제18회 한국정보처리학회 추계학술발표대회 논문집 제9권 제2호 (2002.11)

이동 Ad Hoc 네트워크에서의 보안 취약점에 대한 연구

심학섭, 김태윤
고려대학교 컴퓨터학과
e-mail:100tpig@netlab.korea.ac.kr

A Study for Vulnerabilities of Security in Mobile Ad Hoc Networks

Hak-Sub Sim, Tai-Yun Kim
Dept. of Computer Science & Engineering, Korea University

요 약

무선 통신은 제한된 대역과 단말 기능에 있어서의 제약으로 유선 환경에서 제공받는 서비스를 수용하는데 문제가 된다. 이러한 문제의 해소 방안으로 무선 접속 기능을 향상하기 위한 근거리 사설 무선망인 ad hoc 네트워크가 최근 주목을 받고 있다.

ad hoc 네트워크는 많은 장점들이 있으나 그에 따른 문제점들 또한 많다. ad hoc 네트워크의 특징으로 인하여 기존의 인프라 네트워크에 적용되던 메커니즘들이 적용되기가 어렵다. 특히 무선 연결에 따른 보안 취약점과 중앙 통제를 위한 고정된 제어장치가 없어 인증과 키 관리가 문제가 되고 있다. 따라서 본 논문에서는 ad hoc 네트워크 환경의 특징으로 인하여 발생하는 문제점들과 보안상의 취약점들을 살펴본다.

1. 서론

통신 기기의 발전과 다양한 개인 휴대 단말의 등장은 통신과 컴퓨팅 기능의 자연스러운 통합을 요구하고 있으며, 단순한 기기의 통합뿐만이 아니라 운용 환경과 서비스의 통합을 포함한다. 이러한 컴퓨터 계산 능력과 통신 기술의 급격한 발전으로 인하여 가까운 미래에는 모든 환경이 컴퓨터를 이용한 통신 환경으로 바뀔 것이다.

무선 통신은 이러한 통합의 모티브가 되지만 반대로 제한된 통신 자원으로 인한 제약으로 작용하고 있다. 제한된 대역과 단말 기능에 있어서의 제약은 유선 환경에서 제공받는 멀티미디어 통신 서비스를 수용하는데 문제가 된다. 이러한 문제의 해소 방안으로 무선 접속 기능을 향상하기 위한 근거리 사설 무선망이 최근 주목을 받고 있다. 이는 공용 주파수 대역에서 보편화된 저가의 장비로 유무선 통신 인프라 접속과 기기 상호간의 통신 연결을 주목적으로 하는 ad hoc 네트워크를 기반으로 한다.

ad hoc 네트워크는 중앙 집중화된 관리나 표준화된 지원 서비스의 도움 없이 임시망을 구성하는 무선 이동 호스트들의 집합이다. 이러한 망은 백본 호스트나 다른 이동 호스트로의 연결을 제공하기 위한 고정된 제어 장치를 갖지 않으며, 각 이동 호스트가 라우터로 동작하여 이동 호스트로부터의 패킷을 다른 이동 호스트로 전달한다.

ad hoc 체계는 자기 재구성, 트래픽 분산, 부하 조절 등의 많은 장점들이 있으나, 그에 따른 문제점들도 많다. 네트워크의 위상(topology)이 계속 변하므로 패킷 전달을 위해 경로를 설정하기가 어렵고, 이러한 환경에서 QoS(Quality of Service)를 보장하는 것 또한 어렵다. 대부분의 이동 단말들은 크기가 작고 가벼운 만큼 전원의 보유량이 적다. 따라서 자신의 전원 소비량에 따라 통신에 관련된 기능들이 제약을 받는다.

특히 무선 연결에 따른 취약점이 ad hoc 환경에서는 더욱 두드러져 보안에 문제가 생긴다. ad hoc 네트워크 내의 노드들은 언제나 공격에 노출이 되어 있어 안전한 보안 메커니즘이 필요하다. 게다가 중앙의 통제가 없이 분산된 작업을 수행하므로 인증과 키 관리에 기존의 방법과는 다른 방법이 필요하다.

따라서 본 논문에서는 ad hoc 네트워크 환경의 특징으로 인해 야기되는 보안의 문제점들을 살펴보고자 한다.

본 논문의 구성은 다음과 같다. 2장에서는 네트워크를 안전하게 보호하기 위한 기본적인 보안 사항들을 서술하였고, 3장에서는 ad hoc 네트워크의 특징들을 살펴본다. 4장에서 ad hoc 네트워크의 취약점을 다루고 5장부터 7장까지는 ad hoc 네트워크의 특징으로 인하여 생기는 침입 탐지, 라우팅, 키 관리의 문제점들을 설명한다. 마지막으로 8장에서 결론과 앞으로의 방향을 제시한다.

