Grayhole 공격이 있는 MANET의 전송성능

김영동*

동양대학교

Transmission Performance of MANET under Grayhole Attack

Young-Dong Kim*

Dongyang University

E-mail : ydkim@dyu.ac.kr

요 약

MANET(Mobile Ad-Hoc Network)의 라우팅 기능에 대한 공격인 홀 공격은 네트워크 전송성능에 중요한 영향을 미친다. MANET은 단말기만으로 구성되는 임시 네트워크로 악성공격에 대한 대응이 쉽지 않아 홀 공격에 매우 취약하여 전송성능에 치명적인 영향을 받을 수 있다. 본 연구에서는 홀 공격의 일종은 그레이홀 공격이 MANET의 전송 성능에 미치는 영향을 컴퓨터 시뮬레이션을 사용하여 분석하여 본다. 연구의 대상 트래픽으로는 음성 트래픽을 사용하였으며, 그레이홀 공격의 영향을 블랙홀 공격과 비교하여 본다. 본 연구의 방법과 결과는 MANET에서 악성공격에 대응하기 위한 자료로 활용될 수 있다.

ABSTRACT

As attack to routing function on MANET(Mobile Ad-Hoc Network), hole attack make cause some critical effects. MANET is easily influenced with hole attack and can be critically effected on transmission performance, because it is configured with terminal device as temporary network and dose not have effective means for malicious attack. In this paper, effects of grayhole attack to network performance on MANTE is analyzed with computer simulation. Voice traffic is used in simulation, effects of grayhole attack is compaerd with blackhole attack. The method and result of this paper can be used for data to study grayhoke attack

키워드

MANET, Grayhole Attack, Performance, Simulation

Ⅰ. 서 론

홀 공격(grayhole attack)은 네트워크에서 전송되는 라우팅 정보를 무단으로 생성하거나 위조하여 유통시키는 악성공격의 일종으로 전송기능을 방해하여 네트워크 성능에 치명적인 결과를 초래할 수 있다.

블랙홀(blackhole) 공격, 그레이 홀(grayhole) 공격, 웜홀(wormhole) 공격 등이 대표적인 홀 공격으로 분류된다. 네트워크에서 전송되는 모든 데이터를 블랙홀 노드로 이동되도록 한 후에 폐기함으로서 정보의 정상적인 전송을 방해하는 블랙홀 공격매우 치명적인 공격이다. 그에 비해 그레이홀 공격은 지정된 형식의 데이터를 그레이홀 노드로 전송되도록 하는 방식으로 블랙홀 보다 치명적이지는 않으나 탐지하기가 어려운 문제점을 안고 있다. 한편, 터널방식으로 전송링크를 설정하여 데이터를 임의의 장소로 무단 이동시키는 웜홀 공격 또한 네트워크 라우팅 정보에 중대한 영향을 초래한다.

본 논문에서는 그레이홀 공격이 MANET의 전송성능에 미치는 영향을 분석하여 본다. 그레이홀 공격의 영향을 블랙홀 공격의 영향과 비교하여 분석하였다.

본 연구는 NS-2를 기반으로 하는 컴퓨터 시뮬레이션을 사용하여 수행하였다. 전송대상 트래픽으로는 대표적인 디지털 음성 트래픽인 VoIP(Voice over Internet Protocol) 트래픽을 사

용하였다.

본 논문의 결과로서 그레이홀 공격의 영향이 블랙홀 공격에 비하여 성능 저하가 다소 낮은 것으로 관찰 되었다.

그레이홀 공격이 MANET에서 전송되는 데이터 유형에 대하여 미치는 영향을 살펴보는 것이 추후 과제이며, 본 논문의 연구방법과 분석결과는 MANET에서 블랙홀 공격에 대한 영향을 분석하기 위한 자료로 활용할 수 있을 것으로 생각된다.

II. 그레이홀 공격

그레이홀 공격은 블랙홀 공격이나 웜홀 공격과 같이 네트워크 라우팅 기능에 대한 공격으로 경로의 발견 및 유지, 패킷의 전달 기능을 공격하여 네트워크의 정상적인 전송을 방해하는 악성공격이다.

그레이홀 공격은 라우팅 정보를 무단으로 위조 또는 변경하여 그레이홀 노드로 패킷이 전달되도록하고 그레이홀 노드로 전달된 패킷을 폐기함으로서 일반 노드의 전송기능을 방해한다.[1][2]

공격노드로 전달된 패킷 전체를 폐기하는 블랙홀 노드와는 달리 그레이홀 공격은 지정된 유형의 패킷만을 폐기함으로서 블랙홀 공격과 차별된다.

