블랙홀 공격이 있는 MANET에서 패킷취합전송의 종단간 성능

김영동*

End-to-End Performance of Packet Aggregation Transmission over MANETs under Blackhole Attacks

Young-Dong Kim*

요 약

본 논문에서는 블랙홀 공격이 발생되는 MANET에서 패킷취합전송의 종단간 성능을 여러 종류의 VoIP 트래픽을 대상으로 측정하고 분석하여 보았다. NS-2를 기반으로 구성한 VoIP 시뮬레이터를 이용하여 MOS, 호 연결율, 네트워크지연 및 패킷손실율 종단간 전송성능으로 측정하였다. 측정 결과의 분석을 통하여 블랙홀 공격이 있는 MANET에서 패킷취합전송의 특성을 여러 VoIP 트래픽 별로 제시하였다. 블랙홀 공격이 있는 MANET 환경에서 VoIP 서비스 구현에 요구되는 패킷취합전송의 특성을 본 논문의 결과로 제시하였다.

ABSTRACT

In this paper, end-to-end performances for some VoIP traffics are measured and analyzed over MANET(Mobile Ad-hoc Networks) with packet aggregation transmission under blackhole attacks. A VoIP simulator based on NS-2 is used for performance measure. In the simulation, MOS, call connection ratio, network delay and packet loss rate are measured for end-to-end transmission performance. With analysis of measured data, characteristics of each traffics for performance parameters of packet aggregation transmission is showed on MANET under blackhole attack, As a results of this paper, some considerations be required for packet aggregation transmission are suggested to implement VoIP services on MANET under blackhole attacks.

키워드

MANET, VoIP, Blackhole attack, Packet aggregation, Transmission performance
이동임시망, IP전화, 블랙홀 공격, 패킷취합, 전송성능

Ⅰ. 서 론

인터넷을 비롯한 정보통신망 사용자의 급속한 증가와 스마트폰과 같은 지능형 단말기의 보급 확대는 정보 활용을 통한 편리성 추구라는 긍정적 이용 기회의 제공과 더불어 비합법적 정보취득 기회의 추구, 취득 정보의 악의적 사용 및 정보통신망의 불법적 사용과 같은 부정적 현상의 잦은 발생 원인을 제공하고 있다. 특히 이런 현상은 기반통신구조를 사용하지 않고 임시적으로 구성되어 사용되는 MANET 환경에서는 심각한 결과를 일으킬 수 있다.

스마트폰의 경우에 고성능의 연산기능과 WiFi와 같은 통신기능을 구비하고 있어 통신 단말기로서 순기능적 요소를 갖춘 반면에 이 순기능을 활용한 역기

* 동양대학교 정보통신공학과(ydkim@dyu.ac.kr)
접수일자 : 2012. 10. 15 심사(수정)일자 : 2013. 01. 15 게재확정일자 : 2013. 01. 21

능으로서 정보침해를 받을 가능성 또한 커지고 있다. 스마트폰은 연산기능과 통신기능 때문에 그 자체가 공격의 대상이 될 뿐만 아니라 공격의 수단으로 악용될 수 있으며, 이 현상은 앞으로 지속적으로 심화되어 질 것으로 예상된다.

스마트폰의 급속한 보급은 임시망으로서 MANET 구축의 좋은 환경으로 작용하고 있다. 임시망으로서 MANET 목적 달성에 필요한 적절한 규모의 연산기능과 통신기능을 스마트폰이 갖추고 있기 때문이다. 그러나 MANET의 보급이 지속적으로 이루어지기 위해서는 통신기반 구조 사용이 수월치 못하여 발생되는 문제점들을 해결해야 한다. 이 문제점의 하나가 정보침해 현상이다.

MANET에 대한 정보침해 유형은 매우 다양하지만 그 가운데 대표적인 하나가 블랙홀(blackhole) 공격이다. 블랙홀 공격은 라우팅 정보를 바꿔치기하여 트래픽의 이동위치를 공격자의 의도대로 변화시켜 사용자간에 정보전송이 올바르게 이루어지지 못하게 하는 공격으로 라우팅 기능이 빈번하게 사용되는 MANET의 전송기능에 심각한 영향을 발생시킨다[1][2].

