https://doi.org/10.33778/kcsa.2020.20.5.033

MANET에서 영역-키 기반 보안 라우팅 기법에 관한 연구

양 환 석*, 김 영 선**

요 약

이동 노드로만 구성된 MANET은 모든 노드들이 라우터 역할을 수행한다. 하지만 노드들의 빈번한 이동으로 인한 동적인 토폴로지는 라우팅 성능을 떨어뜨리고 많은 보안 취약점의 원인이기도 하다. 따라서 MANET의 성능을 좌우할 수 있는 라우팅 기법에는 보안이 반드시 적용되어야 한다. 본 논문에서는 영역-키 기반 보안 라우팅 기법 적용을 통해 다양한 라우팅 공격에 효율적으로 대응하고, 안전한 데이터 전송을 위한 기법을 제안하였다. 제안한 기법에서는 영역 기반 네트워크 구조를 이용하였으며, 각 영역내 멤버 노드들을 관리하는 관리 노드를 이용하였다. 또한 각 노드들에 키를 발급하여 이를 이용한 라우팅 기법을 적용함으로써 공격 노드로 부터의 피해를 최소화하였다. 영역 관리 노드는 라우팅 정보를 암호화하기 위한 키 발급과 발급 정보를 관리한다. 데이터 전송을 원하는 멤버 노드는 영역 관리 노드로부터 발급받은 키를 이용하여 라우팅 정보를 암호화한 후, 이를 이용하여 경로 발견을 수행하게 된다. 제안한 기법의 향상된 성능은 CBSR, ARNA 기법과 비교 실험을 통하여 확인하였으며, 실험을 통해 우수한 성능을 확인할 수 있었다.

A Study on the Zone-Key based Secure Routing Scheme in MANET

Yang Hwan Seok*, Kim Young Sun**

ABSTRACT

In MANET consisting of only mobile nodes, all nodes serve as routes. However, the dynamic topology due to frequent movement of nodes degrades routing performance and is also cause of many security vulnerabilities. Therefore, security must be applied to routing techniques that can influence the performance of MANET. In this paper, we propose a technique for efficiently responding to various routing attacks and safe data transmission through application of zone-key based security routing techniques. A zone-based network structure was used, and a management node that manages member nodes in each zone was used in the proposed technique. In addition, the damage from the attacking node was minimized by issuing a key to each node and applying this to a routing technique. The zone management node issues a key for encryption routing information and manages the issuance information. A member node that wants to transmit data encrypts routing information using a key issued from the zone management node, and then performs path discovery using this. The improved performance of the proposed technique was confirmed through a comparative experiment with the CBSR and ARNA technique, excellent performance was confirmed through experiments.

Key words : Secure Routing Protocol, Mobile Ad-hoc Network, Routing Attacks, Authentication Technique

접수일(2020년 11월 30일), 수정일(2020년 12월 23일), 게재확정일(2020년 12월 31일)

* 중부대학교/정보보호학과
** 중부대학교/전기전자공학과(교신저자)

1. 서 론

MANET(Mobile Ad Hoc Network)은 기지국과 같은 중앙 관리가 존재하지 않는 네트워크로서 제한된 통신 범위를 갖는 무선 통신을 이용하여 연결하는 특징을 가지고 있다[1]. 이러한 특징은 많은 보안 취약점에 노출되어 있으며 그 중에서도 라우팅과 관련된 보안 위협이 공격의 유형이 많으면서 그 피해 또한 가장 크다고 할 수 있다. 노드들의 이동으로 인해 경로 설정이 어렵고 많은 보안 취약점에 노출되어 있다[2]. 특히 목적 노드까지의 경로 설정을 위해 이웃 노드들의 도움이 필요한데 이때 이웃 노드들의 악의적인 행동으로 인한 정보 유출 또는 전체 네트워크의 성능이 크게 떨어질 수 있다. 이러한 라우팅 공격을 막기 위하여 그동안 다양한 방법의 보안 라우팅 기법에 대하여 연구가 이루어져 왔다. 그 중에는 네트워크 전역 정보를 수집하는 기법, 네트워크에 참여하는 노드들에 대한 인증 기법, 인프라스트럭쳐가 있는 네트워크와 비슷한 방법인 지리적 라우팅 기법 등이 있다. 하지만 이러한 많은 기법들도 보안 라우팅을 만족시키지 못하고 있는 실정이다. 따라서 MANET 환경에서는 안정된 보안 라우팅 기법이 반드시 필요하다.

