EXPLOITING IPV6 ROUTING HEADERS TYPE 0/2 IN DIFFERENT IP WIRELESS NETWORKS: ATTACK SCENARIO & ANALYSIS

[1]BASSAM NAJI AL-TAMIMI, [2]RAHMAT BUDIARTO, [3]MOHD. ADIB OMAR, [4]KAMAL M. ALHENDAWI
[1,3,4] School of Computer Sciences, Universiti Sains Malaysia, Penang, Malaysia
[2]Networked Computing Center, Surya University, Serpong, Indonesia
[*]Corresponding Author E-mail: bnaa09_nu0186@student.usm.my

ABSTRACT

Mobile IP is an open standard protocol designed by IETF to allow users to move from one network to another while maintaining their own permanent IP addresses. However, the seamless connectivity in different IP networks has introduced new security vulnerabilities. One of the most critical concerns with the IPv6 is IPv6 routing header. IPv6 routing header can be used by an IPv6 source to list one or more intermediate hosts to be visited on the way to a packet's destination. Nevertheless, the feature of IPv6 routing header which has serious vulnerability can be used by attacker to bypass security policies applied on filtering devices such as firewall. This study analyzes the IPv6 routing header feature which can be exploited by attackers to access the protected hosts/networks. Thus, the current study provides a comprehensive view regarding the scenario of attackers within the different IP wireless networks which in turn provide the researchers and practitioners with the threats of attackers. The scenario analysis also leads to developing new mechanisms for covering the security problem of routing header type 0/2 which is still under investigation.

Keywords: *MIPv4; MIPv6; MN; IPv6 Routing Header, Different wireless IP networks*

1. INTRODUCTION

Mobile IP (MIP) security has always a high concern in any internetworking environment. However, it has special significance to be implemented in different IP networks (IPv4/IPv6) [1], since there is no compatibility between the both protocols. Thus, the security concern in different IP networks is considered to be one of the most critical issues in MIP networks. MIP is an open standard protocol designed by Internet Engineering Task Force (IETF) to allow users to move from one network to another while maintaining their own permanent IP addresses [2].

In IP networks, routing is based on fixed IP addresses, similar to a postal letter delivery: once the mobile node moves away from its home network and is no longer reachable using normal IP routing, the mobile node asks its home post office to forward the mail to its new attached network through the local post office there [3]. Thus, when the mobile node leaves its home network to another network, it remains using the same IP address while roaming over a different network. Therefore, MIP ensures that a roaming individual could continue communication without sessions or connections being dropped. MIP which is based on Internet Protocol - IP is more scalable for the Internet and it offers a wide connectivity for users, whether they are roaming within their home network or traveling away from home. MIP is a part of IPv4 and IPv6 as well.

The rest of this study is organized as follows: In Section 2, IP mobility support is summarized. Section 3 introduces the main MIP security concerns in different IP networks. Section 4 gives a brief overview of IPv6 extension headers and then presents various types of IPv6 extension headers and then describes the different types of routing header (type 0 and type 2). Section 5 discusses the attack scenario using routing header types 0/2. Finally, the conclusions are drawn in Section 6.

2. IP MOBILITY SUPPORT FOR IPV6/IPV4

In [4] and [5] the mobility support and its solutions have been explained in details. The following subsections briefly introduce the existing mobility solutions, which involves the basic operations of Mobile IPv4 and Mobile IPv6 to give a clear understanding of both protocols. Moreover, the main differences between the both protocols are introduced.

A. Mobile IPv4

Mobile IPv4 (MIPv4) is the most common solution for mobility on the current IPv4 Internet [4]. IETF has developed MIPv4 to provide the Internet connectivity to mobile devices and users that are attached along with the Internet. MIPv4 introduces three functional entities: Mobile Node (MN), Home Agent (HA), and Foreign Agent (FA), as illustrated in Figure 1.

