디지털산업정보학회 논문지 제13권 제4호-2017년 12월
http://dx.doi.org/10.17662/ksdim.2017.13.4.115

MANET에서 멀티캐스트 보안을 위한 효율적인 그룹 멤버 인증 및 키 관리 기법 연구

양 환 석*

A Study on Efficient Group Member Authentication and Key Management Scheme for Multicast Security in MANET

Yang Hwanseok

〈Abstract〉

The mutual cooperation among nodes is very important because mobile nodes participating in MANET communicate with limited resources and wireless environment. This characteristic is important especially in environment that supports group communication. In order to support the secure multicast environment, it is important enough to affect performance to provide accurate authentication method for multicast group members and increase the integrity of transmitted data. Therefore, we propose a technique to provide the multicast secure communication by providing efficient authentication and group key management for multicast member nodes in this paper. The cluster structure is used for authentication of nodes in the proposed technique. In order to efficient authentication of nodes, the reliability is measured using a combination of local trust information and global trust information measured by neighboring nodes. And issuing process of the group key has two steps. The issued security group key increases the integrity of the transmitted data. The superiority of the proposed technique was confirmed by comparative experiments.

Key Words : Node Authentication, Multicast, Secure Group Key, MANET

Ⅰ. 서론

최근 들어 MANET은 다양한 환경에서 활용되고 있으며 그 중요성 또한 증가하고 있다. 특히 멀티캐스트 환경에서의 그룹 통신에서도 다양하게 활용되고 있다. 하지만 MANET이 가지고 있는 제한된 자원, 노드들의 이동성, 제한된 대역폭 등의 특징들로 인하여 많은 보안 문제가 야기되고 있다[1]. 특히 그룹 통신에 참여하는 노드들에 대한 인증 문제는 네트워크 성능을 크게 좌우한다. 즉, 악의적인 노드들에 의한 잘못된 행동들이 그룹 통신 전체에 큰 영향을 줄 수 있기 때문에 노드들에 대한 정확한 인증 평가가 이루어져야만 한다[2]. 또한 멀티캐스트 전

* 중부대학교 정보보호학과 조교수

송 데이터의 위변조를 통해 그룹 통신에 참여하는 멤버 노드들에게 잘못된 정보를 전송할 수 있기 때문에 전송 데이터에 대한 무결성을 높여야만 한다[3, 4]. 따라서 이를 위해서는 멀티캐스트 환경에 적합한 노드 인증 및 무결성 향상 기법이 적용되어야 한다. 이를 통해서 네트워크 수명을 향상시키고 신뢰도를 높일 수 있게 된다.

본 논문에서는 멀티캐스트 환경에서 신뢰성을 향상시키기 위하여 멀티캐스트 그룹 멤버들에 대한 효율적인 인증 기법과 전송 데이터의 무결성을 향상시키기 위하여 보안 그룹 키 관리 기법을 제안하였다. 본 논문에서는 효율적인 인증을 위하여 클러스터 구조를 이용하였으며, 클러스터내 연결성이 높은 노드가 CA(Certificate Authority)의 역할을 담당한다. CA에서는 노드들의 신뢰도 정보 관리를 위해 클러스터 신뢰도 테이블을 가지고 있다. 노드들에 대한 신뢰도 평가는 로컬 신뢰 정보와 전역 신뢰 정보의 조합으로 이루어진다. 또한 데이터의 무결성 제공을 위한 보안 그룹 키 관리는 크게 두 단계로 이루어져 있다. CA에서는 그룹 키 테이블을 이용하여 소스 노드에게 유일한 그룹 키를 발급해주고 데이터를 수신한 멤버 노드에게 데이터 위변조를 검증할 수 있는 키 발급이 이루어진다. 이러한 과정을 통해 멀티캐스트 데이터의 무결성을 향상시켰다.

본 논문의 구성은 다음과 같다. 2장에서는 기존의 멀티캐스트 환경에서의 보안 라우팅 기법에 대하여 살펴보고 3장에서는 본 논문에서 제안한 인증 기법과 그룹 키 관리 방법에 대하여 설명하였다. 4장에서는 실험을 통해 제안한 기법의 성능을 평가하였으며 마지막으로 5장에서는 결론을 맺는다.

