디지털산업정보학회 논문지 제13권 제3호-2017년 9월
http://dx.doi.org/10.17662/ksdim.2017.13.3.043

MANET의 멀티캐스트 환경에서 신뢰성 향상을 위한 계층기반 암호 프로토콜 기법 연구

양 환 석*

A Study on Hierarchy-based Secure Encryption Protocol for Trust Improvement on Multicast Environment of MANET

Yang Hwanseok

〈Abstract〉

MANET consists of only wireless nodes having limited processing capability. It processes routing and data transmission through cooperation among each other. And it is exposed to many attack threats due to the dynamic topology by movement of nodes and multi-hop communication. Therefore, the reliability of transmitted data between nodes must be improved and security of integrity must be high. In this paper, we propose a method to increase the reliability of transmitted data by providing a secure cryptography protocol. The proposed method used a hierarchical structure to provide smooth cryptographic services. The cluster authentication node issues the cluster authentication key pair and unique key to the nodes. The nodes performs the encryption through two steps of encryption using cluster public key and block encryption using unique key. Because of this, the robustness against data forgery attacks was heightened. The superior performance of the proposed method can be confirmed through comparative experiment with the existing security routing method.

Key Words : Mobile Ad-hoc Network, Data Encryption, Hierarchy-based Protocol

Ⅰ. 서론

MANET(Mobile Ad-hoc Network)은 다양한 무선 통신 모델 중에서 중요한 모델로서 무선 노드들의 참여로만 구성된 동적인 네트워크로서 어떠한 인프라스트럭처도 존재하지 않는다. 따라서 경로 설정 및 데이터 전달은 네트워크에 참여하는 노드들에 의한 다중 홉(multi-hop) 방식으로 이루어진다[1]. 또한 개방형 환경, 노드들의 이동으로 인한 동적인 토폴로지, 중앙관리의 부재, 제한된 통신 대역폭 등과 같은 특징으로 인해 소스 노드와 목적 노드간의 경로 설정 단계 그리고 데이터 전송 과정에는 많은 공격 위협이 존재하고 있다. MANET에서는 제한된

* 중부대학교 정보보호학과 조교수

자원을 활용한 효율적인 그룹 통신을 제공하기 위해 네트워크 계층의 IP 멀티캐스트와 응용 계층의 오버레이 멀티캐스트가 있다. 하지만 멀티캐스트와 같은 그룹 통신 환경에서 도청과 데이터 변조에 의한 공격은 심각한 피해를 야기할 수 있다[2]. 따라서 전송되는 데이터들에 대한 신뢰성을 향상시키고 견고한 무결성을 제공을 위한 연구가 반드시 필요하다.

본 논문에서는 멀티캐스트 환경에서 노드들간 신뢰성을 높이고 전송 데이터에 대한 무결성을 제공하기 위하여 계층기반 보안 암호 프로토콜 기법을 제안하였다. 본 논문에서는 노드들에 대한 암호화 서비스를 원활히 제공하기 위해 전체 네트워크를 계층 구조인 클러스터 형태를 이용하였다. 각 클러스터내의 노드들에게 클러스터 인증 키쌍과 고유키를 발급해주고 키 정보를 관리하기 위한 클러스터 인증노드를 연결수 기반으로 선출하였다. 선출된 각 클러스터 인증노드 서로가 공유할 수 있는 클러스터 공개키와 비밀키를 설정하며, 클러스터 키 관리 테이블에서 노드들에게 발급되는 인증 키쌍과 고유키 정보를 관리하였다. 네트워크에 참여하는 노드들은 두 단계의 암호화 과정을 통해 데이터를 전달한다. 첫 번째 단계에서는 클러스터 인증노드로부터 발급받은 공개키를 이용하여 전송 데이터를 암호화하게 된다. 두 번째 단계에서는 암호화된 데이터를 고유키를 보조키로 이용하여 블록 암호화한 후 데이터를 전송하게 된다. 이렇게 함으로써 전송하는 데이터에 대한 위변조 공격에 대한 안전성을 향상시킬 수 있게 하였다.