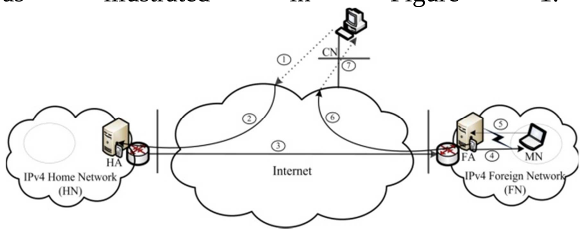

Figure 1: MIPv4 components and its roaming over a foreign network

B. Mobile IPv6

Mobile IPv6 (MIPv6) has inherited a number of features from MIPv4 and provides several other improvements over MIPv4 [5].

Route optimization capability is embedded in all MIPv6 nodes rather than being added as an optional extension with MIPv4. Route optimization [6] has been proposed to provide the MN with the capability to avoid the problem which is called the triangle routing problem for any of its CNs. This problem occurs when the MN is apart from its HA. The CN will not be aware of the MN's current location. Therefore, the CN must tunnel the packets through the MN's HA in an indirect path. While the MN can tunnel the packets to the CN directly by updating a CN of a MN's new CoA using a Binding Update message (BU), a CN can forward the packets directly to a MN without the need for the HA to redirect the packets. Furthermore, the essential entities involved in the operation of MIPv6 are the MN, HA, and CN are depicted in Figure 2.

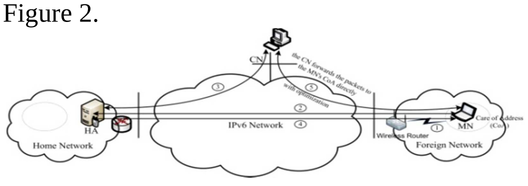

Figure 2: the MIPv6 components and its roaming over a foreign network

C. MIPv4/MIPv6 Comparison

In comparison to the design of MIPv4 protocol, MIPv6 protocol has inherited a number of features and added many other improvements over MIPv4 limitations. Thus, it is significant to highlight in this subsection such essential differences between two protocols; MIPv4 and MIPv6 [5]:

- Foreign Agent is considered to be one of the major MIPv4 elements that are required for optimum functionality, while in MIPv6 such element is not required since simple stateless auto-configuration procedure is provided by IPv6. In particular, this procedure allows MN to seamlessly acquire its care-of address from any foreign network without the need for any intermediate IP support of a Dynamic Host Configuration Protocol (DHCP) [7].
- Route optimization capability is embedded in all MIPv6 nodes as a basic part of the protocol, rather than being added as an optional extension with MIPv4 protocol.
- In mobile IPv6, packets sent to a MN while it is away from its home network using an IPv6 routing header rather than IP encapsulation, whereas in mobile IPv4, packets sent using encapsulation technique for all packets. However, the encapsulation technique is still applicable in mobile IPv6 and the HA can use it for tunneling.
- The MN's HA intercepts the incoming packets that are destined for a MN which is away from its home network using Neighbour Discovery Protocol (NDP) [8] instead of Address Resolution Protocol (ARP) [9] as is used in MIPv4.

3. MIP SECURITY CONCERNS IN DIFFERENT IP NETWORKS

Several studies have been extensively investigated on security concerns and implications of MIP such as [10-13]. However, the security concerns of both MIP protocols (MIPv4 and MIPv6) have been considered separately since their designing period, but a little attention has been given to these protocols in the different environments (i.e., mobility over different IP networks IPv4/IPv6).

Authors in [14] discussed some security issues of IPv4 and IPv6 and also analyzed different security threats that have may emergence due to the implement of various transition mechanisms. The most critical vulnerability related to IPv6 extension headers was identified in [15]. This vulnerability can be occurred due to exploiting the IPv6 routing header (RH) feature which has been more demonstrated and analyzed in many recent studies [10, 16, 17]. According to the IPv6 specification [18], all the nodes that are supporting IPv6 must be able to process IPv6 RHs. On the other hand, such vulnerability potentially can be used by attackers to bypass network security through avoiding Access Control Lists (ACLs) on destination addresses [19].

