https://doi.org/10.33778/kcsa.2021.21.1.121

협업 기법을 이용한 침입탐지 탐지 방법에 관한 연구★

양 환 석*

요 약

무선 노드 외에 어떠한 인프라도 존재하지 않는 MANET은 빠른 네트워크 구성할 수 있는 장점을 가지고 있다. 하지만 노드들의 이동, 무선 매체 등은 MANET이 가지고 있는 보안 취약점의 원인이기도 하다. 특히 네트워크상에 존재하는 공격 노드들에 의한 그 피해는 다른 네트워크에 비해 상당히 크다. 따라서 공격노드들에 대한 탐지 기법과 공격으로 인한 피해를 줄이는 기법도 반드시 필요하다. 본 논문에서는 침입탐지의 효율성을 높이기 위한 계층구조 기법과 공격으로 인한 피해를 줄이기 위해 P2P 메시 네트워크 구성 기법을 적용한 협업 기반 침입탐지 기법을 제안하였다. 제안한 기법에서는 클러스터내 노드들에 대한 신뢰도 평가를 통해 사전에 공격 노드에 대한 네트워크 참여를 배제하였다. 그리고 공격 노드에 의한 공격이 탐지되면 클러스터 헤드간의 P2P 메시 네트워크를 통해 네트워크 전역에 공격 노드 정보를 빠르게 전달함으로써 공격 노드의 피해를 최소화하는 방법을 적용하였다. 제안한 기법의 성능 평가를 위해 ns-2 시뮬레이터를 이용하였으며, 비교 실험을 통해 제안한 기법의 우수한 성능을 확인할 수 있었다.

A Study on Intrusion Detection Method using Collaborative Technique

Yang Hwan Seok*

ABSTRACT

MANET, which does not have any infrastructure other than wireless nodes, has the advantage of being able to construct a fast network. However, the movement of nodes and wireless media are also the causes of security vulnerabilities of MANET. In particular, the damage caused by the attacking nodes existing on the network is considerably greater than that of other networks. Therefore, it is necessary to detection technique for attacking nodes and techniques to reduce damage caused by attacks. In this paper, we proposed a hierarchical structure technique to increase the efficiency of intrusion detection and collaboration-based intrusion detection technique applying a P2P mesh network configuration technique to reduce damage caused by attacks. There was excluded the network participation of the attacking node in advance through the reliability evaluation of the nodes in the cluster. In addition, when an attack by an attacking node is detected, this paper was applied a method of minimizing the damage of the attacking node by transmitting quickly the attack node information to the global network through the P2P mesh network between cluster heads. The ns-2 simulator was used to evaluate the performance of the proposed technique, and the excellent performance of the proposed technique was confirmed through comparative experiments.

Key words : Intrusion Detection, Mobile Ad-hoc Network, P2P Mesh Network, Security

접수일(2021년 03월 03일), 수정일(1차: 2021년 03월 30일), 게재확정일(2021년 03월 31일)

* 중부대학교/정보보호학과

★ 이 논문은 2020년도 중부대학교 학술연구비 지원에 의하여 이루어진 것임.

1. 서 론

MANET(Mobile Ad-hoc Network)은 어떠한 인프라의 도움 없이 무선 노드로만 구성된 네트워크이다. 이러한 특성 때문에 네트워크 구성 어려운 상황에서 빠르게 네트워크를 구성할 수 있는 장점을 가지고 있다[1]. 하지만 무선 노드로만 구성되어 있기 때문에 네트워크에 참여하는 모든 노드들이 라우터 역할을 수행해야만 한다. 하지만 노드들의 이동으로 인한 동적인 토폴로지 특성으로 인해 많은 보안 취약점을 갖고 있다[2]. 따라서 악의적인 노드가 경로 설정 혹은 네트워크에 참여하게 된다면 그 피해는 다른 네트워크에 비해 훨씬 크다. 그리고 전체 네트워크의 성능이 크게 저하될 수 있다. 이러한 문제를 해결하기 위해 그 동안 보안 라우팅 기법, 침입탐지 기법, 노드 신뢰 평가 등 다양한 분야에서 연구가 진행되어 왔다[3].

