IDS가 있는 MANET에서 응용 서비스 트래픽의 전송 성능

김영동*

동양대학교

Transmission Performance of Application Service Traffic on MANET with IDS

Young-Dong Kim*

Dongyang University

E-mail : ydkim@dyu.ac.kr

요 약

MANET(Mobile Ad-Hoc Network)은 단말기만으로 구성되는 임시통신망으로서 설치·운영이 수월한 구조적 장점과 스마트폰의 급속한 보급이라는 환경적 변화로 인하여 기반구조의 사용이 어려운 긴급통신, 레저, 탐험/탐사와 같은 응용 분야에서 그 사용이 급속하게 늘어날 것으로 예측된다. 그러나 통신기반 구조를 사용하지 않은 MANET의 특성은 최근 들어 빈번하게 발생되고 있는 해킹과 같은 정보침해에 매우 취약한 단점을 발생시킨다. 본 논문에서는 이와 같은 MANET에서 정보침해 대응 방안의 하나인 IDS(Intrusion Detection System)가 MANET의 전송성능에 미치는 영향을 분석해 본다. 본 논문에서는 MANET에 대한 침해 유형으로 블랙홀(blackhole) 공격을 가정하고, 블랙홀 공격이 있을 경우 MANET 노드가 IDS를 사용하여 블랙홀 공격에 대응하도록 환경을 설정하였으며, 이를 NS-2를 이용한 컴퓨터 시뮬레이션으로 구현하고 전송 트래픽의 성능을 측정하였다. 본 논문에서는 IDS가 이용자 수준의 성능에 미치는 영향을 분석하기 위해서 응용 서비스 수준의 전송 성능을 측정하였으며, 대상 응용 서비스로는 VoIP를 가정하였다.

ABSTRACT

MANET, which can be constructed with only terminal devices, has structural advantages of ease installation and operation, also has environmental change of rapid supply of smart phone, it's usage can be extended to application area likes as emergency communication, leasure, exploration and investigations. But, as one characteristic of MANET, no use of communicaton infrastructure caused disadvantage of weakness for information intrusion which is frequently occurred, nowadays. In this paper, the effects of IDS(Intrusion Detection System), one of defence tools for information intrusion, is analyzed for transmission performance. Blackhole attack is assumed as a type of intrusion, MANET defence with IDS from intrusions. Computer simulation based on NS-2 used for performance measurement. In this paper, performance measurement is done for application service to analyze application level effects of IDS. VoIP service is used as application service.

키워드

IDS, Blackhole Attack, MANET, VoIP, NS2

Ⅰ. 서 론

MANET(Mobile Ad-Hoc Network)은 기반 구조를 사용하지 않는 통신망으로서 설치와 운용이 수월하기 때문에 군사적 목적, 지진·재난 등의 구조를 위한 긴급통신, 탐험·탐사와 같은 특수 통신에 활용되어왔다. 그러나 최근 들어 고성능 통신 단말기의 급속한 보급으로 MANET의 활용 영역이 특수 통신에서 일반 통신으로 확대되는 경향을 보이고 있다.

한편으로, 그 문제의 심각성이 최근 들어 급증하고 있는 정보침해는 불법적인 정보취득의 정도를 넘어 네트워크 일부 또는 전체에 치명적인 문제를 발생시키고 있다.

정보침해는 기반구조 네트워크에 비해 정보침해에서 보다 더 치명적 문제점을 일으킬 수 있다. 기반구조 네트워크의 경우 네트워크에 침해대비 수단을 마련하여 정보침해에 대비할 수 있으나

단말기들 사이에 임시로 구성되는 MANET의 경우 기반구조 네트워크와 같은 정도의 침해대비 수단을 활용하는 것이 쉽지 않기 때문이다. MANET의 주 응용 환경인 군사적 목적이나 긴급 재난 통신과 같은 상황에서 정보침해가 발생할 경우 그 결과는 매우 심각할 수 있다. 따라서 이와 같은 정보침해를 대비하는 방안을 강구하는 것은 MANET 서비스의 안정성을 확보하는 차원에서 매우 의미있는 일이라 할수있다.

