제19회 한국정보처리학회 춘계학술발표대회 논문집 제10권 제1호 (2003.5)

Ad-Hoc 네트워크에서 안전한 라우팅 설정을 위한 인증 프로토콜

박복녕, 이원준, 이상근
고려대학교 컴퓨터학과
e-mail:happy@korea.ac.kr

An Authentication Protocol for Secure Routing in Ad-Hoc Networks

Bok-Nyong Park, Wonjun Lee, Sangkeun Lee
Dept of Computer Science & Engineering, Korea University

요 약

Ad-Hoc 네트워크는 기존에 설치된 유선망이나 기지국과 같은 기반 구조가 없는 환경에서 이동 호스트들로만 구성되는 임시적인 무선 이동 네트워크이다. Ad-Hoc 통신망은 이동단말기의 이동성 문제로 인하여 보안에서 심각한 문제를 가지고 있는데 아직까지 제안된 Ad-Hoc 통신망 프로토콜에는 충분한 보안에 관한 해결방안이 제시되지 못하고 있는 실정이다. Ad-Hoc 네트워크에서 안전한 라우팅 프로토콜을 설정하기 위해서는 호스트들 사이에 인증을 하여야 한다. 본 논문에서는 Ad-Hoc에서 안전한 라우팅 설정을 위한 인증 프로토콜을 제안한다. 제안한 프로토콜은 해쉬 함수와 디지털 서명을 통하여 노드들을 인증하여 라우팅 설정에 안전성을 제공한다.

1. 서론

인터넷의 확장과 무선통신 기술개발이 이루어짐에 따라 이동 무선 컴퓨팅은 급격히 그 응용 범위와 사용 빈도가 증가될 것이다. 이러한 추세를 가장 잘 반영하는 기술 중의 하나인 Ad-Hoc 네트워크는 기반구조가 없는 네트워크이다. Ad-Hoc 네트워크는 기존 통신 인프라의 도움 없이 무선 인터페이스를 가진 이동 노드들 간에 자율적으로 구성되는 임시적인 네트워크이다[1][2].

Ad-Hoc 네트워크에 관한 연구는 인터넷 IEFT (Internet Engineering Task Force)에서 MANET 작업 그룹(Mobile Ad hoc NETworks Working Group)을 통해 표준화 활동을 활발히 진행 중에 있으며 주로 라우팅 프로토콜에 관한 표준을 정하고 있다.

그러나, 이러한 Ad-Hoc 네트워크에의 라우팅 및 통신망에 관한 연구는 활발한 편이지만 아직까지 미흡하다. 무선링크를 사용하는 무선 네트워크는 고정 네트워크에 비해서 취약한 보안 문제에 직면해 있다. Ad-Hoc 네트워크는 이동 단말기의 이동성 문제로 인하여 보안에서 심각한 문제를 가지고 있는데 반하여, 아직까지 제안된 Ad-Hoc 네트워크 프로토콜에서는 보안에 관련한 충분한 해결방안을 제시하고 있지 못하는 실정이다. 따라서 본 논문에서는 Ad-Hoc에서 안전한 라우팅 설정을 위한 인증 프로토콜을 제안한다. 제안한 프로토콜은 해쉬 함수를 통하여 메시지 무결성을 제공하고, 메시지에 서명을 함으로써 경로를 변경하거나 루프(loop)를 생성하는 spoofing 공격 및 도청 등의 공격을 막을 수 있다.

본 논문에서 2장에서는 Ad-Hoc 네트워크의 기술 및 보안 개요에 대해 살펴보고, 3장에서는 안전한 라우팅을 위한 인증 프로토콜을 제안한다. 4장에서는 제안한 프로토콜에 대한 안전성을 분석하고, 5장에서는 결론 및 향후 연구에 대해서 서술한다.

2. 관련연구

2장에서는 일반적인 Ad-Hoc 네트워크의 특징에 대해 소개하고, Ad-Hoc에서의 보안 개요에 대해 설

명한다.

