TELKOMNIKA, Vol.12, No.4, December 2014, pp. 969~976
ISSN: 1693-6930, accredited A by DIKTI, Decree No: 58/DIKTI/Kep/2013
DOI: 10.12928/TELKOMNIKA.v12i4.540

Trusted Node-Based Algorithm to Secure Home Agent NATed IPv4 Network from IPv6 Routing Header Attacks

Mohamed Shenify
College of Computer Science and Information Technology, Albaha University
P.O. Box 1988, 65431 Albaha, Kingdom of Saudi Arabia
Telp.: +966 7 727 4111, Fax.: +966 7 724 7272
e-mail: maalshenify@bu.edu.sa

Abstract

Providing a secure mobile communication in mixed IPv4/IPv6 networks is a challenging task. One of the most critical vulnerabilities associated with the IPv6 protocol is the routing header that potentially may be exploited by attackers to bypass the security. This paper discusses an algorithm to secure home agent network from the routing header vulnerability, where the home agent network uses IPv4 Network Address Translation *(NAT) router. The algorithm also takes into account multi-hops destination in the routing header. Verification was done through implementation of the algorithm at the Home Agent modul in a testbed network. The experimental results show that the proposed algorithm provides secure communication between Correspondent nodes and Mobile Nodes that moved into the NATed network without causing a significance filtering delay.*

Keywords*: IPv6 security, IPv6 routing header, mobile IP, mixed IP network*

1. Introduction

Due to the direct incompatibility between IPv4 and IPv6 the security concern in mixed IP networks is considered to be one of the most critical issues in mobile Internet Protocol (MIP) networks [1].

Tunneling technique is being used to support mobility in mixed IP networks. The encapsulation of IPv6 packets into IPv4 packets may intruduce new security vulnerabilities, because the security devices of the home agent network may not be able to perform deep traffic inspection on the IPv6 header that contains routing header (RH). The RH has two types: RH type 0 (RH0) and type 2 (RH2).

IPv4 and IPv6 will coexist for a long period of time [2]. During this period, the movement of the mobile nodes (MNs) among networks configured with different IP protocols is unavoidable [3],[4]. Therefore, mobility support in mixed IPv4 and IPv6 networks has gained vital importance.

Many researchers have shown interests in proposing new mechanisms to address the security issue of IPv4 and IPv6 coexistence with mobility support. Several studies have investigated security concerns and implications of MIP such as [5]-[7]. Moreover, authors in [8] discuss security issues of IPv4 and IPv6 and also analyze different security threats that may emerge due to implementation of various transition mechanisms. Vulnerability can occur due to exploitation of the IPv6 RH feature which has been demonstrated and analyzed in many recent studies [9]. All the nodes that support IPv6 must be able to process IPv6 RHs. At the same time, such vulnerability can be used by attackers to bypass network security through avoiding access control lists on destination addresses. In this concern, the firewall policy must block forwarding packets with type 0 RHs (RH0) and permit other types of RHs (RH2) to pass through. Blocking all IPv6 packets containing RHs is, however, not a worthy solution as this could have serious implications for the IPv6 future development. Recently, most of firewall policies block all packets containing RH0. In addition, the default firewall configuration prevents the forwarding of IPv6 traffic with RH0.

The RH functionality which is originally provided by IPv6 can be used to list one or more intermediate nodes to be visited on the way to a packet's destination. At the same time, it can be exploited by the attackers to bypass the traffic filtering mechanism and generate a Denial of Service (DoS) attack [10],[11].

An attacker can exploit the RH in order to generate malicious packets which are performed through specifying a victim node's IP address in the RH. These kinds of packets will

Received September 23, 2014; Revised November 7, 2014; Accepted November 20, 2014

be routed through a public accessible IP address (e.g., network server) and some intermediate nodes to be finally delivered to the victim host. Certainly, the malicious packets will be subjected to a checking process in the server of the intended network. The server forwards these packets based on the IP addresses specified in the RH. Thus, the malicious packets will reach the victim host without breaking any of security policies as shown in Figure 1. Therefore, all packets which are received and passed through the HA must be subjected to an inspection process.