본 논문은 정보침해가 발생되는 MANET에서 정보침해 대응 방안으로서 IDS(Intrusion Detection System)이 응용서비스의 전송 성능에 미치는 영향을 분석해 본다.

정보침해의 형태로서 블랙홀 공격을 사용하였으며, 분석 대상 응용 서비스로서는 VoIP(Voice over Internet Prorocol)을 선택하였다. 성능분석 방법으로는 NS-2를 기반으로한 컴퓨터 시뮬레이션을 사용하였다.

본 논문은 I장에서 서론을 제시하였고, II장에서는 블랙홀 공격, III장에서는 IDS에 대하여 설명하고, IV장에서 시뮬레이션과 성능해석 결과를, V장에서 결론을 제시한다.

II. 블랙홀 공격

블랙홀(blackehole) 공격은 MANET에서 라우팅 정보를 변경하여 패킷의 전송을 방해하는 공격유형으로 네트워크 계층에서 발생되는 공격유형 가운데 하나이다.[1]

블랙홀 공격에서 블랙홀 노드는 라우팅 정보를 변조하여 모든 노드들이 블랙홀 노드로 패킷을 전송하게 하여 이를 수신한 다음에 패킷을 더 이상 전송하지 않고 전송을 종료시켜 송수신을 방해한다.[2][3]

블랙홀 공격 과정을 살펴보면 그림 1과 같다. 그림 1의 MANET은 동적 라우팅 방식의 한 종류인 AODV(Ad-Hoc On-Demand Distance Vector) 라우팅을 사용한다. AODV는 노드가 필요로 할 때에 경로를 생성하여 라우팅 테이블에 관리하는 방식으로, 이 과정에서 RREQ(Route Request), RREP(Request Replay), RRER(Route Error)등의 관리 패킷이 사용된다.

블랙홀 공격이 없는 정상적인 경우에서 노드 1에서 노드 4로의 데이터 전송을 위한 경로설정 과정을 살펴보면 다음과 같다. 노드 1이 노드 4로 전송하기 위해서는 데이터 패킷 전송에 앞서 노드 1은 RREQ 패킷을 사용해서 경로 선정과정을 시작한다. 노드 1의 RREQ 패킷은 브로드캐스팅 방식으로 인접노드들에 전달되고 인접노든 다시 자신에 인접한 노드들에게 노드 1의 RREQ 패킷을 전달한다. 이런 과정을 거쳐 목적지 노드인 노드 4에 노드 1의 RREQ 패킷이 전달되게 된다. 노드 1의 RREQ 패킷을 수신한 노드 4는 노드 1로 RREP 패킷을 송신하여 경로 설정을 완성한다.

그러나 그림 1에서 노드 3이 블랙홀 노드로 동작하므로, 경로 선정과정은 다음과 같이 변형되어진다. 노드 1에 인접한 블랙홀 노드가 노드 1의 RREQ 패킷을 수신하게 되면 자신이 노드 4인 것처럼 RREP 패킷을 설정하여 노드 1로 송신한다. 블랙홀 노드의 RREP 패킷을 수신한 노드 1은 블랙홀 노드를 노드 4로 인식하게 되며 데이터 패킷을 노드 3으로 송신하게 된다. 즉 노드 4로 전송되어야 할 데이터가 블랙홀 노드인 노드 3으로 송신되는 것이다. 노드 1의 데이터 패킷을 가로챈 블랙홀 노드는 더 이상 데이터를 전달하지 않고 전송을 멈추어 데이터 패킷이 노드 4로 전송되는 것을 불가능하게 한다. 블랙홀 노드는 전송되는 패킷을 수신한 다음에 송신을 하지 않아 네트워크 내의 모든 패킷을 자신에게로 흡수되게 한다.

