Regular paper http://dx.doi.org/10.13067/JKIECS.2014.9.7.773

IDS가 있는 MANET에서 이동패턴에 기반한 VoIP 트래픽의 종단간 전송성능

김영동*

End-to-end Transmission Performance of VoIP Traffics based on Mobility Pattern over MANET with IDS

Young-Dong Kim*

요 약

라우팅 정보에 대하여 악성침해를 일으켜 네트워크의 전송성능을 저하시키는 블랙홀 공격에 대한 대응수단으로 IDS(Intrusion Detection System)가 사용되고 있다. 본 논문에서는 IDS가 전송성능에 미치는 영향을 MANET(Mobile Ad-hoc Network)에서 노드의 이동패턴에 기반하여 분석하고, 블랙홀 공격에 대한 효과적인 대응방안을 살펴본다. 성능분석에는 NS-2를 기반으로 한 컴퓨터 시뮬레이션을 사용하며, 응용 서비스로 사용되는 VoIP(Voice over Internet Protocol) 서비스를 대상으로 성능을 측정한다. MOS(Mean Opinion Score)와 호연결율, 종단간 지연을 성능측정 및 분석 파라미터로 사용한다.

ABSTRACT

IDS(Intrusion Detection System) can be used as a countermeasure for blackhole attacks which cause degrade of transmission performance by causing of malicious intrusion to routing function of networks. In this paper, effects of IDS for transmission performance based on mobility patterns is analyzed for MANET(Mobile Ad-hoc Networks), a suggestion for effective countermeasure is considered. Computer simulation based on NS-2 is used in performance analysis, VoIP(Voice over Internet Protocol) as an application service is chosen for performance measure. MOS(Mean Opinion Score), call connection ratio and end-to-end delay is used as performance parameter.

키워드

MANET, Blackhole, IDS, Simulation, Mobility Pattern
이동임시망, 블랙홀, 아이디에스, 시뮬레이션, 이동패턴

Ⅰ. 서 론

MANET(Mobile Ad-hoc Network)은 통신기반구조 사용이 수월하지 않은 환경에서 단말기를 중심으로 구축되는 통신망으로서 재난/재해, 군사, 탐험/탐사 및 취미 활동 등에 다양하게 사용될 수 있다.

MANET의 구성요소로서 단말기와 프로토콜이 매우 중요한 요소를 이루고 있으나 이에 못지않게 MANET이 사용되는 환경 또한 중요한 요소 중에 하나이다. 예로서, MANET 구축 환경이 지상인 경우와

* 교신저자(corresponding author) : 동양대학교 정보통신공학과(ydkim@dyu.ac.kr)
접수일자 : 2014. 06. 02 심사(수정)일자 : 2014. 06. 23 게재확정일자 : 2014. 07. 11

수중인 경우는 그 환경적 특성 서로 달라 설치/운영 방법을 달리해야하며, 통신 품질과 같은 네트워크 성능에서도 서로 차별적인 특성을 보인다. 뿐만 아니라 지상통신환경이라 하더라도 도시지역이나 개활지, 산악지역 등에 따라 환경적 차이가 나타난다. 이런 환경적 차별성은 MANET의 이동 특성과 어우러져 성능 파라미터에 작지 않은 영향을 미치게 된다.

MANET 구축에 대한 환경적 특성을 분석하는 분야의 하나가 이동패턴(mobility pattern)이며, 랜덤이동(random waypoint), 맨해튼모델(Manhattan model), 고속도로모델(freeway model) 등의 여러 이동패턴이 제시되어 연구에 활용되고 있다[1]. 이런 이동 모델들과 더불어 방향이동, 집합이동, 해산이동 등이 이동패턴의 한 분류로 활용되고 있다[2].

한편, MANET은 단말기중심이라는 구성특성으로 인해 정보침해에 인프라 네트워크 보다 매우 취약하다. 침해 탐지나 대비를 위한 서버급 장비의 지원을 받기가 수월치 않으며, 스마트 단말기로의 진화가 악성소프트웨어의 개발과 침투에 대한 용이함을 제공하는 반면에 대응수단 개발과 활용에 사용하기에는 그 기능이 부족한 면이 있기 때문이다[3].

