MANET 기반 VoIP의 침해방지에 관한 연구

윤통일* · 김영동*

*동양대학교

A Study on the VoIP Intrusion prevention over MANET

Tong-il,Yoon* · Young-Dong,Kim**

*DongYang University

E-mail : tongzx@dreamwiz.com · ydkim@dyu.ac.kr

요 약

기반 구조 시스템 없이도 모바일 단말기 노드 사이에서 이동성 보장, 무선 네트워크를 구성할 수 있는 MANET VoIP에 많은 관심을 받고 있다.
하지만 이런 편리성과 다르게 유선 네트워크 시스템보다 외부 네트워크 공격자에 의해 시스템의 접근과 변경이 쉽기 때문에 보안 문제에 큰 이슈가 되고 있다.
이 논문에서는 기본적인 웹 망에서 보안 문제를 해결하는 NAT와 방화벽(Firewall)이 MANET VoIP에서 적합한지 알아보고 이를 해결할 수 있는 기술을 제안한다.

ABSTRACT

The concern which is abundant in MANET VoIP for comprising the mobility guarantee and mobile network is received without the infrastructure system between the mobile terminal node.

However, because the access of system and border is easy, the issue which is big in the security problem becomes more than the wired network system with this convenience by the foreign network attacker differently.

In this paper, we would like to the fundamental web network, NAT and concluding the security problem technology in which Firewall can inquire on MANET VoIP and whether it is appropriate or not which can solve this is proposed.

키워드

VoIP, MANET, NAT, 방화벽(Firewall), AODV

Ⅰ. 서 론

소형화와 자가 무선 네트워크 망을 구축할 수 있는 편리한 단말기의 등장으로 인터넷은 더 이상 고정된 장소에서 사용하는 제약을 벗어나 장소와 시간에 구애받지 않고 어디서나 사용이 가능하다.

광범위한 네트워크를 사용자의 설정만으로 쉽게 구성할 수 있는 반면에 외부에서 네트워크 공격자 역시 무선 네트워크 안에서 사용자의 설정을 접근하여 정보 변경 및 수정으로 보안의 취약점을 보이고 있다.

인터넷은 IPv4 환경에서 부족한 IP주소를 할당받아 외부로부터 데이터 정보를 받게 되는데 네트워크 공격자로부터 침입을 방화벽(Firewall)과 NAT(Network Address Translation) 방법 등으로 침입을 해결할 수 있다.

IP주소를 무한으로 할당 받을 수 있는 IPv6 환경을 사용하면 보안 문제를 쉽게 해결할 수 있지만 이를 위한 전용 장비의 도입, 변경과 유지비용을 고려하면 아직까지는 대중적이지 않는다.

현재는 MANET(Mobile Ad-Hoc Networks) 기반 통신이 주축을 이루어지고 접근이 용이하기 때문에 데이터 정보 뿐만아니라 VoIP같은 실시간 음성 정보 역시 보안 위험을 노출되고 있으며 이를 예방하고 해결책이 필요하다.

본 논문은 Ⅱ장에서 NAT와 방화벽을 살펴보고, Ⅲ장에서는 MANET 기반 라우팅 프로토콜을 설명하고, Ⅳ장에서는 결론을 맺는다.

Ⅱ. 방화벽 & NAT

2.1 방화벽(Firewall)

방화벽은 외부에서 들어오는 데이터 패킷이 위험한 요소를 가지고 있다면 방화벽에서 정해진 규칙에 따라 차단하고, 유용한 패킷은 접근을 허용하여 받음으로써 내부 네트워크를 보호하는 소프트웨어 혹은 하드웨어를 말한다.

표1. 방화벽의 기능

- 접근제어(Access Control) - 인증(Authentication) - 데이터 암호화 - 로깅(Logging) & 감사추적(Auditing)

방화벽의 기능에는 외부에서 내부로 들어오는 패킷들 중 접근이 허용된 리스트를 통해 관리하는 접근제어, 아이디와 패스워드를 이용한 인증방식인 인증기법, 중요한 데이터를 암호화 기법을 사용하여 방화벽까지 전송하는 데이터 암호화, 허용되거나 차단된 접근에 대한 모든 정보(포트번호, 사용자 아이디, 사용내역 등)를 기록하여 유지하는 로깅&감사추적이 있다.[1]

