

# An Efficient IP Traceback mechanism for the NGN based on IPv6 Protocol

Rack-Hyun Kim<sup>1</sup>, Jae-Hoon Jang<sup>2</sup>, Heung-Youl Youm<sup>3</sup>

<sup>1,2,3</sup>Department of Information Security Engineering, Soonchunhyang University,  
Shinchang-myun, Asan-Si, Chungchungnam-do, 336-745, Korea  
{rhkim<sup>1</sup>, pure<sup>2</sup>, hyyoum<sup>3</sup>}@sch.ac.kr

**Abstract.** Protecting against DOS or DDOS attacks can be regarded as one of the most difficult problems on the Internet today. One solution to thwart these attacks is to trace the source of the attacks. However, it is not easy to trace since the attackers usually use the spoofed IP source addresses to hide his or her network location. The key problem includes how to identify the “real” sources of the attacks even though the attackers use spoofed IP address to hide their actual network location. However, the current Internet architecture does not provide any means to identify the real sources of IP packets. Numerous traceback mechanisms have been proposed to “traceback” the real sources. Most of such works have been focused on addressing the traceback issues based on the IP4-based network. In this paper, we analyze the existing IP traceback mechanisms which can be used for traceback mechanisms for NGN based on IPv6 protocol. Furthermore, we propose an efficient IP traceback mechanism based on IPv6 in the NGN. We also discussed the security characteristics of the proposed traceback mechanism for the IPv6-based network..

**Keywords:** Traceback, IPv6, DoS, DDoS

## 1. Introduction

As the Internet becomes pervasive, the vulnerability of some fundamental design aspects of the Internet has also become significant. Among which, Denial-of-Service (DoS) and Distributed DoS (DDoS) pose significant problems, as they are disruptive to the useful traffics and are hard to prevent. The Internet is used in various areas such as communication, information, multimedia and teleconference and its users are continuously increasing. But, despite of the convenience and many proper functions that networking presents, the increase in the Internet users and the Internet usage itself also prompt many reverse functions including violating or even attaching the user's privacy through hacking, information leakage, illegal trespassing and distribution of computer virus. According to a report issued by US-CERT (United States Computer Emergency Readiness Team), as seen in Table 1, attacks through the Internet have rapidly increased every year so that many experts[1] and companies specialized in security make their efforts to respond to such attacks.

**Table 1.** Internet incident analysis data reported from US-CERT

Type	1999	2000	2001	2002	2003	2004(1~4)
Root Compromise	113	157	101	125	137	73
User Compromise	21	115	127	111	587	183
Denial of Service	34	36	760	36	25	435
Malicious Code	0	0	4,764	265	191,306	1,624,762
Web Site Defacement	0	0	236	46	90	28
Misuse of Resources	12	24	7	39	26	35
Other	52	9	108	1,268	535,304	3,433,112
Reconnaissance Activity	222	71	452	488,000	706,441	54,867,634
Totals	454	412	6,555	489,890	1,433,916	59,926,262

Therefore, traceback technologies are developed and studied to improve effective tracing that has been more difficult due to increase in various types of violation and attacks (hacking, cyber attack or criminals), advanced techniques to conceal, disguise or counterfeit, limited traceback that is only possible through analyzing remaining log after being attacked, attacks through overseas proxy servers via many countries and IP spoofing. In addition, because forensics based on traceback is reinforced in cyber criminal and several effects are produced such as defining responsibility, punishment and prevention of re-trespassing, many systems have been developed to prevent hacking. But, current security systems operated in today's online settings are very diverse and scattered so that they are almost impossible to make effective mutual responses to hacking. Thus, some studies on more effective and efficient traceback systems are actively conducted. In addition, NGN (Next Generation Network) being currently developed by ITU-T[2] as one of the next generation networks is an enhanced intelligent future-type network that can cover voice, data and multimedia with only one integral network and effectively support various value-added services. If this NGN as an enhanced intelligent network is established, subscribers will have a more enhanced network and receive and send high capacity data in a more stable and fast speed while service suppliers will save the cost of network establishment and management, consequently leading to providing customers with high quality communication services for lower prices. Today's online-based networks are expected to completely transform to NGN in several years. Therefore, traceback technologies for NGN-based networks need to be researched and developed for more stable traceback technologies.

