Regular paper | Journal of the KIECS. pp. 1411-1416, vol. 10, no. 12, Dec. 31 2015, t. 68, pISSN 1975-8170 | eISSN 2288-2189
http://dx.doi.org/10.13067/JKIECS.2015.10.12.1411

그레이홀 공격이 있는 MANET에서 음성 트래픽의 전송성능

김영동*

Transmission Performance of Voice Traffic on MANET under Grayhole Attack

Young-Dong Kim*

요 약

그레이홀 공격은 MANET의 라우팅 기능에 대한 공격의 하나로 전송되는 패킷의 일부만을 공격의 대상으로 삼고 있어 발견이 쉽지 않은 반면 네트워크의 정상적인 전송기능을 방해한다는 점에서 치명적인 결과를 초래할 수 있다. 본 논문에서는 그레이홀 공격이 MANET 응용 서비스에 미치는 영향을 분석하고, 이를 토대로 그레이홀 공격이 있는 MANET에서 특정한 응용 서비스를 운영하기 위한 침해대응 조건을 제시하였다. 본 연구는 NS-2를 기반으로 한 컴퓨터 시뮬레이션을 사용하여 수행하였다. 시뮬레이션에서 그레이홀 공격 기능은 본 연구에서 구현하여 사용하였다.

ABSTRACT

Grayhole attack, one of attack to MANET routing function, is very severe in point of view of causing results which disturbs normal transmission function of network with uneasy finding of attacks. In this paper, effects of grayhole attack to application service on MANET is analyzed. Based on this analysis, some conditions is suggested for anti-intrusion to operate an application service on MANET under grayhole attack. This study is done with computer simulation based on NS-2 be added grayhole attack function which is implemented in this paper.

키워드

Grayhole, MANET, VoIP, Simulation
그레이홀, 마넷, 음성트래픽, 시뮬레이션

Ⅰ. 서 론

MANET(: Mobile Ad-Hoc Network)은 네트워크 인프라구조의 지원없이 단말기들만으로 구성되는 임시 통신망으로 탐험·탐사를 비롯한 취미활동, 홍수·지진과 같은 긴급재난 상황, 군사용 등 다양한 분야에 활용이 가능하다.

최근 들어 Wi/Fi를 탑재한 스마트 단말기의 급속한 보급은 MANET 활용에 매우 양호한 환경을 제공하고 있다. 스마트 단말기에 제공되는 고성능 하드웨어와 소프트웨어 처리 능력은 MANET 구축 및 활용에 유리하게 작용할 것으로 예상된다.

스마트 단말기의 처리능력과 소프트웨어 탑재 기능은 응용분야 확장이라는 순기능 뿐 아니라 악성 소프트웨어 탑재 가능성을 동시에 증가시키기도 한다.

스마트 단말기에서 악성 소프트웨어 탑재 가능성은

* 교신저자 : 동양대학교 철도전기통신학과
• 접 수 일 : 2015. 11. 16
• 수정완료일 : 2015. 12. 13
• 게재확정일 : 2015. 12. 24
• Received : Nov 16, 2015, Revised : Dec 13, 2015, Accepted : Dec 24, 2015
• Corresponding Author : Young-Dong Kim
Dept. of Electric Railway Communications Engineering, Dongyang University,
Email : ydkim@dyu.ac.kr

MANET 구현에 있어 치명적인 요소로 작용할 가능성이 있다. 단말기가 송수신기 기능과 더불어 네트워크 구성의 핵심요소인 중계기능을 담당해야하는 MANET에서 단말기 기능의 침해는 네트워크 기능의 침해로 연결되기 때문이다. 통신 기반구조의 지원이 수월하지 못한 MANET에서 모든 단말기에 침해대비 기능을 높은 수준으로 탑재하는 것은 쉽지 않은 일이다[1-2].

MANET에 대한 악성 공격은 여러 유형이 있으나 라우팅 기능에 대한 공격이 가장 대표적이다. 라우팅 기능이 MANET에서 차지하는 비중이 커서 이 기능을 공격할 경우 네트워크 전체를 효과적으로 마비시킬 수 있기 때문이다. MANET에 대한 라우팅 공격의 유형으로는 블랙홀(blackhole) 공격, 그레이홀(grayhole) 공격, 웜홀(wormhole) 공격 등이 있다[3].

