디지털산업정보학회 논문지 제13권 제2호-2017년 6월
http://dx.doi.org/10.17662/ksdim.2017.13.2.043

MANET에서 보안 경로와 안전한 데이터 전송을 위한 신뢰 기반 라우팅 기법에 관한 연구

양 환 석*

A Study on Trusted Routing Scheme for Secure Path and Secure Data Transmission in MANET

Yang Hwanseok

〈Abstract〉

Recently, MANET has been used in many fields as the range of applications increases. However, the dynamic topology that MANET has makes it difficult to route and provides the cause of exposure to security vulnerabilities. Therefore, the security features that can be robust to many attacks must have been applied in the routing technique provided in the MANET. In this paper, we propose a secure routing method that secure route is established by reliability evaluation of nodes and secure data communication has applied through key exchange mechanism. The proposed technique used hierarchical structure for efficiency of reliability evaluation of nodes. The reliability of nodes is performed by trust management node and reliability of nodes managed periodically is broadcasted. And the key exchange for secure data transmission is dene without CA as the certificate issuing organization. This allows fast key exchange and the integrity of data transmission improved. The proposed technique improves the security of the data transmission because a secure route to the destination node is established by the reliability evaluation and the data transmission is performed after the key between the source node and the destination node is exchanged through the established route.

Key Words : Secure Routing, Routing Attacks, Trust Evaluate Technique, MANET

Ⅰ. 서론

무선 네트워크의 빠른 발전과 이동 단말의 보급이 광범위하게 진행되면서 MANET의 활용 범위가 네트워크 구성이 어려운 긴급 재난 등의 상황에서 다양화되고 있다[1]. 하지만 MANET은 무선 이동 노드들로만 구성되어 있고 어떠한 고정된 인프라도 없기 때문에 많은 보안 취약점에 노출되어 있다. 특히 노드들의 이동으로 인한 동적인 토폴로지와 무선

* 중부대학교 정보보호학과 조교수

네트워크의 특성으로 인해 보안 라우팅 기법은 절실히 필요하다[2]. 그 동안 보안 라우팅을 위해 많은 연구들이 진행되어 왔지만, Blackhole, Wormhole 등과 같은 공격으로 인한 침해 발생이 빈번히 발생하고 있다. 따라서 MANET의 신뢰성을 높이기 위해서는 보다 안전하고 효율적인 보안 라우팅 기법에 대한 연구가 반드시 필요하다.

본 논문에서는 노드들의 신뢰도 평가 기반 보안 경로 설정 및 키 교환을 통한 보안 데이터 통신을 제공하여 보안 라우팅의 성능을 향상시키기 위한 신뢰도 기반 보안 라우팅 기법을 제안하였다. 제안한 기법에서는 노드들의 신뢰도 평가를 위해 계층 구조인 클러스터 형태를 이용하였으며, 신뢰도 평가는 모든 노드에서 자신의 이웃 노드들의 패킷 포워딩 비율을 측정하여 이루어지도록 하였다. 신뢰 관리 노드는 각 클러스터내의 이동 노드들에 대해 측정된 신뢰도를 관리하는 역할을 수행하고, 이를 기반으로 소스 노드와 목적 노드간의 경로를 설정하게 된다. 소스 노드와 목적 노드는 보다 안전한 데이터 통신을 위하여 서로 키를 생성하고 교환하는 과정을 거쳐 CA 없이 키를 이용한 암호화된 데이터 통신을 수행하게 된다. 이러한 과정을 거쳐 데이터 전송에 무결성을 높였으며 악의적인 노드들의 네트워크 참여를 배제시킴으로써 보안 라우팅의 성능을 향상시킬 수 있게 되었다. 본 논문에서 제안한 신뢰 기반 보안 라우팅 기법의 성능은 실험을 통하여 성능을 확인할 수 있었다.

본 논문의 구성은 다음과 같다. 2장에서는 MANET에 존재하는 라우팅 공격의 종류 및 보안 라우팅 기법들 대하여 살펴보고 3장에서는 본 논문에서 제안한 신뢰 기반 보안 라우팅 기법에 대하여 설명하였다. 4장에서는 실험을 통해 제안한 기법의 성능을 확인하고 마지막으로 5장에서는 결론을 맺는다.

