Regular paper http://dx.doi.org/10.13067/JKIECS.2014.9.6.695

패킷취합전송이 있는 MANET에서 IDS 성능

김영동*

IDS Performance on MANET with Packet Aggregation Transmissions

Young-Dong Kim*

요 약

블랙홀 공격은 라우팅 정보를 무단으로 변경하여 전송성능에 치명적인 영향을 초래할 수 있다. 블랙홀 공격에 대응하는 수단으로서 IDS(Intrusion Detection System) 또는 IPS(Intrusion Prevention System) 등을 사용할 경우 일정 정도의 전송성능을 개선할 수 있다. 본문에서는 블랙홀 공격이 발생되는 MANET(Mobile Ad-hoc Network)에서 IDS가 종단간 성능에 미치는 영향을 패킷취합전송 관점에서 분석한다. 성능분석은 NS-2를 기반으로 구축한 MANET 시뮬레이터를 사용하였으며, 음성 서비스인 VoIP(Voice over Internet Protocol) 트래픽을 대상으로 음성서비스 표준 성능 파라미터인 MOS(Mean Opinion Score), 연결율, 지연 및 패킷손실율을 분석하였고, 본 논문에서 제시한 성능팩터를 활용한 분석을 제시하였다. 성능분석 결과의 하나로 패킷취합전송을 사용하는 MANET에서 블랙홀 공격에 대비한 IDS 조건을 제시하였다.

ABSTRACT

Blackhole attacks having a unauthorized change of routing data will cause critical effects for transmission performance. The transmission performance will be improved to the a certain level by using or having IDS(Intrusion Detection System)/IPS(Intrusion Prevention System) as countermeasures to blackhole attacks. In this papar, the effects of IDS to ene-to-end performance of packet aggregation transmission are analyzed on MANET(Mobile Ad-hoc Network) with IDS under blackhole attacks. MANET simulator based on NS-2 is used to analyze performance parameters as MOS, connection ratio, delay and packet loss rate as standard performance parameters, an another performance factor which is suggested in this paper. VoIP(Voice over Internet Protocol) traffics, one of voice services, is used for performance analysis. A suggestion for IDS implementation on MANET with packet aggregations under blackhole is shown as one of results.

키워드

MANET, Blackhole, IDS, Simulation
마넷, 블랙홀, 아이디에스, 시뮬레이션

Ⅰ. 서 론

MANET(Mobile Ad-hoc Network)은 라우터나 AP(Access Point)와 같은 통신기반구조를 사용하지 않고 단말기를 중심으로 구축되는 임시통신망으로서 군사, 재난, 탐험/탐사, 취미활동과 같은 응용 영역에서 매우 유용하게 활용될 수 있으며, 최근 Wi/Fi 기능을 갖춘 스마트폰 탭을 비롯한 스마트형 단말기의

* 교신저자(corresponding author) : 동양대학교 정보통신공학과(ydkim@dyu.ac.kr)
접수일자 : 2014. 04. 11 심사(수정)일자 : 2014. 05. 23 게재확정일자 : 2014. 06. 16

급속한 보급으로 활용이 증가될 것으로 예상된다.

스마트형 지능 단말기의 급속한 보급은 MANET의 구축환경 개선 및 보급 확대 가능성 향상이라는 긍정적인 요인뿐만 아니라 침해 가능성 또는 기회가 급속하게 증가하는 부정적인 요인도 초래하고 있다.

MANET에 대한 대표적인 정보침해로 라우팅 정보에 변경을 주어 패킷의 정상적인 전송을 방해하는 블랙홀(blackhole) 공격을 들 수 있다[1]. 블랙홀 공격은 MANET내에서 전송되는 패킷들을 블랙홀 노드로 수신되게 함으로서 다른 노드들에 대한 패킷 정상 수신을 방해하는 정보침해이다[2]. 블랙홀 공격에 대응하는 수단으로서는 블랙홀 공격의 발생을 탐지하여 대응하게 하는 IDS(Intrusion Detection System), 블랙홀 공격 발생을 차단하는 IPS(Intrusion Prevention System) 등 이 있다.