블랙홀 공격은 악성노드인 블랙홀 노드가 네트워크 전송경로를 모두 자신을 수신노드로 설정하도록 하여 송신노드로 하여금 블랙홀 노드로 패킷을 전송하게 한 다음 수신한 패킷을 폐기하는 악성 공격이다. 그레이홀 공격은 블랙홀 공격과는 달리 전체 패킷을 폐기하지 않고 선택된 일부 패킷을 폐기하고 나머지는 수신노드로 전송하는 유형의 공격이다. 웜홀공격은 두 노드가 쌍을 이루어 공격하는 복수작용 공격유형으로 두 노드가 전송경로 터널을 이루어 전송 패킷을 정상경로가 아니라 임의의 경로로 이동시키는 유형의 공격이다. 블랙홀 공격과 그레이홀 공격이 악성 노드의 단독작용으로 공격이 가능한 단일노드 기반 공격이라 할수 있다.

그레이홀 공격은 MANET에서 전송되는 일부의 패킷을 공격 대상으로 한다는 점에서 다른 유형의 공격과 다른 난해한 특성을 갖는다. 그레이홀 공격은 공격대상을 선정하는 방법에 따라 그레이홀 공격은 특정 종류의 패킷을 차단하는 방법, 특정 노드로 부터의 패킷을 차단하는 방법, 일정시간동안 패킷을 차단하는 방법과 이들의 조합을 활용한 복합적 공격 등으로 분류된다[4]. 어떤 방법을 사용하더라도 일부의 패킷만을 공격대상으로 하므로 공격 발생을 탐지하는 것이 수월하지 않다[5].

따라서 MANET에서 그레이홀 공격이 전송 성능에 미치는 영향을 분석하는 것은 MANET 구축 및 운용에 있어서 매우 중요한 요소라 할수 있다. 그레이홀 공격이 MANET의 성능에 미치는 영향을 분석한 연구 결과들이 발표되고 있으나 대부분의 연구는 패킷 수준의 손실율과 같은 네트워크 파라미터에 미치는 영향의 분석에 국한되고 있어 응용서비스 차원에서 그레이홀 공격의 영향분석이 필요하다.

본 논문에서는 그레이홀 공격이 전송 성능에 미치는 영향을 네트워크 파라미터를 대상에서 응용서비스 차원에서 분석하고자 한다. 성능분석은 NS(: Network Simulator)-2를 기반으로 본 연구에서 구축한 그레이홀 공격 모듈을 활용한 컴퓨터 시뮬레이션을 사용한다. 분석 대상 응용서비스로는 음성 서비스의 한 유형인 VoIP 서비스를 사용하였다.

본 논문은 II장에서 그레이홀 공격의 원리를 설명하고 III장에서 시뮬레이션 및 성능분석을 기술하며, IV장에서 결론을 맺는다.

II. 그레이홀 공격

그레이홀 공격은 MANET 라우팅 공격의 한 유형으로 송수신 단말기 간의 전송경로 설정 단계에서 그레이홀 노드가 불리우는 악성노드가 네트워크 내에 전파되는 라우팅 정보를 위·변조하여 자신을 경유 하도록 경로를 무단으로 설정한 후 그 경로를 따라 이동하는 패킷을 탈취하여 일부는 폐기하고 일부는 수신노드로 전송시키는 악성공격이다. 그레이홀 공격은 일정시간동안 일정한 위치에서 공격을 감행할 수도 있어 네트워크 전송기능 일부 또는 전체에 대하여 이상을 발생시키거나, 일반노드에 대하여 악의적 영향을 줄 수 도 있다.

