社団法人 電子情報通信学会
THE INSTITUTE OF ELECTRONICS,
INFORMATION AND COMMUNICATION ENGINEERS

信学技報
IEICE Technical Report
IA2009-18, ICSS2009-26(2009-06)

# NGN/IPv6セキュリティ試験システムの設計と評価

力武 健次[†] 衛藤 将史[†] 鈴木 未央[†] 井上 大介[†] 中尾 康二[†,††]
小林 悟史[†††] 秋葉 澄伸[†††]

[†] 情報通信研究機構 インシデント対策グループ 〒184–8795 東京都小金井市貫井北町4–2–1
[††] KDDI株式会社 〒163–8003 東京都新宿区西新宿2–3–2
[†††] 株式会社ディアイティ 札幌開発センタ
〒060-0807 北海道札幌市北区北7条西5丁目8–1 北7条ヨシヤビル8F
E-mail: †rikitake@nict.go.jp

**あらまし** 本発表ではNGNとIPv6プロトコル体系に関する脆弱性の実証試験を行うためのシステム設計手法について提案する．また提案手法に基づいて製作したNGNの基礎技術であるIPv6およびSIPの脆弱性試験システムについてその概要と実験結果を示し，今後のNGNとIPv6の脆弱性研究に関する改善点や方向性について考察する．

**キーワード** NGN, IPv6, SIP, プロトコル脆弱性分析

# Design and Evaluation of NGN/IPv6 Security Test System

Kenji RIKITAKE[†], Masashi ETO[†], Mio SUZUKI[†], Daisuke INOUE[†], Koji NAKAO[†,††], Satoshi KOBAYASHI[†††], and Suminobu AKIBA[†††]

[†] Network Security Incident Response Group, NICT, Japan
4-2-1, Nukui-Kitamachi, Koganei City, Tokyo 184-8795 Japan
[††] KDDI Corporation 2-3-2, Nishi-Shinjuku, Shinjuku-Ku, Tokyo 163-8003 Japan
[†††] Sapporo Development Center, dit Co., Ltd.
Kita 7-Jo Yoshiya Bldg. 8F, 8-1, Nishi 5-Chome, Kita 7-Jo, Kita-Ku, Sapporo City, Hokkaido 060-0807 Japan
E-mail: †rikitake@nict.go.jp

**Abstract** In this paper, we propose a system design methodology for performing vulnerability tests of NGN and IPv6 protocol suites. We present the overview and the experimentation results of a vulnerability test system of IPv6 protocols and SIP based on the proposed design method. The future research direction and issues of the vulnerability of NGN and IPv6 is also outlined.

**Keywords** NGN, IPv6, SIP, protocol vulnerability analysis

## 1. Introduction

Next Generation Networks (NGNs) and Internet Protocol version 6 (IPv6) are two of the most important protocol suites coming in near future. Their security analysis, however, is still in the early stage and many issues are left unresolved.

NGN will eventually replace the current telecommunication infrastructure, which supersedes the public networks for fixed and cellular telephones and Internet. The telephone network functionality of NGN is built upon Voice-over-IP (VoIP), which consists of Session Initiation Protocol (SIP) [1] and the related protocols.

NGN is designed upon IPv6, which has the larger addressing space of 128 bits than the current Internet Protocol version 4 (IPv4), which only has 32 bits. The larger address space of IPv6 allows NGN carriers to accommodate a large number of current and potential customers. While NGNs are considered private and will not be directly connected to the global public IPv6 networks, which is a part of Internet, the protocol characteristics and the potential vulnerabilities are largely derived from IPv6.

IPv6 already has a long history. The specification has been published in 1998 as RFC2460 [2]. Running an IPv6 in a protected LAN is an easy task, since major operating systems including Windows XP and Vista, Linux, and FreeBSD have already incorporated the dual-stack capability of handling IPv4 and IPv6 simultaneously. The potential security issues of IPv6, however, is still mostly undiscovered, due to the lack of real-world IPv6 deployment experience. IPv6 also has new capabilities, such as autoconfiguration and extension headers, which will impose potential vulnerabilities. Analysis of those vulnerabilities is critical for preventing future network incidents.

In this paper, we propose a system design methodology for performing vulnerability tests of NGN and IPv6 protocol suites. First in Section 2, We describe the security issues which inherently exist within NGN and IPv6 protocol suites. We then propose a test system with the design goals and methodology in Section 3. The evaluation of the test results are shown in Section 4. We conclude the paper in Section 5.