Ⅱ. 관련연구

2.1 라우팅 공격의 유형

MANET은 중앙 관리 노드가 없이 이동 노드로만 구성되어 hop-by-hop에 의한 데이터 전송이 이루어지기 때문에 라우팅을 이용한 다양한 공격들에 노출되어 있다. MANET의 라우팅 공격은 악의적인 패킷 주입으로 경로의 단절과 혼란을 야기시키는 active attack과 패킷에 대한 불법적인 도청, 감청을 하는 passive attack이 있다[3-4]. 다음 공격은 대표적인 라우팅 공격들이다. Hello flooding 공격은 공격 노드가 신호 강도가 높은 Hello 패킷을 송신하여 이를 수신한 노드가 공격 노드가 자신의 이웃 노드라고 판단하게 만들어 공격 노드에게 패킷을 송신하게 만드는 공격이다. 이 패킷을 수신한 공격 노드가 패킷을 삭제하여 네트워크를 혼란에 빠뜨리게 한다[5]. Wormhole 공격은 두 개의 악의적인 노드가 정상적인 라우팅 경로보다 짧은 것처럼 속여 데이터 패킷의 도청이나 선택적 포워딩 공격과 같이 활용된다. 이 공격은 두 공격 노드가 서로 떨어진 거리를 다른 노드들에게 실제보다 짧게 보이기 위해 협력하며, 이는 채널을 이용해 패킷을 중계하는 방법을 사용한다[6]. Sybil 공격은 공격 노드가 여러 개의 ID를 생성하여 다른 노드들에게 여러 식별자로 인식하도록 하는 공격으로서 지리적 정보를 이용하는 라우팅 기법에는 매우 위협적이다[7]. Jellyfish 공격은 소스 노드와 목적 노드간의 경로가 설정될 때까지는 정상적으로 RREQ와 RREP를 전송해주며, 자신을 거치는 경로가 설정되고 데이터 전송이 시작되면 패킷 전송을 지연시켜 데이터 전송에 방해를 주는 공격이다.

2.2 보안 라우팅 기법

MANET은 소스 노드와 목적 노드 중간에 존재하는 노드들의 데이터 전달에 의해 이루어진다. 따라서 데이터 전달에 참여하는 노드들의 역할이 매우 중요하며 이 과정에 의해 네트워크 성능이 좌우된다. 하지만 악의적인 노드들에 의해 데이터 전송의 지연 및 패킷 폐기 등과 같은 공격이 발생하면 커다란 피해가 발생할 수밖에 없다. 따라서 경로 설정을 위한 라우팅 기법에는 악의적인 노드를 차단하기 위한 보안 기법이 반드시 적용되어야 한다. SAODV(Secure Ad hoc On-Demand Vector) 기법은 MANET에서 대표적인 라우팅 기법으로서 RREQ와 RREP 인증을 위해 전자서명을 사용하고, 해시 체인을 이용하여 홉을 인증한다. 먼저 최대 홉 수를 설정하고 홉 수 보다 1이 큰 단방향 해시 함수를 만든 후 Seed값을 해시 함수를 통해 변환시킨 RREQ를 생성하여 전달한다. RREQ를 수신한 노드들은 RREQ 패킷을 인증하고 맞으면 같은 방법으로 RREP를 생성하여 전송하게 된다. 이러한 방법으로 RREQ와 RREP에 대한 서명 검사를 통해 안전한 경로를 설정하게 된다[8]. SAR 기법은 노드의 신뢰 수준에 따라 보안 경로를 설정하는 방법이다[9]. 즉, 소스 노드와 목적 노드 사이에 신뢰 수준이 낮은 노드가 발견되면 해당 경로를 이용하지 않고 새로운 보안 경로를 통해 데이터를 전송하는 방법이다. 경로를 탐색하기 위해 송신하는 RREQ 메시지에 각 노드의 신뢰 수준을 포함시켜 문제가 있는 노드는 사전에 경로 설정에서 배제시키는 방법을 이용한다. Ariadne 기법은 DSR 기반 보안 라우팅 기법으로서 MAC와 공유키를 이용한 인증을 사용한다[10]. 소스 노드가 목적 노드까지 경로를 탐색하기 위해서 공유된 비밀키를 이용하여 MAC 값을 생성하여 이를 RREQ에 포함시킨다. 이를 수신한 목적 노드는 RREQ 패킷을 인증하고 이에 대한 RREP 메시지를 송신하면 이를 소스 노드에서 인증하게 된다. 이러한 과정을 통해 소스 노드와 목적 노드와 안전한 보안 경로를 설정하게 된다.