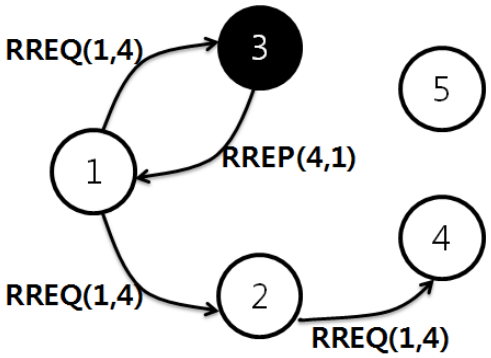

그림 1. 블랙홀 공격.[4]

블랙홀 공격이 발생될 경우 전송이 TCP 방식으로 이루어진다면 정해진 시간 내에 도달되어야 할 TCP_ACK 패킷이 도착하지 않기 때문에 송신 노드는 경로 오류로 판단하고 경로 재설정을 시도하게 된다. 그러나 이 재결정 과정에서도 블랙홀 노드는 RREQ 패킷을 수신하게 되고 RREP 패킷을 사용하여 자신을 수신 노드로 속여 송신 노드가 자신에게로 전송경로를 설정하게 만든다. 한편, UDP 방식은 ACK가 운영되지 않으므로 TCP에 비하여 그 결과가 치명적일 수 있다.

III. IDS

IDS(Intrusion Detection System)은 침해 검출 시스템으로 MANET의 블랙홀 공격과 관련한 IDS로서는 IDSAODV과 대표적이다.

IDSAODV는 AODV에서 라우팅 기능을 조정하여 라우팅 기능에 대한 침해에 대응하는 방식이다. 두 번째 도착한 RREP 패킷을 사용하여 경로를 조정함으로써 블랙홀 공격에 대응할 수 있다.[5]

노드는 RREQ 패킷을 전송한 후에 첫 번째 도

착한 RREP 패킷을 사용하여 경로를 선정하고 데이터 패킷을 전송한다. 이후에 두 번째 RREP 패킷이 도착하면 경로를 다시 설정하여 블랙홀 공격을 피할 수 있게 한다.

그림 2에서 노드 1이 노드 4로 패킷로 경로를 선정하기 위해 RREQ(1,4)를 송신하게 되면 블랙홀 노드인 노드 3이 응답한 RREP(1,4)에 노드 1에 도착하게 된다. 노드 1은 이를 기반으로 노드 3으로 패킷을 송신하게 된다. 이후에 노드 1에 두 번째 RREP(1,4) 패킷이 노드 4로부터 노드 2를 거쳐 도착하면 노드 1은 노드 4로의 전송경로를 노드 2를 경유하는 경로로 재설정한다. 따라서 첫 번째 RREP(1,4)를 거쳐서 설정된 블랙홀 노드인 노드 3으로의 전송은 중단되고 일반노드인 노드 4로의 전송이 정상적으로 이루어지게 된다.

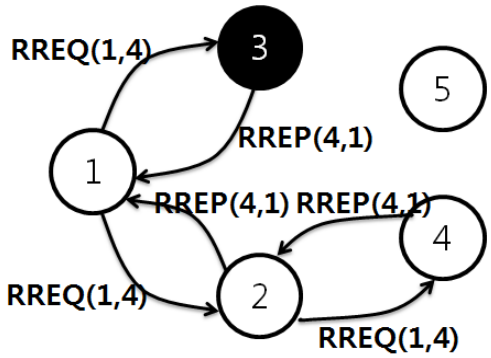

그림 2. IDSAODV.

IV. 전송성능

본 논문에서는 블랙홀 공격이 있는 MANET에서 그 대응 방안 가운데 하나인 IDSAODV가 응용서비스에 미치는 영향을 컴퓨터 시뮬레이션을 사용하여 분석하였다.

시뮬레이터는 NS-2[6]를 기반으로 블랙홀 기능, IDS IDSAODV, VoIP 기능을 추가하여 구축하였다. 블랙홀 기능과 IDSAODV는 일반 AODV 라우팅 프로토콜을 수정하여 구현하였으며, VoIP 기능은 NS2VoIP 모듈[7]을 사용하였다.