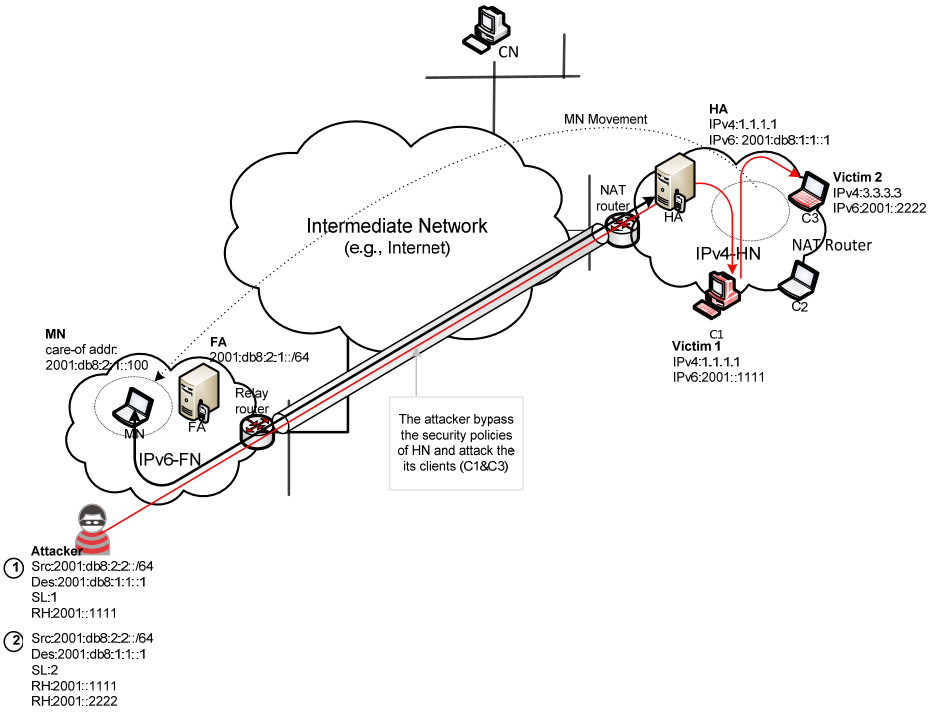

Figure 1. Scenario on Routing Header Attacks

2. Research Method

When a MN moves to a different IP network the tunneling connectivity to the HA is accomplished by using IP encapsulation mechanism. The encapsulated packet consists of IPv4-UDP-IPv6. 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. All of the received packets that are in encapsulated format are subject to a filtration process to protect the Home Network (HN) from possible spoofing attacks. The purpose of checking the RH is to determine whether the type of the RH is either 0 or 2 and either the IPv6 addresses inlcuded in RH2 are valid or not. Figure 2 illustrates the algorithm to filter the incoming packets into the Home Agent (HA) module.

