디지털산업정보학회 논문지 제11권 제4호-2015년 12월
http://dx.doi.org/10.17662/ksdim.2015.11.4.061

ZCN과 N2N 인증 기법을 이용한 패킷 전송에 대한 신뢰성 향상에 관한 연구

양 환 석*

A Study on Trust Improvement of Packets Transmission using ZCN and N2N Authentication Technique

Yang Hwanseok

〈Abstract〉

MANET has various vulnerability in wireless network and is more vulnerable in security because central management is not performed. In particular, routing attack may decrease performance of the overall network because the mobile node acts as a router. In this paper, we proposed authentication technique for improving the reliability of the network by increasing the integrity of the routing control packet and blocking effectively attacks that occur frequently in the inside. The proposed technique is consisted of two authentication methods of ZCN and N2N. ZCN authentication method is to elect CA nodes and monitor the role of the CA nodes. N2N authentication method is for an integrity check on the routing packets between nodes. Index key is determined by combining the hop count value to shared key table issued from CA in order to increase the robustness of the internal attack. Also, the overhead of key distribution was reduced by distributing a shared key to nodes certificated from CA. The excellent performance of the proposed method was confirmed through the comparison experiments.

Key Words : Authentication Technique, Secure Routing, Trust Measurement, MANET

Ⅰ. 서론

오늘날 Mobile Ad Hoc Network(MANET)은 인프라스터럭처가 없이 빠르고 쉽게 구축할 수 있는 장점이 있으며, 낮은 비용 때문에 많은 인기를 얻고 있다. MANET을 구성하는 이동 노드들은 자유롭게 이동할 수 있으며, 호스트로서 또는 라우터로서의 역할을 수행한다[1]. 이러한 특성 때문에 네트워크 내부의 악의적인 노드들에 의한 공격은 그 피해가 매우 클 수밖에 없다. 따라서 네트워크의 신뢰성을 높이고 경로 설정 등을 위한 제어 패킷들에 대한 위변조 공격을 차단하기 위한 인증 기법들이 필요하다[2-3].

본 논문에서는 네트워크의 신뢰성을 향상시키고, 라우팅 패킷들에 대한 무결성을 보장하기 위해 영역 기반 인증 기법을 제안하였다. 제안한 인증 기법을 구현하기 위하여 전체 네트워크를 일정한 크기의 영역으로 분할하였으며, ZCN(Zone Certification Node)

*중부대학교 정보보호학과 조교수

인증 기법과 N2N(Node to Node) 인증 기법으로 구성되어 있다. 먼저, ZCN 인증은 각 영역에서 CA 역할을 담당할 노드들에 대한 인증 기법으로서, CA들을 선출하고, 각 CA들에 대한 신뢰 검사를 통해 인증함으로써, 각 영역의 멤버 노드들에 대한 키 발급과 신뢰 검사를 제대로 수행하는지 인증하는 과정이 된다. N2N 인증은 점대점 인증으로서 노드들간의 라우팅 제어 패킷들에 대한 무결성 검사를 통해 내부 공격에 대한 효율적인 차단을 위한 인증 기법이다. 이 기법에서는 멤버 노드들이 CA로부터 신뢰 검사를 통해 공유키 테이블을 발급받는다. 그리고 제어 패킷을 전달할 때 랜덤수와 홉카운트를 조합한 결과값을 인덱스 키 값으로 활용하여 암호화한 후 전달하여 인증하게 된다. 이 인증 기법을 통해 모든 유형의 제어 패킷들에 대한 인증 검사가 가능하게 된다.

본 논문의 구성은 다음과 같다. 2장에서는 MANET에서의 보안 라우팅 기법들의 특징에 대하여 살펴보고 3장에서는 본 논문에서 제안한 인증 기법에 대하여 기술하였다. 4장에서는 비교 실험을 통해 성능평가를 수행하였고 마지막으로 5장에서 결론을 맺는다.

Ⅱ. 관련연구

2.1 보안 라우팅 기법

SRPTES(Secure Routing Protocol based on Token Escrow Set)은 자신의 보안 정보를 직접 저장하지 않고 해당 정보를 신뢰할 수 있는 제 3자가 보관하도록 하여 노드가 공격을 당하더라도 정보가 유출되지 않도록 하는 기법이다. 따라서 보안 정보를 맡길 수 있는 그룹 TES(Token Escrow Set)을 구성해야만 한다. 그리고 이웃 노드들에게 자신의 정보를 요청하여 보안 정보를 완성시키는 토큰 단계를 수행하고, 생성된 토큰을 이용해 라우팅 테이블을 완성하는 라우팅 단계 마지막으로 경로의 무결성을 점검하고 데이터를 전송하는 단계로 구성되어 있다. 이 기법의 단점은 TES 구성이 쉽지 않다는 것이다[4-5].

