Ad hoc Network에서 라우팅 프로토콜을 위한 보안 메커니즘에 관한 연구

양환석, 김종민, 위승정, 최길환, 이웅기
조선대학교 전산통계학과

A Study on Security Mechanism for Routing Protocol in Ad hoc Network

Hwan-Seok Yang, Jong-Min Kim, Seung-jung Wi, Kil-Hwan Choi, Woong-Ki Lee
Dept. of Computer Science and Statistics, Chosun University

요 약

Ad hoc network는 유선 백본 없이 이동 노드들로만 구성된 네트워크로서 이동 노드들의 움직임이 빈번히 발생하기 때문에 네트워크의 안정성을 유지하기가 어렵다. 또한 중앙 집중화된 보안 기반구조가 아니기 때문에 보안 공격을 받기가 쉽고 노드들이 쉽게 손상될 수 있다. 기존의 보안 방법 중의 하나인 threshold cryptography는 키의 유지와 분배를 위한 효율적인 구조를 제공하였으나 라우팅의 오버헤드가 증가하였고, 네트워크 전역의 트래픽이 증가되었다. 게다가 서비스 거부 공격과 wormhole과 같은 공격은 ARP 또는 IP spoofing을 통하여 쉽게 받을 수 있다. 본 논문에서는 threshold cryptography에 의해 야기되는 오버헤드를 줄이고 노드간의 인증된 패킷 전달을 돕기 위한 새로운 접근 방법을 제안한다.

1. 서론

Ad hoc network를 구성하는 노드들은 제한된 무선 전송 범위 때문에 서로에게 패킷 전송을 도와준다. Ad hoc network에서 어떤 소스 노드로 부터 목적지 노드까지의 multi-hop 경로를 생성하기 위해 패킷을 전달해주는 많은 중간 노드가 필요하다. 그리고 배터리를 사용하므로 에너지의 공급이 일정하지 않다는 특성을 갖는다. 그리고 Ad hoc network는 중앙식 관리나 기지국 같은 고정된 네트워크 infrastructure가 필요하지 않기 때문에 빠르고 낮은 비용으로 네트워크를 구성할 수 있는 장점이 있다. 그러나 이러한 특징이 보안상에 커다란 문제를 야기하는 이유가 된다. 이러한 infrastructure의 부재는 신뢰할 수 있는 노드와 신뢰할 수 없는 노드의 구별을 방해하게 된다. 그리고 Ad hoc network의 또 다른 보안에 취약점은 노드간의 무선 링크이다. 무선 링크는 DoS, 정보 누출, 도청, 방해와 같은 공격에 취약하기 때문이다[2].

Ad hoc network에서의 보안 문제는 수십 년에 걸쳐 광범위하게 연구되어 왔다. 그러한 연구들 중에 키 관리와 비대칭키 분배는 적당한 방법으로 평가되어 왔다[5]. 그러나 라우팅 프로토콜 자체의 보안에 대해서는 상대적으로 적은 연구가 이루어져왔다. Zhou는 ad hoc network를 위한 공개키 구조를 제안하였다[1]. 그리고 Hubaux는 신뢰할 수 있는 노드(trusted party)가 없는 자가 구성 인증 시스템을 제안하였다[3][4]. Kong는 비대칭 메커니즘을 이용한 threshold cryptography 서명을 제안하였다. Threshold cryptography는 공개키와 비밀키 쌍을 이용하는데, 공개키는 한 개만 존재하며, 반면에 비밀키는 그룹을 이루고 있는 노드들에게 일부분씩 공유가 된다. 그러나 threshold cryptography는 라우팅의 오버헤드가 증가되고 네트워크 전역의 트래픽 증가를 초래하였다.