본 논문에서는 악의적인 노드들에 대한 효율적 탐지와 그 피해를 최소화하기 위하여 협업 기반의 침입탐지 기법을 제안하였다. 제안한 기법에서는 공격 탐지의 효율성을 높이기 위하여 계층 구조를 이용하였다. 전체 네트워크를 클러스터로 구성한 후 클러스터 내의 노드들에 대한 정보를 관리하기 위하여 클러스터 헤드를 선출하였다. 클러스터 헤드 노드는 클러스터내의 모든 노드들에 대한 인증을 수행하고, 신뢰 정보를 유지하는 역할을 수행하게 된다. 또한 전체 네트워크에 존재하는 클러스터 헤드들은 P2P 기반의 메시 네트워크를 구성하여 공격이 발생했을 때 이에 대응하도록 하였다. 만약 악의적인 노드가 특정 클러스터에 존재하고 공격이 탐지된다면 해당 클러스터 헤드는 자신과 연결되어 있는 모든 클러스터 헤드에게 공격 노드의 정보를 방송하여 전체 네트워크에서 공격 노드를 배제시킴으로써 그 피해를 줄이게 된다.

본 논문의 구성은 다음과 같다. 2장에서는 MANET에서의 공격 유형 및 탐지 기법에 대하여 살펴보고 3장에서는 본 논문에서 제안한 협업 기반 공격 탐지 기법에 대해 기술하였다. 4장에서는 제안한 기법의 성능 평가를 위해 실험하고 마지막으로 5장에서 결론을 맺는다.

2. 관련연구

2.1 공격 탐지 기법

PCBHA(Prevention of a Co-operative Black Hole Attack) 기법은 AODV 라우팅 프로토콜을 수정하였으며, 모든 합법적인 사용자에게 기본적인 신뢰 수준을 할당한다[4]. 그리고 소스 노드가 방송한 RREQ에 응답한 이웃 노드들중에서 신뢰 값이 가장 높은 이웃 노드를 선택하여 데이터 전송을 수행한다. 소스 노드가 목적 노드로부터 ACK 메시지를 수신하면 데이터 전송에 참여한 이웃 노드들의 신뢰 값을 1 증가시키고, 그렇지 않다면 1을 감소시킨다. 이는 경로상에 블랙홀 노드가 존재한다는 것을 의미하며, 해당 경로를 통한 데이터 패킷을 모두 폐기한다.

CBSR(Curve Based Secure Routing)은 데이터 암호화를 적용한 기법으로서 경로 설정이 5단계로 이루어진다[5]. 이동 노드는 자신의 위치정보를 그룹 키를 이용하여 암호화한 후 이웃에게 전송한다. 그리고 목적 노드에게 자신의 위치와 필요한 정보를 키 체인 중 하나를 이용하여 암호화하여 전송한다. 그리고 경로 설정을 위해 글로벌 키로 암호화 키를 암호화한 후 방송한다. 이러한 과정을 거쳐 라우팅 경로를 형성하게 되는데 이때 설정된 경로는 다중화하게 된다. 목적 노드에서는 여러 경로에서 온 패킷들을 전송받아 내용을 비교하여 변경된 것이 있는지를 판단하게 된다.

2.2 공격 유형

라우팅 프로토콜의 취약점을 이용한 공격은 크게 패킷을 도청 또는 감청을 통해 정보를 탈취해가는 passive 공격과 패킷의 주입이나 삭제 또는 변경을 통해 패킷 전송이 불가능하게하고, 네트워크 전체를 마비시킬 수 있는 active 공격이 있다. 그 피해가 큰 active 공격에는 다음과 같은 공격들이 있다[6, 7].

- 블랙홀 공격 : 악의적인 노드가 위조된 패킷을 소스 노드에게 전송하여 라우팅 경로를 변경하는 공격
- 웜홀 공격 : 두 개의 악의적인 노드가 정상적인 경로보다 최적의 경로인 것처럼 속여 패킷

을 훔치는 공격

- DoS 공격 : 악의적인 노드가 잘못된 RREQ, 데이터 패킷을 전송하여 특정 노드의 자원을 고갈시켜 서비스가 불가능하도록 만드는 공격

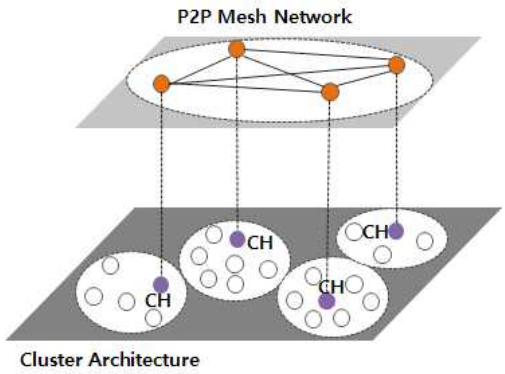
이러한 공격들은 각각의 계층에서 다양한 형태의 공격이 가능하다.