MANET에 대한 악성공격의 하나로 라우팅 기능에 대한 공격이 있다. 라우팅 기능에 대한 공격은 악성노드가 라우팅 기능을 무단으로 위조/변조하여 네트워크 내에 유통시킴으로서 일반 노드들이 네트워크 환경을 정확하게 인식하지 못하도록 하는 공격 유형이며 블랙홀(blackhole) 공격이 대표적이다.

블랙홀 공격은 블랙홀 노드가 발송한 위조된 라우팅 정보로 인해 송신 노드는 전송경로를 블랙홀 노드로 설정하게 되고 이 경로를 따라 블랙홀 노드로 전송된 패킷들을 블랙홀 노드에서 폐기하여 네트워크의 정상적인 전송기능을 마비시키는 악성공격이다.

블랙홀 공격에 대한 대응수단으로서 공격 탐지를 우선으로 하는 IDS(Intrusion Detection System)이나 공격 차단을 우선으로 하는 IPS(Intrusion Prevention System) 사용된다. IDS는 IPS보다 성능 면에서는 우수하지 않으나 활용이 용이하며 네트워크에 미치는 부하가 크지 않은 점으로 인해 MANET에서 사용하기에 편리한 체계이다.

본 논문에서는 이와 같은 MANET의 환경적, 기능적 상황들을 고려하여 MANET에서 블랙홀 공격과 IDS 대응이 이동패턴을 고려한 응용서비스의 전송성능에 미치는 영향을 분석하여 이동패턴과 블랙홀 공격 및 IDS 간의 관계를 규명하고 블랙홀 공격에 대한 대응방안을 제시한다.

본 논문에서는 NS-2를 기반으로 한 컴퓨터 시뮬레이션을 사용 전송성능을 분석한다. 분석 대상 트래픽으로는 음성 서비스인 VoIP(Voice over Internet Protol) 트래픽을 사용한다. 측정 및 분석을 위한 성능 파라미터로는 MOS(Mean Opinion Score), 호연결율 및 종단간 지연을 사용한다

본 논문은 2장에서 블랙홀 공격과 IDS에 관련된 이론을 기술하고, 3장에서는 시뮬레이션 및 성능분석을 제시하며, 4장에서 결론을 맺는다.

II. 블랙홀 공격과 IDS

MANET에 대한 악성 공격의 예로서 라우팅 기능에 대한 공격을 들 수 있다. MANET에서 전송경로 설정을 위해 사용되는 라우팅 정보를 무단으로 위조/변조하여 전파시켜 이를 수신한 일반 노드들이 네트워크 환경을 올바로 인지하지 못하게 하는 공격으로서 블랙홀 공격이 가장 대표적이다.

블랙홀 공격은 블랙홀 노드로 불리는 악성노드가 라우팅 정보를 자신이 수신노드인 것으로 무단으로 위조하여 유통시켜 송신노드가 블랙홀 노드를 수신노드로 인식하게 하여 패킷을 수신노드가 아니라 블랙홀 노드로 전송하도록 하고 수신된 패킷은 폐기하여 정보전송을 방해하는 악성공격으로 그림 1과 같이 동작한다.

그림 1에서 노드 1은 일반노드로서 노드 4로 데이터를 전송하기 위해서 RREQ(1,4) 패킷을 사용하여 경로선정 절차에 들어간다. 노드 1이 배포한 RREQ(1,4) 패킷은 인접 노드인 노드 2와 노드 3으로 전송된다. RREQ(1,4) 패킷을 수신한 노드 3은 자신이 노드 4가 아님에도 마치 수신노드 4인 것처럼 노드가 4가 응답에 사용하는 RREP(4,1) 패킷을 위조하여 송신 노드로 발송한다. 노드 1은 블랙홀 노드 3이 발송한 RREP(4,1)을 수신노드 4가 보낸 경로응답 패킷으로 인식하여 블랙홀 노드 3을 대상으로 노드 4로 전송 경로를 설정하고 데이터 패킷을 블랙홀 노드 3으

로 송신한다. 노드 1이 송신한 데이터 패킷을 수신한 노드 3은 이를 노드 4로 전달하지 않고 폐기하여 데이터 패킷이 노드 4로 수신되지 못하도록 한다.

