다중침해가 있는 MANET에서 VoIP 트래픽의 전송성능

김영동*

Transmission Performance of VoIP Traffics over MANETs under Multi Intrusions

Young-Dong Kim*

요 약

본 논문에서는 여러 유형의 침해가 발생되는 MANET에서 여러 종류의 VoIP 트래픽의 전송성능을 측정하고 분석하여 보았다. 성능측정에는 NS-2를 기반으로 구성한 VoIP 시뮬레이터를 이용하였다. 시뮬레이션을 통하여 MOS, 네트워크지연, 패킷손실율 및 호연결율을 전송성능으로 측정하였다. 측정 결과의 분석을 통하여 다중 침해가 있는 MANET에서 전송 성능 파라메타 별 각 트래픽의 특성을 제시하였다. DDoS 및 블랙홀 침해와 같은 다중 침해가 있는 MANET 환경에서 VoIP 서비스 구현에 필요한 코덱 선택 및 블랙홀 침해 관련 권고 사항을 본 논문의 결과로 제시하였다.

ABSTRACT

In this paper, transmission performance for serval VoIP traffics is meaured and analysised over MANET(Mobile Ad-hoc Networks) under some types of intrusions. VoIP simulator based on NS-2 is used for performance measure. In the simulation, MOS, network delay, packet loss rate and call connection rate is measured for transmission performance. With analysis of measued data, characteristics of each traffics for transmission performance parameters is showed on MANET under multi intrusions, As a results of this paper, some recommendation condtion for codec selection and blackhole intrusion is suggested to implement VoIP services on MANET under multi intrusions like as DDoS and blockhole intrusions.

키워드

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

Ⅰ. 서 론

기반구조를 사용하지 않고 단말기들 사이에 임시로 구성되는 통신 네트워크인 MANET(Mobile Ad-hoc Network)는 설치 및 유지가 수월하여 긴급통신이나 레저목적 같은 개인통신에 편리하게 사용되어질 수 있다.지능형 단말인 스마트폰의 급속한 보급은 기반구조 통신을 사용할수 없는 환경에서 단말기 만으로 구성되는 MANET의 사용을 증가시킬 것으로 예상된다.

인터넷을 기반으로 하는 음성 전화 서비스인 VoIP(Voice over Internet Protocol) 서비스는 유선 인터넷 환경에서 기존의 유선전화서비스를 빠르게 대체하고 있으며, 모바일 영역으로 범위를 확대하고 있다.

그런데 모바일 VoIP는 기지국과 같은 기반통신구조의 사용을 전제로 하는 것으로서 기반구조 사용이 곤란한 환경에서 VoIP 사용을 보장하는 것은 아니다.

* 동양대학교 정보통신공학과(ydkim@dyu.ac.kr)
접수일자 : 2012. 02. 29 심사(수정)일자 : 2012. 03. 23 게재확정일자 : 2012. 04. 07

그러므로 기반구조 사용이 없은 MANET 환경에서 VoIP 시스템과 관련된 연구는 매우 의미있는 일이다[1][2].

스마트폰은 MANET구축 수단 제공과 같이 통신환경에 긍정적인 요인과 더불어 지능형 기능으로 인한 역기능 또한 보유하고 있다. 그 역기능의 하나가 정보침해이다. 사용자 응용 프로그램 실행 기능으로 인해 스마트폰은 그 자체가 침해의 대상이 될 뿐만 아니라 침해의 수단으로 사용될 수 있으며, 스마트폰에 의한 정보침해는 지속적으로 증가할 것으로 예상된다. 스마트폰과 같은 지능형 MANET 단말기에 대한 기능적 발달은 네트워크 관리 측면에서 긍정적인 요소 뿐만 아니라 부정적인 요소도 동시에 발생시키고 있다. 이는 단말기의 발달이 정보침해를 발생시키는 수단으로서는 좋은 환경을 제공하지만 정보침해 대비를 위한 수단으로서는 수월하지 못함을 의미한다. 단말기로서는 정보침해 대비가 수월한 서버급 성능을 확보하기가 쉽지 않기 때문이다.

