MANET에서 악의적인 노드 확인에 기반한 Secure 라우팅 방안

박건우* · 변용성* · 이승찬* · 마용재* · 송주석***

*연세대학교 컴퓨터과학과

A Identification of Malicious Node and Secure Communications in MANET

GunWoo Park* · YongSung Byeon* · SeungChan Lee* · YongJae Ma* · JooSeok Song***

Department of Computer Science, YonseiUniversity

요 약

최근 Mobile Ad-hoc Networks(MANET)에서 보안 요소를 추가한 라우팅 연구가 활발히 진행되어 왔다. 하지만 기존 연구들은 대부분 secure 라우팅 또는 패킷 자체에 대한 악의적인 행위가 이루어지는 부분 중 어느 한 측면에 대해서만 연구되어져 왔다. 이와 같은 방법들은 악의적인 노드를 확인하더라도 라우팅 경로 설정과정에서 악의적인 행위가 이루어지거나 라우팅 경로 설정에 대한 공격은 차단하더라고 패킷에 대한 악의적인 행위가 이루어지면 네트워크 내 보안 측면에서 큰 효율성을 기대할 수 없다. 따라서 본 논문에서는 일정기간 악의적인 행위가 이루어지는 노드를 확인하여 각 노드에 대한 신뢰단계를 구성 후, 획득한 각 노드의 신뢰레벨에 따라 라우팅 경로를 설정함으로써 패킷 및 라우팅 경로 설정에 대해 이루어질 수 있는 악의적인 행위를 효율적으로 대응 할 수 있는 방안인 IMSec(A identification of malicious node and secure communications in MANET)을 제안한다. IMSec은 AODV(Ad-hoc On-demand Distance Vector Routing)를 기반으로 하였다. NS-2 네트워크 시뮬레이션 결과를 통해, 제안된 IMSec은 기존 프로토콜보다 네트워크의 부하를 감소시킨 상태에서 악의적인 노드를 더 정확하고 신속하게 찾아냄을 보였다.

I. 서론

MANET은 노드가 신뢰받는 인증기관을 통해 인증 받는 형식이 아니기 때문에, 멀티 홉 방식에 의해 라우팅을 수행 할 경우 악의적인 중간 노드에 의해* 데이터의 무결성 및 기밀성 문제가 발생 할 수 있다. 특히, 매체를 신뢰할 수 없는 상황에서 암호를 사용하므로, 암호키에 크게 의존하게 된다. 또한, 기지국이나 AP(Access Point)와 같은 하부구조가 없고 노드들의 이동성과 무선 채널의 상태 변화에 따라 네트워크의 토폴로지가 매우 자주 변화한다. 이와 같은 특징 때문에 보안 문제가 확실히 해결된다 할지라도 컴퓨팅 문제가 발생된다거나 노드와 네트워크 전체에 심각한 부하를 줄 수도 있게 된다.[1]. 따라서 보안 측면과 네트워크의 효율성 측면에 모두 적합한 알고리즘 구현이 필요하다.

지금까지 MANET에서 라우팅 공격이나 패킷 전송 시 발생 할 수 있는 여러 형태의 악의적인 행위를 효율적으로 탐지하고 대비하기 위한 많은 보안 대책이 연구되어 왔다[2,3,4,5,6,7]. 하지만 대부분의 연구들은 네트워크의 컴퓨팅 보다는 보안 측면에 중점을 두고 있기 때문에 네트워크 오버헤드가 많이 발생한다. 또한 라우팅 경로에 대한 공격 또는 패킷을 버리거나 변경, 거짓 신고 등의 패킷전달에 대한 공격 중 어느 한 측면에만 중점을 두고 있기 때문에 보다 정확하고 효율적으로 악의적인 행위에 대해 대비할 수 없었다.

