모바일 Ad Hoc 네트워크에서 AODV 프로토콜의 성능 향상을 위한 라우팅 공격 탐지

정회원 이 재 영*, 최 승 권**, 이 병 록*, 김 선 철*, 신 병 곤*, 종신회원 조 용 환*°

Routing Attack Detection for Performance Enhancement of AODV Protocol In Mobile Ad Hoc Networks

Jae-young Lee*, Seung-Kwon Choi**, Byong-rok Lee*, Sun-Chul Kim*,
Byoung-Gon Sin* ***Regular Members,*** Yong-Hwan Cho* ***Lifelong Member***

요 약

Mobile Ad Hoc 네트워크는 이동 노드가 라우터의 역할을 하기 때문에 라우터에 보안 대책을 마련하는 유선 환경의 네트워크와는 다른 보안 대책이 필요하며 이동 노드의 전송영역이 전 네트워크를 포함하지 못하기 때문에 한 노드가 다른 노드로 메시지를 보낼 때 중간 노드가 필요하게 되는데 중간 노드가 신뢰할 수 없는 악의적인 노드라면 안전한 메시지의 전송은 보장할 수 없게 된다. 또한 네트워크를 구성하는 모든 노드는 이동 노드이기 때문에 제한된 용량의 배터리와 제한된 자원을 이용하기 때문에 메시지 전송 시 많은 자원을 필요로 하는 암호화를 수행하기가 어려워지고 그 때문에 유선 환경의 네트워크 보다 보안에 취약 할 수밖에 없다. 마지막으로 네트워크를 구성하는 노드들의 이동성으로 인해 네트워크의 토폴로지가 계속적으로 변화하기 때문에 네트워크의 특성에 맞는 보안 대책이 필요하다. 이에 모바일 Ad Hoc 네트워크에서 AODV 프로토콜의 성능 향상을 위한 라우팅 공격 탐지를 제안한다.

Key Words : MANET, AODV, Detection, DSR, DSDV

ABSTRACT

Since the mobile node acts as the router, the Mobile Ad Hoc network requires the security methods that are different from that of network of the wire environment. Also, since the total network can't be included in the transmission area of the mobile node, when one node sends the message to the other node, we need the middle node. But if the middle node is the unreliable malicious node, we can't guarantee the secure message transmission. Also, because all nodes configuring the network are the mobile nodes, they use the restricted battery capacity and the restricted resources. Therefore, because we have trouble performing the encryption that many resources are required when we sending the message, it is vulnerable to the security than the network of the wire environment. Last, because the network topology continues to change by the mobility of nodes configuring the network, we need the security measure that matches the network characteristics. We suggest the routing attack detection for performance enhancement of AODV protocol in Mobile Ad Hoc networks.

※ 이 논문은 2006학년도 충북대학교 학술 연구지원사업의 연구비지원에 의하여 연구되었음. (This work was supported by the research grant of the Chungbuk National University in 2006)
* 충부대학교 (hamsterc@daum.net), **충북대학교 전기전자컴퓨터공학부 (yhcho@cbucc.chungbuk.ac.kr)
* 조용환 : (yhcho@cbucc.chungbuk.ac.kr)(°:교신저자)
논문번호 : KICS2007-02-063, 접수일자 : 2007년 2월 12일, 최종논문접수일자 : 2007년 6월 15일

Ⅰ. 서 론

고정 기반 시설 없이, 데이터를 송수신하는 서비스를 제공 받음과 동시에 다른 노드들을 위한 데이터를 전달하는 라우터의 기능까지 하는 이동 노드들로 구성된 네트워크를 모바일 Ad Hoc 네트워크라 한다[1][2][3][4].

모바일 Ad Hoc 네트워크에서의 라우팅 프로토콜이 유선 환경의 네트워크에서의 라우팅 프로토콜보다 더욱 보안상의 취약점을 가지는 이유는 모바일 Ad Hoc 네트워크에서는 각 노드들이 호스트로서의 서비스를 받을 뿐만 아니라 라우터로서의 역할을 동시에 수행하기 때문에 모바일 Ad Hoc 네트워크 내의 노드 중 악의적인 노드가 하나라도 존재하여 라우팅 공격을 한다면 잘못된 라우팅 정보를 쉽게 퍼뜨릴수 있고 그렇게 함으로써 전체 네트워크를 마비시킬 수 있기 때문이다[5].

이에 본 논문에서는 모바일 Ad Hoc 네트워크에서 가장 널리 사용되는 AODV 라우팅 프로토콜의 성능 향상을 위한 라우팅 공격 탐지 기법을 제안한다.

본 논문의 구성은 2장에서는 모바일 Ad Hoc 네트워크의 라우팅 프로토콜과, 라우팅에 대한 공격과 탐지에 대해 설명하고, 3장에서는 AODV 라우팅 프로토콜의 성능을 향상 시킬 수 있는 5가지 라우팅 공격에 대한 탐지 기법을 제안하며 4장에서는 제안하는 공격 탐지에 대한 실험과 결과를 분석하고 5장에서는 결론을 맺는다.

Ⅱ. 라우팅 프로토콜

2.1. 라우팅 프로토콜의 분류

모바일 Ad Hoc 네트워크의 기본이 되는 라우팅 프로토콜은 경로 정보를 획득하는 기법에 따라 테이블 관리 라우팅 프로토콜과 요구 기반 라우팅 프로토콜, 그리고 최근에 테이블 관리 라우팅 프로토콜과 요구 기반 라우팅 프로토콜의 장점과 단점을 취합한 하이브리드(Hybrid) 라우팅 프로토콜이 있다[6].