그레이홀 공격 과정을 그림 1[6]에 제시하였다. 그림 1에서 일반노드 1이 일반노드 4로 정보를 전송하기 위해서 RREQ(1,4)를 네트워크 전체에 발송하여 노드 4로의 경로 설정을 시작한다. RREQ(1,4)는 노드 2를 거쳐 수신노드인 노드 4에 도착하게 된다. 이에 앞서 노드 1이 발송한 RREQ(1,4)는 그레이홀 노드인 노드 3에도 도착하게 된다. 노드 3은 자신이 수신노드가 아님에도 불구하고 수신노드가 발송할 수 있는 RREP(4,1)을 위조하여 노드 1로 전송하고, 노드 5를 경유한 노드 4로의 경로를 별도로 설정한다. RREP(4,1)을 수신한 송신 노드 1은 그레이홀 노드 3

을 수신 노드 4로 인식하고 패킷들을 노드 3으로 송신한다. 그레이홀 노드 3은 노드 1로부터 수신된 패킷 가운데 일부 패킷은 폐기하고 일부는 원 수신 노드인 노드 4로 전송한다. 그레이홀 노드는 MANET내의 모든 일반 노드에 대하여 이와 같은 공격을 감행하여 모든 패킷들이 자신에게 집중되도록 함으로서 네트워크 전체 전송기능에 치명적인 영향을 발생시킨다.

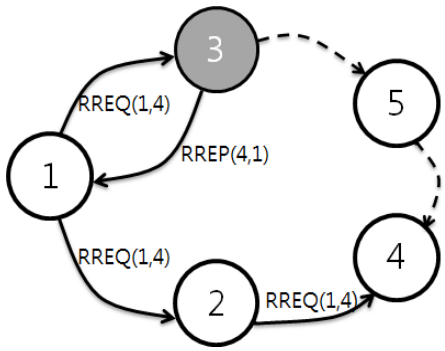

그림 1. 그레이홀 공격
Fig. 1 Grayhole attack

그레이홀 공격은 그레이홀 노드가 폐기할 패킷을 선정하는 방법에 따라서 다양한 형태로 나타난다. 가장 일반적인 형태로는 전송되는 패킷 가운데 일정 유형의 패킷을 폐기하는 방법이 있으며, 이외에도 일정 비율로 패킷을 폐기하는 방법, 특성 노드로부터 전송되는 패킷을 폐기하는 방법, 일정시간 동안 수신한 패킷을 폐기하는 방법과 이들의 조합을 통한 공격방법 등이 있다.

본 논문에서는 일정 비율로 폐기하는 방법을 연구의 대상으로 하였다.

III. 시뮬레이션 및 성능 분석

3.1 시뮬레이터 구현

본 논문에서는 그레이홀 공격이 MANET의 전송성능에 미치는 영향을 컴퓨터 시뮬레이션을 사용하여 분석하였다. 시뮬레이터는 NS-2를 기반으로 그레이홀 공격 모듈을 추가하여 구현하였다.

그레이홀 모듈은 AODV(: Ad-hoc On-Demand Distance Vector)과 blackholeAODV 모듈을 토대로 구현하였다. AODV 모듈은 NS-2 패키지에 기본 기능으로 제공되어 있으며, blackholeAODV은 이 AODV 모듈을 변형하여 구성되어 배포되고 있다. blackholeAODV는 송신노드로부터 블랙홀 노드 자신까지의 경로를 구성한다는 점에서 AODV 기능과는 차이가 나기 때문에 그레이홀 공격에 사용하기 위해서는 AODV 모듈의 라우팅을 기능을 활용해서 보완을 해야 하였다. 이를 위해서 임의의 송신노드에서 수신노드로의 경로를 그레이홀 노드를 경유하도록 설정하기 위해 그레이홀 노드가 최대 시퀀스 번호를 사용해서 응답하도록 했으며, 그 다음으로 그레이홀 노드가 수신노드로 경로를 확보하도록 했다.

본 논문에서 그레이홀 공격은 특정비율로 차단하는 것으로 가정하였으며, 차단 패킷의 선택은 난수를 사용하여 구현하였다.