MANET에서 정보침해 유형은 매우 다양하지만 그 가운데 대표적인 예가 DDoS(Distributed Denial of Service) 침해와 블랙홀(blackhole) 침해이다.

DDoS 침해는 트래픽을 과다하게 발생시켜 네트워크의 기능을 마비시키는 것으로 네트워크 형태에 무관하게 발생될 수 있는 정보 침해 유형이다. DDoS에 의한 MANET 상의 한 노드에 대한 트래픽 집중은 그 노드의 기능의 마비시킨다. MANET에서는 전체 노드가 라우팅 기능을 잘 수행해야 네트워크 기능이 정상을 유지할수 있다. 따라서 DDoS 침해에 의한 일부 노드의 기능 이상은 전체 네트워크의 장애를 발생시켜 네트워크 성능에 치명적인 영향을 주게 된다[3][4].

블랙홀 공격은 라우팅 기능에 영향을 주어 트래픽의 이동 장소를 변형시키는 공격으로 라우팅 기능이 빈번하게 사용되는 MANET에 심각한 영향을 주는 침해 현상이다. 블랙홀 공격의 경우 네트워크 성능 자체는 저하되지 않는 반면에 노드에 도착해야할 정보가 다른 노드로 이동하여 원래의 목적지에 도착하지 않게 되므로 사용자간에 정보전송이 올바르게 이루어지지 않게 되는 침해이다. 따라서 송수신 노드간의 호 연결 자체를 마비시키는 결과를 초래하게 된다[5][6].

본 논문에서는 이와같이 서로 다른 유형의 침해가 다중으로 발생되는 MANET 환경에서 침해가 응용서비스로서 VoIP 트래픽의 전송에 미치는 영향을 분석해보았다. G.711, GSM.AMR, G.723A와 같은 여러 종류의 VoIP 트래픽을 대상으로 성능을 분석하였으며, 분석결과를 사용해서 다중침해대비 관련 권고를 MANET VoIP 서비스 구현 조건으로 제시하였다.

본 논문은 NS(Network Simulator)-2를 기반으로 VoIP 모듈을 추가하여 구성한 시뮬레이터를 사용하여 수행되었다. 시뮬레이션에서 MANET는 750×750[㎡] 규모와 36개의 노드로 구성하였다. 시뮬레이션에서는 MOS, 네트워크지연, 패킷손실율, 호연결율을 측정하였다.

본 논문의 구성은 다음과 같다. I장은 서론이며, II장은 MANET의 침해, III장은 시뮬레이션 및 성능분석 그리고 IV장에서 결론으로 연구결과 및 향후의 연구방향을 제시하였다.

II. MANET의 침해

2.1. MANET 침해 유형

MANET에 대한 침해유형은 네트워크 계층 구조에서 각 계층 별로 다양하게 나타나고 있다. 그러나 네트워크 계층의 패킷전달 기능이나 라우팅기능에 대한 침해가 보다 심각한 현상을 발생시킨다.

패킷전달 기능에 대한 침해는 노드를 대상으로 발생되는 유형으로 침해대상노드에 패킷을 대량으로 유입시켜 노드가 수행해야 할 응용서비스 실행 기능 뿐만 아니라 네트워크 지원 기능의 저하 또는 마비 시킨다. 노드의 기능 이상은 MANET 노드가 수행해야 할 라우팅이나 패킷 전달 기능에 문제점을 발생시켜 네트워크 전체의 기능 이상을 일으킨다. DDoS가 대표적인 예이다.

