모바일 애드 혹 네트워크(Mobile Ad-hoc Networks)에서 홉 카운트 변조 공격으로부터의 라우팅 테이블 보안

Routing Table Protection From an Attack to Falsify Hop Count in Mobile Ad-hoc Networks

김진희, 이재현, 권경희
단국대학교 전자계산학과 컴퓨터과학

Jin-Hee Kim(whitej2@dankook.ac.kr), Jae-Hyun Lee(wogusking@dankook.ac.kr),
Kyung-Hee Kwon(khkwon@dankook.ac.kr)

요약

모바일 애드 혹 네트워크 (Mobile Ad-hoc Networks)에서 AODV 라우팅 알고리즘은 소스 노드에서 목적지 노드까지의 경로를 확보하기 위하여 RREQ(Route Request) 패킷을 전체 네트워크에 브로드캐스트 한다. 이 과정에서 브로드캐스트 되는 RREQ 패킷을 악의적인 목적을 가진 노드들이 수신했을 경우 RREQ 패킷의 필드를 변조하는 공격이 가능하게 된다. 본 논문에서는 RREQ 패킷의 홉 카운트(Hop Count) 필드를 변조함으로써 라우팅 테이블에 대한 공격 시도를 차단하는 방법을 제안한다. 소스 노드에서 목적지 노드까지 경로 설정 시, 홉 카운트 대신 지연(Delay)을 이용하여 최단 경로를 결정하며, 이로 인해 홉 카운트 변조를 통한 공격으로부터 라우팅 테이블을 보호한다. 성능 평가를 위한 시뮬레이션은 NS-2를 이용하였으며, 홉 카운트 변조를 통한 공격이 정상 트래픽에 미치는 영향을 분석하였고, 제안하는 매커니즘을 통해 안전한 데이터의 전송을 확인하였다.

■ 중심어 : | 애드 혹 | 보안 | 성능 | 라우팅 알고리즘 |

Abstract

The AODV routing algorithm in a mobile ad-hoc networks broadcasts RREQ packet to find a route from a source to a destination. An attacker node may intercept a RREQ packet and attack by falsifying a field in that packet. In this paper, we propose a simply modified method which can protect a routing table from an attack to falsify the hop count field in the RREQ packet. When establishing a connection between a source and a destination, we update routing table of each node on the connection based on minimum delay instead of minimum hop count. By doing this, we can protect routing table from an attack to falsify a hop count Our simulation is implemented in Network Simulator(NS-2). We analyze how an attacker affects the mobile ad-hoc networks. The result of the simulation shows that the proposed mechanism transfers a data securely.

■ keyword : | Ad-hoc | AODV | Security | Performance |

접수번호 : #080527-005
접수일자 : 2008년 05월 27일
심사완료일 : 2008년 06월 23일
교신저자 : 김진희, e-mail : whitej2@dankook.ac.kr

I. 서 론

기존의 인프라를 요구하지 않고 이동 노드로만 구성된 애드 혹 네트워크(Ad-hoc Networks)의 등장과 , 이동하면서 언제 어디서나 원하는 시간에 통신할 수 있는 이동 통신 기술의 발달은 우리의 삶에 중요한 요소로서 많은 변화를 가져왔다. 그러나 통신망의 변화와 기술의 발달에도 불구하고 악의적인 사용자가 데이터를 취득하는 보안상의 문제는 아직도 해결해야 하는 심각한 문제이다. 특히, 위치 변화가 잦은 이동 노드로 구성된 애드 혹 네트워크에서 전체 네트워크를 관리 할 수 있는 관리 노드의 부재는 보안에 치명적이라 할 수 있다. 애드 혹 네트워크에서 각각의 노드는 인접 노드들로부터 받은 라우팅 정보를 가지고 효율적인 라우팅을 해야 한다. 즉, 라우터 역할을 해야 하며 애드 혹 네트워크에 존재하는 각각의 모든 노드들이 전체 네트워크의 신뢰적인 동작에 책임을 가져야 함을 의미한다.

기존의 대부분의 라우팅 프로토콜은 자체 보안성을 갖고 설계되지 않았고 이러한 문제점은 라우팅 알고리즘의 암호화와 관련하여 다각적인 연구를 진행하게 했다[3][6-13]. 그러나 잦은 네트워크 위상 변화에 많은 자원을 소비하고 이러한 변화를 반영하는 데 많은 시간을 소요하는 애드 혹 네트워크에서 알고리즘의 암호화는 적합하지 않다. 애드 혹 네트워크에서 노드들은 좁은 대역폭의 무선 링크로 연결되어 있으면서 과도한 플러딩(Flooding) 사용과 주기적인 메시지를 최소화하여 배터리를 절약해야 한다. 따라서 알고리즘의 암호화는 자원소비와 시간소요 측면에서 효율적이지 못하다. 애드 혹 네트워크는 라우팅과 관련하여 여러 가지 취약점[3][5]을 갖고 있고 암호화를 통한 보안이 아닌 다른 해법이 제시되어야 할 것이다.

본 논문은 모바일 애드 혹 네트워크에서 AODV 라우팅 프로토콜 사용 시 발생 가능한 보안상의 공격에서 안전한 데이터의 전송과 성능 향상을 위한 연구이다.