본 연구에서는 그레이홀 공격이 MANET에 미치는 영향을 기존의 연구 결과들이 분석 대상으로 설정한 네트워크 파라미터와는 달리 응용서비스 수준의 전송품질을 분석 대상으로 설정하고, 이를 위한 분석대상 응용 서비스로는 음성서비스를 선택하였다.

음성서비스 모듈은 NS2VoIP 모듈[7]을 사용하여 구현하였다. NS2VoIP 모듈은 VoIP(: Voice over Internet Protocol)을 NS-2에 구현한 기능모듈로 음성서비스의 전송품질인 MOS(: Mean Opinion Score)를 기본 측정 결과로 제공하고 있으며, 시뮬레이션 결과 데이터를 활용할 경우 호연결율인 CCR(: Call Connection Rate)을 분석할 수 있다.

3.2 시뮬레이션 환경

본 연구에서 사용한 MANET은 일정한 규모에서 일반 노드들이 랜덤하게 이동하는 것으로 설정하였다. 노드의 이동속도는 최대 2[㎧]로 랜덤하며, 시나리오 파일에 따라 랜덤 방향으로 이동한다.

일반 노드들은 랜덤 이동 중에 다른 노드와 VoIP 방식으로 음성 데이터를 서로 전송한다. 각 노드가 사용할 수 있는 음성연결의 최대 수는 1로 설정하였다. 따라서 MANET내의 최대 음성연결의 수는 노드수의 1/2을 넘지 못한다.

시뮬레이션에서 사용한 주요 파라미터는 표 1과 같다. 네트워크 규모는 670×670[㎡], 네트워크 내의 노드는 일반노드 49개, 그레이홀 노드 1개를 포함하여

총 50개의 구성되며, 각 노드의 통신프로토콜은 802.11g로 설정하였다.

표 1. 시뮬레이션 파라미터
Table 1. Simulation parameters

Parameters	Values	
Network Scale	670×670[㎡]	
MAC	802.11g	
Routing	AODV	
Nodes	Normal Nodes	49
	Grayhole Nodes	1
VoIP Connection	Max. 25	
VoIP Traffic	GSM.AMR	

3.3 성능 파라미터

VoIP 전송 성능은 MOS, CCR 및 지연이 표준평가척도로 사용되며 요구조건은 MOS 3.6이상, CCR 95[%] 이상, 종단간 지연 300[ms]이하이다[8-10]. 기타 평가척도로 5[%] 이하의 PLR(: Packet Loss Rate)가 사용되기도 한다. 본 논문에서는 성능 파라미터 가운데 표준 평가척도인 MOS, CCR 및 지연을 중심으로 음성 트래픽의 성능을 분석한다.

3.4 성능 분석

시뮬레이션은 그레이홀 공격발생시 폐기되는 패킷 비율을 20[%], 40[%], 50[%], 60[%], 80[%]로 설정하여 수행하였으며, 각각에 대하여 60초간 시뮬레이션을 실행하여 전송성능을 측정하였다.

시뮬레이션 결과를 그림 2~7에 MOS, CCR 및 지연으로 구분하여 제시하였다. 그림 2, 4, 6은 패킷폐기 비율에 따른 각 성능의 변화이고, 그림 3, 5, 7은 각 성능의 평균값이다. 그림 2, 4, 6에서 AODV는 노드에서 고의적인 패킷 폐기가 없는 경우, Backhole은 블랙홀 노드에 수신된 패킷 전량을 폐기하는 경우를 의미한다.

그림 2에서 그레이홀 공격이 있는 MANET에서 MOS는 공격이 없을 때나 블랙홀 공격이 있는 경우에 비하여 패킷 폐기 비율에 따라 성능의 변동이 크게 나타나고 있다. 이는 그레이홀 노드에 모인 패킷 가운데 폐기할 일정비율의 패킷을 난수를 사용하여 선정함에 따라 발생된 현상으로 VoIP 패킷 가운에 폐기되는 패킷이 랜덤하게 선정되어 MOS가 가변적으로 나타나게 된 것이다. 평균 MOS는 그림 3에 의하면 3.6으로 측정되어 VoIP MOS 요구조건을 최저 수준에서 만족하고 있다.