본 논문의 구성은 다음과 같다. 2장에서는 MANET에서 그 동안 연구되었던 멀티캐스트 기법과 보안 라우팅 기법에 대하여 살펴보고 3장에서는 본 논문에서 제안한 계층기반 보안 암호 프로토콜 기법에 대하여 설명하였다. 4장에서는 실험을 통해 제안한 기법의 성능을 확인하였고 마지막으로 5장에서는 결론을 맺는다.

Ⅱ. 관련연구

2.1 멀티캐스트 기법

MANET에서의 멀티캐스트 기법은 크게 네트워크 계층 멀티캐스트와 응용 계층 멀티캐스트로 구분된다. 네트워크 계층 멀티캐스트 기법은 모든 노드들이 멀티캐스트 서비스를 인식하고 있어야 하며, 경로 설정에는 멀티캐스트에 참여하지 않는 노드들도 참여하는 기법이다[3]. 멀티캐스트 데이터 전달 방법에 따라 메시 기반 방식과 트리 기반 방식으로 분류된다[4]. 메시 기반 방식은 노드들의 이동성을 고려하여 다중 전송 경로를 허용하였으며, FGMP (Forwarding Group Multicast Protocol), ODMRP (On-Demand Multicast Routing Protocol) 등이 있다. 트리 기반 방식으로는 AMRIS(Ad Hoc Multicast Routing Protocol Utilizing Increasing id-numberS), MAODV(Multicast Ad hoc On-Demand Distance Vector) 등이 있다[5-6].

오버레이 멀티캐스트라고도 불리는 응용 계층 멀티캐스트 기법은 멀티캐스트 데이터 전송의 효율성을 높이기 위하여 응용 계층에 가상 멀티캐스트 토폴로지를 구성하여 서비스를 제공한다. 이 방법은 응용 계층에서 동작하기 때문에 다양한 기능을 자유롭게 추가로 제공할 수 있으며, 라우팅 프로토콜에 비의존적인 장점을 가지고 있다. 응용 계층 멀티캐스트 기법으로는 PAST-DM(Progressively Adapted Sub-Tree in Dynamic Mesh), AMRoute(Ad hoc Multicast Routing Protocol) 등이 있다[7].

2.2 보안 라우팅 기법

MANET은 이동 노드들에 의한 hop-by-hop 방식으로 경로 설정과 데이터 전송이 이루어지기 때문에 다양한 라우팅 공격에 노출되어 있다. 라우팅 공격은 패킷의 도청이나 감청을 통해 피해를 야기하는 passive 공격과 라우팅 과정에서 잘못된 패킷의 삽입, 폐기 또는 변경을 통해 패킷 전송이 불가능하게 하는 avtive 공격이 있다[8]. 라우팅 공격들 중에서 대표적인 공격은 블랙 홀 공격, 웜 홀 공격, jellyfish attack 등이 있다. 이러한 공격에 대응하기 위한 많은 보안 라우팅 기법들에 대해 연구가 진행되고 있다[9-10].

SEER(Sercure Energy-Efficient Routing) 기법은 단방향 해시 체인을 이용하여 데이터를 인증하며, 기밀성을 향상시키기 위해 이동 노드와 베이스스테이션 사이에 공유된 비밀키를 이용하였다[11]. 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. ARAN(A secure Routing protocol for Ad hoc Networks) 기법은 노드들에 대한 인증 방법과 노드들 사이의 링크 인증을 적용하여 한층 강화된 보안 기능을 제공하였다[12]. 이 기법에서는 노드들의 인증을 담당하는 인증 서버가 있고, 네트워크에 참여하는 노드들은 인증 서버로부터 인증서를 발급받아야 한다. 소스 노드는 경로 탐색시 RREQ 메시지를 인증서를 비밀키로 서명하여 발송한다. 목적 노드에서는 RREP와 인증서를 비밀키로 서명하여 소스 노드에게 전달하게 된다. 소스 노드는 목적 노드의 공개키가 있어야만 경로 응답 패킷의 유효성을 확인할 수 있기 때문에 종단간 인증이 제공되고, 중간 노드들에 대한 검증 과정은 링크간 인증을 제공하는 기법이다.