라우팅 프로토콜에서 최단 경로 설정 시 이용되는 홉 카운트(Hop Count)는 수신 노드에서 시퀀스 넘버가 같은 패킷이 여러 경로를 통해 중복 수신될 경우 홉 카운트가 작은 것이 선택되게 되어 있다. 공격자는 이러한 홉 카운트를 변조하는 방법으로 자신의 노드를 경유하는 경로가 최단경로인 것처럼 믿게 함으로써 소스 노드와 목적지 노드 사이의 모든 데이터를 취득하게 된다. 이러한 홉 카운트를 이용한 공격의 무효화를 통해 다양한 보안 위협 요소를 감소시키고자 하는 것이 본 연구의 목표이다.

II. 관련 연구

AODV에서 라우팅 알고리즘은 동작 방식에 따라 크게 두 가지로 나눌 수 있다.

네트워크 노드들 간에 주기적으로 토폴로지에 대한 정보를 주고받아 라우팅을 수행하는 Proactive 프로토콜과 필요할 때에만 Request/Reply 방식으로 라우팅을 수행하는 Reactive 방식으로 분류 할 수 있다[4][5].

Proactive 방식은 실제 데이터 전송이 없을 경우에도 주기적으로 네트워크 토폴로지 정보를 상호 교환한다. 이러한 주기적인 정보교환은 오버헤드가 크다는 단점을 갖는 반면 경로 설정할 때 신속하게 할 수 있다는 장점이 있다. Reactive 방법은 반드시 교환하고자 하는 데이터가 있을 경우에만 토폴로지 정보를 교환하고 이후에 경로가 설정되면 데이터를 전송하는 방식으로 경로 설정을 하는데 시간이 걸리지만 불필요한 정보 교환이 없기 때문에 트래픽 감소로 자원을 덜 소비한다는 장점이 있다[4]. 또한 이러한 장점은 네트워크의 크기가 커질수록 , 이동성이 큰 노드들 간의 통신일수록 적합한 통신 방법이다.

1. AODV 라우팅 프로토콜

Reactive 라우팅 프로토콜 방식 중 대표적인 것으로 AODV가 있다[2][3][5].

이 라우팅 프로토콜 방식은 경로 설정과 유지 관리를 위해 RREQ(Route Request), RREP(Route Reply), RREP-ACK(Route Reply Acknowledge), RERR(Route Error)의 4개의 제어 패킷(Control Packet)이 필요하다.

RREQ 패킷은 데이터를 전송할 노드가 자신의 라우팅 테이블에 저장된 경로 중 해당 목적지까지의 경로가

없거나, 유효하지 않은 경로를 가지고 있을 경우에 경로 설정을 위해 전송하는 컨트롤 패킷이다.

RREP 패킷은 RREQ 패킷을 수신한 노드가 목적지 노드까지의 유효한 경로를 가지고 있거나, 수신 노드가 해당 목적지 노드일 경우 RREQ 패킷에 대한 응답으로 전송되는 것이다.

RREP-ACK 패킷은 RREQ 패킷을 보낸 소스 노드가 RREP 패킷을 수신한 후 이에 대한 응답으로 사용하는 것이다. RERR 패킷은 노드의 이동이나 고장으로 인하여 경로가 단절되는 상황이 발생했을 경우 경로 단절에 대한 정보를 알리기 위한 패킷이다.

2. 연구 동향

모바일 애드 혹 네트워크에서 라우팅 프로토콜은 많은 보안상의 위협 요소에 노출되어 있으며 이러한 요소는 공격자로 하여금 다양한 형태의 방법으로 공격을 할 수 있게 한다[3][5].

라우팅 정보를 변경함으로써 모든 패킷이 공격자를 경유하게 하는 싱크 홀(Sinkhole) 공격과 RERR 패킷을 전송하여 경로 탐색 과정을 다시 시작하게 함으로써 필요한 부하를 조장하여 네트워크 대역폭을 낭비하게 하는 공격, 그리고 RREP 패킷을 조작하여 데이터가 목적지에 전송할 수 없도록 하는 공격 등이 있다. 또한 공격 노드가 특정노드에게 지속적으로 서비스를 요청하여 유휴상태나 절전 모드로 진입하는 것을 방해하여 배터리 소모를 가속화하는 하는 경우, 잘못된 라우팅 정보를 생성함으로써 패킷 중복 및 루프(Loop)등을 발생시키는 형태의 공격이 있다.

이러한 다양한 공격에 대한 보안으로 인증 및 암호화, 키 설정 및 분배 그리고 침입 탐지 등의 연구가 진행되고 있다[6-13].

DSDV 기반으로 일 방향 해쉬 함수 체인을 이용한 연구[10], 안전한 경로를 제공하기 위한 방법으로 인증서를 이용하여 소스에서 목적지 노드 사이의 중간 노드의 각 홉에서 인증을 하는 ARAN(Authentication routing for ad hoc networks) 프로토콜[11], DSR에 기초한 방식으로 라우팅 메시지 인증을 위하여 TESLA 프로토콜과 전자서명 그리고 MAC(Message Authentication Code)을 이용한 연구는 소스 노드와 목적지 노드사이의 공유키를 이용하여 RREQ 패킷의 MAC값을 포함시켜 전송하는 방법으로 목적지 노드가 RREQ 패킷을 인증하게 한다[12]. 또한 라우팅 메시지를 인증하기 위하여 서명을, 소스 노드와 목적지 노드 사이의 중간 노드들을 인증하기 위하여 해쉬 체인을 이용한 방법으로 중간 노드만큼 해쉬 값을 취하고 해쉬 체인은 홉 카운트 값을 인증하는 연구가 있다[13]. 그러나 위 대부분의 연구에서 제시되는 보안에 대한 해법이 전자 서명과 해시 체인을 이용하는 기법으로 이러한 방법은 오버 헤드가 크다는 단점을 가지고 있다. 따라서 본 논문에서는 오버헤드를 최소화 하는 방법으로 보안에 대한 해결책에 접근하려 한다.

