Regular paper | Journal of the KIECS. pp. 1077-1082, vol. 11, no. 11, Nov. 30 2016, t. 79, pISSN 1975-8170 | eISSN 2288-2189
http://dx.doi.org/10.13067/JKIECS.2016.11.11.1077

그레이홀 공격이 있는 MANET에서 IDS 성능 분석

김영동*

Performance Evaluation of IDS on MANET under Grayhole Attack

Young-Dong Kim*

요 약

MANET 라우팅 기능에 혼란을 초래하여 네트워크 전송기능을 저하시키는 악성공격에 대한 대응수단으로 IDS가 사용된다. 본 논문에서는 전송패킷의 일부를 공격대상으로 하는 그레이홀 공격이 있는 MANET에서 IDS가 전송성능에 미치는 영향을 분석하고, 그레이홀 공격에 대한 효과적인 IDS 조건을 살펴본다. 성능분석은 NS-2를 기반으로 하는 컴퓨터 시뮬레이션을 사용하며, VoIP를 응용서비스로 하여 전송성능을 측정한다. 음성 전송의 표준전송품질척도인 MOS, CCR, 종단간지연 등을 성능측정 및 분석 파라미터로 사용한다.

ABSTRACT

IDS can be used as a countermeasure for malicious attacks which cause degrade of network transmission performance by disturbing of MANET routing function. In this paper, effects of IDS for transmission performance on MANET under grayhole attacks which has intrusion objects for a part of transmissions packets, some suggestion for effective IDS will be considered. Computer simulation based on NS-2 is used for performance analysis, performance is measured with VoIP(: Voice over Internet Protocol) as an application service. MOS(: Mean Opinion Score), CCR(: Call Connection Rate) and end-to-end delay is used for performance parameter as standard transmission quality factor for voice transmission.

키워드

Grayhole, IDS, MANET, VoIP, Simulation,
그레이홀, 아이디에스, 이동 임시망, 음성 트래픽, 시뮬레이션

Ⅰ. 서 론

MANET(: Mobile Ad-Hoc Network)은 단말기만으로 구성되는 임시통신망으로 서버, 방화벽 등 통신 기반구조의 지원이 어려워 정보침해에 매우 취약하다. 특히 사용자 응용 프로그래밍 탑재가 가능한 지능형 단말기의 경우 악성프로그램의 침투는 쉬우나 침해 대응수단의 확보는 수월하지 않다.

MANET의 필수적 요소의 하나인 라우팅 기능에 이상을 발생시켜 정보전송을 방해하거나 마비시키는 라우팅 공격은 대표적인 악성 공격으로 블랙홀(blackhole) 공격, 그레이홀(grayhole) 공격, 웜홀(wormhole) 공격 등 여러 유형이 있다[1].

그레이홀 공격은 라우팅 정보를 무단으로 위변조하여 패킷이 자신에게로 전송되도록 하나 수신한 패킷 전부를 폐기하는 블랙홀 공격과는 달리 일부 패킷만

* 교신저자 : 동양대학교 철도전기융합학과
• 접 수 일 : 2016. 10. 04
• 수정완료일 : 2016. 11. 13
• 게재확정일 : 2016. 11. 24
• Received : Oct. 04, 2016, Revised : Nov. 13, 2016, Accepted : Nov. 24, 2016
• Corresponding Author : Young-Dong Kim
Dept. of Electric Railway Convergence Engineering, Dongyang University,
Email : ydkim@dyu.ac.kr

을 폐기하는 공격이다[2-3]. 그레이홀 공격의 유형은 공격대상 패킷의 선정 방법에 따라, 특정 유형의 패킷을 대상으로 하는 방법, 특정 노드로 부터의 패킷을 대상으로 하는 방법, 일정 기간에 발송 패킷을 차단하는 방법 등이 있으며, 이외에 이들의 조합에 의한 공격 대상을 선정하는 방법 등이 있을 수 있다[3].