## 2. Security issues of NGN and IPv6

One of the primary purposes of NGN is to provide a cost-effective solution of replacing legacy telephone network equipments, by introducing IPv6. The basic services of NGN include [3]:

- SIP-based VoIP service, including the accounting and user authentication services as the IP Multimedia Subsystem (IMS), with the Quality-of-Service (QoS) control;
- access link services to Internet Service Providers (ISP), using PPP over Ethernet (PPPoE) [4]; and
- authentication of terminals and other customer premises by DHCPv6 [5], [6].

The possible attack vectors against NGN include:

- SIP server and client vulnerabilities, e.g., the parsing errors of the SIP header arguments;
- Vulnerabilities of Customer Premise Equipments (CPEs); and
- Malicious activities such as sending IPv6 packets which may cause IPv6 routing errors and gain unauthorized access.

IPv6 introduces new functionality for the ease of operation. The following includes new features added to IPv6 [7]:

- *Large address space* : IPv6 has 128-bit address space. The address has 3 parts: 48 bits for global subscriber prefix [8], 16 bits for subnetting within the prefix, and 64 bits for host identifier inside the network [9].
- *Autoconfiguration* : each IPv6 node has a link-local address, automatically generated from EUI-64 [9, Appendix A]. By using this address and other Neighbor Discovery (ND) protocols [10], each node is guaranteed to have a unique address within the link, e.g., Ethernet. The Router Advertisement (RA) ensures each node to know the appropriate prefixes on the link and the link address of the forwarding router.

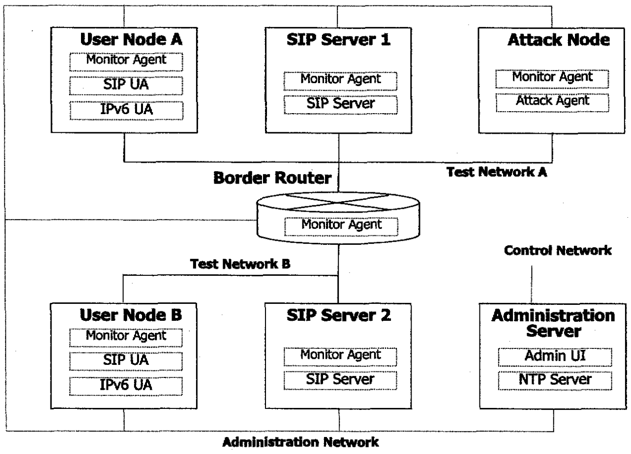


Fig. 1 Test system configuration diagram.

- *Extension headers* : IPv4 has only one header for each packet, including all the necessary options [11, Section 3.1]. IPv6 allows arbitrary number of extension headers to be inserted between the IPv6 header and the transport layer (e.g., TCP) header and payload. Hop-by-Hop Option headers such as Router Alert [12] must be processed by every intermediate routers in the packet delivery path.
- *No fragmentation on routers* : unlike in IPv4, IPv6 does not allow the routers to fragment packets. The fragmentation occurs only on the source host, with the Fragment Header added to each fragment. The source host has to discover the Maximum Transmission Unit (MTU) of the path to the destination host [13].

The possible attack vectors against IPv6 using the added features include:

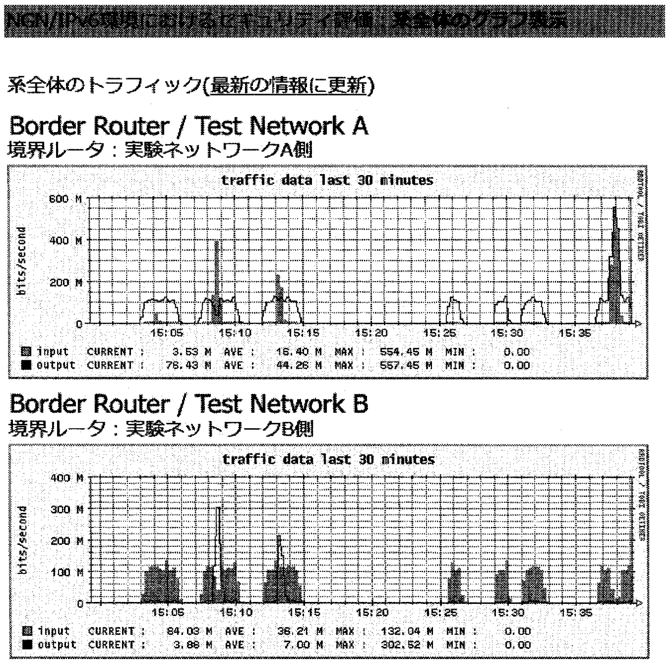
- Tracing how a mobile host moves around networks by using the uniqueness of the lower 64 bits of the address as the host identifier;
- Impersonation and access denial by intervention in the autoconfiguration process; and
- Consuming processing power of hosts and routers by sending packets with malformed extension headers, including one equivalent to the Tiny Fragment Attack for IPv4 [14], [15].