본 논문에서는 블랙홀 공격에 대응하는 수단으로서 IDS가 MANET 전송성능에 미치는 영향을 패킷취합 전송 관점에서 측정하고 분석하였다. 본 논문은 컴퓨터 시뮬레이션을 사용하여 수행하였다. NS-2를 기반으로 한 MANET 시뮬레이터를 구축하여 음성서비스인 VoIP(Voice over Internet Protocol)를 대상으로 전송성능을 분석하였다. 성능 분석에는 음성서비스 표준 성능 파라미터인 MOS(Mean Opinion Score), 호연결율, 전송지연을 및 패킷손실을 사용하였으며, MOS와 호연결율을 종합하여 고려한 새로운 성능팩터를 도입하여 성능분석에 사용하였다. 성능분석 결과의 하나로서 패킷취합전송을 사용하는 MANET에서 블랙홀 공격에 대비한 IDS 조건을 제시하였다.

본 논문은 2장에서 블랙홀 공격, IDS 및 패킷취합전송과 같은 관련이론을 기술하고, 3장에서는 시뮬레이션 및 성능분석을 제시하고, 4장에서 결론을 맺는다.

II. 관련 이론

2.1. 블랙홀 공격

MANET에 대한 대표적인 공격 형태로 라우팅 기능에 대한 공격을 들 수 있다. 라우팅 기능에 대한 공격은 MANET의 중요 기능인 라우팅 기능을 변경시켜 패킷전달이 비정상적으로 수행되게 하는 유형으로 블랙홀 공격이 대표적이다.

블랙홀 공격은 악성노드인 블랙홀 노드가 라우팅 정보를 무단으로 변경하여 자신이 수신노드인 것처럼 MANET에 전파함으로서 패킷이 블랙홀 노드로 이동하게 한 다음 수신한 패킷을 폐기하여 원 수신노드로 패킷을 수신되지 못하도록 하는 공격 형태이다.

그림 1의 블랙홀 공격에서 노드 1은 노드 4로 데이터 패킷을 전송하기에 앞서 RREQ(1,4) 패킷을 사용하여 경로선정 절차에 들어간다. 노드 1이 발송한 RREQ(1,4) 패킷은 노드 1에 인접한 노드 2와 노드 3을 거쳐 전파되어진다. RREQ(1,4)를 수신한 블랙홀 노드 3은 노드 4가 응답해야할 RREP(4,1)을 위조하여 노드 1로 송신한다. 노드 1은 블랙홀 노드 3이 송신한 RREP(4,1)을 노드4가 보낸 것으로 인식하고 노드 3으로 전송경로를 설정하고 데이터 패킷을 송신한다. 블랙홀 노드 3은 데이터 패킷을 수신한 후에 노드 4로 전달하지 않고 폐기하여 데이터 패킷이 노드 4로 수신되지 못하도록 한다. 노드 1에서 노드 4로의 데이터 전송은 정상적으로 수행되지 못한다.

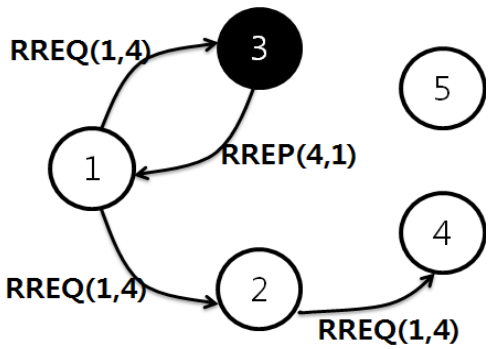

그림 1. 블랙홀 공격
Fig. 1 Blackhole attacks

2.2. IDS

블랙홀 공격에 대응하는 방안의 하나로서 IDS는 블랙홀 공격이 발생될 경우 이를 탐지하는 체계를 의미한다.

그림 2에 제시된 IDS는 MANET을 통과해서 수신되는 RREP() 패킷의 수신시간 차를 이용하여 블랙홀 공격을 탐지하는 방법이다.

