디지털산업정보학회 논문지 제7권 제4호-2011년 12월

# MANET에서 효율적 역추적을 위한 경로관리에 관한 연구

양 환 석* · 양 정 모**

# *A Study of Path Management to Efficient Traceback Technique for MANET*

Yang, Hwan Seok · Yang, Jeong Mo

〈Abstract〉

Recently, MANET(Mobile Ad-hoc Network) is developing increasingly in the wireless network. MANET has weakness because phases change frequently and MANET doesn't have middle management system. Every node which consists of MANET has to perform data forwarding, but traceback is not reliable if these nodes do malicious action owing to attack. It also is not easy to find location of attacker when it is attacked as moving of nodes. In this paper, we propose a hierarchical-based traceback method that reduce waste of memory and can manage path information efficiently. In order to manage trace path information and reduce using resource in the cluster head after network is formed to cluster, method which recomposes the path efficiently is proposed. Proposed method in this paper can reduce path trace failure rate remarkably due to moving of nodes. It can also reduce the cost for traceback and time it takes to collect information.

Key Words : Traceback, Mobile Ad Hoc Network, Intrusion Detection System

## Ⅰ. 서론

최근에 무선 인터넷은 인터넷과 더불어 네트워크의 급속한 발전으로 광범위한 분야에 널리 사용되고 있다. MANET(Mobile Ad-hoc Network)은 무선 네트워크의 연구 분야 중의 하나로 상당히 발전하고 있는 기술이다[1]. MANET은 고정된 인프라 없이 이동 노드들로 구성되어 있으며, 근거리 통신망, 가정 내 개인용 장치들 사이의 통신등 활용 분야가 다양해지고 있다. MANET을 구성하는 이동 노드들은 제한된 자원과 연산 능력 때문에 자원을 효율적으로 사용해야만 한다. 그리고 노드들의 이동성으로 인해 네트워크 위상의 변화가 수시로 이루어지며, 모든 노드들이 데이터 전달 기능을 수행해야 하기 때문에 보안에 취약점을 가지고 있다[2]. 특히 이동 노드로만 구성되어있기 때문에 공격이 탐지되었을 때 역추적 과정이 쉽지 않다는 것이다. 그리고 역추적에 제공되는 경로 정보의 신뢰성에 대한 문제가 있다. 왜냐하면 MANET을 구성하는 모든 노드들은 상황에 따라 라우터의 역할을 수행해야 한다. 그런데 이러한 노드가 공격을 당해 악의적인 동작을 수행한다면 역추적 과정을 신뢰할 수 없게 된다. 그리고 역추적을 하는데 필요한 경로 정보 자료를 수집하는데 오랜 시간이 걸리면 역추적 정확성이

* 중부대학교 정보보호학과 전임강사
** 중부대학교 정보보호학과 교수

떨어질 수 있고, 제한된 자원으로 인해 역추적을 어렵게 만들 수도 있다.

본 논문에서는 MANET을 구성하는 전체 네트워크를 클러스터로 구성한 후, 각 클러스터들 사이의 역추적을 위한 정보의 관리 기법과 추적 경로를 효율적으로 구성하는 방법을 제안하였다. 그리고 클러스터 헤드에 의해 역추적이 수행되기 때문에 노드들의 이동으로 인한 추적 경로의 재구성 성공률이 높아졌으며, 역추적을 위한 트래픽도 감소하였다.

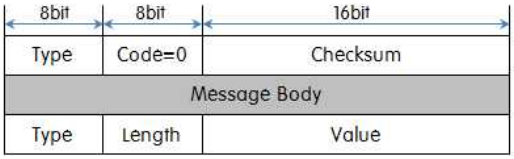
본 논문의 구성은 다음과 같다. 2장에서는 역추적 기법의 종류 및 특징에 대하여 살펴보고 3장에서는 제안한 방법에 대해 기술하였다. 4장에서는 제안한 방법의 성능을 평가하고 5장에서는 결론을 맺는다.

