간헐적 블랙홀 공격이 있는 MANET의 전송성능

김영동*

동양대학교

Transmission Performance of MANET with Intermittent Blackhole Attacks

Young-Dong Kim*

Dongyang University

E-mail : ydkim@dyu.ac.kr

요 약

단말기만으로 구성되는 임시통신망으로서 MANET(Mobile Ad-hoc Network)은 기반구조 통신망에 비하여 설치와 운영이 수월한 구조적 장점, Wi/Fi 기능 및 고성능의 연산 능력을 탑재한 스마트폰의 급속한 보급이라는 환경적 변화를 토대로 통신 기반구조의 사용이 어려운 긴급통신, 레저, 탐험/탐사와 같은 응용분야에서 그 사용이 증가하고 있다. 그러나 통신 기반구조의 사용이 어려운 특성으로 인하여 MANET은 해킹과 같은 정보침해에 매우 취약한 단점을 보이고 있다. 본 논문에서는 이와 같은 MANET에서 정보침해가 전송성능에 미치는 영향을 분석하여 본다. 기존의 결과들이 네트워크에 대한 지속적인 침해가 발생되는 환경을 전제로 한 반면에 본 논문에서는 침해가 간헐적으로 발생되는 것으로 가정하였다. 본 논문은 침해유형으로 블랙홀 공격을 가정하였으며, 음성 트래픽을 전송 대상으로 하였다. NS-2를 이용한 컴퓨터 시뮬레이션을 사용하여 전송 성능을 측정하고 그 결과를 분석하여 보았다.

ABSTRACT

Based on easy construction and operation compared with infra-structure communication netowrks, and rapid spreading of smart phone having high powered calculation ability and Wi/Fi function, usage of MANET(Mobile Ad-Hoc Network), which is configured with simply several terminals, is increased in applications of emergency communications, leisure, explorations. However, because of supporting difficulty of communication infra-structure makes some defects of malicious information intrusion like as hacking. In this paper, effects of transmission performance caused by information intrusion is analyzed. The results of published studies is based on environment of continuous intrusions, but this paper assumed intermittent attacking condition. In this paper, blackhole attack is used for intrusion type to MANET, voice traffic is used as a application traffic. Compuer simulation, based on NS-2, is used for measuring of performance parameters, and the analysis for the simulation results is shown as considerations of this paper.

키워드

MANET, Blackhole Attack, Performance, Simulation, NS-2

Ⅰ. 서 론

전통적으로 MANET(Mobile Ad-Hoc Network)은 기반구조를 사용하지 않은 특성으로 인해 설치 및 운용이 수월해야 하는 군사적 목적, 지진/재난/구조를 우한 긴급통신, 탐험/탐사와 같은 특수통신 등에 활용되고 있다. 최근에는 스마트폰 사용의 급속한 확대로 인해 MANET의 활용은 특수응용영역을 넘어 일반응용분야로 확대될 것으로 예상된다.

한편, 문제의 심각성이 급격하게 증가하고 있는 정보침해는 정보의 불법적 취득을 넘어 네트워크에 치명적인 문제점을 일으키는 단계에 이르고 있으며, MANET을 비롯한 모든 유형의 네트워크에 나타나고 있다.

정보침해 현상은 인프라네트워크의 지원을 받을 수 있는 기반구조 통신망에 비하여 MANET에서 다음의 몇가지 이유로 인해 더 심각하게 나타난다. 첫째로 MANET은 정보침해에 대응할 수 있는 수단으로서 기반구조 통신망에서 사용되는

방화벽과 같은 서버급 장비를 사용하기가 곤란하기 때문이다. 두 번째 원인으로 단말기의 스마트 기능으로 인해서 정보침해를 발생시키는 악성 소프트웨어의 성능의 빠른 증가를 들 수 있다. 마지막으로 MANET의 경우에 단말기 성능이 높은 수준으로 개선되고 있다 하더라도 중계기능과 단말기능을 모두 수행해야 하는 MANET 단말기에 높은 수준의 정보침해 대응 기능을 구축하는 것은 여전히 쉽지 않은 일이기 때문이다. 이런 이유로 인해 일반응용분야는 물론이고 군사통신이나 긴급재난통신과 같은 특수응용분야에서 정보침해가 발생될 경우 그 결과는 매우 심각해질 수 있다.