본 논문에서는 보안 공격에 효율적인 대응과 안전한 데이터 전송을 위해 영역-키 기반 보안 라우팅 기법을 제안하였다. 제안한 기법에서는 노드들의 관리를 위하여 영역 기반 네트워크 구조를 이용하였으며, 영역내 관리 노드를 선출하였다. 데이터 전송을 위해서 소스 노드는 관리 노드에게 키를 요청하면, 관리 노드에서는 해당 노드의 네트워크 정보를 이용하여 키를 발급한다. 소스 노드는 키를 이용하여 라우팅 정보를 암호화함으로써 라우팅 정보를 변형하는 공격에 효율적으로 대응할 수 있게 된다. 본 논문에서 제안한 기법의 성능 평가를 위하여 CBSR, SEER 기법과 비교 실험하였으며, 이를 통해 우수한 성능을 확인할 수 있었다.

본 논문의 구성은 다음과 같다. 2장에서는 기존의 보안 라우팅 기법들의 특징들에 대하여 살펴보고 3장에서는 본 논문에서 제안한 영역-키 기반 보안 라우팅 기법에 대하여 상세히 기술하였다. 4장에서는 비교 실험을 통해 성능평가를 수행하였고 마지막으로 5장에서 결론을 맺는다.

2. 보안 라우팅 프로토콜

SEAD(Secure Efficient distance vector routing in mobile wireless AD hoc networks) 기법은 라우팅 루프 문제를 피하기 위하여 라우팅 테이블 업데이트 요소에 순서 번호를 포함시켰다[3]. 소스 노드가 경로 요청시 임의의 값을 선택하여 단방향 해시 체인을 형성한 후 다음 라우팅 갱신 정보를 전송할 때마다 해시 값을 순서대로 라우팅 테이블 갱신 정보에 포함시켜 전송하게 된다. 이 정보를 수신한 노드는 동일한 해시 체인의 해시 값을 가지고 있기 때문에 주기적으로 들어오는 라우팅 갱신 정보를 인증할 수 있는 기법이다. 이 기법은 노드 인증시 지연과 오버헤드가 발생하는 단점이 있다[4].

CBSR(Curve Based Secure Routing)은 기존의 CBGR (Curve Based Greedy Routing) 기법에 데이터 암호화를 적용한 기법으로서 경로 설정은 5단계로 이루어진다[5]. 먼저 자신의 위치정보를 그룹키를 이용하여 암호화한 후 전송한다. 그리고 베이스스테이션에서 목적 노드에게 자신의 위치와 필요한 정보를 키 체인 중 하나를 이용하여 암호화하여 전송한다. 그리고 경로 설정을 위해 암호화키는 글로벌키로 암호화하여 방송한다. 이러한 과정을 거쳐 설정되는 라우팅 경로는 다중화하게 된다. 목적 노드에서는 여러 경로에서 온 패킷들을 전송받아 내용을 비교하여 변경된 것이 있는지를 판단하게 된다.

SEER(Secure Energy-Efficient Routing) 기법은 단방향 해시 체인으로 정보 인증을 적용하였으며, 노드와 베이스스테이션 사이의 비밀키를 생성한다. 이 기법은 베이스스테이션을 루트로 하는 트리를 생성하고, 단방향 해시 체인을 초기화한다. 노드들이 이웃 노드를 통해 이벤트를 탐지하면 중간 노드를 통해 베이스스테이션에게 데이터가 전달될 수 있게 구성한다. 그리고 베이스스테이션은안전한 데이터 전송을 위해 자신이 관리하는 유일한 단방향 해시 체인을 적용하게 된다[6].