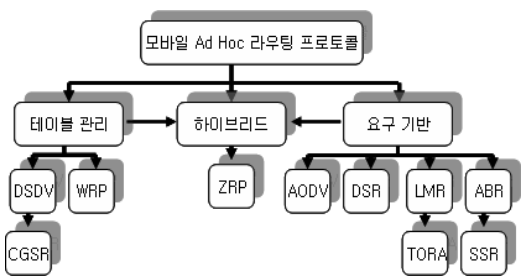

그림 1. 모바일 Ad Hoc 라우팅 프로토콜

2.1.1. AODV

AODV(Ad hoc On-demand Distance Vector)은 DSDV 라우팅 프로토콜과 같이 목적지 순차 번호와 hop by hop 방식을 사용하며 DSR 라우팅 프로토콜과 유사한 경로 탐색 절차와 경로 유지 절차를 사용한다[6].

(1) 경로 탐색 절차

경로 탐색 절차는 전송할 데이터가 있는 소스 노드가 자신의 라우팅 테이블에 목적지 노드로의 라우팅 정보를 가지고 있지 않을 때 시작된다.

목적지 노드로 데이터를 전달하고자 할 때 소스 노드는 RREQ 메시지의 중복을 [Source IP Address, RREQ ID]를 가지고 확인하므로 유일한 값이 되도록 RREQ ID를 1 증가시키고 Source IP Address에 자신의 주소, Destination IP Address에 목적지 노드 주소, 루프 방지를 위해 소스 노드 자신의 라우팅 테이블에 있는 목적지 순차 번호, 소스 순차 번호를 넣어 그림 2-5와 같은 경로 요청 메시지 RREQ를 만들어 방송한다.

만약 RREQ 메시지를 방송 후 일정 시간이 지나도 RREP 메시지가 도착하지 않는다면 RREQ ID를 1 증가시켜 RREQ 메시지를 재방송한다.

방송된 RREQ 메시지를 수신한 노드들은 [Source IP Address, RREQ ID]를 확인하여 중복 메시지인지 아닌지를 판단한다.

중복이면 RREQ 메시지를 삭제하고 중복 메시지가 아니라면 RREQ 메시지의 역경로를 RREP 메시지의 전송을 위하여 라우팅 테이블에 추가하고 Destination IP Address를 확인하여 자신이 목적지 노드인지를 확인한다.

자신이 목적지 노드라면 hop count를 1로, 목적지 순차 번호를 1증가시킨 값을 세팅하여 그림 2-6과 같은 RREP 메시지를 만들어 소스 노드로 유니캐스트한다.

자신이 목적지 노드가 아니라면 자신의 라우팅 테이블에 목적지까지의 경로 정보가 있는지 확인한다.

목적지 노드까지의 경로 정보가 있다면 RREQ 메시지의 목적지 순차 번호와 자신의 라우팅 테이블의 목적지 순차 번호를 비교하여 자신의 라우팅

테이블의 목적지 순차 번호가 RREQ 메시지의 목적지 순차번호보다 크고 Lifetime을 확인하여 유

효하다면 라우팅 테이블의 정보가 목적지 노드로의 유효한 경로 정보임을 판단하여 hop count를 목적지 노드까지의 홉 수에 1을 더하여 넣고, 자신의 라우팅 테이블의 목적지 순차 번호를 세팅하여 RREP 메시지를 만들어 소스 노드로 유니캐스트한다.

만약 자신이 목적지 노드가 아니고 목적지 노드까지의 경로 정보도 가지고 있지 않은 경우에는 자신의 라우팅 테이블의 정보를 갱신하고 위해 RREQ 메시지의 소스 순차 번호와 라우팅 테이블의 소스 노드에 해당하는 목적지 순차 번호를 비교하여 RREQ 메시지의 소스 순차 번호가 더 크다면 RREQ 메시지가 더 최신 메시지이므로 소스 노드의 경로 정보를 수정한다. 그리고 소스 노드로부터의 RREQ 메시지를 다른 노드로 방송하기 위해 hop count값을 하나 증가시키고 TTL 값을 하나 감소시킨다. 마지막으로 IP 헤더를 자신의 주소로 변경하여 다시 방송한다.

RREP 메시지가 도착하면 자신이 RREQ 메시지를 전송한 소스 노드인가를 확인한다.

자신이 소스 노드라면 경로 탐색 절차를 완료하고 탐색된 경로를 통해 메시지를 전달한다.

자신의 소스 노드가 아니라면 RREP 메시지 내의 목적지 노드에 대한 경로 정보가 자신의 라우팅 테이블에 있는지 확인한다.

라우팅 테이블에 목적지 노드의 경로 정보가 없다는 추가하고 경로 정보가 있다면 라우팅 테이블의 목적지 순차 번호와 RREP 메시지의 목적지 순차 번호를 비교한다.

RREP 메시지의 목적지 순차 번호가 더 작거나, 홉 수가 더 크다면 유효하지 않은 경로 정보이므로 라우팅 테이블을 갱신하지 않고 RREP 메시지를 소스 노드로 유니캐스트한다.

RREP 메시지의 목적지 순차 번호가 더 크고 홉 수가 작다면 RREP 메시지의 순경로와 RREP 메시지의 목적지 순차 번호 등 정보를 라우팅 테이블에 추가하고 RREP 메시지를 소스 노드로 유니캐스트한다[6][7].

(2) 경로 유지 절차

메시지를 전송하고 있는 경로이거나 Lifetime이 남아있는 경로들은 그 경로가 유지되고 있는지를 확인하기 위해 Hello 메시지를 이용하게 된다.

만약 일정시간 동안 Hello 메시지를 수신하지 못했다면 경로가 단절되었다고 판단하게 되고 경로가 단절되었다고 판단되면 현재 노드에서 목적지 노드 방향의 다음 홉으로 사용되었던 노드들에게 RERR 메시지를 전달하여 경로의 단절을 알린다.

AODV 라우팅 프로토콜은 라우팅 테이블을 이용하여 일정동안 사용하지 않은 경로는 유효하지 않다고 간주하여 경로 정보를 삭제하기도 한다[6][7].