2.1 Ad-Hoc 네트워크의 특징

Ad-Hoc 네트워크의 특징을 살펴보면, 구성 노드는 이동성을 가지기 때문에 네트워크의 구조 또한 시간에 따라 변화된다. 네트워크의 구조의 동적인 변화는 통신 경로가 항상 동적으로 재구성되어야 함을 의미한다. 또한 Ad-Hoc 네트워크는 기본적으로 무선 인터페이스를 통해 다른 노드와 통신해야 하므로 무선 인터페이스가 본질적으로 가지고 있는 문제점의 하나인 링크 전송 대역상의 제약이 나타난다.

Ad-Hoc 네트워크를 구성하는 이동 노드는 제한된 용량을 가진 배터리를 통해서 에너지를 공급받고 있는 경우가 대부분이고, 일부는 차량에 탑재되거나, 고정된 형태로 사용되어 지속적인 에너지 공급이 가능한 경우도 있다. 에너지상의 제약은 통신 경로 선택의 주요 기준이 되고 있다. 또 다른 특징으로 이동 노드들은 무선 인터페이스를 통해서 통신하기 때문에 원천적으로 물리 계층에서의 보안 문제, 노드간의 인증 문제 등이 존재한다. 그림 1은 일반적인 무선 네트워크와 Ad-Hoc 네트워크를 보인다.

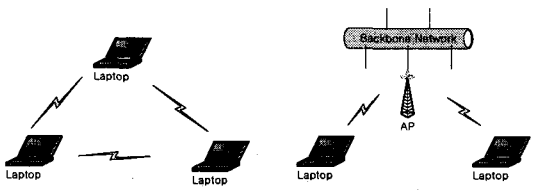

그림 1. Ad-Hoc 네트워크와 일반 무선 네트워크

2.2 Ad-hoc 네트워크의 보안 개요

Ad-Hoc 네트워크는 무선 인터페이스를 사용하기 때문에 유선 네트워크에 비해 훨씬 더 많은 위험에 노출되어 있다. 또한 Ad-Hoc 네트워크에서는 노드의 신분이 서로에게 불확실한 경우가 많으며 멀티-홉 방식에 의해 라우팅을 할 경우 중간 노드에 의해 발생될 수 있는 데이터 보안 문제가 존재한다. 라우팅 프로토콜의 제어 메시지의 경우 대개 브로드캐스팅으로 전달되기 때문에 트래픽보다 더 심각한 문제를 발생시킬 수 있다[3].

2.2.1 연구 영역

Ad-Hoc 네트워크는 무선통신이라는 점과 보안 기반 기술상의 취약성 때문에 많은 보안 문제를 가지고 있다. Ad-hoc 네트워크에서 보안을 위한 연구 영역은 다음과 같은 것들이 있다[4].

- Key management : 인프라가 없는 상황에서 어떻게 키를 관리하고 분배할 것인가?
- Secure routing : DoS를 포함하는 잠재적인 공격에 강한 라우팅 프로토콜을 어떻게 만들 것인가?
- Intrusion detection : 네트워크에 침투를 시도하는 침입자를 어떻게 발견할 것인가?
- Selfishness : Misbehave를 하는 노드들을 어떻게 피할 것인가?

2.2.2 안전한 라우팅

Ad-Hoc 네트워크에서 안전한 라우팅에 관한 연구는 ARAN[5], Ariadne[6], SAR[7] 등에서 연구되었다. ARAN 프로토콜은 인증과 부인방지를 위해 인증서를 이용한다. 이 프로토콜은 공개키 방식의 서명과 인증서로 인증, 메시지 무결성, 부인방지 등을 제공할 수 있으나, 라우팅 테이블 목록을 하나씩 더 유지하여야 하므로 많은 비용이 요구된다. Ariaden 프로토콜은 오직 해쉬함수와 같은 대칭키 암호만을 이용하여 공격을 방어하는 방식이다. 이 프로토콜은 대칭키 암호로 계산량을 줄이나, 지나온 모든 경로들을 다 기록하여한다. SAR은 안전한 라우팅을 결정하는 신뢰 레벨을 이용하여 만든다. 이 프로토콜은 같은 신뢰 레벨을 가진 노들에게만 패킷을 전달하므로, 안전하게 패킷을 전달 할 수 있으나, 신뢰 레벨에서 요구하는 보안 사항을 만족하는 경로와 노드들이 없으면, SAR은 네트워크가 연결되어 있더라도 경로 찾기를 실패한다. 그림 3은 일반적인 안전한 라우팅에 관한 흐름을 보인다.