Ⅱ. 관련연구

2.1 멀티캐스트 보안 라우팅 기법

MANET에서 보안 통신은 매우 중요한 부분이며 이는 브로드캐스트 통신, 무선 매체, 중앙관리 인프라의 부재등으로 인해 많은 보안 위협에 노출되어 있다. 이러한 환경에서 보안 라우팅 프로토콜의 역할은 더욱 중요하다[5]. 특히, 보안 멀티캐스트 라우팅 프로토콜은 제한된 자원과 동적인 네트워크 특성으로 인해 설계가 매우 복잡하다. 게다가 다양한 공격 위협들에 대한 보안 기능을 추가하는 일은 쉽지 않다. 이러한 문제들을 해결하기 위해 그 동안 많은 연구들이 진행되어 왔다[6, 7].

TCSA(Trust based Clustering and Secure Authentication) 기법은 보안 클러스터링과 소스 노드 인증을 적용한 기법이다[8]. 이 기법에서는 신뢰성을 높이기 위하여 소스 노드에서 생성된 암호화 키를 이용하였으며, 모든 멤버 노드들과 소스 노드는 같은 경로를 이용하였다. 그리고 클러스터에 새로운 노드가 들어오면 에이전트 노드에 의해 해당 노드의 신분을 검사하게 된다. 그리고 에이전트 노드에서는 공격 노드에서 의해 데이터 변조가 이루어졌는지 암호화된 데이터를 모니터링하는 역할도 담당한다.

ARAN(Authenticated Routing for Ad hoc Network) 기법은 보안 라우팅 제공을 위해 그룹내의 노드들에게 부가적인 작업을 요구하지 않는 단순한 프로토콜이다[9]. 그리고 공격 노드에 의한 공격을 막고 데이터 무결성 제공을 위해서 공개키 암호 메커니즘을 이용한다. 이 공개키 암호를 이용하여 경로 발견 및 경로 유지를 위한 제어 패킷들에 대한 암호화를 수행한다. ARAN 기법은 보안 경로를 효율적으로 발견할 수 있고 노드들은 인증을 받아야만

네트워크 참여할 수 있게 된다. 따라서 인증, 메시지 무결성, 부인방지 기능을 제공해주게 된다.

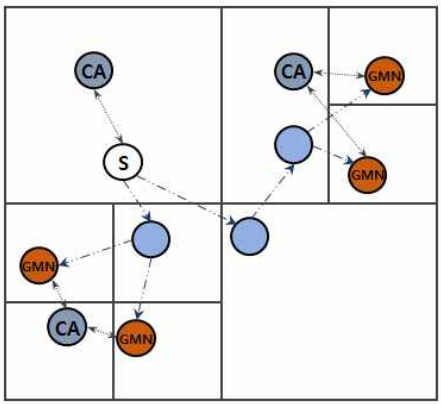
SADSR(Security-aware Adaptive DSR) 기법은 보안 on-demand 라우팅 프로토콜중의 하나로서 모든 노드가 다른 노드들과의 경로 테이블을 가지고 있다. SADSR은 비대칭 암호화 기법을 기초로 디지털 서명을 이용하여 라우팅 프로토콜 메시지를 인증한다[10]. SADSR은 목적 노드까지 여러 개의 경로를 관리하고 네트워크에 있는 각각의 노드에 대한 지역 신뢰도 값을 저장한다. 멀티캐스트 데이터 전송을 위한 경로 설정을 위해서는 먼저 경로상의 모든 노드들에 대한 신뢰도를 계산하여 신뢰도가 가장 높은 경로를 이용하여 데이터를 전송하게 된다. 이렇게 함으로써 데이터에 대한 신뢰도를 높이고 보안 라우팅을 제공해주게 된다.

Ⅲ. 제안한 기법

본 장에서는 멀티캐스트 보안 통신을 제공하기 위하여 그룹 멤버들에 대한 효율적인 인증과 보안 그룹 키 관리 기법에 대하여 설명한다.