2.1.2. 라우팅에 대한 공격과 탐지

(1) 라우팅에 대한 공격

Black Hole : 이 공격에서 악의적인 노드는 가로채고자 하는 메시지의 목적지 노드로의 경로 정보를 거짓으로 만들어 소스 노드에게 응답한다.

라우팅을 요청한 노드가 실제 노드로부터의 응답이 오기 전에 악의적인 노드의 응답을 먼저 받으면 위조된 경로가 생성된다. 악의적인 노드가 통신하는 노드사이에 끼어들 수 있다면 그들 간의 메시지를 이용하여 서비스 거부 공격이나 man-in-the-middle 같은 공격이 가능하다.

Routing Table Overflow : 이 공격에서는 공격자가 존재하지 않는 노드의 라우팅 정보를 생성한다. 이 공격의 목적은 새로운 정보가 생성되는 것을 막거나 프로토콜 적용을 못하게 하는 것이다.

테이블 관리 라우팅 프로토콜이 요청이 있을 때만 경로를 설정하는데 반해 요구 기반 라우팅 프로토콜은 요청이 없더라도 일정시간이 간격으로 라우팅 정보를 갱신한다.

공격자는 네트워크에 있는 라우터에게 과도한 경로 정보를 통보함으로써 간단하게 네트워크를 붕괴시킬 수 있다.

Resource Consumption : 이 공격은 모바일 Ad Hoc 네트워크에서 사용가능한 대역폭과 노드의 배터리 수명을 소비하기 위하여 라우팅 트래픽을 범람시키는 것이다.

Location Disclosure : 이 공격은 노드의 위치나 토폴로지 그리고 네트워크의 구조를 누설할 수 있다. 이 공격으로 목적지 노드에 인접한 노드나 목적지 노드의 물리적인 위치 정보를 얻을 수 있을 것이다.

정보를 이용하여 라우팅 메시지를 만들고 메시지는 잘못된 hop-limit 값을 보내고 잘못된 hop-limit 값을 받은 장치는 ICMP 에러 메시지를 보낸다. 결국 공격자는 어떤 노드가 목적지 노드에 대한 경로를 가지고 있는지 알게 될 것이며 일부의 중간 노드 위치가 알려지면 목적지의 위치에 대한 정보를 얻을 수 있다[8].

3.1.3. 공격 탐지

(1) 경비견과 경로 평가자

경비견(Watchdog)과 경로 평가자(Path rater)는

DSR 라우팅 프로토콜을 기반으로 하는 악의적인 노드 식별 및 조치 방법이다[9].

경비견과 경로 평가자의 기본동작은 각 노드는 데이터를 이웃 노드에게 전송한 후 그 복사 본을 자신의 버퍼에 저장하고 데이터를 전송받은 이웃 노드가 전송받은 데이터를 그 다음 이웃 노드에게 전송하는지를 엿듣는다.

만약 일정 시간 내에 데이터를 전송 받은 이웃 노드가 그 데이터를 다른 이웃 노드에게 전송하면 자신의 버퍼에 저장하고 있던 데이터의 복사 본을 버리고 데이터를 전송 받은 이웃 노드가 일정시간이 지나도 데이터를 그 이웃 노드에게 전송하지 않는다면 데이터를 전송하지 않은 노드의 failure tally를 증가시킨다.

만약 failure tally가 임계치를 초과하게 되면 그 노드가 고의적으로 데이터를 버리는 것으로 판단하고 소스 노드에게 데이터를 전송하지 않은 노드를 신고한다.

(2) CONFIDANT

CONFIDANT(Cooperation Of Nodes: Fairness In Dynamic Ad-hoc NeTwork)는 경비견과 경로 평가자와 비슷하게 각 노드들이 서로를 감시하면서 악의적인 노드를 탐지하는 메커니즘이다[10].

경비견과 경로 평가자와 다른 점은 악의적인 노드를 탐지하고 그 노드들을 피해 메시지를 보내는 것뿐만 아니라 악의적인 노드들을 네트워크에서 고립시켜 네트워크의 서비스를 이용하지 못하도록 하는 것이다.

CONFIDANT에서 정보는 악의적인 노드로부터 직접 피해를 입은 노드에게서 온 것과 피해를 입은 노드로부터 전해진 것 두 가지로 구별하여 서로 다른 가중치를 두어 관리한다.

(3) CORE

Michirdi 와 Molva에 의해 제안된 CORE(a COllaborative REputation Mechanism to enforce node cooperation in mobile ad hoc network)는 역시 경비견과 경로 평가자와 비슷한 방식으로 악의적인 노드를 탐지한다. 그러나 CORE에서는 좀더 정교한 평가 메커니즘을 제공한다[11].

평가 메커니즘은 관찰자 노드 자신에 의한 주관적인 평가와, 다른 노드들에 의한 명확한 평가인 간접적인 평가, 그리고 특정 업무에 따른 행동의 평가인 기능적인 평가를 구별하여 서로 다른 가중치로 노드에 대한 평가 값을 구하게 된다. 평가 값에 따라 노드를 네트워크에서 고립시키거나 노드로 하여금 네트워크에 협조할 수 있도록 격려한다.

(4) Nuglets

앞에서 서술한 메커니즘들이 이미 악의적인 행위를 한 노드들에 대한 대처 방안이라면 Nuglets는 처음부터 노드들이 악의적인 행동을 하지 않도록 유도하는 방법을 제시한 것이다[12].

Ⅲ. 라우팅 공격에 대한 탐지 기법 제안

AODV 라우팅 프로토콜에서의 Sequence Number 공격, Dropping Routing Messages 공격, Data Tempering 공격, Resource Consumption 공격, False Return 공격 등 5가지 공격에 대한 탐지 기법을 제안한다.