In this concern, [20] suggested that the firewall policy must block forwarding packets with type 0 RHs and permitting other types of RHs to pass through. Whereas blocking all IPv6 packets containing RHs is not a worthy solution as this could have serious implications for the IPv6 future development. Recently, most of firewall policies are blocking all packets containing type 0 RHs. In addition, the default firewall configuration prevents the forwarding of IPv6 traffic with type 0 RHs.

As defined earlier in [2], MIP is an open standard protocol designed by IETF to allow users to move from one network to another while maintaining their own permanent IP addresses. RFC 6275 [5] provided new extension headers and some modifications for MIPv6 such as mobility header, type 2 RH and home address option. The specification also provides some security features of MIPv6 which are protect the binding update messages to both HA and correspondent nodes, protect the mobile prefix discovery, and besides that protect the mechanisms of MIPv6 that uses for carrying data traffic. The following is two methods uses for protecting the binding update messages:

A binding update message to a HA is secured by the Internet protocol security (IPsec) [21]. IPsec is defined as a mechanism of securing data traffic between a MN and HA for MIPv6. MIPv6 data traffic that is protected by IPsec includes the binding update and acknowledgement messages [22].

A binding update message to a correspondent node is secured by the Return Routability Procedure (RRP). [5] has standardized and defined the RRP to provide basic protection for MIPv6 binding update messages between a MN and a correspondent node.

Figure 3 describes a topology of binding update messages exchange that are protected by IPsec and RRP and carried on the new MIPv6 extension headers.

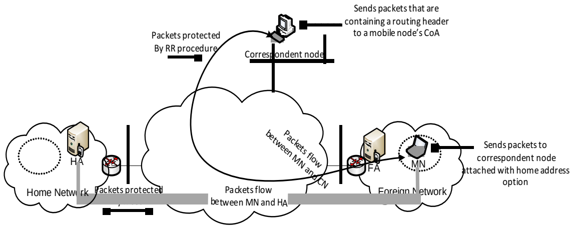
Sends packets that are containing a routing header to a mobile node's CoA
Packets protected By RR procedure
Correspondent node
HA
Home Network
Packets protected
Packets flow between MN and HA
Packets flow between MN and CN
FA
MN
Foreign Network
Sends packets to correspondent node attached with home address option

Figure 3: A topology of protected BU messages

Some of the IPv6 security issues have been discussed in [12, 20]. The feature of IPv6 RH can be used to bypass security policies applied on filtering devices such as firewall. The authors have suggested some solutions to avoid such vulnerability. These solutions should be handled manually by the network managers to assign specific set of hosts to act as MIPv6 HAs and also they should to configure their security systems to prevent any traffic that consist the RH.

4. IPV6 EXTENSION HEADERS

Deering and Hinden [18] defined the IPv6 extension headers which comprise encoded optional Internet-layer information in separate headers. As clarified in this RFC specification the headers may be inserted between the IPv6 header and the upper-layer header such as TCP, UDP or ICMP in an IPv6 packet.

Any IP header is followed by an extension header contains a next header specific value that aims to identify the type of the immediately following extension header. Table 1 presents a list of most commonly used extension headers. The next header value of the immediately preceding IP header refers to the next extension header. The next header values of the successive extension headers pointing to the next extension header and ends up in the last extension header.

TABLE 1: EXTENSION HEADERS

Protocol /Extension Header Name	Keyword	The Value (decimal)
Hop-BY-Hop	HBH	0
TCP	TCP	6
User Datagram	UDP	17
Routing Header	RH	43
Fragmentation Header	FH	44
Encapsulation Security Payload Header	ESP	50
Authentication Header	AH	51
Encrypted Security Payload	ESP	52
ICMPv6	ICMPv6	58
No next header	NULL	59
Destination Options Header	-	60
Mobility Header	MH	135

Figure 4 shows two examples of an IPv6 header; the first example depicts an IPv6 datagram when it has no extension headers conveying its encapsulated TCP segment data. Second example shows an IPv6 datagram with a RH (RH/43 as listed in Table 2.1), an authentication header (AH/51) and TCP segment data (TCP/6).