그림 2에서 블랙홀 노드 3으로 부터 블랙홀 공격을 받아 노드 3을 수신 노드로 오인한 노드 1은 노드 3

으로 데이터 패킷을 송신한다. 이 공격이 진행되는 중에 원 수신노드 4로부터 RREP(4,1) 패킷이 노드 2를 거쳐 노드 1에 도착한다. 노드 1은 노드 4로부터 수신된 RREP(4,1)을 원 수신노드로부터 발신된 패킷으로 판단하고 노드 2를 경유하여 노드 4에 이르는 전송경로로 재설정하고 블랙홀 노드 3에 의하여 설정된 전송경로를 즉시 폐기한다. 블랙홀 노드 3으로의 전송은 중단되며, 원 수신노드인 노드 4로의 데이터 패킷 전송이 시작된다.

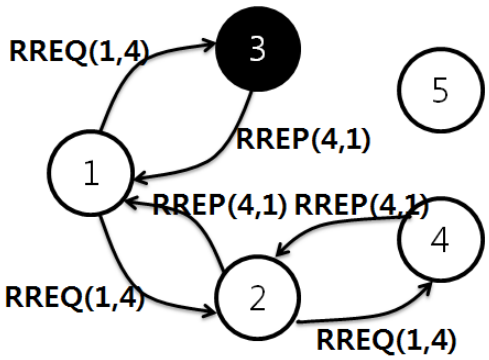

그림 2. IDS AODV[1]
Fig. 2 IDS AODV[1]

2.3. 패킷취합전송

MANET은 기반구조 네트워크에 비하여 전송효율이 낮아 응용트래픽의 양을 축소하거나 전송횟수를 줄이는 등의 여러 가지 전송성능개선 방안이 연구되고 있다.

패킷취합전송은 응용트래픽의 전송횟수를 줄이기 위해 패킷 여러 개를 하나의 패킷에 취합하여 전송하여 전송성능을 개선한다. 특히 전송대상이 음성 트래픽일 경우 단위 패킷의 길이가 짧아 패킷취합방식을 사용할 경우 상당한 수준으로 전송성능을 개선할 수 있어 VoIP와 같은 응용서비스에 매우 유용할 수 있다[3].

MANET에서 패킷취합전송을 사용할 경우 그림 3과 같이 패킷 취합의 수에 비례하여 패킷오버헤드의 축소 및 전송제어절차의 간소화 등을 달성할 수 있어 응용 트래픽의 전송성능개선에 상당히 효과적이다.

정보침해가 발생되는 환경에서 패킷취합전송은 패킷취합전송을 사용하지 않을 때에 비해 유실되는 정보의 단위가 증가된다. 그러므로 전송성능개선을 위해 패킷취합전송이 사용되고, 블랙홀 공격에 대응하여 IDS가 사용되는 MANET 환경에서 패킷취합전송의 종단간 전송성능을 응용트래픽 관점에서 분석해보는 것은 매우 의미 있는 일이다.

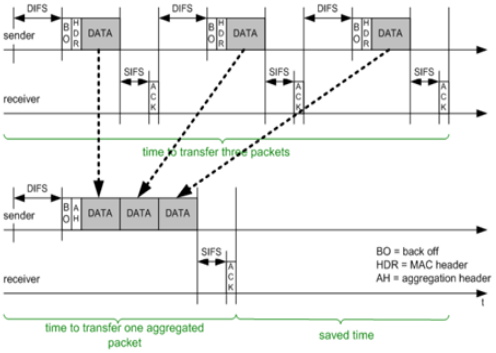

그림 3. 패킷취합전송[3]
Fig. 3 Packet aggregation transmission[3]

III. 시뮬레이션 및 성능 분석

3.1. 시뮬레이터

본 논문에서는 블랙홀 공격에 대하여 IDS로 대응하는 MANET 환경에서 패킷취합전송의 종단간 전송성능을 응용서비스 트래픽의 일종인 음성트래픽을 대상으로 측정·분석한다.

성능측정에는 NS-2를 기반으로 한 컴퓨터 시뮬레이션를 사용하였다. 시뮬레이터는 MANET은 NS-2의 ADHOC 기능을 사용하여 구현하였으며, 블랙홀공격과 IDS 기능은 NS-2의 AODV모듈을 활용하여 구축하였다. VoIP 기능은 NS2VoIP 패치[4]를 사용하였으며 음성 트래픽 표준 규격에 맞추어 생성하였다. 시뮬레이터에서 라우팅 기능으로 일반노드는 AODV 모듈, 블랙홀 노드는 blackholeADOV 모듈, IDS 노드는 IDSAODV 모듈을 사용하였다.