3.1 시스템 개요

MANET에서 안전한 멀티캐스트 환경을 제공해주기 위해서는 멀티캐스트 그룹 멤버들에 대한 인증이 철저하게 이루어져야 하며 전송 데이터들에 대한 무결성을 높이기 위한 보안 그룹 키 관리가 매우 중요하다. 일반적으로 그룹 통신의 암호화와 복호화를 위하여 보안 그룹 키를 사용하는 반면에 본 논문에서는 유일한 식별자로 각 보안 그룹 키를 적용하였다. 먼저 이를 위하여 계층 형태의 클러스터 구조를 적용하였으며, 각 클러스터 마다 연결성이 가장 높은 노드를 CA로 선정하였다. 각 클러스터내의 모든 CA는 각 그룹에게 분배할 그룹 키 테이블(GKT : Gourp Key Table)을 가지고 있다. 또한 그룹 멤버들에 대한 인증을 위해 측정된 신뢰도를 저장하고 있는 클러스터 신뢰도 테이블(CTT : Cluster Trust Table)을 관리한다. 그룹 멤버 인증 기법은 이웃 노드들에 의해 직접 측정되는 로컬 신뢰 정보와 전역 신뢰 정보의 조합에 의해 계산되며 이렇게 계산된 신뢰도를 기준값과 비교하여 멤버 노드에 대한 인증이 이루어지게 된다. CA에서 전송 데이터의 무결성을 높이기 위하여 보안 그룹 키를 분배하는 과정은 크게 두 단계로 이루어진다. 먼저 멀티캐스트 데이터 전달을 위한 소스 노드에게 고유의 키를 발급하는 과정과 멀티캐스트 데이터를 수신한 멤버 노드들에게 무결성 검사를 위해 키를 전송해주는 과정이다. 이러한 과정을 통해 악의적인 노드들은 멀티캐스트 통신에 참여할 수 없게 되어 멀티캐스트 보안 통신을 제공할 수 있게 된다. <그림 1>은 본 논문에서 사용한 네트워크 구조를 보여주고 있다.



<그림 1> 제안한 네트워크 구조

3.2 멀티캐스트 멤버 노드 인증 기법

멀티캐스트 그룹의 멤버 노드들에 대한 효율적인

경량 인증을 위하여 이웃 노드들에 의해 직접 측정되는 로컬 신뢰도(LT : Local Trust)와 해당 노드의 이전 신뢰도 수집에 의한 전역 신뢰도(GT : Global Trust)를 조합하여 계산하게 된다. 이러한 인증 기법은 신뢰도와 네트워크 수명을 향상시킬 수 있다.

로컬 신뢰도 계산은 두 노드간의 신호 강도와 일정 기간 동안의 패킷 전송 대비 에러 비율을 측정하여 이루어진다. 노드 N의 로컬 신뢰 정보를 얻기 위해서는 노드 N의 이웃 노드들에서 RSS(Received Signal Strength)를 식 (1)을 이용하여 측정한다.

$$RSS[dBm] = 10\log_{10}\alpha + \theta[dB] + S_{tx}[dBm] \quad (1)$$

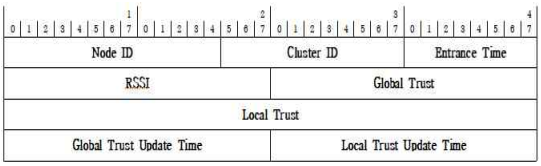
그리고 이웃 노드에서는 노드 N으로부터 일정 기간 동안 수신한 모든 패킷들 중 수신한 전체 패킷과 에러가 난 패킷을 측정한 후 식 (2)를 이용해서 노드들 사이의 전송 비율을 계산한다.

$$AVG(ER) = \sum_{i=1}^{n} MN_i \frac{P_{err}}{P} \quad (2)$$

여기서 P은 두 노드간의 전송된 전체 패킷의 양, P_{Err}은 두 노드간의 에러 패킷의 양을 나타낸다. 이렇게 이웃 노드들에 의해서 계산된 값과 이웃 CA로부터 수 신한 노드들에 대한 전역 신뢰도의 조합으로 노드에 대한 신뢰도를 결정한다. 전역 신뢰도는 노드들이 이전에 속해있던 클러스터에서 평가 받았던 신뢰도의 평균값이며, CA들은 주기적으로 자신이 관리하는 클러스터에 속해있던 노드들에 대한 신뢰도를 이웃 CA들에게 방송하게 된다. 이렇게 수집된 전역 신뢰도와 로컬 신뢰도는 식 (3)에 의해 노드 N의 신뢰도를 계산하게 된다.

$$T(N) = \frac{RSS_{N_i}}{Avg(ER)} \cdot w + GT(N) \cdot (1-w) \quad (3)$$

여기서 w는 노드 N이 클러스터에 들어온 시간에 대한 가중치를 나타낸다. 위 식에 의해 측정된 신뢰도는 노드들의 인증에 사용된다. 즉, 노드 N의 신뢰도가 클러스터내의 평균 신뢰도보다 낮으면 해당 노드에게는 보안 그룹 키를 발급해주지 않는다. 보안 그룹 키를 발급받지 못하면 멀티캐스트 통신 데이터를 확인할 수 없기 때문에 멀티캐스트에서 배제되게 된다. <그림 2>는 CA에서 그룹 멤버 노드들의 신뢰도를 저장 및 관리하기 위한 클러스터 신뢰도 테이블의 구조를 보여주고 있다.