SEER(Sercure Energy-Efficient Routing) 기법은 단방향 해시 체인을 이용하여 인증을 수행하며, 이동 노드와 베이스스테이션 사이에 기밀성 향상을 위해 공유된 비밀키를 이용하였다. 이 기법은 트리를 생성한 후 단방향 해시 체인을 초기화를 수행한다. 이때 트리의 루트는 베이스스테이션이 된다. 그리고 노드가 이웃 노드를 통해 이벤트를 탐지하면 자신이 선택한 중간 노드를 통해 베이스스테이션에게 데이터가 전달될 수 있게 구성한다. 그리고 안전한 데이터 전송을 위하여 자신이 관리하는 유일한 단방향 해시 체인을 이용한다[6].

SRAODV(Secure Routing with AODV)는 인증된 노드들만이 경로 설정에 참여하도록 하여 AODV의 신뢰성을 향상시킨 기법이다[7]. 이 기법에서는 네트워크에 참여하기 전에 CA로부터 공개키를 발급받아야 하며, 이웃 노드들 사이의 그룹 세션키를 생성하고 이를 이용하여 라우팅과 데이터 포워딩이 이루어진다. 이 기법은 키 교환을 통해 인증을 제공한다. 하지만 악의적인 노드가 소스 노드로부터 받은 패킷을 복사하여 전송할 경우 그 패킷을 전송하는 중간 노드들의 자원 낭비가 발생하는 단점을 가지고 있다[8].

ARAN(A secure Routing protocol for Ad hoc Networks) 기법은 강화된 보안 기능을 제공하기 위하여 소스 노드와 목적 노드 사이의 인증과 노드들 사이의 링크 인증을 사용한다. 이 기법에서는 인증서버가 존재하고, 이를 통해서 반드시 인증서를 발급받아야 한다. 소스 노드는 경로 탐색을 위해 인증서를 비밀키로 서명한 RREQ 패킷을 방송한다. 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[9-10].

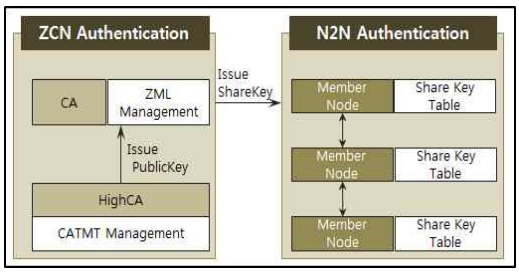
Ⅲ. 제안한 인증 기법

본 장에서는 내부 공격에 대한 강건함을 높이기 위하여 두 개의 인증단계로 구성된 영역 기반 인증 기법에 대하여 기술하였다.

3.1 시스템 구조

이동 노드들로만 구성된 MANET의 신뢰성 향상 및 공격으로 인한 성능 저하를 차단하기 위해서는 노드들에 대한 인증 기법이 매우 중요하다. 왜냐하면 내부 공격자에 의해 제어 패킷 내부의 필드값 조작과 같은 공격은 경로 설정 또는 패킷 유출 등의 막대한 피해를 야기할 수 있기 때문이다. 따라서 본 논문에서는 이러한 내부 공격을 차단하여 신뢰성 향상을 위해 ZCN(Zone Certification Node) 인증과 N2N(Node to Node) 인증 기법을 제안하였다. 제안한 기법에서는 전체 네트워크를 일정한 크기의 영역으로 분할한 영역 기반 구조를 이용하였다. 먼저 ZCN 인증을 위하여 각 영역내에서 1-hop 거리의 이웃 노드가 가장 많은 노드를 CA로 선택하고, 선출된 CA들 중에서 가장 연결수가 높은 노드가 최고 권한을 갖는 CA가 된다. 최고 CA는 주기적으로 CA들의 신뢰를 인증하는 역할을 수행하게 된다. ZCN 인증 기법은 종단간 인증 방식을 적용하였다.