그레이홀 공격은 MANET을 따라 전송되는 패킷의 일부를 공격 대상으로 한다는 점에서 전체를 대상으로 하는 블랙홀 공격과는 다른 특징을 갖는다. 공격대상 패킷 측면에서 볼 때 공격 노출 가능성은 낮은 반면에 공격 탐지는 상대적으로 어려운 면이 있다. 따라서 그레이홀 공격에 대응하는 수단을 갖추는 것은 MANET 설계 및 운용에 있어 매우 중요한 일이다.

MANET에서 악성공격에 대응하는 수단은 대응 방법에 따라 IPS(: Intrusion Prevention System)과 IDS(: Intrusion Detection System)으로 구분된다. IPS는 악성공격 발생 차단 중심 시스템인 반면에 IDS는 침입 탐지 중심의 대응 수단이다. MANET과 같은 단말기 중심으로 구축되는 네트워크에서는 가용장비의 제약으로 인해 IPS에 비해 IDS가 유리하다.

그러므로 그레이홀 공격이 발생되는 MANET에서 IDS가 전송성능에 미치는 영향을 분석·고찰하는 것은 MANET 구축과 운용에 있어 매우 중요하다. IDS가 MANET에 미치는 영향에 대한 연구 결과들[4-5]이 제시되고 있으나 네트워크 수준의 패킷전송 성능에 미치는 영향에 제한되고 있어 응용서비스 구축을 위해서는 사용자 수준의 응용서비스 트래픽의 전송성능 분석이 필요하다.

본 논문에서는 이런 점을 고려하여 그레이홀 공격이 발생되는 MANET에서 IDS가 전송성능에 미치는 영향을 응용서비스 수준에서 분석한다. 대상 응용 서비스로는 VoIP(: Voice over Internet Protocol)서비스를, 분석방법으로는 NS(: Network Simulator)-2를 기반으로 하는 컴퓨터 시뮬레이션을 사용한다. 시뮬레이션 결과 분석을 토대로 IDS 조건을 제시한다.

본 논문은 II장에서 그레이홀 공격과 IDS에 대하여 설명하고 III장에서 시뮬레이션과 성능분석, IDS 조건을 기술하며, IV장에서 결론을 맺는다.

II. 그레이홀 공격과 IDS

2.1 그레이홀 공격

MANET에서 발생될 수 있는 라우팅 공격 가운데 하나인 그레이홀 공격은 그레이홀 노드라 불리는 악성 노드가 일반 노드의 전송경로 설정에 사용되는 라우팅 정보를 탈취하여 무단으로 위변조하고 이를 유통시켜 일반노드의 정보전송 경로를 변경하도록 하여 전송정보를 탈취하고 그 일부를 폐기하는 악성 공격으로 그림 1[3]과 같이 동작한다.

그림 1의 MANET은 리액비트(reactive) 라우팅 방식의 하나인 AODV(: Ad-hoc On-demand Distance Vector) 프로토콜을 사용하여 정보를 전송한다. 그림 1에서 송신 노드는 노드 1, 수신 노드는 노드 4, 그레이홀 노드는 노드 3이다.

노드 1이 노드 4로 정보를 전송하기 위하여 RREQ(1,4)를 송신하여 노드 4로 전송경로 설정을 시도한다. RREQ(1,4)는 노드 1에 인접한 노드를 따라 네트워크 전체로 전파되므로 노드 2와 노드3에 도달된다. 노드 2에 도착한 RREQ(1,4)는 노드 4로 전파되어진다.

RREQ(1,4)를 수신한 노드 3은 자신이 수신 노드 4가 아님에도 불구하고 노드 4가 발송할 수 있는 RREP(4,1)을 위조하여 노드 1에 응답한다. RREP(4,1)를 노드 1은 그레이홀 노드인 노드 3을 정상 수신 노드로 인식하여 노드 3으로 전송경로를 설정한다. 노드 3은 이와는 별도로 노드 5를 경유한 노드 4로의 전송경로도 설정한다.