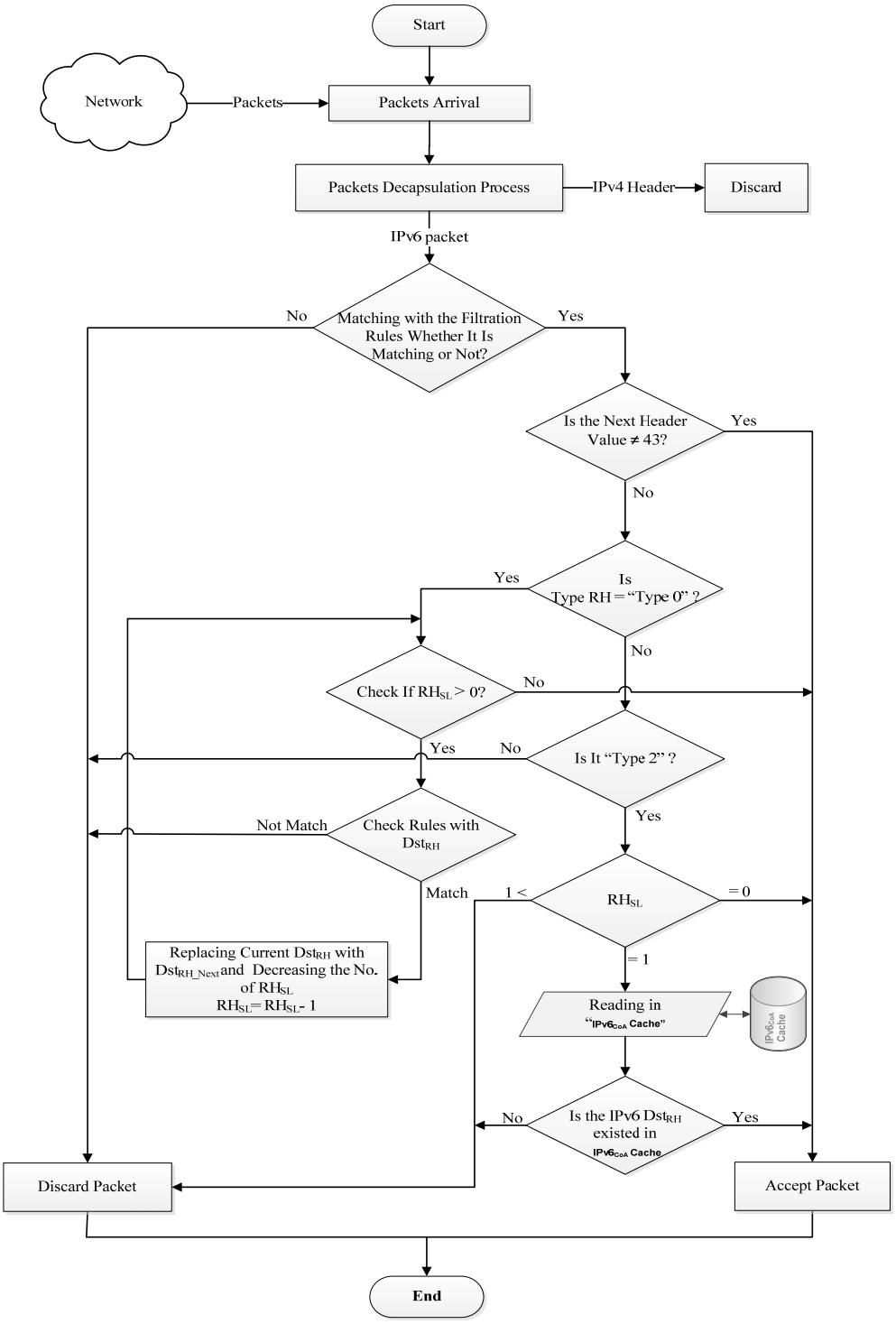

Figure 2. The Proposed Algorithm

A testbed has been set up to verify the proposed algorithm. The testbed topology has three components as follows (See Figure 3).

1. IPv6 traffic emulator is designed to generate IPv6 packets including RH0 and RH2 used to evaluate the performance of the proposed algorithm. Several CNs can simultaneously send packet to a MN stay behind NAT router

2. The algorithm in home network implemented in the HA. This module receives the packets sent through the NAT router and then processes these packets according to the proposed algorithm.
3. HA clients act as MNs moved in into IPv4 only network with NAT. This HA clients are having connection with outsiders and obtaining IPv6 addresses from Teredo server.

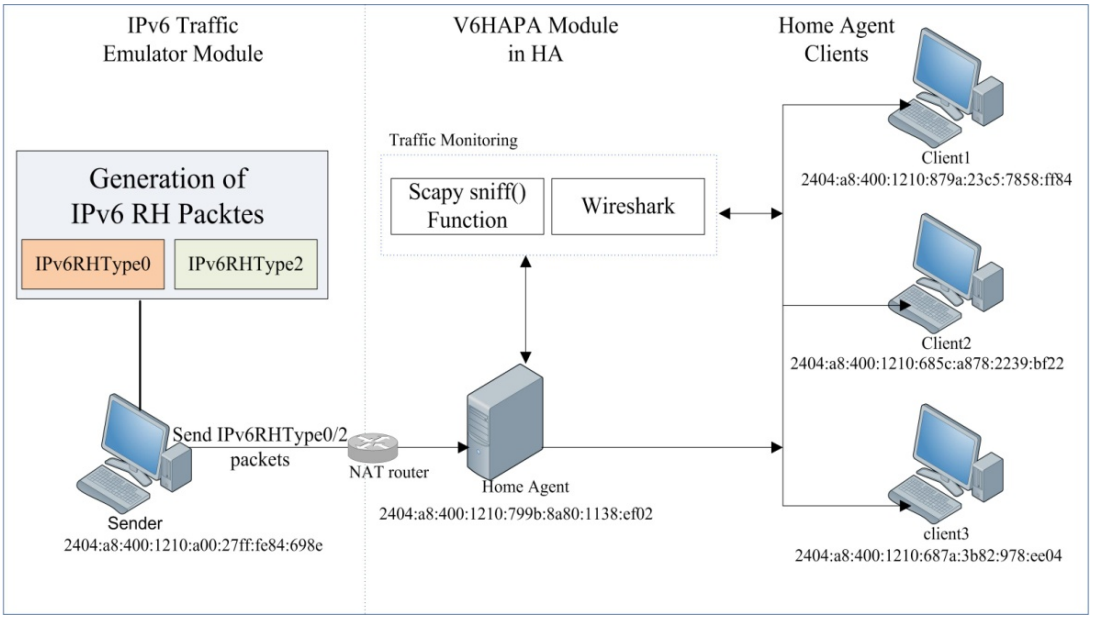

Figure 3. Testbed Topology for the Experiment

Table 1 shows the hardware specifications and the configuration settings for the undertaking experiment.

