Ad-hoc 네트워크에서 ICMP메시지를 이용한 공격 근원지 역추적 기법

정기석*

요 약

Ad-hoc 네트워크는 노드가 자유롭게 이동하면서 네트워크를 구성하는 것으로 기존 유선 인터넷망에서와 같은 공격이 가능하기 때문에 유선망에서의 역추적기법들을 Ad-hoc네트워크에 적용하려는 연구가 이루어지고 있다. 본 논문에서는 DDos공격에 대한 제어기능을 제공하는 iTrace기법을 사용해서 Ad-hoc 네트워크에서 스푸핑된 DDos패킷에 대한 IP 근원지를 역추적할 수 있는 새로운 기법을 제안한다. 제안된 기법은 ICMP형태의 역추적 메시지를 구현하고 지역 네트워크에 배치되는 에이전트와 관리네트워크에 배치되는 서버 사이에 역추적 경로를 구성하여 근원지 역추적을 수행한다. 또한 제안된 기법은 공격이 종료되어도 공격자의 위치를 추적할 수 있으며 IETF에서 제안한 방식을 사용함으로써 표준화를 통해 확장성을 가지고 있다고 할 수 있다. 성능 평가결과 부하, 무결성, 안전성 및 역추적 기능에서 개선된 특징을 보인다.

An Attack Origin Traceback Mechanism using ICMP Message on Ad-hoc Network

Jeong Gi Seog*

ABSTRACT

Ad-hoc network is composed of mobile nodes and has a vulnerability of attack like on conventional wire networks. So, many studies have been conducted to apply the traceback mechanism on wire network to Ad-hoc network. In this paper, a new mechanism that can trace back to IP source of spoofing DDoS packet using iTrace message on Ad-hoc network is proposed. The proposed mechanism implements ICMP Traceback message and the traceback path between agents allocated in local network and a server located in management network. Also the proposed mechanism can trace the position of attacker even after an attack is over and has extendability through standardization by using a mechanism that IETF proposed. Result of performance evaluation shows a great improvement in terms of load, integrity, safety, traceback function as compared with conventional mechanisms.

Key words : Vulnerability, DDoS, Traceback, Ad-hoc Network, ICMP Message

접수일(2013년 6월 7일), 수정일(1차:2013년 6월 17일), 게재확정일(2013년 6월 18일)

* 영동대학교 정보통신보안학과

1. 서 론

Ad-hoc네트워크는 통신 인프라가 없는 지역에서 신속하게 전개될 수 있고 이동 노드들간에 자율적으로 조직 가능한(self organizing)통신망이다. 노드들은 무선인터페이스를 가지며 호스트와 라우터의 기능을 동시에 가진다[1]. Ad-hoc네트워크는 구조적으로 네트워크 중간에서 제어노드, AP(access point) 등 네트워크 디바이스가 없다. 각 노드들은 노드가 구비하고 있는 기능과 자원 그리고 정보를 이용하여 네트워크를 구성하고 통신해야 한다. 노드는 하드웨어적으로 인접노드와 통신을 위하여 인입과 인출포트를 포함하고 있으며 프로세스는 라우팅태스크와 로컬태스크를 처리할 수 있도록 고려되어 있다. 두 통신 노드의 거리가 먼 경우에는 다른 노드들을 경유하여 통신경로를 형성하는데 노드와 노드 사이에 형성되는 통신경로를 홉(hop)이라고 부른다. 노드간 홉에 의하여 형성되는 경로가 길어질수록 통신에 소요되는 자원과 비용이 증가한다. 노드와 홉에 의하여 구성되는 네트워크 토폴로지를 인프라스트럭처리스(infrastructure less) 네트워크라고 부르며 이 방식은 고정된 라우팅 방식에 비하여 노드 이동이 자유롭고 네트워크 위상(topology)이 동적으로 변하는 특징이 있다.