노드 3이 송신한 악성 경로 정보로 인해 노드 1은 노드 4로 전송할 정보를 그레이홀 노드인 노드 3으로의 경로를 따라 전송하게 되고, 노드 4로 전송될 정보를 수신한 그레이홀 노드 3은 노드 4로 전송되어야 할 수신 정보 중 일부를 폐기하고, 일부는 수신노드로 중계함으로서 정상정인 정보전송을 방해한다.

그레이홀 공격은 그레이홀 노드가 폐기할 폐기 대상을 선정하는 방법에 따라 폐기 대상을 무작위로 선택하는 무작위 폐기, 특정 유형의 패킷을 폐기하는 유형별 폐기, 일정 비율로 폐기하는 비율별 폐기, 특정 노드로 전송된 패킷을 대상으로 하는 노드별 폐기, 지정된 시간 동안에 수신된 패킷을 폐기하는 시간별 폐기 등이 있으며, 이외에도 이 방법들을 조합한 다양한

방법이 있을 수 있다. 가장 일반적인 형태의 그레이홀 공격은 특정 유형의 패킷만을 선택적으로 폐기하는 유형별 공격이다. 본 논문에서는 시뮬레이터 구축의 수월성을 고려하여 일정 비율로 폐기하는 방법을 연구의 대상으로 하였다.

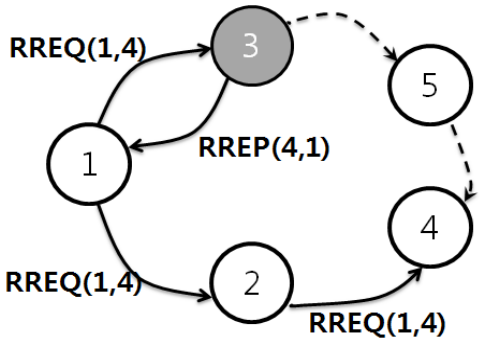

그림 1. 그레이홀 공격
Fig. 1 Grayhole attack

2.2 IDS

그레이홀 공격에 대응하는 수단에는 대응방법에 따라 공격 발생을 차단하는 IPS와 공격을 탐지하는 IDS가 있다. MANET이 단말기간의 협력을 기반으로 구성되는 네트워크인 점을 고려할 때 시스템의 구성과 부하 분담이 적은 IDS가 IPS에 비해 효과적이다.

그레이홀 공격이 있는 MANET에서 IDS는 그림 2와 같다. 그림 2는 그림 1의 네트워크 환경에서 그레이홀 공격에 대응하는 IDS의 한 예로서 정상 수신노드와 그레이홀 노드가 발송한 RREP() 수신시간차[6]를 이용하여 그레이홀 공격을 탐지하는 방법이다.

그림 2에서 노드 3에 의한 그레이홀 공격이 발생되는 상황에서 원 수신 노드인 노드 4가 전송한 RREP(4,1)이 송신 노드 1에 수신된다. 노드 1은 노드 4로부터 수신된 RREP(4,1)을 원 수신노드에 의한 것으로 판단하고 노드 3으로의 전송 경로를 취소한 다음에 노드 4로의 경로를 설정하고 이 경로를 따라 원 수신노드 4로 패킷을 전송한다.

그림 2의 IDS의 경우 그레이홀 노드가 전송경로 기준으로 원 수신노드 보다 송신노드에 근거리에 위치할 경우 효과적인 체계이며, 원거리에 위치할 경우에도 경로 재설정을 통하여 대응할 수 있는 방식이다.