Ⅲ. 신뢰 기반 보안 라우팅 기법

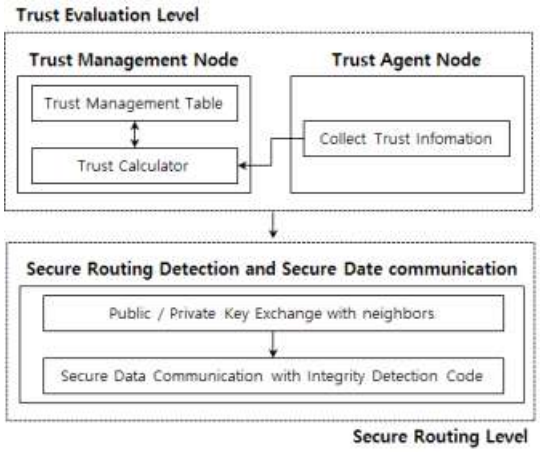
본 장에서는 네트워크에 참여하는 모든 노드들의 신뢰도 평가 및 이를 기반으로 한 보안 경로 설정과 CA의 도움 없이 노드들 간의 키 교환을 통한 보안 데이터 통신이 이루어지는 신뢰 기반 보안 라우팅 기법에 대하여 설명한다.

3.1 제안한 시스템 모델

본 논문에서 제안한 신뢰 기반 보안 라우팅 기법은 네트워크에 참여하는 전체 노드들에 대한 신뢰도 평가와 보안 경로 설정을 위해 계층 구조를 이용하였다. 즉, 각 영역에 있는 노드들의 측정된 신뢰도를 관리하고 그 정보를 제공하기 위한 신뢰 관리 노드와 신뢰 관리 노드를 보조하면서 각 이웃 노드들에 대한 신뢰도를 수집하는 신뢰 에이전트 노드로 이루어져 있다. 본 논문에서 제안한 신뢰 기반 보안 라우팅 기법은 크게 신뢰 관리 모듈, 보안 경로 모듈, 보안 데이터 통신 모듈 세 개의 모듈로 구성되어 있다. 첫 번째 신뢰 관리 모듈은 각 클러스터내의 신뢰 에이전트에 의해 수집된 노드들의 신뢰도 값을 저장하고 주기적으로 이웃 신뢰 관리 노드와 저장되어 있는 신뢰도 정보를 업데이트하게 된다. 노드들에 대한 신뢰도 측정은 이웃 노드들로부터 수신한 트래픽의 양을 기초로 하여 이루어지고, 해당 트래픽이 이웃 노드에 의해 생성된 패킷인지 포워딩 되었는지를 검사하게 된다. 두 번째 보안 경로 모듈은

소스 노드에서 목적 노드까지의 경로 설정시 측정된 신뢰도를 기초로 한 보안 경로 설정을 수행하게 된다. 세 번째 보안 데이터 통신 모듈은 노드들간의 안전한 데이터 통신을 위하여 소스 노드와 목적 노드간의 키 교환 이후 데이터 통신이 이루어진다. 특히 이러한 키 교환은 CA의 존재없이 라우팅 프로토콜의 보안을 제공하기 위한 기법으로서 노드들의 무결성과 부인방지를 제공할 수 있게 된다. 특히 CA로 부터의 인증서 발급과정이 없기 때문에 보다 신속한 인증 과정을 수행할 수 있으며, 인증서 관리 문제를 해결할 수 있게 되었다.

<그림 1>는 본 논문에서 제안한 신뢰 기반 보안 라우팅 기법의 시스템 구조를 보여주고 있다.