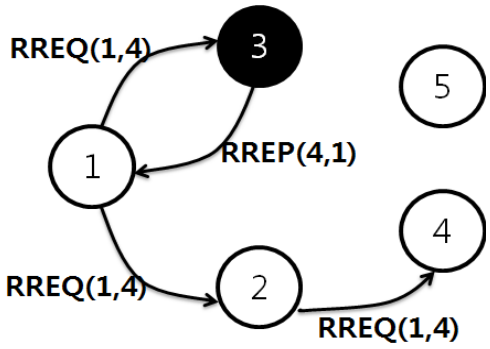

그림 1. 블랙홀 공격[3]
Fig. 1 Blackhole attacks[3]

블랙홀 공격에 대한 대응방안의 하나로서 블랙홀 공격이 발생될 경우 이를 탐지하는 체계를 IDS라 한다. IDS에서 블랙홀 노드를 탐지하는 방법의 하나를 그림 2에 제시하였다. 그림 2에 제시된 IDS는 RREP() 패킷의 수신시간 차를 이용하여 블랙홀 공격을 탐지하는 방법이다.

그림 2에서 블랙홀 노드 3이 RREP(4,1)를 무단으로 사용하여 노드 1이 블랙홀 노드 3으로 데이터 패킷을 전송하게 하는 블랙홀 공격을 감행하고 있는 중에 노드 1이 발송한 RREQ(1,4) 패킷이 노드 2을 거쳐 노드 4에 도달한다.

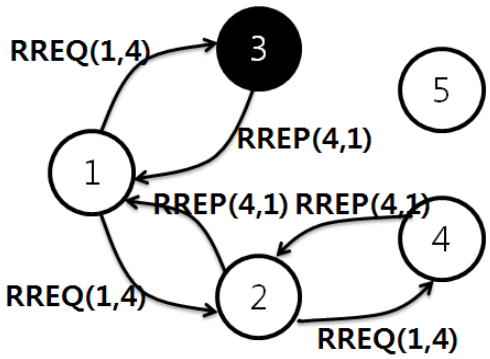

그림 2. IDS AODV[3]
Fig. 2 IDS AODV[3]

원 수신노드인 노드 4는 RREQ(1,4)에 대한 응답으로 RREP(4,1) 패킷을 노드 1로 발송한다. RREP(4,1)을 수신한 노드 1은 RREP(4,1)이 원 수신노드로부터 발신된 패킷으로 판단하여 노드 2를 경유하여 노드 4에 이르는 전송경로로 재설정하고, 블랙홀 노드 3이 위조하여 발신한 RREP(4,1)에 의하여 설정된 전송경로를 즉시 폐기한다. 이 과정을 거쳐 블랙홀 노드 3으로의 전송은 중단되며, 원 수신노드인 노드 4로의 데이터 패킷전송이 시작된다. 이와 같이 RREP() 패킷의 수신시간 차이를 활용하면 간단한 수준의 블랙홀 노드 검출 및 전송경로 복구가 가능하다.

III. 시뮬레이션 및 성능 분석

3.1. 시뮬레이터

본 논문에서는 블랙홀 공격에 대하여 IDS로 대응하는 MANET에서 노드의 이동패턴이 전송성능에 미치는 영향을 음성 서비스 트래픽을 대상으로 분석하였다.

성능측정에는 NS-2를 기반으로 한 컴퓨터 시뮬레이션을 사용하였다. MANET은 NS-2의 ADHOC 기능을 사용하였으며, 블랙홀 기능과 IDS 기능은 NS-2의 AODV를 수정하여 사용하며, VoIP 기능은 NS2VoIP 패치[4]을 사용하여 시뮬레이터를 구성하였다. 전송성능 측정에 사용할 음성 트래픽은 표준 규격에 맞추어 생성하였다. 시뮬레이션에서 라우팅 기능은 NS-2의 AODV 모듈, 추가로 설정한 blackholeAODV 및 idsAODV를 사용하였다.

시뮬레이션에서 일반노드는 블랙홀 공격에 대응하는 수단이 없는 노드이고, IDS 노드는 블랙홀 공격에 대응하여 IDS 기능을 갖춘 노드를 의미한다. 본 논문의 시뮬레이션에서는 블랙홀 노드를 제외한 모든 노드는 일반 노드이나 IDS 기능을 갖춘 것으로 구성된다.