III. 제안하는 메커니즘

본 논문에서는 모바일 애드 혹 네트워크에서 AODV 라우팅 프로토콜 사용 시 발생 가능한 보안상의 공격에서 안전한 데이터의 전송과 성능 향상을 위한 메커니즘을 제안한다.

라우팅 프로토콜에서 최신, 최단 경로 설정 시 이용되는 것으로 RREQ 패킷안의 시퀀스 넘버와 홉 카운트 필드가 있다.

RREQ 패킷을 받은 노드는 소스 아이피 어드레스와 RREQ ID가 동일한 패킷인지 확인하여 동일하면 이미 수신한 패킷으로 간주하여 즉시 폐기하고 그렇지 않을 경우 라우팅 테이블에서 목적지 아이피 어드레스를 확인한다. 자신이 목적지 노드가 아닌 경우 라우팅 테이블에 해당 노드까지 유효한 경로가 있는지 검색하고 경로가 없으면 이웃 노드들에게 자신이 받은 RREQ 패킷의 홉 카운트 필드 값을 1 증가시켜 브로드캐스트 한다. 목적지 노드까지의 경로가 있으면 RREQ 패킷안의 소스 시퀀스 넘버와 라우팅 테이블안의 소스 시퀀스 넘버를 비교한다. 이 과정에서 최신, 최단 경로 설정이 이루어진다. RREQ 패킷안의 시퀀스 넘버 값이 크면 최신 경로로, 시퀀스 넘버가 같은 경우 홉 카운트가 작은 경로가 최단 경로로 라우팅 테이블이 업데이트(Update)

된다.

RREQ 패킷을 수신한 각 노드들은 목적지 노드에서 소스 노드까지의 역 경로(Reverse Path)를 형성하게 되고 이 경로를 이용하여 목적지 노드는 RREP 패킷을 소스 노드로 유니 캐스팅 할 수 있게 된다. 이러한 과정에서 브로드캐스트 되는 RREQ 패킷을 악의적인 목적을 가진 노드들이 수신했을 경우 RREQ 패킷안의 특정 필드의 변조를 통한 공격이 가능하게 된다. 시퀀스 넘버는 크게, 홉 카운트는 작게 하여 라우팅 테이블을 업데이트 시킴으로써 공격 노드를 경유하는 것이 마치 최단 경로가 되는 것처럼 믿게 만드는 것이다.

본 논문은 이러한 RREQ 패킷안의 특정 필드를 변조하는 공격의 유형을 최소화시키기 위한 것이다. 중간 혹은 목적지 노드에서 시퀀스 넘버가 같은 패킷을 중복 수신하였을 경우 홉 카운트가 작은 것을 최단 경로로 설정하던 기존의 방법에서 먼저 RREQ 패킷이 도착한 경로를 최단 경로로 간주하여 경로를 설정하게 하는 메커니즘을 제안한다.

이러한 메커니즘의 연구는 네트워크 환경에서 패킷 전송 시 걸리는 지연(Delay)은 전송거리에 비례[1]하므로 전송 거리가 짧으면 패킷 또한 목적지 노드에 먼저 도착한다는 것에서 출발하였다.

패킷 전송 시 걸리는 지연은 보통 전송지연 또는 소요시간으로 설명된다.

$$\text{지연} = \text{전파지연} + \text{전송지연} + \text{큐잉지연} \quad (1)$$

식 (1)에서 전파지연(Propagation Delay)은 두 라우터간의 거리를 전파속도로 나눈 것으로 거리상 지연을 의미하며 전송지연(Transmission Delay)은 전송량을 대역폭으로 나눈 것으로 서로 다른 대역폭을 갖는 링크들로 구성된 네트워크 환경이라면 전송지연은 지연에 큰 영향을 미치지만 애드 혹과 같은 네트워크 환경에서 같은 대역폭을 갖는 링크들로 구성되어 있다면 전송지연은 문제가 되지 않는다. 큐잉지연(Queuing Delay)은 패킷이 전송되기 전에 라우터의 큐에서 링크에 전송되기를 기다리는 시간이다. 이 때 만약 큐가 비어 있고 전송 되는 패킷이 없다면 큐잉지연은 '0'이 되며 반면에 네트워크에 트래픽이 일시적으로 몰리면서 많은 패킷들이 큐에서 전송되기를 기다리고 있다면 큐잉지연은 길어질 것이다. 따라서 네트워크의 트래픽을 예측할 수 없는 상황에서 큐잉지연이 균일하다고 가정한다면 지연은 단지 전파지연에만 영향을 받는다.