<그림 1> 신뢰 기반 라우팅 시스템 구조

3.2 신뢰도 측정 및 보안 경로 설정

MANET을 구성하는 모든 노드들에 대한 효율적인 신뢰 평가 및 관리를 위하여 본 논문에서는 계층형 네트워크 구조를 사용하였다. 먼저 전체 네트워크는 클러스터 구조를 이용하였다. 각 클러스터 내에서 노드들과의 연결수가 가장 높은 노드를 신뢰 관리 노드로 지정하였으며, 이 노드는 각 클러스터 내의 노드들의 신뢰도 값을 관리한다. 그리고 신뢰도가 저장되어 있는 클러스터 신뢰 테이블(CTT:Cluster Trust Table)을 주기적으로 인접한 클러스터의 신뢰 관리 노드와 정보를 주고받으면서 업데이트를 수행한다. 각 클러스터내의 노드들에 대한 신뢰도 측정은 신뢰 에이전트 역할을 담당하는 모든 노드들에서 이루어진다. 즉, 신뢰도 측정은 각 노드에서 포워딩하는 패킷의 비율을 이용하여 계산된다. 그러나 패킷의 전달은 트래픽 증가, 무선 네트워크의 통신 상태, 악의적인 공격 등 다양한 상황에 따라 제대로 이루어지지 않을 수 있다. 따라서 신뢰도 측정의 신뢰성을 높이기 위하여 패킷 포워딩의 질을 평가에 반영하였다. 먼저 신뢰도를 측정하기 이해서는 이웃 노드들에 대한 모니터링을 통해 자신이 이웃 노드로부터 수신한 패킷에 대해 다음과 같은 내용을 분석한다. 먼저 수신한 패킷의 IP 헤더를 검사하여 해당 패킷이 이웃 노드에 의해 생성된 패킷인지 아니면 이웃 노드도 포워딩을 한 패킷인지 여부를 검사한다. 그런 후 이웃 노드로부터 수신한 패킷의 양을 기초로 하여 패킷을 전달한 이웃 노드에 대한 신뢰도를 식 (1)에 의해 계산된다.

$$T(i) = \alpha \frac{F_i(p_j)}{G_i(p_j)} \times \beta \frac{F_i(D_j)}{G_i(D_j)} \qquad (1)$$

여기서 α와 β는 노드들이 네트워크에 참여한 시간에 따른 가중치를 나타내고, $G_i(p_j)$는 노드 j에서 생성한 패킷을 노드 i에게 전달한 패킷을 의미하며, $F_i(p_j)$는 노드 j에서 노드 i에게 전달한 패킷을 의미한다. 그리고 $G_i(D_j)$는 노드 j에서 생성한 패킷을 노드 i에게 전달한 데이터의 양을 의미하며, $F_i(D_j)$는 노드 j에서 노드 i에게 전달한 데이터의 양을 의미한다. 이는 특정 노드에 의해 생성된 데이터와 전달되는 패킷을 계산하여 노드들이 얼마나 이기적인 행동을 하는지를 판단하여 신뢰도를 계산

하였다.

소스 노드와 목적 노드간의 보안 경로는 위에서 언급한 방법으로 계산된 각 노드들에 대한 신뢰도를 기반으로 설정된다. 네트워크 참여하는 모든 노드들에 대한 신뢰도 정보는 신뢰 관리 노드에서 신뢰 정보 테이블(TIT:Trust Information Table)에 저장되어 있다. <그림 2>는 신뢰 정보 테이블의 구조를 보여주고 있다.

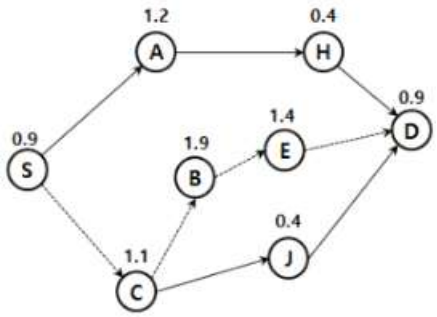
<표 1> 신뢰정보 테이블

Node ID	Neighbor Node	Trust Value	Save_Time	Cluster ID
i	j	1.9	07:11:09	C_2
	k	1.2	07:13:42	C_1
s	c	1.4	06:59:13	C_1
	i	0.9	07:07:54	C_3

<표 1>에서 보듯이 노드 i에 대한 신뢰도는 노드 i로부터 패킷을 수신한 모든 이웃 노드들, 노드 j와 노드 k에 의해 계산된 값이 저장되어 있다. 이렇게 각각의 이웃 노드들에 의해 측정된 신뢰도 값은 식 (2)에 의해 다시 계산된다.

$$T(K) = avg\,(\sum_{i=0}^{n} T_i(K)) \qquad (2)$$

소스 노드(S)는 목적 노드(D)까지 경로를 설정하기 위하여 RREQ 메시지를 방송하게 된다. 이 메시지를 수신한 노드들은 목적 노드까지 패킷을 전달하게 되고, RREQ의 응답을 통해 목적 노드까지의 여러 경로가 찾게 된다. 소스 노드에서는 응답을 통해 얻은 목적 노드까지의 여러 경로들 중에서 신뢰도 값이 가장 높은 경로를 데이터를 전송하기 위한 보안 경로로 설정하게 된다. <그림 2>는 신뢰도 기반 경로 설정의 예를 보여주고 있다. 그림에서 보여주듯이 소스 노드(S)에서 목적 노드(D)까지의 경로는 경로 1인 S->A->H-->D와 경로 2인S->C->B->E->D가 있다. 경로의 길이는 경로 1이 짧지만 전체 경로의 평균 신뢰도 값은 경로 2가 높다. 따라서 신뢰도를 기반으로 설정된 보안 경로는 반드시 최단 경로가 되지는 않는다.