This paper examines today's study trends on TCP/IP traceback technologies and analyzes the characteristics and strength and weak points of each traceback technique. This paper also examines the direction of further traceback technologies. Based on findings from these examinations and analyses, this paper tries to extract several requirements for security in applying traceback to NG to get security indexes for the development of traceback technologies.

This paper is organized as follows. In Section 2 the concept and category of traceback are presented, in Section 3 the current IP-based traceback techniques are surveyed, in section 4 the concept and characteristics of NGN and security

requirements are derived. In section 5 we present an efficient IP traceback mechanism based on IPv6 protocol in NGN and analyze the characteristics of the proposed mechanism in terms of security, etc. And finally, we conclude this paper with section 6.

## **2. Traceback**

Traceback is a technology to analyze and trace the hacker location in real time using the network in case of attacking. There are various traceback technologies depending on communication environments and connection methods, and various techniques are applied according to traceback methods.

Traceback techniques can be classified according to connection methods, response ways and application techniques. First, they are TCP connection traceback and IP traceback depending on their connection methods. TCP connection traceback uses the characteristics of TCP communication way for connection-oriented communication way. This way mainly uses the characteristics of connection chains for traceback. To the contrary, since IP traceback uses non-connection-oriented communication way, it analyzes remaining logs in the attacked system and traces the attacker's location with such traces.

Second, in terms of response ways, they can be divided into passive methods, which use remaining traces in the attacked system to trace the attacker's location, and active methods, which can block the hacker's attempt in advance. Currently, many researchers and companies are making their efforts to develop active preventive systems to block the attempt of hacking itself in real-time. Third, they can be classified into network-based traceback and host-based traceback according to in which location a traceback module is installed in the participant's systems. In the network-based traceback way, the traceback module shall be installed in sever, router, gateway or other devices that are connected with the network and control the network to obtain traceback information from the data (control and user data and header) passing through the network. In the host-based traceback way, the traceback module shall be installed in each host of the networks participated in the communication to traceback with information obtained from the host.

Each traceback way has its own strength and weak points according to network settings and operation methods. Therefore, a new traceback way that compensates all of them shall be immediately developed.

## **3. IP Traceback**

IP traceback technology is the one that can traceback the source of spoofed attack packet and re-organize attack graph by tracing attack paths and the packet sender/receiver. There are several representative techniques such as the technique using marking methodology focusing on packets, the technique controlling delivery path information of the source packet through deformation of ICMP protocol and other protocols and the technique using management protocol from the aspect of

network structure. Every traceback method has its own strength and weak point as showed in [2] and has different performance according to its deployment location of traceback module and the characteristics of hacking method. Existing IP Traceback methods can be categorized as proactive or reactive tracing. Proactive tracing (such as packet marking and messaging) prepares information for tracing when packets are in transit. Reactive tracing starts tracing after an attack is detected.

#### **4. Security and functional requirements for Traceback in NGN**

NGN is a network to supply pack-based communication services. In case that it is established, the subscribers will have a more enhanced network and receive and send high capacity data in a more stable and fast speed while service suppliers will save the cost of network establishment and management, consequently leading to providing customers with high quality communication services for lower prices. In NGN environment where broadband services with sound, data, video and multimedia information are provided via various heterogeneous networks, protecting NGN infra is a prerequisite condition to provide safe services. However, it is expected that new security threats will emerge when integrating existing networks because current security threats that each network has will be combined and accumulated. Therefore, resolving this problem will be the one to be settled previously. Therefore, this paper examines several methods to solve these security threats in NGN environment.

##### **4.1 Security threat in NGN**

NGN is a next generation convergence network that can provide seamless broadband multimedia services converging today's various networks such as communication, broadcasting and internet anytime and anywhere. Among those various networks, the Internet becomes a backbone to realize NGN. Furthermore, since various heterogeneous networks provide services based on IP, each network's weak points might have influence on other network users and such damages and ripple effects will be significant and serious. In addition, the Internet is changed from IPv4 to IPv6 so that transforming into IPv6 is a key point to connect all of the IT devices in the world into the one.

