디지털산업정보학회 논문지 제11권 제3호-2015년 9월
http://dx.doi.org/10.17662/ksdim.2015.11.3.069

# 신뢰도와 키를 이용한 보안 라우팅 기법에 관한 연구

양 환 석*

# *A Study on Secure Routing Technique using Trust Value and Key in MANET*

Yang Hwanseok

〈Abstract〉

MANET is composed of only the mobile nodes have a limited transmission range. The dynamic topology by the frequent movement of nodes makes routing difficult and is also cause exposed to security vulnerabilities. In this paper, we propose the security routing technique consisted of mechanism of two steps in order to respond effectively to attack by the modification of the routing information and transmit secure data. The hierarchical structure is used and the authentication node that issues the key of the nodes within each cluster is elected in this proposed method. The authentication node manages key issues and issued information for encrypting the routing information from the source node. The reliability value for each node is managed to routing trust table in order to secure data transmission. In the first step, the route discovery is performed using this after the routing information is encrypted using the key issued by the authentication node. In the second step, the average reliability value of the node in the found path is calculated. And the safety of the data transmission is improved after the average reliability value selects the highest path. The improved performance of the proposed method in this paper was confirmed through comparative experiments with CBSR and SEER. It was confirmed a better performance in the transmission delay, the amount of the control packet, and the packet transmission success ratio.

Key Words : Secure Routing, Hash Chain, Trust Value, MANET

## Ⅰ. 서론

이동 노드들로만 구성된 MANET(Mobile Ad Hoc Network)은 기지국 또는 AP와 같은 중앙 관리가 존재하지 않으며, 서로 간의 무선 통신을 이용하여 연결하는 특징을 가지고 있다[1]. 이러한 이유로 통신 범위내의 모든 이동 노드들을 발견하고 peer-to-peer 방식으로 통신하게 된다. 즉, 모든 이동 노드들은 데이터 전송을 위한 라우터 역할과 데이터 전송의 호스트 역할을 수행해야한다. 또한 노드들의 이동으로 인한 동적인 토폴로지 때문에 경로 설정이 어렵고 많은

*중부대학교 정보보호학과 조교수

보안 취약점에 노출되어 있다[2-3]. 특히 목적 노드까지의 경로 설정을 위해 이웃 노드들의 도움을 받아야 하는데, 이때 이웃 노드들의 악의적인 행동으로 인해 정보 유출 또는 전체 네트워크의 성능이 크게 떨어질 수 있다. 따라서 MANET 환경에서는 안정된 보안 라우팅 기법이 반드시 필요하다.

본 논문에서는 잘못된 라우팅 정보를 이용한 공격과 안전한 데이터 전송을 위한 보안 라우팅 기법을 제안하였다. 제안한 기법에서는 노드들의 인증 및 신뢰도 관리를 위하여 계층 구조인 클러스터를 이용하였으며, 클러스터내의 인증 노드를 선출하였다. 경로 발견을 위한 소스 노드에서는 라우팅 정보의 위변조를 막기 위하여 인증 노드에게 키를 요청하면, 인증 노드에서는 해당 노드의 MAC 주소를 이용하여 키를 발급해주게 되며, 소스 노드에서는 이 키를 이용하여 해시함수를 암호화하여 전달하게 된다. 이렇게 함으로써 라우팅 정보를 변형하는 공격을 효율적으로 차단할 수 있게 된다. 그리고 데이터 전달을 위한 보안 기능을 향상시키기 위하여 노드들의 신뢰도 값을 이용하였다. 이를 위하여 인증 노드에서는 라우팅 신뢰 테이블에 노드들의 신뢰도 값을 관리하고 설정된 다중 경로에 대해서 노드들의 평균 신뢰도 값이 가장 높은 경로를 이용하여 데이터를 전송함으로써 데이터 전송의 안전성을 향상시켰다. 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 MANET에서의 라우팅 공격과 보안 라우팅 기법들의 특징들에 대하여 살펴보고 3장에서는 본 논문에서 제안한 보안 라우팅 기법에 대하여 상세히 기술하였다. 4장에서는 비교 실험을 통해 성능평가를 수행하였고 마지막으로 5장에서 결론을 맺는다.