3.2. 시뮬레이션 환경

본 논문에서는 노드의 이동패턴이 블랙홀 공격 및 IDS이 있는 MANET의 전송성능에 미치는 영향을 분석하기 위해서 컴퓨터 시뮬레이션에서 노드의 이동패턴을 사용하였다.

노드의 이동패턴으로 랜덤이동, 고정이동, 방향이

동, 해산이동 및 집합이동을 고려하였다. 랜덤이동은 MANTET내의 노드들이 랜덤한 방향으로 이동하며, 고정이동에서는 노들이 이동하지 않고 고정되며, 방향이동은 노들이 모두 같은 방향으로 이동하며, 해산이동은 노드들이 네트워크의 가장자리로 이동을 하며, 집합이동은 노드들이 네트워크의 중심부로 이동을 의미한다. 이와 같은 노드의 이동패턴은 시나리오 파일에 정의된다. 1회의 시뮬레이션에서 MANET 내의 모든 노드들은 동일패턴으로 이동하는 것으로 간주한다.

시뮬레이션에서 각 노드들은 일정규모의 MANET에 랜덤하게 배치되며 시나리오 파일에 정의된 이동패턴에 따라 지정된 이동을 시뮬레이션 전체 기간 동안 지속한다. 노드들은 이동패턴 따라 최대 2[㎧]의 속도로 이동하며 VoIP 트래픽을 송수신 한다. 이 때 노드가 생성 가능한 연결의 수는 최대 1로 가정하며, 블랙홀 노드는 연결을 생성하지 않는 것으로 한다. 따라서 MANET내의 연결의 최대 수는 블랙홀 노드를 제외한 일반 노드 수의 1/2이다.

시뮬레이션에서 사용된 파라미터는 표 1과 같다.

표 1. 시뮬레이션 파라미터
Table 1. Simulation parameters

Parameters	Values	
Network Scale	670×670[㎡]	
MAC	802.11g	
Routing	A O D V	
Nodes	Normal Nodes	29
	Blackhole Nodes	1
VoIP Connection	Max. 15	
VoIP Traffic	G.723.1	

3.3. 성능 파라미터

VoIP 전송 성능에는 MOS, 지연 및 호연결율이 표준 평가척도로서 사용되며 요구수준[5-7]은 각각 MOS 3.6 이상, 종단간 지연 300[㎳] 이하, 호연결율 95[%] 이상이다. 이외의 평가척도로서 패킷손실율이 5[%] 이하 요구수준으로 사용되기도 한다.

3.4. 시뮬레이션 결과

시뮬레이션은 시도된 호연결의 수에 따라 구분하여 각 측정별로 60초 동안 실시하였다. 블랙홀 공격은 시뮬레이션 전체 기간 동안 지속적으로 발생되는 것으로 설정하였다.

시뮬레이션 결과를 그림 3~8에 제시하였다. 그림에서 각 데이터는 이동패턴(블랙홀 공격 유/무)로 표시하였다. 예를 들면 Directional(Blackhole)은 블랙홀 공격이 있는 환경에서 노드들이 방향이동을 하는 경우를 의미한다. 그림에서 Random은 랜덤이동, Fixed는 고정이동, Directional은 방향이동, Dismissal은 해산이동, Assembly는 집합이동을 의미한다.

그림 3과 4는 MOS를 제시하고 있다. 그림에서 MOS는 요구수준인 3.6을 충족하고 있으나 구간에 따라 다소 변동을 보이고 있다. 특히 집합이동인 경우가 다른 이동패턴에 비하여 블랙홀 공격에 취약한 것으로 나타났으며 IDS로 대응한 후에도 MOS의 회복이 낮은 것으로 측정되었다. 이는 집합이동의 경우 노드 집중에 따라 나타난 현상으로 분석된다.