Ad hoc network에서 라우팅 프로토콜의 역할은 multi-hop 경로를 중간 노드들이 알 수 있도록 해주는 것으로서 가장 대표적인 라우팅 프로토콜 중에 on demand 라우팅 프로토콜이 있다. On demand 라우팅 프로토콜의 특징 중의 하나는 경로 발견과 경로 유지가 분리되어 있다는 것이다. 경로 발견을 하기 위해서는 경로 요구 패킷을 방송하고 이에 대한 응답을 수집하는 것이다. 이러한 패킷 방송 메커니즘은 자신 스스로 보안상의 커다란 허점을 노출하는 것이다.

본 논문에서는 *threshold cryptography*를 조합한 경로 발견 프로토콜을 이용하여 라우팅 프로토콜에서의 보안 문제에 대한 새로운 방법을 제안하였다.

본 논문의 구성은 다음과 같다. 2장에서는 ad hoc network에 존재하는 공격의 유형을 살펴보고, 3장에서는 제안한 방법에 대하여 설명하였다. 4장에서는 제안한 방법의 성능을 평가하고 마지막으로 5장에서는 결론을 맺는다.

2. Ad hoc network에서의 공격유형

Ad hoc network에 대한 공격 유형은 크게 두 가지로 나누어 볼 수 있다. 첫째로, ad hoc network의 기본적인 메커니즘인 라우팅에 대한 공격이다. 그리고 둘째로 보안 메커니즘이나 키 관리 메커니즘에 대한 공격이다.

서비스 거부 공격은 중앙 집중화된 자원을 오버플로우시켜 더 이상의 정상적인 운영을 못하게 하거나 고장을 일으키는 것이다. 배터리 소모 공격이나 전파 방해는 다른 노드나 사용자에게 서비스 거부 공격을 가할 수 있는 방법들이 된다. 만일 공격자가 충분한 계산 능력과 대역폭을 가지고 있다면, 소규모의 ad hoc network는 고장 나거나 쉽게 폭주를 일으킬 수 있게 된다.

Impersonation 공격은 신뢰된 다른 노드들 몰래 네트워크에 합류하여 잘못된 라우팅 정보를 내보내고 다른 신뢰된 노드로 가장하여 관리자 권한을 획득하고 시스템에 접근을 하는 것이다. 이는 자신을 이웃 노드로 가장하여 잘못된 명령을 내리거나 다른 노드의 상태정보를 얻을 수 있게 된다. 이러한 공격은 강력한 인증 메커니즘을 사용함으로써 피할 수 있다. 그리고 또 다른 공격으로는 라우팅 프로토콜에 의해 발생되는 패킷을 공격하는 것이다. 이러한 공격은 정보의 변경, 중요한 데이터의 폭로, 다른 프로토콜 엔티티로부터 적법한 서비스의 절도나 프로토콜 엔티티의 네트워크 서비스의 거부를 일으킬 수 있다.

라우팅에 대한 공격으로는 잘못된 라우팅 정보를 다른 노드들에게 방송함으로써 이루어진다. Ad hoc network는 동적으로 변화하기 때문에 실제 공격과 토폴로지의 변경을 구별 짓는 일이 매우 힘들다. 공격자들은 특정한 노드에 라우팅 요구가 빈번하게 발생하면, 그 노드가 네트워크 내에서 중요한 기능을 하는 노드라 추측하여 공격을 할 것이고, 이로 인해 네트워크가 마비되는 일이 발생할 수도 있게 된다.

3. 제안한 방법

전형적인 키 기반 보안 구조는 대칭 암호나 비대칭 암호에 대하여 키의 유지가 신뢰성 있게 유지되어야만 한다. 그러나 ad hoc network에서의 노드들은 에너지 공급의 한계를 가지고 있고 의도적인 공격에 취약하게 된다.