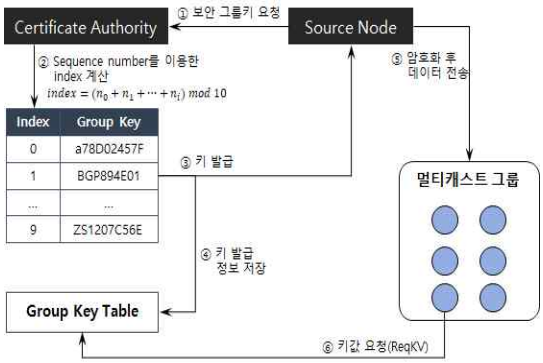


<그림 2> 클러스터 신뢰도 테이블 구조

3.3 보안 그룹 키 관리 기법

멀티캐스트 그룹에 데이터를 전송하고자 하는 소스 노드는 전송 데이터에 대한 무결성을 보장하기 위하여 자신이 속한 클러스터내의 CA에게 그룹 키 발급을 요청한다. 소스 노드로부터 그룹 키 발급을 요청받은 CA는 소스 노드의 신뢰도를 검사한 후, 만약 신뢰도가 기준값 이상이 되면 그룹 키 발급과정을 거쳐 발급하게 된다. 먼저 그룹 키 발급을 위해서 소스 노드가 보낸 그룹 키 요청 패킷의 sequence number의 각 자리수를 더한 후 10으로 나눈 나머지를 계산하여 그룹 키 테이블의 인덱스에서 해당 숫자에 매칭이 되는 키 값을 소스 노드에게 송신하게 된다. 이러한 방법을 통해 본 논문에서는 그룹 통신의 암/복호화를 위해 유일한 키를 적용하였다. CA에서 소스 노드에게 키 값을 발급하면 이웃하는 CA들에게 암호화 통신을 통해서 해당 정보를 전송하게 된다. 따라서 네트워내의 모든 CA들은

키 발급 정보를 공유하게 된다. 소스 노드는 이러한 키 값을 이용하여 그룹 멤버들에게 전송할 멀티캐스트 데이터를 암호화하여 전송하게 된다. 이렇게 암호화된 데이터는 목적 노드까지의 경로에 악의적인 노드가 존재한다하더라도 데이터가 암호화 되어 있기 때문에 해당 데이터의 변조가 불가능하게 되며, 만약 변조가 된다하더라도 데이터를 수신한 멤버 노드에서 키 값을 이용해 무결성을 검사하여 위변조 사실을 알 수 있기 때문에 데이터에 대한 보안을 강화시키는 장점을 갖게 된다. 데이터를 수신한 그룹 멤버 노드들은 암호화가 된 데이터의 키를 자신이 속한 클러스터의 CA에게 소스 노드의 ID가 포함되어 있는 키 값 요청 패킷인 ReqKV을 송신하게 된다. CA에서는 해당 노드의 신뢰도 검사 후 그룹 키 테이블에서 소스 노드에게 발급된 키를 검색하여 키 값을 RepKV를 전송하게 된다. 키 값을 수신한 멤버 노드는 데이터의 무결성을 검사하여 멀티캐스트 데이터의 위변조를 확인하게 된다. <그림 3>은 보안 그룹 키를 이용한 데이터 전송 및 확인 과정을 보여주고 있다.



<그림 3> 그룹 키 발급 및 데이터 전송과정

Ⅳ. 성능분석

4.1 실험 환경

본 논문에서 제안한 그룹 멤버 인증 및 보안 그룹 키 관리 기법의 성능평가를 위하여 ns-2 시뮬레이터를 이용하였다. 그리고 각 이동 노드들은 멀티캐스트 그룹의 가입 및 탈퇴가 반복되도록 랜덤으로 이동하였으며 노드들의 이동 속도는 0 ~ 20m/s로 하였다. 실험 시간은 300초로 하였으며 실험 시간동안 10개의 공격 노드에서 블랙홀 공격을 각각 5회씩 실행하였다. 단 본 실험에서는 이동 노드들의 배터리 소모는 고려하지 않았다. <표 1>에서는 실험에 사용한 환경변수 값을 보여주고 있다.