3.1. Sequence Number 공격 탐지

AODV 라우팅 프로토콜은 노드들 간에 가장 최근의 경로 정보를 유지하기 위해 단조롭게 증가하는 목적지 순차 번호를 이용하여 목적지 노드로의 경로를 생성하고 유지한다.

새로운 경로는 RREQ 메시지의 응답으로 각 노드들이 전송한 RREP 메시지들 중 목적지 순차 번호가 크거나 홉 수가 적은 RREP 메시지가 선택되어 그 정보를 가지고 설정되기 때문에 악의적인 노드는 목적지 순차 번호를 크게 조정함으로써 네트워크에 문제가 있는 라우팅 정보를 주입시킬 수가 있다.

이렇게 악의적인 노드는 잘못된 라우팅 정보를 퍼트림으로써 경로 안에 자신을 포함시키고 Black Hole 공격을 실행 할 수가 있다.

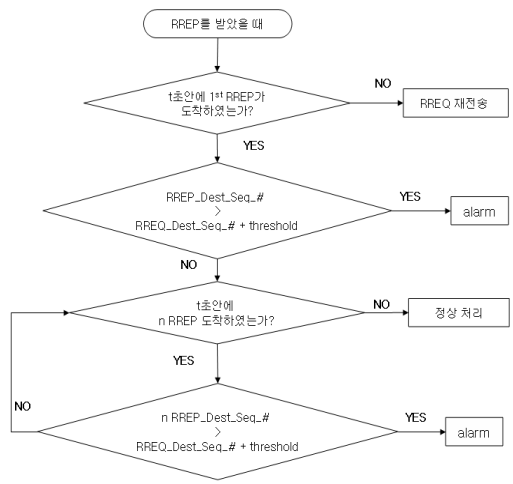

그림 2. Sequence Number 공격 탐지 순서도 (소스노드가 RREP 메시지를 받았을 때)

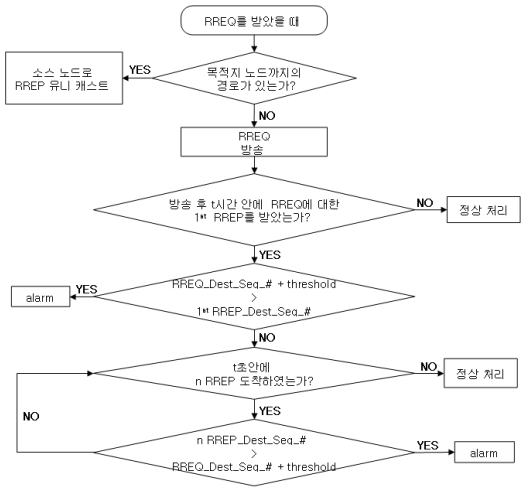

그림 3. Sequence Number 공격 탐지 순서도(중간 노드가 RREQ 메시지를 받았을 때)

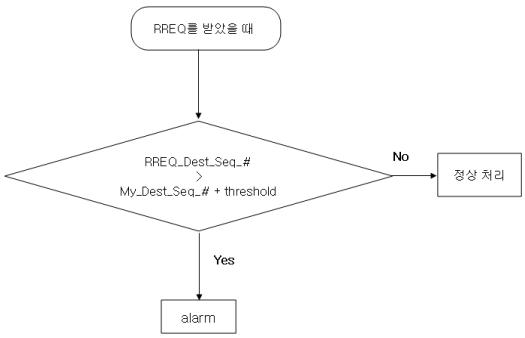

그림 4. Sequence Number 공격 탐지 순서도 (목적지노드가 RREQ 메시지를 받았을 때)

3.2. Dropping Routing Messages 공격 탐지

모바일 Ad Hoc 네트워크와 같은 무선의 이동 환경의 네트워크는 제한된 배터리의 수명과 제한된 자원들 때문에 노드에 기존 유선의 고정된 환경의 네트워크와는 차이가 있다.

모바일 Ad Hoc 네트워크의 이동 노드들은 대부분 메시지를 전달하거나 라우팅 프로토콜에 참여할 때 자원을 소비하게 된다. 이때 악의적인 노드가 자신의 자원 소모를 줄이기 위해서 또는 네트워크의 성능을 저하시키기 위해 고의적으로 다른 노드의 메시지는 전달해주지 않으면서 자신의 메시지만을 전달하려고 할 수 있다. 만약 선의의 노드가 악의적인 노드와만 연결이 되어 있다면 선의의 노드는 자신의 메시지를 다른 노드로 전달할 수 없게 되고 나아가서는 네트워크의 나머지 노드들로부터도 고립

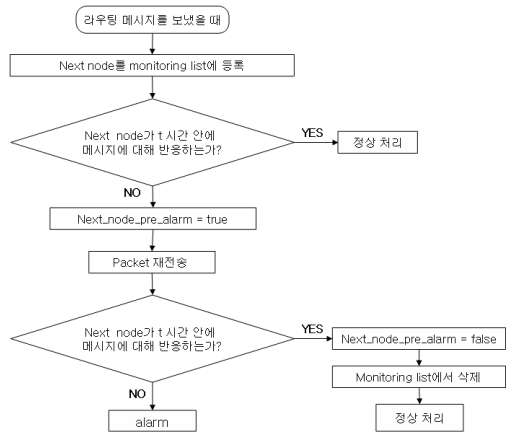

그림 5. Dropping Routing Message 공격 탐지 순서도

될 수 있다[4][10].

네트워크와 연관되는 모든 노드가 무차별 노드이기 때문에 이웃하는 노드들은 악의적인 노드가 라우팅 메시지를 전송했는지를 탐지할 수 있다. 하지만 어떤 노드는 악의를 갖지 않았는데도 노드의 트래픽 과부하 때문에 라우팅 메시지를 전송하지 못했을 경우도 있다.