ARAN(A secure Routing protocol for Ad hoc Networks) 기법은 소스 노드와 목적 노드 사이의 인증과 노드들 사이의 링크 인증을 적용한 기법이다. 이 기법은 인증 서버를 통해 네트워크에 참여하는 노드들은 인증서를 발급받는다. 경로 탐색을 위해

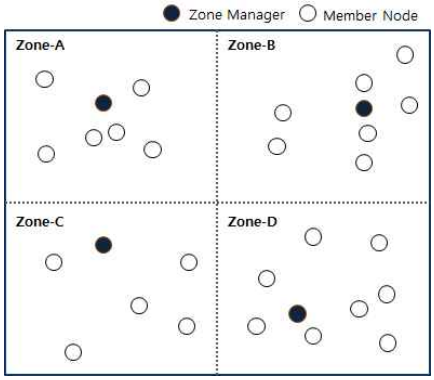
RREQ 메시지와 인증서를 비밀키로 서명하여 방송한다. 목적 노드에서는 RREP와 인증서를 비밀키로 서명하여 소스 노드에게 전달하게 된다. 중간 노드들에 대한 검증 과정은 링크간 인증을 제공하는 기법을 이용한다[7].

3. 영역-키 기반 보안 라우팅 기법

본 장에서는 전체 네트워크를 일정한 크기의 영역으로 구성한 후 각 영역 관리 노드에 의한 키 발급을 통해 보안 라우팅을 제공하는 기법을 제안하였다.

3.1 영역 기반 네트워크 구조

계층형 네트워크 구조는 노드 수가 많거나 이동이 빈번한 경우에도 데이터 처리율과 지연 같은 시스템 성능을 보장할 수 있기 때문이다. 따라서 본 논문에서는 효율적인 라우팅 지원을 위해 전체 네트워크를 일정한 크기의 영역으로 나눈 네트워크 구조를 적용하였다. 각 영역내의 노드는 크게 영역 관리 노드(Zone Manager)와 멤버 노드(Member node)로 구성된다.



(그림 1) 영역 기반 네트워크 구조

각 영역 관리 노드는 각 존의 유일한 ID를 부여받게 되고 영역 내의 멤버 노드들에 대한 정보를 관리한다. 외부 영역에서 자신이 관리하는 영역으로 새로운 노드가 이동하게 된다면 해당 노드에 대한 신뢰 정보를 얻기 위해 영역 관리 노드들간의 정보 교환이 이루어진다. 이러한 정보를 기초로 하여 멤버 노드들에 대한 신뢰 평가 및 인증을 통해 멤버 노드들이 네트워크 참여할 수 있도록 한다. (그림 1)은 본 논문에서 영역 기반 네트워크 구조를 보여주고 있다.

3.2 Zone Manager 선출

영역 관리 노드는 영역내 멤버 노드들의 신뢰 정보를 관리하는 역할을 수행하기 때문에 중요한 노드이다. 멤노 노드들에 대한 잘못된 정보를 관리하게 된다면 악의적인 노드들의 네트워크 참여를 배제시킬 수 있기 때문이다. 본 논문에서 영역 관리 노드 선출은 모든 멤버 노드들이 이웃 노드들에 대한 신뢰 값을 HELLO 메시지와 함께 전송을 한다. 여기서 신뢰도 값은 노드들이 패킷 전달에 참여한 비율로서 최대값은 1이 된다. 이렇게 이웃 노드가 많고 패킷 전달에 참여도가 높은 노드를 영역 관리 노드로 선출하게 된다. 영역 관리 노드가 선정되면 멤버 노드들은 네트워크 참여를 위하여 영역 관리 노드로부터 키를 발급받아야 한다. 그래서 영역 관리 노드는 멤버 노드들에 대한 신뢰 평가를 위하여 TMT(Trust Management Table)을 관리하게 된다. TMT는 영역 관리 노드들끼리 주기적인 정보 교환을 통해 업데이트가 진행된다. TMT의 구조는 (그림 2)에서 보여주고 있다.