<표 1> 실험에 사용한 환경 변수

Parameter	Value
Network Size	1000 × 1000
Number of Nodes	100, 200
Pause Time(Sec)	20
Attack Type	Blackhole
Maximun no. of Conns	15
Application Traffic	CBR
MAC Protocol	IEEE 802.11 DCF

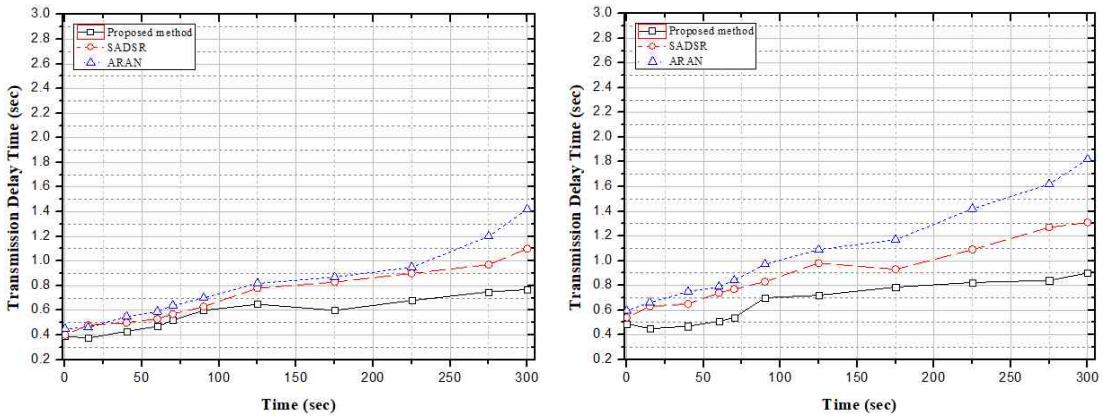
4.2 성능 평가

이 장에서는 멀티캐스트 보안 성능을 향상시키기 위해 본 논문에서 제안한 기법의 성능 측정 결과에 대하여 설명하며, 성능 측정은 ARAN 기법, SADSR 기법과 비교 실험하였다. 본 논문에서 제안한 그룹 멤버 인증과 키 관리가 공격이 존재하는 상황에서도 제대로 이루어진다면 패킷 전송과 처리에서 좋은 결과를 얻을 수 있을 것이다. 따라서 성능 평가 기준

은 공격 유무에 따른 데이터 전송 지연 시간과 평균 처리율로 설정하였다.

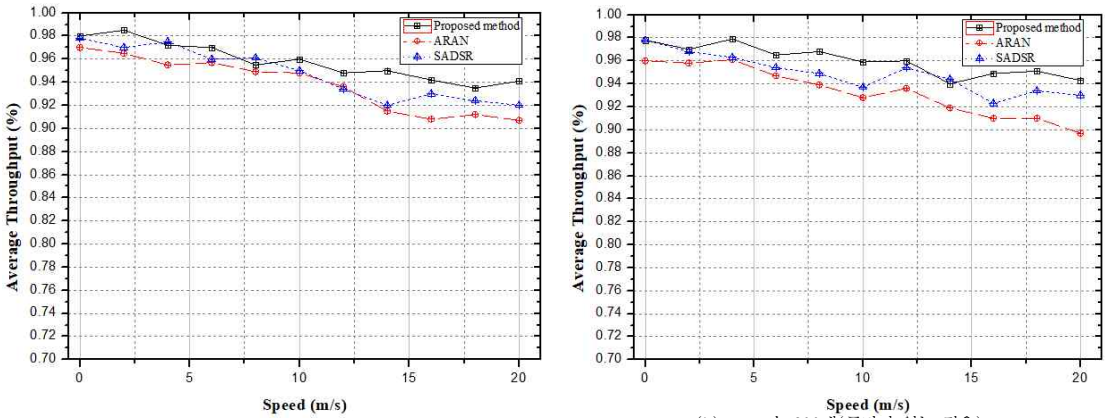
<그림 4>에서는 소스 노드에서 목적 노드들까지 멀티캐스트 데이터 전송시 공격 유무에 따른 평균 전송 시간 측정 결과를 보여주고 있다. ARAN 기법은 다른 기법들에 비해 많은 오버헤드가 발생하였는데 그 이유는 보안 경로 발견을 위한 지연 시간과 전송 데이터의 암호화 계산 시간 때문이다. SADSR 기법은 다중 경로 중 신뢰도가 높은 경로 선택을 통한 데이터 전송이 이루어지기 때문에 좋은 성능 결과를 보여주었지만 다중 경로에 대한 신뢰도 계산으로 인해 오버헤드가 발생하였다. 제안한 기법에서는 노드들의 이동에 따른 신뢰 정보 교환으로 인한 지연 시간이 다소 길게 나타나는 결과를 보여주었지만 수신 강도를 기초로 한 데이터 처리율이 노드들의 신뢰도에 반영되어 공격 유무에 큰 영향을 받지 않으면서 좋은 결과를 보여주었다.