The above arguments do not cover all of NGN and IPv6 related security issues. We rather intend to point out the major differences and issues when deploying NGN and IPv6 as a part of existing telephone and Internet networks.

Table 1 Specification of vulnerability test system hosts.

| CPU & memory | Pentium D / Xeon ≥ 2GHz, ≥1Gbytes |
|---|---|
| OS | FreeBSD 6.4-RELEASE (i386) |
| SIP UA | Asterisk [16] IPv6 [17] |
| SIP server | OpenSER 1.2.3 (now OpenSIPS [18]) |
| SNMP agent | Net-SNMP 5.4.2 |
| SNMP logger | MRTG 2.16.2 |
| HTTP server | thttpd 2.25b |
| Traffic logger | tcpdump (of FreeBSD 6.4-RELEASE) |
| Traffic counter | ip6fw (of FreeBSD 6.4-RELEASE) |
| Log visualization | RRDTool 1.0.50 |

All hosts are synchronized by NTP;
All hosts are connected with 1000BASE-T GbE.



NGN/IPv6環境におけるセキュリティ評価：系全体のグラフ表示

系全体のトラフィック(最新の情報に更新)

Border Router / Test Network A
境界ルータ：実験ネットワークA側

```
■ input   CURRENT :   3.53 M  AVE :  16.40 M  MAX :  554.45 M  MIN :   0.00
■ output  CURRENT :  76.43 M  AVE :  44.26 M  MAX :  557.45 M  MIN :   0.00
```

Border Router / Test Network B
境界ルータ：実験ネットワークB側

```
■ input   CURRENT :  84.03 M  AVE :  36.21 M  MAX :  132.04 M  MIN :   0.00
■ output  CURRENT :   3.88 M  AVE :   7.00 M  MAX :  302.52 M  MIN :   0.00
```

Fig. 2 Snapshot of Web browser output showing the Border Router Traffic. (English captions added later)

## 3. Design goals and methodology

We conducted a series of experiments on a vulnerability test system specifically built for the testing purpose from December 2008 to March 2009, to systematically confirm protocol vulnerabilities of NGN and IPv6.

We decided to choose basic attack scenarios and vulnerabilities of SIP over IPv6 (SIP/IPv6) and IPv6 malformed packets for the following reasons:

- SIP/IPv6 is a critical function of NGN;
- On IPv6-based networks including NGN, an arbitrary set of equipments not necessarily authorized by the service providers can be connected to the networks and may send malformed packets; and
- Malformed packets on IPv6 can easily cause redirection or disruption of legitimate communication.

Table 2 Summary of SIP/IPv6 attack scenarios and results.

| | Successful? | Scenario Summary |
|---|---|---|
| 1) | No | Injection of UDP traffic into an established RTP session to block the established audio link |
| 2) | Yes | Sending large number of SIP INVITE requests to a SIP server for preventing a new legitimate call |
| 3) | Partially | Sending large number of SIP REGISTER requests to a SIP server for preventing a legitimate call to continue |
| 4) | Partially | Sending impersonated SIP REGISTER requests to block new calls from a legitimate SIP UA |
| 5) | Yes | Sending impersonated SIP BYE requests to drop a legitimate established call |

Our design goals for the vulnerability test system are as follows:

- open-source based subsystems for easy maintenance;
- independent monitor agents and administration network between the subsystem hosts for precise collection of test results; and
- Web-based administration and visualization framework of test results, for easy operation and reproducible attack simulation.