Threshold cryptography에서 노드들은 다른 인증된 노드들로부터 완전한 서명을 구축하기 위해 충분한 부분적인 서명을 수신해야만 한다. 노드들은 인증을 위해 인증 요구 신호(CREQ)를 송신하고 이를 수신한 다른 노드들은 자신이 인증 요구 신호에 대해 처리를 해줄 수 있다면 부분적인 서명(CREP)을 보내줄 것이다. 인증 요구 신호를 송신한 노드는 일정한 시간이내에 충분한 응답을 수신한다면 유효한 서명을 만들기 위해 CREP를 모으게 된다. 이와 비슷한 방법으로, 경로 발견 프로토콜 역시 RREQ를 송신하고 이를 수신한 다른 노드들로부터 수신한 RREP를 모으게 된다. 이 두 가지의 차이점은 응답 메커니즘에 있다. RREQ 패킷은 목적지 노드가 RREP를 송신하고 노드들은 일정 시간이내에 반대경로로 응답을 전달한다. 반대로 CREQ는 여러 개의 노드들로부터 부분적인 서명을 받는 것이 필요하다. 그러므로 자격이 있는 노드들은 CREP를 갖는 응답을 하는 것이 아니라 다른 노드들에게 CREQ를 전달해 준다. 다양한 주소 지정 방법은 멀티캐스트 주소와 같이 여러 노드들에 도달할 수 있도록 사용하곤 한다. 그럼에도 불구하고, 완전한 서명의 재구성의 목적은 어떤 인증된 목적지 노드로부터 서비스의 요구를 확인하기 위해 사용되어진다. 클라이언트가 찾는 서비스가 재구성된 완전한 서명으로 성공적으로 이루어졌다 할지라도 여전히 목적지 노드까지의 경로를 얻기 위해 RREQ 송신이 필요하다.

3.1 패킷의 조합

본 논문에서는 네트워크를 구성하는 노드들을 서명 확인을 할 수 있는 노드(AN, Authority Node)와 인증을 위해 요구 신호를 송신하는 노드(RN, Request Node)로 구분하였다. 본 논문에서 제안하는 방법은 threshold cryptography에 의해 야기되는 오버헤드를 줄이고 RN이 AN들로부터 충분히 부분적인 서명을 쉽게 받을 수 있도록 하는 것이다. RN들은 자신이 인증이 필요할 때마다 CREQ를 송신한다. CREQ가 타임아웃이 되기 전에 RN들은 충분한 부분 서명을 모으기 위해 자신에게 오는 CREP 신호를 모으고 그 사이에 다른 RN들로부터 송신된 CREQ 신호의 전달을

도와준다. 반대로, AN들은 CREQ 신호에 주의를 기울인다. AN이 CREQ를 수신할 때, CREQ 신호가 유효한지 여부를 검사한다. 만약 이 신호가 유효하다면 AN는 자신의 부분 서명을 소스 노드에게 CREP 신호로 보내준다. 그리고 만약에 CREQ가 타임아웃이 되지 않았다면 CREQ를 포워드 하게 된다. 만약 CREQ가 유효하지 않거나 또는 타임아웃이 되었다면 AN는 수신한 패킷을 삭제하게 된다. RN이 완전한 서명을 성공적으로 재 수집한다면 서비스를 위해 목적지 AN과 연결을 시도할 것이다. RN은 경로 안으로 RREP를 끼워 넣어 또 다른 방송을 시작하는 것이 필요하게 된다. RREQ는 인증을 위한 CREP가 자신의 패킷 안에 유사한 정보를 가지고 있기 때문에 패킷안의 내용을 고려해 보아야 한다. 따라서 RN은 CREP에 이미 충분한 정보를 가지고 있기 때문에 경로를 찾기 위해 두 번째 플러딩을 할 필요가 없게 되는 것이다.

3.2 노드간의 경로 보호

키 분배와 유지는 좋은 비밀 공유 구조를 통해서 이루어져야만 한다. 그러나 악의 있는 노드들은 DoS를 이용해 RN 또는 AN을 목표로 삼을 수 있다. ARP poisoning에서 공격은 목적지 AN에 관한 위조된 ARP 정보를 송신함으로써 실행될 수 있다.