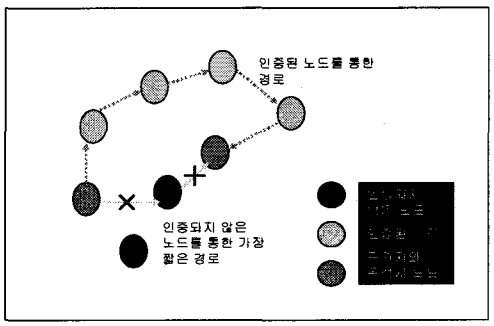

그림 3. 안전한 라우팅

3. 안전한 라우팅을 위한 인증 프로토콜

무선 매체를 통한 통신은 신호인터페이스, 전파방

해, 도청, 왜곡에 영향 받기 쉽다. 침입자는 민감한 라우팅 정보 혹은 전파방해와 라우팅 정보의 전파 혹은 나쁜 인터럽트정보와 라우터의 조작에 의한 왜곡을 쉽게 도청한다. 라우팅 프로토콜은 이런 문제를 해결하기 위해 라우터들간에 신뢰성을 높이기 위해 인증을 해야 한다.

3.1 인증 모델

논문에서 제안하는 환경은 컨퍼런스 환경으로 네트워크의 모든 노드들은 전체가 공유하는 공유키를 가지고 있으며, 또한 자신의 공개/비밀키 쌍을 가지고 있다고 가정한다. 제한하는 프로토콜은 AODV [8]에 기반하여 전개한다. 그림 2는 논문에서 적용하는 AODV의 경로 탐색 과정을 보인다.

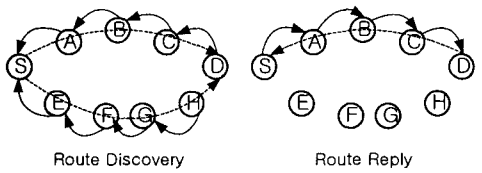

그림 2. 경로 탐색

프로토콜의 메시지에서 RREQ와 RREP는 패킷 유형 식별자이고, IP_X는 근원지 주소와 목적지 주소, ID_X는 전송하는 노드의 ID, t는 타임스탬프, r은 난수, k는 공유키 이다. 또한 Sig_X는 X의 서명을 나타내고, H는 해쉬함수를 나타낸다.

3.2 인증 프로토콜

근원지 노드 S가 목적지 노드 D로 라우팅을 할 경우 제안한 인증 프로토콜은 경로 요청과 경로 응답 과정으로 이루어진다. 전체적인 프로토콜 흐름을 보면 그림 4와 같다.

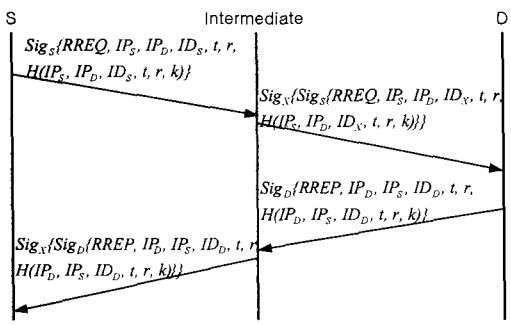

그림 4. 프로토콜 흐름도

3.2.1 경로 요청 과정

근원지 노드 S는 루트 요청을 위해 RREQ메시지를 이웃 노드들에게 브로드캐스트함으로써 목적지 D에 대한 경로 설정을 시작한다.