## Ⅱ. 관련연구

MANET을 구성하는 노드들은 라우터 기능을 수행하는데 이러한 노드들이 공격으로 인해 악의적인 행동을 하게 된다면 역추적은 불가능하게 된다. 그리고 노드들의 이동으로 인해 공격자의 위치를 찾아내는 것 또한 쉽지 않다. 본 장에서는 기존의 역추적 기법들의 특징에 대하여 살펴보도록 한다.

### 2.1 역추적 기법의 종류

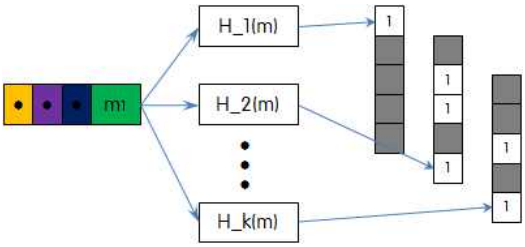
MANET은 노드들의 이동으로 인한 위상이 수시로 변하고 자원이 제한적이기 때문에 기존의 유선 환경에서 사용되었던 역추적 기법들을 그대로 적용할 수가 없다. 역추적 기법은 크게 ICMP 메시지를 사용한 기법, 로깅을 이용한 기법, PPM을 적용한 기법으로 나눌 수 있다. IP의 역추적을 위해 IETF가 제안하는 ICMP 기반의 iTrace-CP 방법이 있다[3]. 이 기법은 각 지역 네트워크에 설치된 에이전트가 역추적시 iTrace 메시지를 생성하여 서버에 전송하게 되고, 관리 네트워크에 설치된 서버는 각 지역 네트워크에 설치된 에이전트들로부터 수신한 iTrace 메시지를 이용하여 침입자의 역추적을 수행하게 된다. <그림 2>는 iTrace 메시지의 구조를 보여주고 있다.




<그림 1> iTrace 메시지 구조

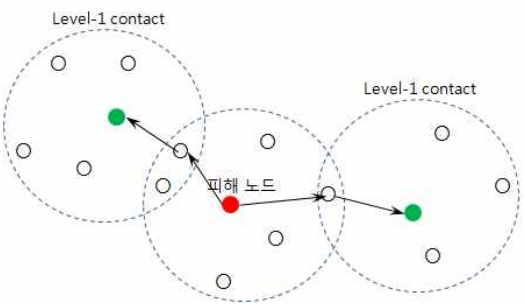
iTrace-CP 기법은 ICMP 메시지를 생성하여 목적지까지 IP 패킷과 함께 동일한 경로를 사용하여 전달된다. 패킷이 목적지까지 가는 모든 경로 정보를 ICMP 메시지에 저장함으로써 역추적을 가능하게 하는 것이다. 이 기법의 단점은 공격자의 위치를 역추적하기 위해서는 ICMP 메시지를 수집해야하며, 따라서 공격자의 위치가 이동되는 경우에는 추적이 쉽지 않다는 것이다. 두 번째로 로깅을 이용한 기법으로는 Hotspot-based Traceback, SWAT(Small World-based Attacker Traceback) 등이 있다[4-5]. Hotspot-based traceback 기법은 Bloom filter에 감시된 패킷의 TTL(Time-to-Live) 정보를 저장할 수 있는 TBF(Tagged Bloom Filter)를 이용한 역추적 기법이다. Bloom filter는 매우 간단한 비트-벡터를 사용하여 입력 값이 특정 집합에 속하는 요소인지를 판단해주는 필터이다. Bloom filter의 크기를 m, 저장될 요소의 수를 n이라고 할 때, 모든 요소에 대하여 k 개의 해싱 함수를 사용하여 k 개의 해싱 인덱스 값을 구하되 해싱 인덱스 값은 1에서 m 사이에 있도록 한다. 이 값은 m-bit bloom filter의 주소 값으로 사용되며, 이 주소에 해당하는 비트-벡터 값을 1로 설정한다. <그림 2>는 2차원 bloom filter의 구조를 보여주고 있다. 이 기법은 TBF에 저장된 TTL 정보와 인접 노드들의 정보를 이용하여 공격자를 추적하게 된다. 이 기법은 인접 노드들의 정보를 이용하기 때문에 공격자의 위치까지의 전체 경로를 추적하는 것이 아