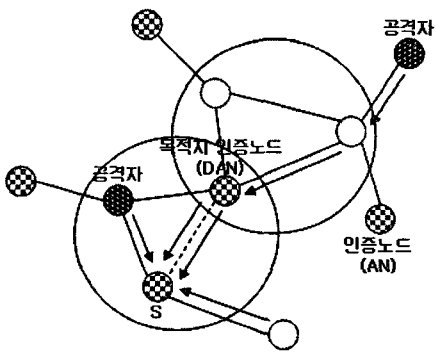

그림 1. ARP 변질을 통한 DoS 공격

그림 1에서 보이는 것처럼 의심스러운 노드는 소스 노드를 속이기 위해 자신의 MAC 주소를 갖는 RREP를 송신함으로써 다양한 공격을 할 수 있다. ARP poisoning을 막는 가장 일반적인 방법은 각각의 노드에서 정적 ARP 테이블을 이용하는 것이다. 이 방법의 단점은 주소 변환이 어렵다는 것이다. 성능 향상의 중요한 문제는 그림 2에서 보인 것처럼 응답 신호에 의해 야기되는 broadcast storm을 제거하는 것이다. 잘 설계된 정적 ARP 테이블은 변환할 수 있는 IP 주소와 불필요한 방송을 제거하는 일이 아직도 남아있다.

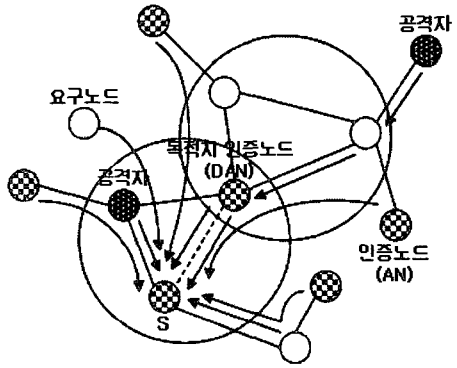

그림 2. 응답 방송 폭주

그룹 서명 구조는 공유된 보안을 막을 수는 있으나 자신의 라우팅 정보를 보호할 수는 없다. 노드 S의 똑같은 전파 전송 범위 내에서 S와 AN의 거리가 S와 DAN의 거리보다 짧다면 AN은 RREQ 메시지에 대한 응답을 하지 않을 것이다.

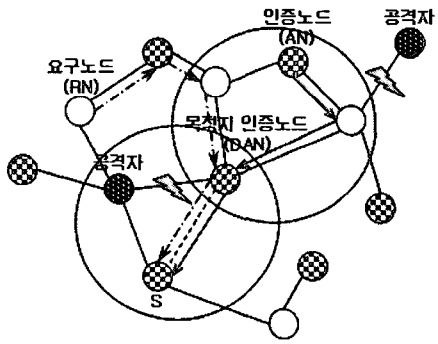

그림 3. 분산된 응답

그림 3에서는 침입자가 메시지를 위조하기 전에 부분적인 서명을 얻기 위해 AN으로부터 인증이 필요하다. 노드 S와 침입자 거리가 노드 S와 DAN의 거리보다 커야하고 같은 전파 전송 범위 내에 위치하게 되면, DAN을 향한 DoS 공격은 실패하게 될 것이다. 왜냐하면, DAN에 패킷이 도착할 때, 패킷은 DSR 알고리즘 자체에 의해 폐기되기 때문이다. 그리고 RREQ 메시지가 DAN에게 도착하였을 때 서명을 요구해야만 한다. DAN에 RREQ에 대해 서명을 한 후에, 이 패킷들은 서명 확인을 위해 다른 AN을 통과

할 수 있어야 하고 소스 노드 S에게 RREP를 송신해야 한다. 그리고 노드들로부터의 응답 중에 DAN을 포함하고 있는 경로를 선택하면 된다. 이렇게 함으로써 네트워크 전역의 오버헤드를 줄일 수가 있게 된다. 그리고 모든 응답들이 DAN을 통하여 되돌아오기 때문에 응답 시간은 보다 더 균등하게 된다. 그리고 노드들이 부분적인 서명을 수집하는 동안 노드들 간의 경로를 보호할 수 있게 된다.