표2. 방화벽 시스템의 종류

베스천 호스트	로깅과 모니터링 구현, 접근의 허용과 차단하는 일반적인 방화벽의 기능을 가지고 있다.
스크링 라우터	네트워크, 전송 계층에서 실행되며 출발지와 목적지의 IP주소와 포트 번호를 에 대한 접근제어가 가능하다.
단독-홈 게이트웨이	베스천 호스트 구조, 기본적인 방화벽의 기능을 수행한다.
이중-홈 호스트	내부 혹은 외부 네트워크의 분리된 이중-홈을 지나 서비스를 이용하는 방법으로 효율적인 트래픽을 관리할 수 있다.
스크린 호스트	이중-홈 + 스크린 라우터의 장점을 혼합한 방화벽 시스템으로 스크링 라우터에서 1차적 패킷 필터링으로 방어, 프로시와 같은 서비스로 2차 방어를 하는 기법이다.
스크린 서브넷	외부와 내부 네트워크 사이에 완충지대를 가지는 구조로 서브넷에 DMZ(Demilitarized Zone)와 방화벽이 위치한다. 외부의 침입이 어렵다

2.2 NAT(Network Address Translation)

현재 사용되고 있는 IPv4 환경에서는 공인 IP주소가 사용되고 있는 인터넷에 비해 IP 수가 많이 부족하여 외부 공격자로부터 접근이 쉽기 때문에 보안에 취약하다.

IP 수가 무한인 IPv6 환경을 사용한다면 문제를 쉽게 해결할 수 있겠지만 장비 설치와 변경의 비용이 많이 들기 때문에 대중화가 쉽게 이루어지지 않고 있다.

NAT는 IP 수의 부족을 해결하기 위한 방법으로 내부 네트워크에서 사설 IP주소를 공인 IP주소로 상호 변환하는 방법으로 사용되고 있으며 보안 문제를 해결하고 있다.[1][2]

표3. NAT의 종류

풀콘 (Full Cone)	내부에서 외부로 하나의 데이터가 전송되며 외부에서 내부로 데이터가 전송할 때 맵핑된 내부 장비에게 릴레이 하는 NAT
리스트릭 콘 (Restricted Cone)	내부에서 외부로 IP 주소를 통해 전송된 적이 있는 데이터만 릴레이 하는 NAT
포트 리스트릭 콘 (Port Restricted Cone)	전송이 되었던 데이터의 포트 에서만 내부로 데이터가 전송되며 나머지 데이터는 버리는 NAT
시메트릭 콘 (Symmetric Cone)	내부에서 외부로 데이터가 전송될 때 외부 주소에 따라 내부 포트가 변경되는 NAT

Ⅲ. MANET 환경의 보안 해결방법

3.1 MANET 라우팅 프로토콜

MANET은 이동 단말기가 기반 구조 없이 자율적이고 독립적으로 라우팅 프로토콜을 이용하여 무선 네트워크를 구축할 수 있다.

첫째, 프로엑티브(Proactive)은 애드 혹 네트워크를 위한 방식으로 테이블 기반 방식이라고도 한다. 자신을 제외한 모든 라우팅 정보를 유지하여 경로를 설정할 때 경로 획득 절차가 불필요하여 시간과 노드가 적게 소요하는 장점이 있으나 모든 라우팅의 정보를 유지하기 위하여 오버헤드가 증가하여 대규모 무선 네트워크에는 적합하지 않다. 대표적으로 DSDV, OLSR등의 라우팅 프로토콜이 있다.

둘째, 리엑티브(Reactive)은 프로엑티브의 단점을 해결하기 위하여 제안된 방식으로, 다른 말로 요구 기반 방식이라고도 한다.

데이터 정보의 요구가 있을 때 이동 경로를 탐색하고 설정을 하는 방식으로 AODV, DSR등의 라우팅 프로토콜이 있다. 오버헤드가 적게 발생한다는

장점이 있으나 지연 시간이 길어서 실시간 통신에서는 적합하지 않으며 제어 트래픽이 많이 발생할 수 있다.
셋째, 하이브리드(Hybrid)은 프로엑티브와 리엑티브 방식의 장점을 합친 기법으로 ZRP 라우팅 프로토콜이 있다.
이동 단말기에 라우팅 존(Zone)을 유지하여 존 안에서는 프로엑티브 방식을, 존 바깥 지역에서는 라우팅 패킷이 필요할 때에 리엑티브, 방식을 사용하여 주변 노드를 검색하여 정보를 전송하는 방식이다.[3][4]