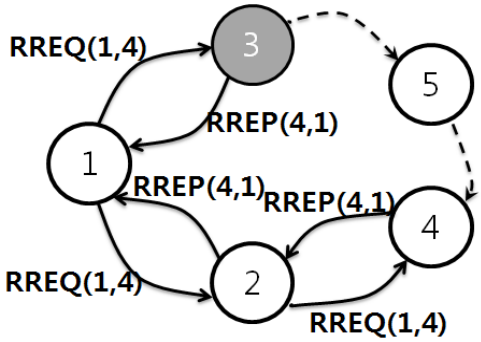

그림 2. 그레이홀 공격 대응 IDS
Fig. 2 IDS against grayhole attack

III. 시뮬레이션 및 성능 분석

3.1 시뮬레이터 구현

본 논문에서는 그레이홀 공격이 발생되는 MANET에서 IDS가 전송성능에 미치는 영향을 컴퓨터 시뮬레이션을 사용하여 분석하였다. 시뮬레이터는 NS-2를 기반으로 그레이홀 공격 모듈[3], IDS 모듈[6]을 추가하여 구현하였다. 그레이홀 공격은 특정비율로 차단하는 방법을 가정하고, 난수를 사용하여 차단할 패킷을 선택하도록 시뮬레이터 모듈을 구성하였다.

그레이홀 공격에 대응한 IDS가 MANET의 전송성능에 미치는 영향을 기존의 네트워크 파라미터와는 달리 본 논문에서는 응용서비스 관점의 전송품질을 사용하여 분석한다. 이를 위하여 음성 서비스를 분석대상 응용서비스로 선정하였다.

시뮬레이션에서는 NS2VoIP 모듈[7]을 사용하여 음성트래픽을 처리하였다. NS2VoIP는 NS-2에 VoIP(: Voice over Internet Protocol)을 구현한 모듈로 음성서비스의 표준 전송품질인 MOS(:Mean Opinion Score), 호 연결율인 CCR(: Call Connection Rate), 종단간 지연 등을 분석할 수 있다.

3.2 시뮬레이션 환경

시뮬레이션에서 각 노드들은 MANET 내에서 최대 2[㎧]의 속도로 시나리오 파일에 따라 랜덤이동을 한다. 일반 노드들은 랜덤 이동 중에 다른 노드와 VoIP 방식에 따라 음성 데이터를 AODV 프로토콜을 사용하여 서로 전송한다. 각 일반 노드들은 그레이홀 공격에

대비하여 IDS 기능을 갖춘 AODV를 사용하며 그레이홀 노드는 그레이홀 공격 기능을 갖춘 AODV 프로토콜을 사용한다. 각 노드는 하나의 연결만을 설정할 수 있다. 시뮬레이션에서 사용한 주요 파라미터는 표 1과 같다.

표 1. 시뮬레이션 파라미터
Table 1. Simulation parameters

Parameters	Values	
Network Scale	670×670[㎡]	
MAC	802.11g	
Routing	AODV, idsAODV	
Nodes	Normal Nodes	49
	Grayhole Nodes	1
VoIP Connection	20 (Max. 25)	
VoIP Traffic	GSM.AMR*	

* GSM.AMR : Global System for Mobile communication Adaptive Multi Rate

3.3 성능 파라미터

VoIP 전송성능의 표준평가척도로는 MOS, CCR 및 지연이 사용되고 있으며, 표준품질 요구조건으로 MOS≥3.6, CCR≥95[%], 종단간 지연≤300[㎳]이 사용된다[8-10]. 비표준평가척도로서 PLR(: Packet Loss Rate)≤5[%]가 사용되기도 한다. 본 논문에서는 표준평가척도인 MOS, CCR 및 종단간 지연을 사용하여 음성트래픽의 성능을 분석한다.

3.4 성능 분석

시뮬레이션은 그레이홀 공격시 폐기되는 패킷비율을 10[%]~90[%] 범위에서 10[%]씩 증가시키며 수행하였으며, 전송성능은 각 60초간의 시뮬레이션을 통하여 측정하였다.

시뮬레이션 결과를 그림 3~8에 MOS, CCR 및 지연으로 구분하여 제시하였다. 그림 3, 5, 7은 각각 패킷 폐기 비율에 따른 각 성능의 변화이고, 그림 4, 6, 8은 각 성능평가척도의 평균값이다. 그림에서 AODV는 악성공격이 발생되지 않은 경우이고, Grayhole은 그레이홀 공격이 발생되는 경우, Blackhole은 블랙홀 공격이 발생되는 경우, IDS는 그레이홀 공격에 대하여 IDS로 대응하는 경우의 측정값을 의미한다.