Node ID	Trust	Zone History	Certificate Time	Key
2	0.4	Z-A Z-C Z-B	20:09:12	Za89l2mnt@ceoypsuuTabvrl
9	0.7	Z-D	19:10:48	TuyPPo12!qazwsxeupwoerlv
...	...	...	...	...
3	0.5	Z-B Z-A	18:16:33	Yy198498wQOpmhkeelkjsfT

(그림 2) TMT 구조

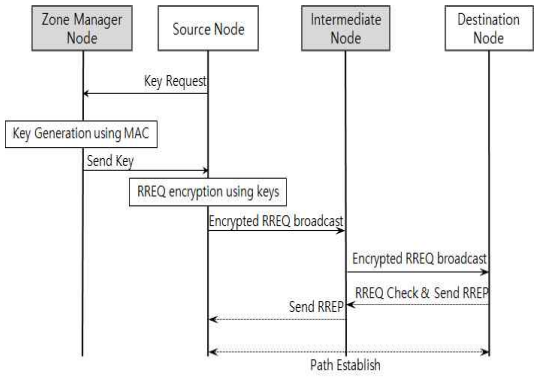
3.3 키 기반 보안 라우팅

본 절에서는 악의적인 노드들에 의해 라우팅 공격에 대한 효율적으로 대응할 수 있는 키 기반 보안 라우팅 기법에 대하여 설명한다. 노드들간 경로 업데이트를 위해 목적 필드 또는 다음 홉의 주소를 조작하는 라우팅 정보 위변조 대응을 위한 노드 인증 기법을 적용하였다. 본 논문에서 인증 노드의 역할은 영역 관리 노드가 수행하며 키 발급 과정은 다음과 같다. 소스 노드는 경로 발견을 위해 인증 노드에게

키 발급을 요청한다. 키 발급 요청을 수신한 인증 노드는 각 노드들의 고유한 값을 이용한 키 생성을 위해 키 발급 요청 노드의 MAC 주소를 이용하여 키를 생성하여 전달하게 된다. 이렇게 발급된 키 정보는 영역 관리 노드가 인증 키 테이블에 저장 관리하며, 노드들의 이동으로 인해 정보 교환시 해당 테이블의 정보를 활용하게 된다.

소스 노드는 영역 관리 노드로부터 수신한 키를 이용하여 RREQ를 방송하게 된다. 기존의 단방향 해시함수 기법은 중간 노드에서 자신이 수신한 해시 값의 유효성 검사가 어려운 단점이 있었다. 본 논문에서는 이를 보완하기 위하여 RREQ를 수신한 이웃 노드에서는 인증 노드로부터 자신이 수신한 RREQ에 대한 유효성 검사를 실시하게 된다. 이러한 방법으로 악의적인 노드들에 의한 라우팅 정보 위변조 공격을 차단시킬 수 있게 된다. 그리고 이동 노드들이 주기적으로 그들의 라우팅 테이블을 교환하거나 이웃 노드들에게 해시 값을 방송하지 않아도 되는 장점을 갖게된다. 특히 이러한 주기적인 업데이트로 인한 라우팅 오버헤드를 상당히 줄일 수 있으며, 영역 관리 노드에 의한 키 관리로 신뢰도를 높일 수 있는 장점도 갖게 된다.

(그림 3)은 위에서 설명한 영역 관리 노드를 이용한 키 생성 및 경로 발견 과정을 보여주고 있다.