때문에 Dropping Routing Messages 공격의 탐지에서는 두 경우를 구분하기 위해 처음에는 pre_alarm으로 처리하고 이 상태에서 다시 라우팅 메시지를 전송하지 못한 노드로 라우팅 메시지를 보내 경고 여부를 결정한다.

3.3. Data Tempering 공격 탐지

악의적인 노드는 정상적인 라우팅 메시지를 받아 메시지의 내용을 임의로 변경하여 전송할 수 있다. 이렇게 악의적인 노드가 라우팅 메시지를 변경하여

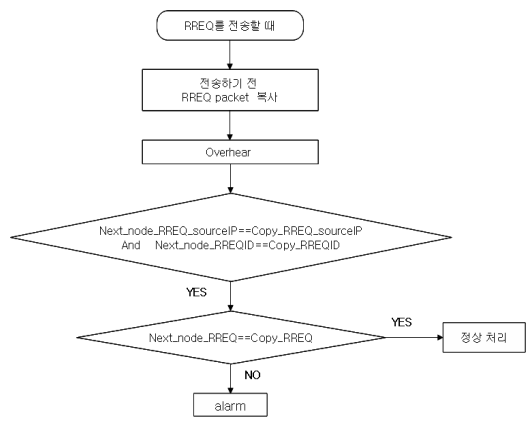

그림 6. Data Tempering 공격 탐지 순서도

이웃 노드에게 전송하게 되면 정당한 노드가 경로 설정 할 수 없어 데이터를 전송하지 못함은 물론이고 네트워크로부터 고립될 수도 있다[13].

노드가 경로 설정을 위해 RREQ 메시지를 만들어 이웃 노드에게 방송하기 전에 전송할 RREQ 메시지를 버퍼에 복사하여 둔다. 그리고 이웃 노드가 자신이 전송받은 RREQ 메시지를 이웃 노드에게 방송할 때 노드는 그 RREQ 메시지를 받아 자신의 버퍼에 저장된 복사본과 비교한다.

비교 결과 두개의 메시지가 다르면 이웃 노드가 악의적인 노드임을 판단하여 경고 처리한다

3.4. Resource Consumption 공격 탐지

Resource Consumption 공격은 악의적인 노드가 빈번하고 불필요한 라우팅 메시지를 만들어 보냄으로써 네트워크와 노드 양쪽의 자원을 소비하게 하려고 시도하는 것이다.

Resource Consumption 공격에 사용되는 라우팅 메시지는 RREQ 메시지와 RERR 메시지만으로 구성되는데 그 이유는 AODV 라우팅 프로토콜의 특성상 채택되지 못한 RREP 메시지는 자동으로 버려지기 때문이다.

이 공격의 목적은 네트워크를 잘못된 라우팅 메시지로 채워 범람시키고 부적절한 메시지로 사용가능한 네트워크의 대역폭을 소비하고 노드의 에너지와 처리 능력을 소비하려는 것이다[4][13].

Resource Consumption 공격 탐지는 RREQ 메시지와 RERR 메시지를 전송 받는 모든 노드에서 시작된다. 라우팅 메시지를 전송하거나 전송받는 모든 노드는 다른 모든 노드들의 기록을 보관하며 기록에는 최근에 특정 노드로부터 받은 라우팅 트래픽과 함께 그 노드가 보낸 메시지들의 수와 시간을 기록한 카운터와 타이머가 있다.

특정 노드로부터 새로운 라우팅 메시지를 받으면 카운터를 증가시키고 t 시간동안 기다린다. t 시간동안 같은 노드로부터 전송되어 오는 메시지의 수를 카운터에 기록하고 카운터가 임계값에 도달하면 라우팅 메시지를 전송한 노드가 비정상적으로 traffic을 생성한다는 것을 탐지하고 공격 처리한다.

3.5. False Return 공격 탐지

악의적인 노드를 식별하여 공격을 탐지 하는 경우 네트워크를 구성하는 모든 노드는 신고 테이블을 유지한다.

False Return 공격은 악의적인 노드가 임의의 정상 노드를 악의적인 노드로 거짓 신고하여 신고 테이블에 기록되게 하는 공격이다. 신고 테이블에 등록이 되면 다른 노드의 경로 설정에 응답할 수 없음은 물론이고 자신의 경로 설정도 불가능하게 된다[9].

공격 탐지가 가능한 모든 노드는 신고 테이블을 둔다. 신고 테이블에는 악의적인 노드와 악의적인 노드를 신고한 신고 노드가 기록된다.

악의적인 노드가 계속적으로 임의의 노드를 계속 거짓 신고하는 경우에는 신고 테이블에 신고 목록이 계속 추가 된다. 때문에 어느 노드 하나가 신고테이블에 신고자로 k번 이상 기록되면 거짓 신고자로 식별되어 더 이상 네트워크에 참여 할 수 없게 한다.

False Return 공격 탐지는 경고가 있고 경고 메시지가 전송될 때 시작된다. 어떤 노드가 경고 처리되어 신고 테이블에 등록될 때는 먼저 신고 테이블에서 신고 노드를 검색하게 된다. 신고 노드를 검색해 신고 횟수가 k이상이 되면 다시 신고 테이블에