애드 혹 네트워크에서 전송거리는 홉 카운트로 설명한다. 따라서 큐잉지연이 균일하다고 가정한다면 네트워크상에서 패킷 지연은 홉 카운트로 설명할 수 있고 홉 카운트가 작은 것이 전송 거리가 짧으므로 목적지 노드에 먼저 도착하게 되는 것이다. 각각의 노드에서 서로 다른 경로로 시퀀스 넘버가 같은 중복 패킷을 수신하였을 경우 RREQ 패킷이 먼저 도착한 경로 즉, 최소 지연 값을 갖는 경로를 최단 경로로 간주하여 이 후에 도착한 중복 패킷은 폐기 시킨다는 것이 본 논문의 메커니즘이다. 이러한 메커니즘은 라우팅 업데이트 시 홉 카운트를 이용한 경로 설정을 불필요하게하며 공격자에 의한 홉 카운트 변조 공격을 무의미 하게 한다.

표 1. 기존 알고리즘

```
if ((RREQ의 시퀀스 넘버가
     라우팅테이블의 시퀀스 넘버보다 크거나)
    (RREQ의 시퀀스넘버와
     라우팅테이블의 시퀀스 넘버가 같고
     RREQ의 홉카운트가
     라우팅테이블의 홉 카운트보다 작으면))
    {
      라우팅테이블 정보 업데이트
              ;
              :
    }
```

표 2. 제안하는 알고리즘

```
if (RREQ의 시퀀스 넘버가
      라우팅테이블의 시퀀스 넘버보다 크면)
     {
   라우팅테이블 정보 업데이트
              ;
              :
    }
```

[표 1]과 [표 2]는 중간노드나 목적지 노드에서

RREQ 패킷을 수신했을 경우 라우팅 테이블을 업데이트하는 부분이다. 음영으로 처리된 부분이 기존 알고리즘과 제안하는 매커니즘에서 다른 부분으로 홉 카운트를 이용한 라우팅 업데이트 부분을 제거 시킨 것이다.

Ⅳ. 시뮬레이션

1. 시뮬레이션 환경과 프로토콜

시뮬레이션은 네트워크 시뮬레이터인 NS-2를 이용하였으며 다음과 같은 가정 하에 연구를 진행하였다.

첫째, TCP 타입은 TCP Reno 이다. 이는 TCP의 여러 가지 구현 중 대표적이며 가장 많이 이용되는 것이 Reno이기 때문이다.

둘째, 패킷 송수신 방법은 반이중(half-duplex) 으로 가정하였다.

셋째, 시뮬레이션 공간은 670 * 670 으로 전송 범위는 250m로 하였으며 노드의 개수는 50개로 랜덤하게 위치시켰으며 트래픽은 CBR(Constant bit rate)과 TCP 사용하였다.

넷째, 시뮬레이션 과정 중 RREQ 패킷을 수신한 노드 중 패킷내의 시퀀스 넘버와 라우팅 테이블의 시퀀스 넘버가 같은 노드 하나를 선택해서 공격자 노드(노드 2, 노드 15)로 한다

거리에 따른 신호 세기 감소는 Free space 모델과 Two-ray Ground 모델로 구성되었다. Free space 모델은 MH가 100m 이내에 위치하면 거리에 따른 신호 세기는 1/r2 만큼 감소하며 250m 이내에 위치하면 1/r4 만큼 감소한다. 물리계층의 802.11에서 전송방식은 DSSS(Direct Sequence Spread Spectrum)이며 채널 접근방식은 CSMA/CA를 사용한다. [표 3]의 시뮬레이션과 관련된 파라미터는 NS-2에서 기본으로 설정된 것을 그대로 적용하였으며 시뮬레이션 시간은 50초간 지속된다.

[표 3]의 시뮬레이션 모델을 적용하여 설계한 네트워크 토폴로지가 [그림 1]이다. 50개의 모바일 노드를 랜덤하게 위치시켜 소스 노드를 8번으로 목적지 노드를 2번으로 설정하여 트래픽을 발생 시켰다. [그림 1]에서 'A영역'과 'B영역'이란 소스 노드 외에 다른 노드에서의 트래픽이 발생할 경우 트래픽이 발생하는 노드 위치를 설명하기 위한 표기이다. 소스 노드와 목적지 노드를 두고 왼쪽 부분을 'A영역'으로 오른쪽 부분을 'B영역'으로 설명한다. 소스 노드에서 목적지 노드로의 경로 설정 과정에서 큐잉지연이 미치는 영향을 분석하기 위하여 소스 노드 외에 'A영역'과 'B영역'의 다른 노드에서도 트래픽을 발생시켜 큐잉지연을 유도하였다. '공격자 노드'란 시뮬레이션 과정 중에 중간 혹은 목적지 노드에서 RREQ 패킷을 수신했을 경우 수신한 패킷 내 시퀀스 넘버가 라우팅 테이블의 시퀀스 넘버와 같을 경우의 수신노드를 의미하는 것으로 공격 가능한 노드를 의미한다. 이러한 노드들 중 하나가 공격자 노드가 되어 수신한 RREQ 패킷의 홉 카운트를 변조하여 브로드캐스트 하게 하였다. 소스 노드와 목적지 노드의 연결 경로 상에 공격자 노드를 위치 시켜 패킷이 공격자 노드를 경유하게끔 하기 위함이다.