## Ⅱ. 관련연구

### 2.1 라우팅 공격

MANET은 무선 환경의 특성상 패킷 도청 또는 감청 등 공격이 쉬운 구조이고, 이동 노드들로만 경로를 설정하고 데이터 전송이 이루어지기 때문에 다양한 라우팅 공격에 노출되어 있다. 라우팅 공격은 패킷의 도청이나 감청을 통해 보안 상황이 요구되는 환경에서 많은 피해를 야기할 수 있는 passive 공격과 라우팅 과정에서 잘못된 정보를 삽입, 폐기 또는 변경함으로써 경로 설정을 방해하거나 패킷 전송이 불가능하게 하는 avtive 공격으로 나눌 수 있다[4-5]. 이러한 라우팅 공격들 중에서 대표적인 공격은 블랙 홀 공격, 웜 홀 공격, jellyfish attack 등이 있다.

블랙 홀 공격은 공격 노드가 잘못된 라우팅 정보를 소스 노드에게 전송함으로써 경로를 변경하는 공격이다. 즉, 경로 발견을 위한 RREQ 패킷을 분석하여 공격 노드는 소스 노드에게 목적 노드까지의 최단 경로가 마치 자신인 것처럼 RREP를 전송하여 목적 노드로 전송되어야 할 패킷을 모두 가로채는 공격이다[6]. 웜 홀 공격은 두 개의 공격 노드가 이웃 노드들을 마치 가까이에 있는 것처럼 속여서 소스 노드에게 두 노드가 이루고 있는 경로가 최적인 것처럼 속여서 데이터 패킷을 도청하는 방법과 공격 대상 노드를 많은 경로에 포함시켜 공격 노드의 에너지를 고갈시키는 방법이 있다[7]. Jellyfish attack은 공격 노드가 경로 발견을 위한 RREQ나 RREP 패킷을 정상적으로 전송하여 자신을 통한 경로가 설정되게 한 후에 데이터 패킷의 전송 지연 또는 폐기를 통해 데이터 전송에 방해를 주는 공격이다[8].

### 2.2 보안 라우팅 기법

CBSR(Curve Based Secure Routing)은 기존의 CBGR (Curve Based Greedy Routing) 기법에 데이터 암호화를 적용한 기법으로서 5단계의 과정을 거쳐 경로 설정이 이루어진다[9]. 먼저 이동 노드들은 이웃 노드들에게 자신의 위치정보를 그룹 키를 이용하여 암호화한 후 전송한다. 그리고 베이스스테이션에서 목적 노드에게 자신의 위치와 필요한 정보를 키 체인 중 하나를 이용하여 암호화하여 전송한다. 그리고 경로 설정을 위해 글로벌 키로 암호화키를 암호화하여 방송한다. 이러한 과정을 거쳐 라우팅 경로를 형성하게 되는데 이때 설정된 경로는 다중화하게 된다. 목적 노드에서는 여러 경로에서 온 패킷들을 전송받아 내용을 비교하여 변경된 것이 있는지를 판단하게 된다.

SEAD(Secure Efficient distance vector routing in mobile wireless AD hoc networks) 기법은 DSDV(Destination Sequcenced Distance Vector) 프로토콜에 라우팅 루프 문제를 피하기 위하여 테이블 업데이트 요소에 순서 번호를 포함시켰다. 이 기법은 라우팅 벙보를 수신하는 측에서 송신자를 인증하는 방식으로서 경로를 요청하는 노드가 해시 체인을 형성한 후에 라우팅 테이블 갱신 정보에 해시 값을 포함시켜 전송한다. 이웃 노드에 대한 인증 철차는 TELSA, TIK 등을 사용할 수 있으며, 인증시 지연과 오버헤드가 발생하는 단점이 있다[9].