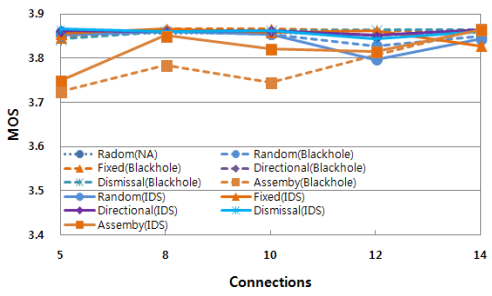

그림 3. MOS
Fig. 3 MOS

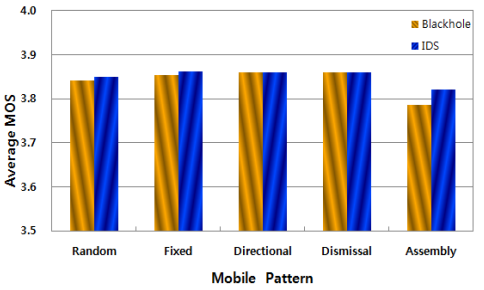

그림 4. 평균 MOS
Fig. 4 Average MOS

그림 5와 6은 시도된 호연결에 대한 성공한 호연결율을 제시하고 있다. 블랙홀 공격이 없을 경우에 호연결율은 100[%]에 이르고 있으나 블랙홀 공격이 발생될 경우 시도된 연결수가 증가할수록 낮아졌으며 그 변동폭이 20[%]~80[%]로 매우 컸다. 블랙홀 공격에 대해 IDS로 대응한 경우에 호연결율이 일정 정도 회복되었으나 요구조건 95[%]를 충족하지 못하였다.

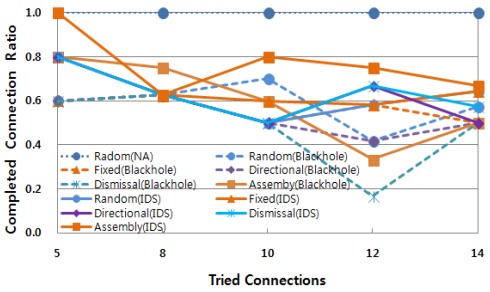

그림 5. 호연결율
Fig. 5 Call connection rate

그림 6에 의하면 블랙홀 공격에 대하여 집합이동의 호연결율이 가장 양호한 것으로 나타났으며, 방향이동과 해산이동의 경우 비교적 취약 취약한 것으로 나타났다. 해산이동의 경우 블랙홀 공격시 호연결율이 48[%]로 가장 낮았으며, IDS 대응시에는 집합이동의 호연결율이 78[%]로 가장 높았다. 블랙홀 공격과 IDS 대응시 호연결율 개선 정도는 랜덤이동이 5[%]로 가장 낮았으며, 집합이동이 18[%]로 가장 높았다. 그러나 모든 경우에서 호연결율 요구조건 95[%]가 충족되지 못하였다.

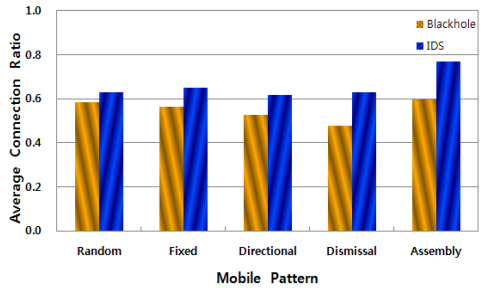

그림 6. 평균 호연결율
Fig. 6 Average call connection rate

그림 7과 8에 종단간 지연을 제시하였다. 그림 6에 의하면 모든 구간에서 지연 요구조건 300[ms]가 충족됨을 알 수 있다. 그러나 집합이동의 경우 지연의 변동이 다른 이동에 비하여 크게 나타났으며, 그림 7에 의하면 평균값 역시 다른 이동패턴에 비하여 높았다.