Ad-hoc 네트워크에서의 공격 근원지에 대한 역추적방식은 네트워크상에 패킷이 전송되는 과정에서 사전에 라우터는 역추적 경로 정보를 생성하여 이를 패킷에 삽입하거나 패킷의 목적지 IP주소로 전달하여 주기적으로 관리하는 방식이다. 해킹 공격이 발생하면 이미 생성·수집된 역추적 정보를 분석하여 해킹 공격의 근원지를 찾는 방법이다. 역추적기법으로는 PPM (Probabilistic Packet Marking)기법[2], ICMP 메시지를 변형한 iTrace기법[3] 등이 사용되고 있다. Ad- hoc 네트워크 역시 기존 유선망에서와 같은 다양한 공격, SYN flooding과 같은 서비스거부공격 등이 가능하기 때문에 유선망에서의 역추적기법들을 Ad-hoc네트워크에 적용하려는 연구가 이루어지고 있다[4]. 따라서 본 논문에서는 DDos공격에 대한 제어기능을 제공하는 iTrace기법을 사용해서 Ad-hoc 네트워크에서 스푸핑된 DDos패킷에 대한 IP근원지를 역추적할 수 있는 새로운 기법을 제안한다.

본 논문의 구성은 2장에서 Ad-hoc네트워크 보안에 대해서 살펴보고 3장에서는 역추적기술에 대해서 분석하고 4장에서 제안한 iTrace기법을 소개하고 5장에서 성능분석을 한다. 마지막으로 6장에서 결론을 맺는다.

2. 관련연구

2.1 Ad-hoc 네트워크 특징

노드의 이동성으로 인해 Ad-hoc네트워크의 위상은 끊임없이 변한다. 이러한 Ad-hoc네트워크의 특징은 응용 솔루션을 요구하고 접근방법은 고정망의 환경과는 매우 다르게 다루어져야 한다. 이러한 특징의 Ad-hoc네트워크를 이동성(mobile), 다중홉(multi-hop) 그리고 다중매체(multimedia)의 3M네트워크라고도 한다[5].

주요한 Ad-hoc네트워크의 특징을 정리하면 다음과 같다.

- 모든 노드는 이동성을 가진다.
- 노드들은 종단시스템과 중계시스템의 역할을 모두 수행한다. 즉, 호스트와 라우터의 기능을 동시에 가진다.
- 네트워크의 위상은 동적으로 변화한다.
- 이동 노드는 배터리의 제약을 받는다.
- 불안정한 링크 특성을 가지며 무선 대역폭의 제약과 채널 품질이 다양하다.
- 여러 노드 간의 협력을 통한 분산운영 기능을 갖는다.

2.2 Ad-hoc 네트워크의 제한사항

Ad-hoc네트워크는 여러 측면에서 다음과 같은 제한사항을 가지고 있다.

- 동적인 위상변화(dynamic topology)
  노드의 이동성으로 인해 Ad-hoc네트워크의 위상은 지속적으로 변한다. 다중홉인 네트워크의 위상은 임의적이고 빠르게 변할 수 있다.

• 대역폭 제약
Ad-hoc네트워크에서 가용한 대역폭은 고정네트워크에 비해 매우 낮은 용량을 갖는다.

• 에너지 제약
Ad-hoc네트워크의 노드들은 배터리로 동작하기 때문에 배터리에 의존적일 수밖에 없다.

• 보안문제
Ad-hoc네트워크는 노드의 이동성 문제로 인하여 보안에 심각한 문제를 가지고 있는데 아직까지 충분한 해결방안이 제시되지 못하고 있는 실정이다.

2.3 Ad-hoc 네트워크 보안

보안 문제는 일반 유선 네트워크에서도 존재하고 있지만 이동 Ad-hoc네트워크는 무선 인터페이스를 사용하기 때문에 유선네트워크에 비해 훨씬 더 많은 위험에 노출되어 있다. 기본적으로는 Ad-hoc네트워크의 보안 요구 조건은 다른 통신네트워크에서 요구되는 것과 동일하다. 그러나 이동 Ad-hoc네트워크에서는 노드의 신분이 서로에게 불확실한 경우가 많으며 멀티홉방식에 의해 라우팅을 할 경우 악의적인 중간 노드에 의해 발생될 수 있는 데이터의 무결성 및 기밀성 문제가 존재한다. Ad-hoc네트워크는 같은 물리적 위치에 놓인 노드간에 자연발생적으로 조성되므로 모든 노드가 다른 노드에 대한 신뢰할 만한 공개키를 갖거나 다른 노드의 신뢰 증명에 대한 보증을 할 수 없다. 따라서 키 사이에 신뢰할 수 있는 관계를 형성하고 이를 이동 Ad-hoc네트워크 전반에 분배하는 것이 주요 과제가 된다.