3. 협업기반 공격탐지 기법

본 장에서는 하이브리드 구조를 적용한 협업 기반 침입탐지 기법에 대해 설명하였다. 제안한 기법은 침입탐지의 성능을 높이기 위해서 계층구조 기반 메시 네트워크를 적용하였다.

3.1 시스템 구조

본 논문에서는 공격 탐지의 성능을 향상시키기 위하여 계층 구조와 협업 방식을 적용하였다. 공격 탐지를 위해 네트워크에 참여하는 노드들의 관리를 위하여 계층구조인 클러스터 구조를 적용하였다. 이를 위하여 전체 네트워크를 클러스터로 형성한 후 각 클러스터내의 노드를 관리하기 위하여 클러스터 헤드를 선출하였다. 클러스터 헤드 선출은 클러스터 형성 후 모든 노드가 자신의 상태를 방송한 후 이웃 노드의 수가 가장 많은 노드를 클러스터 헤드로 선출하게 된다. 클러스터 헤드 노드는 자신이 관리하는 클러스터내의 모든 노드들에 대한 신뢰도 값을 관리하게 된다. 네트워크에 처음 참여하는 노드들은 모두 비인증 노드가 된다. 비인증 노드들은 클러스터 헤드로부터 신뢰도를 평가받은 후 멤버 노드로 승인을 받게 된다. 그리고 DoS, DDoS와 같은 공격에 의한 네트워크 마비, 혹은 데이터 전송 오류로 인한 심각한 피해를 차단하기 위해서 협업 방식을 적용하였다. 이를 위해 클러스터 헤드들 간의 P2P 기반 메시 네트워크를 구성하여 서로 관리하는 노드들의 정보 교환 및 악의적인 공격 발생 시 해당 경로를 이용함으로써 그 피해를 최소화 시킬 수 있도록 하였다. 본 논문에서 적용한 네트워크 구조를 (그림 1)에서 보여주고 있다.



(그림 1) 네트워크 구조

3.2 계층구조를 이용한 공격 탐지

본 논문에서는 계층구조인 클러스터를 이용하여 공격 탐지 기법을 적용한다. 이를 위해서 각 클러스터 헤드가 클러스터내 멤버 노드들에 대한 신뢰평가 기법을 제안하였다. 클러스터내 멤버 노드들은 클러스터 헤드로부터 신뢰도 측정을 받을 때 사용되는 매개변수로 경로 응답 시간, 패킷 전달 비율로 하였다. 멤버 노드들에 대한 평가는 각 노드들이 패킷 송수신때 이루어지며, 클러스터 헤드에서는 각 노드들에 대한 패킷 전송 비율, 경로 응답 시간, 이동 시간 정보, 신뢰도, 상태 등의 정보를 관리하게 된다.

각 노드들은 이웃 노드로부터 RREQ 패킷을 수신하게 되면 클러스터 헤드에게 해당 노드의 상태와 신뢰값을 확인한 후, 인증이 된 멤버 노드인 경우에는 패킷을 전달하지만, 신뢰도 값은 높지만 패킷 전달 비율과 경로 응답 비율이 클러스터내 평균 이하인 경우에는 클러스터 헤드로부터 수신한 기준값 범위 이내에서 패킷 전달이 이루어진다. 그러나 신뢰값도 평균 이하이고 패킷 전달 비율과 경로 응답 비율이 클러스터내 평균 이하인 경우에는 해당 패킷을 폐기하게 된다. 이와 같은 방법으로 신뢰받지 못한 노드의 RREQ 패킷의 전달과 응답을 제한함으로써 악의적인 노드들의 플러딩 공격을 막을 수 있게 된다. 그리고 데이터 플러딩을 차단하기 위해서는 다음과 같은 과정을 거치게 된다. 먼저 이웃 노드로부터 패킷을 수신하면 해당 노드에 대한 정보를 확인하게 된다. 만약 확인된 값들이 클러스터내 평균 이상이면 패킷은 전달되지만

그렇지 않다면 패킷은 폐기되고 이웃 노드의 신뢰도는 감소하게 된다. 그리고 클러스터내 평균 이하의 노드로부터 패킷을 수신하면, 신뢰도 값뿐만 아니라 무결성 검사를 실시하게 된다. 이러한 방법으로 플러딩 공격을 방지할 수 있게 된다.

