DDoS 침해가 있는 MANET에서 VoIP 트래픽의 성능

김영동*

Performance of VoIP Traffics over MANETs under DDoS Intrusions

Young-Dong Kim*

요 약

본 논문에서는 DDoS 침해가 있는 MANET을 대상으로 VoIP 트래픽의 전송 성능을 측정하고 분석하여 보았다. 측정된 결과의 분석을 통하여 DDoS 침해가 있는 MANET에서 침해대비조건을 제시하였다. 성능측정에는 NS-2를 기반으로 구성한 VoIP 시뮬레이터를 이용하였다. 시뮬레이션을 통하여 MOS, 네트워크지연, 패킷 손실율 및 호연결율 전송성능으로 측정하였다. 본 논문의 결과로서 DDoS 침해가 있는 MANET에서 VoIP 서비스를 운영하기 위해서는 침해가 10초 이상 지속되지 않토록 해야 함을 확인하였다.

ABSTRACT

In this paper, Transmission performance over MANET(Mobile Ad-hoc Networks) under DDoS Intrusions is evaluated. Intrusion counterplan requirement, which have to be used for MANET under DDoS intrusions, is suggested through this evaluation. VoIP simulator based on NS-2 network simulator is used for performance measurement. MOS, network delay, packet loss rate and call connetion rate is measured with this simulation. Finally, requirement of intrusion continuing time shorter then 10 seconds is suggested for VoIP service over MANETs under DDoS intrusions.

키워드

MANET, VoIP, DDoS, Performance, Simulation
이동임시망, IP전화, 디도스, 성능, 시뮬레이션

Ⅰ. 서 론

기반구조를 사용하지 않은 MANET(Mobile Ad-hoc Network)은 단말기들 사이에 임시로 구성되는 네트워크로 설치 및 유지가 편리해 탐사, 화재, 전쟁, 지진과 같은 긴급/재난 통신에 편리하게 사용될 수 있으며 최근 들어 스마트 폰과 같은 지능형 통신 단말기의 급속한 보급에 따라 그 응용영역이 확대될 것으로 예상된다.

MANET 응용분야의 확대는 MANET이 처리할 트래픽이 데이터중심으로부터 음성과 영상을 비롯한 멀티미디어로 전환됨을 의미한다. 가장 급속하게 증가될 것으로 예상되는 트래픽으로 VoIP(Voice over Internet Protocol)을 들수 있다.

VoIP는 인터넷을 기반으로 제공되는 음성전화서비스로 유선인터넷에서 기존 유선전화를 급속하게 대체하고 있으며 모바일 영역으로 그 서비스를 확대되고 있다. 그러나 모바일 VoIP는 기지국과 같은 통신 기반구조의 사용을 전제로 하는 것이므로 기반구조의 지원이 어려운 통신환경에서 VoIP 사용을 보장하는 것이

* 동양대학교 정보통신공학부(ydkim@dyu.ac.kr)
접수일자 : 2011. 06. 28 심사(수정)일자 : 2011. 07. 18 게재확정일자 : 2011. 08. 12

아니다. 따라서 통신기반구조의 지원없이 임시적으로 구성되는 MANET 환경에서 VoIP 시스템 구현과 트래픽 성능 분석은 의미있는 연구라 할 수 있다[1][2].

한편, 최근 스마트폰의 급속한 보급은 MANET 구축과 활용에 좋은 환경을 제공함과 동시에 정보침해의 수단제공과 기회증가와 같은 통신환경의 급속한 변화를 초래하고 있다. 스마트 폰이 보유하고 있는 지능형 기능으로 인해 스마트 폰 자체가 정보침해의 대상이 될 뿐만 아니라 정보침해의 수단으로 사용될 가능이 크게 증가하고 있는 것이다. 정보침해의 이런 경향은 더 증가되어질 것으로 생각된다.