Therefore, this paper tries to identify various vicious attacks and find solutions to these matters.

##### **4.1.1 NGN Security Threat**

Security threats in NGN are largely (1) message wiretapping, robbed and damaged confidential information, unwanted spam, forgery of identification, terminal contamination with virus/worm/spyware, privacy violation, service unavailability and traffic flooding attack through excessive traffic concentration from the user's perspective, and (2) pirating service, attacking or rejecting a certain service, unauthorized disclose of network structure, unauthorized network setting or structure change from the service provider's perspective.

In addition, even though they are not clearly defined as threats, change in the setting of network facilities such as fire walls is required to provide multimedia services. For NGN security, many countermeasures shall be drawn up to remove these threats.

#### **4.1.2 Security Threat diversion to IPv6**

The following shows some expected security threats that might occur for transition to IPv6 environment. Not only the existing threatening factors in IPv4 but also new threatening factors in IPv6 might complicatedly take place. Even though it is expected that worm that uses scanning and this or other viruses will significantly decrease because IPv6 address space extends to 128 bit but, tunneling or dual stack technology that transform IPv4 to IPv6 may lead to some security problems. IPv6 is vulnerable by the following attack or threatening factors as in [4].

- Dictionary Attack
- Unauthorized access
- Header manipulation and fragmentation
- Layer 3/4 spoofing
- ARP and DHCP
- Broadcast amplification attacks: smurf
- Routing attacks
- Virus and Worm
- Translation, commutation and tunneling mechanism
- Sniffing
- Application Layer Attack
- Rogue devices
- Man-in-the-middle Attack
- Flooding

#### **4.2 General Requirements for Traceback**

The general requirements for the traceback functions can be listed as follows[4].:

- **Compatibility:** The traceback protocol is required to be compatible with existing protocols and NGN structure including hardware and software.
- **Insignificant network traffic overhead:** The traceback mechanism is recommended not to increase the network traffic significantly.
- **Minimal impact on complexity:** The traceback mechanism is recommended to support minimum impact on complexity for incremental implementation
- **Robustness:** The traceback mechanism is recommended to be very effective and robust against DDoS
- **Minimal overhead in terms of time and resources:** The traceback mechanism is recommended to have a minimum impact on overhead in terms of time and resources.
- **Partial deployment of a traceback function:** A traceback mechanism is recommended to function even when only partially deployed across routers.

- **Minimum change:** A traceback mechanism is recommended to require a small hardware change on the routers in the NGN.
- **Few packets required:** A traceback mechanism is recommended to allow the victim to identify the attack path after only a small number of packets.
- **Scalability:** A traceback mechanism is recommended to scale to a large number of attackers while maintaining accuracy (as measured by incorrect implication of non-attacking end hosts and routers (false positives), and the failure to identify true attack end hosts and routers (false negatives)).
- **Locality:** A traceback mechanism is recommended to allow an attack victim to perform traceback locally, without communicating with any router or ISP.
- **Multi-domain traceback:** A traceback mechanism is required to identify the attacker who resides on the other domain.

### 4.3 Functional Requirements for the Traceback mechanism

The functional requirements for the traceback mechanism can be listed as follows[6].:

- ① If the traceback is regarded as a service, the response time of traceback is recommended to satisfy the real-time processing requirements of network events.
- ② The traceback mechanism is recommended to be able to determine the source of a network event based on the characters of this event. For example, the source of DDoS traffic is determined by the traffic characters.
- ③ The traceback mechanism is recommended to be able to determine the source of a network event based on sample packets of this event.
- ④ The traceback mechanism is recommended to be able to determine the sender of spoofed packets.
- ⑤ The traceback mechanism is recommended to be able to determine the sender of packets which transferred through different domains.
- ⑥ If there exists an application layer route, the traceback mechanism is recommended to be able to ascertain the information of the entities on the application layer route, especially the information of the first entity. For example, in email service, the first forwarding mail server is ascertained by the traceback mechanism based on the received email.
- ⑦ The traceback mechanism is recommended to be able to ascertain the information of the entities on the network layer route, especially the information of the first entity. For example, the ingress router is located by the traceback mechanism based on the received packets.
- ⑧ The traceback mechanism is recommended to be able to ascertain the geographical information (such as the building address) and logical network location information (such as the location information in the domain of a certain network operator) of a network entity based on its IP address and the time when the IP address is used.