라우팅 패킷을 안전하게 보호하고 메시지의 무결성을 제공하기 위하여 N2N 인증 기법을 적용하였다. N2N 인증 기법은 모든 유형의 제어 패킷들에 대한 검사를 실시하기 위하여 점대점 인증 방식을 적용하였다. 그리고 인증을 위한 키 분배의 오버헤드를 줄이기 위하여 각 영역의 CA로부터 인증 받은 후 키 테이블 생성 방식을 적용하였다. 본 논문에서 제안한 인증 기법의 시스템 모델은 <그림 1>에서 보여주고 있다.

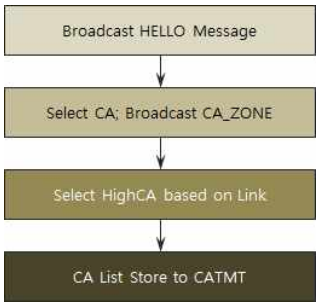


<그림 1> 제안한 시스템 모델 구조

3.2 ZCN 인증 기법

네트워크를 구성하는 노드들에 인증을 위하여 전체 네트워크를 일정한 영역으로 분할한 후 서로가 수신하는 제어 패킷들에 대한 무결성 검사를 통해 인증을 하기 위한 평면 구조를 이용하였다. 하지만 각 영역내의 노드들에 대한 인증서 발급과 키 테이블 제공해주는 역할을 수행할 CA 노드가 필요하다. 따라서 노드들은 자신의 이웃 노드에게 HELLO 메시지를 전송하여 이웃 노드가 가장 많은 노드를 CA로 선출한다. 이렇게 선출된 CA는 자신의 ID를 포함한 CAZONE을 이웃하는 CA들에게 방송하여 연결수가 가장 높은 노드가 HighCA가 된다. <그림 2>는 각 영역의 CA 역할을 수행하는 노드를 선출하는 과정을 보여주고 있다.

HighCA는 각 CA들에 대한 정보를 저장하기 위한 CATMT(CA Trust Measure Table)을 관리하게 되며, CA들에 대한 신뢰 평가는 주기적으로 이루어지게 된다.



<그림 2> CA 선출 과정

또한 CA는 HighCA에게 인증 요청을 위하여 CA_CERT_RQ 방송하면, 이 요청 메시지를 수신한 HighCA는 CH_CERT_RP 메시지를 이용하여 공개키가 서명된 인증서를 발급하게 된다. 인증서는 다음과 같은 내용을 담고 있다.

$CERT\_CA_K$ = [ID, Pub_K,, Trust, Issue_Time, Expire_Time]Pri_K

HighCA에서 각 영역의 CA들에 대한 신뢰 검사를 위한 주기적으로 종단간 인증을 수행한다. HighCA는 CATMT에 등록되어 있는 CA들에게 Key_Update_Time을 이용하여 키 테이블 갱신 시간을 요청하게 된다. 만약 키 테이블 갱신 시간이 주어진 기준 시간보다 늦게 이루어진다면 해당 CA의 신뢰 값을 1씩 감소시킨다. <그림 3>은 CA들에 대한 신뢰 평가 pseudo code를 보여주고 있다.

```
if(SendToHighCA(CA_CERT_RQ))
   SetShareTable(CA_CERT_RP);
while(1) {
    while(CATMT != Null) {
        if(CA_K_Trust != 0) {
            CA_K_Update = SendToCA(CERT_CA_K);
            if(Update_Threshold > CA_K_Update)
                CA_K_Trust - 1;
        }
    }
}
```