한편, 스마트폰과 같은 지능형 단말기의 보급에 기반하여 새로운 응용서비스가 개발되고 있는데 그 가운데 하나가 VoIP(Voice over Internet Protocol)이라 불리우는 음성 서비스이다. VoIP 서비스는 유선인터넷서비스에 도입할 목적으로 개발되어 현재에는 기존의 회선교환형 전화서비스를 대체함은 물론 모바일 인터넷으로 도입이 확대되고 있으며, 향후 MANET으로 적용이 넓어질 것으로 판단된다.

음성 트래픽의 경우 패킷의 길이가 짧아 각각을 독립적으로 전송할 경우 오버헤드의 증가로 인한 전송율의 감소가 발생된다. 이를 개선하기 위한 수단으로 패킷취합전송이 고려되고 있다. 패킷취합전송은 짧은 길이의 패킷을 일정크기의 단위패킷에 모아 전송함으로서 패킷의 전송효율을 증가시키는 방안이다[3].

패킷취합전송 환경에서 블랙홀 공격이 발생되면 영향을 받는 데이터의 규모가 패킷취합을 사용하지 않을 경우에 비하여 증가할 가능성이 크다. 따라서 블랙홀 공격이 발생되는 환경에서 패킷취합전송의 성능을 분석하는 것은 매우 의미 있는 일이다.

본 논문에서는 블랙홀 공격이 발생되는 MANET 환경에서 패킷취합전송에 따른 종단간 성능을 분석하여보았다. 전송성능은 VoIP 서비스를 전제로 한 음성 트래픽을 대상으로 하였다.

본 논문은 NS(Network Simulator)-2를 기반으로 VoIP 모듈을 추가하여 구성한 시뮬레이터를 사용하여 수행되었다. 시뮬레이션은 750×750[㎡] 규모와 30개의 노드로 구성되는 MANET을 대상으로 수행하였으며, MOS, 호연결율, 종단간지연, 패킷손실율을 측정하였다.

본 논문의 구성은 다음과 같다. Ⅱ장은 블랙홀 공격, Ⅲ장은 패킷취합전송, Ⅳ장은 시뮬레이션 및 성능분석 그리고 Ⅴ장에서 결론으로 연구결과 및 향후의 연구방향을 제시하였다.

Ⅱ. 블랙홀 공격

MANET에 대한 대표적인 침해유형의 하나가 라우팅 기능에 대한 공격이다[4]. 라우팅 공격은 네트워크 내에서 전달되는 패킷을 송수신자가 원하는 원래의 목적지가 아닌 공격자가 의도한 곳으로 이동시킬 목적으로 시도된다. 주로 라우팅 파라메타 값을 추가하거나 변경하는 형태로 이루어지는 라우팅 공격에는 블랙홀(blackhole), 그레이홀(grayhole), 웜홀(warm-hole)공격 등이 있다.

블랙홀 공격은 라우팅 정보를 변경하여 모든 노드들이 블랙홀 노드로 패킷을 전송하게 하고 이를 수신한 블랙홀 노드는 자신에게로 수신되어진 패킷을 더 이상 전송하지 않고 폐기함으로서 MANET의 전송기능을 방해하는 공격이다. 블랙홀 공격은 공격노드가 지리적으로 MANET의 가운데 위치할 경우 가장 효과적인 공격을 시도할 수 있으나, 그렇지 않은 경우라 하더라도 MANET의 전송기능에 치명적인 손상을 입힐 수 있다.

MANET에서 블랙홀 공격은 그림 1과 같이 발생된다. 그림 1의 MANET은 5개 노드로 구성되며, 노드 1/2/4/5는 일반노드이고 노드 3은 블랙홀 노드이다. 각 노드들은 ADOV(Ad-Hoc On-Demand Distance Vector) 방식을 사용하여 경로를 선정한다. AODV는 RREQ(Route Request), RREP(Request Replay), RRER(Route Error) 등의 제어 패킷이 사용하여 패킷전송 요구가 있을 경우에 패킷전송에 사용될 경로를 생성하고 관리하는 동적 라우팅 방식이다.

그림 1에서 블랙홀 공격이 없는 정상상태인 경우, 노드 1은 노드 4로 정보전송을 위해, RREQ 패킷을 사용하여 경로선정 과정을 시작한다. 노드 1의 RREQ 패킷은 브로드캐스팅 방식으로 인접노드를 거쳐 노드 4에 도달된다. 노드 1로부터의 RREQ 패킷을 수신한 노드 4는 RREP 패킷을 노드 1로 전송하여 경로 선정을 완성한다[2].