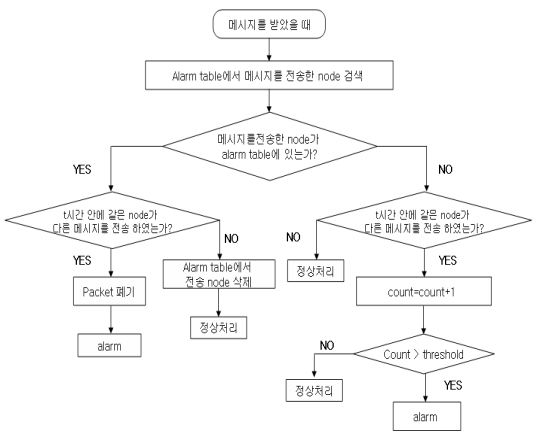

그림 7. Resource Consumption 공격 탐지 흐름도

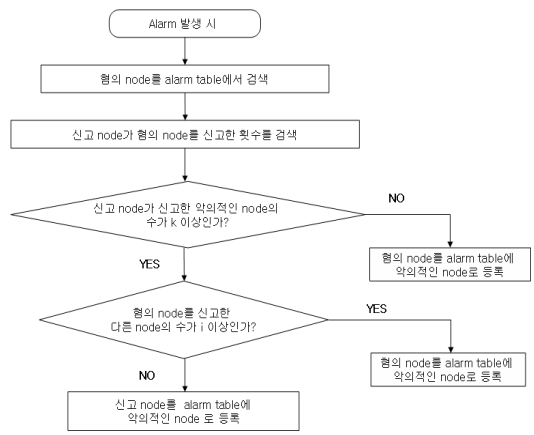

그림 8. False Return 공격 탐지 흐름도

서 악의적인 노드가 이전에 다른 노드에게 신고 된 적이 있는지를 검색한다. 신고 횟수가 i 이하라면 신고 노드를 거짓 신고자로 식별되고 거짓 신고자가 신고한 노드는 신고 테이블에서 삭제되며 신고 노드가 신고 테이블에 악의적인 노드로 등록된다.

3.6. 경고 처리

노드가 악의적인 노드를 탐지하면 이웃 노드에게 악의적인 노드의 존재를 알리는 그림 9와 같은 RALA(Routing Alarm) 메시지를 방송한다.

RALA 메시지에는 악의적인 노드의 IP 주소와 악의적인 노드의 목적지 순차 번호, 악의적인 노드를 탐지한 신고 노드의 주소, 신고 노드의 목적지 순차 번호를 담게 된다.

각 노드가 방송된 RALA 메시지를 수신하면 자신이 유지하고 있는 신고 테이블에 RALA 메시지의 내용을 추가하게 된다.

신고 테이블에 악의적인 노드로 등록된 노드는 다른 노드의 경로가 될 수 없음은 물론이고 어떤 종류의 트래픽도 전송하지 못하게 된다.

신고 테이블에 기록된 악의적인 노드는 일정 시간이 지난 뒤 또 다른 노드로부터 다른 신고가 없다면 신고 테이블에서 삭제된다.

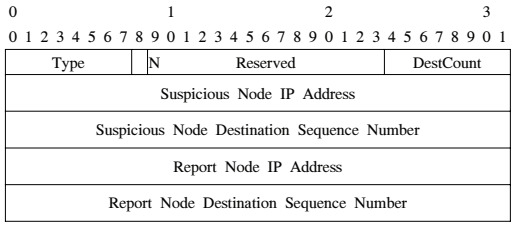

그림 9. RALA 메시지 형식

표 1. RALA 메시지

필 드 명	역 할
TYPE	RALA 메시지임을 구분해주는 것으로 값은 5
N	No delete flag
Reserved	0으로 보내고 받는 쪽에서는 무시
DestCount	RALA 메시지 안에 포함된 도달 할 수 없는 목적지 노드들의 수
Suspicious node IP Address	악의적인 노드의 IP 주소
Suspicious node Destination Sequence Number	악의적인 노드의 목적지 순차 번호
Report node IP Address	신고 노드의 IP 주소
Report node Destination Sequence Number	신고 노드의 목적지 순차 번호

표 2. 신고 테이블

필 드 명	역 할
Suspicious Node IP Address	악의적인 노드 IP 주소
Suspicious Node Destination Sequence Number	악의적인 노드 목적지 순차 번호
Report Node IP Address	신고 노드 IP 주소
Report Node Destination Sequence Number	신고 노드 목적지 순차 번호
time	신고 시간

Ⅳ. 실험 및 결과 분석

4.1. 실험 환경

1000m*1000m 지역에 5개에서 30개의 노드를 무작위로 배치하고 각 노드의 전파 전송 범위는 250m이며, 대역폭은 IETF에서 무선 네트워크의 대역폭으로 규정한 2Mbps, 송신 노드는 초당 2개의 패킷을 보내며, 총 시뮬레이션 시간은 1000초 이다.

노드의 움직임은 random waypoint를 사용하여 이동할 목적지를 무작위로 선택하고 노드의 이동 속도는 최저 4m/sec에서 최대 20m/sec로 목적지를 향해 움직이며, 노드의 수는 최소 5개에서 최대 30개까지로 한다. 이동 노드는 목적지에 도달한 후 10초 동안 머물다 다른 목적지로 이동한다.

실험은 노드의 이동 속도를 8m/sec로 하고 공격을 하는 노드가 1개일 때 참여하는 노드의 수를 5, 10, 15, 20. 25, 30개로 변경했을 때와, 참여하는 노드 수를 1개, 공격을 하는 노드 1개일 때, 노드의 이동 속도를 4m/sec, 8m/sec, 12m/sec, 16m/sec, 20m/sec로 변경했을 경우 2가지 경우에서의 전송률 구하였다.

전송률은 소스 노드가 목적지 노드로 전송한 모든 메시지에 대한 목적지 노드가 수신한 메시지의 비율로 정의한다.