SEER(Sercure Energy-Efficient Routing) 기법은 정보의 인증을 위하여 단방향 해시 체인을 이용하였으며, 이동 노드와 베이스스테이션 사이에 공유된 비밀키를 이용하여 기밀성을 향상시켰다. 이 기법은 베이스스테이션을 루트로 하는 트리를 생성하고, 단방향 해시 체인을 초기화한 후 이동 노드들이 자신의 이웃 노드를 통해 이벤트를 탐지하면 자신이 선택한 중간 노드를 통해 베이스스테이션에게 데이터가 전달될 수 있게 구성한다. 그리고 베이스스테이션에게 안전하게 데이터를 전송하기 위하여 각 노드들은 자신이 관리하는 유일한 단방향 해시 체인을 이용하게 된다[10].

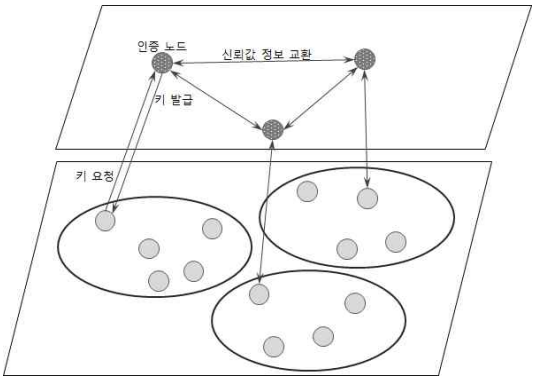
## Ⅲ. 제안한 보안 라우팅 기법

본 장에서는 MANET에서 라우팅 정보를 위변조하는 라우팅 공격을 차단하고, 라우팅 신뢰 테이블을 이용한 메시지 전송 보안 기능 제공 기법에 대하여 기술하였다.

### 3.1 시스템 구조

MANET에서 라우팅 프로토콜은 전체 네트워크의 성능을 좌우할 만큼 매우 중요한 역할을 맡고 있다. 특히 고정된 인프라가 없이 이동 노드로만 구성되어 있는 MANET에서는 라우팅 프로토콜이 많은 기능을 제공해 주어야만 한다. 그리고 어떤 네트워크 환경에서도 매우 중요한 부분이 신뢰이고, 네트워크 시스템에서 가장 중요한 신뢰의 응용이 인증이라 할 수 있다. 신뢰는 기존의 암호화 보안 기법 보다 더 많은 문제를 해결할 수 있다. 기존의 많은 보안 기법들로는 디지털 서명, 단방향 해시 알고리즘 등이 적용되어 왔었다. 하지만 이러한 기법들로는 이동 노드들사이의 신뢰 관계를 완전히 해결할 수 없다. 또한 경로 설정 또는 업데이트시 다음 홉의 정보나 목적노드 필드를 조작하는 공격을 차단할 수 있는 방법을 제공하지 못한다. 따라서 본 논문에서는 sequence number나 routing metric을 수정하여 잘못된 라우팅 정보를 생성하는 공격을 차단하고 노드들의 신뢰도 값을 이용하여 메시지 전송 보안 기능을 제공하기 위한 라우팅 기법을 제안하였다. 제안한 기법을 위하여 전체 네트

워크를 계층형 구조인 클러스터 형태를 이용하였다. 최초의 인증 노드는 각 클러스터내의 노드들 중에서 연결수가 가장 높은 노드를 선택하였으며, 라우팅 정보의 변조를 막기 위해 키를 생성해주고 관리해주는 역할을 담당하게 된다. 또한 클러스터내의 노드들에 대한 신뢰도 값이 저장되어 있는 라우팅 신뢰 테이블을 관리함으로써 데이터 전송 보안 기능을 제공하게 된다. <그림 1>은 본 논문에서 제안한 네트워크 구조를 보여주고 있다.




