신뢰 모델을 이용한 보안 라우팅 기법에 관한 연구

양 환 석*

요 약

이동 노드로만 구성된 MANET은 응급 상황에서 신속하게 네트워크를 구축할 수 있는 장점 때문에 다양한 환경에 적용되고 있다. 그러나 노드들의 이동으로 인한 동적 토폴로지와 링크 실패는 많은 라우팅 취약점을 노출하고 있으며, 네트워크 성능을 크게 떨어뜨릴 수 있는 요인이 된다. 본 논문에서는 신뢰 모델을 기반으로 한 안전한 라우팅 프로토콜 기법을 제안하였다. 제안한 기법에서는 노드들에 대한 효율적인 신뢰 평가 및 관리를 위해 영역 기반 네트워크 구조를 이용하였다. 노드들의 신뢰 평가는 노드들의 제어 패킷과 데이터 패킷의 폐기 비율 측정을 통해 이루어졌으며, 라우팅의 효율을 높이기 위하여 트래픽 검사를 실시하고 과도한 트래픽을 발생시키는 경로에 존재하는 노드들에 대한 DSN 검사하여 비정상행위 노드를 탐지하였다. 제안한 기법을 통해 경로상에 공격이 존재하더라도 안전하게 데이터 전송이 이루어짐을 실험을 통하여 확인하였다.

A Study on Secure Routing Technique using Trust Model in Mobile Ad-hoc Network

Hwan Seok Yang*

ABSTRACT

MANET composed of only mobile node is applied to various environments because of its advantage which can construct network quickly in emergency situation. However, many routing vulnerabilities are exposed due to the dynamic topology and link failures by the movement of nodes. It can significantly degrade network performance. In this paper, we propose a secure routing protocol based on trust model. The domain-based network structure is used for efficient trust evaluation and management of nodes in the proposed technique. The reliability evaluation of nodes was performed by the discard ratio of control packet and data packet of the nodes. The abnormal nodes are detected by performing traffic check and inspecting of nodes on a path that generates excessive traffic in order to increase the efficiency of routing. It is confirmed through experiments of the proposed technique that data transmission is performed securely even if an attack exists on the path.

Key words : Secure Routing, Trust Model, Abnormally Detection, Mobile Ad-hoc Network

접수일(2017년 9월 30일), 게재확정일(2017년 10월 27일)

* 중부대학교/정보보호학과

1. 서 론

MANET(Mobile Ad-hoc Network)은 어떠한 인프라의 도움없이 이동 노드로만 구성되어 hop-by-hop으로 데이터를 전송하기 때문에 라우팅 프로토콜의 성능이 매우 중요하다[1]. 그러나 동적인 토폴로지와 무선 네트워크의 취약점을 이용한 라우팅 공격은 네트워크 전체를 마비시킬 만큼 위협적이다. 경로상에 존재하는 다양한 공격 등으로 패킷 손실이나 경로 연결 실패가 발생하게 된다면 소스 노드와 목적 노드까지의 새로운 대체 경로를 검색하고 구성하는데 많은 시간이 발생하게 되며, 이로 인한 오버헤드도 크게 된다[2][3]. 따라서 다양한 공격에도 강건한 보안 라우팅 기법은 반드시 필요하다.

본 논문에서는 패킷 폐기 비율 검사를 통한 신뢰도 측정을 이용한 보안 라우팅 및 트래픽과 DSN 검사를 통한 비정상행위 탐지 기법을 제안하였다. 제안한 기법에서는 노드들의 효율적인 신뢰도 평가를 위하여 영역 기반 네트워크 구조를 적용하였으며 각 영역에는 노드들의 신뢰 평가 정보를 관리하는 신뢰 관리 노드(Trust Management Node)를 이용하였다. 각 노드들에 대한 신뢰도 측정은 노드들이 제어 패킷과 데이터 패킷을 정확하게 전달하는지를 검사하여 패킷 폐기 비율이 높은 노드들은 낮은 신뢰도를 갖게 되고 네트워크 참여를 배제시켰다. 그리고 비정상행위 노드 탐지를 위하여 소스 노드와 목적 노드간의 경로상의 트래픽을 검사하고, 해당 경로상에 트래픽이 영역내 평균 트래픽보다 높다면 해당 경로에 존재하는 중간 노드들의 DSN을 검사하여 잘못된 DSN을 이용한 노드나 존재하지 않는 노드 ID에 패킷을 전송하는 비정상행위 노드를 탐지하도록 하였다.