Figure 1 shows the configuration of subsystems. The entire system consists of 7 subsystem hosts, remotely controllable from the Administration Server. Table 1 shows the specification of the subsystem hosts. Fig. 2 shows an example of Web browser screen, which represents the output of the traffic monitoring system. The administrator of the test system can start each test by choosing the appropriate screen and click the buttons of Web browser. All collected data can be downloadable via the administration Web interface.

## 4. Evaluation of our test results

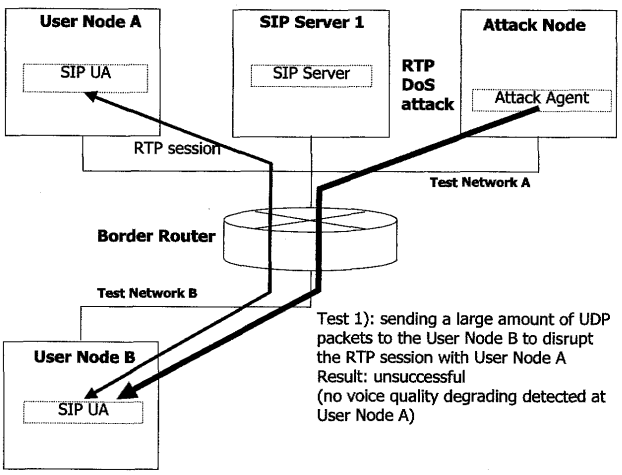
We selected 5 scenarios for SIP/IPv6 tests, and 7 scenarios for IPv6 malformed packet tests. We repeated the tests and all the results were reproducible.

### 4.1. SIP/IPv6 attack tests and results

Table 2 shows the summary of the scenarios and results for the SIP/IPv6 tests.

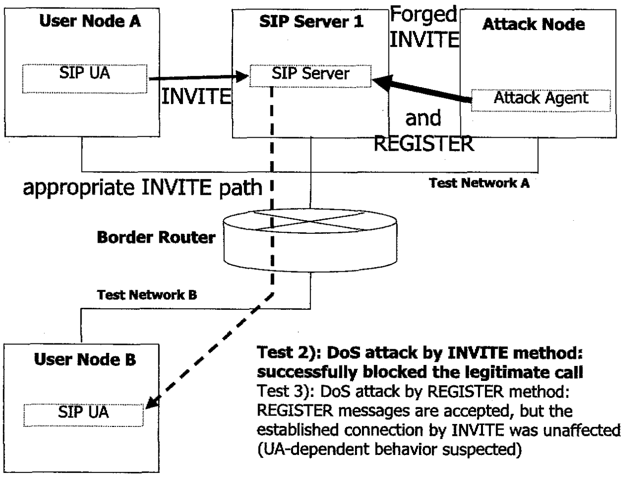
Figure 3 describes the test 1). In test 1), the RTP traffic carries a repetitive recording of female voice. We noticed no quality degradation of the voice during the attack.

Figure 4 describes the test 2) and 3). Flooding attack with SIP INVITE methods successfully blocked the SIP Server 1 from accepting a legitimate INVITE request. On the other hand, flooding with SIP REGISTER did not affect the established connection. Asterisk software for the SIP



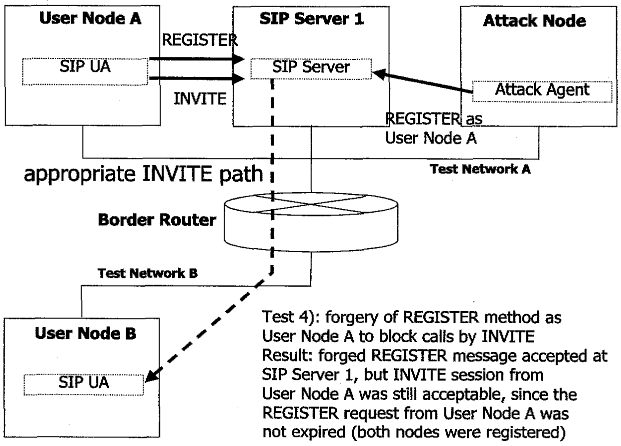
Test 1): sending a large amount of UDP packets to the User Node B to disrupt the RTP session with User Node A
Result: unsuccessful
(no voice quality degrading detected at User Node A)

Fig. 3 SIP/IPv6 attack test 1).