<그림 1> 제안한 네트워크 구조

## 3.2 키 기반 라우팅 설정

라우팅 프로토콜이 잘못된 라우팅 정보를 생성하는 공격에 효율적으로 대응할 수 있는 방법을 제공하는 것은 매우 중요하다. 하지만 경로 업데이트시 다음 홉이나 목적 필드 조작을 차단하고 목적 노드로부터 최초의 업데이트 메시지로부터 복제된 똑같은 메트릭을 사용하는 공격을 차단하는 것은 쉽지 않다. 이러한 라우팅 정보를 위변조하는 공격에 효과적으로 대응하기 위하여 인증 노드를 이용한 해시기반 인증 방법을 적용하였다. 인증 노드의 선택은 네트워크 참여 비율값이 높은 노드를 선택하였으며, 식 (1)에 의해 계산된다.

$$AN = \frac{Count \times Packet\ size}{Entrance\ time\ (\mathrm{sec})} \quad (1)$$

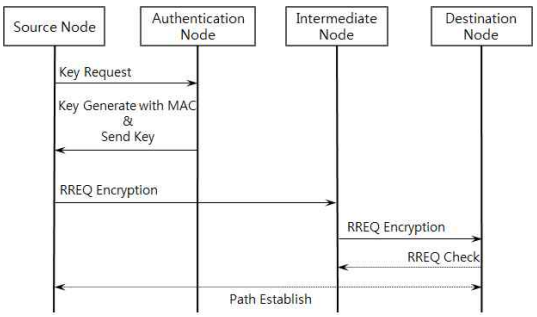
먼저, 경로 발견을 위한 소스 노드에서는 인증 노드에게 키 생성을 요구하게 된다. 키 생성 요청을 수신한 인증 노드에서는 소스 노드의 MAC 주소를 이용하여 키 값을 생성하여 소스 노드에게 전달하게 된다. 이때, 해시 값을 요구하는 노드들에 대한 요청 기록을 KRRT(Key Request Record Table)에 저장 및 관리함으로써 공격이 발생하였을 때, 공격 노드 탐색에 이용하게 된다. <표 1>은 KRRT 구조를 보여주고 있다.

<표 1> KRRT 테이블 구조

| Node ID | Authentication Node ID | Request Time | Key Value |
|---|---|---|---|
| C | K | 14:10:28 | 83DJK31P11ALH02 |
| A | K | 14:11:52 | F200394TW9932JD |
| ... | ... | ... | ... |
| F | Z | 15:12:30 | TEPO831109AYYT4 |

소스 노드에서는 인증 노드로부터 수신한 키값을 이용하여 해시 값을 암호화하여 RREQ를 방송하게 된다. 기존의 단방향 해시함수 기법 같은 경우에는 중간 노드에서 자신이 수신한 해시 값의 유효성 검사가 어려운 단점이 있었다. 이를 보완하기 위하여 RREQ를 수신한 이웃 노드에서는 인증 노드로부터 소스 노드에 대한 키를 요청하여 자신이 수신한 RREQ에 대한 유효성 검사를 실시하게 된다. 이와 같은 방법으로 RREQ를 수신한 중간 노드들도 인증 노드에게 키를 요청한 후 수신한 키를 이용하여 해시 값을 암호화하여 이웃 노드들에 전달하는 과정을 거치게 된다. 이렇게 함으로써 악의적인 노드들에 의한 라우팅 정보 수정 공격을 차단시킬 수 있게 된다. 그리고 이러한 메커니즘은 이동 노드들이 주기적으로 그들의 라우팅 테이블을 교환하거나 이웃 노드들에

게 해시 값을 방송하지 않아도 된다. 특히 이러한 주기적인 업데이트로 인한 라우팅 오버헤드를 상당히 줄일 수 있으며, 인증 노드에 의한 키 관리가 이루어짐으로써 그 신뢰도를 매우 높일 수 있는 장점을 갖게 된다.




<그림 2> 키 생성 및 경로발견 과정

<그림 2>는 위에서 설명한 인증 노드를 이용한 키 생성 및 경로 발견 과정을 보여주고 있다.