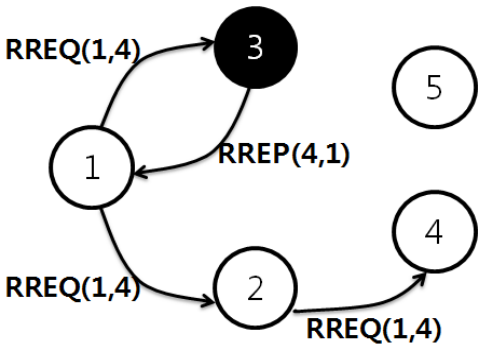

그림 1. MANET에서 블랙홀 공격[2]
Fig. 1 Blackhole attack on MANET[2]

블랙홀 공격이 있을 경우, 블랙홀 노드 3은 노드 1에서 노드 4로 경로설정을 위해 전송되어진 노드 1의 RREQ 패킷이 자신에게 수신되었을 때, 마치 자신이 노드 4인 것처럼 RREP 패킷을 거짓으로 설정하여 노드 1로 송신한다. 블랙홀 노드 3의 RREP 패킷을 수신한 노드 1은 블랙홀 노드 3을 노드 4로 인식하여 데이터 패킷을 송신하게 된다. 노드 1의 데이터 패킷을 가로챈 블랙홀 노드 3은 데이터 패킷을 노드 4로 전달하지 않고 폐기하여 노드 1에서 노드 4로 이동해야할 패킷의 전송을 방해한다.

III. 패킷취합전송

기반구조 네트워크에 비해 상대적으로 전송환경이 취약한 MANET의 전송성능 개선을 위해서는 이동되는 트래픽 양을 줄이는 것이 필요하다.

트래픽 양의 축소라는 관점에서 작은 규모의 패킷을 일정 규모의 큰 패킷에 모아서 전송하는 패킷취합전송방식은 MANET 전송성능 개선에 중요한 요인이 된다[3].

VoIP와 같은 음성전송 서비스에 패킷취합전송을 사용할 경우 그림 2와 같이 송신단에서 인코딩된 단위 데이터 여러 개를 취합하여 하나의 패킷으로 구성하여 송신하고 수신단에서 이를 분해하여 각 단위 데이터 별로 디코딩하여 수신하는 방식이다. VoIP 전송에서 패킷취합전송은 패킷오버헤드 비중을 줄여 패킷 전송효율을 증가시키며, 이는 음성통화품질의 향상으로 이어진다.

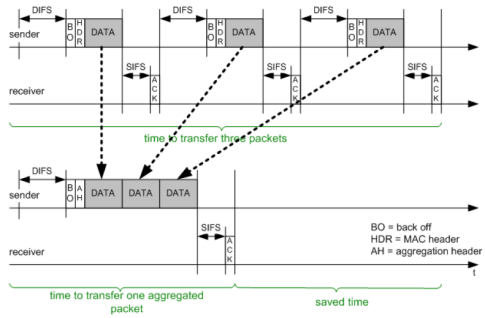

그림 2. 패킷취합전송[3]
Fig. 2 Packet aggregation transmission[3]

라우터의 지원이 가능한 기반구조 네트워크이나 메쉬 네트워크에서 패킷취합은 여러 소스에서 생성되는 트래픽을 전송경로 상에서 동일 경우 라우터를 대상으로 하나의 패킷에 취합하여 전송하는 경우에 매우 효과적이다. 그러나 본 논문에서는 대상 네트워크가 라우터 등의 통신기반구조를 사용하지 않은 MANET임으로 고려하여 단일 소스에서 발생되는 여러 단위 데이터를 하나의 패킷에 취합하여 구성하는 것으로 가정한다.

IV. 시뮬레이션 및 성능분석

3.1. 시뮬레이터

본 논문은 블랙홀 공격이 있는 MANET에서 패킷취합전송의 종단간 성능측정을 컴퓨터 시뮬레이션을 사용하여 수행하였으며, 측정 대상 응용서비스로는 VoIP를 사용하였다.

시뮬레이터는 NS-2 2.33을 기반으로 NS2VoIP 패치를 사용하여 구축하였다[5][6]. MANET은 NS-2의 ADHOC 기능을 사용하여 구성하고, VoIP 트래픽은

NS2VoIP 기능을 사용하여 코덱 규격에 맞추어 생성하였다. 블랙홀 공격은 NS-2의 AODV를 수정한 blackhole-AODV를 사용하여 구현하였다.