그림 1에 제시된 그레이홀 공격에서 그레이홀 노드는 노드 1이 노드로 4로 전송경로를 설정하기 위하여 전파시킨 정상적인 RREQ(4,1) 패킷에 대하여 위조된 비정상 RREP(1,4)을 발생시켜 전송 경로를 노드 1에서 자신으로 설정하도록 한다. 노드 1은 위조된 RREP(1,4)의 수신에 근거하여 노드 4로의 경로를 악성노드인 그레이홀 노드 3으로 설정하고 패킷을 송신한다.

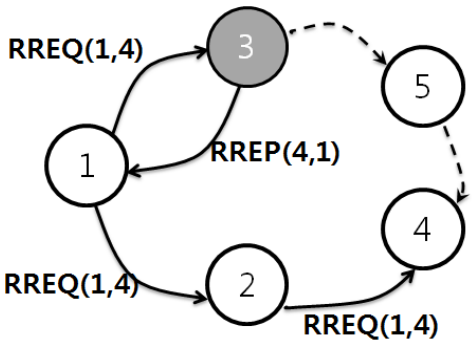

그림 1. 그레이홀 공격.

그레이홀 노드 3은 노드 1로부터 수신된 패킷 가운데 지정된 유형의 패킷을 선별적으로 폐기하여 노드 1의 전송을 방해한다.

그레이홀 공격의 선별적 패킷 폐기는 전송성능의 저하 측면에서는 블랙홀 공격에 비하여 다소 유리한 점이 있으나, 공격의 발견과 대처가 수월하지 못하다는 점에서는 매우 불리한 것도 있다.

III. 시뮬레이션 및 전송성능

본 논문에서는 그레이홀 공격이 MANET 전송성능에 미치는 영향을 컴퓨터 시뮬레이션을 사용하여 분석하였다. 전송성능을 분석하기 위한 대상으로 음성트래픽을 사용하였다.

본 논문의 시뮬레이터는 NS-2[3]를 기반으로 AODV 라우팅 기능을 수정한 grayholeAODV 모듈[4], NS2VoIP 모듈[5]을 사용하여 구축하였다. grayholeAODV는 그레이홀 노드 기능에 사용하며, NS2VoIP는 VoIP 서비스 기능에 사용하였다.

그레이홀 공격에서 폐기대상 패킷은 NS-2 시뮬레이터에 그림 2과 같이 반영하였다. 랜덤넘버를 사용하여 폐기대상 패킷을 선정하였다.[4]

```
//If destination address is itsself
if ( (u_int32_t)ih->saddr() == index)
    forward((grayholeaodv_rt_entry*) 0, p, NO_DELAY);
else if ((rand()%6)==3 || (rand()%6)==4 || (rand()%6)==1)
// For grayhole attack in the wireless adhoc ~
    drop(p, DROP_RTR_ROUTE_LOOP);
```

그림 2. 폐기대상 패킷의 선정 과정.[1][4]

시뮬레이션에서 사용한 파라미터는 다음과 같다.

네트워크 규모 : 750X750[㎡]
노드 수 : 30 (일반노드:29, 그레이홀노드:1)
노드 이동 : 최대 2.0[㎧] 랜덤 이동
라우팅 : AODV
MAC : 802.11g
VoIP 트래픽 : GSM.AMR

그림 3은 시뮬레이터의 작동 과정을 보여준다. 그림 3에서 30개의 노드들은 750X750[㎡]의 MANET내에 임의의 위치에 랜덤하게 분포하고 있으며 시뮬레이션의 시작과 함께 최대 2.0[㎧]의 속도로 랜덤이동을 한다. 노드들은 이동 중에 임의의 노드들과 음성트래픽을 전송한다. 이때 한 노드가 처리할 수 있는 연결의 수는 1로 가정하였으며 최대 연결의 수는 노드의 1/2이다.

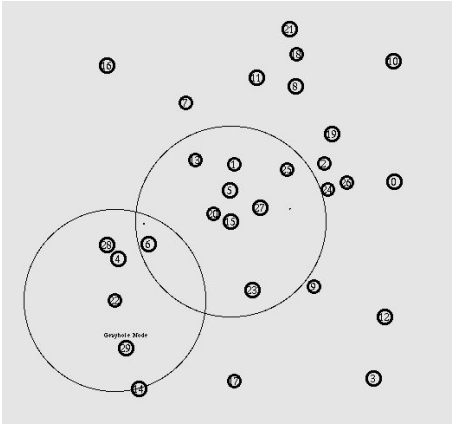

그림 3. 시뮬레이션 과정.

그림 4와 5에 시뮬레이션 결과로서 MOS(Mean Opinion Score)와 호연결율을 각각 제시하였다. 그림 4와 5는 시뮬레이션을 600[초] 동안 실시하여 얻은 결과로, 그레이홀 공격이 없는 경우(AODV), 그레이홀 공격이 있는 경우(GHAODV), 블랙홀 공격이 있는 경우(BHAODV)를 비교하여 제시하고 있다.