본 논문의 구성은 다음과 같다. 2장에서는 MANET에서의 보안 라우팅 기법에 대하여 살펴보고 3장에서는 본 논문에서 제안한 신뢰 모델 기반 보안 라우팅 기법에 대해 기술하였다. 4장에서는 제안한 기법의 성능 평가를 위해 실험하고 마지막으로 5장에서 결론을 맺는다.

2. 관련연구

2.1 보안 라우팅 기법

MANET에서 라우팅 공격은 패킷의 도청이나 감청에 해당하는 passive 공격과 라우팅 과정에서 잘못된 정보를 삽입, 폐기 또는 변경하는 active 공격으로 나눌 수 있다[4]. 이러한 라우팅 공격을 차단하기 위해 많은 보안 라우팅 기법들이 제안되어 왔다[5].

ARAN(A secure Routing protocol for Ad hoc Networks) 기법은 소스 노드와 목적 노드 사이의 인증과 중간 노드들 사이의 링크 인증을 적용한 기법이다[6]. 소스 노드는 경로 탐색시 RREQ와 인증서를 비밀키로 서명한 후 전송하고 목적 노드는 RREP와 인증서를 비밀키로 서명하여 전달하게 된다. 소스 노드는 목적 노드의 공개키가 있어야만 경로 응답 패킷의 유효성을 확인할 수 있고, 중간 노드들에 대한 검증 과정은 링크간 인증을 제공하는 기법이다. CBSR(Curve Based Secure Routing)은 기존의 CBGR (Curve Based Greedy Routing) 기법에 데이터 암호화를 적용한 기법으로서 경로 설정은 5단계로 이루어진다[7]. 소스 노드는 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. 이러한 과정을 거쳐 라우팅 경로를 설정한다. 목적 노드에서는 여러 경로에서 온 패킷들을 전송받아 내용을 비교하여 변경된 것이 있는지를 판단하게 된다. SEER(Sercure Energy-Efficient Routing) 기법은 정보의 인증을 위하여 단방향 해시 체인을 이용하였다. 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[8].

3. 신뢰 모델 기반 보안 라우팅 기법

3.1 네트워크 구조

MANET은 어떠한 중앙관리 없이 이동 노드로만 구성되어 있기 때문에 네트워크를 구성한 노드들에 대한 신뢰평가 및 관리가 쉽지 않다. 따라서 본 논문에서는 노드들의 신뢰도 관리 효율성을 높이기 위하여 네트워크를 일정 크기의 영역으로 분할한 영역 기반 네트워크 구조를 적용하였다. 각 영역에는 노드들의 신뢰도를 저장 및 갱신하는 신뢰 관리 노드가 있다. 신뢰 관리 노드에서는 영역내 노드들로부터 측정한 이웃 노드들에 대한 신뢰도를 수집한 후 일정 시간 후에 이웃 신뢰 관리 노드들에게 신뢰도 정보를 방송한다. 본 논문에서 사용한 신뢰 모델은 라우팅 과정에서 이웃 노드들에 대한 패킷 폐기 비율을 기준으로 측정하게 된다. 즉, 이웃 노드들이 자신이 수신한 제어 패킷과 데이터 패킷들을 전달하지 않고 폐기한 비율을 측정하여 계산된다. 이렇게 측정된 신뢰도 값은 자신이 속한 영역의 신뢰 관리 노드에게 송신하게 된다. 또한 라우팅 발견 과정에서 DSN 검사를 통해 잘못된 IP DSN을 사용하는 비정상행위 노드 탐지를 제공함으로써 신뢰성 높은 라우팅을 제공할 수 있게 되었다.