MANET에서 발생되는 정보침해는 단말기의 기능 저하에 국한되지 않고 네트워크 전체에 치명적인 영향을 발생시킬수 있다. MANET의 단말기의 하드웨어적 소프트웨어적 기능이 증대되므로 침해를 일으키는 기능을 탑재하기가 매우 용이해진 만면에 이를 방지하기 위한 기능면에서 볼 때 현재의 단말기의 기능이 취약하여 기반통신구조에서 사용되는 방화벽과 같은 네트워크 침해방지 기능을 탑재하기가 곤란하기 때문이다.

네트워크측면에서 정보침해는 트래픽을 과다하게 발생시켜 네트워크의 기능을 마비시키는 것이 가장 일반적인 유형이다. 인프라네트워크에서는 침해를 일으키는 노드가 일반적으로 고정되어지므로 침해현상이 발생될 경우 그 결과로 나타나는 트래픽 폭주현상의 탐지가 비교적 수월하고 폭주현상을 발생시키는 노드나 그 영역을 차단할 경우 차단된 이외의 네트워크 영역에 트래픽 장애 발생을 최소화할 수 있어 침해현상을 네트워크 일부분으로 축소시킬수 있다.

그러나 MANET에서는 네트워크에 연결되는 모든 노드가 라우팅과 같은 네트워크 기능을 수행해야 전체 네트워크의 기능이 유지되므로 특정 노드의 침해가 전체 네트워크에 통신장애를 발생시킬수 있어 인프라네트워크에 비해 치명적인 영향을 초래할 수 있다[3][4].

본 논문에서는 이와같은 MANET의 정보침해 현상이 MANET의 트래픽 전송에 미치는 영향을 컴퓨터 시뮬레이션을 통하여 분석하고 그 결과를 활용하여 정보침해의 정도에 따른 통신서비스 구현 조건을 제시한다. 본 논문에서 분석 대상 MANET 서비스로 향후 사용이 증가될 것으로 판단되는 VoIP 서비스로 했으면 정보침해 유형으로는 네트워크 트래픽에 가장 큰 영향을 발생시키는 DDoS(Distributed Denial of Service)를 사용하였다.

본 논문에서 사용한 시뮬레이터는 NS(Network Simulator)-2를 기반으로 VoIP 모듈을 추가하여 구성하였으며, 시뮬레이션에서 사용된 MANET은 1000 × 1000m 급 이상의 MANET으로 하였다. 시뮬레이션으로 측정한 파라메타로는 MOS, 네트워크지연, 패킷손실율, 호연결율로 하였다.

본 논문의 구성은 다음과 같다. I장은 서론이며, II장은 MANET 정보침해, III장은 시뮬레이션과 성능분석 그리고 IV장에서 결론으로서 연구결과 및 향후의 연구방향을 제시하였다.

II. MANET 정보침해

MANET은 통신기반구조를 사용하지 않고 단말기를 중심으로 구성되는 임시네트워크여서 인프라네트워크에서 사용되는 방화벽 같은 기능이 잘 갖추어진 정보침해방지 장치들을 사용하기가 용이하지 못하다.

모바일 단말기는 스마트 기능을 갖추고 있다 하더라도 하드웨어적 소프트웨어적 처리능력은 인프라네트워크 장비에 비하여 극히 제한적이다. 반면에 오히려 MANET 단말기는 네트워킹 기능과 응용서비스 기능을 동시에 제공해야 한다. 이 기능에 더하여 추가적으로 정보침해대책으로서 예방, 탐지 및 대응 기능을 부가하는 것은 단말기 성능의 저하를 초래할 수 있으며, 결국 네트워크 성능의 저하를 일으키는 원인으로 작용한다.

MANET에서 정보침해는 주로 링크계층에 대한 침해와 네트워크 계층에 대한 침해로 분류된다. 링크계층에 대한 침해는 멀티-홉으로 구성되는 통신경로를 단절시켜 네트워크의 기능을 마비시키는 현상을 초래한다[3].