2. 기본적인 보안 요소

네트워크를 안전하게 보호하기 위해서는 유효성, 기밀성, 무결성, 인증, 부인방지 등과 같은 사항들을 고려해야 한다[1].

- 유효성(Availability)

언제든지 원하는 네트워크 서비스가 가능해야 한다. 악의적인 목적을 가진 사용자가 통신을 하는 인터페이스에 재밍(jamming) 신호를 가하거나 라우팅 프로토콜에 손상을 입힘으로써 서비스를 방해할 수 있다. 보다 더 강력한 공격으로 특정 노드의 전원을 공격하는 방법도 존재한다. 공격을 당한 노드는 전원을 다 소모해 결과적으로 네트워크 서비스를 받지 못하게 된다[2].

- 기밀성(Confidentiality)

허가되지 않은 사용자에게 정보가 유출되어서는 안된다. 군사 정보와 같은 민감한 정보의 전송시에는 기밀성이 필요하다. 라우팅 정보 또한 기밀성이 유지되어야 한다. 전쟁시 자신의 위치에 대한 정보는 적에게 유용한 정보가 될 수 있다.

- 무결성(Integrity)

전송된 메시지가 훼손되지 않았음을 보장해야 한다. 악의적인 목적의 공격이나 전파 전달시의 오류로 인하여 메시지가 훼손될 수 있다.

- 인증(Authentication)

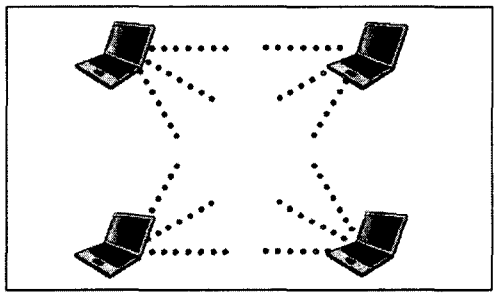
통신하고자 하는 상대방 개체의 신원을 확인해야 한다. 인증 절차가 없으면 악의적인 목적의 사용자가 정당한 노드로서 행동할 수 있다. 그로 인하여 중요한 정보에 대한 허가되지 않은 접근이 가능해지고 다른 노드들과의 동작을 방해할 수 있다.

- 부인방지(Non-repudiation)

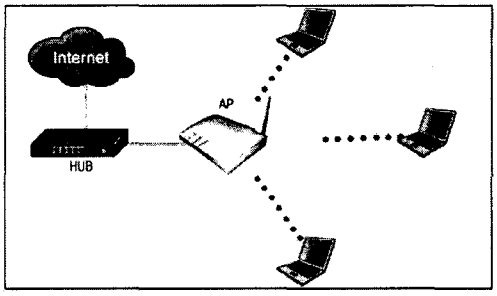
자신이 보낸 메시지에 대해 부인할 수 없도록 하는 것으로, 손상된(compromised) 노드를 발견하고 격리할 때 유용하게 사용된다. 예를 들어, 노드 A가 노드 B로부터 잘못된 메시지를 받았을 경우, 노드 A는 이 메시지를 이용해 다른 노드들에게 노드 B가 손상되었음을 알릴 수 있다.

3. MANET(Mobile Ad hoc Network)의 특징

MANET은 무선으로 연결된 라우터 또는 호스트들로 이루어진 시스템으로, 모든 라우터와 호스트들은 임의로 이동하고 멋대로 구성된다. 따라서 네트워크의 위상은 빠르게 변화하고 예측할 수가 없다. 그러한 네트워크는 독립적으로 또는 인터넷에 연결된 형태로도 작동할 수 있다. 또한 <그림 1>, <그림 2>에서 나타나듯이, ad hoc 네트워크는 인프라 네트워크와는 달리 중앙 통제를 위한 고정된 제어장치를 갖지 않는다.



<그림 1> ad hoc 네트워크



<그림 2> 인프라 네트워크

MANET은 다음과 같은 특징들을 갖는다[3].

- 각각의 이동 단말은 호스트나 라우터의 기능을 수행할 수 있다.
- 네트워크 동작에 대한 중앙 제어가 없으므로 네트워크 제어와 관리를 단말들이 맞는다.
- 직접 전송할 수 있는 범위를 벗어난 목적지까지

데이터 패킷 전송은 여러 중간 노드들을 거쳐 전송된다.

- 노드들이 이동하므로 네트워크 위상은 빠르게 변화하고 단말들간의 연결도 시간이 지남에 따라 변화한다.
- 무선 연결의 특징인 높은 비트 에러율이 MANET에서는 더욱 심하다.
- MANET에서의 노드들은 크기가 작고 가벼운 만큼 CPU 처리 능력이 떨어지고 메모리 크기가 작으며 전원 보유량이 낮다.