3.1.1 AODV(Ad-hoc On-Demand Distance Vector)

AODV는 소스 노드의 필요에 따라 경로 설정되는 리엑티브 라우팅 프로토콜로 소스 라우팅 방식의 DSR(Dynamic Source Routing)의 문제점을 개선한 프로토콜이다.[4]

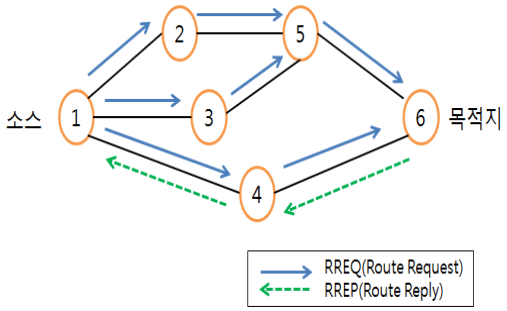

그림 1. AODV 경로 과정

그림 1은 AODV 경로 과정이다.
RREQ(Route Request) 패킷은 연결 요청을 하는 패킷이고, 요청이 들어온 패킷을 목적지에서 응답하는 패킷이 RREP(Route Reply) 패킷이다.
상호 간의 패킷 교환으로 통신 연결이 설정된다.
AODV는 이웃 노드에게 라우팅 정보를 전달할 때 암호화와 인증 과정의 보안이 되어 있지 않아서 패킷 전송시 모든 노드에서 수정이 가능하고 무선 망으로 네트워크 구성하는 특성상 접근성이 용이하다.
외부 공격자가 내부로 접근하여 임의로 공격자의 라우팅 경로를 최단 경로로 수정 및 변조하여 실사용자로 하여금 패킷 손실, 네트워크 성능을 저하시킬 수 있다.[4]

Ⅳ. 결 론

무선 망에서 네트워크를 구축하여 노드에게 전송할 때 외부에서 침입이 쉽기 때문에 보안에 많이 취약하다. 방화벽은 노드의 이동성으로 매번 새로운 경로를 검색해야 하는데 허용된 등록자의 패킷 정보와 불필요한 정보를 기억하고 차단해야 하므로 단말기의 기록 용량을 많이 사용되어 시스템 과부화 현상으로 사용하기에는 적합하지 않는다.

NAT의 경우 소프트웨어적인 설정으로 이동을 하면서 이용이 가능하지만 새로운 경로와 사용자 정보를 매번 변경을 해야 하는 불편함을 가지고 있다.

현재 MANET 환경에서는 라우팅 프로토콜을 사용해서 이동 노드들의 데이터 정보를 대체 경로 혹은 다중 경로를 이용하여 외부의 네트워크 공격을 임시적으로 피하는 보안 해결책이 연구되고 있다.
하지만 라우팅 프로토콜인 AODV에서는 목적지까지의 라우팅 정보를 획득하는 지연 시간이 길어지고, 노드들의 이동성으로 경로가 중간에 자주 끊기는 등 VoIP와 같은 실시간 통신에는 부적합한 문제점을 보이고 있다.

새로운 단말기와 네트워크 기술의 등장으로 이동을 하면서 기반 구조없이 무선 망을 구축하여 사용할 수 있는 MANET은 현재 여러 방법으로 연구되고 있으나 접근성이 용이한 특성상 완전한 보안문제를 해결할 수 없다.
라우팅 프로토콜을 이용하여 경로 탐지, 복구로 보안을 해결하는 방법도 있겠지만 VoIP 시스템에 기본이 되는 SIP 프로토콜을 수정하여 보안을 해결하는 방법을 추후 연구 과제로 계획하고 있다.

참고문헌

[1] D. Richard Kuhn, Thomas J. Walsh, Steffen Fries, “Security Considerations for Voice Over IP Systems”, Jan. 2005, pp52-62.

[2] Johann Thalhammer, “Security in VoIP-Telephony Systems”, 10.1.1.85.7213.pdf, pp43-49

[3] 장영민, “NS-2 네트워크 시뮬레이터의 활용”, 2008, pp209-pp224.

[4] 서현곤, 김기형, “애드 혹 네트워크에서 AODV에 기반한 효율적인 경로 복구 기법”, KNOM Review 제6권 제1호, 2003.6

[5] 이재현, 김진희, 권경희, “애드혹 센서 네트워크에서 AODV 라우팅 정보변조 공격노드 탐지 및 추출기법, 2008.06