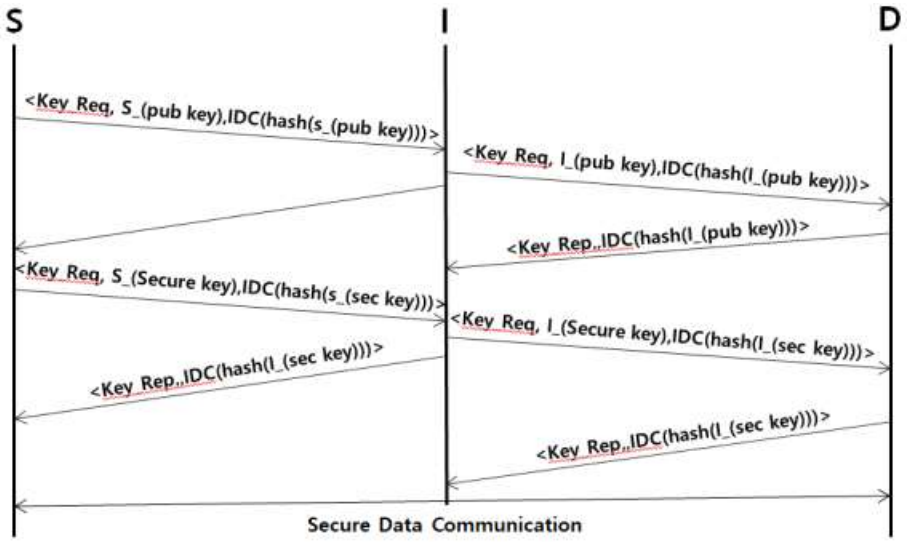


<그림 2> 신뢰도 기반 경로 설정

3.3 보안 데이터 전송 기법

앞 절에서 언급한 방법으로 소스 노드와 목적 노드 사이에 보안 경로를 설정한 후 안전한 데이터 전송을 위하여 키 교환 기법을 적용하였다. 이는 보안 경로 설정을 위해 노드들에 대한 신뢰도 검사 및 이를 기반으로 경로를 설정했지만 이러한 과정을 통해서 악의적인 노드를 완벽하게 배제할 수는 없기 때문에 보안성과 데이터 전송의 무결성을 높이기 위해 적용하였다. 그리고 인증서 발급을 위한 CA (Certificate Authority)의 존재 없이 노드들 간의 키 교환을 통해 신속한 보안 기능을 제공해준다. 노드들간의 키 교환은 다음과 같은 방법으로 이루어진다. 먼저 소스 노드는 보안 데이터 전송을 위해 설정된 보안 경로의 노드들에게 자신의 공개키와 공개키 해시 서명을 송신한다. 패킷을 수신한 목적 노드는 공개키와 공개키의 무결성 검사 코드(IDC: Integrity Detection Code)를 포함하는 응답 메시지

를 전송한다. 이렇게 공개키 정보 교환이 완료되면 소스코드는 공유키를 생성하여 목적노드의 공개키로 암호화하여 전송한다. 그리고 소스 노드는 목적노드에게 전공하고자 하는 데이터를 공유키로 암호화하여 전송하게 된다. 이러한 기법을 통해 데이터 전송의 안전성과 무결성을 높이게 된다. 앞에서 설명한 과정은 <그림 3>에서 보여주고 있다. 그림에서 Key_Req는 는 키 동의 요청, S_(pub_key)는 소스 노드의 공개키, IDC(hash(S_(pub_key)))는 자신의 공개키에 대한 무결성 검사 코드를 의미한다. Key_Rep는 는 키 동의 응답, S_(sec_key)는 소스 노드의 비밀키, IDC(hash(S_(sec_key)))는 자신의 비밀키에 대한 무결성 검사 코드를 의미한다.