따라서 MANET에서 정보침해의 영향을 분석해보는 것은 매우 의미 있는 일이다. MANET에서 대표적인 정보침해 유형인 블랙홀 공격이 있는 전송환경에 대한 성능 분석은 여러 연구에서 이루어져왔다.[1][2][3] 이 연구들에서는 블랙홀 공격이 지속적으로 발생되어지는 상황을 전제로 이루어진 결과들이다.

본 연구에서는 MANET에서 블랙홀 공격이 간헐적으로 시도되는 환경에서 전송성능을 분석하였다. 이를 통하여 블랙홀 공격의 공격시간이 전송성능에 미치는 영향을 고찰해보았다. 분석대상 응용서비스로는 VoIP 트래픽을 사용하며, 분석도구로는 NS-2를 기반으로 한 컴퓨터 시뮬레이션을 사용하였다.

II. 블랙홀 공격

MANET에 대한 정보침해 유형은 프로토콜 모델의 각 계층별로 매우 다양하게 나타나고 있다. 그 가운데 가장 대표적인 침해 유형이 홀(hole) 공격이다.

홀 공격은 MANET의 핵심 기능 중에 하나인 라우팅 기능에 대한 공격으로 라우팅 정보를 변경하거나 마비시켜 송/수신측 사이의 정보전달이 이루어지지 못하도록 하거나 네트워크 자체를 마비시켜 버리는 결과를 발생시키는 공격 유형이다.

홀 공격에 대한 예로는 블랙홀(blackhole) 공격, 그레이홀(grayhole) 공격, 웜홀(wormhole) 공격 등이 있으며, 이 가운데 블랙홀 공격이 네트워크 성능 측면에서 가장 위협적이다.

블랙홀 공격은 라우팅 정보를 불법적으로 변경하여 MANET 내의 모든 노들이 블랙홀 공격을 시도한 블랙홀 노드를 수신노드로 인식하도록 하게 하여, 다른 모든 노들이 패킷을 블랙홀 노드인 자신에게로 전송하게 하고 이를 수신한 다음에는 패킷을 폐기하여 본래의 수신측에 전송되지 못하도록 하는 형태의 공격이다.[1][2][3]

AODV(Ad-Hoc On-Demand Distance Vector) 라우팅에서 발생되는 블랙홀 공격 과정을 그림 1에 제시하였다. 동적 라우팅 방식의 하나인 AODV 라우팅은 노드가 필요로 할 때에 경로를 생성하고, 라우팅 테이블에 이를 관리하는 방식으로 RREQ(Route Request), RREP(Request Replay), RRER(Route Error)등의 패킷을 사용하여 경로를 관리한다.

그림 1에서 노드 1/2/4/5는 일반노드이고, 노드 3은 블랙홀 노드이다. 노드 1이 노드 4로 전송하기 위해 먼저 노드 1이 RREQ 패킷을 사용해서 경로 선정과정을 개시한다. 만약 노드 3이 블랙홀 노드가 아닌 일반노드인 경우라면, 노드 1의 RREQ 패킷은 브로드캐스팅 방식으로 RREQ 패킷이 MANET내의 모든 노드들에 전달한다. 목적지 노드인 노드 4에 노드 1의 RREQ 패킷이 전달되면, 노드 4는 노드 1로 RREP 패킷을 송신하여 경로 설정을 완성하게 된다.

그러나, 노드 3이 블랙홀 노드로 동작할 경우, 노드 1에 인접한 블랙홀 노드가 노드 1의 RREQ 패킷을 수신하게 되면 자신이 노드 4인 것처럼 RREP 패킷을 설정하여 노드 1로 송신한다. 노드 1이 블랙홀 노드의 RREP 패킷을 수신하면, 노드 1은 블랙홀 노드를 노드 4로 인식하고 데이터 패킷을 노드 3으로 송신한다. 즉, 노드 4로 전송되어야 할 데이터가 블랙홀 노드인 노드 3으로 전송되는 것이다. 노드 1의 데이터 패킷을 가로챈 블랙홀 노드는 노드 1로부터 전송되어온 데이터를 노드 4로 전달하지 않고 폐기하여 노드 4로의 데이터 전송을 마비시킨다.