한편 블랙홀 공격의 경우 블랙홀 공격 대상 노드들에서 전송되는 패킷이 전량 폐기됨에도 블랙홀 공격의 영향에 있지 않은 노드들 간의 전송에 의한 성능이 측정된 것으로 높은 MOS 수준을 보이고 있다.

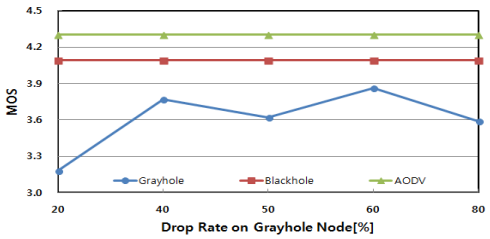

그림 2. 패킷 폐기율에 따른 MOS
Fig. 2 MOS on packet drop rate

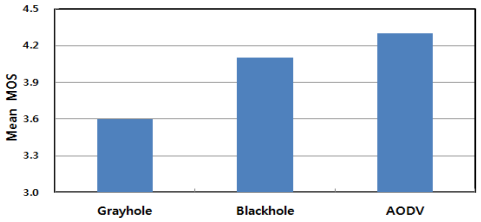

그림 3. 평균 MOS
Fig. 3 Mean MOS

그림 5에서 CCR은 MOS와는 달리 블랙홀 공격에 비하여 다소 높게 측정되었지만, 패킷 폐기 비율에 따라 변동되었다. 그림 6에서 평균 CCR은 요구수준 95[%]에 비해 매우 낮은 30[%] 수준이었다.

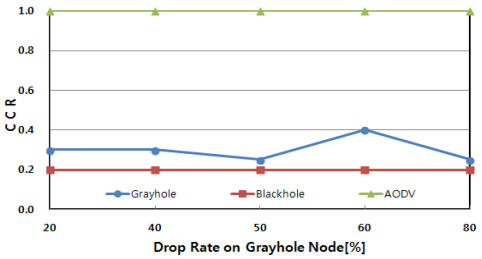

그림 4. 패킷 폐기율에 따른 CCR
Fig. 4 CCR on packet drop rate

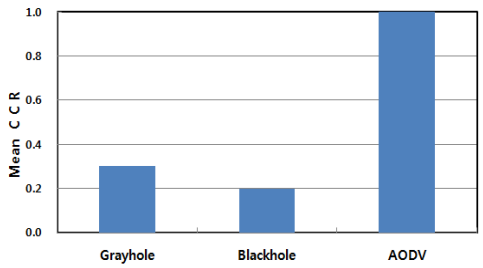

그림 5. 평균 CCR
Fig. 5 Mean CCR

종단간 지연은 그림 6과 그림 7에 제시한 바와 같이 그레이홀 노드에서 폐기되는 패킷의 비율에 따라 다소 변동이 발생되고 있으나 대부분의 경우에 요구조건 300[ms]를 만족하고 있으며, 평균지연은 250[ms]로 분석되었다.

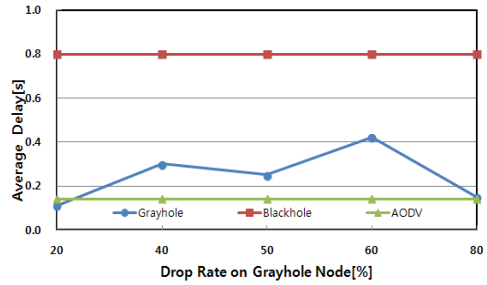

그림 6. 패킷 폐기율에 따른 지연
Fig. 6 Delay on packet drop rate

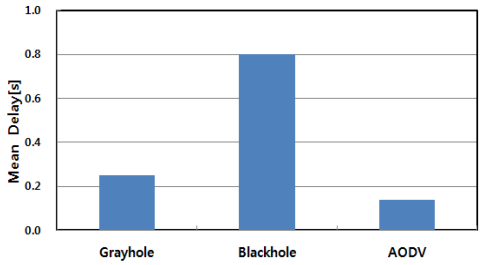

그림 7. 평균 지연
Fig. 7 Mean delay

3.5 대응 조건

그레이홀 공격이 있는 MANET에서 음성 트래픽은 블랙홀 공격이 발생되는 경우와 달리 MOS에 저하가 발생되며, CCR은 영향을 덜 받는 것으로 나타났다. 이는 그레이홀 노드가 폐기하는 패킷의 수준에 영향을 받아 발생되는 현상으로 분석되었다.