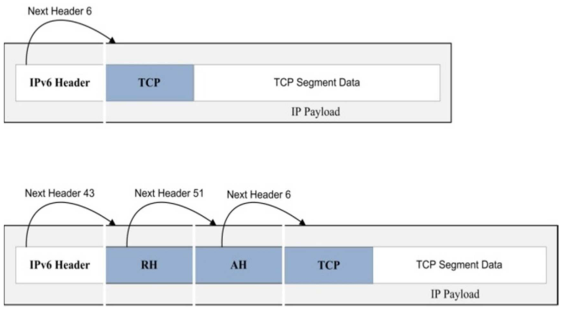

Figure 4: Example of IPv6 chaining extension headers

4.1 IPv6 Routing Headers

The IPv6 RH is identified by a next header (NH) value of 43 in the immediately preceding header. There are two types of RHs supported in IPv6, type 0 RH and type 2 RH. IPv6 type 0 RH is analogous to loose source and record routing option in IPv4 [23]. IPv6 type 2 RH is used in the implementation of MIPv6.

The IPv6 RHs can be used by an IPv6 source to list one or more intermediate hosts to be visited on the way to a packet's destination [18]. The next header value in the immediately preceding header indicates the next header type of packet extension header (e.g., the value of 43 in the IPv6 next header indicates the RH).

IPv6 RH comprises of four fields. The size of each field is 8 bit, as illustrated in Figure 5 and Table 2:

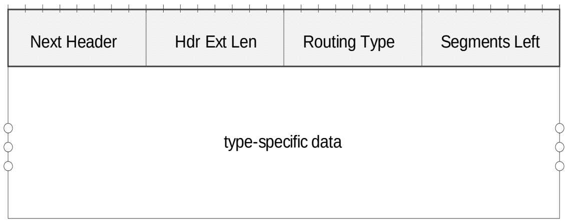

Figure 5: Extension Routing Header Format

Table 2: Extension Routing Header field descriptions

Field	Description
Next Header	Contains the next header value which is immediately following the RH.
Hdr Ext Len	Identifies the RH length.
Routing type	Defined for a particular RH type, here two values used are 0 and 2.
Segments Left	Specifies the number of the intermediate hosts remaining in the rout to be visited before reaching the final destination. It refers to a list of IP addresses (up to 25).
Type-specific data	variable-length field, of a format determined by the routing type
Next Header	Contains the next header value which is immediately following the RH.

A) Type 0 Routing Header

The IPv6 Type 0 RH (RH0) is analogous to loose source and record routing option in IPv4 [23]. This functionality which is originally provided by IPv6 can be used to list one or more intermediate hosts to be visited on the way to a packet's destination. On the other hand, it can be exploited by the attackers to bypass the traffic filtering mechanism and generate a Denial of Service (DoS) attack [12, 20, 24]. Figure 6 provides the format of the RH0.

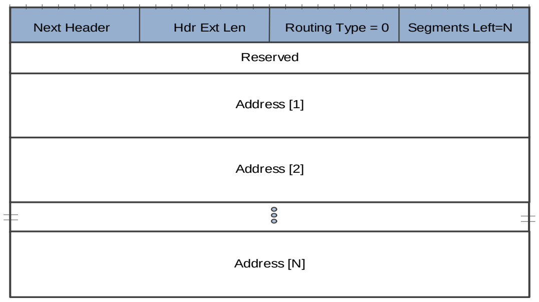

Figure 6: Type 0 RH format

B) Type 2 Routing Header

IPv6 Type 2 (RH2) was originally defined in RFC 3775 [25]. It proposed to be used by the correspondent node or the HA to carry only the MN's own home address when it is roaming away from home network. This specification has also restricted the number of IPv6 addresses that have to be carried by RH2 to be only one IPv6 address. However, the [26] extends the format of RH2 to be able to carry number of IPv6 addresses. The following Figure 7 provides the format of RH2.