반면에 라우팅 기능 침해는 노드에 대한 침해와는 달리 네트워크의 기능에 대한 침해 유형으로 라우팅 정보의 파라미터 값을 추가하거나 변경하여 패킷의 올바른 전달을 방해할 목적으로 시도된다. 블랙홀(black hole), 그레이홀(gray hole), 웜홀(warm hole) 침해 등이 대표적이다.

2.2. DDoS 침해

DDoS는 악성 노드가 네트워크의 특정 노드에 대하여 트래픽을 집중적으로 전송시켜 그 노드의 송수신 기능을 마시키는 침해 유형이다.

단말기 중심으로 운용되는 MANET은 방화벽이나 서버급 침해 방지 시스템 사용이 곤란한 환경에서 사용되는 네트워크이므로 MANET에 대한 DDoS 공격은 네트워크 전체에 치명적인 영향을 주게 된다. 복수개의 DDoS 노드가 일반노드에 대하여 트래픽을 발생시키면 그 노드는 기능이 저하되거나 또는 중단되어 네트워크 전체의 트래픽 전송이 마비되는 현상을 발생시키는 것이다. 그림 1은 이와 같은 DDoS 침해의 예이다.

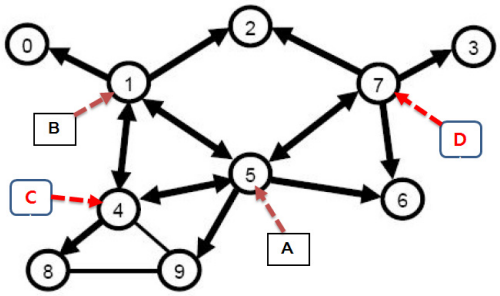

그림 1. MANET에서 DDoS 침해[7]
Fig. 1 DDoS intrusions on MANET[7]

그림 1에서 DDoS 노드 A,B,C,D가 일반노드 1,4,5,7에 대하여 각각 그림과 같이 공격을 시도하여 노드의 기능을 현저하게 저하시키거나 마시키면 노드 1,4,5,7은 MANET 에 대해 라우팅 및 중계기능을 제공할 수 없게 되므로 네트워크는 {0},{2},{3},{6},{8,9}로 분리되어 통신기능을 상실하게 된다[7].

2.3. 블랙홀 침해

라우팅 기능의 침해 가운데 한 종류인 블랙홀 침해는 라우팅 정보를 변경하여 모든 노드들이 블랙홀 노드로 패킷을 전송하게 하고 이를 수신한 블랙홀 노드는 더 이상 패킷을 전송하지 않고 흡수하여 네트워크의 전달기능을 마비시키는 침해이다[6].

그림 2는 블랙홀 공격 과정을 보여주고 있다. 그림 2에서 노드들은 동적 라우팅 방법 가운데 하나인 ADOV(Ad-Hoc On-Demand Distance Vector)라우팅을 사용하여 경로를 선정한다. AODV는 패킷 전송 요구가 있을 경우에 전송경로를 생성하는 방식이며 RREQ(Route Request), RREP(Request Replay), RRER(Route Error)등의 제어 패킷을 사용하여 경로를 생성하고 관리한다.

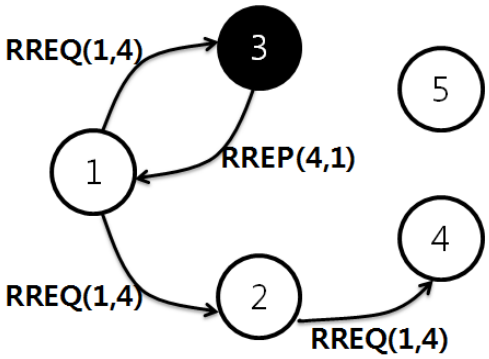

그림 2. MANET에서 블랙홀 침해[5]
Fig. 2 Blackhole intrusions on MANET[5]

그림 2에서 노드 3은 블랙홀 노드이고 노드1,2,4,5는 일반 노드이다. 노드 1은 노드 4로 전송하기 위해서 RREQ 패킷을 사용하여 경로선정 과정을 시작한다. 노드 1의 RREQ 패킷은 브로드캐스팅 방식으로 인접노드를 거쳐 노드4에 전달된다. 노드 1로부터의 RREQ 패킷을 수신한 노드 4는 RREP 패킷을 노드 1로 전송하여 경로 선정을 완성한다[5].