그림 3과 4에서 그레이홀 공격이 있는 MANET에서 일반 노드가 그림 3과 같이 동작하는 IDS로 대응할 경우 MOS는 10[%] 정도 개선된 평균 3.9로 측정되어 요구 조건인 3.6을 충족하는 것으로 나타났다. 다만 시뮬레이션에서 그레이홀 노드에서 난수를 사용하여 일정비율로 패킷을 폐기하도록 시뮬레이터를 구성함에 따라 폐기 대상 패킷이 랜덤하게 선정되어 MOS 값에 다소 변동이 발생하였다. 블랙홀 공격의 경우 블랙홀 공격 대상 노드들이 전송하는 패킷은 전량 폐기되고 공격 대상이 아닌 노드들이 전송하는 MOS만 측정되므로 높은 수준을 유지하고 있다.

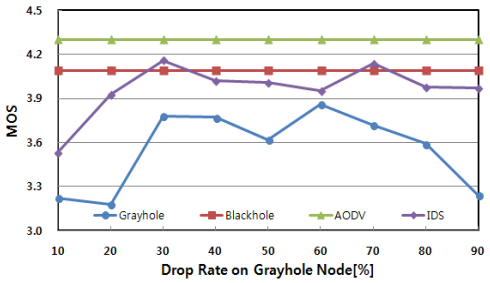

그림 3. 패킷 폐기율에 따른 MOS
Fig. 3 MOS on packet drop rate

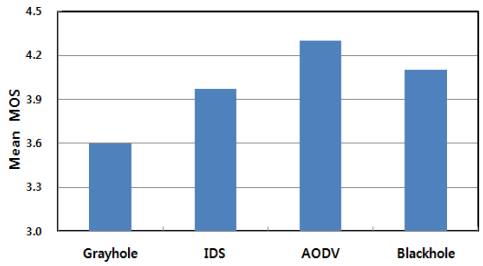

그림 4. 평균 MOS
Fig. 4 Mean MOS

그림 5와 6에서 CCR은 그레이홀 공격에 대하여 IDS로 대응한 경우 평균 56[%]로 나타나서 요구 수준 95[%]에는 약 39[%] 정도 미달하였으나 IDS로 대응하지 않은 경우에 비해 약 87[%]의 성능개선이 있었다. CCR 요구수준 미충족은 IDS의 그레이홀 공격 탐지 시간과 관련이 있는 것으로 분석된다.

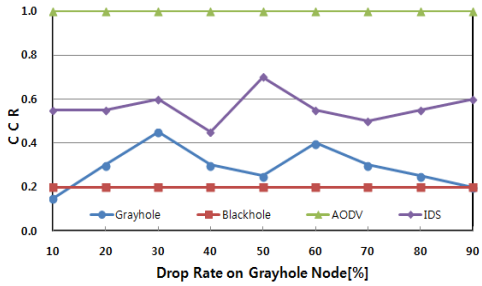

그림 5. 패킷 폐기율에 따른 CCR
Fig. 5 CCR on packet drop rate

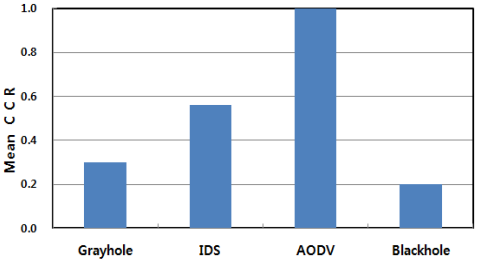

그림 6. 평균 CCR
Fig. 6 Mean CCR

종단간 지연은 그림 7과 그림 8에 제시한 바와 같이 그레이홀 노드에서 폐기되는 패킷의 비율에 따라 다소 변동이 발생되고 있으나 평균지연이 250[ms]로 측정되어 요구조건 300[ms]를 만족하고 있는 것으로 나타났으며, IDS로 대응한 경우 200[ms]로 나타나서 약 20[%]정도의 개선이 있었다.