일반노드는 AODV 방식으로 라우팅을 수행하며, 블랙홀 노드는 blackhole-AODV를 사용하여 라우팅 기능에 대한 공격을 시도한다. 블랙홀 공격은 시뮬레이션 중에 일정 기간 동안 발생되어지며, 블랙홀 노드와 일반노드는 랜덤하게 선정하였다.

3.2 시뮬레이션 환경

시뮬레이션에서 일반노드와 블랙홀 노드를 비롯한 각 노드들은 일정 규모의 MANET내에 랜덤하게 분포하며, 최대 2[㎧]의 랜덤속도로 랜덤방향으로 독자적으로 이동한다. 일반노드는 랜덤이동 중에 다른 일반노드들과 VoIP 트래픽을 송수신한다. 블랙홀 노드는 VoIP 트래픽을 생성하지 않는 것으로 간주하였다.

한 노드가 생성할 수 있는 최대 VoIP 연결수는 1로 설정하였다. 따라서 생성 가능한 최대 VoIP 연결수는 전체 일반노드 수의 1/2이다. VoIP 트래픽은 G.711, G.723.1, G.729A, GSM.AMR 규격에 맞추어 생성하였다. 기타 시뮬레이션 파라미터는 표 1과 같다.

표 1. 시뮬레이션 파라미터
Table 1. Simulation parameters

파라미터	설정값	
네트워크 규모	750×750[㎡]	
MAC	802.11b	
라우팅	AODV	
노드수	일반노드	29
	블랙홀 노드	1
VoIP 연결 수	최대 14	
VoIP 트래픽	G.711, G.723.1, G.729A, GSM.AMR	

3.3 성능 파라미터

MANET의 종단간 전송성능으로서 VoIP 성능평가 척도에는 MOS, 종단간지연, 호연결율, 및 패킷손실율이 주로 사용된다[7][8][9][10]. 본 논문에서 사용한 MOS, 종단간지연, 호연결율에 대한 요구수준은 표 2와 같다[7]. 표 2에서 MOS의 요구수준은 3.6 이상으로 이동전화의 요구수준급이며, 유선전화의 요구수준 4.0에 비하여는 다소 낮은 값이다.

MOS 요구수준은 3.6 은 미디엄(medium) 품질 수준이며, 이 보다 낮은 수준인 수용(accceptible) 품질 수준 2.0이 제시되고 있지만[11] 본 논문에서는 3.6을 요구수준의 기준으로 사용한다.

종단간지연은 300ms 이하, 호연결율은 95%이상이 각각의 요구수준이다.

표 2. 모바일 VoIP 전송품질
Table 2. Transmission quality of mobile VoIP

품질지표		요구수준
통화품질	MOS	≥3.6
	종단간지연	≤300ms
접속품질	호연결율	≥95%

기타 서비스 품질로서 패킷손실율 요구수준은 5%로 가정하였다[7].

3.4 시뮬레이션 결과 및 분석

전송성능측정을 위한 시뮬레이션은 3.1~3.3절의 조건에 맞추어 패킷취합수에 따라 구분하여 수행하였다.시뮬레이션은 각각 60초간 실시하였으며, 블랙홀 공격은 시뮬레이션 기간 동안 지속하여 발생되도록 하였다.

시뮬레이션 결과를 그림 3~6에 제시하였다. 각 그림에서 시뮬레이션 결과는 트래픽별로 블랙홀 공격이 없는 경우(NA, No Attack)와 블랙홀 공격이 있는 경우(BA, Blackhole Attack)로 구분하여 표시하였다.

그림 3은 MOS 측정 결과이다. 그림 3에서 블랙홀 공격에 대한 패킷취합전송의 MOS 요구조건 충족여부는 트래픽 별로 달리 나타나고 있다. GSM.AMR은 블랙홀 공격이 있는 MANET 환경에서 패킷취합이 낮은 쪽이 더 큰 MOS 값을 보이며, G.729A의 경우는 패킷취합이 높은 쪽이 MOS 충족에 더 유리하다. G.723.1의 경우는 패킷취합수에 따라 블랙홀 공격이 있는 경우와 없는 경우의 MOS 값 변화가 매우 커서 블랙홀 공격에 불리한 특성을 보이고 있다. G.711트래픽의 경우 블랙홀 공격의 유무에 무관하게 대부분의 MOS 요구조건을 충족하지 못하고 있다.