Ⅲ. 계층기반 보안 암호 프로토콜 기법

본 장에서는 MANET의 멀티캐스트 환경에서 높은 데이터 신뢰성과 안전한 암호화 서비스를 제공하기 위한 계층기반 보안 암호 프로토콜(HSEP : hierarchy-based Secure Encryption Protocol) 기법을 제안하였다.

3.1 HSEP 시스템 구조

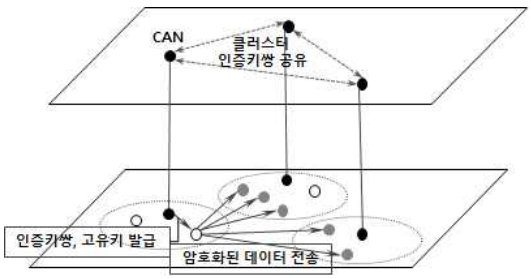
MANET에서 멀티캐스트 환경을 지원해주기 위해서는 멀티캐스트에 참여하는 노드들에 대한 여러 가지 정보를 유지해야 하는 어려움이 있다. 그리고 이를 위해 주기적인 제어 메시지를 송수신해야하기 때문에 네트워크 성능에도 많은 영향을 미친다.

HSEP 기법은 멀티캐스트 환경에서 노드들이 전송하는 데이터의 신뢰성을 높이고 무결성을 제공하기 위해 계층기반 구조인 클러스터를 이용하였다. 각 클러스터에는 클러스터내의 노드들에게 키를 발급해주는 클러스터 인증노드(CAN : Cluser Authentication Node)를 선출한다. 초기 클러스터 형성시 클러스터 인증노드 선출은 각 노드들의 연결수를 기반으로 하였다. 이렇게 선출된 클러스터 인증노드는 서로간의 공유할 수 있는 클러스터 공개키와 클러스터 비밀키 쌍$(C_P(k), C_S(k))$을 설정하게 된다. 이렇게 설정한 키쌍은 멀티캐스트 환경에서 데이터를 전공하고자 하는 클러스터내의 노드들에게 발급해준다. 그리고 클러스터 키쌍의 노

출로 인한 피해를 막기 위해 각 클러스터 인증노드는 주기적으로 클러스터 공개키와 비밀키 쌍을 갱신한다.

멀티캐스트 환경에서 데이터를 전송하기 위한 노드는 먼저 클러스터 인증서버로부터 클러스터 공개키를 발급받은 후 두 단계의 암호화 과정을 거친 후에 데이터를 전송하여 데이터의 신뢰성과 무결성을 제공함으로써 안전한 데이터 전송을 할 수 있게 된다. 첫 번째 단계는 클러스터 인증노드로부터 받은 공개키를 이용한 암호화를 수행한다. 두 번째 단계는 암호화된 데이터를 고유키를 보조키로 이용한 블록 암호화 과정을 수행하게 된다.

<그림 1>는 본 논문에서 제안한 HSEP 기법의 시스템 구조를 보여주고 있다.



<그림 1> HSEP 시스템 구조

3.2 HSEP 멤버 관리

본 논문에서 제안한 HSEP 기법의 효율성을 높이기 위해서는 클러스터내 노드들에 대한 관리가 철저히 이루어져야 한다. 즉, 클러스터 인증노드로부터 발급되는 키 관리가 제대로 이루어져야 안전한 데이터 전송을 보장할 수 있기 때문이다. 특히 클러스터 키를 발급받은 노드가 다른 클러스터에 이동하였을 때 해당 노드에 대한 클러스터 키 발급을 위한 과정들이 원활하게 이루어져야 한다.

클러스터 인증노드는 클러스터내 노드들에게 데이터 전송시 암호화를 위한 클러스터 키 발급 정보를 클러스터 키 관리 테이블(CKMT : Cluster Key Management Table)에 저장하게 된다. 이때 클러스터 키쌍과 각 노드별 고유키 값(u_p)을 함께 발급하게 된다. 이동 노드는 전공하고자 하는 데이터 암호화에 클러스터 공개키를 이용하며, 노드별로 부여되는 고유키는 블록 암호화에 사용된다. <그림 2>는 CKMT의 구조를 보여주고 있다.