네트워크 계층 침해는 라우팅 기능과 패킷전달 기능에 대한 침해를 의미한다. 라우팅 기능 침해는 라우팅 테이블을 변화시켜 통신경로를 허락없이 변경시키는 것을 의미한다. 패킷전달침해는 패킷전달 기능에 변화를 주어 네트워크의 기능을 저하시킨다. 패킷전달 침해를 사용할 경우 DoS(Denial of Service) 침해를 발생시킬 수 있는데 패킷전달기능에 변화를 주어 패킷이 폭주하도록 해 노드의 기능을 차단시킬 수 있기

때문이다[4].

MANET에서 네트워크 침해는 그림 1과 같이 발생되어질 수 있다. 그림 1에서 악성노드가 일반노드에 대하여 2단계에 걸쳐서 침해를 시도하고 있다. 1단계로 악성노드인 A와 B가 일반노드인 5와 1을 각각 공격하고 있다. 이 침해로 인해 노드 1과 노드 5가 기능을 상실하게 되면 네트워크는 노드{0}, 노드{2,3,6,7}, 노드{4,8,9}의 3개로 분리된다. 다음단계로 악성노드 C와 D가 일반노드 노드 4와 7에 대하여 추가로 공격을 시도하면, 네트워크는 노드{0}, 노드{2}, 노드{3}, 노드{6}, 노드{8,9}로 완전히 분리되어 그 기능을 상실하게 된다.

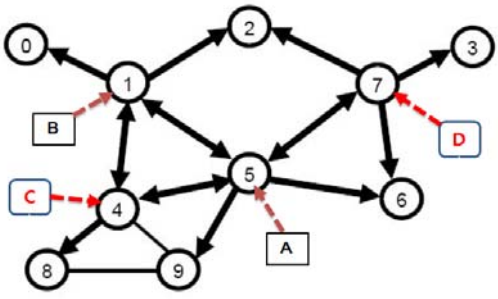

그림 1. MANET에서 노드 침해
Fig. 1 Node intrusions on MANET

그림 1과 같이 MANET의 기능을 마비시키는 침해현상은 링크계층에 대한 침해나 네트워크계층에 대한 침해 어느 것을 사용하더라도 가능하다. 링크계층의 침해를 사용할 경우, 노드 1과 5의 라우팅 테이블을 공격하여 노드 1과 5에서 다른 영역으로 경로가 설정되지 못하도록 할수 있다. 네트워크 계층에 대한 침해일 경우, 노드 4과 노드 7에서 패킷전달기능을 마비시켜 경로는 설정되어 있다 하더라도 패킷이 다른 영역으로 전달되지 못하도록 할 수 있다. 그러므로 어떤 유형의 침해가 있더라도 통신응용서비스 관점에서 보면 네트워크 기능이 마비되어 통신기능이 두절되는 것으로 보여지게 된다.

본 논문에서는 이런 현상을 가정하여 MANET에서 악성노드가 일반노드를 공격하여 침해를 일으킬 경우 그 침해가 응용 서비스 전송 성능에 미치는 영향을 분석해 본다.

III. 시뮬레이션과 성능분석

3.1. 시뮬레이터

본 논문에서 사용한 시뮬레이터는 NS-2 2.33을 기반으로 NS2VoIP 패치를 사용하여 구축하였다[5][6]. NS2VoIP는 NS-2가 제공하지 않는 VoIP 기능을 지원한다. MANET 기능은 NS-2가 제공하는 ADHOC 기능을 사용하였으며 MANET의 이동성은 NS-2 ADHOC 기능이 요구하는 형식에 맞추어 구성하였다. VoIP 트래픽은 NS2VoIP 기능을 사용하여 코덱 규격에 맞추어 생성하도록 하였다.

