보안공학연구논문지 *Journal of Security Engineering*
Vol.12, No.4 (2015), pp.415-426
http://dx.doi.org/10.14257/jse.2015.08.06

VANET 상에서 안전한 라우팅을 위한 효율적인 웜홀 공격 탐지 및 제거 기법 설계

이병관[1], 정은희[2]

A Design of an efficient Wormhole Attack Detection and Removal Scheme for Secure Routing on VANET

ByungKwan Lee[1], EunHee Jeong[2]

요 약

본 논문에서는 VANET 상에서 안전한 라우팅을 위한 웜홀 공격 탐지 및 제거 기법 설계를 제안한다. 제안된 기법에서는 AODV의 RREP와 라우팅 테이블에 이웃노드목록을 추가하고, 메시지 전송 경로 설정 응답 메시지인 Route_ACK를 설계하였다. 그리고 메시지 전송 경로 생성 시에 이웃노드목록, 홉(hop) 수를 이용하여 웜홀 공격 여부를 판단하고, Route_ACK를 이용하여 웜홀 노드를 검출하도록 설계하였다. 그 결과 웜홀 노드를 제외시킨 데이터 전송 경로를 선정하여 데이터를 전송함으로써 AODV보다 데이터 전송량이 평균적으로 36% 증가하였다. 따라서 본 논문에서는 제안하는 기법을 이용하여 안전하고 신뢰성이 높은 VANET을 구축하였다.

핵심어 : 웜홀 공격 탐지, 홉 카운트, 이웃노드목록, 라우팅 프로토콜, 바넷

Abstract

This paper proposes “A Design of an efficient Wormhole Attack Detection and Removal Scheme for Secure Routing on VANET”. The proposed scheme appends the list of neighboring nodes to the RREP and Routing table of AODV and designs Route_ACK which is a response message about message transmission route setting. Whenever it generates the message transmission route, it designs to judge a wormhole attack by using the list of neighboring nodes and hop counts and to detect a wormhole node by using the Route_ACK. Therefore, it’s data delivery quantity is improved by about 36 % than AODV because it transmits data through the data transmission route which excluded the wormhole nodes. Because of the proposed scheme, the paper can make the VANET more safe and reliable.

Keywords : Wormhole attack detection, Hop count, Neighbor node list, Routing protocol, VANET

접수일(2015년07월18일), 심사의뢰일(2015년07월19일), 심사완료일(1차:2015년07월28일)
게재확정일(2015년08월05일), 게재일(2015년08월31일)

1210-701 강릉시 범일로 579번길 24. 가톨릭관동대학교 컴퓨터공학과.
email: bklee@cku.ac.kr
2(교신저자) 245-711 삼척시 중앙로 346. 강원대학교 지역경제학과
email: jeongeh@kangwon.ac.kr
* 이 논문은 2014년도 정부(교육부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임(NRF- 2013R1A1A2062415)

ISSN: 1738-7531 JSE

1. 서론

현재, 휴대용 이동 단말기의 보편화, 기기의 소형화, 사용 시간의 증가, 그리고 사용 가능 지역의 확대등과 같은 기술의 발달에 따라 소비자들은 점차 다양한 분야에서 다양한 목적을 충족시킬 수 있는 네트워크 환경을 요구하기 시작했다. 즉, 시간과 장소의 제약을 뛰어넘어 언제 어디서든지 인터넷을 비롯한 네트워크에 접속하여 다양한 작업을 수행하기를 희망하는데, 이와 같은 대중의 요구사항을 충족시키기 위해 등장한 것이 바로 MANET(Mobile Ad hoc Network)이다[1][2]. 하지만, MANET은 기본적으로 네트워크내의 모든 단말에 데이터를 전송하는 브로드캐스팅 방식을 사용하기 때문에, 단말은 다른 사람의 송수신 내용을 쉽게 청취할 수 있어 의도된 수신자 이외의 다른 사람이 데이터를 도청하거나, 이로 인한 악의적인 공격을 당할 가능성이 높다[3].