표 3. 시뮬레이션 모델

트래픽 타입		CBR,TCP	
물리계층	Propagation 모델	Free space (r:거리)	$\frac{1}{r^2}$ (100m)
		Two-ray Ground reflection	$\frac{1}{r^4}$ (250m)
	MAC	802.11 DSSS (Direct Sequence Spread Spectrum)	
	채널 접근방식	CSMA/CA	
토폴로지		670 * 670 grid(노드수 50개)	

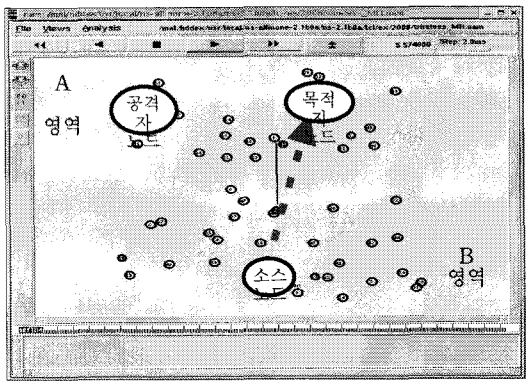


그림 1. 시뮬레이션을 위한 네트워크 토폴로지

시뮬레이션은 네 가지 방법으로 진행하였다.

첫 번째 방법은 소스 노드에서 목적지 노드로 발생하는 트래픽 외에 다른 노드에서의 트래픽 발생은 전혀 없게 하였다. 경로 설정 이루어지는 과정에서 다른 노드로부터 발생하는 트래픽의 영향을 받지 않게 위함이다.

두 번째 방법은 소스 노드에서 목적지 노드로 가는 트래픽 외에 A영역의 다른 노드에서 목적지 노드로 많은 트래픽을 발생시켰다. A영역에서의 혼잡을 만들기 위함이며 소스 노드 외에 주변 다른 노드로부터의 트래픽 발생으로 A영역 내에서 큐잉지연을 유도하였다.

세 번째 방법은 두 번째 방법과 같은 방법으로 B 영역에서 많은 트래픽을 발생하여 B영역에서의 큐잉지연을 유도하였다.

두 번째와 세 번째 방법에서 큐잉지연은 경로가 설정되는 순간에서 데이터 전송이 있는 동안 지속된다.

네 번째 방법은 B영역에서 일시적인 큐잉지연을 유도하였다. 경로 설정이 이루어지는 순간에만 트래픽을 발생시키고 경로 설정 이후 데이터 전송이 있는 동안에는 큐잉지연을 없애기 위해 B영역에서 트래픽 발생을 정지시키는 방법으로 시뮬레이션 하였다.

2. 시뮬레이션 결과

성능 평가는 위 네 가지 방법으로 시뮬레이션 하여 각각 소스 노드와 목적지 노드에서 송신량과 수신량을 체크해 보았다. 제안하는 메커니즘 적용 전과 후에 그리고 공격자 노드에 의해 공격을 당했을 경우에 송·수신량을 비교하였다.

[그림 2]와 [그림 4][그림 6][그림 8]은 소스 노드에서의 패킷 송신량을 의미한다. 기존 알고리즘을 적용했을 경우와 제안하는 메커니즘을 적용했을 경우 소스 노드에서의 패킷 송신량을 비교한 그림으로 그래프의 '기존'이 기존 알고리즘을, '제안' 은 제안한 메커니즘을 적용했을 경우를 의미한다.

[그림 3]과 [그림 5][그림 7][그림 9]는 목적지 노드와 공격자 노드에서의 패킷 수신량을 의미한다. 기존이란 '기존' 알고리즘을 적용했을 경우 즉 공격이 들어가기 전을 의미하며 '공격'은 기존 알고리즘에서 RREQ 패킷의 홉 카운트 변조 공격이 가해졌을 경우를 의미한다. '제안'은 제안하는 메커니즘에 공격이 가해졌을 경우를 의미하는 것으로 그래프의 상단선이 목적지 노드인 2번 노드에서의 패킷 수신량을 의미하고 그래프의 하단선이 공격자 노드인 7번 또는 15번에서의 패킷 수신량을 의미한다.

[그림 1]의 토폴로지 환경에서 최단 경로는 B영역을 경유한다.

[그림 2]와 [그림 3]은 첫 번째 방법으로 시뮬레이션 한 결과이다. 소스 노드인 8번에서 목적지 노드인 2번으로의 트래픽 발생 외에 다른 노드에서의 트래픽 발생이 없는 경우이다. 즉 네트워크상에 큐잉지연이 전혀 발생하지 않는 경우이다.