본 연구에서 사용된 시뮬레이션 환경은 다음과 같다.

네트워크 규모 : 750X750[㎡]
노드 수 : 30(일반노드 : 29, 블랙홀노드 : 1)
라우팅 : AODV
MAC : 802.11g
VoIP 트래픽 : GSM.AMR

일정한 영역에 랜덤하게 분포한 노들은 시나리오파일에 정해진 값에 따라 네트워크 내에서 랜덤방향과 랜덤속도로 이동한다. 노드 이동속도는 최대 2.0[m/s]로 설정하였다.

네트워크 내의 노드들은 랜덤 이동을 하는 중에 VoIP 트래픽을 송신하거나 수신한다. 한 노드가 생성할 수 있는 연결의 수는 1로 설정하였다. 따라서 네트워크에서 생성될 수 있는 연결의 최대 수는 14이다. 14개의 연결은 총 30개의 노드 가운데 블랙홀 노드를 제외한 일반노드 29가 생성할수 있는 VoIP 연결의 최대수를 의미한다.

시뮬레이션은 각 측정 점에 대하여 600초 동안 실행하였다. 시뮬레이션 결과로서 VoIP 전송 성능 파라메타로 많이 사용되는 MOS와 연결율을 그림 3와 4에 각각 제시하였다.

그림 3은 노드수가 30일 때 연결의 수에 따른 MOS의 변화를 블랙홀 공격이 없는 경우(AODV), 블랙홀 공격이 있으나 IDS를 사용하지 않은 경우(BHAODV) 그리고 블랙홀 공격에 대하여 IDS를 사용하여 대응한 경우(IDSAODV)를 비교하여 제시하고 있다. 그림 3에서 연결수는 성공한 연결수가 통화를 시도한 연결수를 의미한다.

그림 3에서 MOS는 성공한 연결에 대하여 측정된 통화품일로서 블랙홀 공격이나 IDS의 사용여부에 따라 다소 변화가 있으나 세 경우 모두 VoIP 통화품질 기준인 3.6을 충족하고 있다. 그러나 AODV가 높고, BHAODV가 가장 낮으며, IDSAODV가 그 중간 품질을 보이고 있어 블랙홀 공격과 IDS를 사용한 대응이 전송에 미치는 영향을 살펴볼수 있다.

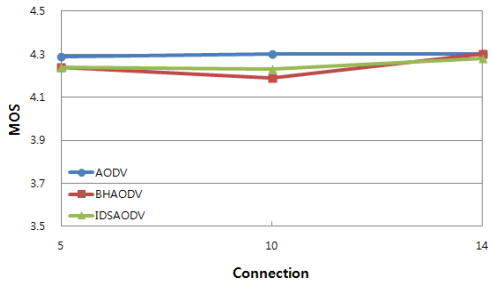

그림 3. MOS.

그림 4는 블랙홀 공격과 IDS 대응에 대한 호 연결율을 제시하고 있다. 블랙홀 공격이 없을 경우(AODV) 시도한 모든 연결이 성공하여 통화가 이루어진, 반면에 블랙홀 공격이 있고 IDS 대응을 시도하지 않은 경우(BHAODV)는 호 연결율은 약 60%정도이다. 반면에 블랙홀 공격에 대하여 IDS로 대응한 경우(IDSAODV)는 호 성공률이 약 80%까지 증가하여 IDS가 없는 경우에 비하여 약 20%정도의 호 연결율 개선이 되었다. 그러나 개선의 정도는 VoIP 연결율 기준인 95%에 비하여 약 15% 정도 낮다.

그림 4에서 제시된 연결율은 블랙홀 노드의 영향으로 시도한 연결이 성공되지 않거나, 연결이

성공하였다 하더라도 음성트래픽이 전송되지 않아서 연결이 성립되지 않은 경우를 제외한 연결의 비율을 의미한다.