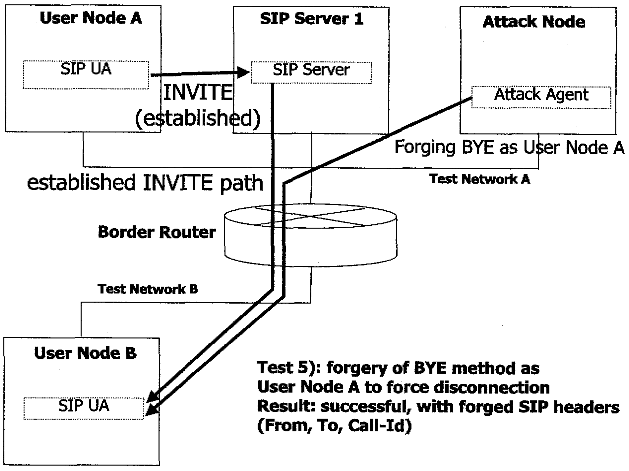
**Test 2): DoS attack by INVITE method: successfully blocked the legitimate call**
Test 3): DoS attack by REGISTER method: REGISTER messages are accepted, but the established connection by INVITE was unaffected (UA-dependent behavior suspected)

Fig. 4 SIP/IPv6 attack test 2) and 3).



Test 4): forgery of REGISTER method as User Node A to block calls by INVITE
Result: forged REGISTER message accepted at SIP Server 1, but INVITE session from User Node A was still acceptable, since the REGISTER request from User Node A was not expired (both nodes were registered)

Fig. 5 SIP attack test 4).



**Test 5): forgery of BYE method as User Node A to force disconnection**
**Result: successful, with forged SIP headers (From, To, Call-Id)**

Fig. 6 SIP/IPv6 attack test 5).

Table 3 Summary of IPv6 malformed packet attack scenarios and results.

| | Successful? | Scenario Summary |
|---|---|---|
| 1a) | No | DoS attack sending malformed Jumbo Payload packets with a large length parameter but with a small actual payload length |
| 1b) | Yes | DoS attack sending malformed fragment packets (first fragment only as incomplete packets) |
| 2) | No | DoS attack sending packets with large number of Pad1 options |
| 3) | Yes | Sending impersonated Neighbor Advertisement (NA) packet to Border Router |
| 4) | Yes | Sending impersonated Router Advertisement (RA) packet to Border Router |
| 5) | No | Sending overlapped IPv6 packet fragments to establish a forged TCP connection |
| 6) | Yes | Amplified DoS sending packets with large number of Routing Header 0 (RH0) options |

Note: continuous HTTP transmission performed during each scenario to detect packet disruption and redirection

UAs did not support the session timer and did not send any re-INVITE request. We consider this lack of feature was the cause of attack failure on 3).

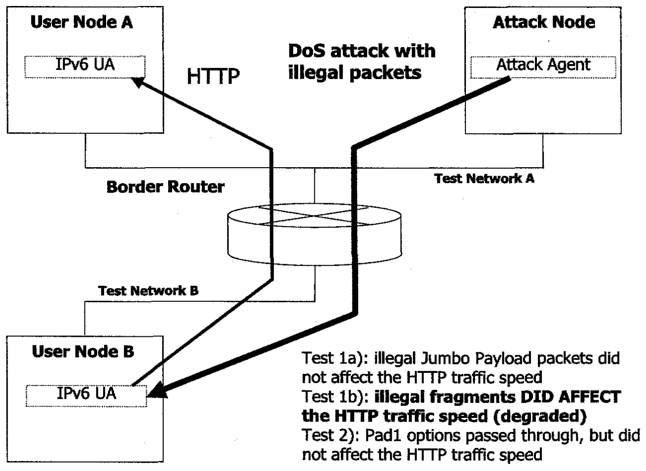
Figure 5 describes the test 4). While the INVITE session takeover was not successful, the OpenSER actually accepted the forged REGISTER requests from Attack Node as User Node A. The legitimate REGISTER request from the User Node A, however, did not expire either, so the INVITE request from User Node A was still successfully completed.

Figure 6 describes the test 5). Forgery of a BYE request with `From:`, `To:`, and `Call-Id:` header set of an established connection successfully took down the connection. We assume no IPv6-level address verification was performed.