4. MANET의 취약점

이러한 ad hoc 네트워크의 두드러진 특징으로 인하여 보안 요건을 만족하기에는 많은 문제들이 존재한다[4].

첫째, 무선 연결을 사용함으로써 ad hoc 네트워크는 도청(eavesdropping), 위장(impersonation), 메시지 왜곡 등의 공격에 취약하다. 공격자는 비밀 정보를 도청하거나 잘못된 메시지를 추가하고 변경할 수 있을 뿐만 아니라 정당한 노드로 위장할 수도 있다.

둘째, 통신 상태가 좋지 않은 물리적인 보호가 취약한 환경에서 노드들의 로밍(roaming)은 무시할 수 없을 정도의 비율로 손상이 발생한다. 유선 네트워크와 달리 ad hoc 네트워크의 노드들은 포획되거나 손상될 수 있는 위험에 항상 노출되어 있다. 따라서 외부에서의 악의적인 공격뿐만 아니라 네트워크 내부의 손상된 노드들에 의한 공격도 고려해야 한다.

셋째, 네트워크의 위상과 구성원이 수시로 바뀌므로 ad hoc 네트워크는 동적이다. 특정 노드가 손상된 노드로서 제외됐을 경우, 노드들간의 신뢰 관계 또한 변하게 된다.

마지막으로, ad hoc 네트워크를 위한 현재의 MAC(media access control) 프로토콜들은 매우 취약하다. 예를 들어, 경쟁 기반의 메커니즘에서 노드들은 충돌 회피와 복구 등의 미리 정해진 규칙들을 따라야만 한다. ad hoc 환경에 좀 더 적합한 경쟁이 자유로운 메커니즘에서 각각의 노드는 채널의 독점적인 사용을 위해 다른 노드들과의 동의를 얻어야만 한다. 위의 두 가지의 경우에서 만약 어느 한 노드가 이러한 규칙을 지키지 않을 경우, 통신 채널의 할당이 불공평해지고 네트워크의 성능에 영향을 미치게 된다.

ad hoc 네트워크를 보호하기 위해 침입 탐지와 같은 기술들을 사용할 수 있다. 또한 라우팅과 같은 기본적인 메커니즘부터 키 관리 시스템과 같은 네트워크의 보안 메커니즘까지 보호되어야 한다..

5. MANET에서의 침입 탐지

네트워크에 대한 침입이 발생했을 때 암호화나 인증과 같은 침입 예방 기술들이 첫 번째의 방어선이 된다. 그러나 이와 같은 기술들은 침입을 줄여줄 뿐 제거하지는 못한다. 따라서 침입이 발견되면 공격의 초반에 피해를 최소한으로 줄이고 증거들을 모아 역으로 공격을 할 수 있도록 침입 탐지 기술이 같이 사용된다.

침입 탐지의 주된 동작은 사용자와 프로그램의 행동들을 관찰하는 것으로, 특히 정상적인 행동과 침입을 뚜렷하게 구분하는 것이다. 따라서 시스템이 공격을 당하고 있는지를 결정하기 위해 증거들을 수집하게 되고, 이러한 증거들은 게이트웨이와 같은 데이터가 집중되는 곳에서 수집된다..

그러나 트래픽 감시가 주로 스위치, 라우터, 게이트웨이에서 이루어지는 유선 네트워크와 달리 ad hoc 네트워크는 그러한 트래픽이 집중되는 지점이 없어 침입 탐지 기법을 적용시키기가 힘들다. 따라서 네트워크 내의 모든 노드들이 침입 탐지에 부분적으로 참여하는 방식이 필요하다[4].

6. MANET에서의 라우팅 메커니즘

ad hoc 네트워크에서 각각의 노드들은 중계기의 역할을 수행하므로 라우팅 메커니즘이 보다 더 취약하다. 예를 들어, 악의적인 목적을 가진 사용자가 거짓 라우팅 정보를 퍼트림으로써 전체적인 네트워크를 마비시킬 수 있다. 또한 몇몇 노드들은 자신의 전원 소비를 줄이기 위해 패킷 전달을 수행하지 않을 수도 있다.

라우팅 프로토콜을 위협하는 요소로서 외부의 공격자와 내부의 손상된 노드를 들 수 있다. 전자의 경우, 공격자는 라우팅 정보의 왜곡, 잘못된 라우팅 정보의 삽입, 오래된 라우팅 정보의 재사용 등 다양한 공격을 가하게 된다. 이러한 경우 비효율적인 라우팅과 재전송 등을 유발시켜 과부하를 일으키게 할 수 있고, 네트워크를 분할시킬 수도 있다. 그러나 각 노드들은 전자서명과 같은 암호학적 기법을 사용함으로써 이러한 공격으로부터 라우팅 정보를 보호할 수 있다.