3. 역추적 기술

3.1 Ad-hoc네트워크 역추적 기술

역추적(traceback)은 통신네트워크(인터넷)를 이용하여 공격을 시도하는 공격자의 위치를 실시간으로 분석하고 추적하는 기술을 말한다. 역추적은 통신환경과 연결방법에 따라 다양한 방법이 존재하며, 각 역추적 방법에 따라 다양한 기법이 적용된다. 연결방법, 대응방식, 적용기법에 따라 분류할 수 있으며 연결방법에 따라 분류하면 TCP연결 역추적과 IP역추적으로 구분할 수 있다. TCP연결 역추적은 TCP통신방식의 특성을 이용하여 연결 지향성 통신방식에서 사용되는 역추적방식이다. 이 방식은 주로 연결 체인의 특성을 이용하여 역추적한다. 반면 IP역추적기법은 비연결지향성 통신방식을 이용하여 공격을 당한 시스템에 남겨진 로그를 분석하고 그 흔적으로 공격자의 위치를 추적한다.

Ad-hoc 네트워크 역추적기술은 IP기반 역추적 기술들을 바탕으로 연구되고 있다. 하지만 앞에서 언급된 Ad-hoc네트워크의 제한사항으로 인해서 유선 IP 환경에서 이용되는 역추적기술을 Ad-hoc네트워크에서 그대로 적용할 수 없으며 Ad-hoc 네트워크에서 역추적을 어렵게 한다[6].

3.2 기존 역추적 기술 분석

IP역추적 기술은 해킹 공격에 대해 스푸핑된 공격 패킷의 근원지 IP를 역추적할 수 있는 기술로서 IP역추적을 위해 공격 경로와 패킷의 송신자를 추적한다. 대표적인 기법으로는 패킷을 중심으로 마킹 방법론을 사용한 기법, ICMP프로토콜과 같은 프로토콜 등에 대한 변형을 통해 근원지 패킷의 전달경로 정보를 관리하는 기법 그리고 네트워크 구조 측면에서 관리 프로토콜을 이용하는 방법 등이 있다[7]. 각각의 기법은 인터넷 환경에서 DoS 및 DDoS공격에 장단점을 가지고 있으며, 적용방법 및 해킹공격의 특성에 따라서 각기 다른 성능을 보인다.

(1) Proactive tracing

네트워크상에 패킷이 전송되는 과정에서 사전에 역추적 경로 정보를 생성하여 이를 패킷에 삽입하여 목적지로 전달하는 방법으로, 주기적인 관리하에서 해킹 공격이 발생하면 이미 생성·수집된 역추적 경로 정보를 분석하여 해킹공격의 근원지를 찾는 방법이다.

1)PPM(probabilistic packet marking)기법

PPM은 네트워크를 구성하는 라우터에서 자신을

지나는 패킷에 라우터 정보를 삽입하여 스푸핑된 패킷의 실제 경로를 찾는 방법으로 라우터에서는 패킷 IP헤더에 자신의 IP주소를 마킹하여 다음 라우터에 전송한다. 라우터에는 많은 패킷이 지나가기 때문에 일정한 확률로 패킷을 샘플링하는 노드샘플링(node sampling), 에지샘플링(edge sampling)등을 이용하여 네트워크 상태를 유지한다. 마킹된 패킷을 받은 후 시스템이 공격을 받게 되면 수집된 패킷의 헤더 정보를 가지고 공격 경로를 재구성하여 공격자의 위치를 추적한다.