Node ID	Auth_Key	Uni_Key	Issue_Time	Req_Time
G	(P_G, S_G)	aff0xtoqprw	13:58:48	13:58:21
A	(P_A, S_A)	qczx012okg	13:30:12	13:30:02
B	(P_B, S_B)	u7r29kh2ua	15:05:06	15:04:54

<그림 2> CKMT 구조

클러스터 노드로부터 클러스터 키를 발급받은 노드가 다른 클러스터로 이동을 한 경우에는 해당 클러스터 인증노드로부터 클러스터 인증키를 재발급받아야만 한다. 먼저 이동을 한 노드는 자신이 이동한 해당 클러스터 인증노드에게 자신의 정보와 이전 클러스터 인증 노드로부터 발급받은 클러스터 키쌍을 클러스터 인증노드에게 전송한다. 이 정보를 수신한 클러스터 인증노드는 노드로부터 수신한 클러스터 인증 키쌍을 자신이 소유하고 있는 키쌍과 일치하는지 비교한다. 만약 일치한다면 노드가 있었던 이전 클러스터 인증서버에게 노드에게 발급한 고유키 값의 일치여부를 검사한 후 만약 일치한다면 해당 노드에게 클러스터 인증 키쌍과 고유키 값을 재발급해주게 된다. <그림 3> 클러스터 인증 키쌍의 재발급 과정에 대한 의사코드를 보여주고 있다.

```
if (keyRequst(struct Cluster_K ck, uni_key))
{
    while (CKMT != EoF)
    {
        if (CKMT.p(k) == ck.p(k) && CKMT.s(k) == ck.s(k))
        {
            rev = sendToCluster(CluserID, uni_key);
            if (rev)
            {
                KeyIssue(Node_ID);
            }
            else
            {
                reject(Node_ID);
            }
        }
    }
}
```

<그림 3> 클러스터 인증 키쌍 재발급 의사코드

3.3 계층기반 보안 암호화

계층기반 보안 암호 프로토콜은 전송 데이터의 신뢰성을 높이고 무결성을 제공하기 위한 암호화 과정은 크게 두 단계로 구성되어 있다. 먼저 첫 번째 단계는 소스 노드가 클러스터 인증노드로부터 발급받은 클러스터 공개키를 이용하여 전송하고자 하는 데이터를 암호화하게 된다. 암호화는 식 (1)에서 보여주고 있다.

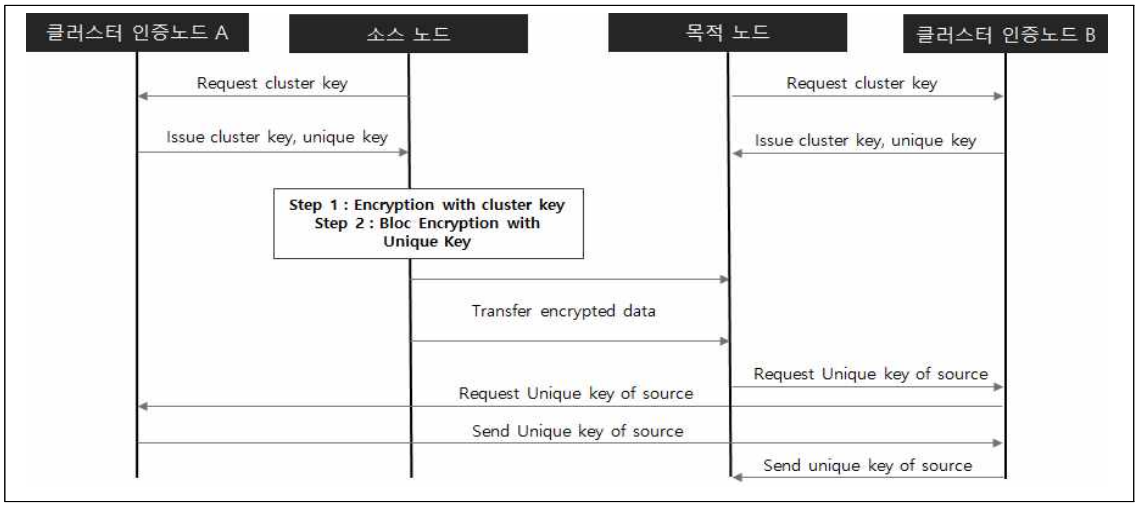
$$E(M_i) = \sum_{i=1}^{n} (C\_P(k, M_i)) \quad (1)$$