<그림 5>은 소스 노드에서 전송한 데이터의 평균 처리율 결과를 보여주고 있다. ARAN 기법은 경로 발견 및 유지의 성능은 기존의 AODV보다 효과적이고 노드들의 인증을 통한 네트워크 참여가 결정되기 때문에 인증과 무결성의 성능은 제공해주지만 공개키 암호화에 대한 높은 오버헤드로 인해 전체 처리율은 떨어지는 결과를 보였다. SADSR 기법은 디지털 서명을 통한 라우팅 패킷들에 대한 인증을 수행하기 때문에 공격이 존재하는 상황에서도 좋은 결과를 보여주었다. 다만 다중 경로에 대한 많은 신뢰도 계산이 다소 성능을 떨어뜨렸다. 제안한 기법이 다른 기법들에 비해 가장 좋은 결과를 보여주었다. 먼저 이웃 노드들에 의한 로컬 신뢰 측정이 빠르게 이루어지고 그룹별 유일한 그룹 보안 키 발급을 통한 데이터 무결성 제공이 성능이 좋아 공격이 존재해도 크게 영향을 받지 않은 우수한 성능을 확인할 수 있었다.



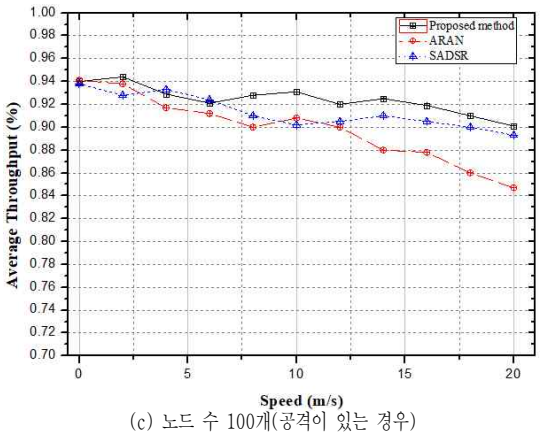
(a) 공격이 없는 경우 (b) 블랙 홀 공격이 있는 경우

<그림 4> 종단간 전송 지연 시간

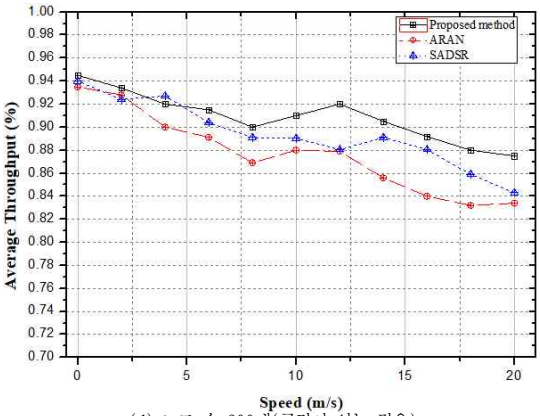


(a) 노드 수 100개(공격이 없는 경우)

(b) 노드 수 200개(공격이 없는 경우)



(c) 노드 수 100개(공격이 있는 경우)



(d) 노드 수 200개(공격이 있는 경우)

<그림 5> 노드 수와 공격 유무에 따른 패킷 전달 비율

V. 결론

본 논문에서는 MANET의 멀티캐스트 환경에서 노드들에 대한 효율적인 인증과 무결성 향상에 대해 초점을 맞추었다. 이를 위하여 노드들에 대한 효율적인 인증을 위해 클러스터 기법을 적용하였으며, 두 단계로 이루어진 보안 그룹 키 관리 방법을 제안하였다.