2)iTrace(ICMP Traceback)

iTrace는 라우터에서 일정한 확률로 패킷을 샘플링하여 ICMP메시지에 역추적정보를 삽입한 후 피해자에게 송신함으로써 역추적정보를 전달하는 기법이다.

확률적으로 샘플링한다는 측면에서는 확률적 패킷 마킹 기법과 비슷하게 보일 수 있으나 샘플링된 패킷에 역추적정보를 마킹하는 것이 아니라 라우터가 ICMP메시지를 발생시켜 message body부분에 라우터가 생성한 역추적정보를 구성한 후 패킷의 목적지로 전달한다.

iTrace메시지는 ICMP패킷의 message body에 역추적 정보를 입력한 메시지이다. iTrace메시지를 생성할 때 초기 TTL(Time To Live)필드값은 255로 설정되어 전달된다. iTrace메시지를 받은 시스템은 공격이 발생하면 라우터가 생성한 iTrace 메시지의 TTL값을 확인하여 홉 단위로 공격경로를 추적한다.

(2) Reactive tracing

해킹 시도가 발견되면 연결되어 있는 상태에서 공격경로를 홉 단계로 추적해 공격근원지를 추적해 가는 기법이다.

1)해쉬기반 역추적

해쉬기반 역추적기법은 SPIE(source path isolation engine)역추적 관리 시스템을 중심으로 네트워크내에 서브그룹을 구성하여 네트워크를 관리한다[8].

SPIE는 DGA(data generation agent)를 가지는 라우터, SCARs(SPIE Collection and Reduction Agents), STM(SPIE Traceback Manager)로 구성된다. 패킷이 라우터를 통과할 때 라우터에 포함되어 있는 DGA가 해당 패킷의 IP헤더 및 페이로드를 이용해 해쉬 데이터를 생성하고 bloom filter구조로 저장한다. SCARs는 특정 네트워크 영역을 담당하고 역추적을 하기 위한 패킷 정보를 수집 및 분석한다. STM은 역추적 요청을 적절한 SCARs에 전달하고 SCARs로부터 역추적 분석 결과를 전달 받아 경로를 재구성하는 등의 역할을 수행한다.

2)IPSec기반 역추적

IPSec기반의 역추적기법은 오버레이 네트워크 기반 역추적 기법에서 공격자가 터널링 과정에서 거짓 정보를 보낼 수 있는 취약점을 보완하기 위해 제시된 기법이다. 이 기법은 네트워크에 대한 위상을 각 라우터가 알고 있다는 전제하에 이루어진다. 시스템이 공격을 받으면 이웃 라우터와 피해 시스템간에IPSec 연결을 구성한다. IPSec터널연결을 한 라우터에 공격 패킷이 지나가면 IPSec 연결을 통해 피해 시스템에 공격정보를 보낸다. 해당 라우터들을 대상으로 이 과정을 반복하고 반복된 과정을 통해 공격 패킷의 전송 경로를 수집하고 분석하여 공격 경로를 재구성한다.

3.3 역추적 기술분석

역추적을 위한 요구사항에 대한 기존의 역추적기술의 만족 여부를 비교 분석한 결과를 <표 1>에 나타내었다. 역추적기법을 분석하기 위한 요구사항 항목들은 다음과 같다[8].

① 실시간으로 역추적 가능해야 한다.
② 트래픽의 특징을 이용한 역추적이 가능해야 한다.
③ 샘플링한 패킷을 기반으로 역추적이 가능해야 한다.
④ IP위조 패킷을 보낸 근원지를 추적할 수 있어야 한다.
⑤ 다른 네트워크에서 전송되는 패킷의 근원지를 추적할 수 있어야 한다.