특히, 실제로는 원거리에 있는 두 개의 악의적인 노드가 마치 서로 이웃하고 있는 것처럼 주변 노드들을 속이고 터널을 형성하여 정상적인 라우팅 경로보다 더욱 짧은 홉 수를 거쳐 패킷이 전달되는 것처럼 거짓 정보를 근원지 노드에 전달함으로써 근원지 노드가 웜홀이 포함된 경로를 선정하는 웜홀 공격이 발생한다면, 일차적으로 네트워크 정보를 몰래 도청하고, 이차적으로는 전송 데이터를 삭제, 위조하는 등의 공격이 발생할 수 있다.

본 논문에서는 VANET에서 발생할 수 있는 라우팅 공격인 웜홀 공격을 탐지하고 웜홀 노드를 제거하는 기법을 제안한다. 제안하는 웜홀 공격 탐지와 웜홀 노드 제거 기법은 데이터 전송 경로 설정 시에 이웃노드목록, 홉(hop) 수를 이용하여 웜홀 공격 여부를 판단하도록 설계하고, 제안된 Route_ACK를 이용하여 웜홀 노드를 검출하고, 웜홀 노드를 VANET 내의 모든 노드에게 공지함으로써 웜홀 노드를 제외시킨 데이터 전송 경로를 선정함으로써 데이터 패킷을 손실 없이 정확하게 전달하고자 한다.

본 논문의 구성은 다음과 같다. 2장에서는 관련연구를 설명하고 3장에서는 본 논문에서 제안하는 웜홀 공격 탐지와 웜홀 노드 제거 기법 설계를 설명한다. 그리고 4장에서는 제안하는 기법의 성능을 분석하고 5장에서 결론을 맺는다.

2. 관련 연구

2.1 AODV Routing Protocol

AODV 라우팅 프로토콜은 1999년 C. Perkins가 제안한 Ad hoc 네트워크에서 가장 대표적인 On-demand 방식의 라우팅 프로토콜로 RREQ(Routing REQuest), RREP(Routing REPly), RERR(Routing ERRor) 등의 라우팅 패킷을 사용하여 라우팅 경로를 설정한다[3-6].

RREQ는 소스 노드가 목적지 노드를 찾을 때 경로 탐색을 요청하기 위해 사용하는 메시지로 그 형식은 [표 1](a)과 같다. RREQ가 목적 노드까지 전파되는 과정에서 RREQ를 수신한 중간 노드가

목적 노드까지의 경로 정보를 가지고 있다면 중간 노드에서 [표 1](b)의 형식인 RREP 메시지를 생성하여 RREQ를 생성한 소스 노드까지 유니 캐스트 방식으로 전송한다. 그렇지 않을 경우 즉, 목적 노드까지의 경로 정보를 가지고 있지 않은 중간 노드는 RREQ 메시지를 이웃 노드로 다시 브로드캐스팅 한다[3].

[표 1] AODV의 메시지 형식과 라우팅 테이블
[Table 1] The message format of AODV and routing table.

(a) The RREQ message

Type	J	R	G	D	U	Reserved	Hop Count
Broadcast ID							
Destination IP Address							
Destination Sequence Number							
Source IP Address							
Source Sequence Number							

(b) The RREP message

Type	R	A	Reserved	Prefix Sz	Hop Count
Destination IP Address					
Destination Sequence Number					
Source IP Address					
Life Time					

(c) The Hello Message

Type	Length	Hello Interval
Hello Interval	...	

(d) routing Table

Destination IP Address
Destination Sequence Number
Hop Count
Next Hop
Life Time

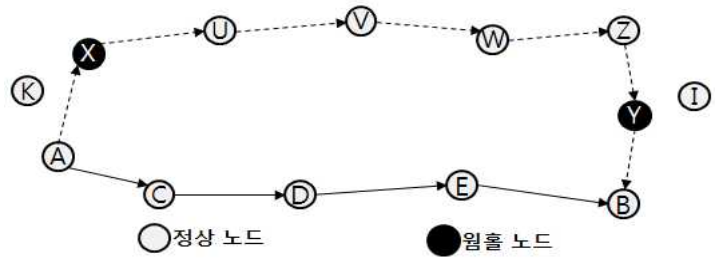
논문에서는 기존의 AODV 라우팅 프로토콜을 사용하고, RREP 메시지와 라우팅 테이블에 이웃 노드목록을 추가하고, Route_ACK 메시지를 설계하고 이 Route_ACK 메시지에 홉 카운트와 이웃 노드목록을 추가하여 이웃노드목록과 홉 수를 이용하여 웜홀 공격과 웜홀 노드를 탐지하도록 설계한다.