4.2. 결과 및 분석

Sequence Number 공격의 탐지에서 제안하는 AODV 라우팅 프로토콜 라우팅 프로토콜은 이동 노드의 수가 5개로 가장 적을 때 전송률이 가장 낮고, 20~25개일 때 전송률이 최대가 되는 것을 알 수 있었다

이동 노드의 속도가 높아지면 전송률이 떨어지는 것을 볼 수 있었는데 이는 이동 노드의 이동 속도가 증가하면 네트워크의 토폴로지가 이동 속도가 낮을 때 보다 훨씬 더 많이 변화하여 네트워크를 구성하는 각 노드들의 경로 설정이 훨씬 더 빈번하

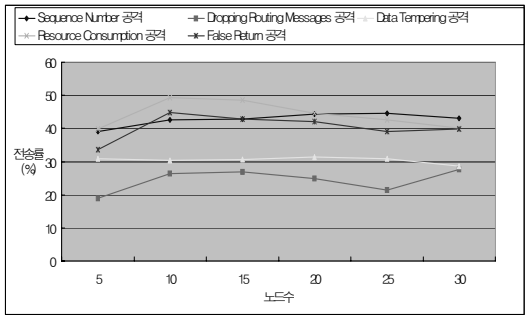

그림 10. 공격 하의 전송률 (참여 노드수 변경)

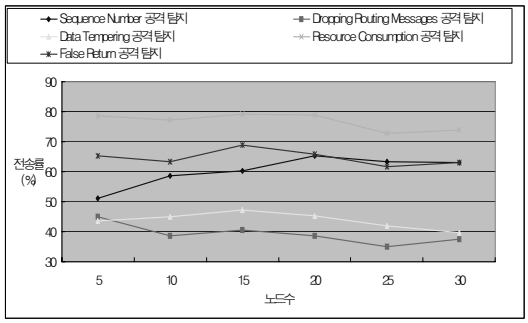

그림 11. 제안한 공격 탐지 시 전송률 (참여 노드수 변경)

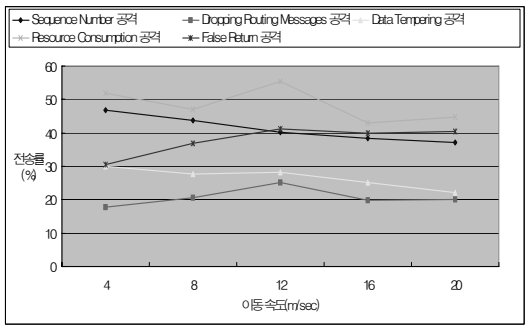

그림 12. 공격 하의 전송률 (노드의 이동속도 변경 시)

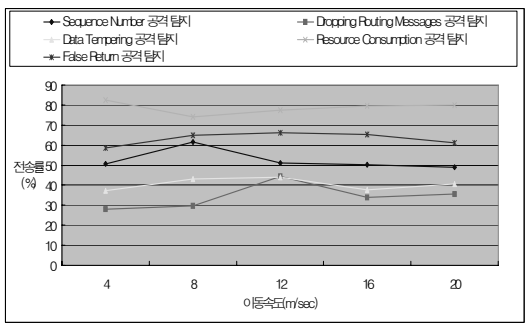

그림 13. 제한한 공격 탐지시 전송률 (노드의 이동속도 변경 시)

게 요구되어지므로 RREQ 메시지의 수가 많아지게 된다. 때문에 악의적인 노드는 RREQ 메시지에 대한 응답으로 Sequence Number 공격에 이용될 악의적인 RREP 메시지를 생성하고 전송할 기회가 더 많아지므로 공격의 기회도 더 많아진다.

Dropping Routing Message 공격의 탐지에서는 악의적인 노드의 공격이 있을 때 전송률이 현격하게 낮아지는 것을 볼 수 있었다. 특히 노드의 수가 적을 때 그 피해가 심했는데, 이는 노드의 수가 적어지면 네트워크의 거의 모든 노드가 경로 설정에 참여하게 되고 악의적인 노드가 경로에 포함될 가능성이 높아지고 악의적인 노드가 경로의 홉으로 사용되면 메시지의 전송은 거의 불가능하다 볼 수 있다.

또한 이동 노드의 이동 속도가 증가하면 참가 노드들이 경로 탐색 절차를 더 빈번하게 요구하게 되고 그렇게 되면 네트워크 상에 RREQ 메시지와 RREP 메시지의 수가 많이 늘어나게 된다. 이때 악의적인 노드가 자신에게 전송되어지는 라우팅 메시지를 더 많이 drop 함으로 네트워크의 접속을 더 효율적으로 방해하기 때문에 이동 노드의 이동 속도가 증가할 때 전송률이 낮아진다.

Dropping Routing Message 공격에서는 제안하는 AODV 라우팅 프로토콜에서도 개선이 아주 높은 수준으로 이루어지는 것은 아닌데 그 이유는 제안하는 AODV 라우팅 프로토콜도 단지 악의적인 노드의 존재를 각 노드에게 알려줄 뿐 악의적인 노드가 메시지를 drop 하지 못하도록 강제적으로 취할 수 있는 방법이 없기 때문이다.

Data Tempering 공격에서도 공격이 있는 상태의 AODV 라우팅 프로토콜에서의 전송률이 많이 떨어짐을 볼 수 있었고 제안하는 공격 탐지 기능을 갖는 AODV 라우팅 프로토콜에서도 전송률이 많이 개선되지는 않는데 이 역시 제안하는 AODV 라우팅 프로토콜은 단지 Data Tempering 공격을 하는 악의적인 노드를 다른 노드에게 알려주어 경로 설정 시 참고가 되는 정보를 전달하기만 할 뿐 악의적인 노드가 메시지를 변경하지 못하도록 강제적으로 취할 수 있는 방법이 없기 때문이다.

Resource Consumption 공격에서는 악의적인 노드의 공격이 있는 상태의 AODV 라우팅 프로토콜보다 제안하는 공격 탐지 기능을 갖는 AODV 라우팅 프로토콜에서 전송률이 월등히 개선됨을 볼 수 있는데 이는 악의적인 노드를 감시하여 메시지의 수가 임계치를 넘으면 바로 악의적인 노드에서 온 모든 메시지를 drop하고 다른 노드들에게 알리기

때문에 Resource Consumption 공격에 대해 제안하는 AODV 라우팅 프로토콜이 가장 효과적이라는 것을 알 수 있다.