그림 2에서 노드 1에 인접한 블랙홀 노드인 노드 3이 노드 4로 보내어져야 하는 노드 1의 RREQ 패킷을 수신하면 블랙홀 노드는 자신이 마치 수신 노드인 노드 4인 것처럼 RREP 패킷을 설정하여 노드 1로 송신한다. 블랙홀 노드의 RREP 패킷을 수신한 노드 1은 블랙홀 노드인 노드 3을 노드 4로 인식하여 데이터 패킷을 송신하게 된다. 노드 1의 데이터 패킷을 가로챈 블랙홀 노드는 노드 4로 데이터 패킷을 내보내지 않고 폐기하여 전송기능을 마비시킨다[5].

III. 시뮬레이션 및 성능분석

3.1. 시뮬레이터

본 논문은 다중 침해가 있는 MANET의 성능측정을 컴퓨터 시뮬레이션을 사용하여 수행하였으며, 응용서비스로는 VoIP를 대상으로 하였다.

시뮬레이터는 NS-2 2.33을 기반으로 NS2VoIP 패치를 사용하여 구축하였다[8][9]. MANET 기능은 NS-2의 ADHOC 기능을 사용하였으며, VoIP 트래픽은 NS2VoIP 기능을 사용하여 코덱 규격에 맞추어 생성하도록 하였다.

DDoS 및 블랙홀 침해를 다중침해로 설정하고, 침해를 일으키는 악성노드는 정해진 기간 동안 DDoS 또는 블랙홀 침해를 발생시키도록 시뮬레이터를 구성하였다. 악성노드는 무작위로 선택하였으며, 침해대상 일반노드는 역시 랜덤하게 선정하였다.

3.2 시뮬레이션 환경

시뮬레이션에서 일반노드와 악성노드를 비롯한 각 노드들은 정해진 규모의 MANET내에 랜덤하게 분포하며, 최대 2㎧이하의 랜덤 속도와 랜덤한 방향으로 독립적으로 이동한다. 즉 일반노드들은 악성노드로부터 발생되는 DDoS나 블랙홀 침해가 있는 환경 하에서 최대 2㎧속도의 랜덤 이동 중에 다른 일반노드들과 VoIP 트래픽을 송수신한다.

한 노드가 생성할 수 있는 최대 VoIP 연결수는 1로 설정하였다. 따라서 MANET의 최대 VoIP 연결수는 전체 일반노드 수의 1/2이하이다. VoIP 트래픽은 G.711, G.729A, GSM.AMR 규격에 맞추어 생성하였으며, 기타 시뮬레이션 환경은 표 1과 같다.

표 1. 시뮬레이션 파라미터
Table 1. Simulation parameters

파라메터	설정값	
네트워크 규모	750×750[㎡]	
MAC	802.11g (54Mbps)	
라우팅	AODV	
노드수	일반노드	30
	블랙홀 노드	1
	DDoS 노드	5
VoIP 연결 수	최대 15	
VoIP 트래픽	G.723.1, G.729A, GSM.AMR	

3.3 성능 파라미터

본 논문에서는 MOS, 종단간지연, 호성공율, 패킷손실율을 MANET의 VoIP 성능평가척도로 사용하였으며, 각각의 요구수준은 표 2와 같다[7].

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 패킷손실율 요구수준은 5%로 가정하였다[7].