We consider the result of test 5) is particularly alarming among the conducted SIP/IPv6 tests. We also notice test 3) and 4) are highly dependent on the SIP UA implementation, and should be investigated further for different attack timings.

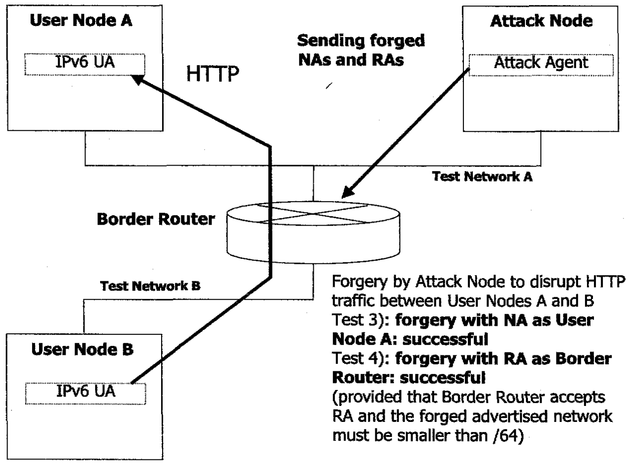
### 4.2. IPv6 malformed packet attack tests and results

Table 2 shows the summary of the scenarios and results for



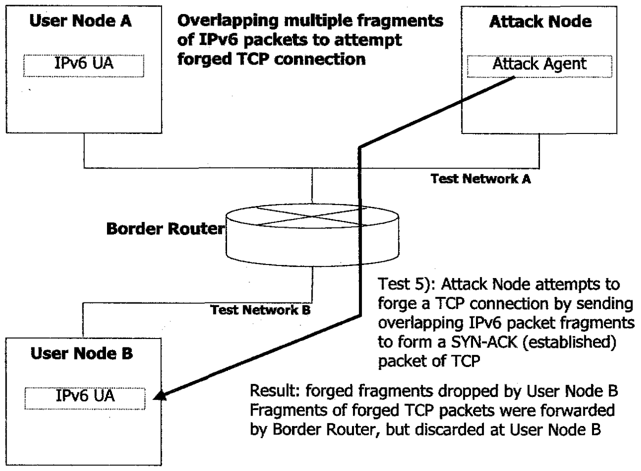
Test 1a): illegal Jumbo Payload packets did not affect the HTTP traffic speed
Test 1b): **illegal fragments DID AFFECT the HTTP traffic speed (degraded)**
Test 2): Pad1 options passed through, but did not affect the HTTP traffic speed

Fig. 7 IPv6 malformed packet attack test 1a), 1b), and 2).



Forgery by Attack Node to disrupt HTTP traffic between User Nodes A and B
Test 3): **forgery with NA as User Node A: successful**
Test 4): **forgery with RA as Border Router: successful**
(provided that Border Router accepts RA and the forged advertised network must be smaller than /64)

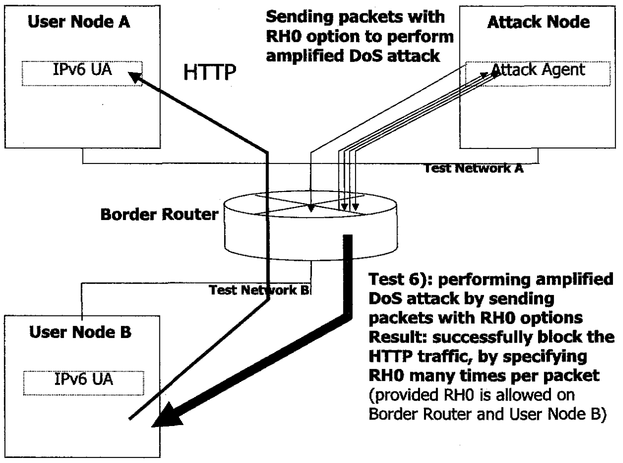
Fig. 8 IPv6 malformed packet attack test 3) and 4).



Test 5): Attack Node attempts to forge a TCP connection by sending overlapping IPv6 packet fragments to form a SYN-ACK (established) packet of TCP

Result: forged fragments dropped by User Node B
Fragments of forged TCP packets were forwarded by Border Router, but discarded at User Node B

Fig. 9 IPv6 malformed packet attack test 5).