그림 4는 그레이홀 공격이 있는 MANET에서 음성 트래픽의 전송성능을 제시한 것으로 대표적인 전송품질인 MOS를 보여주고 있다. 그림 4에서 MOS에 대한 그레이홀 공격의 영향은 블랙홀 공격과 마찬가지로 미미한 것으로 관찰되었다. 그레이홀 공격에도 불구하고 요구조건 3.6을 상회하여 만족하는 것으로 나타났다.

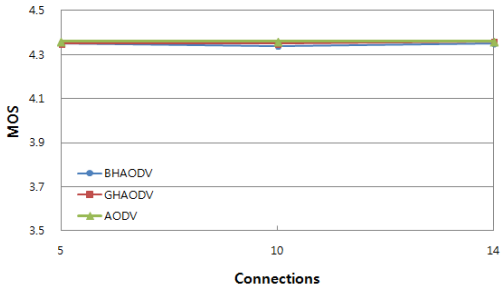

그림 4. MOS.

그림 5는 호 연결율로 연결을 시도한 호와 연결에 성공한 호의 비율은 나타낸다. 그림 5에서 그레이홀 공격이 있는 경우의 호연결율이 75[%]로 블랙홀 공격이 있는 경우의 호연결율 54[%]에 비하여 약 20%정도 높은 것으로 관찰되었으나 호연결율 요구조건 95[%]에는 매우 낮은 것으로 관찰되었다. 있다.

그림 4와 5에 의하면 그레이홀 공격의 영향이 블랙홀에 비하여 다소 낮으나 공격이 없는 경우에 대하여 호 연결율이 MOS에 비하여 많은 영향을 받는 것으로 나타났다.

이는 MOS가 성공한 연결에 대하여 측정한 값이 기인한 것으로 호 연결이 이루어진 후에는 악성공격의 영향이 덜하기 때문이다. 따라서 그레이홀 공격이 발생될 경우 호 연결율을 개선하기 위한 방안의 연구가 요구된다.

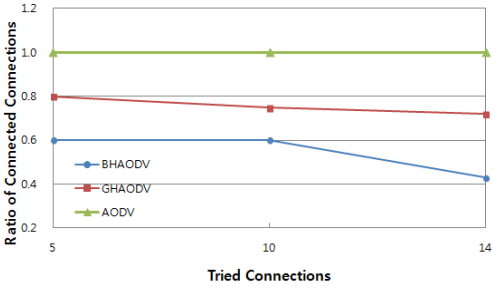

그림 5. 호 연결율.

Ⅳ. 결 론

본 논문에서는 그레이홀 공격이 있는 MANET의 전송성능을 컴퓨터 시뮬레이션을 사용하여 분석하였다.

NS-2를 기반으로 하여 구축한 시뮬레이터에서 VoIP 트래픽을 대상으로 전송성능을 측정한 결과로서 MOS와 호연결율의 변화를 시도한 호연결수를 중심으로 살펴 보았다.

그레이홀 공격의 영향은 MOS에 비하여 호 연결율에 대하여 더 심각한 것으로 측정되었으나 블랙홀 공격에 비해서는 다소 영향이 약한 것으로 관찰되었다. MANET에서 그레이홀 공격에 대비하여 호 연결율을 안정적으로 운영하기 위한 방안의 모색이 필요함을 알 수 있었다.

본 논문의 연구방법과 연구결과는 MANET에서 그레이홀 공격에 대한 영향분석 및 대응방안 마련 수단의 연구에 사용할 수 있다.

그레이홀 공격이 MANET 환경에서 그레이홀 공격의 영향을 폐기되는 패킷의 유형을 포함하여 다양한 측면에서 분석하는 것이 추후 과제라 할 수 있다.

참고문헌

[1] B. H. Karthik Pai, H. R. Nagesh, N. Chiplunkar, “Detection and Performance Analysis of Various DOS Attacks under Collaborative Environment”, Proceedings of ERCICA 2013, pp. 722~729, 2013.

[2] G. Neekhra, S. Patel, A. Verma, A.

Chaurasia, “Effect of Grayhole Attack With Ids Technique For Aodv Routing Using Network Simulatior”, Proceedings of IJARCET, Vol. 3, Issue 12, pp. 4184~4190.
[3] http://nsnam.isi.edu/nsnam.
[4] J. Kaur, V. Kumar, “An Effectual Defense Method against Gray Hole Attack in Wireless Sensor Network”, Proceedings of IJCSIT, vol.3, no. 3, pp.4523~4528, 2012.
[5] 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, Oct., 2007.