본 논문에서는 악의적인 행위의 빈도수에 의한 각 노드의 신뢰 레벨을 결정하고 해당 정보를 이용하여 라우팅 경로를 설정함으로써 악의적인 행위에 효율적으로 대응 할 수 있는 방안인 IMSec(A Identification of Malicious Node and Secure Communications in MANET)을 제안한다.

본 연구는 정보통신부 및 정보통신연구진흥원의 대학 IT연구센터 육성·지원사업의 연구결과로 수행되었음

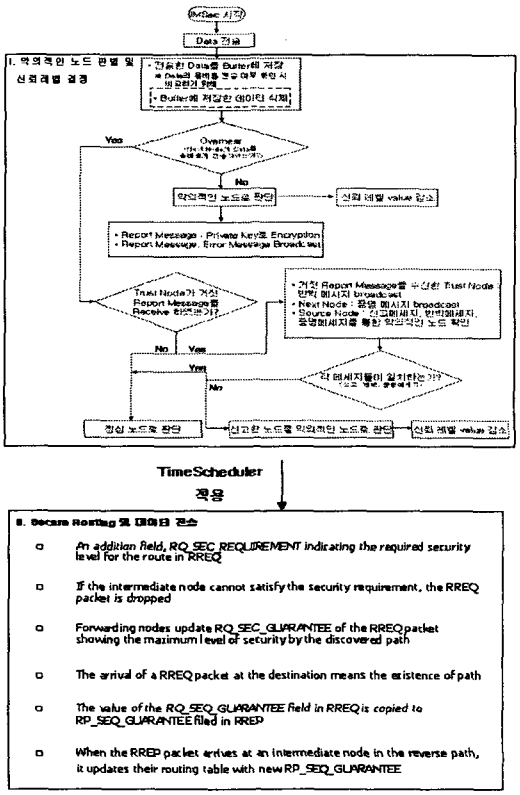
*준 회 원: 연세대학교 컴퓨터과학과 석사과정

***종신회원: 연세대학교 컴퓨터과학과 정교수

2절에서는 제안하는 프로토콜인 IMSec에 대해 자세히 알아보고, 3절에서는 성능 평가를 통해 IMSec의 효율성을 증명해 본다. 마지막으로 4절에서는 결론을 제시한다.

II. IMSec(A Identification of Malicious Node and Secure Communications in MANET)

IMSec은 네트워크 내에서의 보안성을 높이기 위해 두 단계의 과정을 거친다. 첫 번째 단계는 네트워크 내에 존재하는 각 노드들의 신뢰 정도를 판단하기 위한 단계로써 각 노드들의 악의적인 행위를 확인하여 각 노드마다 신뢰 레벨을 결정하는 단계이다. 두 번째 단계는 정해진 신뢰 레벨을 바탕으로 경로를 설정하여 데이터 패킷을 보낸다. IMSec은 AODV를 기반으로 하였으며 동작과정은 그림 1과 같다[8].