니고 공격 경로 중의 신뢰할 수 있는 경로의 일부분을 찾는 것을 목표로 한다. 그리고 역추적을 위한 요청이 브로드캐스 기반이기 때문에 네트워크의 성능이 상당히 떨어질 수 있는 가능성이 있다.




<그림 2> 2차원 Bloom filter

SWAT 기법은 트래픽의 패턴과 양을 비교하여 트래픽의 시그니쳐를 생성한다. 그리고 이 정보를 이용하여 공격자를 역추적하는 기법이다. 따라서 공격 경로의 정보를 제공해주는 노드를 효과적으로 찾기 위해 <그림 3>과 같이 small world-based contact model을 확장하여 적용하였다.




<그림 3> small world-based contact 생성

공격이 탐지되었을 때 피해 노드는 <그림 3>과 같이 먼저 인접 contact를 구성한 후에 이들에게 역추적 요청 메시지를 송신한다. 이후에 수신된 트래픽의 패턴과 양을 비교하여 실제 공격 위치를 찾아간다. 이 기법에서는 모든 노드들이 네트워크의 트랙픽을 감시해야하기 때문에 오버헤드가 높다는 단점이 있다. 마지막으로 PPM을 사용한 기법으로 Contact-based Traceback 기법과 ZSBT 기법이 있다[6-7]. Contact-based Traceback 기법은 PPM 기법을 그대로 무선 네트워크에 적용한 기법으로 sink 노드와 contact들 사이의 메시지 교환을 통해 역추적을 수행한다. 그리고 ZSBT 기법은 전체 네트워크를 zone으로 나눈 후, 특정 노드를 지나는 패킷에 IP 주소 대신에 노드가 속한 zone-id를 추가하는 기법이다. 그리고 나머지 과정은 유선 환경에서의 PPM 기법과 거의 유사하다. 이 기법의 단점은 역추적 과정의 주체가 피해 노드이기 때문에 역추적 과정의 신뢰도가 떨어진다는 점이다. 그리고 zone의 크기에 따라 역추적 정보 수집에 시간이 길어진다. 표 1은 위에서 설명한 역추적 기법들의 특징을 비교하였다.

<표 1> 역추적 기법의 특징 비교

| 기 법 | 특 징 | 단 점 |
|---|---|---|
| ICMP | • IP패킷과 함께 동일한 경로 사용<br>• 목적지까지의 모든 경로를 ICMP 메시지에 저장 | • 공격자의 위치 변동시 역추적이 쉽지 않음 |
| PPM | • 일정한 확률로 패킷에 정보 마크<br>• 지연발생시 패킷의 크기가 늘어나지 않음 | • 역추적을 위한 최소한의 패킷의 필요<br>• 패킷의 단편화 발생시 역추적 불가능 |
| Logging | • 자신을 통한 모든 패킷에 정보 저장<br>• 공격이 완료된 후에도 역추적 가능 | • 자원과 시간이 많이 요구됨<br>• 많은 로그 정보의 관리 |

## Ⅲ. 제안한 방법

본 장에서는 MANET을 구성하는 전체 네트워크를 클러스터 형태로 구성한 후, 각 클러스터들 사이의 역추적을 위한 정보의 관리 기법과 추적 경로를 효율적으로 구성하는 방법을 제안하였다.