노드들에 대한 정확한 인증을 제공하기 위하여 이웃 노드들에 의해서 직접 측정되는 로컬 신뢰도와 노드들의 이전 클러스터에서의 신뢰도 값을 측정한 전역 신뢰도 값을 조합하고 노드들이 네트워크에 참여하는 시간에 따라 가중치를 두어 보다 정확한 신뢰도 측정 방법을 제공하였다. 특히 이웃 노드들에게서 측정되는 로컬 신뢰도는 노드들간의 신호 강도 및 패킷 전송률을 기반으로 측정되기 때문에 노드들의 이기적인 행동에 대한 판단을 수행할 수 있었다. 그리고 일반적인 그룹 통신과는 달리 유일한 보안 그룹 키를 적용하여 그 보안성을 더욱 향상시킬 수 있었다. 즉, 소스 노드가 그룹 통신에 전송할 데이터

의 암호화를 위해 사용하는 키 발급은 소스 노드가 요청한 패킷의 sequence number의 각 자리수 값을 더한 후 나머지 값을 구하여 이를 인덱스로 하는 키 값을 이용하여 암호화를 수행하게 된다. 이렇게 암호화된 데이터를 수신한 그룹 멤버 노드들은 자신이 속한 클러스터내 CA에서 키 요청 패킷(ReqKV)을 송신하여 해당 암호 키를 수신받아 그룹 통신 데이터의 위변조를 검증하게 된다. 본 논문에서는 실험을 통해 노드 수와 공격 유무에 따른 전송 지연 시간과 평균 처리율을 성능평가 기준으로 하여 ARAN 기법, SADSR 기법과 비교 실험하였다. 실험을 통해 제안한 기법의 우수한 성능을 확인할 수 있었다.

참고문헌

[1] C. Gui, P. Mohapatra, "Scalable Multicasting in Mobile Ad Hoc Networks," Proceedings of IEEE INFOCOM, 2004.

[2] K. Lyes, C. Soumaya, "Intelligent QoS management for multimedia services support in wireless mobile ad hoc networks," Computer Networks, 2010, Vol. 54, No. 10, pp. 1692-1706.

[3] 김정삼, "무선 센서네트워크에서 네트워크 수명 극대화 방안," 디지털산업정보학회지, 제10권, 제2호, 2014, pp. 47-59.

[4] B. Brian, S. Shaya, "Mobile ad hoc network broadcasting: A multicriteria approach," International Journal of Communication Systems, 2011, Vol. 24, No. 4, pp. 438-460.

[5] M. Manjul, R. Mishra, Joytsna, and K. Singh, "Link utilization based multicast congestion control," Communications and Network, 2013, Vol. 5, pp. 649-653.

[6] S. Kim and Y.-J. Cho, "Efficient multicast scheme based on hybrid ARQ and busy tone for multimedia traffic in wireless LANs," Applied Mathematics and Information Sciences, 2014, Vol. 8, No.1, pp. 171-180.

[7] 오일, 최승원, 김수민, 김경훈, 금동현, "2.4Ghz ISM(Industrial Scientific Medical) 밴드에서 간섭을 회피하기 위한 무선 센서 노드의 채널 선택 방법," 디지털산업정보학회지, 제10권, 제4호, 2014, pp. 109-116.

[8] T. Sasanth, S. Umar, and D. Bellam, "A study on data security in MANETS," International Journal of Computer Science Engineering & Technology, 2013, Vol. 3, No. 11, pp. 408-415.

[9] K. S. Rao, R. S. Kumar, P. Venkatesh, R. V. S. Naidu, and A. Ramesh, "Development of energy efficient and reliable congestion control protocol for multicasting in mobile ad hoc networks compare with AODV based on receivers," International Journal of Engineering Research and Applications, 2012, Vol. 2, No. 2, pp. 631-634.

[10] A. A. Mo'men, H. S. Hamza, and I. A. Saroit, "Secure Multicast Routing Protocols in Mobile Ad-Hoc Networks," International Journal Communication System, 2014, Vol. 27, No. 11, pp. 2808-2831.

■ 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 11월 17일
수 정 일 : 2017년 12월 05일
게재확정일 : 2017년 12월 05일