False Return 공격에서는 악의적인 노드의 거짓 신고를 탐지하는 것으로 네트워크를 구성하는 노드의 개수가 적을 때 악의적인 노드를 탐지하여 전송률을 높일 수 있는 것임을 알 수 있다.

Ⅴ. 결 론

본 논문에서는 AODV 라우팅 프로토콜의 성능을 향상 시킬 수 있는 공격 탐지를 기법 제안하였다.

제안한 공격 탐지는 5가지 유형의 공격을 하는 악의적인 노드를 탐지하고 탐지한 결과를 경고 메시지 RALA를 방송함으로 네트워크를 구성하는 노드들에게 알려 각 노드로 하여금 자신이 유지하는 신고 테이블에 악의적인 노드를 등록하여 경로 설정에 도움이 되게 하는 것이다.

악의적인 노드 1개가 공격하는 상태에서 네트워크 노드 수를 변경시켰을 때의 전송률과, 노드의 이동 속도에 변화가 있을 때의 전송률을 구하여 각 공격에 대한 탐지를 평가하였다.

악의적인 노드가 존재할 경우 네트워크를 구성하는 노드의 수가 적을수록, 노드의 이동 속도가 높을수록 전송률은 낮아졌다.

제안한 5가지 유형의 공격에 대한 탐지 방법들 중 Resource Consumption 공격에서 전송률의 개선이 가장 두드러짐을 알 수 있었다.

앞으로는 악의적인 노드의 악의적인 행위를 적극적으로 막아 네트워크로 고립시킬 수 있게 하는 대책을 마련하는 연구가 필요하다. 또한 점점 더 다양해지는 공격에 대비한 다양한 탐지 방법의 연구가 필요하다.

참 고 문 헌

〔1〕 C. E. Perkins, "Ad hoc Networking", Addsion-Wesley Publishing Company, 2000.

〔2〕 C. K. Toh, "Ad-hoc Mobile Wireless Networks: Protocols and System", Prentice Hall PTR, 2002.

〔3〕 Songwu Lu, and Lixia Zhang, "Security in Mobile Ad Hoc Network : Challenges and Solutions.", IEEE Wireless Communications, 2004.

〔4〕 L. Buttyan and J. P. Hubaux, "Report on a Working Session on Security in Wireless Ad Hoc Networks" Mobile Computing and Communications Review, Vol. 6, No. 4. 2002.

〔5〕 E. M. Royer, C-K Toh, "A Rewiew Routing Protocols for Ad-Hoc Mobile Wireless Network." IEEE Personal Communication 6(2). 1999.

〔6〕 S. Marti and T. J. Giuli and K. Lai and M. Baker, "Mitigating routing misbehavior in mobile ad hoc network", Mobile Computing and Networking, pp15~22, Vol. 2, No 4. 2000.

〔7〕 이정은, "이동 Ad Hoc 환경에서 AODV 기반의 분기 노드를 이용한 대체 경로 라우팅 기법", 경희대 대학원 이학석사학위논문. 2004.

〔8〕 배재호(2004), MANET에서 악의적인 노드의 효율적인 검출 방안, 연세대학교 대학원, 공학석사학위논문.

〔9〕 P. Papadimitratos and Z.J.Haas, "Secure Routing for Mobile Ad Hoc Networks," SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002), San Antonio, TX, January. p27~31. 2002.

〔10〕 Sonja Buchegger and Jean-Yues Le Boudec (2002), "Performance Analysis of the CONFIDANT Protocol: Cooperation Of Nodes - Fairness In Distributed Ad-hoc Networks", In roceedings of IEEE/ACM Workshop on Mobile Ad Hoc Networking and Computing (MobilHOC), Lausaanne, CH, pp.10~15, Vol 5, No. 4. June.

〔11〕 P. Michiardi, R. Molva (2002), "Core: A COllaborative REputation Mechanism to enforce node cooperation in Mobile Ad Hoc Networks." in Communication and Multimedia Security 2002 Conference.

〔12〕 L. Buttyan and J. P. Hubaux(2001), "Stimulation Cooperation in Self-Organizing Mobile Ad Hoc Networks." Technical Report No. DSC/2001/046, Swiss Federal Institute of Technology, Lausanne, Auguest.

〔13〕 Lidong Zhou, Zygmunt J. Haas, "Securing Ad Hoc Network". IEEE Network, Special Issue on Network Security, November/Decenber, 1999.

이 재 영 (Jae-young Lee) 정회원

2007년 2월 충북대학교 컴퓨터공학과 대학원 졸업(공학박사)
2007년 3월~현재 충북대학교 전기전자컴퓨터공학부 초빙교수
<관심분야> 침입탐지, 라우팅

최 승 권 (Seung-Kwon Choi) 정회원

2001년 8월 충북대학교 컴퓨터공학과 대학원 졸업(공학박사)
현재 중부대학교 강의 전담교수
<관심분야> 멀티미디어 콘텐츠, 게임디자인, 유비쿼터스 네트워킹

이 병 록 (Byong-rok Lee) 정회원

2006년 8월 충북대학교 컴퓨터공학과 대학원 졸업 (공학박사)
현재 충북대학교 BK21연수연구원
<관심분야> 유비쿼터스 네트워킹, 멀티미디어통신, 무대제어 설비 의용공학, 영상처리

김 선 철 (Sun-Chul Kim) 정회원

현재 신명전기공사 대표이사
<관심분야> 멀티미디어 통신, 유비쿼터스 네트워킹,, RFID, 무선통신

신 병 곤 (Byoung-Gon Sin) 정회원

현재 충북대학교 컴퓨터공학과 대학원 재학(박사과정)
<관심분야> 유비쿼터스 네트워킹, 무선통신

조 용 환 (Yong-hwan Cho) 종신회원

한국통신학회논문지 제31권 제8A호 참조