본 논문에서 사용한 시뮬레이터에서 일반 노드는 블랙홀 공격에 대응 수단을 갖지 못한 노드를 의미하며, IDS 노드는 일반 노드가 블랙홀 공격에 대한 대응수단으로 IDS를 갖출 때를 의미한다. 본 논문의 시뮬레이션에는 블랙홀 노드를 제외한 노드는 전체가

일반노드이거나 IDS 노드로 구성하였다.

3.2. 시뮬레이션 환경

시뮬레이션에서 일반 노드, IDS 노드 및 블랙홀 노드는 정해진 규모의 MANET에 랜덤하게 분포하며, 각 노들은 최대 2[m/s]의 랜덤속도로 랜덤방향으로 서로 독립적으로 이동한다. 일반 노드, IDS 노드는 랜덤 이동 중에 VoIP 트래픽을 송수신한다. 블랙홀 노드는 VoIP 트래픽을 전송하지 않는 것으로 간주하였다.

시뮬레이션에서 한 노드가 생성 가능한 VoIP 최대 연결 수는 1로 설정하였다. 따라서 MANET내에 존재할수 있는 최대 연결수는 전체 일반노드, IDS 노드 수의 1/2이다. 일반노드가 전송하는 VoIP 트래픽은 GSM.AMR, G.723.1, G.729A, iLBC 규격에 따라 생성하였다.

기타 시뮬레이션 파라미터는 표 1과 같다.

표 1. 시뮬레이션 파라미터
Table 1. Simulation parameters

Parameters	Values	
Network Scale	750×750[m²]	
MAC	802.11b	
Routing	A O D V	
Nodes	Normal Nodes	29
	Blackhole Nodes	1
VoIP Connections	Max. 10	
VoIP Traffics	GSM.AMR G.723.1, G.729A, iLBC	

3.3. 성능 파라미터

VoIP 전송 성능에는 MOS, 지연 및 호연결율이 표준평가척도로서 사용되며 요구수준[5-7]은 표 2와 같다. 또 다른 평가척도로서 패킷 손실율이 5[%]이하 요구수준으로 사용되고 있다.

이외에 본 논문에서는 3.5절에 제시된 성능 팩터를 새로운 평가척도 도입하여 사용하며, 0.835를 요구수준으로 사용한다.

표 2. 모바일 VoIP 전송 품질
Table 2. Mobile VoIP transmisson quality

Quality Index		Requirements
Call Quality	MOS	≥3.6
	Delay	≤300[ms]
Establish Quality	Call Connection Ratio	≥95[%]

3.4. 시뮬레이션 결과

시뮬레이션은 3.1~3.3절에 제시된 조건에 맞추어 패킷취합수에 따라 구분하여 각 측정별로 60초 동안 실시하였다. 블랙홀 공격은 시뮬레이션 전 기간에 지속적으로 발생되는 것으로 설정하였다.

그림 4~7에 GSM.AMR 트래픽에 대한 시뮬레이션 결과를 블랙홀 공격이 없는 경우(AODV)와 블랙홀 공격이 있는 경우(BHAODV), IDS로 대응하는 경우(IDSAODV)로 구분하여 제시하였다.

그림 4에서 블랙홀 공격이 있는 경우 패킷취합수가 증가함에 따라 MOS가 상당히 유동적인 것으로 나타났으나, IDS로 대응한 경우에 안정적이 되어 요구수준 3.6에 수렴하는 것으로 나타났다.

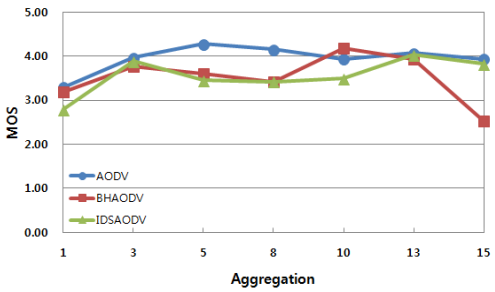

그림 4. MOS
Fig. 4 MOS

그림 5에서 호 연결율은 블랙홀 공격이 있는 경우에 패킷취합수의 증가에 따라 그 성능이 평균 40%로 급격하게 감소된다. 특히 패킷취합수가 15인 경우 20%까지 감소하는 것으로 나타났다. 반면에 IDS로 대응하는 경우 호연결율 요구수준 95%에는 도달하지 못하였으나 평균 55%까지 향상되었다.