그림 4는 호연결율을 제시하고 있다. 그림 4에서

블랙홀 공격이 있을 경우, G.711 트래픽이 다른 트래픽에 비해 호연결율이 비교적 높게 나타난 반면에 G.723.1은 낮게 나타나고 있다. 그러나 모든 트래픽에 대해 전 구간에서 패킷취합수에 무관하게 요구조건 95%가 충족되고 있지 못하다. 블랙홀 공격에 의하여 발생되는 라우팅 기능의 이상 현상에 의한 결과이다.

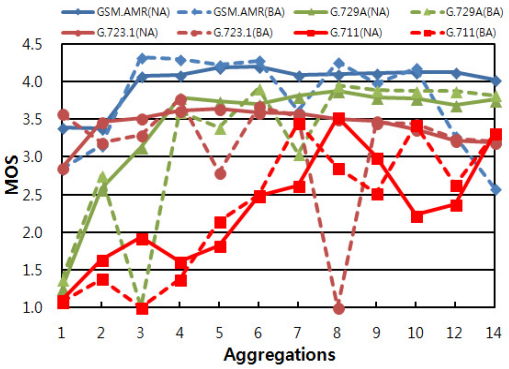

그림 3. MOS
Fig. 3 MOS

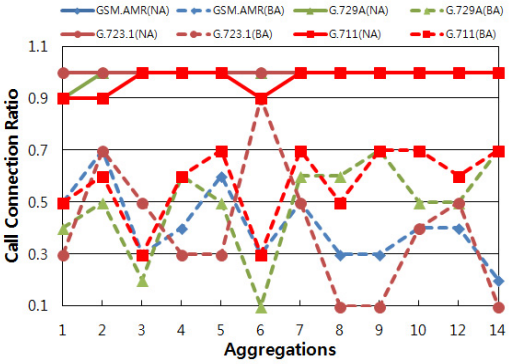

그림 4. 호연결율
Fig. 4 Call connection rate

그림 5는 네트워크 지연을 보여주고 있다. 그림 5에서 GSM.AMR 트래픽은 블랙홀 공격이 발생되더라도 대부분의 패킷취합 경우에서 종단간지연 요구수준인 300[㎳]를 만족시키기고 있지만 G.729A는 블랙홀 공격이 시도되면 패킷취합에 따른 지연 변동이 매우 큰 것으로 나타났다. G.723.1은 그 정도가 G.729A 보다는 다소 낮지만 역시 패킷취합에 따라 지연변동이 발생하고 있다. G.711의 경우는 패킷취합이 커지면 지연이 급격하게 낮아지고 블랙홀 공격이 시도되면 지연은 더 낮아지는 경향을 보이고 있지만 지연조건을 충족할 수 있는 수준은 아닌 것으로 측정되었다.

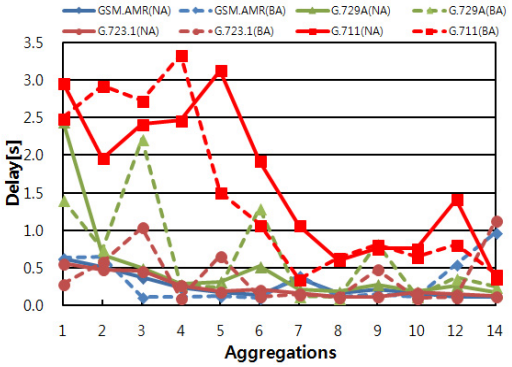

그림 5. 네트워크 지연
Fig. 5 Network delay

그림 6은 패킷손실율 결과이다. 그림 6에서 G.711을 제외한 GSM.AMR, G.729A, G.723.1 트래픽 모두 패킷취합수가 4이상일 경우 블랙홀 공격에 무관하게 요구조건 5%를 만족하고 있다.