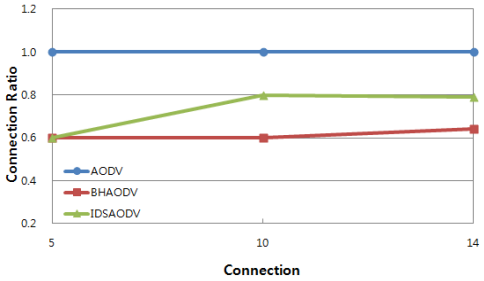

그림 4. 연결율.

그림 3와 4에서 VoIP 서비스를 사용하는 MANET상을 대상으로 한 블랙홀 공격은 VoIP 통화품질 보다는 연결율에 더 큰 영향을 미치며, IDS를 사용한 개선 역시 통화품질 보다는 연결율 개선에 더 양호한 결과를 내는 것으로 확인되고 있다.

V. 결 론

본 논문에서는 블랙홀 공격에 대한 대응 수단으로 IDS를 사용하는 MANET에서 응용서비스로서 VoIP 트래픽의 전송성능을 컴퓨터 시뮬레이션을 사용하여 분석하여 보았다.

NS-2를 사용하여 구현한 시뮬레이레이터를 사용하여 VoIP 성능으로서 MOS와 호연결율을 측정하였다.

통화품질로서 MOS는 블랙홀 공격이 없는 경우, 블랙홀 공격이 있는 경우, 블랙홀 공격에 IDS로 대응한 경우 모두에 대하여 측정값이 VoIP 통화품질 기준인 3.6을 만족하였다. 그러나 블랙홀 공격이 있는 경우는 다소 낮았으며, IDS를 사용한 경우는 IDS를 사용하지 않은 경우에 비해 MOS 값이 다소 개선되었다.

반면에 호 연결율은 블랙홀 공격이 있는 경우 60%정도로 낮았고, IDS로 대응한 경우 80%정도로 개선되었다. 그러나 연결율 기준인 95%에는 못미쳤다.

VoIP 서비스에 대한 블랙홀 공격과 IDS를 사용한 대응은 통화품질 보다는 연결설정에 더 큰 영향을 미치고 있음을 확인하였다.

본 논문의 결과는 MANET에서 VoIP 구현을 위한 기본적인 자료 및 MANET에서 블랙홀 공격과 IDS 사용이 응용서비스에 미치는 영향의 분석 방법으로 활용될 수 있을 것으로 생각된다.

블랙홀 공격이 있는 MANET 환경에서 응용서비스 품질 기준을 만족시킬수 있는 적절한 IDS 대응 방안을 모색하는 것이 추후 과제라 이다.

참고문헌

[1] G. Sandhu, M. Dasgupta, "Impact of Blackhole Attack in MANET", International j. of Recent trends in Engineering and Technology, Vol.3, No.2, pp.183-186, May, 2010.

[2] S. Sharma, R. Gupta, "Simulation Study of Blackhole Attack in the Mobile Ad Hoc Networks", Journal of Engineering Science and Technology, Vol.4, No.2, pp. 243-250, 2009.

[3] R. Goyal, P. A. Ghosh, "Evaluation of Cooperative Black Hole Attack in AODV Routing Protocol in MANET", BLB-International Journal of Science & Technology, Vol. 1, No. 2, pp.161-170, 2010.

[4] 김영동, "블랙홀 공격이 있는 MANET에서 VoIP 트래픽의 전송성능", 한국해양정보통신학회, 2011 추계종합학술대회 논문집, 2011.10.

[5] S. Dokurer, Y. Erten, C. Acar, "Performance analysis of ad-hoc networks under black hole attacks", SoutheastConf, Proceeding of IEEE, pp.148-154, March. 2007.

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

[7] A. Bacioccola, C. Cicconetti, G. Stea, "User-level Performance Evaluation of VoIP using ns-2", Proceedings of 2nd International Conference on Performance Evaluation Methodology and Tools, Oct., 2007.