4. 실험 및 결과

이 장에서는 본 논문에서 제안한 방법은 OPNET Modeler MANET 모듈을 이용하여 성능 평가하였다. 성능 평가의 목표는 노드들의 서로 다른 이동 속도와 ARP 캐시 크기에 따른 성공 요구 비율의 성능 평가이다.

성공 요구 비율은 성공적인 요구 수를 전체 요구 수로 나눈 값으로 표시한다. 실험에 사용한 전체 노드의 수는 40개이며 그 중에 인증 노드는 15개, 나머지 노드는 요구노드이고 네트워크의 크기는 400m × 400m이다. 각 요구 노드는 평균 100초 동안에 인증 노드들로부터 서명을 모으기 위해 연결을 시도한다. 전체 시뮬레이션 시간은 600초가 주어졌다.

그림 4는 캐시 크기에 따른 이동 노드와 고정 노드 간의 성공 요구 비율을 보여주고 있으며, 그림 5는 노드들의 이동 속도에 따른 성공 비율을 보여주고 있다.

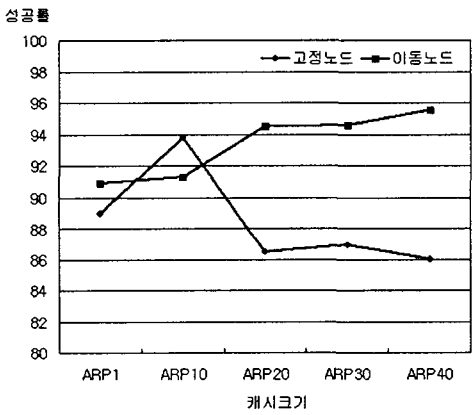

그림 4. 캐시 크기에 따른 성공률

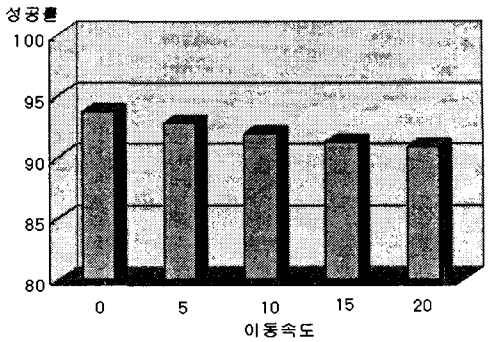

그림 5. 이동속도에 따른 성공률

5. 결론

본 논문에서는 threshold cryptography에 의해 야기되는 오버헤드를 줄이고 인증된 패킷의 전달을 돕기 위한 방법을 제안하였다. 그리고 802.11b에서는 주소 구조를 이용하고 있기 때문에 ARP cache poisoning을 피할 수 있는 방법이 없다. 본 논문에서는 ad hoc network를 구성하는 노드들이 정적 ARP 테이블을 이용하여 ARP cache poisoning을 피할 수 있는 방법과 다양한 공격으로부터 노드들 간의 경로를 보호할 수 있는 방법을 보였다.

향후 연구로는 기존의 제안된 여러 가지 라우팅 프로토콜에서의 구현에 대한 연구가 이루어져야 할 것이다.

[참고문헌]

[1] L. Zhou and J. Z. Hass, "Securing Ad Hoc Networks," IEEE Network Magazine, vol. 13, no.6, 1999.

[2] A. Shamir, "How to Share a Secret," CACM, 22(11):612-613, 1979.

[3] S. Capkun, L. Buttyan and J. P. Hubaux, "Self-Organized Public-Key Management for Mobile Ad Hoc Networks," ACM International Workshop on Wireless Security, 2002.

[4] L. Buttyan and J. P. Hubaux, "Stimulating Cooperation in Self-Organizing Mobile Ad Hoc Networks," to appear in ACM, vol. 8 No 5, October 2003.

[5] C. Cater, S. Yi, and R. Kravets, "ARP Considered Harmful: Manycast Transactions in Ad Hoc Networks," IEEE WCNC 2003.