2.2 웜홀 공격

2.2.1 캡슐화 웜홀

캡슐화 웜홀 공격은 웜홀 노드가 패킷에 캡슐을 씌워 홉 수를 증가하지 않도록 하는 공격으로 [그림 1]과 같다. A는 송신 노드, B는 수신 노드이고, A와 B의 1 hop 범위 내의 노드 X와 Y가 웜홀 노드라고 하자. A가 B에게 패킷을 전송할 때, 1 hop 거리에 있는 X와 C에게 패킷을 전송하면, X가 패킷에 캡슐을 씌워서 U-V-W-Z 경로를 거쳐서 Y에게 전달하므로 hop 수는 증가하지 않게 된다. Y는 패킷의 캡슐을 풀어서 B에게 전달하므로, 결국 A는 A-X-Y-B라는 경로를 얻게 된다. 또한 A는 A-C-D-E-B라는 정상적인 경로를 얻게 되지만, A는 라우팅 정책에 따라 hop 수가 적은

A-X-Y-B 경로를 선택하므로 비정상적인 패킷 전달이 발생할 수 있다[7-9].

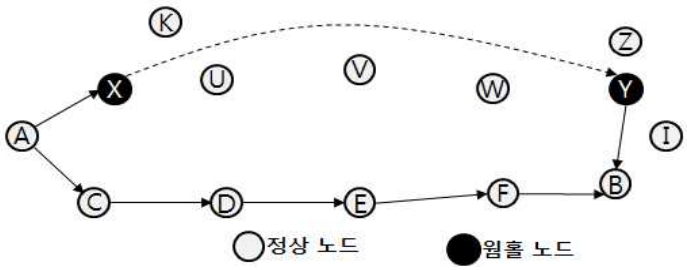


[그림 1] 캡슐화 웜홀 공격

[Fig. 1] Encapsulation Wormhole Attack

2.2.2 터널링 웜홀

터널링 웜홀 공격은 일반적으로 웜홀 노드들 사이에서 외부의 채널을 가지고 실행되는 공격으로 [그림 2]와 같다. A는 송신 노드, B는 수신 노드, X와 Y는 웜홀 노드이라고 할 때, A가 패킷을 전송하면, X가 외부 터널을 통해 Y에게 패킷을 전달한다. 그리고 Y는 패킷을 B에게 전달하므로 A는 A-X-Y-B인 경로를 획득한다. 또한 A는 정상적인 A-C-D-E- F-B인 경로를 획득하지만, 라우팅 정책으로 hop 수가 작은 A-X-Y-B인 경로를 선택한다. 하지만 이 경로에는 웜홀 노드인 X와 Y가 있으므로 패킷의 정상적인 송수신은 불가능하다[7-9].



[그림 2] 터널링 웜홀 공격

[Fig. 2] Tunneling Wormhole Attack

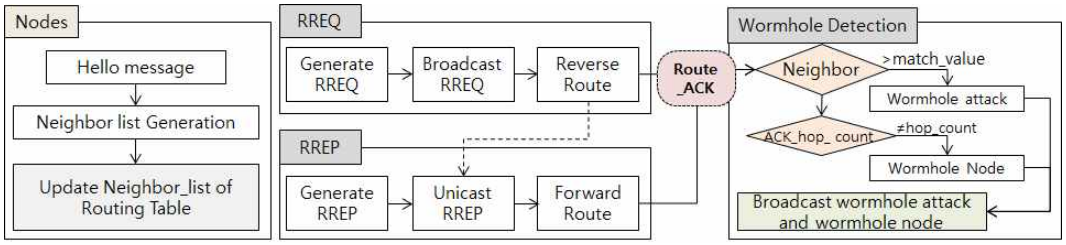
본 논문에서는 이웃노드목록, 홉(hop) 수, Route_ACK를 이용하여 이러한 캡슐화 웜홀 공격과 터널링 웜홀 공격을 탐지하고자 한다.