Follow table 2 shows functional requirements for analysis of traceback.

**Table 2.** Comparisons of the existing mechanisms in term of security requirements

Traceback mechanism	①	②	③	④	⑤	⑥	⑦	⑧
Link Test[5]	X	O	X	X	O	X	X	X
Logging	X	O	X	X	O	X	X	X
PPM[10]	X	O	O	X	X	X	O	X
iTrace[11]	X	O	O	X	X	X	O	X
Hash TB[12]	O	O	X	X	X	X	O	X
IPSec TB[13]	O	O	X	O	X	X	O	X
Overlay TB[14]	O	O	X	X	X	X	O	X

#### 4.4 Countermeasures for IPv6 Network Attacks and Intrusion

There are countermeasures for network attacks and intrusions in IPv6 environment; countermeasures in the respect of technological view points and functional characteristics that should be supported by intrusion detection and prevention systems.

Countermeasures of ESP(Encapsulating Security Payload) traffic that could circumvent a firewall are cutting down all traffics sent to some hosts except specific hosts that is already verified their reliability, and establishing a firewall as a reliable middle node to apply security policies that force to pass through all IPSec procedures, achieved between terminal nodes, to the firewall, and checking the contents of IPSec packet after decrypting by cooperating with distributed firewall or personal firewall. Countermeasures for privacy extension methodologies of RFC3041 and DAD(Duplicate Address Detection) are supporting IP addresses changed by privacy extension methodologies in access control lists in the firewall. DAD could be abused by Denial of Service (DOS) attack, we should use all packets for this operation after authenticating using AH header of IPSec, or support DAD packet monitoring functionalities in a firewall or intrusion detection/prevention systems. Countermeasures for ND mechanisms and automatic address set up are needed to guarantee reliabilities of messages which are required to perform specific mechanisms, because ND mechanisms and automatic address setup mechanisms, essential elements to achieve IPv6 protocol properly, could be misused by various security attacks. Therefore, to execute this mechanism safely, we should use SEND(SEcuring Neighbor Discovery) or support monitoring and management functionalities, targeted required messages to perform that mechanisms at a firewall and intrusion detection/prevention systems. One of countermeasures for IPv6 extension headers is supporting filtering policies that consider hosts existing on the passage root to prevent from circumventing traffic filtering policies and tracing policies by using routing extension headers. The other one is supporting packet filtering that is capable of checking usages of all packets, including IPv6 extension header, to prevent from circumventing packet filtering policies and being abused by fragment overlapping and DOS attack. Last one is supporting rules about intrusion detection/prevention.

## 5. Proposed traceback mechanism

In this Section, We will discuss the proposed IP traceback mechanism. It is based on the following functions;

- **Packet Marking** : Routers probabilistically or deterministically mark path information in packets as they travel through the Internet. Victims reconstruct attack paths from path information embedded in received packets. Packet marking techniques can be subdivided in Deterministic Packet Marking (DPM) and Probabilistic Packet Marking (PPM). Our algorithm lies under the PPM category.
- **Packet Digesting** : Routers probabilistically or deterministically store audit logs of forwarded packets to support tracing attack flows. Victims consult upstream routers to reconstruct attack paths.
- **Traceback Module** : Forward packets to all routers are installed traceback module to improve the traceback of packet's path.
- All routers in network that Received packet check and process Hop-by-Hop options header.
- For support safety of proposed mechanism, attacker or third eavesdropper is not knows used elements and operating process.

### 5.1 IPv6 Hop-by-Hop header

Hop-by-Hop extension header and Destination option have TLV(Type-Length-Value)[7][8][9].