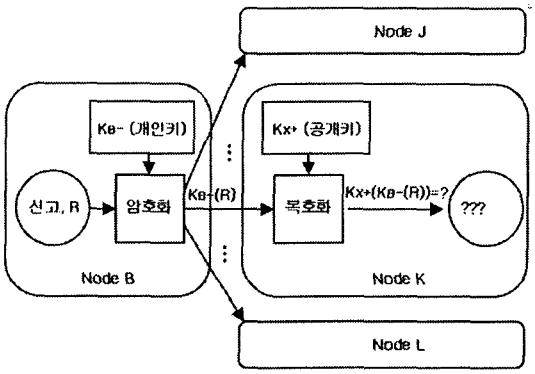


(그림 1) IMSec 동작과정

MANET에 속한 노드는 데이터를 전송 후 전송한 데이터를 버퍼에 저장하고 다음 노드의 전달 과정을 overhear하여 자신이 보낸 메시지와 비교한다. 만약 어떠한 노드를 악의적인 노드라고 판단하게 되면 신고하는 노드는 자신의 개인키로 신고 메시지를 암호화 하여 네트워크 에러 메시지와 함께 broadcast 한다. 신고 메시지는 거짓 신고를 당하는 노드가 overhear 할 수 있기 때문에 거짓 신고를 당하는 노드는 이에 대응하는 반박(retort) 메시지를 broadcast 한다. 이때, 악의적인 노드를 신고하는 메시지와 반박 메시지를 수신한 목적지 노드 또는 반박 메시지를 보낸 노드의 이웃 노드들은 신고와 반박 메시지를 증명하기 위한 증명 메시지를 broadcast 한다. 이와 같은 과정에서 소스 노드는 신고, 반박, 증명 메시지를 모두 수신하게 되며 수신한 모든 메시지를 비교하여 악의적인 노드를 결정한다. 악의적인 노드가 결정되면 소스 노드는 별도의 캐쉬에 해당 노드의 신뢰 레벨을 감소시키고 갱신된 신뢰 레벨을 broadcast 한다.

3.1 악의적인 노드 확인

Case 1 : 다른 노드로 위장하여 거짓신고



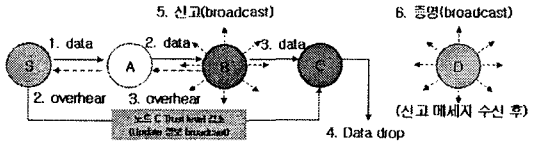
(그림 2) 위장 신고하는 악의적인 노드 확인

개인키와 공개키를 이용한 비대칭 암호방식을 사용함으로 다른 노드의 ID를 이용하여 다른 노드인 것처럼 위장하여 거짓 신고하는 악의적인 노드를 확인한다. 그림 3과 같이 만약 노드 B가 노드 X인 것처럼 위장하여 거짓 신고를 하더라도 노드 B는 노드 X의 개인키를 모르므로 자신의 개인키로 암호화를 한다. 그러면 이 거짓 신고를 수신한 각 노드들은 노드 X의 신고인줄 알고 노드 X의 공개키로 신고 메시지를 복호화 한다. 그렇지만 노드 X의 개인키로

암호화되지 않았으므로 정상적으로 복호되지 않고 오류를 발생시키므로 각 노드들은 이 신고가 잘못된 신고임을 알게 되므로 노드 B는 다른 노드로 위장하여 거짓 신고를 할 수가 없게 된다.

Case 2 : 악의적인 노드의 데이터 버림 및 변경

악의적인 노드가 데이터를 버리거나 변경하는 경우 악의적인 노드의 전송을 overhear 한 노드가 악의적인 노드를 신고하게 된다. 이때, 신고 메시지를 받은 목적지 노드는 증명 메시지를 소스 노드로 보내 신고를 증명한다.



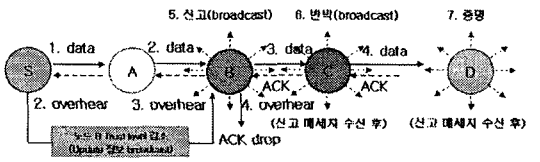
(그림 3) 데이터를 버리는 악의적인 노드 확인

그림 3의 경우 신고 메시지와 증명 메시지를 받은 소스 노드는 신고 메시지의 신고 된 메시지와 증명 노드가 보낸 메시지를 비교하여 노드 C가 목적지 노드에게 메시지를 보내지 않았다는 것을 확인하고 C를 악의적인 노드로 판단한다. 소스 노드는 노드 C에 대한 신뢰 레벨을 감소시키고 갱신된 신뢰 레벨을 이웃노드에게 알린다.

Case 3 : 다른 노드를 임의로 거짓 신고하는 경우

악의적인 노드가 자신의 이웃이 아닌 전혀 상관없는 다른 임의의 노드를 거짓으로 신고할 경우 목적지 노드의 증명 메시지로 목적지 노드가 데이터를 수신한 것을 확인 할 수 있고, 신고를 당한 노드의 반박 메시지로 그의 이웃 노드들이 증명 메시지를 보냄에 따라 악의적인 노드를 판단 할 수 있다.