여기서 $C_P(k)$는 클러스터 공개키를 나타내고, M은 소스 노드가 전송할 데이터를 의미한다. 두 번째 단계에서는 이전 단계에서 생성된 암호문을 클러스터 인증노드가 노드들에게 발급한 고유키 u_p를 이용한 블록 암호화를 수행한다. 먼저 이전 단계에서 생성된 암호문 $E(M_i)$를 다음 식 (2)와 같이 왼쪽과 오른쪽으로 반으로 나누어 구성한다.

$$E(M_i) = (L_0, R_0) \quad (2)$$

각 $i = 1, 2, , \cdots, n$번째 회전에서 중심을 기준으로 새로운 왼쪽과 오른쪽은 식 (3)과 식 (4)에 의해 계산된다.

$$L_i = R_{i-1} \quad (3)$$



<그림 4> 계층기반 보안 암호 프로토콜 동작 과정

$$R_i = L_{i-1} \oplus F(R_{i-1}, u_{p_i}) \quad (4)$$

여기서 u_{p_i}는 i번째 회전에 사용되는 보조키이며, 이 보조키는 클러스터 인증노드로부터 노드별로 부여한 고유키가 된다. 이러한 과정을 거쳐 얻어진 최종 암호문은 식 (5)와 같다.

$$C(E(M)) = (L_n, R_n) \quad (5)$$

위와 같은 과정을 거쳐 생성된 암호문을 멀티캐스트 그룹에 전송하게 되면 이를 수신한 노드들은 자신이 속한 클러스터 인증노드에게 소스 노드의 고유키를 요구하게 된다. 이 요청을 수신한 클러스터 인증노드는 해당 클러스터 인증노드에게 고유키를 요청한 후 수신한 고유키를 멀티캐스트 노드에게 전달해준다. 이러한 암호화 과정을 통해 악의적인 노드들에 의한 데이터 변조 및 도청 공격에 대한 강건함을 제공해줄 수 있다. <그림 3>은 계층기반 보안 암호 프로토콜의 동작 과정을 보여주고 있다.

Ⅳ. 모의실험 및 결과

4.1 실험 환경

이 장에서는 본 논문에서 제안한 계층기반 보안 암호 프로토콜 기법의 성능을 평가하였다. 성능 평가를 위해 NS-2 시뮬레이터를 이용하였으며, 다음과 같은 환경에서 실험하였다. 실험에 사용한 네트워크의 크기는 1000×1000, 데이터 전송 범위 200m로 하였다. 이동 노드 모델은 random-way point 모델로서 0 ~ 20 m/s 사이의 속도로 이동하고 pause time은 20초로 하였다. 전체 모의실험 시간은 300초로 하였다. 실험 초기에 클러스터를 형성하는 최초 과정에서 악의적인 노드는 클러스터 키를 요청하지 않게 설정하였다. 그리고 제안한 기법의 성능을 측정하기 위해 실험시간 동안 10개의 공격 노드마다 임의의 시간에 각각 5회의 공격을 수행하였다. 단, 이동 노드들의 배터리 소모는 고려하지 않고 실험하였다. <표 1>은 성능 평가를 위한 환경변수 값들을 보여주고 있다.