종단간 지연은 그림 6과 같이 패킷취합수의 증가에

따라 개선되는 것으로 나타났다. 그러나 블랙홀 공격이 있는 경우 종단간 지연에 변동이 있는 것으로 관찰되었다. 블랙홀 공격에 대하여 IDS로 대응한 경우 그 변동 폭이 일정한 수준으로 개선되었다.

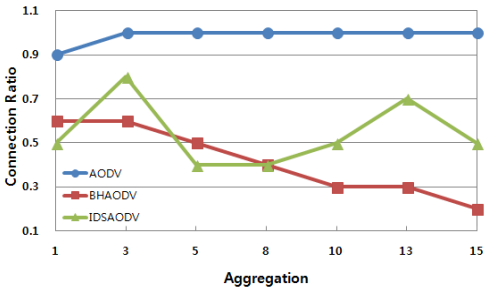

그림 5. 호 연결율
Fig. 5 Call connection rate

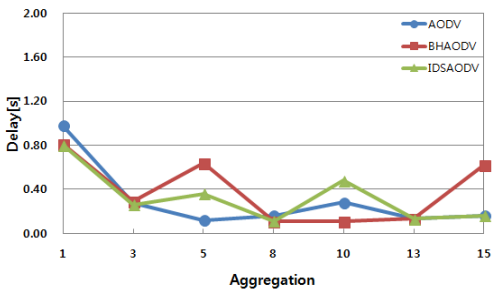

그림 6. 종단간 지연
Fig. 6 End-to-end delay

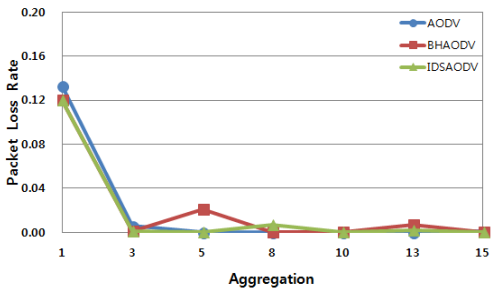

그림 7. 패킷손실율
Fig. 7 Packet loss rate

패킷손실율의 경우 그림 7과 같이 대부분 구간에서 요구조건 5[%]이하를 만족하는 것으로 나타났다.

3.5 제안 및 분석

그림 4에 제시된 MOS는 성공된 연결을 대상으로 측정한 결과로서 시도하였으나 성립되지 않은 연결은 고려되지 않았다. 이는 블랙홀 공격과 같은 침해가 발생되지 않은 상황을 전제로 한다면 타당할 수 있으나, 블랙홀 공격과 같은 침해가 발생될 경우에는 실패한 연결을 고려한 MOS를 관찰하는 것이 성능분석에 유리하다.

본 논문에서는 실패한 연결을 감안하기 위하여 호 연결율과 MOS를 종합적으로 고려한 성능팩터를 사용하였다. 이 성능팩터는 MOS와 호 연결율을 각각 50%의 비율로 하고 이를 합산한 최대 성능이 1로 다음과 같다.

$$PF = MOS / 5.0 \times 0.5 + CCR \times 0.5 \quad (1)$$

여기서, PF(Performance Factor) 성능팩터, CCR(Call Connection Ratio)는 호 연결율을 의미하며, MOS / 5.0은 측정된 MOS값을 최대 MOS 값인 5로 나눈 것으로 정규화 MOS를 뜻한다.

표 2의 MOS 요구조건 3.6과 호연결율 요구조건 0.95를 고려한 요구조건을 식(1)에서 환산하면 0.835이며, 이 값을 성능팩터 요구조건으로 사용한다.