Next Header	Hdr Ext Len=2	Routing Type=2	Segments Left=1
Reserved			
Home Address			

Figure 7: Type 2 Routing Header format

The RH of type 2 could be employed in such cases: a node sends a binding acknowledgement message, a HA / a correspondent is performing route optimization, or a HA sends a mobile prefix advertisement message.

The MN would not be able to receive the packet directly that refers to the destination address of its home address. This occurs when it is far away from its home. The MN's home network receives such a packet. If packets are needed to be directly sent to the MN that is apart from home by a correspondent node, a RH2 is required by this node. Accordingly, the packet's destination address is set to the MN's care-of address. The RH2 carries the home address. Hereby, such a packet is routed directly to the MN. The MN processes the RH by replaces the packet's destination address with its home address involved in the RH2.

5. CRITICAL ANALYSIS

In this section, the researchers view the problem that might encounter mobile home networks due to the IPv6 RH exploiting. A new policy that could cover the problem is also suggested toward assisting the network specialists in the detection of such security bug.

5.1 Vulnerability of Using IPv6 Routing Header

An attacker can exploit the functionality provided by IPv6 RH0 in order to generate malicious packets which performed through specifying the victim IP address in the RH. These kinds of packets will be routed through public accessible IP address (e.g., network server) and some intermediate hosts to be finally delivered by the victim host. Certainly, the malicious packets will be subjected to check process via the server of the intended network. Then the server forwards these packets based on the IP addresses specified in the RH. Thus, the malicious packets will reach to victim host without breaking any of the security policies.

Such this vulnerability enables attackers to bypass the protected network, and then it might eventually be possible to create the opportunity for Denial of Service attack (DoS) or Distributed Denial of Service attack (DDoS). This vulnerability results in such case: with every new attachment of a MN with an IPv6 network, all the clients of its HA would become susceptible to attacks. Thus, all packets which are received and passed through the HA must be subjected to inspection process.

5.2 Vulnerability of Using IPv6 Routing Header (Scenario I)

Figure 8 illustrates a scenario of how the home network can be attacked. Figure 8 presents the movement of MN between different IP networks. It also reveals the possibility for attacking the network through using routing header. It is clear that the MN moves from its IPv4 home network to another network supported by IPv6. With regard to the location of the attacker, if the visited IPv6 network is under attack then the attacker can launch its attack towards the IPv4 home network based on the information obtained from visited mobile.

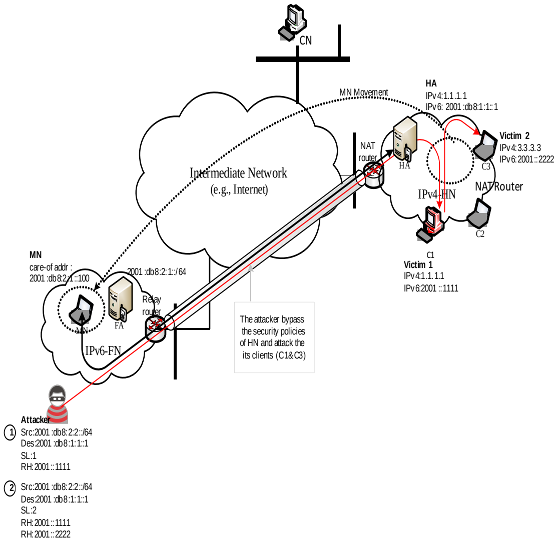

Figure 8: Routing Header Attack Scenario I

5.3 Vulnerability of Using IPv6 Routing Header (Scenario II)

Figure 9 shows the second scenario followed by the attacker in case of RH2. This scenario is different from the one presented in the previous section. In this concern, the attack can occur whenever the MN moves from IPv6 to IPv4.