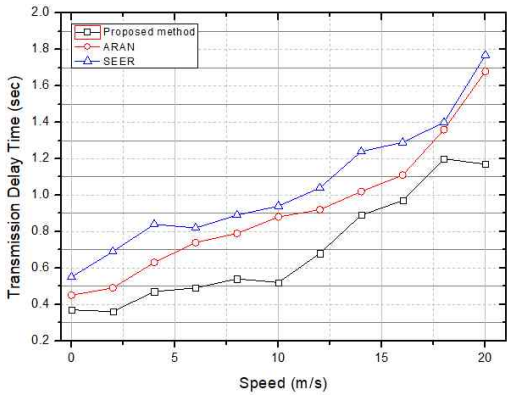
<표 1> 환경 변수

Parameter	Value
Number of Nodes	50, 100
Attack Type	Blackhole
Malicious Node	10
MAC Protocol	IEEE 802.11 DCF
Packet Size	CBR 512 bytes

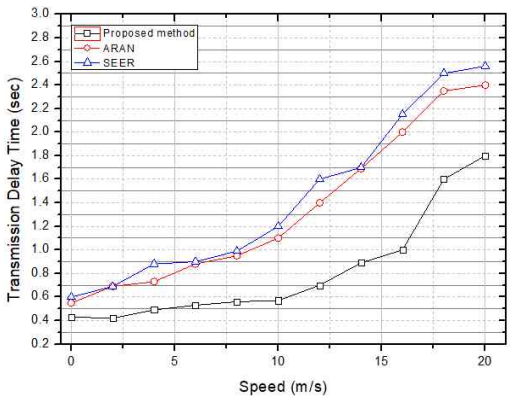
4.2 실험 결과

본 논문에서는 제안한 계층기반 보안 암호 프로토콜의 우수한 성능을 측정하기 위하여 SEER, ARAN 기법들과 비교 실험을 하였으며, 성능 평가 기준은 노드 수와 공격 유무에 따른 패킷 전달 비율과 종단 간 전송 지연 시간으로 하였다.

<그림 4>는 공격 유무에 따른 종단간 전송 지연 시간의 측정 결과를 보여주고 있다. ARAN 기법은 노드들 서로가 소유하고 있는 공개키를 가지고 서로 간의 인증하는 과정을 거쳐 패킷이 전달되기 때문에 지연 시간이 길게 나타났으며, SEER 기법은 단방향 해시 함수를 이용해 베이스스테이션에게 데이터를 달하는데 해시값의 유효성 검증 절차가 없기 때문에 공격에 의한 잘못된 라우팅 정보에 큰 영향을 받아 성능이 떨어졌다. 제안한 기법은 데이터를 수신한 목적 노드가 클러스터 인증 노드에게 소스 노드의 고유키를 수신하는 단계 때문에 다소 지연시간이 길