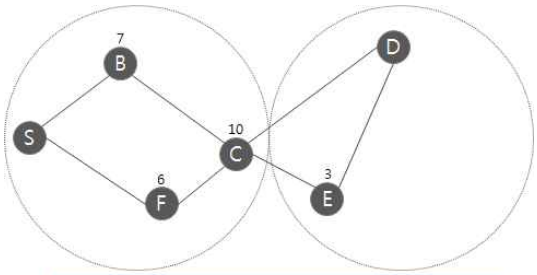
## 3.3 신뢰 경로 선택 기법

라우팅 정보의 안전성이 확보되었다 하더라도 전송되는 메시지에 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 본 논문에서는 클러스터 내의 모든 노드들에 대한 신뢰도 값은 인증 노드가 관리하는 라우팅 신뢰 테이블에 저장 및 유지된다. 라우팅 신뢰 테이블에는 노드들이 네트워크에 참여한 시간과 각각의 노드들로부터 자신이 데이터 전달에 참여한 결과를 주기적으로 수신하여 각 노드들에 대한 신뢰도 값을 관리하게 된다. <표 2>은 라우팅 신뢰 테이블의 구조를 보여주고 있다.

<표 2> 라우팅 신뢰 테이블

| Node ID | Cluster ID | Trust Value | Update Time | Entrance Time |
|---|---|---|---|---|
| G | C_1 | 8 | 14:08:48 | 13:58:21 |
| A | C_2 | 12.4 | 13:35:52 | 13:30:02 |
| ... | ... | ... | ... | ... |
| K | C_1 | 9.8 | 15:30:50 | 15:04:54 |

소스 노드에서 경로 설정을 위해 RREQ 패킷을 송신하고 목적 노드까지의 경로를 얻게 된다. 각 경로에 존재하는 노드들에 대한 신뢰도 값을 인증 노드에 요청하여 이렇게 얻어진 목적지까지의 다중 경로에 대한 평균 신뢰도 값을 계산하게 된다. 이 신뢰값이 가장 높은 경로를 선택하여 데이터를 전송하게 된다. 만약에 똑같은 신뢰도 값을 갖는 하나 이상의 경로가 존재하게 된다면 제안한 기법에서는 짧은 경로를 선택하게 된다. <그림 3>은 신뢰도 값을 이용한 경로 선택의 예를 보여주고 있다.




| Type | Cluster ID | Trust Value |
|---|---|---|
| Path 1 | S – B(7) – C(10) – D | 8.5 |
| Path 2 | S – F(6) – C(10) – E(3) - D | 8.3 |
| Path 3 | S – F(6) – C(10) - D | 8 |
| Path 4 | S – B(7) – C(10) – E(3) - D | 6.3 |

<그림 3> 신뢰 경로 선택 방법

<그림 4>는 위에서 설명한 보안 라우팅 기법의 pseudo code를 보여주고 있다.

```
init(AN);
Source_Key = Request_to_Key(AN);
do
{
    Broadcast(encryp(RREQ));
    if(check(RREQ))
    {
        Send_to_Source(RREP);
        Max_Calculate(Path_TrustValue);
    }
}while(Path_Establish);
```

## Ⅳ. 성능분석

### 4.1 실험 환경

본 논문에서 보안 라우팅 프로토콜의 성능을 평가하기 위하여 NS-2 시뮬레이터를 이용하였다. 네트워크 크기 1500 × 1500에 이동 노드 100개를 위치시켰으며, 이동 노드들은 네트워크를 자유롭게 이동하면서 위치를 임으로 변화시키는 random waypoint mobility 모델을 이용하였다. 또한 라우팅 프로토콜의 성능을 평가하기 위하여 실험 시간동안 블랙 홀 공격과 웜 홀 공격을 각각 10회 발생시켰다. <표 3>은 실험에 사용한 환경 변수를 보여주고 있다.