**Test 6): performing amplified DoS attack by sending packets with RH0 options**
**Result: successfully block the HTTP traffic, by specifying RH0 many times per packet**
(provided RH0 is allowed on Border Router and User Node B)

Fig. 10 IPv6 malformed packet attack test 6).

the IPv6 malformed packet tests.

Figure 7 describes test 1a), 1b), and 2). We observed the Border Router did not forward the malformed Jumbo Payload packets. On the other hand, malformed IPv6 fragment packets severely affects the attack target when the target accepts fragments without limitation[*1] .

Figure 8 describes test 3) and 4). Forged NAs and RAs successfully redirected the packets away from the target. NAs are cached at Border Router so the successful forgery may affect long after the forgery is complete. We should note that for making test 4) successful, Border Router must listen to RIPng [19] and the advertised route prefix value must be larger than 64.

Figure 9 describes test 5), trying to forge a TCP connection by sending fragments of TCP *established* (SYN+ACK) packets [20]. Border Router had a firewall rule set to pass TCP connections from User Node B only and block those to User Node B, by only allowing the *established* packets. The fragments of TCP attack packets were successfully got around of the firewall rule set and forwarded to User Node B, but the Node discarded the whole fragments.

Figure 10 describes test 6). In this test RH0 option was specified 88 times for each packet, and we observed amplified traffic of 500Mbps. We should note that RH0 is now *deprecated* [21], and in this test RH0 was intentionally enabled[*2] .

We consider the result of test 3) is particularly noteworthy among the conducted IPv6 malformed packet tests. While forgery of Neighbor Advertisement is also possible for IPv4 [22], being able to attack for all IPv6 links is a new vulnerability. We also consider test 1b) is notable by disclosing the vulnerability of fragment packet processing in end nodes.

## 5. Conclusions and future work

We proposed a system design methodology for conducting vulnerability tests of NGN, focused on SIP/IPv6, and IPv6

[*1] : setting sysctl variables `net.inet6.ip6.maxfrags` and `net.inet6.ip6.maxfragpackets` to -1 allows a host to accept all fragments without limitation. See `sys/netinet6/frag6.c` of FreeBSD kernel source tree.

[*2] : By setting sysctl variable `net.inet6.ip6.rthdr0_allowed` to 1.

malformed packets. We presented the test cases and the experimentation results.

NGN has a detailed secure access scheme based on Authentication and Key Agreement (AKA) with nested IPsec key exchange over SIP [23, Section 5]. SIP itself, however, still includes many possible attack vectors such as dictionary-based password attacking [24, Section 2]. Secure RTP (SRTP) [25] and ZRTP key agreement protocol for SRTP [26] are also proposed to cryptographically protect real-time data transmission over RTP.

As IPv6 becomes more popular, more documents on IPv6 security are published, such as RFC4864 [27] about local network protection, US DoD Standard Profiles [28], and Cisco Press book of IPv6 Security [29]. We believe that the absence of systematic and reproducible testing methodology, however, is still one of the key factors that vulnerabilities are still persistent on network software and appliances. In this paper we showed an example of testing system, which is applicable to perform regression tests to prevent releasing bugs in actual products.

Our future research fields on IPv6 security may include the following issues:

- address scanning based on the implicit structure of IPv6 host identifier and EUI-64 algorithm;
- Flooding possibility of U-bit of OSPF for IPv6 [30, Section A.4.2.1];
- threats imposed by ICMPv6 [31] messages, including:
  - redirection;
  - Duplicate Address Detection (DAD);
  - flooding to multicast addresses;
  - Man-in-the-middle attack using RA; and
- obtaining network configuration by monitoring RA messages and polling to well-known multicast addresses [32].

## Acknowledgments

Our thanks go to Hiroki Takakura, Hiroki Nogawa, Song Jung Suk and Masaya Yamagata for their valuable suggestions and comments.

### References

[1] J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley, and E. Schooler, "SIP: Session Initiation Protocol," June 2002. RFC3261.

[2] S. Deering and R. Hinden, "Internet Protocol, Version 6 (IPv6) specification," 1998. RFC2460.

[3] K. Rikitake and K. Nakao, "NGN and Internet: from coexinstence to integration," Proceedings of ITU-T "Innovations in NGN" Kaleidoscope Conference, pp.315–322, ITU-T, May 2008. DOI: 10.1109/KINGN.2008.4542282.