Table 1. Hardware Specifications and Configuration Settings

Installation & configuration settings	Sender	Receiver	Clients
Operating System	Linux Fedora 13	Linux Fedora 13	Windows 7
PC manufacturer	Acer® PC	Acer® PC	Dell® PC
Processor	Intel® Core™ 2 CPU, E4500 @ 2.20GHz	Intel® Core™ 2 CPU, E4500 @ 2.20GHz	Intel® Core™ 2 CPU, E4500 @ 2.20GHz
RAM	2 GB	2 GB	4 GB
Implementation	Scapy 2.2.0 , Python	C programming language	Configuration
Traffic Monitoring tool	Scapy sniffing function	Wireshark, Scapy sniffing function	Wireshark , Scapy sniffing function
IPv6 Address	2404:a8:400:1210:a00 :27ff:fe84:698e	2404:a8:400:1210:7 99b:8a80:1138:ef02	**C1.** 2404:a8:400:1210:879a:23 c5:7858:ff84 **C2.** 2404:a8:400:1210:685c:a8 78:2239:bf22 **C3.** 2404:a8:400:1210:687a:3b 82:978:ee04

Five scenarios are used in the experiments as follows.
Scenario 1: multiple CNs send IPv6 packets containing 50% normal packets and 50% suspicious packets. Each RH type are conducted 10 runs in the experiment, starting with 500 packets up to 5000 packets with 500 packets increament.

Scenario 2: Five CNs are emulated to craft and send simultaneously 5000 IPv6 packets to the HA. Three CNs send IPv6 packets containing RH0, while the rest send packets without RH0. According to [12] the majority of observations should be at least 60% of the population as a normal packets. Hence, in this paper 70% normal packets (i.e., packets without RH0) and 30% malicious (packets that include RH0) are considered to be the representative of the majority of the packets. The packets which include RH0 are distributed as follows:

(1) 20% of the packets have matched IP destination addresses with the authorized list, and
(2) 10% of those packets have unmatched IP destination addresses (i.e., suspicious packets) in the RH. The unmatched packets can be divided into 7% malicious packets and 3% normal packets.

Experiments are conducted for this scenario, and the results have been subsequently used to calculate the accuracy of the proposed algorithm in terms of preventing the HA from RH0 vulnerability using Equation (1) and Equation (2).

$$Accuracy = \left(\frac{TP+TN}{TP+TN+FP+FN}\right) * 100\% \quad (1)$$

$$False\ Positive\ rate\ = \left(\frac{FP}{(FP+TN)}\right) * 100\% \quad (2)$$

In this paper, the false positive is defined as the situation in which the actual normal packet is detected as an attack. False positive occurres because the proposed algorithm rejects all the suspicious packets (i.e., malicious and normal packets) carrying unmatched IPv6 routing header addresses.

Scenario 3: Five CNs are emulated to send IPv6 packets to HA clients through NAT and the proposed algorithm module in HA. The CNs are divided into three sets. The first set has two nodes which are intended to generate and send suspicious packets with RH2 (containing unregistered IPv6 destination address). The second set contains two nodes that generate and send packets without RH2. The last set represents an authorized CN which intends to generate packets containing RH2 with valid IPv6 destination address. The generated packets sent by the authorized CN are specified with only one RH destination IP address per packet. The embedded IP addresses within the RH2 must be matched with the home address of the MN that has already stored in the IPv6CoA_cache. Total number of packets is 5000.

Scenario 4: Same as Scenario 1, but with the ratio of normal packet to malicious packet is set to 40% to 60%.

Scenario 5: Same as Scenario 1, but with the ratio of normal packet to malicious packet is set to 60% to 40%.

3. Results and Analysis

Two aspects of performances are considered in the experiments; performance in term of packet filtering process time and accuracy in detecting malicious packets.