Case 4 : 정상적인 노드를 거짓 신고하는 경우

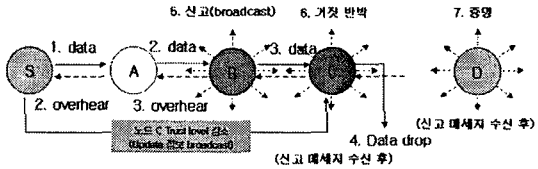


(그림 4) 정상적인 노드를 거짓 신고하는 악의적인 노드 확인

그림 4의 경우 노드 C는 정상적으로 목적지 노드에게 데이터를 보냈지만 악의적인 노드 B는 목적지 노드에게서부터 전송된 ACK 메시지를 버리고 노드 C를 악의적인 노드라고 거짓 신고한다. 이때, 노드 B의 신고 메시지를 수신한 노드 C는 자신이 악의적인 노드가 아님을 반박하는 반박 메시지를 네트워크로 broadcast 하게 된다.

또한, 신고 메시지를 수신한 목적지 노드 역시 증명 메시지를 broadcast 하게 된다. 신고, 반박, 증명 메시지를 모두 수신한 소스 노드는 신고 메시지에 신고 된 메시지와 증명 메시지가 첨부되어 있다면 노드 C는 목적지 노드에게 메시지를 전송 하였다고 판단하고 노드 B를 악의적으로 거짓 신고 한 노드로 판단한다. 따라서 소스 노드는 노드 B에 대한 신뢰 레벨을 감소시키고 업데이트 된 정보를 이웃 노드들에게 알린다.

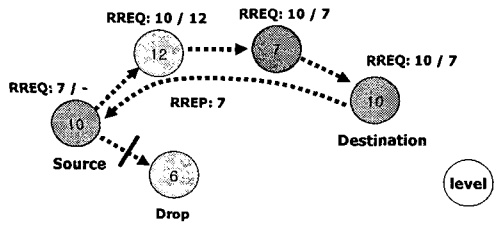
Case 5 : 악의적인 노드의 거짓 반박



(그림 5) 거짓 반박하는 악의적인 노드 확인

악의적인 노드가 자신의 악의적인 행위에 대해 신고 당했을 경우 이를 거짓으로 반박 할 수 있다. 이와 같은 경우 그림 5에서 볼 수 있듯이 노드 B에 의해 신고 된 메시지와 목적지 노드가 수신한 메시지가 다르게 된다. 따라서 노드 C의 반박은 거짓으로 확인되고 노드 C가 악의적인 노드로 판단되어 진다. 이후 소스 노드는 노드 C에 대한 신뢰 레벨을 감소시키고 업데이트 된 정보를 이웃 노드들에게 알린다.

3.2 Secure Routing 경로를 통한 데이터 전송



(그림 6) Secure 레벨이 높은 경로 설정

그림 6과 같이 소스 노드는 악의적인 노드 확인을 통해 구축된 각 노드의 신뢰 레벨을 기반으로 일정 수준의 신뢰 레벨을 요구하여 그에 만족하는 경로를 설정하게 된다. 즉 RREQ를 전송 할 때 신뢰 레벨이 어느 정도 되어야하는지에 대한 정보를 실어 보냄으로써 해당 레벨 이하인 신뢰도를 갖는 노드는 경로 설정 시 제외하고 일정 수준의 신뢰 레벨로 이루어진 노드들로 구성된 경로를 설정하여 데이터 패킷을 전송한다.