네트워크 침해는 DDoS 공격을 가정하였다. 침해를 일으키는 악성노드는 일정한 기간 동안 일반노드에 대하여 트래픽을 지속적으로 전송하여 일반노드의 기능을 저하 또는 마비시키도록 하였다. 악성노드는 무작위로 선택하였으며, 그 악성노드에 의하여 침해대상이 될 일반노드는 역시 난수를 사용하여 랜덤하게 선정하였다.

3.2 시뮬레이션 환경

본 논문의 시뮬레이션에서 각 노드들은 악성노드와 일반노드를 불문하고 지정된 규격의 MANET내에 랜덤하게 분포하며, 시나리오 파일에 정해진 랜덤 값에 따라 노드별로 랜덤 방향과 랜덤 속도로 독립적으로 이동한다. 노드의 이동속도는 사람의 이동속도를 감안하여 2㎧이하로 설정하였다. 이 속도는 최대 7㎞/h의 이동속도를 의미한다.

각 노드들은 침해가 있는 MANET에서 최대 2㎧속도의 랜덤 이동 중에 다른 노드들과 VoIP 트래픽을 송신하거나 수신한다. 하나의 노드가 생성할 수 있는 최대 VoIP 연결수는 1로 설정하였다. 따라서 하나의 MANET내에 존재할 수 있는 최대 VoIP 연결수는 네트워크 내에 존재하는 악성노드를 제외한 일반노드 전체수의 1/2이하이다. 이외에 본 논문의 시뮬레이션 환경은 다음과 같다.

시뮬레이션에서 VoIP 트래픽은 MANET에서 가장 우수한 전송성능을 보여주는 GSM.AMR 코덱 규격에 맞추어 비트율 12.2kbps, 샘플간격 20㎳, 샘플크기 31바이트, 페이로드 31바이트로 생성되며, 패킷취합방식을 사용하여 4개의 VoIP 패킷을 취합하여 송신된다[7].

표 1. 시뮬레이션 파라미터
Table 1. Simulation parameters

파라메터	설정값
라우팅	AODV
MAC	802.11g (54Mbps)
네트워크규모	1×1㎞, 2×2㎞, 3×3㎞
노드수	50(일반노드 40 악성노드 10)
VoIP 연결 수	20
코덱	GSM.AMR
네트워크 지연	지수분포

3.3 성능 파라미터

본 논문에서 구성한 시뮬레이터를 사용하여 분석 가능한 성능평가척도는 MOS, 호연결율, 네트워크 지연, 패킷손실율이다. 이 파라메타들은 VoIP 성능평가에 사용되는 평가척도이며, 모바일 네트워크를 기준을 한 각 요구수준은 표 2와 같다[8].

표 2에서 MOS는 음성전화 통화품질 평가척도로 ITU-T P.800에 의하면 VoIP전화의 경우 이동전화와 같은 수준인 3.6이상이 요구된다. 이는 유선전화의 MOS 요구수준인 4.0 보다 0.4 정도 낮은 값이다. 모바일 네트워크에 대한 VoIP 패킷의 종단간 전송지연의 요구수준은 유선 VoIP의 150㎳의 2배인 300㎳이다. 300㎳ 지연은 사용자에게 인식되어지나 수용할 만한 정도의 요구수준으로 이동통신의 음성통화의 지연수준인 260~280㎳보다 다소 큰 지연이다. 호연결율은 접속품질로서 요구수준이 95%이다.

표 2. 모바일 VoIP 전송품질
Table 2. Transmission Quality of Mobile VoIP

품질지표		요구수준
통화품질	MOS	≥3.6
	종단간 지연	≤300ms
접속품질	호성공율	≥95%

기타 서비스 품질로서 패킷손실율은 전송패킷에 대한 손실된 패킷의 비율로 1%~5%의 수준으로 제시되고 있다[8]. 본 연구에서는 그 요구수준을 5%로 가정하여 사용한다.