<그림 3> 신뢰 평가 pseudo code

3.3 N2N 인증 기법

N2N 인증 기법은 내부 공격 노드들에 의한 패킷 정보 변조와 같은 공격을 차단하기 위하여 적용하였다. 즉, 메시지의 무결성을 제공하기 위해서이다. 이를 위하여 영역내의 모든 노드들은 각 영역의 CA들에게 등록과정을 거치게 된다. 먼저 각 CA는 beacon 방송을 통해 영역내의 노드들을 선택하게 된다. 노드 M이 CA의 beacon을 수신하게 되면 공개키와 함께 JOIN 메시지를 방송하게 된다. CA에서는 노드 M의 공개키를 ZML(Zone Member List)에 저장하고, 각 노드들 간의 인증을 위해서 사용할 키 테이블을 보내주게 된다. 이와 같은 과정을 거쳐서 모든 노드들은 K_0에서 K_{n-1}의 인덱스로 구성된 공유키 테이블을 갖게 된다. 이 공유키 테이블을 이용한 노드들 간의 인증과정은 다음과 같다. 먼저 노드 A에서 패킷 전송시 암호화를 위해서 (랜덤수 + 홉 카운트) % 7의 결과값을 공유키 테이블에서 인덱스 값으로 선택한다. 선택된 키로 암호화 과정을 거친 후 패킷에 추가하여 이웃 노드에게 전송하게 된다. 패킷을 수신한 이웃 노드에서는 홉 카운트와 공유키 테이블의 인덱스를 이용하여 암호화 정보와 그 내용을 비교하게 된다. 비교 결과가 일치한다면 같은 방법으로 암호화하여 이웃 노드에게 패킷을 전달하면 된다. 그러나 만약 내용이 일치하지 않는다면 해당 패킷의 정보는 변조되었다는 것을 의미하기 때문에 이 패킷을 폐기하고, 이웃 노드의 정보를 CA에게 전송하게 된다. 이와 같은 방법을 통해 공격자가 제어 패킷내에 필드 값을 변경하게 된다면 이는 경로상에 존재하는 다른 인증 노드들에 의해 쉽게 탐지될 수 있게 되며, 모든 유형의 라우팅 제어 패킷을 인증할 수 있는 장점을 갖게 된다.

Ⅳ. 성능분석

4.1 실험 환경

본 논문에서 제안한 인증 기법의 성능 평가를 위해서 NS-2 시뮬레이터를 이용하였다. 이동 노드의 모델은 random way point mobility 모델이고 네트워크 크기는 1000 × 1000에 이동 노드 100개, 200개를 위치시켰다. 공격 노드의 수는 10개로 하였으며 300초의 실험 시간동안 black hole attack을 30회 발생시켰다. 실험에 사용한 환경 변수는 <표 1>에서 보여주고 있다.

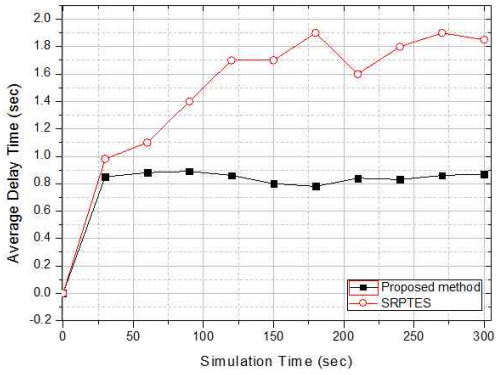
<표 1> 실험에 사용한 환경 변수

Parameter	Value
MAC Protocol	IEEE 802.11 DCF
Speed	0~20 m/s
Packet Size	512 bytes
Transmission Range	250 m
Traffic Rate	10 packet/sec
Traffic	CBR

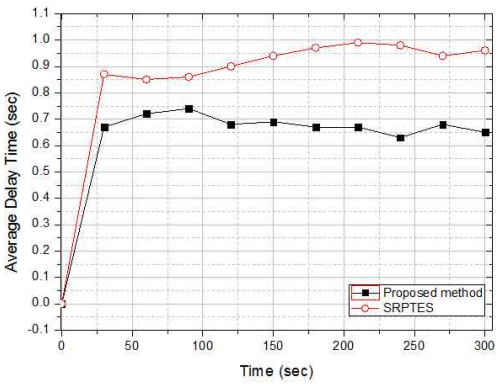
4.2 성능 평가

제안한 인증 기법의 성능 평가를 위해서 SRPTES 기법과 비교 실험을 하였으며, 성능 평가 기준은 종단간 평균 지연 시간, 평균 패킷 전달 비율, 평균 처리율로 설정하였다. 종단간 평균 지연 시간은 소스 노드로부터 목적 노드까지 성공적으로 전송된 패킷의 평균을 나타낸다. 그리고 평균 패킷 전달 비율은 전송한 전체 패킷의 수와 성공적으로 수신한 패킷 수의 비율을 의미한다. 마지막으로 평균 처리율은 시간 동안에 전송된 전체 데이터의 수를 나타낸다.