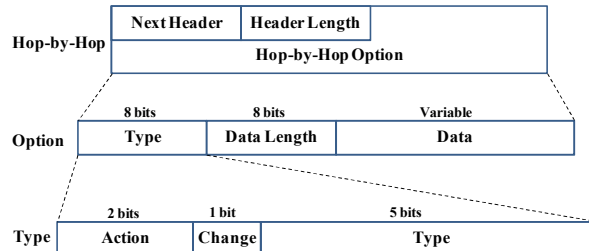


Fig 1. Hop-by-Hop header structure

We use Hop-by-Hop Header to store a mark the reasons are two fold; first, the Hop-by-Hop option is processed by every router en-route. Second, it provides the larger space to store a mark as shown in Figure 1. Figure 2 describes IPv6 formal address format, and proposed option in Hop by hop option header is shown in Figure 3.

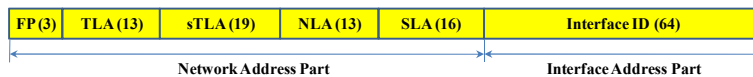
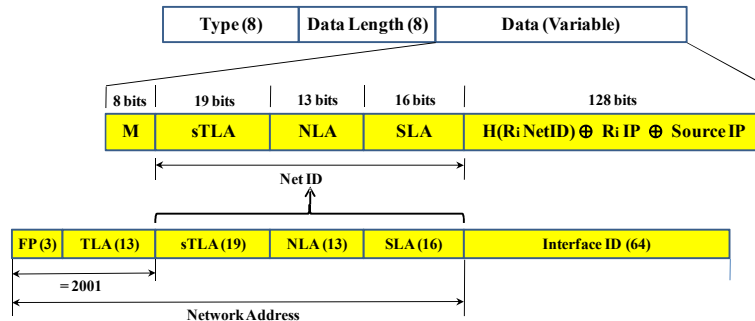


Fig 2. IPv6 formal address format



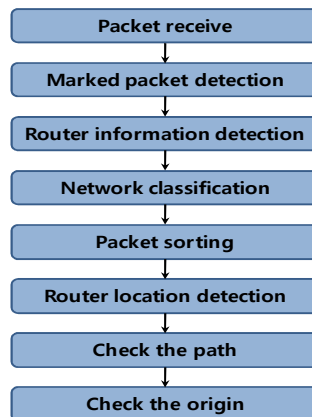
**Fig 3.** Marking information of proposed packet

Victim that attack from attacker marks with Hop-by-Hop option field traceback information. The Following items explain marking information of Data field in Hop-by-Hop option field.

- **M(8bits)** : Determine whether a packet marking. If the marking is not marking a packet.
- **NetID(48bits)** : Top 64bits of 128bits of IPv6 are network address part. FP and TLA(16bits) of this part are defined 2001 value. So that, we marks 48bits of back on packet. In this paper, sTLA, NLA and SLA are used as the NetID.
- **Data(128bits)** :  $H(Ri\ NetID) \oplus Ri\ IP$  (marking Router i's IP)  $\oplus$  Source IP

## 5.2 Traceback

Following steps(Figure 4) will be followed in proposed traceback mechanism.



**Fig 4.** Flowchart for proposed traceback mechanismt

Follow figure 5 presents the operational environment for the proposed traceback mechanism. And figure 6 shows to check out packet routing and origin based on marked packets.