### 3.1 클러스터의 형성

본 논문에서는 자원의 낭비를 줄이면서 경로 정보를 효율적으로 관리할 수 있는 역추적 기법을 제안하였다. 따라서 MANET을 구성하는 전체 노드를 1-hop 거리에 있는 이웃 노드들로 클러스터를 형성한다. 클러스터를 형성 후 전체 클러스터를 관리하는 클러스터 헤드를 선출할 때, 링크 수뿐만 아니라 신뢰도 값을 이용하였다. 왜냐하면, 공격자 역추적시 악의적인 행동을 하여 역추적을 방해하는 노드들을 배제하기 위해서이다. 뿐만 아니라 링크 수가 많은 클러스터 헤드는 많은 경로 정보를 유지할 수 있기 때문에 보다 정확한 추적 경로를 제공할 수 있게 된다.

### 3.2 역추적 정보의 수집

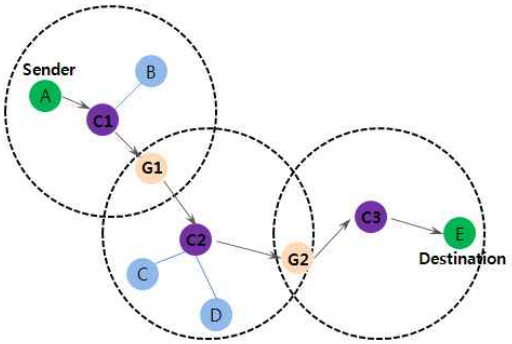
네트워크를 구성하는 모든 노드들은 패킷을 전송할 때, 자신이 속한 클러스터 헤드에게 <그림 4>와 같은 구조의 역추적 정보를 송신한다.

| Own IP Address | | |
|---|---|---|
| Sender IP Address | | |
| Own Trust Value | Hash Value | TTL |

<그림 4> 역추적 정보 구조

위 <그림 4>에서 보여준 구조에서 해시 함수는 SHA-1을 사용했고 신뢰도 값은 0 ~ 10 범위의 값을 갖으며, 네트워크에 처음으로 참여하는 노드는 초기 값으로 1을 갖도록 설정된다. <그림 5>에서는 송신 노드 A가 목적지 노드 E에게 패킷을 전송하는 과정을 보여주고 있으며 각 클러스터 헤드들은 <그림 4>의 구조의 역추적 정보를 수집하게 된다.

클러스터 헤드는 인접한 노드로부터 수신한 역추적 정보를 근거로 하여 패킷의 흐름을 재구성하게 된다. 그



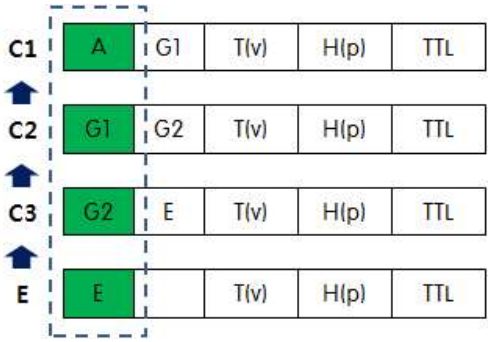

<그림 5> 역추적 경로 수집 과정

리고 각 클러스터 헤드가 멤버 노드로부터 수신한 모든 정보를 저장 및 유지하게 된다면 클러스터 헤드의 자원 소모에 대한 문제가 발생하게 될 것이다. 그리고 이러한 문제는 클러스터내의 멤버 노드의 수가 많아진다면 문제는 더욱더 커지게 된다. 따라서 각 클러스터 헤드는 소스 노드와 추적 경로의 터미널 노드 IP주소 그리고 신뢰도 값, 해쉬 값, TTL 값을 저장한다. 위 <그림 5>에서 클러스터 헤드 C1은 멤버 노드 A, B, G로부터 수신한 역추적 정보를 기반으로 (A, G, T(v), H(p), TTL)의 경로 정보를 저장하게 된다. 이렇게 추적 경로의 정보를 계산하여 저장하면 클러스터 헤드의 자원의 낭비를 막을 수 있을 뿐만 아니라 멤버 노드들이 증가하여도 자원의 사용량이 크게 증가하지 않는다.