<표 3> 실험에 사용한 환경 변수

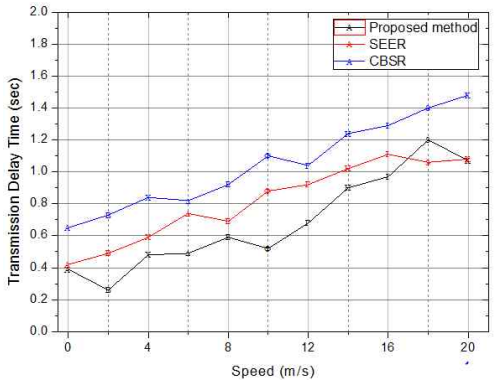
| Parameter | Value |
|---|---|
| Transmission range | 200m |
| MAC Protocol | IEEE 802.11 DCF |
| Speed | 0~20 m/s |
| Simulation Time | 300 sec |

### 4.2 성능 평가

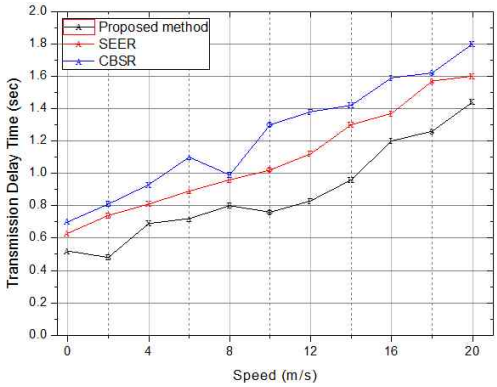
본 논문에서는 CBSR, SEER 기법과 비교 실험을 통해서 제안한 보안 라우팅 프로토콜의 성능을 평가하였으며, 종단간 전송 지연시간, 제어패킷 오버헤드, 패킷 전송 비율을 성능 평가 기준으로 설정하였다.

<그림 5>는 소스 노드와 목적 노드 사이의 전송 지연시간 측정 결과를 보여주고 있다. 이 실험에서는 블랙 홀 공격과 웜 홀 공격이 존재할 때와 그렇지 않을 때의 전송 지연시간을 비교하였다. 그림에서 보듯이 공격이 존재하지 않을 때와 공격이 존재하는 경우에는 성능의 차이를 보였다. SEER 기법은 경로 설정을 위해 중간 노드를 통해 베이스스테이션에게 데이터를 전달하는데 단방향 해시 함수를 이용한다. 하지만 해시 값의 유효성을 검증하지 않기 때문에 공격에 의한 잘못된 라우팅 정보에 의해 지연시간이 길게 나타났으며, CBSR 기법은 소스 노드가 자신의 위치 정보를 베이스스테이션에 전송해주면 글로벌 키를 이용한 암호화를 실행하기 때문에 공격에 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. 특히 웜 홀 공격의 탐지가 어려워 블랙 홀 공격보다 세 기법 모두 성능이 좋지 않은 것을 확인할 수 있었다.

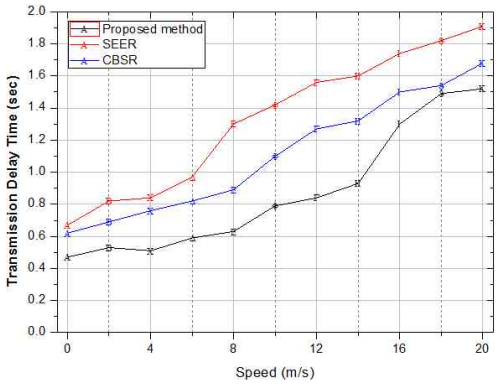
라우팅 프로토콜의 성능을 나타내는 중요한 지표 중에 하나가 경로 설정이다. 즉 제어 패킷의 양이 많을수록 전체 네트워크의 성능이 떨어지는 것을 의미하며 각 노드에서 송신하는 제어 패킷의 양을 측정함으로써 라우팅 프로토콜의 성능을 평가하였다. <그림 6>에서 보여주듯이 CBSR 기법은 소스 노드와 베이스스테이션과 위치 정보 전송, 목적 노드와의 정보 교환 그리고 경로 설정을 위해 암호화된 데이터 방송 때문에 측정 결과가 높게 나타났으며, SEER 기법은 베이스스테이션을 루트로 하는 트리 생성과 비밀키 유지를 위한 제어 패킷의 양이 다소 높게 측정되었다. 그리고 제안한 기법도 해시 정보 교환과 신뢰도 값 조회로 인해 다소 높은 결과를 보여 주었으나, 세 기법들 중에서는 가장 우수한 성능을 보였다.