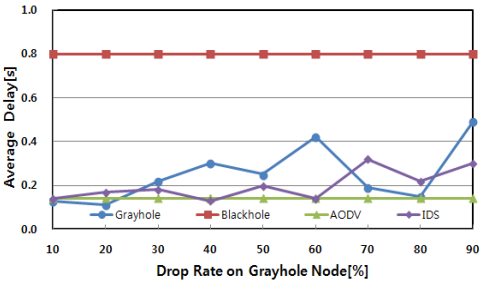

그림 7. 패킷 폐기율에 따른 지연
Fig. 7 Delay on packet drop rate

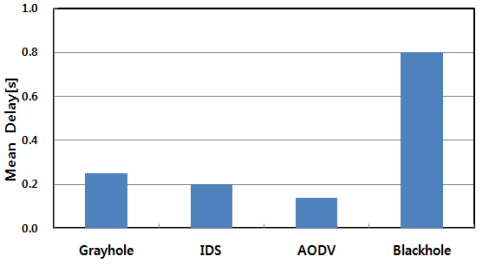

그림 8. 평균 지연
Fig. 8 Mean Delay

3.5 IDS 조건

그림 1과 같은 그레이홀 공격이 있는 MANET에서 그림 2와 같은 IDS로 대응할 경우 음성 트래픽의 전송 성능은 3.4절에서 살펴본 바와 같이 표준 품질 평가척도 가운데 MOS와 지연은 요구 조건을 충족하고 있는 것으로 나타났으며, CCR은 요구 조건에 미달하고 있는 것으로 측정되었다. 따라서 음성 서비스를 대상으로 하는 MANET에서 그레이홀 공격에 대한 대응수단으로서 IDS는 호 연결율을 개선할 수 있어야 한다.

그림 3~6에서 블랙홀 공격과 그레이홀 공격을 비교하여 살펴보면 그레이홀 공격의 경우 블랙홀 공격에 비해 호 연결율이 일정 부분 양호하나 MOS는 악화되고 있는 것으로 나타나고 있어 악성공격이 발생할 경우 MOS와 CCR은 트레이드오프 관계에 있는 것으로 판단된다. 따라서 그레이홀 공격에 대응한 IDS를 설계할 경우 CCR이 개선되는 정도에 따라 MOS가 악화될 가능성이 있어 두 평가척도의 변화정도를 비교하여 살펴야 한다.

Ⅳ. 결론

본 논문에서는 그레이홀 공격이 있는 MANET에서 IDS로 대응한 경우 음성 트래픽의 전송 성능을 컴퓨터 시뮬레이션을 사용하여 분석하였다.

컴퓨터 시뮬레이션을 통한 음성 트래픽의 성능 분석 결과 MOS와 지연은 각각 3.9와 200[ms]로 요구조건 3.6과 300[ms]를 충족하는 것으로 나타났으나 CCR은 56[%]로 IDS로 대응하기 전에 비하여 87[%]

의 개선이 있었으나 요구조건 95[%]에는 39[%] 미달하는 수준이었다.

따라서 그레이홀 공격이 발생되는 MANET에서 음성서비스 품질 유지 목적으로 사용되는 IDS는 CCR을 개선할 수 있는 기능을 갖추어야 한다.

음성 서비스 MANET에서 CCR을 개선할 수 있는 IDS의 개발이 필요하며, 이를 위해서는 GSM.AMR 트래픽 이외에 여러 음성 트래픽의 전송성능 및 다양한 MANET 환경 하에서 전송성능 분석이 추가로 요구된다.

감사의 글

이 논문은 2015년도 동양대학교 학술연구비의 지원으로 수행되었음.

References

[1] 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.

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

[3] Y. Kim, "Transmission Performance of Voice Traffic on MANET under Grayhole Attack," *J. of the Korea Institute of Electronic Communication Sciences*, vol. 10, no. 12, Dec. 2015, pp. 1411-1416.

[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, Dec. 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 Technologies*, vol. 3, no. 3, 2012, pp. 4523-4528.

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

[7] A. Bacioccola, C. Cicconetti, and G. Stea, "User - level Performance Evaluation 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, Aug. 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, Jan. 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