3.4 시뮬레이션 결과 및 분석

본 논문에서는 시뮬레이션을 3.1~3.3절의 조건에 따라 수행하였다. 시뮬레이션은 VoIP 연결수에 따라 VoIP 트래픽을 G.723.1, G.729A, GSM.AMR 코덱으로 구분하여 수행하였다. 시뮬레이션은 각각 180초간 실시하였으며, 침해는 시뮬레이션 기간 동안 지속하여 발생되도록 하였다. 시뮬레이션 결과를 그림 2~5에 제시하였다.

그림 2는 MOS 측정 결과이다. 그림 2에서 침해가 없을 경우 G.231.1, G.729A, GSM.AMR 모두 MOS 요구수준 3.6을 충족하고 있다. 반면 다중침해가 있을 경우, GSM.AMR은 MOS 요구수준 3.6을 충족하지만 G.729A는 요구수준을 충족하고 있지 못하며, G.723.1은 연결수에 따라 가변적이다. 이는 GSM.AMR 트래픽이 다른 트래픽에 비해 DDoS나 블랙홀 침해에 강함을 보여주는 결과이다.

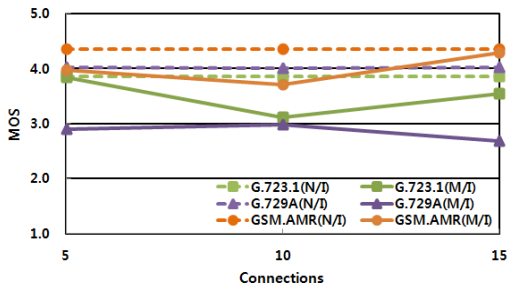

그림 2. MOS
Fig. 2 MOS

그림 3은 네트워크 지연 결과이다. 그림 3에 의하면 GSM.AMR 트래픽은 지연요구수준인 300㎳를 만족시키기고 있지만 G.729A는 지연요구수준을 충족하지 못하고 있으며, G.723.1은 가변적이다.

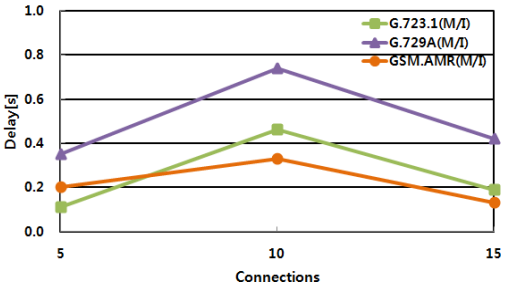

그림 3. 네트워크 지연
Fig. 3 Network delay

그림 4는 패킷 손실율을 제시하고 있다. 그림 4에서 GSM.AMR 트래픽은 패킷 손실율 요구수준 5%를 충족시키고 있지만, G.723.1은 요구 수준을 충족하지 못하며, G.729A는 측정지점에 따라 가변적 결과를 보여주고 있다.

.

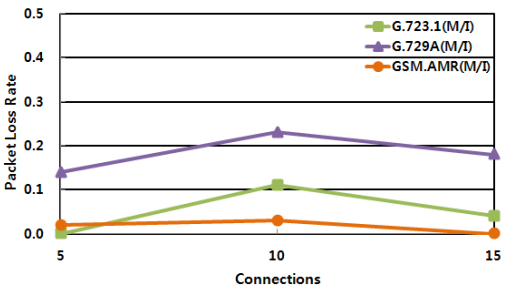

그림 4. 패킷 손실율
Fig. 4 Packet loss rate

그림 5는 호 연결율 측정 결과이다. 이 결과는 시도된 연결 가운데 성공한 연결의 비율을 나타낸 것으로서 G.723.1와 GSM.AMR이 30~50%, G.729A가 20~80%의 성공율을 보여, 모든 트래픽이 전 측정 구간에서 요구 주순 95%를 충족하지 못하고 있다

그림 5의 호 연결율 결과는 주로 블랙홀 침해에 의하여 발생되는 결과로서 MANET 환경에서는 블랙홀 침해가 DDoS에 비해 치명적임을 보여주고 있다.