반면에 손상된 노드들의 위협에 대해서는 이러한 방어책이 비효율적이다. 어느 한 라우팅 정보가 무효임이 밝혀졌을 경우, 그 정보가 손상된 노드에 의해 생성된 것인지 네트워크 위상의 변화로 인하여 무효가 된 것인지 구분하기가 어렵다.

따라서 ad hoc 네트워크 환경에서는 임의의 두 노드간에 여러 개의 경로가 존재할 수 있으므로, 라우팅 프로토콜은 손상된 노드를 우회하는 경로를 찾을 수 있어야 한다[5].

7. MANET에서의 키 관리 시스템

ad hoc 네트워크에서 보안 메커니즘을 보호하는 것은 매우 중요한 문제이다. 그 중 키 설정(establishment)이 가장 중요하고 복잡한 이슈이다. 키 설정은 키 전송(transport)과 키 합의(agreement)로 이루어진다.

키 전송은 생성하거나 가지고 있는 비밀 값을 상대방에게 안전하게 전달하는 것이다. 키 합의는 둘 또는 그 이상의 그룹이 공유하는 키를 생성하기 위해 서로의 정보를 주고받는 것으로 공유된 키는 공유한 그룹 이외에는 예측이 불가능하다. 이러한 두 방법들은 대칭/비대칭 암호 기법에 기반을 두고 있다.

대칭 키 암호는 신뢰할 수 있는 온라인 서버가 필요하므로, 비대칭 키 암호가 ad hoc 네트워크에 보다 더 적합하다고 볼 수 있다. 그러나 비대칭 키 방식은 폐기된 키의 리스트를 서버에서 유지해야하므로 이것 또한 ad hoc 네트워크 환경에 부적합하다. 게다가 상대방 노드의 신뢰할 수 있는 공개키를 얻는 방법이 결정적인 문제가 되고 있다[5].

8. 결론

본 논문에서는 ad hoc 네트워크의 특징으로 인하여 야기되는 문제점들과 특히 보안의 취약점들을 살펴보았다. 지금까지 살펴본 문제점들을 살펴보면 대략 다음과 같다.

ad hoc 네트워크는 무선으로 연결된 라우터 또는 호스트들로 이루어진 시스템으로, 모든 라우터와 호스트들은 임의로 이동하고 멋대로 구성된다. 무선 연결을 사용함으로써 에러가 많고 외부의 공격에 취약하다. 노드들은 크기가 작고 가벼운 만큼 CPU의 처리 능력이 떨어지고 전원의 보유량도 적다. 또한 전원의 소비량에 따라 기능의 제약이 따른다.

유선 네트워크와는 달리 게이트웨이나 스위치 등의 트래픽이 집중되는 지점이 없어 침입 탐지의 적용이 어렵다. 모든 노드들이 이동하므로 라우팅 정보가 수시로 변하고 사소한 라우팅 정보의 변형도 네트워크의 성능에 영향을 미친다. 또한 위상의 변화로 인하여 갱신된 라우팅 정보와 손상된 노드에 의해 생성된 라우팅 정보를 구분하기가 어렵다. 중앙 통제를 위한 고정된 제어장치가 없어 신뢰할 수 있는 공개키의 분배가 어렵다. 이러한 문제점들로 인하여 현재 ad hoc 네트워크에서는 보안을 유지하기가 어려운 실정이다.

앞으로의 연구 과제로는 이러한 ad hoc 네트워크의 보안 취약점들을 고려한 구체적인 보안 메커니즘 설계가 이루어져야 할 것이다.

참고문헌

[1] L. Zhou and Z. Haas, "Securing Ad Hoc Networks", IEEE Network, 13 (6), pp. 24-30, 1999.

[2] F. Stajano and R. Anderson, "The Resurrecting Duckling: Security Issues for Ad-hoc Wireless Networks", In Proceedings of the 7th International Workshop on Security Protocols, 1999.

[3] 김동완, 이성식, "이동 Ad Hoc 망 기술 개요", TELECOMMUNICATION REVIEW 제10권 1호, pp. 158-169, 2000.

[4] Y. Zhang and W. Lee, "Intrusion Detection in Wireless Ad-Hoc Networks", ACM MOBICOMM, pp. 275-283, 2000.

[5] J. Hubaux, L. Buttyan, and S. Capkun, "The Quest for Security in Mobile Ad Hoc Networks", ACM MobiHOC, pp. 146-155, 2001.