(그림 3) 키 기반 경로발견 과정

소스 노드와 목적 노드간 안전한 경로가 설정되어 있다 하더라도 전송되는 데이터에 대한 보안성이 보장되는 것은 아니다. 따라서 소스 노드와 목적 노드간의 전송되는 데이터의 보안성을 향상시키기 위해서는 소스 노드와 목적 노드간의 신뢰성 높은 경로 확립이 무엇보다 중요하다 할 수 있다. 따라서 소스 노드와 목적 노드까지 설정된 여러 경로들 중에서 각 경로에 존재하는 노드들에 대한 평균 신뢰도 값을 계산하여 신뢰도가 가장 높은 경로를 선택하여 데이터를 전송하게 된다. 만약에 평균 신뢰도 값이 똑같은 경로가 여러개 존재하게 된다면 길이가 짧은 경로를 선택하여 데이터 전송의 효율성을 높이도록 하였다. (그림 4)는 경로상에 존재하는 각 노드들의 신뢰도를 이용한 경로선택을 하는 보안 라우팅 기법의 pseudo code를 보여주고 있다.

```
double cal_trust(Node_ID, Zone_ID) {
    double trust = 0;
    self.node_Id = Node_ID;
    self.zone_Id = Zone_ID;
    if(self.node_Id)
        trust = Reqest_Trust(self.node_Id, self.zone_Id);
    return trust;
}

select_Neighbor(*path) {
    double avgTrust = 0;
    int sum = 0;
    while (path != NULL) {
        path = cal_trust(node_Id, zone_Id);
        sum += path;
        }
    avgTrust = sum / sizeof(path);
}
```

(그림 4) 제안한 보안 라우팅 pseudo code

4. 실험 및 결과

4.1 실험 환경

이 장에서는 본 논문에서 제안한 영역-키 기반 보안 라우팅 기법의 성능을 평가하였다. 성능 평가를 위하여 ns-2 시뮬레이터를 사용하였으며, 다음과 같은 환경에서 실험을 실시하였다. 먼저 실험에 사용한 네트워크의 크기는 1000×1000, 전송 범위 200m, 실험 시간은 300초로 하였다. 실험 시간동안 5개의 공격 노드에서 블랙홀 공격을 각각 5회씩 실행하였다. 실험에 사용한 이동 노드 모델은 random-way point 모델이고 0 ~ 20 m/s 사이의 속도로 이동한다. <표 2>는 실험에 사용한 환경변수를 보여주고 있다.

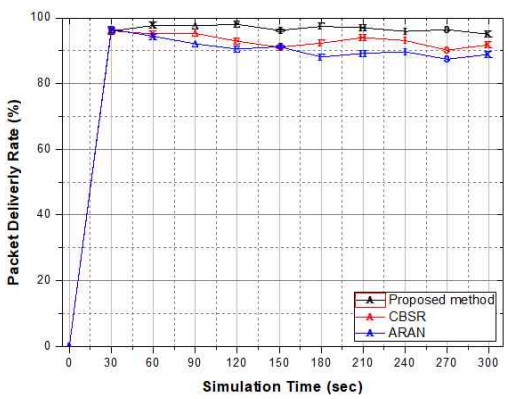
<표 1> 실험에 사용한 환경 변수

parameter	values
Network size	1000m×1000m
Routing Protocol	AODV
Speed	0~10m/s
Pause Time(sec)	20
Bandwidth	2MB
Number of Node	50
Traffic	CBR
MAC Protocol	IEEE 802.11 DCF

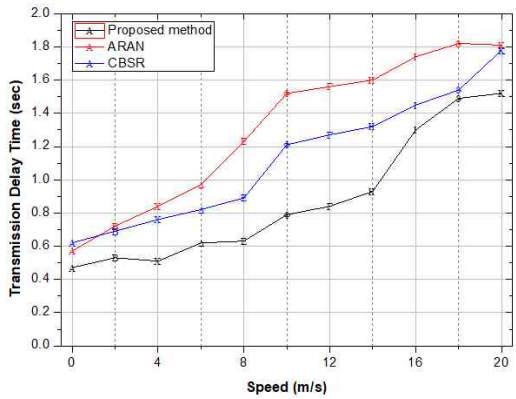
4.2 실험 결과

본 논문에서는 CBSR과 ARAN 기법들과 비교 실험을 통하여 제안한 기법의 우수한 성능을 측정하였으며, 성능 평가 기준은 패킷 전달 비율, 데이터 전달 지연 시간, 제어 패킷의 양으로 설정하였다.