3. 웜홀 공격 탐지와 웜홀 노드 제거 기법 설계

본 논문에서는 제안하는 웜홀 공격 탐지와 웜홀 노드 제거 기법은 기존의 AODV 라우팅 프로

토콜을 이용하여 메시지 전송 경로를 설정 시에 이웃 노드 목록, 홉 수, Route_ACK를 이용하여 웜홀 공격과 웜홀 노드를 탐지하도록 설계하였다. 이때 AODV의 RREP 메시지와 라우팅 테이블에 이웃노드목록 필드를 추가하였고, 새로운 경로 확정을 알리는 Route_ACK 메시지를 설계하였다.

[그림 3]은 본 논문에서 제안하는 웜홀 공격 탐지와 웜홀 노드 탐지 기법에 대한 전체적인 흐름을 설명한 것이고, [표 2]는 본 논문에서 사용하는 메시지 구조를 설명한 것이다.



[그림 3] 제안하는 웜홀 공격 및 웜홀 노드 탐지 절차

[Fig. 3] The procedure of wormhole attack and wormhole node

[표 2] 이웃노드목록이 추가된 메시지 형식과 라우팅 테이블

[Table 2] The message format and routing table which is appended neighbor node list.

(a) The RREP message

Type	R	A	Reserved	Prefix Sz	Hop Count
Destination IP Address					
Destination Sequence Number					
Source IP Address					
Life Time					
Neighbor_list					

(b) The Routing Table

Destination IP Address
Destination Sequence Number
Hop Count
Next Hop
Life Time
Neighbor_list

(c) The Route_ACK message

Type	Length	Hop Count
Neighbor_list		
ACK_hop_count		

3.1 이웃 노드 목록 생성

본 논문에서는 기존의 AODV 라우팅 테이블에 이웃 노드 목록 필드를 추가하고, 모든 노드들이 주기적으로 브로드캐스트 함으로써 노드가 네트워크에 연결되어 있음을 알리는 Hello 메시지를 이용하여 이웃 노드 목록을 생성하고, 이 목록을 라우팅 테이블의 이웃 노드 목록 필드에 저장하도록 설계한다. 그리고 노드들은 주기적으로 수신하는 Hello 메시지로 자신의 라우팅 테이블에 저장

되어 있는 이웃 노드 목록과 비교하여 라우팅 테이블의 이웃 노드 목록을 갱신하도록 설계함으로써 항상 자신과 연결된 노드들로 이웃 노드 목록을 유지하고, RREP 또는 Route_ACK 메시지를 수신하였을 때, 이 이웃 노드 목록과 비교하여 웜홀 노드를 탐지하는데 이용하도록 설계한다.

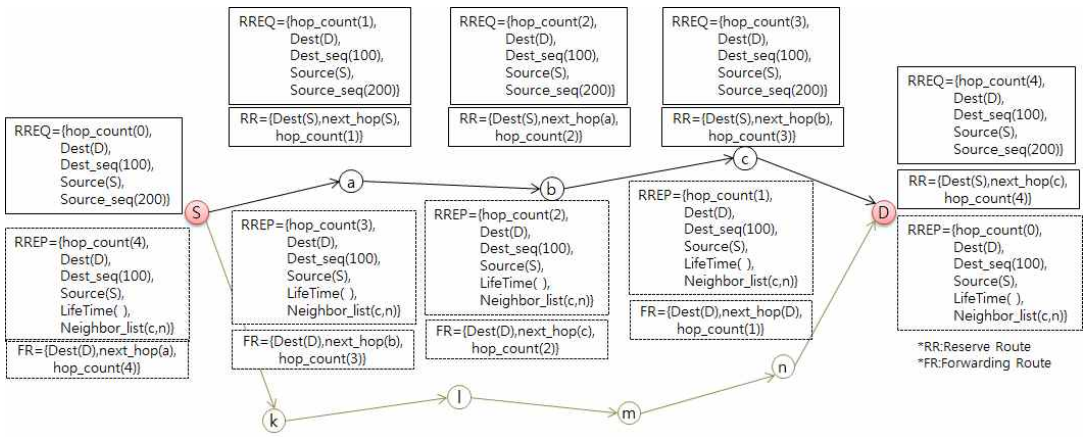
라우팅 테이블의 이웃 노드 목록에 이웃 노드로 추가하거나 삭제하는 조건은 다음과 같다.