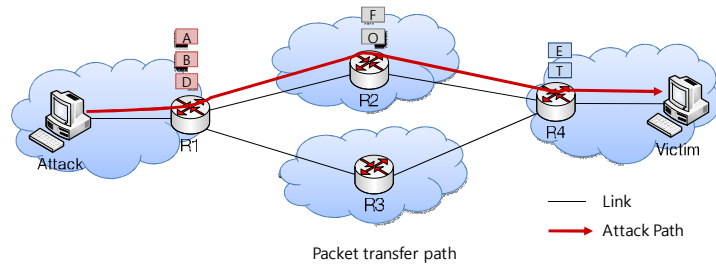


Fig 5. Operation environment for proposed traceback

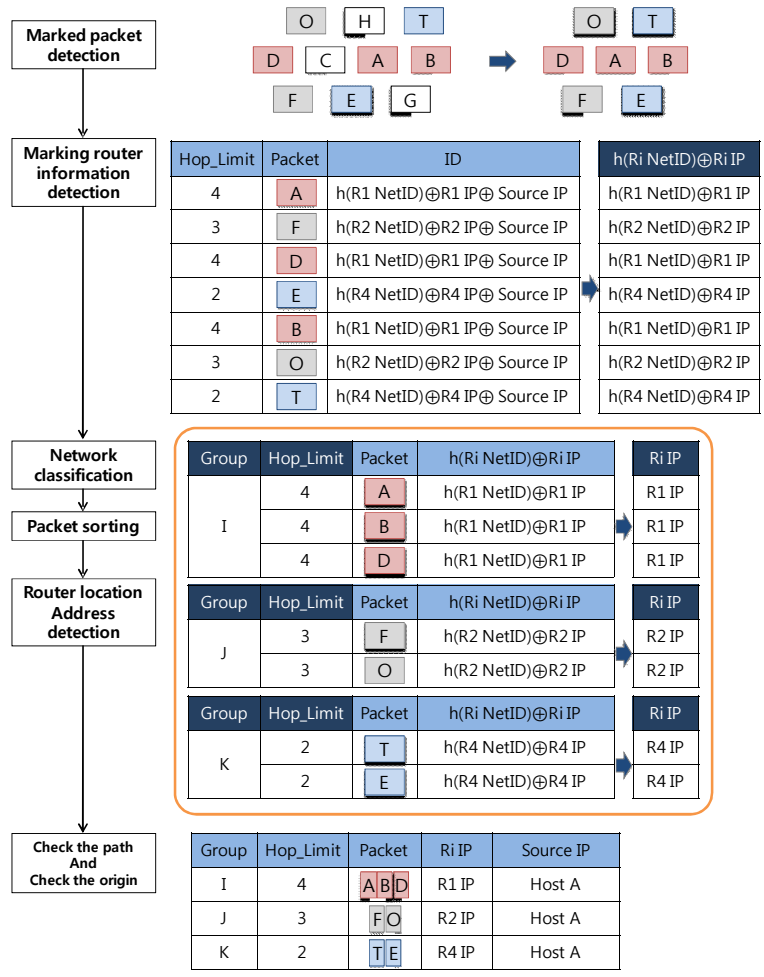


Fig 6. Operation process for proposed traceback

## 6. Analysis

In this Section, We will discuss functional and safety proposed IP traceback mechanism based on requirements of traceback.

### 6.1 Anaysis of the proposed traceback mechanism

Table 3 shows the comparision results in terms of management system overhead, network overhead, router overhead, extensibility, traceback and IPv6 support based on proposed traceback mechanism.

Table 3. Comparison of the proposed scheme with the existing mechanisms in terms of operation

Function Mechanism	Management system overhead	Network overhead	Router overhead	Extensibility	Traceback	IPv6 support
Link Test	X	X	X	△	▽	○
Logging	X	X	X	△	▽	○
PPM	▽	▽	□	△	△	X
iTrace	▽	▽	□	△	△	X
Hash based TB	△	▽	□	▽	△	X
IPSec based TB	△	▽	□	▽	△	○
Overlay network TB	△	▽	□	▽	△	○
Proposed TB	▽	▽	□	△	△	○

○: possible, △: high/good, □: middle, ▽: low/bad, X: impossible

Proposed mechanism in this paper, when compare to existing mechanism, the results are good in many functional features and because only proposed mechanism to marking using IPv6 field, proposed mechanism is scalable than IPsec traceback and overlay network mechanism.

### 6.2 Anaysis of the proposed traceback mechanisms in term of safety

In this section, we compared the proposed mechanism with the existing mechanism in the terms of safety of traceback.

Table 4. An each mechanism safety analysis

Function Mechanism	DDoS opposition	Origin source IP forgery opposition	IP spoofing opposition	Integrity
Link Test	X	X	X	X
Logging	X	X	X	X
PPM	▽	▽	▽	▽
iTrace	▽	▽	□	□
Hash based TB	△	▽	▽	▽

IPSec based TB	▽	△	△	△
Overlay network TB	△	▽	▽	△
Proposed TB	△	□	△	△

O: possible, △: high, ▽: low, □: middle, X: impossible

Proposed mechanism is similar to the IPSec and safety in safety analysis, is more safety than PPM and iTrace in DDos, origin source IP forgery, IP spoofing opposition and integrity.