<그림 3> 노드간 키 교환 과정

Ⅳ. 모의실험 및 결과

4.1 실험 환경

본 장에서는 신뢰 기반 라우팅 기법의 성능을 평가하기 위하여 NS-2 시뮬레이터를 이용하여 다음과 같은 모의실험 환경에서 실험하였다. 이동 노드는 네트워크를 자유롭게 이동하면서 위치를 임으로 변화시키는 random way point 모델로서 50개를 이용하였다. 전체 모의실험 시간은 600초로 하였다. 실험 시간동안에 Hello flooding 공격과 Jellyfish 공격을 각각 10번씩 발생시켰다. <표 2>에서는 모의실험을 위해 사용한 환경변수들을 보여주고 있다.

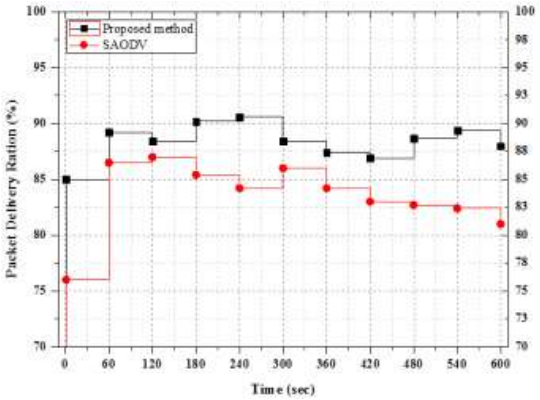
<표 2> 실험에 사용한 환경 변수

Parameter	Value
Transmission Range	250m
Network Size	1000m × 1000m
MAC Protocol	IEEE 802.11 DCF
Packet Size	512 bytes
Speed	0~20 m/s
Traffic Type	CBR/UDP

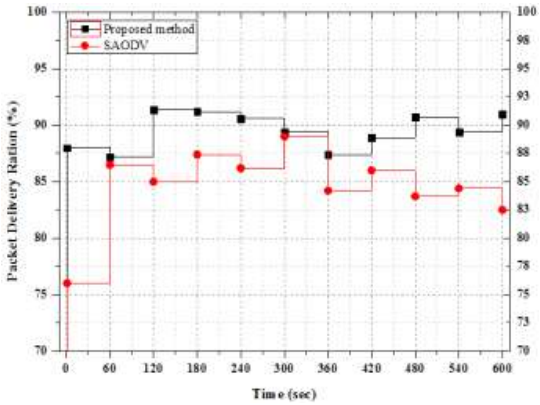
4.2 실험 결과

본 논문에서는 SAODV기법과 비교 실험을 통하여 본 논문에서 제안한 라우팅 기법의 성능을 평가하였으며, 성능 평가 기준은 공격 발생 유무에 따른 PDR(Packet Delivery Ratio), 종단간 지연시간, 경로 선택 시간을 성능 평가 기준으로 설정하였다.

<그림 4>에서는 라우팅 프로토콜의 주요한 성능 평가 기준인 PDR에 대한 측정 결과를 보여주고 있다. 그림에서 보듯이 공격이 존재하지 않을 때는 두 개의 기법이 성능 차이가 나지 않았으나 공격이 존재하는 경우에는 두 기법에 성능차이가 큰 것을 확인할 수 있었다. 먼저, Hello flooding 공격에 대해서 SAODV는 좋은 성능을 보여주었다. 즉 공격 노드가 발생한 Hello 패킷을 수신해도 RREP에 대한 인증 과정을 거치기 때문에 공격 노드를 경유하는 경로 설정을 피할 수 있기 때문에 우수한 성능을 보여주었다. 하지만 Jellyfish 공격을 발생한 상황에서는 SAODV 기법의 성능은 좋지 않았다. SAODV 기법은 경로 발견을 위한 RREQ와 RREP에 대한 인증을 수행한 후 경로를 설정하고 데이터 전송시에는 특별한 보안 기법이 적용되지 않는다. 따라서 경로 설정까지는 정상적인 동작을 취하는 Jellyfish 공격에 대해서는 크게 성능이 떨어지는 결과를 확인할 수 있었다. 하지만 제안한 기법은 경로 설정 이후에도 소스 노드와 목적 노드와 키 교환 과정을 수행한 후 데이터 전송이 이루어지기 때문에 Jellyfish 공격에 대해서도 우수한 성능의 결과를 얻을 수 있었다.