3.2 신뢰 모델 및 보안 라우팅

영역내 노드들에 대한 신뢰도 측정은 각 이동 노드의 이웃 노드들에 대해 라우팅 과정에서 이루어진다. 먼저 신뢰도 측정은 제어 패킷 폐기 비율과 데이터 패킷 폐기 비율을 이용하여 계산된다. 먼저 라우팅 과정에서 경로 발견을 위한 제어 패킷들을 전송하는 과정에서 특정 시간동안 이웃 노드들이 제어 패킷을 정확하게 전달하는지 비율을 측정한다. 이는 식 (1)에 의해 계산된다.

$$C(k) = \sum_{i=0}^{t} \frac{D_i(p)}{F_i(p)} \quad (1)$$

여기서 $F_i(p)$는 이웃 노드에 전송된 전체 제어 패킷을 의미하고, $D_i(p)$는 이웃 노드에 의해 폐기된 패킷을 나타낸다. 그리고 데이터 전송시 이웃 노드들에 의해 폐기되는 데이터는 식 (2)에 의해 계산된다.

$$DP(k) = \sum_{i=0}^{t} \frac{Dd_i(p)}{Fd_i(p)} \quad (2)$$

위 식에서 $Fd_i(p)$는 이웃 노드에 전송된 전체 데이터 패킷을 의미하고, $Dd_i(p)$는 이웃 노드에 의해 폐기된 데이터 패킷을 나타낸다. 이렇게 측정된 패킷 폐기 비율에 t 시간동안 이웃 노드에 전송한 제어 패킷과 데이터 패킷의 비율에 따라 가중치 $w1$과 $w2$가 결정되며 노드 k에 대한 신뢰도 값은 식 (3)에 의해 계산된다.

$$T(k) = w1 \bullet C(k) + w2 \bullet DP(k) \quad (3)$$

이렇게 측정된 노드들에 대한 신뢰 정보는 신뢰 관리 노드의 영역 신뢰 테이블(ZTT:Zone Trust Table)에서 관리된다. (그림 1)은 영역 신뢰 테이블 구조를 보여주고 있다.

Node ID	C(k) ratio	DP(k) ratio	Trust Value	Save_Time
S	36	7	0.6	15:12:09
A	5	16	0.81	15:03:11
H	12	22	0.48	15:29:13
D	19	8	0.76	15:07:21

(그림 1) 영역 신뢰 테이블 구조

각 노드들에 대해 측정된 신뢰도를 기반으로 한 라우팅 과정은 다음과 같다. 소스 노드는 목적 노드에 데이터를 전송하기 전에 자신의 라우팅 테이블에서 목적 노드를 검색한다. 만약 존재한다면 신뢰 관리 노드에게 자신의 이웃 노드들 중 신뢰도가 가장 높은 노드의 정보를 받아 해당 노드에게 데이터를 전달하게 된다. 만약 중간 노드에서 신뢰도 값이 임계값보다 작은 이웃 노드가 존재하게 된다면 경로 발견을 위한 RREQ 패킷을 전송하여 신뢰도가 높은 새로운 노드를 찾게 된다. 소스 노드의 라우팅 테이블에 목적 노드까지의 경로를 찾을 수 없다면 RREQ 패킷을 방송하여 목적 노드까지의

경로 발견 과정을 거치게 된다. 발견된 경로 상에 존재하는 노드들의 신뢰도 값을 계산하여 경로 길이 대비 신뢰도 값이 가장 높은 경로를 선택한 후 데이터 전송을 수행하게 된다. 이와 같은 과정을 반복하여 목적 노드까지 경로 설정 및 데이터 전송이 이루어지게 된다. (그림 2)는 목적 노드까지 데이터 전송과정에 대한 의사코드를 보여주고 있다.

```
if(Dest == RoutingTable.find(ip))
{
    if(Node(immediate k) >= theshold(t)) {
        Data.send(Node(immediate k));
    }
    else {
        Broadcast(Dest);
    }
}
else
{
    for(i=0; i<=n; i++) {
        T.path[i] = Broadcast(Dest);
        T.trust[i] = T.path[i]/hop;
    }
    Data.send(Max(T.turst[i]));
```