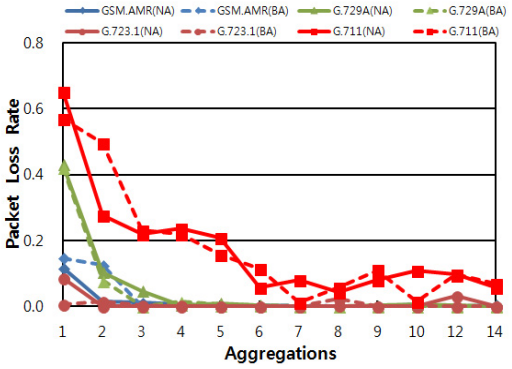

그림 6. 패킷손실율
Fig. 6 Packet loss rate

그림 3~6의 결과에 의하면 블랙홀 공격이 있는 MANET에서 패킷취합전송은 패킷취합전송을 사용하지 않은 경우에 비하여 일정정도 전송성능 개선이 이루어지고 있지만, 전송품질 요구조건 충족 여부는 트래픽 별로 전송품질 측정 파라메타에 따라 상반되게 나타나고 있다. 따라서 블랙홀 공격이 있거나 예상되는

MANET에서 음성서비스구현을 위해서는 MANET 서비스 조건과 트래픽과의 상관관계를 분석하여 적절한 전송품질이 달성될 수 있도록 해야 한다.

V. 결 론

본 논문에서는 블랙홀 공격이 있는 MANET에서 VoIP 트래픽의 전송성능을 패킷취합전송 관점에서 컴퓨터 시뮬레이션으로 분석하여 블랙홀 공격이 종단간 전송성능에 미치는 영향을 측정하고 분석하여 보았다.

본 논문에서 제시한 연구 결과로서 블랙홀 공격이 발생되는 MANET에서 음성서비스 구현에 요구되어지는 패킷취합전송방식을 사용할 경우 전송품질을 보장을 위해 구현환경에 적합한 코덱을 사용하여 트래픽을 생성해야 한다. 이 과정에서 MANET 서비스 조건과 트래픽특성과의 상관관계를 분석하여 적절한 전송품질이 달성되도록 해야 하며, 블랙홀 침해에 취약한 것으로 나타나 호연결율을 보장하기 위한 적절한 대비방안이 강구되어야 한다.

본 논문에서 제시한 연구방법과 결과는 MANET에서 음성 서비스 시스템 설계, 구축 및 운영에 있어 필요한 자료로서 사용될 수 있을 것으로 생각한다.

본 논문의 결과를 확장하여 다양한 규격과 다양한 특성을 갖는 MANET 환경에서 블랙홀 공격이 MANET 응용서비스에 미치는 영향과 공격 대비 기능을 구축하는 것이 추후 연구 과제이다.

참고 문헌

[1] H.Simaremare, R.Sari, "Performace Evaluation of AODV variants on DDoS, Blackhole and Malicious Attacks", IJCSNS, Vol. 11, No. 6, pp. 277-287, 2011.

[2] 김영동, “블랙홀 공격이 있는 MANET에서 패킷취합에 따른 음성 트래픽의 전송성능”, 한국전자통신학회 종합학술대회논문집, 6권, 1호, pp. 368~367, 2012.6.

[3] N. Bayer, M. Castro, P. Dely, A. Kassler, "VoIP service performance optimization in pre-IEEE 802.11s Wireless Mesh Networks", IEEE Int. Conf. on Circuits & Systems for Communications (ICCSC 2008), pp. 75-79, 2008.

[4] 이철승, "MANET 기반 MD5 보안 라우팅에 관한 연구", 한국전자통신학회논문지, 7권, 4호, pp. 797~803, 2012.

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

[6] 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 (VALUETOOLS 2007), pp. 1-10, 2007.

[7] 김영동, "대규모 MANET에서 VoIP 트래픽의 종단간 성능", 한국전자통신학회논문지, 6권, 1호, pp. 49~54, 2011.

[8] 나성훈, 신현식 "VoIP 보안관련 주요기술에 대한 분석", 한국전자통신학회논문지, 5권, 4호, pp. 385~390, 2012.

[9] 김범준, "소프트웨어 기반 모바일 VoIP 서비스 품질 측정", 한국전자통신학회논문지, 6권, 1호, pp. 55~60, 2011.

[10] 김동연, 김범준, "와이브로를 통한 모바일 VoIP 서비스의 측정기반 품질평가 방안", 한국전자통신학회논문지, 5권, 5호, pp. 528~533, 2010.

[11] 최대우, "IEEE 802.11b WiFi 환경에서 음성코딩 방식에 따른 VoIP 용량분석", 한국전자통신학회논문지, 7권, 2호, pp. 243~248, 2012.

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, 정보보호