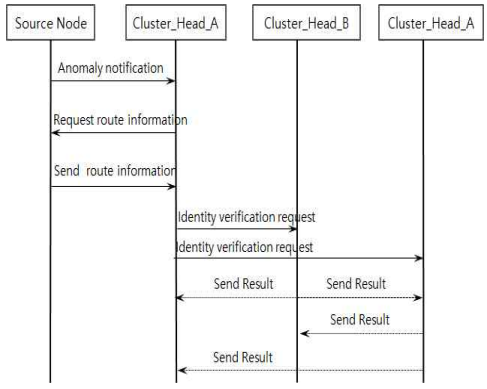
```
while(True) {

    if(Packet.type == RREQ){
        for(i = 0; i <= Buffer; i++) {
            if(src_Addr.trust() >= clusterAvg()) {
                packet[i].broadcast();
            else if((transmit.ratio() >= transmit.avg()) ||
                    (reponse.time() >= reponse.avg())) {
                packet[i].broadcast();
            else
                packet[i].drop();
            }
        }

    else {
        if(src_Addr.trust() >= clusterAvg()) {
                packet[i].dst_Addr.forward();
            else if((transmit.ratio() >= transmit.avg()) ||
                    (reponse.time() >= reponse.avg())) {
                packet[i].dst_Addr.forward();
            else
                packet[i].drop();
                src_Addr.trust().decrease();
            }
        }
}
```

(그림 2) 계층구조를 이용한 공격탐지의사코드

3.3 P2P 메시 기반 공격 대응

소스 노드와 목적 노드간의 경로 설정 단계나 데이터 전송 단계에서 악의적인 공격 노드들에 의한 공격은 좁게는 노드들간의 패킷 전송에 영향을 미칠 수 있으며, 넓게는 전체 네트워크 성능에 큰 영향을 미칠 수도 있다. 따라서 본 논문에서는 공격 노드들에 의한 공격이 발생하더라도 그 피해를 최소화하고 그에 대응할 수 있도록 하기 위하여 P2P 메시 기반 기법을 적용하였다. 본 논문에서는 적용한 네트워크 구조는 계층 구조인 클러스터 구조를 적용하였다. 이때 선출되었던 각 클러스터내의 클러스터 헤드 노드들은 공격 대응을 위해 서로가 P2P 메시 네트워크로 연결한 후 유지하게 된다.

만약 특정 노드에서 공격으로 인해 데이터 전송이 이루어지지 않는다면 해당 노드는 자신이 속한 클러스터 헤드에게 목적 노드까지의 경로를 전송하게 된다. 해당 경로 정보를 수신한 클러스터 헤드는 자신과 연결되어 있는 모든 클러스터 헤드 노드에게 경로 정보를 전달하게 된다. 이를 수신한 클러스터 헤드는 자신의 클러스터내에 해당 노드의 존재 여부를 확인한 후 만약에 존재한다면 해당 노드의 신뢰도 검사를 진행하게 된다. 만약 해당 노드의 신뢰도가 높고 패킷 전송 비율, 경로 응답 시간이 평균 이상이면 이를 무시하지만, 만약 기준값 이하의 정보를 갖는 노드라면 해당 노드에 대한 정보를 모든 클러스터 헤드에게 전송하여 해당 노드를 네트워크에 참여하는 것을 배제시키게 된다. 이와같은 기법을 적용함으로써 공격 노드에 의한 네트워크 성능 저하를 차단하고 공격 발생시 다른 경로를 통해 데이터 전송이 이루어질 수 있도록 지원하게 된다. 그림 3은 P2P 메시 기반 절차를 보여주고 있다.