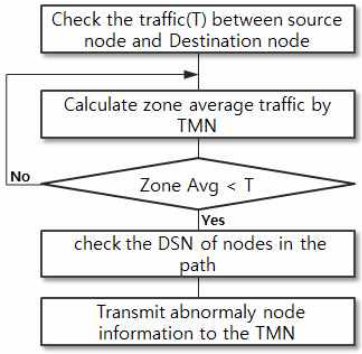
(그림 2) 데이터 전송 의사코드

3.3 비정상행위 탐지

라우팅 과정에서 악의적인 노드의 비정상행위는 블랙홀 공격, 웜홀 공격, 이기적인 행위 등 다양하게 존재하고 이러한 행위로 인해 네트워크 성능은 크게 저하될 수밖에 없다. 따라서 본 논문에서는 라우팅 과정에서 노드들의 비정상행위 탐지를 위하여 크게 두 단계의 과정을 거친다. 먼저 노드에 대한 트래픽 검사를 통해 의심스러운 노드를 탐지하고 해당 노드의 경로 테이블 엔트리에 존재하는 DSN를 통해 비정상행위를 하는 악의적인 노드를 탐지하게 된다. 먼저 t시간 동안 소스 노드와 목적 노드까지의 트래픽을 측정하게 된다. 여기서 t값은 소스 노드와 목적 노드 사이의 RTT(Round Trip Time)를 이용하며, 트래픽의 평균값은 식 (4)에 의해 계산된다.

$$T = \frac{1}{RTT\sqrt{\frac{2B}{3}p + T_0 \min\left\{1, 3\sqrt{\frac{3B}{8}p}\right\} p(1+32p^2)}} \quad (4)$$

여기서 T_0 시간초과, p는 패킷 손실률을 나타낸다. 식 (4)에 의해 측정된 값이 영역의 평균 트래픽 보다 높으면 해당 경로에 악의적인 노드가 존재하는 것으로 판단한다. 그리고 해당 경로에 존재하는 노드들이 전달한 패킷들의 DSN을 검사하여 잘못된 DSN을 탐지하게 된다. AODV는 목적 노드까지 loop-free를 보증하기 위하여 DSN에 의존하기 때문에 잘못된 DSN 검사는 비정상행위 노드 탐지를 위한 중요한 요소이다. 인증서를 발급받은 멤버 노드들이 데이터 전송을 위한 단계에서 발생할 수 있는 공격에 대비하기 위하여 라우팅 정보 검사를 실시하게 된다. 이 과정에서 존재하지 않는 노드 ID에 응답을 하거나 잘못된 DSN을 이용해 패킷을 전송한 비정상행위 노드를 탐지하게 된다. 탐지된 노드의 정보는 신뢰 관리 노드에게 전송하여 신뢰도 값을 0으로 설정하여 해당 노드의 라우팅 참여를 배제시킨다. 위에서 설명한 비정상행위 탐지 과정을 (그림 3)에서 보여주고 있다.



(그림 3) PIT 구조

4. 실험 및 결과

4.1 실험 환경

이 장에서는 신뢰 모델 기반 보안 라우팅 기법의 성능을 평가하였다. 성능 평가를 위해 ns-2 시뮬레이터를 이용하였으며, 실험을 위한 환경설정은 다음과 같다. 실험에 사용한 네트워크 크기는 1500×1500, 실험 시간은 300초로 하였다. 이동 노드 모델은 random-way point 모델이고 0~20 m/s 사이의 속도로 이동한다. 그리고 노드들의 배터리

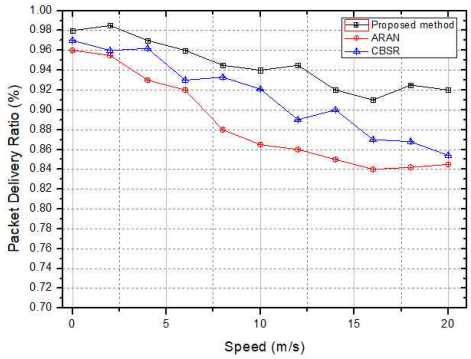
소모는 고려하지 않았다. <표 1>은 실험에 사용한 환경변수를 보여주고 있다.