(그림 5)에서는 패킷 전송 비율 측정 결과를 보여주고 있다. CBSR 기법은 베이스스테이션에서 노드들의 위치 정보를 관리하기 때문에 노드들의 이동에도 높은 패킷 전송 비율을 보여주었으며, ARAN 기법은 노드들의 인증을 위한 공개키 배분 문제와 신뢰된 인증 서버의 선택의 어려움으로 인해 세 기법들 중에서 가장 성능이 떨어지는 결과를 보였다. 제안한 기법은 노드들의 이동이 많더라고, 영역 관리 노드들에 의한 노드 관리와 키를 이용한 경로 설정이 이루어지기 때문에 공격이 존재하는 상황에서도 우수한 결과를 보여주었다.



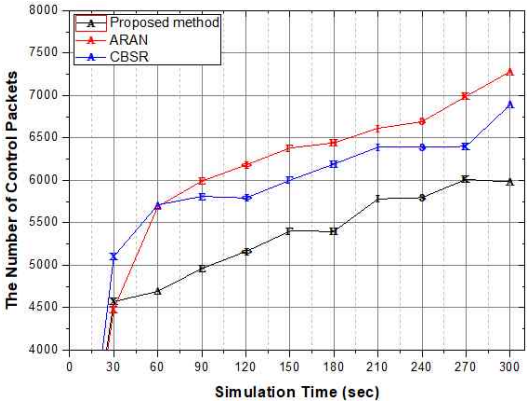
(그림 5) 패킷 전달 비율



(그림 6) 전송 지연 시간

소스 노드와 목적 노드 사이의 전송 지연시간 측정 결과는 (그림 6)에서 보여주고 있다. 이 성능 기준은 라우팅 프로토콜의 경로 설정의 우수성을 평가하기 위한 것이다. ARAN 기법은 각 노드들이 공개키를 가지고 있어야 하고, 이들을 서로 인증하는 과정이 필요하기 때문에 지연시간이 길게 나타났다. CBSR 기법은 글로벌 키를 이용한 암호화를 실행하기 때문에 공격에 존재하는 상황에서 전송 지연시간에 대해 좋은 성능을 보였다. 제안한 방법에서는 라우팅 정보 변조 차단과 다중 경로 중에서 신뢰도 값이 높은 경로를 이용하기 때문에 노드들의 이동이나 공격에도 우수한 성능을 보였다.

(그림 7)은 제어 패킷의 양을 측정한 결과를 보여주고 있다. 제어 패킷의 양이 많다는 것은 네트워크의 전체적인 성능이 떨어진다는 것을 의미하는 것으로 이는 라우팅 프로토콜의 성능을 확인할 수 있는 기준이라 할 수 있다. 제어 패킷의 양은 노드들의 이동, 경로 설정 및 경로 유지와 관련이 있다. 그림에서 보듯이 ARAN 기법은 인증 서버와 비밀키 교환 그리고 노드들간의 키 공유를 위한 제어 메시지로 패킷의 양이 적지 않음을 확인할 수 있었다. CBSR 기법은 위치 정보 전송, 목적 노드와의 정보 교환 그리고 경로 설정을 위해 암호화된 데이터 방송 때문에 측정 결과가 높게 나타났으며, 제안한 기법에서는 영역 관리 노드로부터 인증 받은 노드들은 경로 설정 및 데이터 전송을 위해 더 이상의 제어 패킷이 발생하지 않기 때문에 가장 우수한 성능을 보임을 확인 할 수 있었다.