(a) Hello flooding 공격이 있는 경우

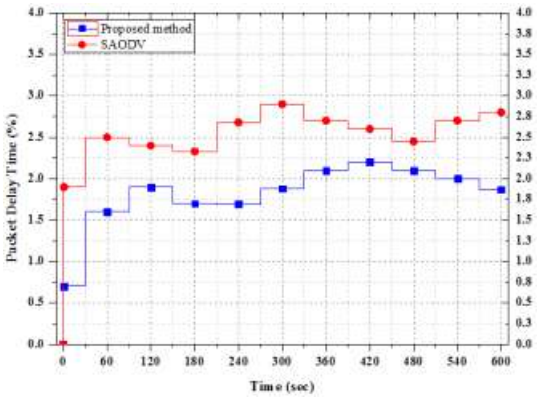


(b) Jellyfish 공격이 있는 경우

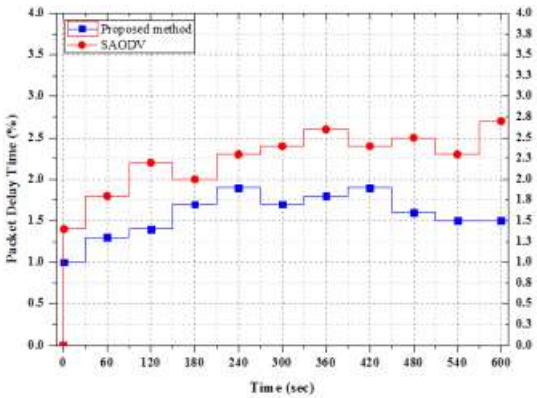
<그림 4> 패킷 전달 비율 결과

<그림 5>는 소스 노드와 목적 노드 사이의 전송 지연시간 측정 결과를 보여주고 있다. 이 실험에서는 Hello flooding 공격과 Jellyfish 공격이 존재할 때의 전송 지연시간을 비교하였다. SAODV 기법은 안전한 경로 설정을 위해 RREQ와 RREP에 대한 TTL 값과 전자서명을 이용하기 때문에 Hello flooding 공격시 지연 시간 성능은 우수하지만 Jellyfish 공격 발생시 경로 설정 이후의 악의적인 공격에 대한 보안 성능이 떨어지기 때문에 지연 시간이 길게 나타났다. 제안한 기법은 노드들의 신뢰

도를 기반으로 한 경로 설정과 그 이후에 소스 노드와 목적 노드간의 키 교환 과정을 거친 후에 데이터 전송이 이루어지기 때문에 종단간 지연 시간은 다소 길게 나타났으나 공격 여부에는 큰 영향을 받지 않는 강건함을 가지고 있는 것을 확인할 수 있었다.



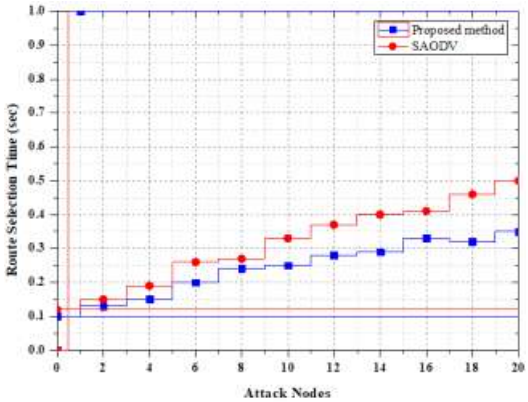
(a) Hello flooding 공격이 있는 경우



(b) Jellyfish 공격이 있는 경우

<그림 5> 전송 지연 시간 측정 결과

<그림 6>은 제안한 라우팅 기법의 효율성을 측정하기 위한 경로 선택 시간의 실험 결과를 보여주고 있다. 경로 선택 시간은 공격에 의한 노드들의 신뢰도에 따라 데이터 경로를 빠르게 변경할 수 있어야 라우팅 프로토콜의 성능이 향상될 수 있기 때문이다. 결과에서 보여주듯이 제안한 기법은 신뢰관리 노드에서 이웃 노드들에 대한 신뢰도를 관리하고 있기 때문에 신속한 경로 선택이 이루어 졌지만 SAODV기법은 경로 변경시 새로운 경로발견 과정을 거쳐야 하기 때문에 성능이 좋지 않았다.