3.4 시뮬레이션 결과 및 분석

본 논문에서는 3.1~3.3절의 조건에 따라 컴퓨터 시뮬레이션을 실행하였다. 시뮬레이션 시간은 비교적 짧은 통화군에 속하는 생계형 근로자의 이동전화 평균통화시간 40초[9]와 사무직종사자의 이동전화 평균통화시간 90초[10]를 고려하여 60초로 하였다.

시뮬레이션에서 침해는 0/10/20/30/40/50초간 지속되는 것으로 간주하였으며, 네트워크 규모별로 1×1㎞, 2×2㎞ 및 3×3㎞로 크기를 구분하여 시뮬레이션을 수행하였다.

시뮬레이션 결과를 그림 2~4에 제시하였다. 그림 2~4는 각각 MOS, 네트워크 지연 및 패킷 손실율을 보여준다.

그림 2는 침해시간에 따른 MOS를 보여주고 있다. 그림 2에서 약 20초 이내의 침해 있을 경우 MOS가 기준 3.6을 만족하는 것을 볼 수 있다. MANET 규모가 1×1㎞일 때 MOS가 가장 낮았다. 노드가 인접할수록 악성노드가 일반노드에 침해를 발생시키기 수월하기 때문이다. 그러나 2×2㎞와 3×3㎞ 규모의 경우 면적이 각각 4㎢와 9㎢로 그 내에 50여개 정도의 노드가 있은 경우 규모의 차이에서 오는 인접성은 크지 않게 된다.

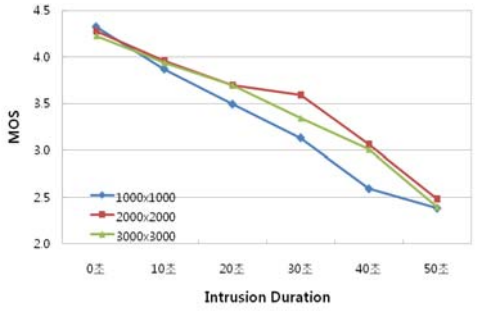

그림 2. MOS
Fig. 2 MOS

그림 3은 네트워크 지연을 보여주고 있다. 그림 3에서 지연 요구 조건인 300㎳를 만족시키기 위해서는 MANET 규모에 따라 차이가 있는 것으로 보여지나 침해가 10초 미만으로 발생되어야함을 관측할 수 있다.

그림 4는 패킷 손실율을 보여주고 있다. 그림 4에서 패킷 손실율 요구 조건인 5%을 만족시키기 위해서는 침해가 약 10초 이내로 지속되어야 함을 알수 있다.

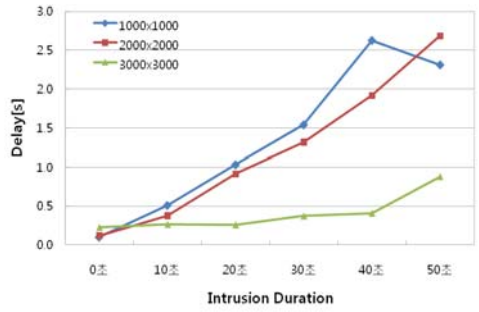

그림 3. 네트워크 지연
Fig. 3 Network delay

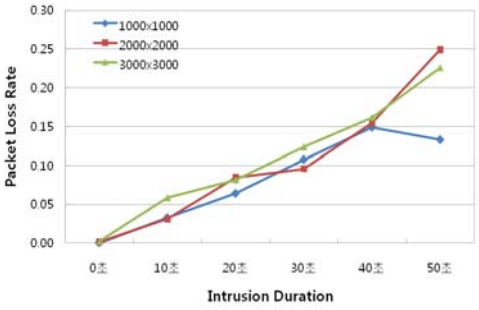

그림 4. 패킷 손실 율
Fig. 4 Packet loss rate

한편, 호연결율은 전체 시뮬레이션 구간에서 침해 시속시간에 무관하게 100%에 이르는 것으로 측정되었다. 호의 연결에서는 침해가 발생되어 트래픽처리율이 낮아진다 하더라고 일정시간 대기하면 연결이 완성되어질 수 있기 때문이다.