### 3.3 클러스터간의 역추적

앞 절에서 설명하였던 방법으로 각 클러스터 헤드는 자신들의 멤버 노드들로부터 수신한 역추적 정보를 저장하고 있다. 만약 <그림 5>의 노드 E로부터 패킷 p에 대한 역추적이 요청되었다고 가정한다면 클러스터간의 역추적 정보의 교환 과정은 <그림 6>과 같이 계산된다.

먼저 노드 E는 자신이 속한 클러스터 헤드 C3에게 자신의 IP 주소와 패킷 p에 대한 해쉬 값, 신뢰도 값 그리고 TTL 값을 전송한다. 역추적 요청을 수신한 클러스터




<그림 6> 클러스터간 역추적 경로 계산

헤드 C3는 인접한 클러스터 헤드 C2에게 쿼리를 송신하게 된다. 같은 방법으로 이 쿼리는 클러스터 헤드 C1까지 전달되게 된다. <그림 6>은 각 클러스터 헤드가 저장한 역추적 정보를 기반으로 한 추적 정보 계산 과정을 보여주고 있다. 그림에서 나타나듯이 각 클러스터 헤드가 패킷 p에 대해 저장하고 있는 추적 정보를 확인해 보면 relay 노드의 IP 주소가 중복됨을 확인할 수 있게 된다. 따라서 중복된 노드를 제거하게 되면 추적 경로는 E → A임을 알 수 있게 된다.

# Ⅳ. 실험 및 결과

## 4.1 실험 환경

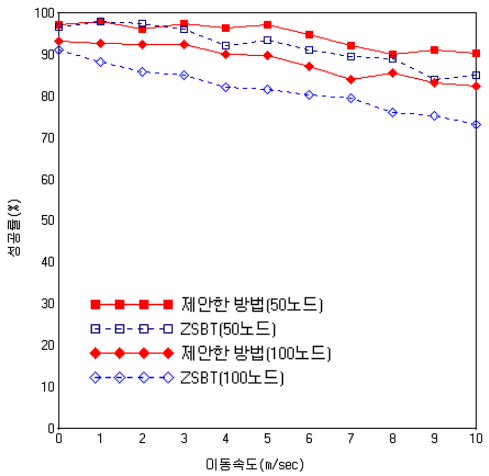
본 논문에서 제안한 역추적 기법의 성능을 분석하기 위해 클러스터링 기법에 기반을 둔 ZSBT 기법과 비교 실험하였다. 실험을 위해서 <표 1>에서와 같은 환경에서 ns-2 시뮬레이터를 이용하였다. 실험에 사용한 노드의 수는 50개, 100개이고 각 실험 시간은 300초로 하였다. 패킷의 크기는 64byte, 데이터 전송 범위는 200m로 하였으며 10번 반복 실험 하였다. 그리고 본 논문에서는 각 노드들의 배터리 소모량은 고려하지 않고 실험하였다.

<표 1> 실험 환경

| | |
|---|---|
| 네트워크 크기 | 1000m × 1000m |
| 이동속도 | 0 ~ 10 m/s |
| 라우팅 프로토콜 | AODV |
| MAC 프로토콜 | IEEE 802.11 DCF |
| 이동성 모델 | Random way point |