그림 8은 패킷취합수에 따른 GSM.AMR 트래픽의 성능팩터 변화를 제시하고 있다. 그림에서 블랙홀 공격이 없으며 패킷취합을 사용할 경우 성능팩터가 요구조건인 0.835를 만족하고 있지만, 블랙홀 공격이 있을 경우와 IDS로 대응한 경우 모두에서 요구조건 0.835가 충족되지 않는다. 그러나 IDS로 대응한 경우 평균 0.55에서 0.64로 약 14[%]정도 성능이 개선되었다. 비록 성능이 향상되었음에도 요구조건 0.835에 도달하지 못하는 것은 그림 5와 같이 호 연결율이 매우 낮은데 원인이 있다.

그림 9는 표 1에서 제시한 시뮬레이션 대상 트래픽인 GSM.AMR, G.729A, G.731.1, iLBC의 성능팩터를 제시하고 있다. 이 결과는 그림 8과 같이 각 패킷취합별로 성능팩터를 구한 후에 평균을 구한 것이다.

그림에서 본 논문에서 사용한 네 종류의 트래픽 모두 블랙홀 공격 및 IDS 대응의 경우 대해 요구수준 0835를 충족하지 못하고 있다. 그러나 GSM.AMR, G.721.1 및 iLBC의 경우 블랙홀 공격과 IDS 대응 간

의 성능 차가 컷으며, G.723.1과 iLBC의 경우는 IDS 대응시에 성능팩터가 비교적 큰 것으로 나타나 패킷 취합을 사용하여 성능저하를 일정정도 방지할 수 있는 것으로 나타났다.

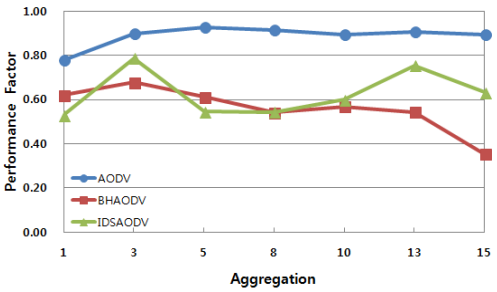

그림 8. 성능 팩터
Fig. 8 Performance factor

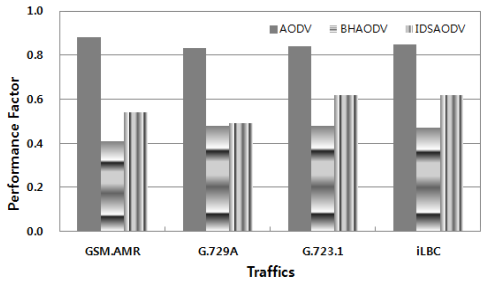

그림 9. 성능 팩터 비교
Fig. 9 Comparison of performance factor

그림 10은 종단간 지연을 제시하고 있다. 그림에서 G.723.1과 iLBC가 블랙홀 공격이 발생할 경우 종단간 지연 성능 저하가 가장 큰 것으로 나타났으나 IDS로 대응할 경우 성능 개선이 커서 요구조건 300[ms]를 충족하는 것으로 나타났다. 반면에 GSM.AMR은 블랙홀 공격의 영향을 적게 받는 것으로 나타났다.

그림 11에서 패킷손실율은 G.729A를 제외한 GSM.AMR, G.723.1, iLBC의 트래픽 모두가 요구조건 5[%]이하를 충족하는 것으로 나타났다.

그림 9~11을 고려하면 블랙홀 공격에 대하여 IDS로 대응한 경우 종단간 지연과 패킷손실율은 요구조건을 일정한 정도로 충족하는 반면에 성능팩터의 경우는 개선정도가 낮아 요구조건을 충족하지 못하고 있다. 이는 호 연결율에서 발생되는 문제이다. 따라서 블랙홀 공격이 있는 패킷취합전송 MANET에서 사용되는 IDS는 호연결율을 효과적으로 개선할수 있는 기능을 갖추어야 한다.