첫째, 수신한 Hello 메시지에 대한 정보가 라우팅 테이블의 이웃 노드 목록에 존재하지 않으면, 새로운 이웃으로 판단하여 라우팅 테이블의 이웃 노드 목록에 추가한다.

둘째, 라우팅 테이블의 이웃 노드 목록에 존재하지만 일정한 시간(ALLOWED_HELLO_LOSS * HELLO_INTERVAL)이내에 수신한 Hello 메시지가 없으면, 라우팅 테이블의 이웃 노드 목록에서 제거한다.

3.2 메시지 전송 경로 생성 절차

[그림 4]와 같이 VANET 상의 노드가 배치되어 있을 때, 본 논문에서 제안하는 메시지 전송 경로 생성절차는 다음과 같다.



[그림 4] 메시지 전송 경로 생성 절차

[Fig. 4] The generation procedure of message transmission route

[1단계] 근원지 노드 S는 목적지 노드 D까지의 메시지 전송 경로를 생성하기 위해, RREQ 메시지를 생성하고 브로드캐스트 한다.

RREQ Message = {hop_count(0), Dest(D), Dest_seq(100), Source(S), Source_seq(200)}

[2단계] RREQ 메시지를 수신한 중간 노드 ⓐ는 RREQ 메시지의 목적지 주소를 확인함으로써 자신이 목적지 노드인지를 확인한다. 만약 RREQ 메시지를 수신한 노드가 목적지 노드가 아니면, 중간노드는 라우팅 테이블의 목적지 노드 주소, 목적지 시퀀스 번호, 홉 카운트, 넥스트 홉, Life time을 기록하고, RREQ 메시지를 브로드캐스트 한다.

RREQ Message = {hop_count(1), Dest(D), Dest_seq(100), Source(S), Source_seq(200)}
Routing Table = {Dest(D), Dest_seq(100), hop_count(1), next_hop(S),
Life_time(ACTIVE_ROUTE_TIMEOUT)}
Reverse_Route = {Dest(S), next_hop(S), hop_count(1)}

[3단계] 중간 노드들은 RREQ 메시지가 목적지 노드에 도착할 때까지 2단계를 반복되고, 각각의 중간 노드는 라우팅 테이블을 갱신한다.

중간노드 ⓒ의 경우,
RREQ Message = {hop_count(3), Dest(D), Dest_seq(100), Source(S), Source_seq(200)}
Routing Table = {Dest(D), Dest_seq(100), hop_count(3), next_hop(ⓑ),
Life_time(ACTIVE_ROUTE_TIMEOUT)}
Reverse_Route = {Dest(S), next_hop(ⓑ), hop_count(3)}

[4단계] 목적지 노드 D가 RREQ 메시지를 수신하면, 목적지 노드 D는 라우팅 테이블에 RREQ 메시지에 대한 정보를 기록하고, Reverse_Route를 생성한다. 그리고 난 후에, 목적지 노드 D는 RREQ에 대한 응답 메시지인 RREP 메시지를 생성하고, Reverse_Route의 next_hop 필드가 가리키는 노드 ⓒ로 RREP 메시지를 유니캐스트 한다.

Routing Table = {Dest(D), Dest_seq(100), hop_count(4), next_hop(ⓒ),
Life_time(ACTIVE_ROUTE_TIMEOUT)}
Reverse_Route = {Dest(S), next_hop(ⓒ), hop_count(4)}
RREP Message = {hop_count(0), Dest(D), Dest_seq(100), Source(S),
Life_time(MY_ROUTE_TIMEOUT), Neighbor_list(ⓒ,ⓝ)}

[5단계] RREP를 수신한 노드는 RREP 메시지의 근원지 노드인지를 확인하고, 근원지 노드가 아니면 RREP 메시지의 hop_count를 증가시키고 Forwarding Route를 설정한 후에, Reverse_Route의 next_hop필드가 가리키는 노드로 RREP를 유니캐스트 한다. 이 절차는 RREP 메시지가 근원지 노드 S에 도착할 때까지 반복하여 수행한다. RREP 메시지를 수신한 중간 노드 ⓑ인 경우,

RREP Message = {hop_count(2), Dest(D), Dest_seq(100), Source(S),
Life_time(MY_ROUTE_TIMEOUT),Neighbor_list(ⓒ,ⓝ)}
Forwarding_Route = {Dest(D), next_hop(ⓒ), hop_count(2)}

[6단계] 근원진 노드 S가 RREP 메시지를 수신하면, 근원지 노드 S는 Forwarding_Route를 완성시키고, hop_count가 가장 작은 경로를 메시지 전송경로로 선정한다. 근원지 노드 S의 경우, Forwarding_Route = {Dest(D), next_hop(ⓐ), hop_count(4)}로 설정함으로써 메시지 전송 경로가 Ⓢ-ⓐ-ⓑ-ⓒ-Ⓓ로 설정된다.