(a) 공격이 없는 경우

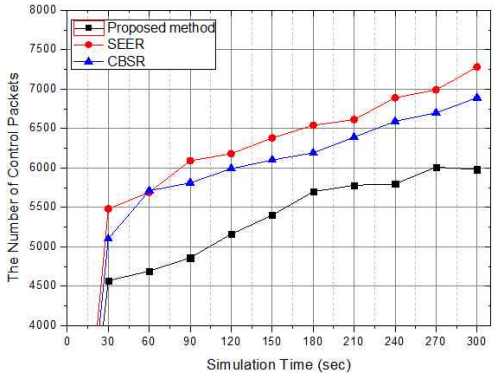



(b) 블랙 홀 공격이 있는 경우



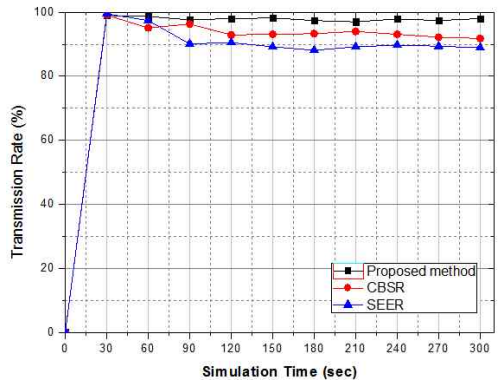

(c) 웜 홀 공격이 있는 경우

<그림 5> 종단간 전송 지연 시간




<그림 6> 제어 패킷의 양 측정 결과

라우팅 프로토콜의 경로 유지 안정성을 측정하기 위하여 <그림 7>에서는 패킷 전송 비율을 측정한 결과를 보여주고 있다. CBSR 기법은 베이스스테이션에서 소스 노드의 위치 정보를 관리하고 있기 때문에 노드들의 이동에도 패킷 전송 비율이 높았으며, SEER 기법에서는 노드들의 이동으로 인한 경로 정보 관리가 어려워 성능이 떨어졌다. 제안한 기법에서는 인증 노드에 의한 신뢰도 값 관리가 잘 이루어져 신뢰도가 높은 경로를 이용한 패킷 전송으로 패킷 전송 비율에서도 안정된 결과를 확인할 수 있었다.




<그림 7> 패킷 전송 성공 비율

## Ⅴ. 결론

MANET은 무선 통신을 이용하기 때문에 적은 비용으로 효율적이고 편리하지만 많은 보안 위협에 노출되어 있으며 그 중에서도 라우팅 프로토콜에 대한 보안이 매우 중요하다고 할 수 있다.

본 논문에서는 라우팅 정보의 변형 공격을 차단하고 신뢰할 수 있는 데이터 전송을 제공하기 위한 보안 라우팅 기법을 제안하였다. 제안한 라우팅 기법을 위하여 계층 구조의 클러스터를 적용하였으며, 키 발급 및 노드들의 신뢰값 관리를 위하여 인증 노드를 이용하였다. 라우팅 정보의 위변조를 차단하기 위하여 인증 노드에서는 소스 노드의 MAC 주소를 이용한 키를 발급해주면, 소스 노드에서는 키를 이용하여 해시 값을 암호화하여 RREQ 패킷을 전송하게 된다. 이러한 방법의 목적 노드까지 RREQ 패킷이 전송되기 때문에 공격 노드들에 의한 라우팅 정보 위변조에 효율적으로 대처할 수 있게 되었다. 또한 데이터 전송 신뢰 향상을 위하여 노드들의 신뢰도 값을 기반으로 한 경로 설정을 수행하였으며 이를 위하여 인증 노드에서는 각 노드들에 대한 신뢰도 값을 라우팅 신뢰 테이블에 관리하였다. 그리고 평균 경로 신뢰값을 이용하여 선택된 여러 경로들 중에서 가장 높은 값을 갖는 경로를 선택하여 데이터 전송의 안전성을 향상시켰다. 본 논문에서 제안한 기법의 성능 평가를 위하여 CBSR, SEED 기법과 종단간 전송 지연 시간, 전송 성공 비율, 제어 패킷을 비교 실험하였으며, 실험을 통해 우수한 성능을 확인할 수 있었다.