따라서 그레이홀 공격이 발생되는 MANET에서 음성 서비스를 구현하기 위해서는 MOS와 CCR을 개선하기 위한 대책이 강구되어야 한다. 이는 블랙홀 공격이 있는 경우에 요구되던 CCR개선에 비하여 대응 조건이 악화된 것을 의미한다.

또한 패킷의 일부만을 폐기하는 그레이홀 공격이 패킷의 전량을 폐기하는 블랙홀 공격에 비하여 응용서비스 수준에서 영향이 더 심각한 것을 보여주는 현상이라 할 것이다.

Ⅳ. 결론

본 논문에서는 그레이홀 공격이 있는 MANET에서 음성 트래픽의 전송 성능을 컴퓨터 시뮬레이션을 사용하여 분석하였다. 본 논문에서는 이를 시뮬레이션을 수행하기 위하여 그레이홀 공격 모듈을 구현하였다.

컴퓨터 시뮬레이션을 통한 음성 트래픽에 대한 성능 분석 결과 MOS와 CCR이 전송품질 요구조건을 충족하지 못할 뿐 아니라 가변적인 값을 가지는 것으로 그레이홀 공격의 영향에 민감한 것으로 나타났다. 이는 블랙홀 공격이 있는 경우 CCR만 영향을 받는 것과는 달리 그레이홀 공격이 응용서비스에 미치는 영향이 심각한 것을 보여주는 결과이다.

패킷유형별, 송신노드별, 공격시간별 등 다양한 공격 유형에 대한 그레이홀 공격의 영향 분석, GSM.AMR 이외의 음성 트래픽, 그레이홀 노드의 위치 및 노드의 이동 패턴 등의 다양한 MANET 환경에 대한 그레이홀 공격의 영향을 분석하는 것과 이에 대한 대응방안을 강구하는 것이 추후 과제라 할수 있다.

감사의 글

이 논문은 2014년도 동양대학교 학술연구비의 지원으로 수행되었음.

References

[1] Y. Kim, "Transmission Performance of Application Service Traffic on MANET with IDS," In *Proc. of Conf. on Korea Institute of Information anc Communication Engineering 2012*, vol. 16, no. 1, Busan, Korea, May, 2012, pp. 584-587.

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

[3] 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, 2011, pp. 277-287.

[4] G. Neekhra, S. Patel, A. Verma, and A. Chaurasia, "Effect Of Grayhole Attack With Ids Technique For Aodv Routing Protocol Using Network Simulator," *Int. J. of Advanced Research in Computer Engineering & Technology*, vol. 3, issue 12, 2014, pp. 4184-4190.

[5] J. Kaur and V. Kumar, "An Effectual Defense Method against Gray Hole Attack in Wireless Sensor Networks," *Int. J. of Computer Science and Information Technologues*, vol. 3, no. 3, 2012, pp. 4523-4528.

[6] Y. Kim, "Transmission Performance of MANET under Grayhole Attack," In *Proc. of Conf. on Korea Institute of Information and Communication Engineering 2015*, vol. 19 no.1, Tongyeong, Korea, May, 2015, pp. 639-641.

[7] 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.

[8] 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, 2012, pp. 747-752.

[9] 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.

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

저자 소개

김영동(Young-Dong Kim)

1984년 광운대학교 전자통신공학과 졸업(공학사)
1986년 광운대학교 대학원 전자통신학과 졸업(공학석사)
1990년 광운대학교 대학원 전자통신학과 졸업(공학박사)
1995년~현재 동양대학교 철도전기통신학과 교수
※ 관심분야 : 통신프로토콜, MANET, VoIP, 컴퓨터 시뮬레이션, ICT 융합 등