3.3 웜홀 공격 탐지 및 웜홀 노드 삭제

본 논문에서는 제안하는 웜홀 공격 탐지 밋 웜홀 노드 제거 기법은 첫째, 3.2절에서 근원지 노드는 목적지 노드로부터 전달받은 RREP 메시지 중에서 이웃노드목록을 이용하여 웜홀 공격을 탐지하고, 둘째, RREP 메시지를 전달받은 근원지 노드가 Route_ACK 메시지를 새롭게 생성된 메시지 전송 경로(NEW_ROUTE)로 전송함으로써 메시지 전송 경로를 알릴 때, ACK_hop_count를 비교하면서 웜홀 노드를 탐지하도록 설계한다.

웜홀 공격 탐지 절차는 다음과 같다.

[1단계] 근원지 노드는 RREP 메시지를 통해 목적지 노드의 이웃노드목록을 전달받는다.

[2단계] 근원지 노드는 메시지 전송 경로를 최종적으로 설정하기 전에, 목적지 노드의 이웃노드목록과 근원지 노드의 이웃노드목록을 비교하여 일치하는 이웃노드의 수를 찾는다.

[3단계] 이때 자신의 이웃노드목록과 일치하는 이웃 노드 수가 클수록 웜홀 노드의 존재 가능성이 높으므로 웜홀 공격이 발생하였다고 판단하고, 모든 노드들에게 새롭게 생성된 경로에 웜홀 공격이 발생하였음으로 브로드캐스트 한다.

[4단계] 근원지 노드는 새로운 RREQ 메시지를 생성하고 브로드캐스트 하여 새로운 경로를 생성한다.

본 논문에서는 웜홀 노드 탐지하기 위해 근원지 노드가 RREP를 수신하였을 때, 본 논문에서 세안하는 Route_ACK 메시지를 새롭게 생성한 경로에 전송함으로써 웜홀 노드를 탐지하도록 설계하였다.

[1단계] 웜홀 공격이 발생하였음을 판단한 근원지 노드는 최종 hop_count와 근원지 노드의 이웃노드 목록을 포함시킨 [표 2]의 Route_ACK 메시지를 생성하고, 근원지 노드는 Route_ACK 메시지를 Forwarding route에 따라 목적지 노드에 유니캐스트 한다.

[2단계] Route_ACK 메시지를 전달받은 중간노드는 ACK_hop_count를 1씩 증가시킨 후에 다음 노드에 전달한다.

[3단계] Route_ACK 메시지를 전달받은 중간노드는 Route_ACK메시지의 ACK_hop_count 값과 라우팅 테이블의 hop_count와 일치하는지를 비교한다. 만약 비교결과가 거짓이면, 이전 노드들 중에 웜홀 노드가 존재한다고 판단하고, 해당 노드가 웜홀 노드임을 알리는 메시지를 모든 노드들에게 브로드캐스트 한다.

[4단계] 웜홀 알림 메시지를 수신한 노드들을 라우팅 테이블과 이웃노드목록에서 웜홀 노드를 제거한다.

[5단계] 만약 경로내의 중간 노드가 웜홀 알림 메시지를 받았다면, RRER 메시지를 근원지에게 전송하여 웜홀노드를 제외시킨 메시지 전송 경로를 재설정한다.