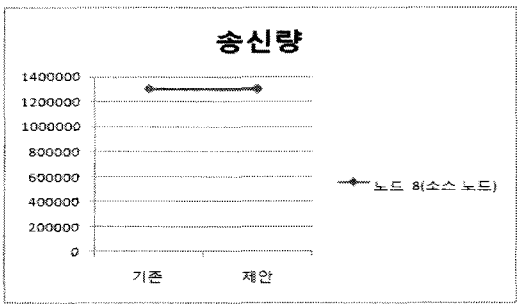


그림 2. 큐잉지연이 없는 경우 소스 노드에서의 패킷 송신량

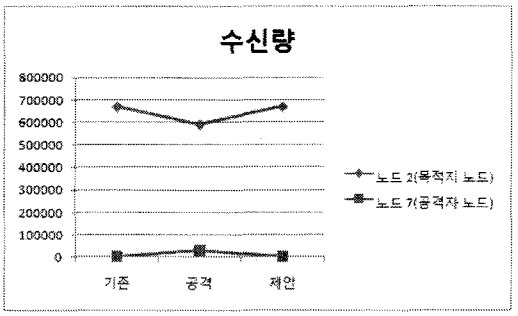


그림 3. 큐잉지연이 없는 경우 목적지 노드와 공격자 노드에서의 패킷 수신량

따라서 소스 노드와 목적지 노드 사이에서 경로 설정 시 다른 노드의 트래픽 영향을 전혀 받지 않으므로 소스 노드에서 패킷 송신량과 목적지 노드에서 패킷 수신량이 기존 알고리즘과 제안하는 메커니즘을 적용했을

경우 같은 것을 확인 할 수 있다. 목적지 노드에서 RREQ 패킷이 먼저 도착한 경로는 곧 홉 카운트가 작은 경로가 되며 따라서 소스 노드와 목적지 노드 사이에서 패킷량에 전혀 변화가 없는 것이다. 수신량을 나타내는 그래프 3에서 하단은 공격자 노드 7번이 수신하는 패킷량을 나타낸 것이다. 기존 알고리즘에서 노드 7번은 실제 최단 경로 상에 놓이지 않으며 공격 노드가 되기 전까지 노드 7번을 경유하는 패킷은 전혀 없다. 그러나 노드 7번이 공격자 노드가 되면서 즉 노드 7번이 RREQ 패킷의 홉 카운트 변조를 통해 자신을 경유하는 경로가 최단 경로 인 것처럼 믿게 하면서 7번을 경유하는 패킷이 생기는 것이다.

제안하는 메커니즘에서는 홉 카운트를 이용한 공격이 성공 되지 않으면서 공격자 노드를 경유하는 패킷이 전혀 없는 것을 확인 할 수 있다.

최단 경로 설정 시 홉 카운트가 작은 경로가 최단 경로로 설정되는 것과 홉 카운트를 고려하지 않고 최소 지연 값을 갖는 경로를 최단 경로로 간주했을 경우 결과가 같게 나타난 것이다.

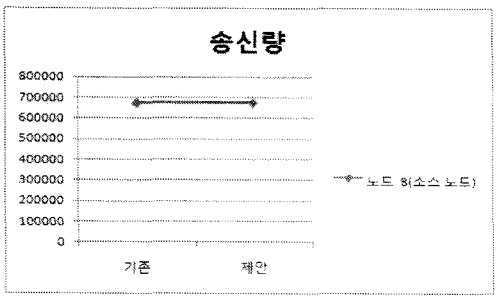


그림 4. A영역에서 지속적인 큐잉지연 발생 시 소스 노드에서의 패킷 송신량

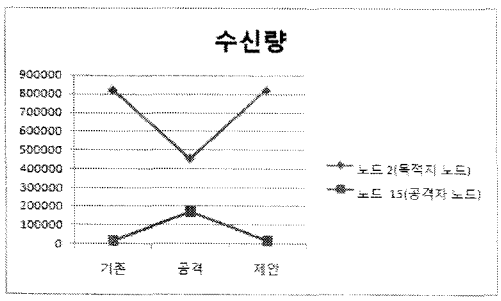


그림 5. A영역에서 지속적인 큐잉지연 발생 시 목적지 노드와 공격자 노드에서의 패킷 수신량

[그림 4]와 [그림 5]는 두 번째 방법으로 시뮬레이션 한 결과이다. 그림 제목에서 '지속적인 큐잉지연'이란 경로가 설정이 이루어지는 순간에서부터 데이터 전송이 있는 동안 계속된 큐잉지연을 의미한다. [그림 1]에서 소스노드에서 브로드캐스트 한 RREQ 패킷은 A영역에서의 많은 트래픽으로 경로 설정 시와 데이터 전송이 있는 동안 큐잉지연이 유발되면서 큐잉지연도 없고 홉 카운트도 작은 B영역의 경로를 통해 먼저 도착하게 된다. 따라서 시뮬레이션 방법 1을 통해 나온 결과와 방법 2를 통해 나온 결과가 같은 것을 확인 할 수 있다. 즉 기존 알고리즘과 제안하는 메커니즘의 소스 노드에서 패킷 송신량과 목적지 노드에서의 패킷 수신량이 같음을 확인하였다.