<표 1> 환경 변수 값

Parameter	Values
Number of Nodes	100개
Routing protocol	AODV
Traffic	CBR
Attack Nodes	10개
Transmission range	150m

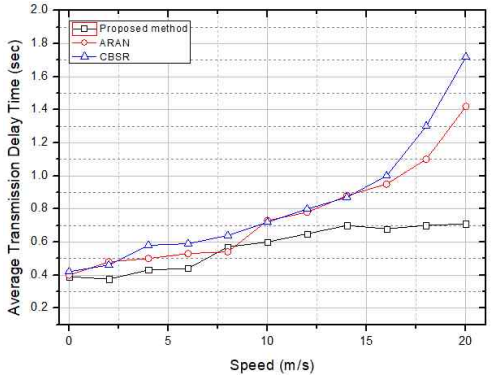
4.2 실험 결과 분석

본 논문에서는 ARAN과 CBSR 기법과 비교 실험을 통하여 제안한 기법의 우수한 성능을 평가를 위하였으며 성능 평가 기준은 패킷 전달 비율, 평균지연시간, 제어패킷의 양으로 하였다.



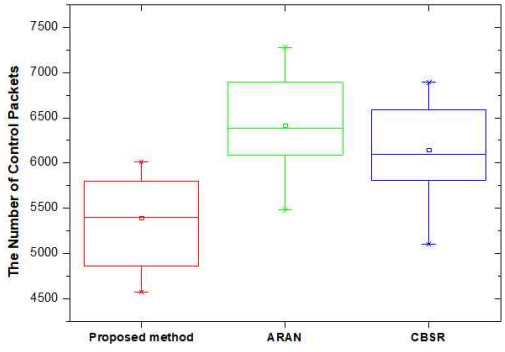
(그림 4) 패킷 전달 비율

(그림 4)에서는 악의적인 노드들에 의한 공격이 존재하는 상황에서 패킷 전달 비율을 측정한 결과를 보여주고 있다. 그림에서 보듯이 ARAN 기법은 노드 인증을 위한 공개키 발급과 인증 서버 선택으로 인해 성능이 좋지 않았으며, CBSR 기법은 목적 노드까지의 다중 경로설정을 적용하여 공격이 발생하여도 전달 비율이 많이 떨어지지는 않았다. 제안한 기법은 노드들의 패킷 폐기 비율을 이용한 신뢰도를 측정하고 경로상의 비정상행위 노드를 탐지하기 때문에 우수한 성능을 보였다.



(그림 5) 평균지연시간

소스 노드에서 목적 노드에 데이터 전송을 위해 걸린 평균지연시간 측정 결과는 (그림 5)에서 보여주고 있다. ARAN 기법은 노드들이 공개키를 소유하고 있어야하며 이를 이용한 인증 단계로 인해 지연시간이 길게 나타났고 CBSR 기법은 위치 정보를 포함시킨 적절한 커브를 패킷에 인코딩을 하는 과정을 거치기 때문에 좋지 않은 결과를 보였다. 제안한 기법은 신뢰관리 노드에 의해 노드들에 대한 신뢰도가 측정되어 관리되기 때문에 일반적으로 소요되는 경로 설정시간 이외에는 지연되는 요소가 존재하지 않은 세 기법중 가장 좋은 결과를 보였다.



(그림 6) 제어 패킷의 양

제어 패킷의 양은 네트워크 전체 성능을 나타낸다. ARAN 기법은 인증 서버와 키 교환 그리고 노드들간의 공개키 공유 때문에 제어 패킷의 양이 많았으며,

CBSR 기법은 위치정보 및 전역 키 교환 과정으로 인해 제어 패킷의 양이 다소 많은 결과를 보였다. 제안한 기법은 노드들의 신뢰도 측정 및 정보 교환으로 인해 제어 패킷의 양이 많은 결과를 보였지만 다른 기법들에 비해 우수한 성능을 보였다.