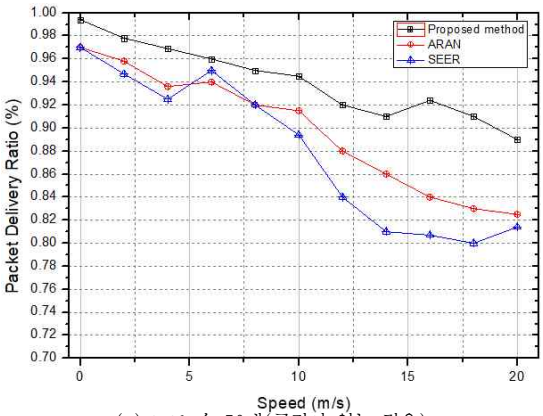


(a) 공격이 없는 경우

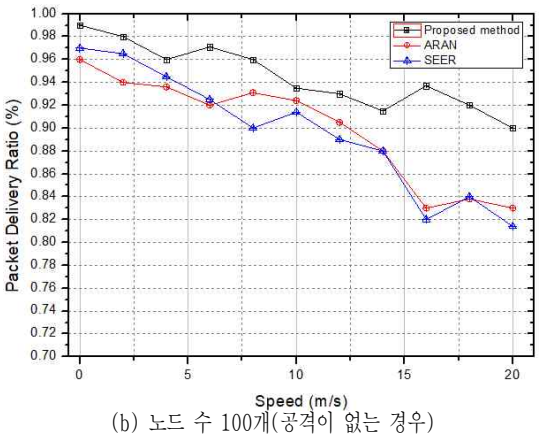


(b) 블랙 홀 공격이 있는 경우

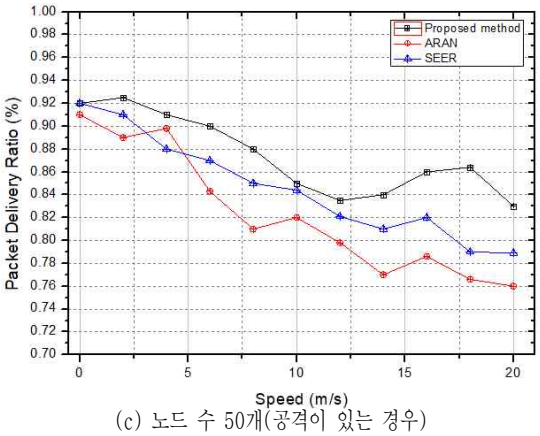
<그림 4> 종단간 전송 지연 시간



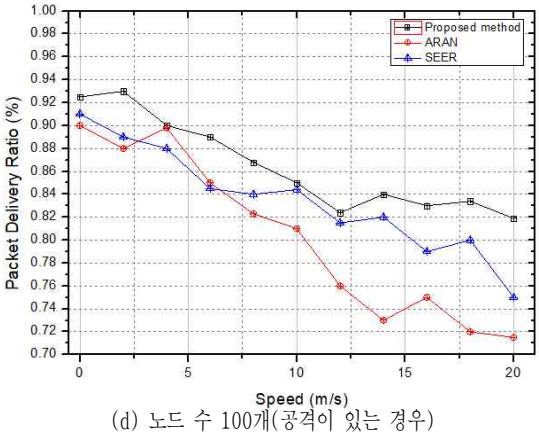
(a) 노드 수 50개(공격이 없는 경우)



(b) 노드 수 100개(공격이 없는 경우)



(c) 노드 수 50개(공격이 있는 경우)



(d) 노드 수 100개(공격이 있는 경우)

<그림 5> 노드 수와 공격 유무에 따른 패킷 전달 비율

었지만 두 단계의 암호화 과정을 통해 공격에는 큰 영향을 받지 않는 성능을 보여주었다.

<그림 5>는 노드 수와 공격 유무에 따른 패킷 전달 비율을 측정하였다. 그림에서 확인할 수 있듯이 ARAN 기법은 노드들의 인증을 위한 공개키 배분 문제와 인증 서버의 선택이 노드들의 이동으로 인해 좋은 결과를 얻지 못하였으며, SEER 기법은 노드들의 이동으로 인한 베이스스테이션을 루트로 하는 트리 생성과 비밀키 관리 때문에 경로 관리가 어려워 성능이 다소 떨어지는 결과를 보여주었다. 제안한 기법은 노드들의 이동이 빈번하게 발생하더라도 계층기반 클러스터 인증노드들 간의 키 공유와 클러스터 인증노드에 의해 노드들이 발급한 클러스터 인증키가 관리되고 노드들의 정보가 유지되기 때문에 패킷 전달 비율에서 우수한 결과를 보여주었다. 다만 데이터 수신시 소스 노드에 대한 고유키 확인을 위한 제어 패킷이 다소 증가하는 결과를 보였다.