(그림 3) P2P 기반 공격 대응 절차

4. 실험 및 결과

4.1 실험 환경

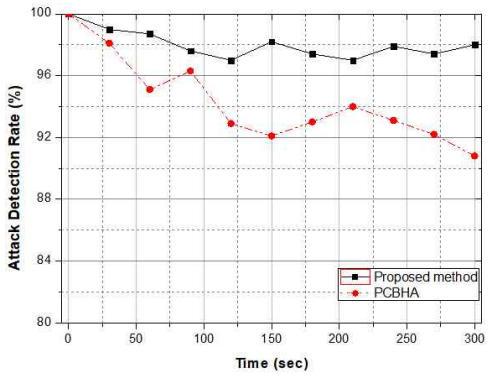
본 장에서는 협업 기반 침입탐기 기법의 성능을 평가하였다.이를 위하여 ns-2 시뮬레이터를 이용하였으며, 실험에 사용한 네트워크의 크기는 1500×1500, 전송 범위는 150m로 하였다. 이동 노드 모델은 random-way point 모델이고 실험 시간동안 10번의 공격을 발생하였다. 본 논문에서는 이동 노드들의 배터리 소모는 고려하지 않았다. 실험에 사용한 환경변수는 <표 1>에서 보여주고 있다.

<표 1> 실험에 사용한 환경 변수

Parameter	Value
Number of Nodes	150
Pause Time(Sec)	20
Routing Protocol	AODV
Traffic	CBR

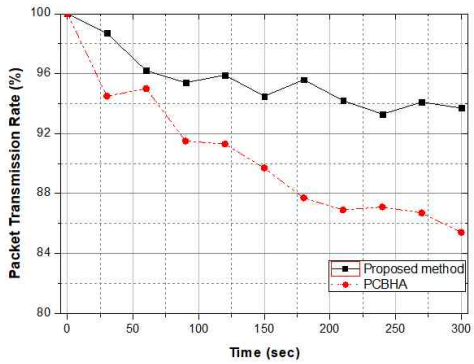
4.2 실험 결과 분석

본 논문에서 제안한 공격탐지 기법의 우수성을 평가하기 위하여 PABHA 기법과 비교 실험하였으며, 성능 평가 기준은 공격 노드 탐지율, 패킷 전달 비율, 그리고 블랙홀 공격에 따른 오탐율로 설정하였다. 블랙홀 공격에 따른 TPR(True Positive Rate)과 FPR(False Positive Rate)를 측정하였다.



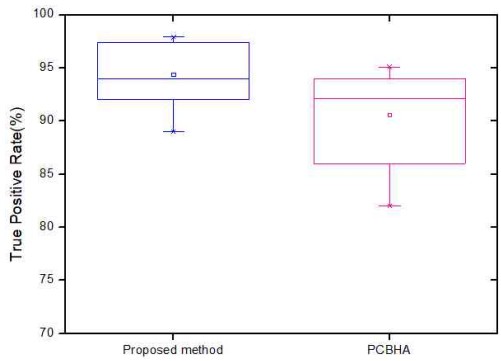
(그림 4) 공격 탐지율

실험 시간동안 발생한 공격 노드에 대한 탐지율에 대한 결과는 (그림 4)에서 보여주고 있다. 그림에서 보여주듯이 공격 탐지율은 제안한 기법이 가장 높은 탐지 결과를 보여주고 있다. PCBHA 기법은 소스 노드와 직접 RREQ 패킷을 주고 받은 노드들에 대해서는 신뢰 평가가 이루어져 공격 탐지가 가능하지만 소스 노드와 목적 노드 사이의 경로밖에서 이루어지는 공격들에 대한 탐지율은 현저히 떨어지는 결과를 보였다. 제안한 기법에서는 각 클러스터 헤드에서 클러스터내의 노드들로부터 공격 노드에 대한 정보를 받고 해당 공격 노드에 대한 정보를 P2P 메시 네트워크를 이용하여 전체 네트워크의 클러스터 헤드에게 전달함으로써 해당 노드에 대한 팀지와 그 피해를 최소화할 수 있는 결과를 보여주었다.



(그림 5) 패킷 전송 비율

(그림 5)는 실험 시간동안 10번의 공격을 발생시켰을 때 노드들간의 패킷 전달 비율을 측정한 결과이다. 이 실험은 공격 발생시 이를 탐지하고 이에 대한 대응 능력을 측정하고자 한 실험으로써 공격 발생시 공격 노드가 참여하는 목적 노드까지의 경로를 빠르게 설정할 수 있는 능력을 확인하였다. PCBHA 기법은 소스 노드와 목적 노드 사이의 공격에 대해서는 빠르게 대응하여 그 결과가 나쁘지 않았으며, 제안한 기법은 소스 노드와 목적 노드 사이의 공격이 아닌 다른 공격들에 대해서도 빠르게 정보를 전달할 수 있어 우수한 결과를 보여주었다.