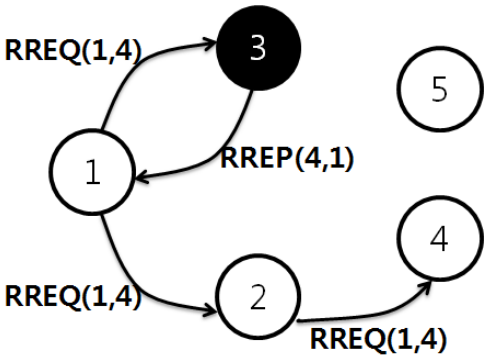

그림 1. 블랙홀 공격.[3]

블랙홀 공격이 발생될 경우 UDP 전송이 TCP 전송에 비해 치명적일 수 있다. TCP 경우 정해진 시간 내에 ACK 패킷이 도착되어 전송성공 유무를 확인할 수 있지만 UDP의 경우 ACK가 운영되지 않기 때문이다.

본 연구에서는 그림 1과 같은 블랙홀 공격이 간헐적으로 발행되는 환경에서 MANET 전송성능을 고찰하여 본다.

III. 전송성능

본 논문에서는 간헐적 공격이 발생되는

MANET에서 응용트래픽의 전송성능을 NS-2[4]를 기반으로 한 컴퓨터 시뮬레이션을 사용하여 분석하였다. 전송성능 측정에 사용된 응용 트래픽으로는 VoIP 서비스를 사용하였다.

VoIP 서비스는 NS2VoIP 모듈을 사용하여 구현하였으며[5], 블랙홀 노드는 NS-2에서 사용하는 AODV 라우팅 프로토콜을 수정하여 구현하였다.

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 노드들은 시나리오파일에 정해진 값에 따라 네트워크 내를 랜덤 방향, 랜덤 속도로 이동한다. 노드 이동속도는 최대 2.0[m/s]로 설정하였으며, 이 속도는 사람의 이동속도는 고려한 것으로 7.2[km/h]를 의미한다.

노드가 지원하는 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 의미하는 것이다.

블랙홀 공격의 간헐성은 전체 시뮬레이션 시간에 대한 블랙홀 공격 시간의 비율로 구현하였으며, 0/25/50/75/100%로 구분하였다. 0%는 블랙홀 공격이 없는 경우, 100%는 시뮬레이션 전 구간에서 블랙홀 공격이 발생되는 것을 의미하며, 25/50/75%는 블랙홀 공격과 시뮬레이션 구간에 대한 비율이다. 즉 25%의 시뮬레이션 구간의 1/4 비율로 블랙홀 공격이 간헐적으로 발생되는 것을 의미하며, 50%의 경우 블랙홀 공격이 시뮬레이션 전 구간 대비 1/2 기간 동안 간헐적으로 발생되는 경우를 의미한다. 75%의 경우 시뮬레이션 구간의 3/4기간 동안에 간헐적으로 발생되는 것을 의미한다.

MANET 내의 노드들은 시나리오 파일에 정해진 랜덤 이동을 하는 중에 VoIP 트래픽을 송신하거나 수신한다.

각각 600초 동안 실행한 시뮬레이션 결과로서 VoIP 전송 성능 파라메타로 많이 사용되는 MOS와 호연결율을 그림 2와 3에 각각 제시하였다. 그림 2와 3에서 AODV는 블랙홀 공격이 없는 경우, BHAIODV(nnn)는 각각 간헐적 블랙홀 각각 숫자 nnn%의 비유율로 발생되는 것을 의미한다.

그림 2는 노드수가 30일 때 연결의 수에 따른 MOS의 변화를 블랙홀 공격이 있는 경우, 없는 경우, 간헐적 공격이 25/50/70%의 비율로 발생되는 경우를 비교하여 보여주고 있다. 그림 2에서 연결의 수는 성공한 연결의 수가 아니라 시도한 연결의 수를 의미한다.

그림 2에서 MOS는 블랙홀 공격이 있을 경우 연결수의 변화와 무관하게 VoIP 통화품질 기준인 3.6을 만족하는 것을 보여주고 있다. 그림 2의 결과는 블랙홀 공격을 받지 않는 노드들에 의한 성공한 연결의 통화품질로 블랙홀 공격이 없는 경우와 비교하여 그 품질의 변화가 거의 없다.