## 7. Conclusion

In real world, protecing against all kinds of attacks on the Internet is nearly impossible. When prevention fails, a mechanism to identify the source(s) of the attack should be started to at least ensure the accountability for these attacks. This is the motivation behind the IP traceback schemes. However, these existing schemes have not been used widely even for IPv4 networks. One of the main reasons was to cause degradation in routing performance, as encoding should be applied to pass the path information through a limited space IPv4 header.

This paper contributes to the traceback mechanism based on the PPM algorithm for IPv6 network. The extension headers is used to allow great flexibility to pass the path information to the victim and since the information of routers are not distributed in different fragments as proposed in [15]; our scheme is not affected by the state explosion problem that is discussed in [16]. In future, we will continue to study other traceback techniques like DPM for NGN based on the IPv6 protocol and compare the results with the existing traceback mechanisms.

## Acknowledgments

“This research was supported by the Ministry of Knowledge Economy, Korea, under the ITRC(Information Technology Research Center) support program supervised by the IITA(Institute of Information Technology Advancement)” (IITA-2009-(C1090-0902-0016))

## References

- [1] <http://www.us-cert.gov/>
- [2] X. Zeltsan, "Guidelines for NGN Security Release," ITU-T, FGNGN, FGNGN-OD-00254, 2005.11.
- [3] J. Han, R. Kim, H. Youm, J. Ryou, "Survey of Traceback techniques and Requirements on Traceback in the NGN Environment", JWIS2008, pp. 267-281, July 2008

- [4] S. Lee, R. Kim, H. Youm, "A Study on EAP Requirements for NGN," CISC 2006'S, 2006
- [5] Stefan Savage, David Wetherall, Anna Karlin and Tom Anderson, "Practical Network Support for IP Traceback," Proc. Of ACM SIGCOMM 2000, pp. 295-306, 2000
- [6] Tian Huirong, Richard Brackney, H. Y. Youm, " Draft text of Rec. X.tb-ucr: Traceback Use Cases and Capabilities" , TD4158, ITU-T SG17, Sep.2008
- [7] R. Hinden, S. Deering, " Internet Protocol Version 6 (IPv6) Addressing Architecture ", RFC 3513, 2003, 4
- [8] S. Deering, R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", RFC 2460, 1998,12
- [9] R. Hinden, M. O'Dell, S. Deering, "An IPv6 Aggregatable Global Unicast Address Format", RFC 2374, 1998.7
- [10] D.X. Song, A. Perrig, "Advanced and Authenticated Marking Scheme for IP Traceback," In Proc. of IEEE INFOCOM Conference, 2001
- [11] Steve Bellovin, Marcus Leech, Tom Taylor, "ICMP Traceback Messages," IETF, draft-ietf-itrace-04, Feb. 2003
- [12] A.C. Snoeren, C. Partridge, L.A. Sanchez, W.T. Strayer, C. D. Jones, F. Tchakountio and S.T. Kent, " Hash-Based IP Traceback," *BBN Technical Memorandum*, No.1284, Feb. 7. 2001.
- [13] H.Y. Chang, R Narayan, S.F. Wu, B.M. Vetter, X. Wang, M. Brown, J.J. Yuill, C. Sargor, F. Jou, F. Gong, " Deciduous : Decentralized Source Identification for Network-based Intrusions," *6th IFIP/IEEE International Symposium on Integrated Network Management*, 1999.
- [14] R. Stone, " Centertrack : An IP Overlay Network for Tracking DoS Floods," *Proc. of 9th USENIX Security Symposium, Denver, Colorado*, pp. 199-212, August, 2000.
- [15] Dawn X. Song and Adrian Perrig, "Advanced and authenticated marking schemes for IP traceback," in Proceedings IEEE Infocomm 2001, April 2001
- [16] Marcel Waldvogel, "GOSSIB vs. IP Traceback Rumors", 18th Annual Computer Security Applications Conference (ACSAC '02).