MANET 기반 VoIP의 보안 취약성 연구

윤통일* · 김영동*

*동양대학교

A Study on the VoIP Security vulnerability over MANET

Tong-il,Yoon* · Young-Dong,Kim**

*DongYang University

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

요 약

VoIP는 저렴한 통신비용, 어디서나 사용 가능한 통화 기능과 부가 서비스를 갖고 있는 기술이다. 하지만 IP기반 사용으로 도청과 스팸 콜(spam call), 서비스 거부(DoS)등 네트워크 공격이 쉽게 노출되어 보안의 취약성을 가지고 있다. 특히, MANET 기반 VoIP 시스템은 유선 네트워크 보다 공격자에게 쉽게 접근 가능에 사용자의 정보 추가와 수정으로 보안 문제에 큰 이슈가 되고 있다.
본 논문에서는 MANET 기반 VoIP 시스템에 침입하는 대표적인 네트워크 공격에 대해 알아보고 이를 해결할 수 있는 기술을 제안한다.

ABSTRACT

VoIP is a communication technique can be used anywhere you can find wifi signal and it costs much lower than conventional mobile service.

However, security of VoIP is not as robust as former, the converse could be easily intercepted and attacked especially in MANETs which the attackers access easier than in wired networks. Sercurity of VoIP system in MANETs is an important issue nowadays.

In this paper, a typical attack method of VoIP systems in MANETs is described and we implement how to prevent it.

키워드

VoIP, MANET, 보안, 네트워크 공격

Ⅰ. 서 론

인터넷의 빠르게 발전하고 증가함에 따라 인터넷 사용이 보편화됨에 따라 광대역 통합망 (BcN : Broadband convergence Network)의 이상 기술로 자리 잡은 VoIP(Voice over Internet Protocol)는 IP망을 기반으로 저렴한 통신비용과 어디서든 이용과 많은 부가 서비스의 제공된 전화 서비스이다.[1]

모든 인터넷 서비스도 마찬가지이지만 VoIP 서비스 역시 네트워크 공격으로 인한 보안의 문제점을 주의해야 한다.

VoIP 시스템에서 네트워크 공격은 별도의 장비를 사용하거나 SIP(Session Initiation Protocol) 서버에서 패킷 정보와 목적지 주소 정보 변경으로 예방할 수가 있다.

그러나 외부에서 들어오는 침입자의 제한을 하거나 시스템 과부하 차단 등을 사용하게 된다면 인터넷의 이용 속도가 많이 저하되고 VoIP의 성능 역시 제대로 발휘하기가 힘이 든다.

무엇보다 기반 구조가 없고 노드 간에 독립적으로 자율적 구성된 무선 네트워크 기술인 MANET(Mobile Ad-Hoc Network)에서는 이러한 네트워크 공격을 방지하고자 별도의 고가 장비 구입이나 매번 소지하고 있어야 하는 번거로움이 있어 인터넷 이용에 어려움이 있다.

MANET은 무선망에서 이동 노드 간에 경로 설정 구성을 가지고 통신을 하기 때문에 네트워크의 설정을 쉽게 변경할 수 있어 유선망 보다 높은 보안 취약성을 가지고 있다.

이에 외부에서 침입하는 네트워크 공격을 보다 안전하게 MANET 기반 VoIP 시스템의 보안 위험을 분석한 예방 및 해결책이 필요하다.
본 논문은 Ⅱ장에서 VoIP 보안 위험의 기본요소들을 살펴보고, Ⅲ장에서는 MANET 기반 VoIP의 보안 취약성을 알아본다. Ⅳ장에서는 결론을 맺는다.

Ⅱ. VoIP 위험 요소들

현재 인터넷은 IP망을 이용하여 발생할 수 있는 위험요소들을 고려할 수 있으나 VoIP만의 서비스를 본다면 가장 주의하며 봐야 할 부분이 몇 가지가 있다.
표 1은 VoIP 주요 보안 위험의 요소에 대한 내용이다.[2]

표 1. VoIP 보안 위험 요소

요 소	내 용
도청	음성 정보 패킷을 불법으로 수집 및 조합. 통화내용을 재생하는 공격.
VoIP 스팸 발송	음성광고 메시지로 사생활 피해를 주는 공격.
서비스 거부(DoS) 공격	단말기와 장비 해킹 혹은 시스템 과부화 패킷을 악의적으로 전송하여 서비스 장애를 유도하는 공격.
서비스 오용 공격	등록 정보 변경 및 추가로 불법적 통신 서비스를 이용하는 공격.
세션 가로채기	양단간 통신에 개입하여 제어 권한을 획득하는 공격.

2.1 도청

양단간의 음성 정보를 해킹하여 엿듣는 공격으로 회선을 공유하는 유선 네트워크의 로컬 망에서 제한적으로 도청이 가능하다.
단, 신호교환방식(IP-PBX)을 사용하여 일반 전화로 인터넷 전화서비스를 하는 경우, 로컬 망에 연결된 단말기에 사용자의 MAC 인증을 부여하여 암호화 기능을 삽입된 경우, MANET 환경처럼 네트워크 공간이 분리될 경우에는 불법 도청하기가 어렵다.

2.2 VoIP 스팸 발송

현재 이메일 서비스와 마찬가지로 비용이 저렴하고 자동화 프로그램의 사용 가능으로 조작이 간단하다.
따라서 불특정 사용자에게 음성으로 저장된 광고성 메일을 전송하므로 사용자의 사생활 침해와 개인 정보 유출할 수 있는 공격 방법이다.
다양한 접속성을 가지고 있는 인터넷의 특성상 스팸 발송자의 추적이 힘들어 심각한 VoIP 보안 취약점으로 볼 수 있다.

