 메시지들은 전송하지 않는다. 노드 B의 이웃 노드 C가 일단 브로드캐스트를 받으면 인증서의 서명을 검증한 후 B의 서명을 제거한다. 노드 C는 자신의 개인키로 서명한 다음 이웃 노드들에게 RDP 메시지를 다시 브로드캐스트 한다.

$$C \rightarrow broadcast : [[RDP, IP_X, cert_A, N_A, t]K_{A^-}]K_{C^-}, cert_C$$

c) 목적지 노드

결과적으로 목적지 X는 RDP 메시지를 받게 되고, 첫 번째로 받은 RDP 메시지와 난수값에 대해 응답을 하게 된다. 여기서 첫 번째로 받은 RDP 메시지가 항상 근원지로부터 가장 짧은 경로로 온다는 보장은 없다. 목적지는 근원지에게 반대 경로로 REP 메시지를 유니캐스트(unicast) 한다.

$$X \rightarrow D : [REP, IP_a, cert_x, N_A, t]K_{X^-}$$

d) REP를 처리하는 중간 노드

REP 메시지를 받은 노드들은 자신에게 RDP 메시지를 보냈던 전 노드에게 REP 메시지를 역으로 보내준다. 송신자는 REP 메시지에 서명을 한다. 노드 D의 근원지로 가는 다음 노드가 C일 경우 메시지는 다음과 같다.

$$D \rightarrow C : [[REP, IP_a, cert_x, N_A, t]K_{X^-}]K_{D^-}, cert_D$$

노드 C는 D의 서명을 검증한다. D의 서명을 제거한 후 자신의 개인키로 서명한 다음 노드 B에게 유니캐스트한다.

$$C \rightarrow B : [[REP, IP_a, cert_x, N_A, t]K_{X^-}]K_{C^-}, cert_C$$

각 노드들은 REP 메시지를 근원지로 보내면서 전 노드의 서명을 검사한다. 이러한 과정을 거침으로써 악의적인 노드들이 X의 메시지를 위장(impersonation)하거나 재전송(replay)하는 공격을 막을 수 있다.

e) 근원지 노드

근원지 노드는 REP 메시지를 받으면 목적지에서 돌아온 난수값과 목적지의 서명이 정확한지를 검증한다. 오직 목적지만이 RDP 메시지에 대해 응답할 수 있을 뿐, 목적지에 대한 경로를 알고 있는 다른 노드들은 응답을 할 수 없다. 다른 프로토콜들은 네트워킹 최적화를 수행하는 반면, ARAN 프로토콜은

최적화는 수행하지 않지만 응답 메시지에 의한 근원지 노드에서의 트래픽과 발생할 수 있는 남용을 줄인다. 오로지 목적지만이 REP 메시지를 보낼 수 있으므로 loop freedom 문제를 쉽게 해결할 수 있다. 단점으로는 ARAN 프로토콜에서는 각각의 노드들이 현재 가능한 근원지-목적지에 해당하는 라우팅 테이블 목록을 하나씩 유지해야 한다. 이것은 안전하지 않은 ad hoc 라우팅 프로토콜에서 사용하는 목적지 당 라우팅 목록을 유지하는 방식보다는 보다 많은 비용이 요구된다.

- 단계 2

두 번째 단계는 목적지의 인증서가 필요하므로 첫 번째 단계가 이루어진 다음 수행된다. 이번 단계는 안전한 최단 경로를 찾기 위해 사용된다. 경로가 발견되면 데이터 전송은 안전하게 이루어질 수 있다.

a) 근원지

근원지 노드는 SPC(Shortest Path Confirmation) 메시지를 이웃 노드들에게 브로드캐스트 한다.(여기서 사용되는 변수들은 단계 1에서 사용되는 것과 같다)

$$A \rightarrow broadcast : SPC, IP_X, cert_X, \{[IP_X, cert_A, N_A, t]K_{A-}\}K_X.$$

SPC 메시지는 SPC 패킷 식별자("SPC"), X의 IP 주소와 인증서로 시작된다. 또한 X의 IP 주소, A의 인증서, 난수값, 타임스탬프가 포함되어있는 서명된 메시지가 추가된다. 이 서명된 메시지는 X의 공개키로 암호화되므로 다른 노드들은 서명된 메시지의 내용을 변경할 수가 없다.

b) 중간 노드

메시지를 받은 이웃 노드 B는 자신의 암호학적 증명서들을 포함시킨 후 다시 브로드캐스트 한다. 노드 B는 받은 SPC 메시지 내에서 암호화된 부분을 서명하고 자신의 인증서를 추가해 X의 공개키로 재차 암호화를 한다. X의 공개키는 A가 보낸 X의 인증서에서 얻을 수 있다.

$$B \rightarrow broadcast :$$
$$SPC, IP_X, cert_X, \{[\{[IP_X, cert_A, N_A, t]K_{A-}\}K_X,]K_{B-}, cert_B\}K_X.$$

SPC 패킷을 받은 노드들은 중복된 패킷을 전송하지 않도록 자신의 라우팅 테이블에 목록들을 추가시킨다. 또한 이러한 목록은 역경로로 가는 목적지 노드에서 보낸 응답 패킷을 제대로된 경로로 보내준다.

c) 목적지 노드

일단 목적지 노드 X가 SPC 메시지를 받으면 우선 모든 서명들이 타당한지를 검사한다. X는 첫 번째로 받은 SPC 메시지에 대해 응답을 하고, 더 짧은 경로를 가지고 있는 SPC 메시지를 받으면 그것에 대해서도 응답을 한다. X는 전 노드인 D에게 근원지 노드로 향하는 RSP(Recorded Shortest Path)를 전송한다.