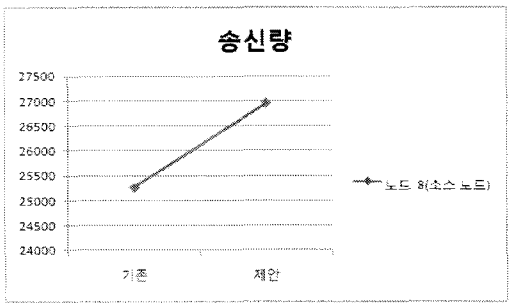


그림 6. B영역에서 지속적인 큐잉지연 발생 시 소스 노드에서의 패킷 송신량

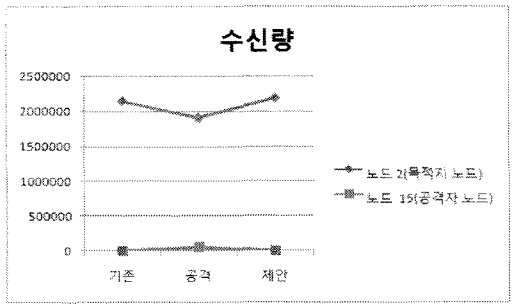


그림 7. B영역에서 지속적인 큐잉지연 발생 시 목적지 노드와 공격자 노드에서의 패킷 수신량

[그림 6]과 [그림 7]은 세 번째 방법으로 시뮬레이션 한 결과이다. 실제 최단 경로는 홉 카운트가 작은 B영역을 통해 경로 설정이 이루어져야 한다. 그러나 B영역

에서 트래픽이 많이 발생할 경우에는 큐잉지연으로 B 영역의 실제 최단 경로를 통한 패킷 전송이 오히려 성능 저하의 원인이 된다. 따라서 B영역에서 트래픽 과부하시에는 홉 카운트를 이용한 경로 설정보다는 우회경로가 되더라도 RREQ 패킷을 먼저 전송시켜주는, 최소 지연 값을 갖는 경로를 데이터 송·수신 경로로 설정하는 것이 성능을 향상 시킬 수 있는 방법이 된다. 거리가 짧더라도 트래픽 과부하로 인해 큐잉지연이 발생한다면 우회 경로로 돌아서 가는 것이 오히려 빠른 길이 될 수 있는 것이다. 실제로 제안하는 메커니즘을 이용했을 경우 소스노드에서 더 많은 송신량을 목적지 노드에서 더 많은 패킷 수신량을 확인하였다.

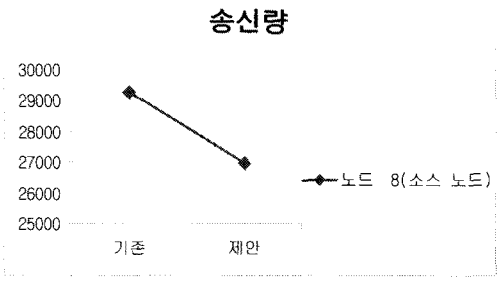


그림 8. B영역에서 일시적인 큐잉지연 발생시 소스 노드에서의 패킷 송신량

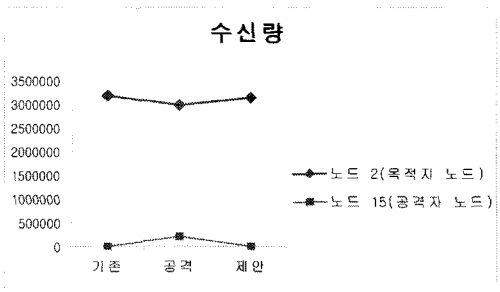


그림 9. B영역에서 일시적인 큐잉지연 발생시 목적지 노드와 공격자 노드에서의 패킷 송신량

라우팅 테이블에서 경로 설정이 잘못 되면 다시 경로 설정이 이루어지기 전까지 실제 최단 경로가 아닌 다른 경로를 통해 지속적으로 전송될 수 있다. [그림 8]과 [그림 9]에서 '일시적인 큐잉지연'이란 경로 설정 순간에만 큐잉지연이 발생하고 경로 설정이 끝난 후 즉, 데이터 전송이 있는 동안에는 큐잉지연이 해제 된 경우를 의미한다. 제안하는 메커니즘 적용 시 패킷 송신량과 수신량이 오히려 기존 알고리즘을 적용했을 경우보다 감소한 것을 확인 할 수 있다. 제안하는 메커니즘을 적용했을 경우 B영역에서의 큐잉지연으로 인해 먼저 RREQ을 전송한 A영역이 최단 경로로 설정되면서 B영역에서 큐잉지연이 해제된 이후에도 데이터는 여전히 A영역을 통해서 전송된다. 따라서 제안하는 알고리즘보다 기존 알고리즘을 적용했을 경우 좀 더 많은 패킷 송신량과 수신량이 확인 된 것이다. 경로 설정 순간에만 큐잉지연이 발생할 경우에는 제안하는 메커니즘이 적합하지 않은 경우로 해석 된다.

V. 결 론

이동성을 갖는 애드 혹 네트워크와 같은 환경에서 라우팅 프로토콜은 대부분 보안에 취약하며 다양한 방법으로 공격자에 의해 공격 당 할 수 있다.

본 논문에서는 다양한 공격 형태 중 RREQ 패킷의 홉 카운트 필드를 변조하는 공격을 무효화 시키는 방법을 제안하였다.

시뮬레이션 결과 네트워크에 큐잉지연이 없는 상황에서는 기존 라우팅 알고리즘과 제안하는 메커니즘을 적용했을 경우 소스 노드에서의 송신량과 목적지 노드에서의 수신량의 변화가 없었으며, 지속적인 큐잉지연의 발생할 경우에는 제안하는 메커니즘이 일시적인 큐잉지연이 발생할 경우에는 기존 알고리즘이 적합한 경우로 확인되었다.