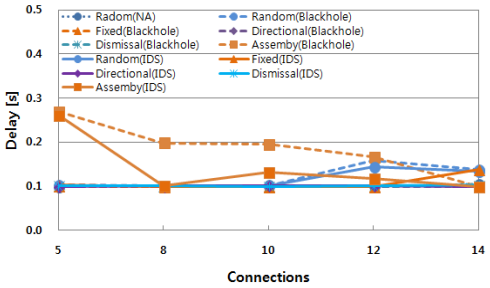

그림 7. 지연
Fig. 7 Delay

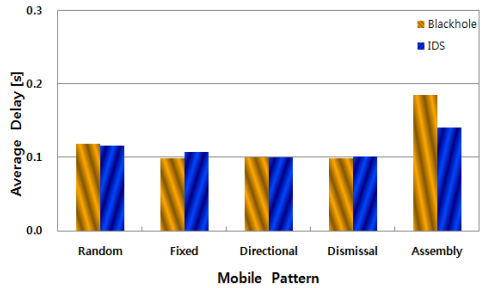

그림 8. 평균 지연
Fig. 8 Average delay

그림 3~6에 의하면, 성능 파라미터 별로 블랙홀 공격과 IDS 사용에 따른 성능에 차이가 발생되었다. 호연결율의 경우, 블랙홀 공격에 대응하여 IDS를 사용한 경우에 호연결율 개선이 평균 66[%]로 측정되었으나 요구조건 95[%]에 29[%]가 미달하였다. MOS의 경우 요구조건 3.6을 충족하며 약 0.12[%]의 성능개선이 있었고, 종단간 지연의 경우 요구조건 300[ms]를 충족하며 약 7[%]의 개선이 있었다. 이를 고려하여 볼 때 블랙홀 공격에 대하여 호연결율이 매우 취약한 것으로 나타났다.

또한 이동패턴별로 살펴보면 가장 심각한 성능저하가 발생되는 호연결율의 경우 블랙홀 공격 발생시에 이동패턴별 성능의 차이가 15[%]로 크게 발생하였다.

특히, 방향이동과 해산이동에 대한 성능저하가 다른 이동패턴에 비하여 크게 나타났으며, IDS로 대응한 경우에 대한 성능회복 또한 미진하였다.

따라서 음성서비스를 제공하는 MANET의 경우 블랙홀 공격에 대응하여 호연결율의 저하를 방지할 수 있는 효과적인 IDS의 개발이 필요하며, 이동패턴에 따른 호연결율의 성능차를 최소화 할 수 있는 방안이 요구된다.

Ⅳ. 결 론

본 논문에서는 블랙홀 공격에 대응 수단으로서 IDS 성능을 분석하기 위해 다양한 이동패턴을 고려한 MANET에서 IDS가 전송성능에 미치는 영향을 컴퓨터 시뮬레이션을 사용하여 분석하여 보았다.

시뮬레이션 결과 블랙홀 공격에 MOS나 종단간지연 보다 호연결율이 더 민감한 것으로 분석되었으며, IDS로 대응한 경우에 호연결율이 요구조건에 62~77[%]이며, 노드의 이동패턴별로 차이가 15[%] 정도 되는 것으로 관찰되었다.

따라서 MANET에서 안정적인 음성 서비스를 제공하기 위해서는 호연결율 요구조건을 충족하며, 이동패턴별 호연결율의 차이를 최소화할 수 있는 IDS 개발이 요구된다.

본 연구의 방법과 결과는 블랙홀 공격이 발생되는 네트워크에서 블랙홀 공격의 영향 분석, IDS로 대응한 경우의 전송성능 평가에 활용될 수 있다.

다양한 노드 이동패턴에 대한 블랙홀 공격과 IDS 대응에 대한 성능분석, 그 평가에 기반한 효과적인 IDS의 개발이 향후 연구 과제이다.

감사의 글

본 논문은 2013년도 동양대학교 교내연구지원 사업의 지원으로 수행되었음.

References

[1] A. Gupta, H. Sadawarti, and A. Verma, "Performance Analysis of MANET Routing Protocols in Different Mobility Models," *Int. J. of Information Technology and Computer Science,* vol. 5, no. 6, June 2013, pp. 73-82.

[2] Y. Kim, "End-to-End Performance of VoIP based on Mobility Pattern over MANETs," *Int. J. of Maritime Information and Communication Sciences*, vol. 7, no. 3, Sept. 2009, pp. 309-313.

[3] Y. Kim, "Transmission Performance of Application Service Traffic on MANET with IDS," In *Proc. Conf. on KIICE 2012*, vol. 16, no. 1, May 2012, pp. 584-587.

[4] A. Bacioccola, C. Cicconetti, and G. Stea, "User - level Performance Evluation of VoIP using NS-2," In *Proc. 2nd Int. Conf. on Performance Evaluation Methodologies and Tools*, Nantes France, Oct. 2007.

[5] 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.

[6] 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.

[7] 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 전자통신공학과 졸업(공학석사)

1990년 광운대학교 대학원 전자통신공학과 졸업(공학박사)

현재 동양대학교 정보통신공학과 교수

※ 관심분야 : 통신프로토콜, MANET, VoIP, 컴퓨터 시뮬레이션, 수중통신