$$X \rightarrow D : [RSP, IP_A, cert_X, N_A, route]K_{X-}$$

결국 근원지 노드는 RSP 패킷을 받게 되며, SPC 메시지에 사용했던 난수값이 맞는지를 검증한다. 장점으로는 메시지들을 서명함으로써 중간 노드들이 경로를 변경하는 것을 막을 수 있다. 우선 악의적인 노드들은 SPC 메시지의 경로 길이를 늘리기 위해 정당한 인증서가 추가적으로 필요하며, 둘째로 암호화된 데이터의 무결성을 깨기가 어려우므로 기록되어 있는 경로 길이를 줄이거나 변경할 수가 없다.

3.3 경로 유지

ARAN 프로토콜은 on-demand 프로토콜이며, 노드들은 어느 경로가 유효한지를 알고 있어야 한다. 유효하지 않은 경로에서 받은 데이터는 노드들이 에러 메시지(ERR)를 생성하는 원인이 된다. ERR 메시지는 근원지 노드로 가는 역방향 경로로 전송된다. 또한 노드의 이동으로 인하여 실제로 유효한 경로상의 링크가 깨지는 경우를 알리기 위해 ERR 메시지가 사용한다. 모든 ERR 메시지는 서명되어져야 한다. 근원지 A와 목적지 X의 사이의 경로에 대한 노드 B가 이웃 노드 C에게 보내는 ERR 메시지는 다음과 같다.

$$B \rightarrow C : [ERR, IP_A, IP_X, cert_C, N_B, t]K_{B-}$$

이 메시지는 추가적인 변경 없이 근원지 노드로 향하는 경로로 전송된다. 난수값과 타임스탬프로 ERR 메시지가 최근에 생성된 것인지를 확인할 수 있다. 메시지가 서명되어 전송되므로 악의적인 목적을 가진 노드들이 함부로 ERR 메시지를 생성해 전송할 수 없다. ERR 메시지를 서명함으로써 제공되는 부인방지는 각각의 ERR 메시지가 누가 생성해서 보냈는지를 검증할 수 있게 해준다. ERR 메시지의 전송은 가급적 지양해야 한다.

3.4 키 폐지

인증서가 폐지되어야 할 상황이 발생하면 신뢰할 수 있는 인증 서버 T는 인증서가 폐지되었음을 알리는 메시지를 Ad Hoc 그룹에게 브로드캐스트 한다. 폐지된 인증서를 $cert_r$이라고 했을 때, 다음과 같은 메시지가 전송된다.

$$T \rightarrow broadcast : [revoke, cert_r]K_{T-}$$

이 메시지를 받는 노드들은 자신의 이웃 노드들에게 다시 브로드캐스트 한다. 폐지된 인증서가 정상적으로 만료될 때까지 폐지 통지서는 저장되어야 하며, 폐지된 인증서를 가지고 있는 노드의 이웃 노드들은 현재 신뢰할 수 없는 노드들 통해 전송이 이루어지는 것을 막기 위해 경로를 다시 설정해야 한다.

이러한 방법이 전혀 문제가 없는 것은 아니다. 만약 두개의 ad hoc 네트워크를 연결하는 유일한 연결점 역할을 하는 노드의 인증서가 아직 폐지 과정 중이라면, 그 노드는 다른 한쪽 방향으로는 폐지 메시지를 전달하지 않을 것이다. 결국 네트워크를 분할하게 되는 결과를 초래한다. 위와 같은 상황을 막고 폐지 통지서를 빠르게 확산시키기 위해, 어느 한 노드가 새로운 이웃을 만나면 서로 자신의 보유하고 있는 폐지 통지서의 요약 정보를 교환한다. 요약 정보가 서로 일치하지 않으면 폐지 통지서를 확산하기 위해 다시 브로드캐스트 된다.

4. 결론

Ad Hoc 통신망에 대한 라우팅 관련 문제점을 도출하여 보고 도출된 문제를 해결하기 위한 방법으로 ARAN프로토콜을 설명하였고 ARAN프로토콜에 대한 추가적인 프로토콜을 제시하였다. 향후에는 Ad Hoc 통신망에서 QoS를 보장해주는 프로토콜에 관한 연구가 이루어져야 한다.

참고문헌

[1] Jim Binkley and William Trost, Authenticated Ad Hoc Routing at the Link Layer for Mobile Systems, Wireless Networks 7, 139-145, 2001.

[2] Bridget Dahill, Brian Neil Levine, Elizabeth Royer, and Clay Shields, A Secure Routing Protocol for Ad Hoc Networks, Technical Report TR01-37, Department of computer Science, University of Massachusetts, August 2001.

[3] Panagiotis Papadimitratos and Zygmunt J. Haas, Secure routing for mobile ad hoc networks, SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002), January 2002.

[4] Yih-Chun Hu, Adrian Perrig, and David B. Johnson, Ariadne: A Secure On-Demand Routing Protocol for Ad hoc Networks, Technical Report TR01-383, December 2001.

[5] Lidong Zhou and Zygmunt J. Haas, Securing Ad Hoc Networks, IEEE Network Magazine, 13(6):24-30, November/December 1999.

[6] Frank Stajano and Ross Anderson, The Resurrecting Duckling: Security Issues for Ad-hoc Wireless Networks, The 7th International Workshop on Security Protocols, LNCS 1796, Springer-Verlag, 1999.