<표 1> IP역추적 기술 분석

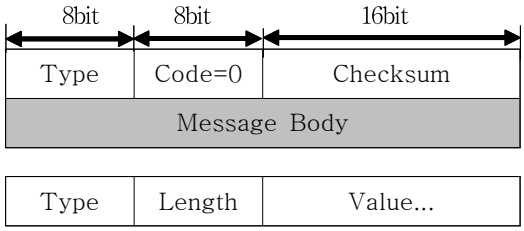
기법	①	②	③	④	⑤	⑥	⑦	⑧
PPM	x	o	o	x	x	x	o	x
iTrace	x	o	o	x	x	x	o	x
Hash TB	o	o	x	x	x	x	o	x
IPSecTB	o	o	x	o	x	x	o	x
overlayTB	o	o	x	x	x	x	o	x

⑥ 응용 서비스에서 제공하는 정보를 이용하여 서비스를 제공하는 서버의 위치를 추적할 수 있어야 한다.
⑦ 수신받은 패킷의 정보를 이용하여 패킷 전송이 시작된 네트워크 시스템의 위치를 추적 할 수 있어야 한다.
⑧ IP주소와 시간을 이용하여 네트워크의 위치 정보를 확인할 수 있어야 한다.

4.제안된 iTrace역추적 기법

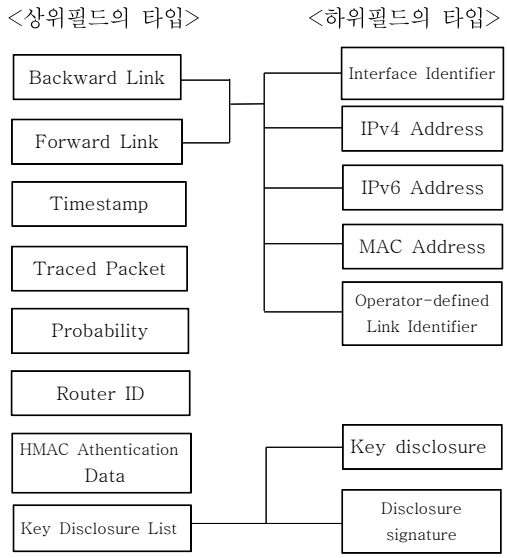
4.1 iTrace 메시지 구조

IP역추적을 위해 사용하는 iTrace 메시지(ICMP Trace Message)는 <그림 1>과 같은 구조를 가지며 ICMP패킷의 Message Body에 일련의 스트링으로 포함된다. Message Body는 하나 이상의 TLV (Type-Length-Value)엔트리로 구성된다. Type 필드는 상위 요소가 0x81에서 0x87의 범위를 가진다[3]. 코드 필드는 항상 0(no code)으로 설정되고 수신자는 반드시 이를 허용해야 한다.



<그림 1> iTrace메시지 형태

여기에서 상위필드의 전방링크(Forward Link)와 후방링크(Backward Link)는 역추적 패킷에 대한 이동경로를 제공하고, iTrace메시지 연결 구성을 위한 경로 정보를 제공한다. HMAC 인증을 사용하여 공격자에 의한 위조 iTrace 메시지를 방지하며 인증알고리즘으로는 MD5와 SHA-1모두 사용 가능한데, 여기서는 MD5알고리즘을 사용한다.



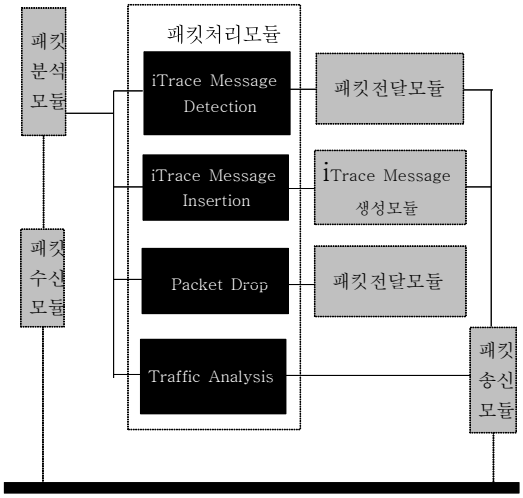
<그림 2> iTrace메시지 타입

4.2 에이전트 시스템 구조

에이전트는 각 지역 네트워크에 설치되어 트래픽 수집, 패킷분석, iTrace 메시지 탐지, iTrace 메시지 생성, 비정상 패킷 처리를 수행하게 된다. 에이전트 시스템은 특정 IP에서 비정상 트래픽 현상이 발생하면 해당 IP를 감시하고, 문제 시스템을 찾아 해당 시

스템의 정보와 수상한 출발지 IP를 서버에 신고하게 된다.