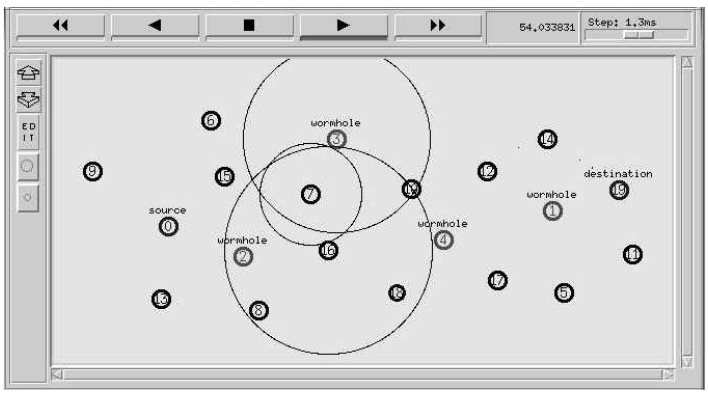
4. 웜홀 공격 탐지와 웜홀 노드 제거 기법 평가

본 논문에서 제안하는 웜홀 공격 탐지와 웜홀 노드 제거 기법은 NS-2[10] Simulator를 이용하였으며, 모의실험 환경 파라미터는 [표 3]과 같이 정상 노드의 수를 16개, 웜홀 노드를 4개로 총 20개, 메시지 전송 범위는 250m이고, Traffic type은 CBR, 패킷 크기는 512byte, 메시지 interval은 3초로 설정하였고 실험시간은 60sec 동안 진행되었다.

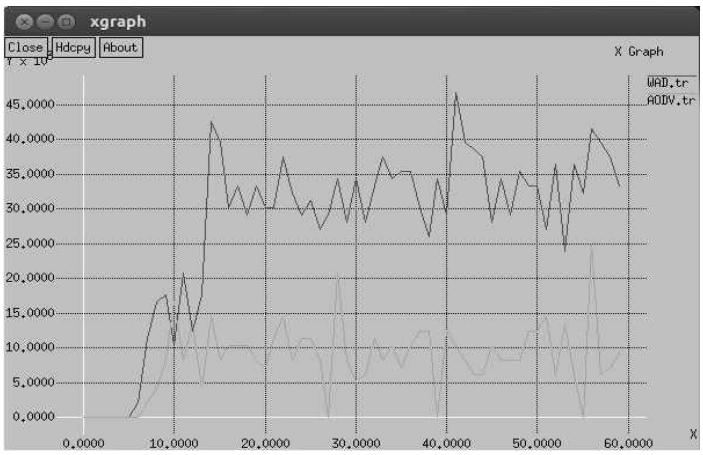
[표 3] 시뮬레이션 파라미터들
[Table 3] Simulation Parameters

Parameters	Values
Simulation Time	60sec
Simulation Area	1000 × 1000m
the number of normal node	16
the number of wormhole node	4
Traffic type	CBR(UDP)
Packet size	512 bytes
Transmission Range	250m
Message interval	3 sec

[그림 5]는 정상 노드, 웜홀 노드, 근원지 노드, 목적지 노드의 배치 상태를 설명하고 있으며, 모의실험에서는 웜홀 노드가 메시지 전송 경로에 포함되어 메시지를 전송할 때, 메시지를 다음 노드에 전달하지 않고 삭제하도록 설정하였다.



[그림 5] 정상 노드와 웜홀 노드의 배치 현황
[Fig. 5] The arrangement status of normal node and wormhole node



[그림 6] 데이터 전송량 비교

[Fig. 6] The comparison of packet transmission quantity

[그림 6]은 본 논문에서 제안한 기법과 기존의 AODV를 이용하여 근원지 노드가 목적지 노드에 메시지를 전송한 결과를 설명한 것으로, 웜홀 노드를 제외한 나머지 노드로 메시지 전송 경로를 생성한 제안 기법의 데이터 전송량이 기존의 AODV보다 평균적으로 약 36%정도 향상되었다. 그 이유는 웜홀 노드가 포함된 AODV의 경우, 웜홀 노드가 메시지를 목적지에 전달하지 않고 메시지를 버리기 때문에 데이터 전송량이 제안한 기법보다 낮게 나타난다.

5. 결론

본 논문에서는 VANET에서 발생할 수 있는 라우팅 공격인 웜홀 공격을 탐지하고 웜홀 노드를 제거하는 기법을 제안한다. 제안하는 웜홀 공격 탐지와 웜홀 노드 제거 기법의 특징은 다음과 같다.