반면에 MOS, 네트워크 지연, 패킷손실율은 블랙홀 침해보다는 DDoS 침해에 더 영향을 받는 것으로 보여진다. 이는 트래픽의 유형에 따라 그 전송특성이 상이하여 그로 인해 침해에 따른 통신품질도 달리 측정되는 것으로 분석된다.

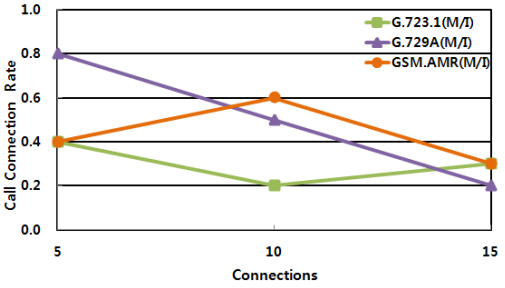

그림 5. 호 연결율
Fig. 5 Call connection rate

3.5 침해 대비 권고

3.4절의 시뮬레이션 결과 분석에서 살펴본 바와 같이 DDoS 침해와 블랙홀 침해가 동시에 발생되는 다중 침해 가능성이 있는 MANET에서 VoIP 시스템을 구축할 경우, MOS 품질을 위해서는 DDoS 침해 대비 수단이 필요하며, 호연결율 요구수준을 충족하기 위해서는 적절한 블랙홀 침해 대비 알고리즘이 요구된다. 침해 대비 수단은 단말기 단위로 설치되어야 하며, 아울러 단말기는 GSM.AMR와 같이 다중 침해에 강한 코덱을 사용해서 트래픽을 생성해야 한다.

Ⅳ. 결 론

본 논문에서는 DDoS 침해와 블랙홀 침해가 동시에 존재하는 MANET에서 VoIP 트래픽의 전송성능을 컴퓨터 시뮬레이션으로 분석하여 다중 침해가 트래픽 전송에 미치는 영향을 분석하였다.

본 논문에서 제시한 연구 결과로서 다중침해가 발생되는 MANET에서 VoIP 구현을 위해서는 통신 품질을 보증을 위해 GSM.AMR과 같은 적절한 코덱을 사용하여 트래픽을 생성하야 하며, 호연결율을 보장하기 위해서는 블랙홀 침해 대비 기능이 지원되어야 한다.

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

본 논문의 결과를 확장하여 다양한 규격과 다양한 특성을 갖는 MANET 환경에서 다중침해가 MANET 응용 서비스에 미치는 영향과 침해 대비 기능을 구축하는 것이 추후 연구 과제이다.

참고 문헌

[1] 김영동, "대규모 MANET에서 VoIP 트래픽의 종단간 성능", 한국전자통신학회논문지, 6권, 1호, pp. 49~54, 2011.

[2] 김영동, "MANET에서 패킷 취합을 이용한 VoIP 성능 개선", 한국전자통신학회논문지, 5권 3호, pp. 275~280, 2010.

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

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

[5] 김영동, “블랙홀 공격이 있는 MANET에서 VoIP 트래픽의 전송성능”, 한국해양정보통신학회 종합학술대회 논문집, 15권, 2호, pp.637~640, 2011.

[6] 김영동, “DDoS와 블랙홀 공격이 있는 MANET에서 VoIP 트래픽의 전송성능”, 한국전자통신학회 종합학술대회논문지, 5권, 2호, pp.432~435, 2011.

[7] 김영동, “DDoS 침해가 있는 MANET에서 VoIP 트래픽의 성능”, 한국전자통신학회논문지, 6권 4호, pp.493~498, 2011.

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

[9] 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, Oct., 2007.

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 정보통신공학과 교수

※ 관심분야 : 통신프로토콜, MANET, VoIP, 컴퓨터 시뮬레이션, 정보보호