패킷 수신 모듈은 지역 네트워크의 패킷들을 수신하여 패킷 분석 모듈로 전송하며 패킷 분석 모듈은 수신한 패킷을 분류하여 패킷처리모듈로 보낸다. 패킷처리모듈에서는 iTrace 메시지 탐지, iTrace메시지 생성, 비정상패킷 처리, 트래픽 분석을 한다.



<그림 3> 에이전트 시스템 구조

4.3 서버 시스템

서버는 관리네트워크에 설치되며 지역 네트워크에 설치되어 있는 에이전트로부터 iTrace메시지를 수신하여 역추적 경로를 구성하고 침입에 따른 정책을 에이전트들에게 전송하는 역할을 한다.

침입정보를 수신하게 되면 서버 시스템은 해당 패킷에 대한 패킷 차단정책을 각 에이전트에게 전송하고 iTrace메시지 생성 명령을 송신하게 된다. 에이전트로부터 iTrace메시지 수신 후 서버의 iTrace메시지 인증 블록에서는 iTrace메시지의 유효성을 검증하게 된다[9].

5. 성능분석

일반적으로 역추적 기법들을 비교 평가하는 항목[10]들을 사용하여 기존의 역추적기법과 제안한 역추적기법을 비교·분석하였다. Ad-hoc네트워크는 기존의 유선망에서의 허브장치 등과 유사하게 라우팅 기능을 수행하게 되며 기존의 역추적 기법도 라우터에 역추적 기능을 추가하는 방식이므로 제안한 Ad-hoc 기반의 역추적기법을 기존의 라우터중심 역추적기법들과 비교하였다.

필터링 기법[11]은 라우터에서의 접근제어 기능을 제공하며 SYN flooding기법과 유사하게 전체적인 네트워크의 부하 및 피해 네트워크에 부하를 주는 형태가 아니라 라우터 자체에서 패킷에 대한 검사를 수행하는 기법이다. 따라서 추가적인 메모리 요구가 없으나 역추적기능을 제공하지 못하며 보안기능 및 DDos 대응 기능도 제공하지 못하고 있다. 로깅(logging) 기법은 라우터에서 패킷정보에 대한 로그정보를 관리하며 라우터에 대해 많은 메모리를 필요로 하고 일부 역추적 기능을 제공하지만 전반적으로는 낮은 보안구조와 DDoS공격 대응에 취약점을 보인다.

PPM은 관리네트워크 부하는 적으나 피해 네트워크는 많은 부하를 필요로 한다. 또한 많은 메모리를 요구한다. 그러나 확장성이 좋으며 경로 재구성 패킷의 수를 줄일 수 있다. 기존의 iTrace기법은 관리네트워크 부하는 적은 반면 피해 시스템에서 역추적 경로 재구성시 많은 부하를 필요로 한다. 그러나 역추적 기능 및 확장성 측면에서 적절하다고 할 수 있다. DDoS공격에는 취약한 특성을 보인다. 전체적으로 현재까지 제시된 IP역추적 기법을 검토하였을 경우 대부분 기존 라우터에 대한 변형 및 추가적인 네트워크 부하가 발생한다는 것을 알 수 있다.

제안한 기법은 네트워크 부하가 적고 역추적경로 재구성에 필요한 패킷의 수를 줄일 수 있으며 DDos 대응에 양호함을 보였다. IP역추적 기법과 제안한 기법의 성능 비교 평가 결과를 <표 2>에 나타내었다.