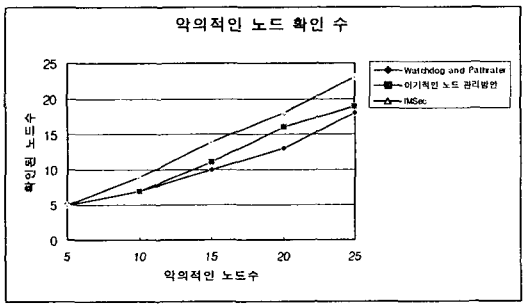
III. 성능평가

여기서는 제안 알고리즘의 성능을 분석하기 위한 시뮬레이션 결과를 제시한다. 시뮬레이션은 ns-2를 사용하였다. 성능 평가는 라우팅 측면에서의 신속성과 정확한 악의적인 노드 판별에 대해 실시하였다.

<표 1> 이동성(mobility) 및 트래픽(traffic) 모델

Terrain Dimensions	1000 * 1000 (m)
Number of Nodes	50
Number of Malicious Nodes	5, 10, 15, 20, 25개
Simulation Time	900 sec
Routing protocol	AODV
Traffic	- CBR - Packet size : 512 Kbytes - Packet Inteval : 5 packet/s
Movement	- Random waypoint - pause Time : 0 ~ 900 sec - speed : min 0, max 25m/s

4.1 악의적인 노드 판별 시간

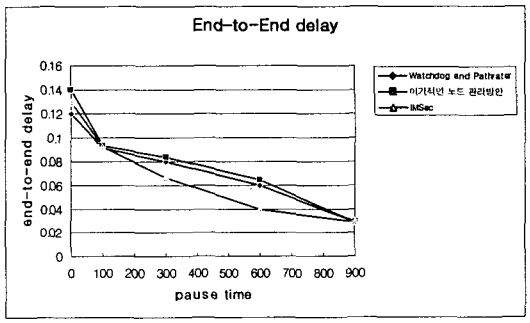


(그림 7) 악의적인 노드 검출 수

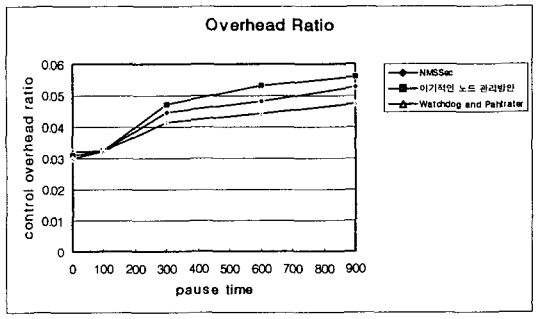
그림 7에서 볼 수 있듯이 기존 연구된 방법들은 악의적인 행위가 계속 이루어지지 않는다는 사실을 간과했고 threshold값을 적용함으로써 일정시간 지속되는 네트워크 수명주기 동안 악의적인 노드 검출이 제대로 이루어지지 않고 있음을 확인 할 수 있다. 하지만 IMSec의 경우 악의적인 행위가 발생하는 즉시 관련 노드를 악의적인 노드로 선별 관리함으로써 네트워크 수명주기 동안 가능한 많은 수의 악의적인 노드가 검출됨을 알 수 있다.

4.2 라우팅 측면의 신속성

기존 연구되었던 방법들은 악의 적인 행위가 이루어 질 때 마다 해당 횟수를 테이블에 저장해 두고 저당된 값이 threshold를 초과하였을 경우 해당되는 노드를 악의적인 노드로 최종 판단한다. 따라서 threshold를 초과하기 전 까지는 악의적인 노드에게 수차례의 메시지를 계속 보내게 됨으로써 라우팅의 신속함이 떨어지게 된다.