S -> A : $Sig_S\{RREQ, IP_S, IP_D, ID_S, t, r, H(IP_S, IP_D, ID_S, t, r, k)\}$
A -> B : $Sig_A\{Sig_S\{RREQ, IP_S, IP_D, ID_A, t, r, H(IP_S, IP_D, ID_A, t, r, k)\}\}$
B -> C : $Sig_B\{Sig_S\{RREQ, IP_S, IP_D, ID_B, t, r, H(IP_S, IP_D, ID_B, t, r, k)\}\}$
C -> D : $Sig_C\{Sig_S\{RREQ, IP_S, IP_D, ID_C, t, r, H(IP_S, IP_D, ID_C, t, r, k)\}\}$

메시지들은 노드의 메시지로 서명되어 있다. 노드는 경로 설정을 할 때마다 난수 값을 단순하게 증가시킨다. 그러면 노드들은 가장 최근의 난수 값을 타임스탬프와 함께 저장한다.

각각의 노드들은 자신이 어느 이웃 노드로부터 메시지를 받았는지 기록한다. 그 다음 받은 메시지를 자신의 개인키로 서명해 자신의 이웃 노드들에게 브로드캐스트 한다. 노드들은 (r, ID_X) 쌍을 비교하여 예전에 이미 받았던 메시지들은 전송하지 않는다. 노드 A의 이웃 노드 B가 브로드캐스트를 받으면 메시지의 서명을 검증한 후 이전 노드 A의 서명을 제거한 후, 자신의 개인키로 서명한 다음 이웃 노드에게 RREQ 메시지를 다시 브로트캐스트 한다.

노드들 간에 이와 같은 과정을 거친 후, 목적지 D는 RREQ 메시지를 받게 되고, 첫 번째로 받은 RREQ 메시지와 난수값에 대해 응답을 하게 된다.

3.2.2 경로 응답 과정

목적지는 근원지에게 반대로 RREP 메시지를 유니케스트 한다.

D -> C : $Sig_D\{RREP, IP_D, IP_S, ID_D, t, r, H(IP_D, IP_S, ID_D, t, r, k)\}$
C -> B : $Sig_C\{Sig_D\{RREP, IP_D, IP_S, ID_C, t, r, H(IP_D, IP_S, ID_C, t, r, k)\}\}$
B -> A : $Sig_B\{Sig_D\{RREP, IP_D, IP_S, ID_B, t, r, H(IP_D, IP_S, ID_B, t, r, k)\}\}$
A -> S : $Sig_A\{Sig_D\{RREP, IP_D, IP_S, ID_A, t, r, H(IP_D, IP_S, ID_A, t, r, k)\}\}$

RREP 메시지를 받은 노드들은 자신에게 RREQ 메시지를 보냈던 전 노드에게 RREP 메시지를 역으로 보내준다. 송신자는 메시지에 서명을 한다. 노드 C는 전송 받은 메시지의 서명을 검증한 후, 이전 노드 D의 서명을 제거한 후 자신의 개인키로 서명하여 노드 B에 전송한다. 각 노드들은 RREP 메시지를 근원지 노드 S로 전송하면서 전 노드의 서명을 검증한다. 이러한 과정을 거침으로써 악의적인 노드들이 X의 메시지를 위장하거나 재전송하는 공격을 막을 수 있다.

근원지 노드는 RREP 메시지를 받으면 목적지에서 돌아온 난수 값과 목적지의 서명이 정확한지를 검증한다. 오직 목적지 노드만이 RREP 메시지에 대한 응답을 할 수 있을 뿐, 목적지에 대한 경로를 알고 있는 다른 노드들은 응답을 할 수 없다.