<그림 6> 경로 선택 시간 측정 결과

Ⅴ. 결론

MANET에서 라우팅 프로토콜의 성능은 전체 네트워크 성능을 좌우할 만큼 매우 중요한 역할을 담당하고 있다. 따라서 많은 공격에 노출이 되어 있는 라우팅 기법에는 반드시 보안 기법이 적용되어야 한다. 본 논문의 목표는 소스 노드와 목적 노드간의 신뢰성 높은 경로를 설정하기 위하여 네트워크에 참여하는 노드들에 대한 신뢰도를 측정 및 관리하고, 데이터 전송에 있어 무결성을 제공하기 위하여 CA 없이 노드간의 키 교환을 통해 안전한 데이터 전송을 제공하는 것이다. 네트워크에 참여하는 노드들에 대한 신뢰도 평가 및 관리의 효율성을 위하여 계층 구조를 사용하였고, 계층 관리 노드에 의해 측정된

신뢰도를 관리하였다. 노드들의 신뢰도는 모든 노드에서 이루어지며, 측정 기준은 노드에서 포워딩하는 패킷의 양으로 하였다. 이렇게 측정된 노드들의 신뢰도의 평균값이 가장 높은 경로를 보안 경로서 선택하였으며, 경로 설정 이후에 소스 노드와 목적 노드간의 키 교환 과정을 거친 후에 데이터 전송이 이루어지게 되는 과정으로 이루어져 있다. 본 논문에서 제안한 기법의 성능을 평가하기 위하여 SAODV 기법과 PDR, 종단간 지연시간을 비교 실험하였으며 실험을 통해 제안한 기법이 PDR에서는 평균 8.2%, 종단간 지연시간은 평균 10.6%의 우수한 성능을 확인할 수 있었다.

참고문헌

[1] Sevil Şen, John A. Clark and Juan E. Tapiador, "Security Threats in Mobile Ad Hoc Networks Auerbach Publications," 2011, pp. 1-20.

[2] Durgesh Wadbude and Vineet Richariya, "An Efficient Secure AODV Routing Protocol in MANET," International Journal of Engineering and Innovative Technology, Vol. 1(4), 2012, pp. 274-279.

[3] ditya Bakshi, A.K.Sharma and Atul Mishra, "Significance of Mobile Ad-Hoc Networks (MANETs)," International Journal of Innovative Technology and Exploring Engineering (IJITEE), Vol.2(4), 2013, pp. 1-5.

[4] harma, D., V. Kumar, and R. Kumar, "Prevention of Wormhole Attack Using Identity Based Signature Scheme in MANET," Comput. Int. in Data Mining, 2016, pp. 475-485.

[5] 양환석, "신뢰도와 키를 이용한 보안 라우팅 기법에 관한 연구," 디지털산업정보학회지, 제11권, 제3호, 2015, pp. 69-77.

[6] Kumar, V., and R., Kumar, "An Optimal Authentication Protocol Using Certificateless ID-Based Signature in MANET," Security in Comp. & Comm., 2015, pp. 110–112.

[7] Maulik, R., and N. Chaki, "A Comprehensive Review on Wormhole Attacks in MANET," Int. Conf. on Com. Info. Syst. and Industrial Management Applications, 2013, pp. 233-238.

[8] M. Hossain, V. Raghunathan, Aegis, "A lightweight rewall for wireless sensor networks," Distributed Computing in Sensor Systems, 2010, pp. 258-272.

[9] 왕종수, 서두옥, "Sparse M2M 환경을 위한 DTMNs 라우팅 프로토콜," 디지털산업정보학회지, 제10권, 제4호, 2014, pp. 11-18.

[10] G. Acs, L. Buttyan, and L. Dora. "Misbehaving router detection in link-state routing for wireless mesh networks," In Proc. of WoWMoM, 2010, pp. 1–6.

■ 저자소개 ■

양 환 석
(Yang Hwanseok)

2011년 9월~현재
중부대학교 정보보호학과 조교수
2006년 2월~2011년 2월
호원대학교 사이버수사경찰학과 연구교수
2005년 2월 조선대학교 전산통계학과(이학박사)
1998년 2월 조선대학교 전산통계학과(이학석사)

관심분야 : 정보보호, 침입탐지시스템, MANET
E-mail : yanghs@joongbu.ac.kr

논문접수일 : 2017년 05월 14일
수 정 일 : 2017년 06월 01일
게재확정일 : 2017년 06월 12일