## 참고문헌

[1] P. Papadimitratos and Z. J. Haas, “Secure Message Transmission in Mobile Ad Hoc Networks,” Elsevier Ad Hoc Networks J., Elsevier, vol. 1, no. 1, 2003, pp. 193-209.

[2] Y. C. Hu, A. Perrig, and D. B. Johnson, “Packet Leashes: A Defense against Wormhole Attacks in Wireless Ad Hoc Networks,” Proc. 22nd Ann. Joint Conf. IEEE Computer and Communications Societies (INFOCOM 2003), IEEE Press, 2003, pp. 1976-1986.

[3] S. Marti, T. J. Giuli, K. Lai and M. Baker, “Mitigating Routing Misbehavior in Mobile Ad Hoc Networks,” Proc. 6th Annual ACM/ IEEE Int’l. Conf. Mobile Computing and Networking, 2000, pp. 255-265.

[4] A. A. Pirzada, C. Mcdonald, and A. Datta, “Performance Comparison of trust-based Reactive Routing Protocols,” IEEE Trans. Mobile Computing, vol. 5, Issue 6, June 2006, pp. 695-710.

[5] P. Papadimitratos and Z. J. Haas, “Secure Routing: Secure Data Transmission in Mobile Ad Hoc Networks,” Proc. ACM Wksp. Wireless Security 2003, Sept. 2003, pp. 41-50.

[6] 양환석, 양정모, “MANET에서 효율적 역추적을 위한 경로관리에 관한 연구,” 디지털산업정보학회 논문지, 제7권, 제4호, 2011, pp. 31-37.

[7] P. A. R Kumar, S. Selvakumar, “Distribute Denail-of-Service (DDoS) Threat in Collaborative Environment - A survey of DDoS Attack Tools and Traceback Mechanism” IEEE International Advance Computing Conference (IACC 2009), March 2009, pp. 1275-1280.

[8] M. N. Iqbal, J. A. Khan, F. Umer, N. Javaid, I. Haq, M. Shakir, “Security Enhancement of Pro-active Protocols in Mobile Ad-hoc

Networks," 2013.

[9] S. A. Mahdi, M. Othman, H. Ibrahim, J. M. Desa and J. Sulaiman" Protocols For Secure Routing And Transmission In Mobile Ad Hoc Network: A Review" Journal of Computer Science, vol. 9, no. 5, 2013, pp. 607-619.

[10] 왕종수, 서두옥, "극단적인 네트워크 환경을 위한 효율적인 라우팅 알고리즘," 디지털산업정보학회 논문지, 제8권, 제1호, 2012, pp. 171-179.

■ 저자소개 ■

양 환 석
Yang Hwanseok

2011년 9월~현재
중부대학교 정보보호학과 조교수
2006년 2월~2011년 2월
호원대학교 사이버수사경찰학과
연구교수
2005년 2월 조선대학교 전산통계학과(이학박사)
1998년 2월 조선대학교 전산통계학과(이학석사)

관심분야 : 정보보호, 침입탐지시스템, MANET
E-mail : yanghs@joongbu.ac.kr

논문접수일: 2015년 8월 18일
수 정 일: 2015년 8월 28일
게재확정일: 2015년 9월 4일