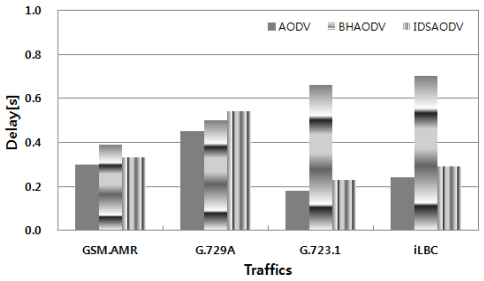

그림 10. 종단간 지연 비교
Fig. 10 Comparison of end-to-end delay

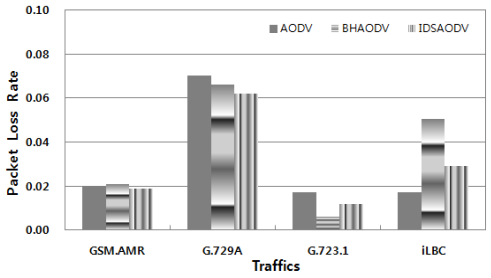

그림 11. 패킷손실율 비교
Fig. 11 Comparison of packet loss rate

Ⅳ. 결 론

본 논문에서는 블랙홀 공격에 대하여 IDS로 대응하는 MANET에서 패킷취합 전송이 전송성능에 미치는 영향을 컴퓨터 시뮬레이션을 사용하여 측정하고 분석하였다.

성능분석에는 기존의 MOS, 호연결율, 종단간지연, 패킷손실율을 사용하였으며, MOS와 호연결율을 종합적으로 고려한 성능팩터를 제시하였다. 시뮬레이션 결과 분석에 의하면 G.729A를 제외한 GSM.AMR, G.731.1, iLBC 트래픽은 블랙홀 공격에 대하여 IDS로 대응하면 패킷취합이 있을 경우 성능 개선이 있었다. 그러나 호 연결율의 성능저하로 인하여 성능팩터의 경우 요구조건 0.835에 미치지 못하므로 호 연결율을 개

선할수 있는 새로운 형태의 IDS의 구현이 요구된다.

본 논문의 결과는 블랙홀 공격이 발생되는 MANET에서 VoIP를 포함한 응용서비스의 적절한 운용을 위한 기본적인 자료로 사용될 수 있을 것으로 생각한다. 여러 MANET 운영 환경에 대한 시뮬레이션을 통하여 블랙홀 공격과 IDS대응의 영향을 분석하고 서비스 요구조건에 부응하는 운영방안을 모색하는 것이 추후 과제라 할 수 있다.

감사의 글

본 논문은 2013년도 동양대학교 교내연구지원 사업의 지원으로 수행되었음.

References

[1] Y. Kim, "Transmission Performance of Voice Traffic with Packet Aggregations on MANET under Black Hole Attacks," In *Proc. Conf. on The Korea Institute of Electronic Communication Sciences 2012*, vol. 6, no. 1, June 2013, pp. 368-371.

[2] H. Simarenare and R. Sari, "Performance Evaluation of AODV Variants on DDoS, Blackhole and Malicious Attacks," *Int. J. of Computer and Networks Security*, vol. 11, no. 6, June 2011, pp. 277-287.

[3] N. Bayer, M. Castro, P. Delay, A. Kassler, Y. Koucheryavy, P. Mitoray, and D. Staehle, "VoIP service performance optimization in pre-IEEE 802.11s Wireless Mesh Networks," In *IEEE Int. Conf. on Circuits & System for Communications (ICCSC2008)*, Shanghai, China, May 2008, pp. 75-79.

[4] A. Bacioccola, C. Cicconetti, and G. Stea, "User - level Performance Evluation of VoIP using NS-2," In *Proc. of 2nd Int. Conf. on Performance Evaluation Methodologies and Tools*, Nantes France, Oct. 2007.

[5] D. Choi, "Evaluation of VoIP Service Quality under the Roaming of Mobile Terminals," *J. of The Korea Institute of Electronic Communication Sciences*, vol. 7, no. 4, Aug. 2012, pp. 747-752.

[6] D. Choi, "Evaluation of VoIP Capacity for IEEE 802.11b WiFi Environment under Voice Coding Methods," *J. of The Korea Institute of Electronic Communication Sciences*, vol. 7, no. 2, Apr. 2012, pp. 243-248.

[7] B. Kim, "Software-based Quality Measurement of Mobile VoIP Services," *J. of The Korea Institute of Electronic Communication Sciences*, vol. 6, no. 1, Jan. 2011, pp. 55-60.

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, 수중통신