<그림 4>은 종단간 평균 지연 시간을 측정한 결과를 보여주고 있다. 이 측정 결과는 노드들의 이동에 따른 안정된 패킷 전송의 성능을 의미한다. SRPTES 기법은 노드의 수가 적을 때 성능이 더 좋지 않았다. 이는 노드들의 이동으로 인해 노드 수가 적을 때 TES의 구성이 어렵고, 토큰 상실로 인한 Seed 값 복구가 어려워 성능이 떨어지는 결과를 보였다. 제안한 방법에서는 점대점 인증을 통해 경로상에 존재하는 악의적인 노드들에 대한 배제가 효율적으로 이루어짐에 따라 우수한 결과를 보여주고 있다. 특히 노드들의 이동에도 큰 영향을 받지 않는 것을 확인할 수 있었다. 그림에서 확인할 수 있듯이 제안한 기법이 SRPTES 기법에 비해 평균적으로 약 20% 정도 우수한 성능을 보였다.



(a) 100 노드

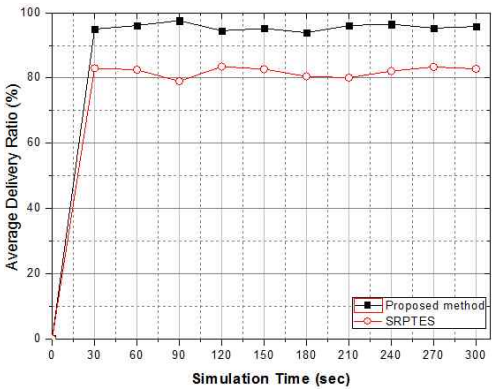


(b) 200 노드

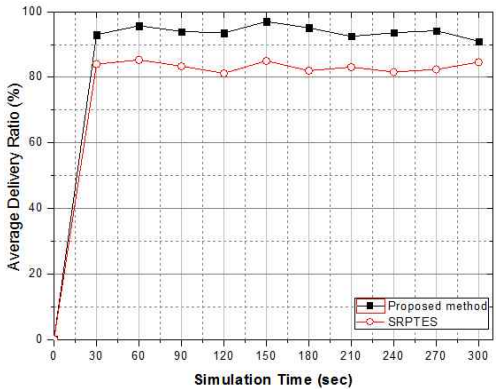
<그림 4> 종단간 평균 지연 시간

평균 패킷 전달 비율은 악의적인 공격 노드들에 의한 공격들에 얼마나 강건한 성능을 보이는지 측정할 수 있는 지표라고 할 수 있다. <그림 5>에서 보듯이 SRPTES 기법은 Seed 체인을 해시 함수를 통해 해시하여 패킷의 위변조 여부를 판단하게 된다. 하지만 노드의 수와 이동으로 인해 노드 밀도가 낮은 지역에서는 TES 구성이 어렵거나 또는 공격 노드가 여기에 포함에 제대로 된 인증이 이루어지 않는 경우가 발생하여 성능이 떨어졌다. 하지만 제안한 기법에서는 라우팅 패킷에 대한 무결성 검사가 N2N 인증 기법을 통해 이루어지기 때문에 악의적인 노드들에 의한 경로 정보 위변조 탐지 성능이 우수하였다. 평균 패킷 전달 비율 실험을 통해서 제안한 기법은 평균적으로 94%의 높은 패킷 전달 비율을 보여주었고 이는 노드들의 수나 이동에 큰 영향을 받지 않으면서 악의적인 노드들에 제어 패킷 변조 공격에 대한 강건함을 확인할 수 있었다.

<그림 6>은 평균 처리율에 대한 결과를 보여주고 있다. 그림에서 보듯이 SRPTES 기법은 노드들의 이동에 따른 문제로 인하여 전체적으로 처리율이 낮게 나타났다. 하지만 제안한 기법에서는 두 과정으로 이루어진 인증 기법으로 패킷 전송을 위한 경로설정시 악의적인 노드들에 대한 탐지가 잘 이루어져 패킷 전송에 안전한 경로가 선택됨에 따라 우수한 처리 결과를 확인할 수 있었다.