## 4.2 실험 결과

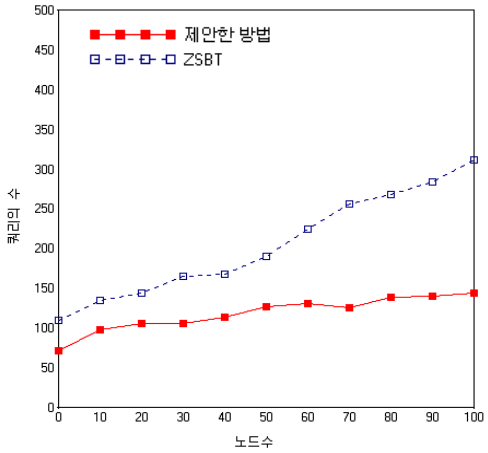
본 논문에서 제안한 기법의 효율성을 평가하기 위하여 추적 경로의 성공 비율, 경로 추적 쿼리의 수, 자원의 사용량 측정을 평가의 기준으로 하였다. <그림 7>에서는 제안한 기법과 ZSBT 기법과의 역추적 성공률을 측정하였다. 그림에서 나타난 것처럼 제안한 기법이 평균적으로 ZSBT 기법에 비해서 높은 성공률을 보였다. 특히 노드들의 이동 속도가 빨라졌을 때도 제안한 기법이 높은 성공률을 유지하였다. 노드들의 빠른 이동으로 인한 역추적 정보의 부족을 클러스터링을 이용한 집중화도 추적 경로 정보 관리를 통하여 막을 수 있었다.



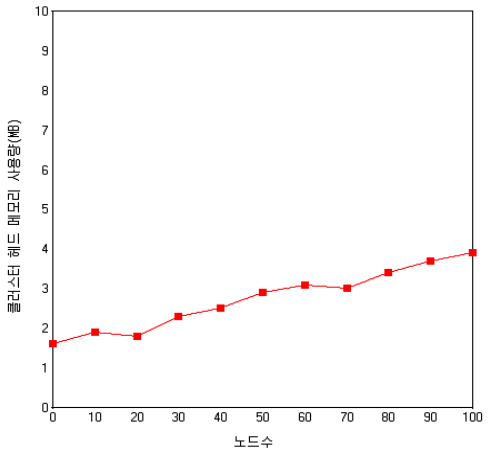

<그림 7> 역추적 성공률

노드들 사이에 역추적을 위한 전송된 쿼리의 수를 측

적하였다. 쿼리의 수가 많아질수록 네트워크 전체의 성능은 저하된다. <그림 8>에서 알 수 있듯이 노드들의 수에 비례하여 쿼리의 수도 증가하였다. 반면에 제안한 기법은 클러스터 헤드들 사이에서 역추적이 수행되고 해쉬값을 저장한 노드들이 쿼리를 전송하기 때문에 노드들의 수가 많다하더라도 쿼리의 수가 크게 증가하지 않았다.