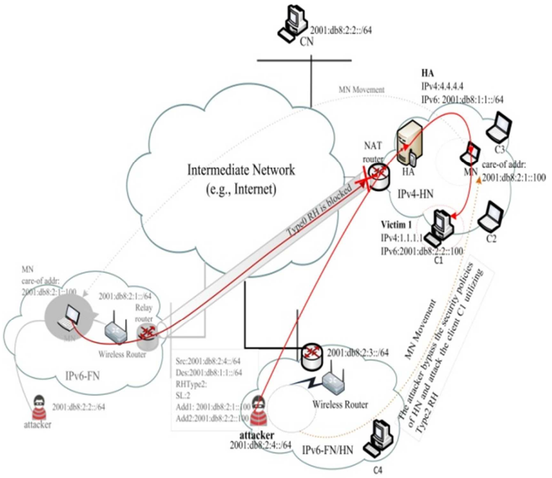

Figure 9: Routing Header Attack Scenario II

When the MN moves away from its IPv6 home network to a new location (IPv4 network) as illustrated in Figure 9, it must detect whether or not it has attached with a different network. Once the MN obtained the IPv6 care-of address, it updates its HA by sending binding update message then the attacker located at IPv6 network can exploit the obtained information in the attack of the home network, and particularly, the attacker uses Type 2 RH.

5.4 Suggested: Filtering Processes

In this study, we suggest that, a packet filtering process should be take place. When the MN moves to a different IP network the tunneling connectivity to the HA is accomplished by using IP encapsulation mechanism. Whenever this technique is used, the first receiver node forwards the packet to the final destination based on the inner IPv6 header, and then, the packet is decapsulated and forwarded to the next nodes, whereas; the list of IP addresses attached in the RH justifies this process.

A packet filter is used to examine and make decisions about the recipient packets. It should be designed to inspect packets based on type of IP version, source IP, type of the next extension header, IPv6 RH type and on RH IPv6 destination addresses to determine that packet should be allowed through or denied. Whereas the key security policies of a packet filter either allowing or denying packets based on IP address.

6. CONCLUSION

In this study, some solutions that have been suggested to prevent or mitigate the vulnerability of IPv6 RH are introduced. The potential security vulnerability of the IPv6 RH relating to MIP in different IP networks (IPv4/IPv6) is analyzed through scenarios. For this reason, we provide two analytical scenarios in order to approach the security problem resulted in different wireless networks.

The worth mentioning, the scenario analysis of attack indicates that there is a considerable possibility to have security problem in the coexistence different MIP networks which in turn brings forth for suggesting and developing new techniques to be consistent with seamless connectivity. Finally, this helps in covering of the problem of IPv6 RH in different network environments.

REFRENCES:

[1] S. M. Ahmadi, "Analysis towards Mobile IPV4 and Mobile IPV6 in Computer Networks," *International Journal of Intelligent Systems and Applications (IJISA)*, vol. 4, p. 33, 2012.

[2] C. Perkins, " IP mobility support," *Request for Comments RFC 2002, Mobile IP Working Group*, 1996.

[3] M. S. Taylor, *et al.*, *Internetwork mobility: the CDPD approach*: Citeseer, 1997.

[4] C. Perkins, "RFC 3344: IP mobility support for IPv4," *The Internet Society, http://tools.ietf.org/html/rfc3344,* vol. (Obsoletes: 3220), 2002.

[5] J. Arkko, *et al.*, "RFC 6275:Mobility support in IPv6," *The IETF, http://tools.ietf.org/html/rfc6275,* vol. (Obsoletes: 3775), 2011.