<표 2> IP역추적 기법 성능 비교 평가

항목 / 기법	구성 요소	작동방식	피해 네트워크 부하	역추적 기능	무 결성 제공	DDoS 대응	경로 재구성 패킷수	무선패킷 분류	네트워크 처리율
Ingress filtering	라우터	패킷 필터링	x	x	x	x	x	x	Δ
로깅	라우터	로그	x	◇	x	x	x	x	◇
PPM	라우터	패킷 마킹	↑	◇	◇	▽	n-1	x	▽
iTrace	라우터	ICMP	↑	Δ	◇	x	x	x	◇
제안한 기법	라우터	ICMP	↓	Δ	Δ	Δ	n-1	o	▽

o:A x:N/A ↑:높음 ↓:낮음 △:좋음 ◇:보통 ▽:나쁨 n:라우터수

6. 결 론

Ad-hoc네트워크는 환경이 빠르게 변하기 때문에 구성이나 규모를 예측하기 어렵다. 이런 이유가 Ad-hoc네트워크에서 역추적을 어렵게 만든다. 하지만 Ad-hoc네트워크에서도 기존 인터넷망에서 발생하는 공격의 위협이 존재한다.

본 논문에서는 Ad-hoc 네트워크에서 ICMP메시지를 이용한 공격 근원지 역추적 기법을 제안하였다. 제안한 역추적기법은 공격이 종료되어도 공격자의 위치를 추적할 수 있으며 IETF에서 제안한 방식을 사용함으로써 표준화를 통해 확장성을 가지고 있다고 할 수 있다. 또한 제안된 방식은 네트워크 상에서 DDos 해킹공격에 대한 판단·제어 기능을 제공하면서도 피해 네트워크에서는 스푸핑된 해킹공격 근원지를 효율적으로 역추적할 수 있는 새로운 기법이다. 제안한 기법은 기존의 기법보다 부하, 무결성, 안전성 및 역추적 기능에서 개선된 특징을 보인다.

참고문헌

[1] 김길한, 이형우, “Ad-hoc 네트워크에서의 패킷 마킹 기법을 이용한 공격 근원지 역추적 기법” 한국멀티미디어학회 춘계학술발표대회 논문집, pp.21-24, 2004년 5월.

[2] D.X.Song,A.Perrig,“Advanced and Authenticated Marking Scheme for IP Traceback,” In Proc. of IEEE INFOCOM Conference, 2001.

[3] Steve Bellovin, Marcus Leech, Tom Taylor , "ICMP Traceback Message," IETF, draft-ietf-itrace-04, Feb, 2003.

[4] 이동희, 여돈구, 장재훈, 염흥렬, “Ad-hoc 네트워크 역추적 기술 동향,” 한국정보보호학회 학회지 제20권 제4호, pp.85-93, 2010년 8월.

[5] 박정두, 김영용, “Ad Hoc 최신 기술 동향”, 대한전자공학회 텔레콤 제19권 제2호, pp.72-83, 2003년 12월.

[6] Y Kim, A Helmy, "Attacker Traceback with cross-layer Monitoring in Wireless Multi-hop Networks", SASN, Oct. 2006.

[7] Alex C. Snoeren, Craig Patridge et al, "Single-packet IP traceback," IEEE/ACM Transactions on Networking ,Vol10, issue6, Dec. 2002.

[8] 한정화, 김락현, 류재철, 염흥열, “역추적 기술 및 보안 요구사항 분석”, 한국정보보호학회 학회지 제18권 제5호, pp.132-140, 2008년 10월.

[9] 채철주, 이성현, 김지현, 이재광, “iTrace 메시지를 이용한 침입자 역추적 시스템 설계 및 구현,” 정보과학회 추계학술대회 논문집, 제32권 제2(I)호, pp.88-90, 2005년 11월.

[10] A.Belenky and N. Ansari, "On IP Traceback," IEEE Communication Magazine, pp142-153,

July, 2003.

[11] P.Ferguson and D. Senie. "Network ingress Filtering: Defeating denial of service attacks which employ IP source address spoofing," RFC 2827, May. 2000.

[저 자 소 개]

정 기 석 (Gi-seog Jeong)

1983년 2월 고려대학교 전자공학과 학사
1988년 8월 고려대학교 전자공학과 석사
1992년 8월 고려대학교 전자공학과 박사
현재 영동대학교 정보통신보안학과 교수

email : gsjeong@yd.ac.kr