(그림 8) End-to-End delay



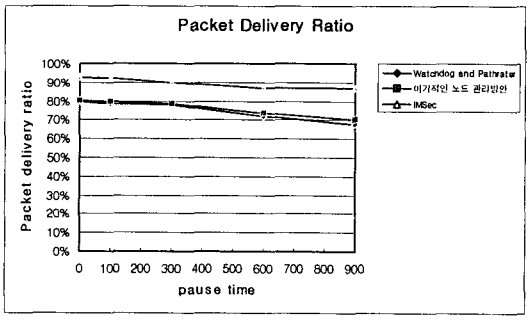
(그림 9) Overhead Ratio

하지만 그림 8,9에서 볼 수 있듯이 IMSec의 경우 어떤 노드가 단 한번의 악의적인 행위를 하더라도 그에 대한 신고, 반박 및 증명이라는 과정을 통해 여러 번의 중복되는 소스 노드의 전송과정을 거치지

않고 악의적인 노드를 판별해 낼 수 있어 오버헤드를 줄이고 더욱 신속하게 올바른 라우팅 과정을 수행 할 수 있다.

4.3 정확한 악의적 노드 판별에 의한 패킷전송

MANET에서 기존의 악의적인 노드 판별 및 차단하는 알고리즘들은 데이터 버림, 데이터 변조 또는 거짓 신고 등과 같은 악의적인 행위가 지속적으로 이루어짐에 따라 threshold를 초과 할 경우 그 노드를 악의적인 노드라고 판단하여 네트워크의 동작에서 제외시킨다. 하지만 실제 네트워크에서 적용 할 때 악의적인 노드는 악의적인 행동을 연속적으로 계속하지는 않을 것이다. 따라서 IMSec은 한번의 악의적인 노드의 올바르지 않은 행동을 차단함으로써 더욱 정확하게 악의적인 노드를 판별하여 효과적으로 라우팅 경로 설정 후 패킷을 정상적으로 전달 할 수 있다.



(그림 10) Packet Delivery Ratio

IV. 결론

MANET은 그 특성상 유선 네트워크에 비해 공격에 매우 취약하다. 따라서 악의적인 노드의 공격으로 데이터가 변조, 손실되거나 라우팅 경로가 회손되었을 경우에 그 피해가 심각하다. 따라서 적극적이고 안전한 보안 대책이 강구되어져야 한다.

제안한 알고리즘은 악의적인 노드 확인 과정에서는 신고, 반박, 증명 메시지를 통해 기존의 신고 테이블 이용 시 증가할 수 있는 오버헤드와 threshold 사용 시 발생 할 수 있는 악의적인 노드 검출 시간 지연 및 에러율을 감소시킴을 확인하였다. 또한 악의적인 행동을 하는 노드의 확인을 통해 각 노드의 신뢰 레벨을 결정하고 신뢰 레벨에 대한 정보 활용을 통해 보안 측면이 양호한 노드가 존재하는 경로를 설정하여 데이터를 전송함으로써 MANET에서 발생할 수 있는 라우팅 공격 양상에 효율적으로 대처할 수 있음을 확인하였다.

[참고 문헌]

[1] Hao Yang, Haiyun Luo, Fan Ye, Songwu Lu, and Lixia Zhang, " Security in Mobile Ad Hoc Networks: Challenges and Solutions", IEEE Wireless Communications, 2004.

[2] S. Marti et al., "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks", ACM MOBICOM, 2000

[3] B. Awerbuch et al., "An On-Demand Secure Routing Protocol Resilient to Byzantine Failures", ACM WiSe, 2002.

[4] 나가진, 도인실, 편혜진, 채기준, "Secure Mechanism to manage selfish nodes in Ad hoc Network", JCCI, 2004.

[5] J.Broch, D.Johnson & D.Maltz, "The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks", http://ietf.org/internet-drafts/draft-ietf-manet-dsr-09.txt, IETF Internet draft, 15 April 2003, Work in progress.

[6] Y. Hu, A. Perring, and D. Johnson, "Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks", ACM MOBICOM, 2002.

[7] Y. Hu, D. Johnson, and A. Perring, "Sead: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks", IEEE WMCSA, 2002.

[8] S.R.Das & C.E.Perkins, "Ad hoc On-Demand Distance Vector(AODV) Routing for Mobile Ad Hoc networks", http://www.ietf.org/rfc/rfc3561.txt, July 2003.