5. 결 론

라우팅 프로토콜의 성능은 MANET의 전체 성능을 좌우할 만큼 매우 중요하지만 동적인 토폴로지로 인해 많은 보안 위협에 노출되어 있는 실정이다. 본 논문에서는 보안 라우팅 제공 및 비정상행위 노드 탐지를 위하여 신뢰 모델 기반 보안 라우팅 기법을 제안하였다. 제안한 기법은 노드들에 대한 신뢰 측정 및 관리의 효율성을 높이기 위하여 영역 기반 네트워크를 적용하였다. 노드들에 대한 신뢰도 측정은 제어 패킷과 데이터 패킷의 폐기 비율을 측정하였다. 그리고 노드가 송신하는 전체 패킷 중에서 제어 패킷과 데이터 패킷의 비율을 고려한 가중치를 적용하였다. 또한 비정상행위 노드 탐지를 위해서 소스 노드와 목적 노드간의 경로상의 트래픽을 측정하였다. 특정 경로에서 발생하는 트래픽이 영역내 평균 트래픽보다 높다면 해당 경로에 존재하는 노드들이 송신하는 패킷의 DSN을 검사하여 잘못된 DSN을 송신한 노드를 비정상행위 노드로 간주하여 신뢰 관리 노드에게 해당 노드의 정보를 제공하여 해당 노드를 악의적인 노드로 여겨 네트워크 참여를 배제시키도록 하였다. 본 논문에서 제안한 기법의 성능을 평가하기 위하여 ARAN 기법, CBSR 기법과 비교 실험하였으며, 제안한 기법이 우수한 성능을 보임을 확인할 수 있었다.

참고문헌

[1] Misra, S., Krishna, P.V. and Abraham, K.I. “A stochastic learning automata-based solution for intrusion detection in vehicular ad-hoc networks,” Security and Communication Networks, Vol. 4, No. 6, pp.666-677, 2011.

[2] Jha, V., Khetarpal, K. and Sharma, M. “A survey of nature inspired routing algorithms for MANETs,” Proceedings of the 3rd International Conference on Electronics Computer Technology, 8-10 April, Kanyakumari, India, pp.16-24, 2011.

[3] Chen, Y. R., L. Yu, Q. F. Dong, Z. Hong. “Power Control in Wireless Sensor Network Based on Nearest Neighbor Algorithm,” J. Zhejiang Univ. Eng Sci., Vol. 44, pp. 1321-1326, 2010.

[4] Abusalah, L., Khokhar, A., & Guizani, M. “A survey of secure mobile ad hoc routing protocols,” IEEE Communications Surveys & Tutorial, 10(4), pp. 78-93, 2008.

[5] Goyal, T., Batra, S., & Singh, A. “A literature review of security attack in mobile ad-hoc networks,” International Journal of Computer Applications, 9(12), pp. 11-15, 2010.

[6] Zapata, M. G. & Asokan, N. “Secure ad hoc on-demand distance vector (SAODV) routing,” ACM Mobile Computing and Communications Review, 3(6), pp. 106-107, 2002.

[7] Taneja S., & Kush, A. “A survey of routing protocols in mobile ad hoc network,” International Journal of Innovation, Management and Technology, 1(3), pp. 279-285, 2010.

[8] Tomar, P., Suri, P. K., & Soni, M. K. “A comparative study for secure routing in MANET,” International Journal of Computer Applications, 4(5), pp. 17-22, 2010.

〔저자소개〕

양 환 석 (Hwan-seok Yang)
1998년 2월 조선대학교 이학석사
2005년 2월 조선대학교 이학박사
2007년 3월 호원대학교 연구교수
2011년 9월 ~ 현재 중부대학교 정보보호학과 조교수
email : yanghs@joongbu.ac.kr