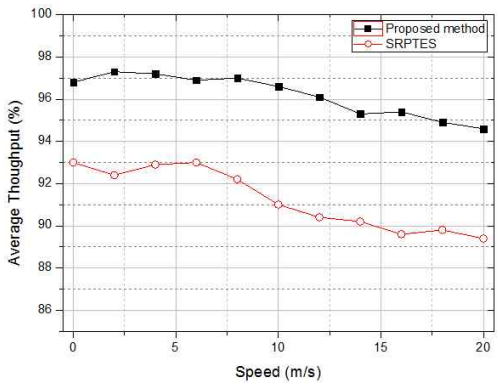


(a) 100 노드



(b) 200 노드

<그림 5> 평균 패킷 전달 비율



<그림 6> 평균 처리율

Ⅴ. 결론

본 논문에서는 라우팅 제어 패킷의 변조 공격을 차단하여 무결성을 보장하고, 네트워크의 신뢰성을 향상시키기 위하여 인증 기법을 제안하였다. 제안한 인증 기법은 크게 ZCN 인증과 N2N 인증 기법으로 구성되어 있다. 제안한 인증 기법을 위해서 전체 네트워크를 일정 크기의 영역으로 분할한 영역 기반 구조를 이용하였다. 먼저 ZCN 인증 기법은 각 영역의

CA 노드를 선출하여 영역내 멤버 노드들에 대한 신뢰 평가를 통해 공유키 발급 역할을 제대로 수행하는지 CA를 인증하는 과정이다. CA들에 대한 인증을 위하여 종단간 인증 방법을 이용하였다. 즉, CA들 중에서 연결성이 가장 높은 HighCA를 선출한 후, CA들에 대한 인증이 이루어지게 된다. N2N 인증은 노드들간의 라우팅 제어 패킷의 무결성을 검사함으로써 내부 공격 노드들에 대한 인증을 수행하게 된다. 즉, CA로부터 공유키 테이블을 발급받은 노드들은 경로 설정시 랜덤수와 홉 카운트를 조합한 결과값을 공유키 테이블의 인덱스 값으로 이용하여 암호화한 후 패킷을 이웃 노드에게 전송한다. 이 패킷을 수신한 이웃 노드는 공유키 테이블로 복호화하였을 때 값의 동일 유무로 제어 패킷의 위변조 여부를 검사하게 되는 방법이다. 이러한 인증 기법을 통해 네트워크의 신뢰성을 크게 향상시켰다. 본 논문에서 제안한 기법의 성능 평가를 위하여 SRPTES 기법과 종단간 평균 지연 시간, 평균 패킷 전달 비율, 평균 처리율을 비교 실험하였으며, 실험을 통해 우수한 성능을 확인할 수 있었다.

참고문헌

[1] Aarti and S. S. Tyagi, “Study of MANET : Characteristics, Challenges, Application and Security Attacks,” International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 3, No. 5, 2013, pp. 252-257.

[2] A. K. Gupta, H. Sadawati and A. K. Verma, “Review of various routing protocols for MANETs,” International Journal of Information and Electronics Engineering, Vol. 1, No. 3, 2011, pp. 251-259.

[3] Shaveta, P. Singh and R. Preet, “Reviewing MANETs & Configuration of Certificate Authority(CA) for node Authentication,” IJCSIT, Vol. 4, No. 6, 2013, pp.974-978.

[4] S. Mishra and N. Mod, “GSM Mobile Authentication Based on User SIM,” IJCST, Vol. 2, Issue 6, 2014, pp. 121-125.

[5] P. Papadimitratos and Z. J. Haas, “Secure Routing: Secure Data Transmission in Mobile Ad Hoc Networks,” Proc. ACM Wksp. Wireless Security 2003, Sept. 2003, pp. 41-50.

[6] Jin-Hee Cho, Ananthram Swami and Ing-Ray Chen, “A Survey on Trust Management for Mobile Ad Hoc Networks for Mobile Ad-Hoc Networks,” IEEE Communication Surveys & Tutorials, Vol. 13, No. 4, 2011, pp. 562-583.

[7] S. Dabideen, B. R. Smith and J. J. Garcia-Luna-Aceves, “An End-to-End Solution for Secure and Survivable Routing in MANETs,” 7th International Workshop on Design of Reliable Communication Networks, Washington DC, 25-28 October 2009, pp. 183-190.

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

[9] Roopaligarg and Himika Sharma, “Comparison between Sybil Attack Detection Technique: Lightweight and Robust,” International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, Vol. 3, issue 2, 2014, pp. 7142-7147.

[10] 양환석, “Wireless Ad Hoc Network에서 보안 영역과 노드 인증을 이용한 보안 라우팅 기법에 관

한 연구," 디지털산업정보학회지, 제10권, 제3호,
2014, pp. 161-169.

■ 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 : 2015년 11월 14일
수 정 일 : 2015년 11월 27일
게재확정일 : 2015년 12월 1일