(그림 6) 블랙홀 공격 오탐율

블랙홀 공격에 따른 오탐율 결과를 (그림 6)에서

보여주고 있다. PCBHA 기법은 소스 노드와 목적 노드간의 경로 설정 후 공격에 대한 판단이 이루어지기 때문에 노드들의 이동으로 인한 경로 재설정등에 의해 오탐율이 증가하였으며, 제안한 기법에서는 계층구조와 협업을 적용하여 공격 탐지를 판단하기 때문에 오탐율이 상대적으로 낮은 결과를 보였다.

5. 결 론

MANET은 어떠한 인프라의 도움 없이 이동 노드로만 구성되어 있기 때문에 다양한 보안 취약점이 존재한다. 특히, 네트워크에 참여하는 모든 노드들이 라우터 역할을 수행하야 하기 때문에 악의적인 노드에 의한 잘못된 행동은 전체 네트워크에 커다란 피해를 입힐 수 있다. 따라서 네트워크에 존재하는 공격 노드들에 대한 탐지와 그 공격으로 인해 피해를 줄일 수 있는 대책이 반드시 필요하다.

본 논문에서는 이러한 악의적인 노드들에 의한 공격을 효율적으로 탐지하기 위하여 계층구조인 클러스터 형태를 적용하였으며, 공격 노드에 의한 피해를 최소화 시키기 위하여 클러스터 헤드간의 P2P 메시 네트워크를 구성하여 정보를 공유할 수 있는 협업 기법을 제안하였다. 클러스터 내의 모든 노드들에 대한 평가는 클러스터 헤드에 의해서 이루어지며, 클러스터 헤드에서 멤버 노드들에 대한 정보를 유지하게 된다. 그리고 각 클러스터 헤드들은 P2P 방식의 메시 네트워크를 구성하고 있으면서 특정 클러스터 헤드로부터 공격 노드에 대한 정보를 수신하게 된다면 해당 자신과 연결된 다른 클러스터 헤드에게 이를 방송하게 된다. 이렇게 공유된 공격 노드의 정보를 이용하여 네트워크 참여를 배제시킴으로써 공격으로 인한 피해를 최소화시킬 수 있게 하였다. 본 논문에서 제안한 기법의 성능 평가는 PABHA 기법과 비교 실험을 하였으며 실험을 통해 침입탐지의 우수성을 확인할 수 있었다.

참고문헌

[1] E Vishnu Balan, M K Priyan, C Gokulnath and G Vsha Devi, "Fuzzy Based Intrusion Detection Systems in MANET", science direct elsevier Procedia Computer Science, vol. 50, pp. 109-114, 2015.

[2] S. S. Zalte and V. R. Ghorpade2, "Pre-Path and Post-Path Security to Mobile Adhoc Network", 2017 IJSRSET, vol. 3, pp. 575-578.

[3] S. Sreenivasa Chakravarthi and Suresh Veluru, "A Review on Intrusion Detection Techniques and Intrusion Detection systems in MANETS", 2014 Sixth International Conference on Computational Intelligence and Communication Networks 2014 IEEE, pp. 730-737.

[4] Naeem Razal, Muhammad Umar Aftabl, Muhammad Qasim Akbar2, Omair Ashraf3 and Muhammad Irfan4, "Mobile Ad-Hoc Networks Applications and Its Challenges" in Communications and Network, pp. 131-136, 2016.

[5] Tarek M. Mahmoud, Abdelmgeid A. Aly and M. Omar Makram, "A Modified AODV Routing Protocol to Avoid Black Hole Attack in MANETs", International Journal of Computer Applications (0975-8887), vol. 109, no. 6, pp. 27-33, January 2015.

[6] Meddeb, R., Triki, B., Jmili, F., & Korbaa, O., "An effective IDS against routing attacks on mobile ad hoc networks", Frontiers in Artificial Intelligence and Applications, pp. 201 - 204, 2018.

[7] Borkar, A., Donode, A., & Kumari, A., "A survey on intrusion detection system (IDS) and internal intrusion detection and protection system (SA-IDPS)", In 2017 International conference on inventive computing and informatics (ICICI).

〔저자소개〕

양 환 석 (Hwan-seok Yang)
1998년 2월 조선대학교 이학석사
2005년 2월 조선대학교 이학박사
2007년 3월 호원대학교 연구교수
2011년 9월 ~ 현재 중부대학교
정보보호학과 부교수
email : yanghs@joongbu.ac.kr