(그림 7) 제어 패킷의 양

5. 결 론

이동 노드로만 구성된 MANET은 무선 통신을 이용해 빠르게 네트워크를 구축할 수 있기 때문에 적은 비용과 편리한 장점을 가지고 있다. 하지만 이러한 특징들은 많은 보안 위협에 노출되어 있는 실정이다. 특히 MANET의 성능에 큰 영향을 미치는 라우팅 프로토콜에 많은 보안 취약점이 존재한다 본 논문에서는 라우팅 정보의 위변조 공격을 차단하고 신뢰할 수 있는 데이터 전송을 제공하기 위해 영역-키 기반 보안 라우팅 기법을 제안하였다. 이를 위해 영역 기반의 네트워크 구조를 이요하였으며, 각 영역의 노드들을 관리할 수 있는 영역 관리 노드가 인증 노드의 역할을 수행하였다.

인증 노드에서는 소스 노드의 MAC 주소를 이용한 키를 발급해주었으며, 소스 노드는 이 키를 이용한 RREQ 패킷 전송으로 라우팅 정보의 위변조를 차단하였다. 또한 노드들간 안전한 데이터 전송을 위해 경로 설정시 경로상에 존재하는 노드들의 신뢰도 값을 기반으로 하였다. 그리고 선택된 여러 경로들 중에서 가장 높은 값을 갖는 경로를 선택하여 데이터 전송의 안전성을 향상시켰다.

본 논문에서 제안한 기법의 성능 평가를 위하여 CBSR, ARAN 기법과 패킷 전달 비율, 종단간 전송 지연 시간, 제어 패킷 양을 비교 실험하였으며, 실험을 통해 우수한 성능을 확인할 수 있었다.

참고문헌

[1] Anjum, S. S., Md Noor, R., & Anisi, M. H., “Review on MANET based communication for search and rescue operations,” Wireless Personal Communications, Vol.94, pp.31 - 52, 2017.

[2] Chatterjee P, Ghosh U, Sengupta I, Ghosh SK , “A trust enhanced secure clustering framework for wireless ad hoc networks,” Springer Wireless Networks, Vol.20, No.7, pp.1669 - 1684, 2014.

[3] Fleury, M., Kanellopoulos, D., & Qadri, N. N, “Video streaming over MANETs: An overview of techniques. Multimedia Tools and Applications,” pp.23749-23782, 2019.

[4] K. Park and H. Lee, "On the Effectiveness of Route-based Packet Filtering for Ditributed DoS Attack Prevention in Power-Law Internet," Proc. ACM SIGCOMM'01, pp.15-26, 2001.

[5] Moussaoui, A., & Boukeream, A., “A survey of routing protocols based on link-stability in mobile ad hoc networks,” Journal of Network and Computer Applications, Vol.47, pp.1 - 10, 2015.

[6] Di Pietro, R., Guarino, S., Verde, N. V., & Domingo-Ferrer, J., “Security in wireless ad-hoc networks－A survey,” Computer Communications Journal, Vol.51, pp.1 - 20, 2014.

[7] Il Yong Kim and Ki Chang Kim, "A Resource-efficient IP Traceback Technique for Mobile Ad-hoc Networks Based on Time-tagged Bloom Filter," ICCIT. Nov. 2008.

〔저자소개〕

양 환 석 (Hwan-seok Yang)
1998년 2월 조선대학교 이학석사
2005년 2월 조선대학교 이학박사
2007년 3월 호원대학교 연구교수
2011년 9월 ~ 현재 중부대학교
정보보호학과 조교수
email : yanghs@joongbu.ac.kr

김 영 선 (Young-sun Kim)
2006년 2월 단국대학교 전기공학과 (공학박사)
2006년~2010년 : 성균관대학교 정보통신공학부 연구교수
2010년~2011년 : MIT Post Doctoral Fellow
2012년 3월 ~ 현재 중부대학교
전기전자공학과 부교수
email : yskim@joongbu.ac.kr