Ⅴ. 결론

MANET은 제한된 능력을 갖고 있는 이동 노드들에 의해 다중 홉 방식으로 데이터를 전달하는 네트워크이다. 이러한 특성 때문에 경로 설정이 어렵고 경로 설정 및 데이터 전송에 많은 노드들이 참여하기 때문에 보안 위협에 쉽게 노출되어 있다. 특히 악의적인 노드들에 의한 데이터 위변조 공격은 네트워크 성능을 크게 떨어뜨릴 수 있으며, 멀티캐스트와 같은 그룹통신 환경에서는 그 피해가 더욱 커질 수밖에 없다. 따라서 본 논문에서는 계층기반 보안 암호화 프로토콜 기법 제안을 통해 데이터 위변조 공격에 강건함을 갖고, 전송 데이터에 대한 신뢰성을 향상시키고 무결성을 높였다. 이를 위해서 클러스터 형태의 계층구조를 이용하였으며, 이는 노드들이 암호화에 사용할 수 있는 클러스터 인증키와 고유키의 발급과 관리를 용이함을 높였다. 노드들에게 발급되는 클러스터 인증키는 각 클러스터 인증노드들 간의 공유를 통해 키의 효율성을 높일 수 있었다. 그리고 클러스터 인증키의 노출에 대한 피해를 막기 위해 주기적으로 키를 업데이트 하였다. 또한 각 노드들에 발급되는 고유키를 이용한 블록암호화는 노드들에게 발급되는 클러스터 인증 키쌍이 노출되었다 하더라도 그로 인한 피해를 차단시킬 수 있도록 보안을 더욱 강화할 수 있게 되었다.

제안한 계층기반 보안 암호화 프로토콜 기법의 성능을 측정하기 위하여 SEER 기법, ARAN 기법과 비교 실험하였으며, 실험을 통해 우수한 보안 성능을 확인하였다.

향후에는 암호화의 성능은 높이면서 이동 노드들의 에너지 소모를 줄일 수 있는 경량 암호화 기법에 대한 연구가 수행되어져야 할 것이다.

참고문헌

[1] S. Maity, R. Hansdah, “Self-organized public key management in manets with enhanced security and without certificate-chains,“ Comput. Networks, 2014, pp. 183-211.

[2] H. Rifa-Pous, J., Computational and energy costs of cryptographic algorithms on handheld devices,” in: Future Internet, Vol. 3, 2011, pp. 31-48.

[3] 정관수, “Interactive Multipath Routing Protocol for Improving the Routing Performance in Wireless Sensor Networks,” 디지털산업정보학회지, 제11권, 제3호, 2015, pp. 79-90.

[4] 차시호, 이종언, 류민우, “차량의 이동 방향과 거리 기반의 그리디 애니캐스트 포워딩 프로토콜,” 디지털산업정보학회지, 제13권, 제1호, 2017, pp. 79-85.

[5] K. Hamouid, K. Adi, “Self-certified based trust establishment scheme in ad-hoc networks,“ 5th IFIP International Conference on New Technologies, Mobility and Security, NTMS, IEEE 2012, pp. 1-7.

[6] M. Devi, S.C. Pandian, “An efficient autonomous key management with reduced communication computation costs in mobile ad hoc network,” J. Comput. Sci., Vol. 9, No. 10, 2013, pp. 1260-1266.

[7] P. Memarmoshrefi, R. Seibel, D. Hogrefe, “Bio-inspired self-organized public key authentication mechanism for mobile ad-hoc networks,“ Lect. Notes Inst. Comput. Sci., Soc. Inform. Telecommun. Eng., Vol. 87, 2012, pp. 375-386.

[8] 김정삼, “무선 센서네트워크에서 네트워크수명 극대화 방안,” 디지털산업정보학회지, 제10권, 제4호, 2014, pp. 47-59.

[9] P.B. Velloso, R.P. Laufer, D. Cunha, O.C.M.B. Duarte, G. Pujolle, “Trust management in mobile ad hoc networks using a scalable maturity-based model,” IEEE Transactions on Network and Service Management, Vol. 7, No. 3, 2010, pp. 172-185.

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

[11] F. Bao, I.R. Chen, M. Chang, J.H. Cho, “Hierarchical trust management for wireless sensor networks and its applications to trust-based routing and intrusion detection,” IEEE Transactions on Network and Service Management, Vol. 9, No. 2, 2012, pp. 169-183.

[12] P. Nyeung, J. Ostergaard, “Information and communications systems for control-by-price of distributed energy resources and flexible demand,” IEEE Transactions on Smart Grid, Vol. 2, No. 2, 2011, pp. 334-341.

■ 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 08월 16일
수 정 일 : 2017년 09월 01일
게재확정일 : 2017년 09월 07일