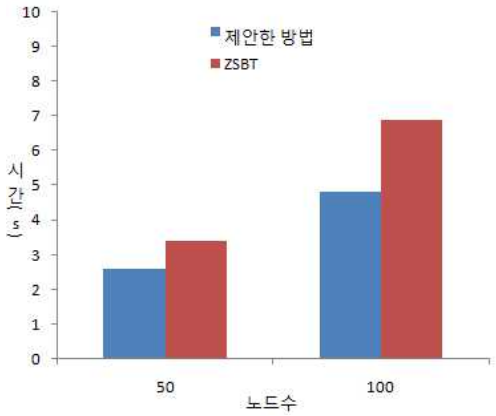



<그림 8> 경로 추적을 위한 쿼리 수




<그림 9> 클러스터 헤드의 메모리 사용량

제안한 기법에서 추적 경로의 정보는 멤버 노드들로부터 수신한 경로 정보를 계산한 후 클러스터 헤드에 저장된다. 따라서 클러스터 헤드들의 메모리 소모를 측정하였다. <그림 9>에서 볼 수 있듯이 네트워크의 노드의 수가 100개일 경우에도 클러스터 헤드의 메모리 소모량은 4M정도임을 확인할 수 있었다. 그리고 제안한 방법에서 역추적에 대한 요구 시간이 ZSBT 기법에 비해 적은 시간이 소요되었다. 왜냐하면 ZSBT 기법에서는 역추적을 위해 네트워크내에 모든 노드들에게 쿼리를 송신한 후 정보를 수집하기 때문에 많은 시간이 소모된다. 게다가 수집된 정보의 구별도 어렵고 상당한 시간이 소요되기 때문이다. 반면에 제한한 기법에서는 클러스터 헤드들 사이에서만 역추적 정보가 교환되기 때문에 그만큼 요구 시간도 줄어들게 되었다. <그림 10>에서는 노드가 50개, 100개일 때 역추적에 대한 정보를 얻는데 걸린 평균시간을 보여주고 있다.




<그림 10> 역추적 경로 요구 평균시간

## Ⅳ. 결론

본 논문에서는 MANET에서 DoS나 DDoS 공격시 공격자의 위치를 찾기 위한 역추적 기법을 제안하였다. 네트워크를 구성하는 전체 노드를 클러스터로 형성한 후 클러스터 헤드에서 추적 경로 정보를 관리하고 자원의

사용량을 줄이기 위하여 경로를 효율적으로 재구성하는 기법을 제안하였다. 본 논문에서 제안한 기법은 노드들의 이동으로 인해 야기되는 경로 추적 실패 비율을 현저히 줄일 수 있었다. 그리고 역추적을 위한 비용을 줄이고 정보 수집의 시간을 단축시킬 수 있었다.

## 참고문헌


[1] 유응구, "MANET에서의 에너지를 고려한 라우팅 프로토콜," 디지털산업정보학회, 디지털산업정보학회논문지 제3권, 제 3호, 2007.

[2] 최윤정, "침입탐지시스템의 정확도 향상을 위한 개선된 데이터마이닝 방법론," 디지털산업정보학회, 디지털산업정보학회논문지 제6권, 제 1호, 2010.

[3] S. M. Bellovin, "ICMP Traceback Messages," Internet Draft:dfaft-bellovin-itrace-00. txt, March 2000.

[4] Y. Huang and W. Lee, "Hotspot-based Traceback for Mobile Ad Hoc Networks," Proceedings of the ACM Workshop on Wireless Security, September 2005.

[5] Y. kim and A. Helmy, "SWAT: Small World-based Attacker Traceback in Ad-hoc Networks," Proceedings of the 36th Hawaii International Conference on System Science, HICSS'03, 2002, p.57a.

[6] Q. Zhang, X. Zhou, F. Yang, and X. Li, "Contact-based Traceback in Wireless Sensor Networks," Proceedings of the International Conference on Wireless Communications, Networking and Mobile Computing 2007 (WiCom2007), September 2007, pp. 2487-2490.

[7] X. Jin, Y. Zhang, Y. Pan, and Y. Zhou, "ZSBT:A Novel Algorithm for Tracing DoS Attackers in MANETs," EURASIP Journal of Wireless Communications and Networking, Vol. 2006, Article ID 96157, 2006, pp. 1-9.


■ 저자소개 ■


양 환 석
Yang, Hwan Seok

2011년 9월~현재
중부대학교 정보보호학과 전임강사
2002년 2월 조선대학교 전산통계학과(이학박사)
1998년 2월 조선대학교 전산통계학과(이학석사)
1996년 2월 호원대학교 전산계산학과(이학사)

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

양 정 모
Yang, Jeong Mo

1997년 3월~현재
중부대학교 정보보호학과 교수
1997년 2월 단국대학교 수학과(이학박사)
1989년 2월 동국대학교 수학과(이학석사)
1984년 2월 동국대학교 수학과(이학사)

관심분야 : 정보보호, 암호수학, 암호학
E-mail : jmyang@joongbu.ac.kr



논문접수일 : 2011년 9월 28일
수 정 일 : 2011년 10월 17일
게재확정일 : 2011년 10월 20일