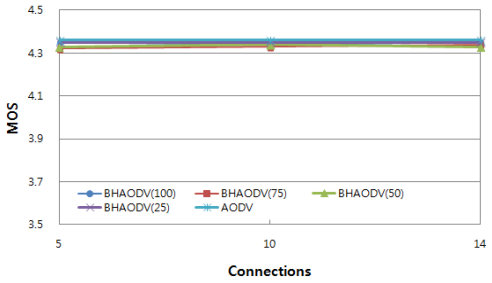

그림 2. MOS.

그림 3은 호 연결율로 블랙홀 공격이 있을 경우 연결을 시도한 수와 성공한 연결의 수의 비를 제시하고 있다. 블랙홀 공격이 없을 경우 시도한 모든 연결이 성공하여 통화가 이루어진 반면에 100% 비율의 지속적 블랙홀 공격이 있을 경우에 통화에 성공한 호 연결율은 약 43~60%정도이다. 이는 호 성공률 기준인 95%에 비하여 매우 낮은 값이다. 25/50/75% 비율의 간헐적 공격이 있는 경우는 25%의 경우 그 영향이 비교적 크지 않게 나타나고 있지만, 75% 비율의 간헐적 공격의 경우 100% 비율의 지속적 공격과 거의 유사한 형태를 보이고 있다. 50% 비율의 간헐적 공격의 경우 다소 낮은 호 성공율을 기록했다.

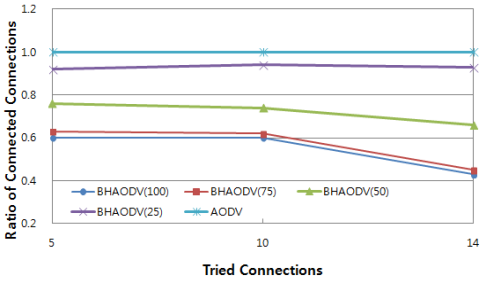

그림 3. 호 연결율.

본 논문에서 측정한 실패한 연결은 블랙홀 노드의 영향으로 시도한 연결이 성립되지 않은 경우, 연결이 성립되었다 하더라도 음성트래픽이 전송되지 않아서 연결이 성립되지 않은 것과 같은 경우를 의미한다.

그림 2와 3에서 MANET을 대상으로 한 간헐적 블랙홀 공격은 MOS 보다 호 연결율에 더 큰 영향을 미치는 것으로 관찰 되었다.

Ⅳ. 결 론

본 논문에서는 간헐적 블랙홀 공격이 있는 MANET에서 VoIP 트래픽의 전송성능을 컴퓨터 시뮬레이션을 사용하여 분석하여 보았다.

NS-2를 기반으로 구현한 컴퓨터 시뮬레이션에서 VoIP 전송성능으로서 MOS와 호연결 율을 측정하고 고찰하여 보았다.

간헐적 블랙홀 공격이 있을 경우 MOS는 거의 일정한 수준을 유지했으며, 호 연결율은 블랙홀 공격시간의 비율에 가중하여 100% 비율의 지속적 공격에 가까운 성능저하를 보였다. 특히 75% 이상의 비율로 간헐적 공격이 있을 경우 100% 비율의 지속적 공격과 거의 유사한 성능 저하가 관찰되었다.

본 논문의 결과는 블랙홀 MANET에서 VoIP 구현을 위한 기본적인 성능 자료 및 간헐적 블랙홀 공격이 응용서비스에 미치는 영향의 분석 방법으로 활용될 수 있을 것으로 생각된다.

간헐적 블랙홀 공격이 있는 MANET에서 다양한 네트워크 환경에 대한 전송성능 및 간헐적 블랙홀 공격 대응 방안을 살펴보는 것이 추후의 연구 과제이다.

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 Technolgy, Vol.4, No.2, pp. 243-250, 2009.

[3] 김영동, “블랙홀 공격이 있는 MANET에서 VoIP 트래픽의 전송성능”, 한국해양정보통신학회, 종합학술대회 논문집, 제15권, 제2호, pp. 637-640, 2011.

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

[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.