첫째, 제안하는 기법은 RREP 메시지와 라우팅 테이블에 이웃 노드 목록 필드를 추가하여 데이터 전송 경로 설정 시에 이 이웃노드 목록과 hop count를 이용하여 웜홀 공격을 탐지하도록 설계하였다.

둘째, 제안하는 기법에서는 웜홀 노드를 탐지하는 Route_ACK 메시지를 설계하였다.

셋째, 제안하는 기법은 제안된 Route_ACK를 새로운 메시지 전송 경로에 따라 목적지노드에 전달함으로써 메시지 전송 경로 내에 포함되어 있는 웜홀 노드를 탐지하도록 설계하였다.

그 결과, 제안하는 기법은 웜홀 노드를 제외시킨 데이터 전송 경로를 선정함으로써 데이터 전송량이 기존의 AODV에 비해 평균적으로 36% 개선되었으며, 좀 더 안전하고 신뢰성이 높은 VANET 시스템을 구축할 수 있다.

References

[1] S. Corson, and J. Macker, Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations, http://www.ietf.org/rfc/rfc2501.txt, Jun 25 **(2015)**

[2] Aditya Goel and Ajaii Sharma, Performance Analysis of Mobile Ad-hoc Network Using AODV Protocol, International Journal of Computer Science and Security. **(2002)**, Vol.3, No.5, pp.334-343.

[3] EunHee Jeong, and Byungkwan Lee, A SAODV(Secure AODV) Routing Protocol based on GSK(Group Secret Key) to detect a Packet Injection Attack, Journal of Security Engineering. **(2013)** Vol.10, No.6, pp.681-694.

[4] C. E. Perkins and E. M. Royer, Ad-Hoc On-Demand Distance Vector Routing, Proc. 2nd IEEE Mobile Computer Systems and Applications **(1999)**, February 25-26, New Orleans, LA, USA.

[5] C. E. Perkins, E. M. Royer, and S.R Das, Ad hoc on-demand distance vector (aodv) routing, IETF Internet draft, http://tools.ietf.org/html/draft-ietf-manet-aodv-11, Jun 01 **(2015)**.

[6] C.E. Perkins, E. Beliding-Royer, and S. Das, Ad hoc on-demand distance vector (AODV) routing, IETF Internet draft, http://www.ietf.org/rfc/rfc3561.txt, Jun 01 **(2015)**.

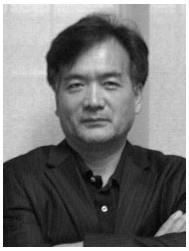
[7] Intae Kim, Seungjin Han and Junghyun Lee, Wormhole Detection using Multipath in Sensor Network, KSCI review. **(2007)**, Vol.15, No.1, pp.77-81.

[8] Issa Khalil, Saurabh Bagehi and Nesss B. Shroff, LITEWORP: A Lightweight Countermeasure for the Wormhole Attack in Multihop Wireless Networks, In Proceedings of the International Conference on Dependable System and Networks, **(2005)**, June 28 – July 1, Yokohama, Japan.

[9] A. VANI and D. Sreenivasa Rao, A Simple Algorithm for Detection and Removal of Wormhole Attacks for Secure Routing In Ad Hoc Wireless Networks, IJCSE. **(2011)**, Vol.3, No.6, pp.2377-2384.

[10] NS-2 simulator, http://www.isi.edu/nsnam/ns/ Jun 20 **(2015)**.

Authors



이병관 (ByungKwan Lee)

1979년 2월 : 부산대학교 기계설계학과 졸업
1986년 2월 : 중앙대학교 전자계산공학과 석사
1990년 2월 : 중앙대학교 전자계산공학과 박사
1988년 3월 ~ 현재 : 가톨릭관동대학교 공과대학 컴퓨터공학과 교수
관심분야 : 네트워크 보안, 인터넷 보안, IoT, 빅데이터

정은희 (EunHee Jeong)

1991년 2월 : 강릉대학교 통계학과 졸업
1998년 2월 : 관동대학교 전자계산공학과 석사
2003년 2월 : 관동대학교 전자계산공학과 박사
2003년 9월 ~ 현재 : 강원대학교 인문사회과학대학 지역경제학과 교수
관심분야 : 인터넷 보안, 전자상거래 보안, IoT, 빅데이터