[4] L. Mamakos, K. Lidl, J. Evarts, D. Carrel, D. Simone, and R. Wheeler, "A Method for Transmitting PPP Over Ethernet (PPPoE)," February 1999. RFC2516.

[5] R. Droms (Editor), J. Bound, B. Volz, T. Lemon, C. Perkins, and M. Carney, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)," 2003. RFC3315.

[6] Internet Assigned Numbers Authority (IANA), "DHCPv6 and DHCPv6 options." `http://www.iana.org/assignments/dhcpv6-parameters`.

[7] S. Hagen, IPv6 Essentials, 2nd ed., O'Reilly & Associates, 2006. ISBN-13: 978-0-596-10058-2.

[8] IAB and IESG, "IAB/IESG Recommendations on IPv6 Address Allocations to Sites," September 2001. RFC3177.

[9] R. Hinden and S. Deering, "IP Version 6 Addressing Architecture," February 2006. RFC4291.

[10] T. Narten, E. Nordmark, and W. Simpson, "Neighbor Discovery for IP Version 6 (IPv6)," December 1998. RFC2461.

[11] J. Postel, "Internet Protocol," 1981. RFC791 (also STD5).

[12] C. Partridge and A. Jackson, "IPv6 Router Alert Option." RFC 2711, Oct. 1999.

[13] J. McCann, S. Deering, and J. Mogul, "Path MTU Discovery for IP version 6," 1996. RFC1981.

[14] G. Ziemba, D. Reed, and P. Traina, "Security Considerations for IP Fragment Filtering," 1995. RFC1858.

[15] I. Miller, "Protection Against a Variant of the Tiny Fragment Attack," 2001. RFC3128.

[16] Digium, Inc., "Asterisk." `http://www.asterisk.org/`.

[17] Viagénie, "The Asterisk port to IPv6 Project." `http://www.asteriskv6.org/`.

[18] The OpenSIPS Project, "openSIPS." `http://www.opensips.org/`.

[19] G. Malkin and R. Minnear, "RIPng for IPv6." RFC 2080, Jan. 1997.

[20] S. Krishnan, "Handling of overlapping IPv6 fragments." INTERNET-DRAFT ietf-6man-overlap-fragment-02.txt, March 8, 2009.

[21] J. Abley, P. Savola, and G. Neville-Neil, "Deprecation of Type 0 Routing Headers in IPv6," December 2007. RFC5095.

[22] S. Cheshire, "IPv4 Address Conflict Detection," July 2008. RFC5227.

[23] D. Sisalem, J. Floroiu, J. Kuthan, U. Abend, and H. Shulzrinne, SIP Security, John Wiley & Sons, 2009. ISBN 978-0-470-51636-2.

[24] H. Dwivedi, Hacking VoIP: Protocols, Attacks, and Countermeasures, No Starch Press, 2009. ISBN 978-1-59327-163-3.

[25] M. Baugher, D. McGrew, M. Naslund, E. Carrara, and K. Norrman, "The Secure Real-time Transport Protocol (SRTP)," March 2004. RFC3711.

[26] P. Zimmermann, A. Johnston, and J. Callas, "ZRTP: Media Path Key Agreement for Secure RTP." INTERNET-DRAFT draft-zimmermann-avt-zrtp-15.txt, 4 March 2009.

[27] G.V. de Velde, T. Hain, R. Droms, B. Carpenter, and E. Klein, "Local Network Protection for IPv6," May 2007. RFC4864.

[28] DISR IPv6 Standards Technical Working Group, "DoD IPv6 Standard Profiles for IPv6 Capable Products Version 2.0." 1 August 2007, `http://www.nav6tf.org/documents/DISR_IPv6_Product_Profile_v20_FINAL_Aug07_ITSC_Approved.zip`.

[29] S. Hogg and E. Vyncke, IPv6 Security: Protocols, Attacks, and Countermeasures, Cisco Press, 2009. ISBN 978-1-58705-594-2.

[30] R. Coltun, D. Ferguson, J. Moy, and A. Lindem, "OSPF for IPv6," July 2008. RFC5340.

[31] A. Conta, S. Deering, and M. Gupta, "Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification," March 2006. RFC4443.

[32] R. Hinden and S. Deering, "IPv6 Multicast Address Assignments," July 1998. RFC2375.