4. 안전성 분석

Ad-Hoc 네트워크에서 안전한 라우팅을 구축하기 위해서는 Ad-Hoc 네트워크의 특성을 잘 이용하여야 한다. Ad-Hoc 네트워크를 위한 라우팅 프로토콜을 동적으로 변화하는 위상을 수용하기 위해 과거의 라우팅 정보를 다루어야만 한다. 타협된 노드에 의해 잘못된 라우팅 정보를 생성하는 것은 과거의 라우팅 정보로 간주된다. 라우팅 프로토콜이 정당하지 않은 노드에 의해 결함을 가지고 있다는 것을 발견하면 결함 노드를 우회할 수 있어야 한다. 인증을 통해 라우팅 프로토콜이 결함을 가지고 있다는 것을 발견하고 대체 경로를 이용할 수 있다. 그러나 안전한 라우팅은 전송된 메시지가 항상 근원지로부터 가장 짧은 경로로 온다는 보장은 없다.

프로토콜의 난수 r과 타임스탬프 t는 재전송 공격(replay attack)을 막는다. 경로 요청 단계에서 노드들은 메시지를 자신의 서명키로 서명한 다음 자신의 이웃 노드들에게 전송한다. 이러한 서명을 함으로써 경로를 변경하거나 루프(loop)를 생성하는 spoofing 공격을 막을 수 있다. 또한 경로 응답 단계에서 각 노드들은 RREP 메시지를 근원지로 보내면서 전 노드의 서명을 검사한다. 이러한 과정을 거침으로써 악의적인 노드들이 X의 메시지를 위장(impersonation)하거나 재전송 하는 공격을 막을 수 있다. 프로토콜의 해쉬 함수는 해쉬값을 비교하여 통신하는 상대 노드가 신뢰할 수 있는 노드인지를 인증하고, 메시지 무결성을 보호하며, 서명을 통해 부인 방지를 제공할 수 있다.

5. 결론 및 향후 연구

Ad-Hoc 네트워크는 기존 통신 인프라에 의존하지 않고, 신속하게 통신망을 구성할 수 있으며 단말기 이동에 빨리 적응을 할 수 있는 장점을 가지는 통신망이다. 그러나, Ad-Hoc 네트워크는 무선 네트워크의 취약성과 잦은 위상 변화로 인해 다양한 형태의 공격을 당하기 쉽다. 본 논문에서는 해쉬 함수와 디지털 서명을 사용하여 Ad-Hoc 네트워크에서 노드를 인증하여 라우팅 설정에 안정성을 제공한다.

그러나 제안한 프로토콜은 안전성을 높일 수는 있으나, 안전하지 않은 라우팅 프로토콜에 비해 오버헤드가 커질 수 있으며, 적용 환경이 제한되어 있다. 따라서 라우팅 설정에 안전성을 제공하면서도 오버헤드가 적고 좀 더 광범위한 환경에 적합한 라우팅 프로토콜에 관한 연구가 향후 과제이다.

참고문헌

[1] C-K Toh, "Ad Hoc Mobile Wireless Networks", Prentice Hall PTR 2002.

[2] Charles E. Perkins, "AD HOC NETWORKING", Addison Wesely 2000.

[3] Lidong Zhou and Zygmunt J. Haas, "Securing Ad Hoc Networks", IEEE Network Magazine, December 1999.

[4] Jean-Pierre Hubaux, "Security of Wireless Ad Hoc Networks", Working Session on Security in Ad Hoc Networks. June 12, 2002

[5] Bridget Dahill, Brian Neil Vevine, Elizabeth Royer, Clay Shields, "A Secure Routing Protocol for Ad Hoc Networks", August 28, 2001

[6] Yih-Chun Hu, Adran Perrig, David B. Johnson, "Ariadne: A Secure On-Demand Routing Protocol for Ad hoc Networks", MobiCom 2002, September 23-26, 2002.

[7] S. Yi, P. Naldurg, and R. Kravets, "Security-Aware Ad Hoc Routing for Wireless Networks", UIUCDCS-R-2001-2241, August 2001.

[8] C. E. Perkins and E. M. Royer, "AD-hoc On-Demand Distance Vector Routing", Proc. 2nd IEEE Wksp. Mobile Comp. Sys. and Apps., Pages 90-100, February 1999.