기존 알고리즘은 홉 카운트가 작은 경로가 최단 경로가 된다. 그리고 경로가 짧다는 것은 큐잉지연이 없을 경우 RREQ 패킷이 목적지 노드에 먼저 도착할 수 있다는 것을 의미한다. 이러한 사실은 큐잉지연이 없을 경우라면 경로 설정시 홉 카운트 대신 최소 지연 값을 갖는 경로를 최단 경로로 설정해도 송·수신되는 패킷량의 결과가 다르지 않다는 것을 의미한다. 기존의 홉 카운트를 이용한 경로 설정은 오히려 악의적인 노드에

의해서 또 하나의 공격 요소가 될 뿐이고 우리는 제안하는 메커니즘을 통해 이러한 공격 요소를 하나 제거하였다.

향후 연과 과제로는 큐잉지연이 발생할 수 있는 좀 더 다양한 환경을 가지고 시뮬레이션 해야 할 것이며, 본 논문에서는 고려되지 않은 사항으로 RREQ 패킷안의 필드 중 홉 카운트 변조를 통한 공격 외에 시퀀스 넘버의 변조를 통한 공격에 대한 보안 방법을 찾는 것이다.

참 고 문 헌

[1] L. P. Larry and S. D. Bruce, Compuer Networks "Computer Networks : A Systems Approach," Morgan Kaufmann, 1999.

[2] 서현곤, 김기형, "애드 혹 네트워크 네트워크에서 AODV 에 기반한 효율적인 경로 복구 기법", KNOM Review, 제6권, 제1호, pp.1-8, 2003(6).

[3] 이명진, 김미희, 채기준, 김호원, "센서 네트워크에서 AODV 라우팅 정보 변조공격에 대한 분석", 정보처리학회 논문지 C, 제14-C권, 제3호, pp.0229-0238, 2007.

[4] 김종천, 김영용, "AD Hoc 통신망 프로토콜 개발 동향", Telecommunications Reviw, Vol.12, No. 3, 2002.

[5] 김한식, 박현희, 강병석, 백상헌, 강철희, "모바일 애드혹 네트워크에서 안전한 라우팅을 위한 경로 조사 기법", 한국통신학회 '07 하계 학술 발표 논문집, 2007.

[6] M. G. Zapata and N. Asokan, "Security ad hoc routing protocols," ACM Wise2002, Vol.10, No.1, pp.1-10, 2002(10).

[7] S. J. Lee, B. H. Han, and M. H, Shin, "Robust routing in wireless ad hoc networks," in proc. ICCP2002, Vol.6, pp.73-78, 2002(8).

[8] M. G. Zapata, "Secure Ad hoc On-Demand Distance Vector SAODV) outing," IEEE Internetdraft, draft-guerrero-manet-saodv-06.txt>, 2006(9).

[9] K. Sanziri, B. Dahill, B. N. Levine, and E. M. B. Royer, "A secure routing protocol for ad hoc networks," in proc. ICNP2002, Vol.10, No.10, pp.78-87, 2002(11).

[10] Y. C. Hu, D. B. Johnson, and A. Perrig, "Sead: Secure efficient distance vector routing in mobile wireless Ad Hoc networks," Proc. of Fourth IEEE Workshop on Mobile Computing Systems and Applications (WMCSA '02), pp.3-13, 2002.

[11] K. Sanzgiri, "A Secure Routing Protocol for Ad Honc Networks," ICNP IEEE Press, 2002.

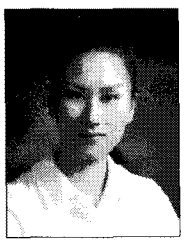
[12] Y. C. Hu, A. Perrig, and D. Johnson, "Ariadne A secure on demand routing protocol for Ad Hoc networks," Proc. of the 8th ACM International Conference on Mobile Computing and Networking, 2002.

[13] M. G. Zapata, "Secure Ad Hoc On-Demand Distance Vector (SAODV) Routing," Internet Draft: draft-guerrero-manetsaodv- 00.txt, Work in Progress, 2002.

[14] http://www.ietf.org/rfc/rfc3561.txt.

저 자 소 개

김 진 희(Jin-Hee Kim) 정회원



- 1999년 : 한국방송통신대학교 전 자 계산학과(이학사)
- 2001년 : 단국대학교 전자계산학과 컴퓨터과학(이학석사)
- 2007년 : 단국대학교 전자계산학과 컴퓨터과학(이학박사)

<관심분야> : 컴퓨터 네트워크, TCP/IP, 이동 컴퓨팅

이 재 현(Jae-Hyun Lee) 정회원

- 2000년 : 단국대학교 전자계산학과 졸업(학사)
- 2003년 : 단국대학교 대학원 전자계산학과(이학석사)
- 2007년 : 단국대학교 전자계산학과 박사수료

<관심분야> : ad hoc 네크워크, 홈 네트워크, IPv6, RFID

권 경 희(Kyung-Hee Kwon) 정회원

- 1976년 : 고려대학교 물리학과 (이학사)
- 1986년 : Old Dominion Univ. Dept. of Computer Science(M.S.)
- 1992년 : Louisiana State Univ. Dept. of Computer Science(Ph.D.)
- 1979년 ~ 1984년 : 산업연구원 연구원
- 1993년 ~ 현재 : 단국대학교 교수

<관심분야> : 컴퓨터 네트워크, 알고리즘 분석 및 설계, 웹 공학, 이동 컴퓨팅