2.3 서비스 거부 공격

서비스 거부(Dos: Denail of Service) 공격은 공격자가 불필요한 패킷을 사용자의 시스템에 집중적으로 보내 자원 고갈로 더 이상 통화 서비스나 네트워크의 접속 서비스를 사용 할 수 없는 공격이다.

2.4 서비스 오용 공격 / 세션 가로채기

서비스 오용 공격은 VoIP 서비스의 정식 사용자 등록 정보를 침입하여 사용자의 정보를 변경 및 추가하여 요금을 지불하지 않고 불법적으로 VoIP 서비스를 이용해서 금전적 피해로 유발한 공격이다.
세션 가로채기는 네트워크 공격자가 VoIP 사용자 등록 혹은 호 설정 부분에서 제어 권한을 획득하여 도청, 서비스 거부 공격, 서비스 오용 공격 등 정보를 조작할 수 있다.

Ⅲ. MANET 보안 요소 해결

앞에서 언급했듯이 MANET은 유선망과는 다르게 네트워크 접근이 쉬워 사용자 등록 정보, 위치 경로 설정등을 간단하게 변경할 수 있다. 때문에 보안 위험성이 높아 실사용자들의 서비스 이용에 불편을 줄 수 있다.
이를 해결하는 방법에는 네트워크 공격자가 무선망을 통해 쉽게 접근을 할 수 없도록 하는 방법이 있다.

3.1 IP주소 중복 탐색

인터넷을 사용하기 위해서는 IP주소를 할당 받아 사용을 한다.
현재 IPv4는 인터넷의 급속도로 발전되고 분산되어 IP주소 고갈 문제점이 되고 있다.
이에 128bit로 구성되어 있는 IPv6의 등장으로 더 이상 IP주소 고갈의 문제를 해결할 수 있지만 IPv6버전 사용은 전용 기기의 비용과 시간적 문제로 대중화가 되지 않는다.
그래서 아직까지는 IPv4를 사용하여 네트워크의 연구가 계속 진행되고 있다.
MANET 환경에서 노드 이동으로 단말기 스스로가 IP주소 생성 및 할당을 받아 통신을 하므로 각 노드 확인을 위한 중복되지 않는 순수한 IP주소를

가지고 있어야 한다.
그러나 IP 자원 고갈 문제로 DAD(Duplicate Address Detection) 과정을 통해 중복 IP주소 탐지를 거치지 않고 메시지를 연속적으로 전송하여 사용자 단말기에 DoS 공격을 발생할 수가 있다.
이에 노드 스스로가 단방향 방식으로 해쉬 함수를 이용하여 IP주소를 성하여 DAD 과정을 거쳐 DoS 공격을 방지하는 보안 기법이 있다.[3]

3.2 프로토콜 알고리즘

MANET 환경에서는 테이블 기반(Table Driven) 방식과 요구 기반(On-Demand Driven) 방식 프로토콜을 사용한다.
테이블 기반 방식은 필요한 목적지 경로에 대해 즉시 경로를 제공하지만 필요하지 않는 경로를 유지해야 하므로 무선 자원 낭비를 초래하는 문제점을 가지고 있다.
요구 기반 방식은 망 전체로 부터 요구와 응답된 경로 설정 등의 경로를 찾을 수 있으나 경우에 따라 통신 지연의 문제점을 갖고 있다.
이런 각 기반 방식의 장점을 모은 Zone Routing Protocol(ZRP)이 등장하여 각 노드를 Zone이라는 범위의 안전한 경로를 설정할 수가 있다.
이 경로 설정 보안 알고리즘을 S-ZRP(Secure Zone Routing Protocol)을 제안하여 대칭, 비대칭 키를 해쉬함수 방식으로 대신 사용하여 단말기의 전력소비를 줄이고 경로설정 속도를 빠르게 탐색하는 방법이 있다.[4]
이처럼 MANET 환경에서 새로운 프로토콜을 사용하거나 목적지 주소 중복 탐지하여 네트워크 침입 공격을 방지할 수 있다.
하지만 실시간 통화 서비스를 중점인 MANET 기반 VoIP 시스템에서는 아직 미흡한 방법으로 볼 수 있다.

V. 결 론

본 논문에서는 현재 상용화 되고 있는 VoIP 서비스에 대한 보안 위험요소에 대해 알아보았다.
현재 MANET 기반 VoIP 서비스의 보안 취약점을 해결하기 위해 보안 장비 시스템을 사용하거나 프로토콜을 수정하여 서버를 추가하는 방법 등으로 해결할 수 있다.
하지만 아직까지 VoIP 시스템의 기본 프로토콜인 SIP를 사용하여 보안 해결책에 대한 연구는 미흡하다.
이에 간소화시킨 SIP 서버를 이용하여 MANET 기반 VoIP 시스템에 침입하는 네트워크 공격을 방지하는 연구가 추후 과제이다.

참고문헌

[1] 박진범, 백형구, 원용근, 임채태, 황병우, “VoIP 보안 취약점 공격에 대한 기존 보안 장비의 대응 분석 연구”, 정보보호학회지, 제17권 제5호(pp 57-64), 2007.10

[2] 한국정보보호진흥원, “VoIP 정보보호가이드”, 2005.12

[3] 서대열, 김진철, 김경목, 오영환, “MANET 환경에서 Zone Routing Protocol을 이용한 안전한 경로설정 보안 알고리즘 S-ZRP", 전자공학회 논문지, 제43권 4호(pp 13-21), 2006.04

[4] 임정미, 박창섭, “MANET 환경에서 중복 주소 탐지에 대한 DoS 공격을 방지하는 보안 기법과 성능 평가”, 멀티미디어학회 논문지, 12권, 8호(pp 1099-1108), 2009.08