[6] C. E. Perkins and D. B. Johnson, "Route optimization for mobile IP," *Cluster Computing*, vol. 1, pp. 161-176, 1998.

[7] R. Droms, "RFC 2131–Dynamic Host Configuration Protocol, 1997," *Network Working Group, http://tools.ietf.org/html/rfc2131*, 1997.

[8] T. Narten, *et al.*, "RFC 2461 Neigbhour Discovery for IP Version 6 (IPv6), 1998," *URL reference: http://www.ietf.org/rfc/rfc2461. txt,* vol. (Obsoletes: 2461), 1998.

[9] S. Cheshire, "RFC 5227: IPv4 Address conflict detection," *Network Working Group, http://tools.ietf.org/html/rfc5227,* vol. (Updates: RFC 826), 2008.

[10] E. Durdağı and A. Buldu, "IPV4/IPV6 security and threat comparisons," *Procedia-Social and*

Behavioral Sciences, vol. 2, pp. 5285-5291, 2010.

[11] D. Zagar, *et al.*, "Security aspects in IPv6 networks-implementation and testing," *Computers & Electrical Engineering*, vol. 33, pp. 425-437, 2007.

[12] S. Convery and D. Miller, "IPv6 and IPv4 threat comparison and best-practice evaluation (v1. 0)," *Presentation at the 17th NANOG*, 2004.

[13] M. La Polla, *et al.*, "A survey on security for mobile devices," *IEEE COMMUNICATIONS SURVEYS & TUTORIALS*, vol. Vol. 15, 2013.

[14] P. Shanmugaraja and S. Chandrasekar, "Accessible Methods to Mitigate Security Attacks on IPv4 to IPv6 Transitions," *European Journal of Scientific Research*, vol. Vol. 77, pp. 165-173, 2012.

[15] P. Savola, "Security of IPv6 routing header and home address options," Technical report, IETF. http://tools.ietf.org/html/draft-savola-ipv6-rh-ha-security-00. Accessed 25Aug 2011.2002.

[16] S. Frankel, *et al.*, "Guidelines for the secure deployment of IPv6," *NIST Special Publication*, vol. Vol. 800, p. 119, 2010.

[17] V. Karthikeyan and Prittopaul.P, "A Survey on Vulnerability of Type 0 Routing Header in IPv6," *International Journal of Computer Science and Management Research*, vol. Vol 2, 2013.

[18] S. Deering and R. Hinden, "RFC 2460: Internet Protocol, Version 6 (IPv6) Specification," *Network Working Group*, vol. (Obsoletes: 1883), 1998.

[19] P. Biondi and A. Ebalard, "IPv6 Routing Header Security. http://www.secdev.org/conf/IPv6_RH_security-csw07.pdf. Accessed 10 Feb 2012.," ed, 2007.

[20] J. Abley, *et al.*, "Deprecation of type 0 routing headers in IPv6," *draft-ietf-ipv6-deprecate-rh0-01 (work in progress)*, 2007.

[21] K. Seo and S. Kent, "RFC 4301: Security architecture for the internet protocol," *Network Working Group, http://tools.ietf.org/html/rfc4301*, vol. (Obsoletes: 2401), 2005.

[22] A. Patel, *et al.*, "RFC 4285 :Authentication Protocol for Mobile IPv6," *draft-patel-mip6-rfc4285bis-00 (work in progress)*, 2006.

[23] D. B. Johnson, "Mobile host internetworking using IP loose source routing," DTIC Document1993.

[24] M. Wadhwa and M. Khari, "Security Holes in Contrast to the New Features Emerging in the Next Generation Protocol," *International Journal of Computer Applications*, vol. 20, 2011.

[25] D. Johnson, *et al.*, "RFC 3775: Mobility support in IPv6," *IETF*, *June*, 2004.

[26] P. Thubert and M. Molteni, "IPv6 reverse routing header and its application to mobile networks," *Work in Progress*, 2007.