3.5 침해대비조건

3.4 절의 시뮬레이션 결과 분석에서 살펴본 바와 같이 DDoS 침해가 발생할 가능성이 있는 MANET에서 VoIP 시스템을 구축할 경우, 그 침해는 MOS, 네트워크 지연 및 패킷손실율과 같은 서비스품질 요구조건을 감안할 때 10초 이상 지속되지 않토록 해야 한다. 이는 침해를 탐지하고 복구하는데 걸리는 시간이 10초 이내 임을 의미하는 것이며, 일반 사용자의 경우 통화품질에 차이를 거의 인식하지 못하게 된다.

Ⅳ. 결 론

본 논문에서는 DDoS 침해가 있는 MANET에서 VoIP 전송성능을 컴퓨터 시뮬레이션을 통하여 분석하고 침해대비 조건을 제시하였다.

본 논문에서 제시한 연구 결과로서 DDoS 침해가 있는 MANET에서 VoIP 서비스를 적절하게 제공하기 위해서는 평균통화시간을 1분으로 가정할 경우 침해대비시간은 10초 이내였다.

본 논문에서 제시한 연구방법과 결과는 MANET에서 VoIP 시스템 설계, 구축 및 운영에 있어 침해분석 및 대비에 필요한 자료로서 중요하게 사용될 수 있을 것으로 생각한다.

본 논문의 결과는 평균적 분석을 사용한 결과로서 실시간적 결과와 그 분석을 활용하여 DDoS 침해가 MANET 응용서비스에 미치는 영향에 대한 추가의 연구가 향후 필요하다.

참고 문헌

[1] M. Castro, A. Kassler, "SIP in hybrid MANETS - A gateway based approach", Proceedings of Swedish National Computer Networking Workshop, Lulea, Sweden, Vol. 4, pp.3~6, Oct., 2006.

[2] M. Castro, A. Kassler, "Challenges of SIP in Internet Connected MANETs" Proceedings of International Symposium of Wireless Pervasive Computing, San Juan, Puerto Rico, Vol. 2, pp.2~7, Feb., 2007.

[3] Young-Dong Kim, "Transmission Performance of MANETs based on Mobility of Attacking Nodes", Proceedings of KIECES 2011, Vol.5, No.1, pp.324~327, Jun., 2011.

[4] G. Kumar, J. Singh, "Truth of D-DoS Attacks in MANET", Global Journal of Computer Science and Technology; Vol. 10, No. 15, pp.15~22, Dec., 2010.

[5] http://nsnam.isi.edu/nsnam.

[6] A. Bacioccola, C. Cicconetti, G. Stea, "User-level Performance Evaluation of VoIP using ns-2", Proceedings of 2nd International Conference onf Performance Evaluation Methodology and Tools, Vol.2, pp.1~10, Oct., 2007.

[7] 김영동, "대규모 MANET에서 VoIP 트래픽의 종

단간 성능", 한국전자통신학회 논문지, 6권, 1호, pp. 49~54, 2011.
[8] 김영동, "MANET에서 패킷 취합을 이용한 VoIP 성능 개선", 한국전자통신학회 논문지, 5권, 3호, pp. 275~280, 2010.
[9] http://k2man.com/3985
[10] http://mobile.uplus.co.kr/jsp/cc/priceplan/message_fix.jsp

저자 소개

김영동(Young-Dong Kim)

1984년 광운대학교 전자통신공학과 졸업(공학사)
1986년 광운대학교 대학원 전자통신공학과 졸업(공학석사)
1990년 광운대학교 대학원 전자통신공학과 졸업(공학박사)
현재 동양대학교 정보통신공학부 교수
※ 관심분야 : 통신프로토콜, MANET, VoIP, 컴퓨터 시뮬레이션