3.1. Filtration Time

Figure 4 displays the time required to filter the same amount of packets while the size of packets also increased in accordance with the IPv6 RH0. The figure also leads to the conclusion that when the number of IPv6 RH addresses increase, the time required for the filtration process also increased. It is worth noting that the developed algorithm requires more time to filtrate the matched packets than unmatched packets. The reason behind this observation is that the filtration process for matched packets continues until the last RH IP address while in case of unmatched packets the filtering process stops when at least one of those IP addresses does not match with the IP addresses in the dataset. Hence, it can be concluded that this algorithm performs better considering the time required for filtering the unmatched packets.

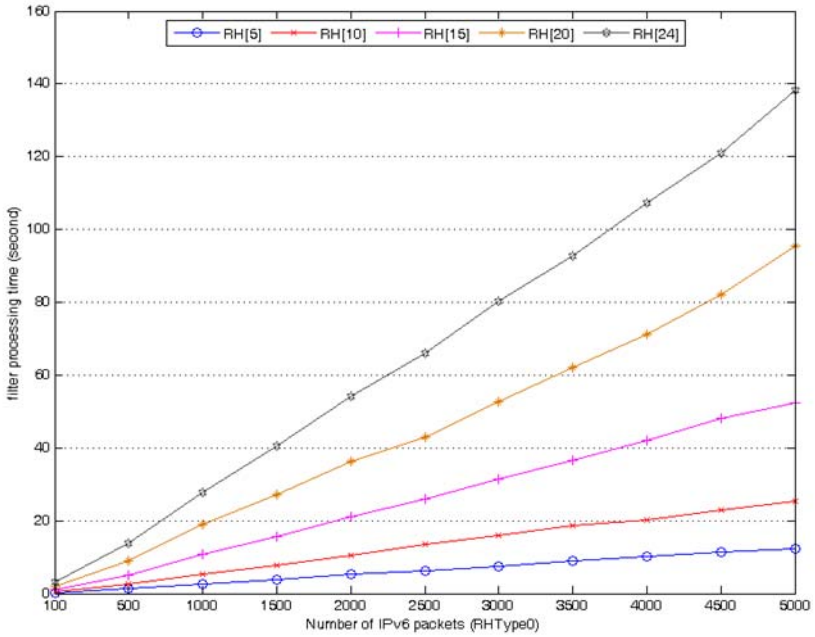

Figure 4. Filter Processing Time vs. Number of IPv6 Packets with RH0 [5]-[24]

Figure 5 shows the filtration processing time on RH2 which containing and not containing multi-hop IP addresses, and also the one without any security policy in the HA. The proposed algorithm affects the network performance in terms of filtering delay. The filtration process time for packet containing multi-hop RH2 is higher than non-multi-hop packet.

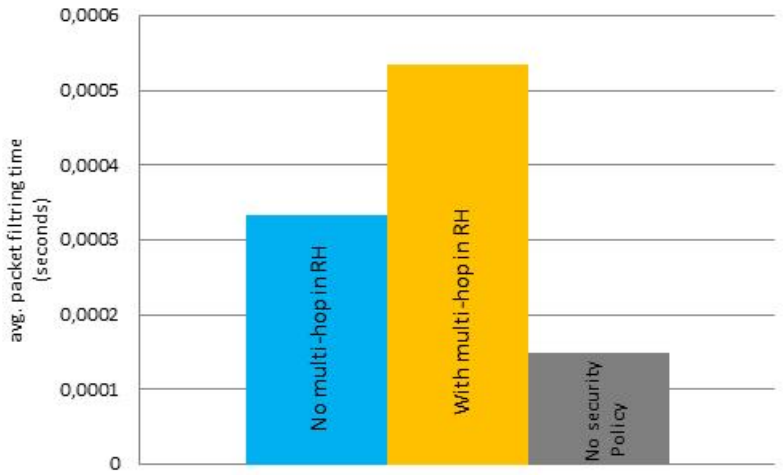

Figure 5. Average Packet Filtering Time on RH2

3.2. Accuracy

In Figure 6, the plot with red color represents the case when the number of malicious packets is greater than normal packets. In this concern, the number of malicious packets is a multiple of normal packets. However, the blue line represents the case at which the number of normal packets is greater than the malicious packets. Based on this figure, it is obvious that the accuracy of the proposed algorithm performs better when the number of malicious packets

greater than normal packets. The cause of better accuracy is mainly resulted from the decreament of the false positive rate.

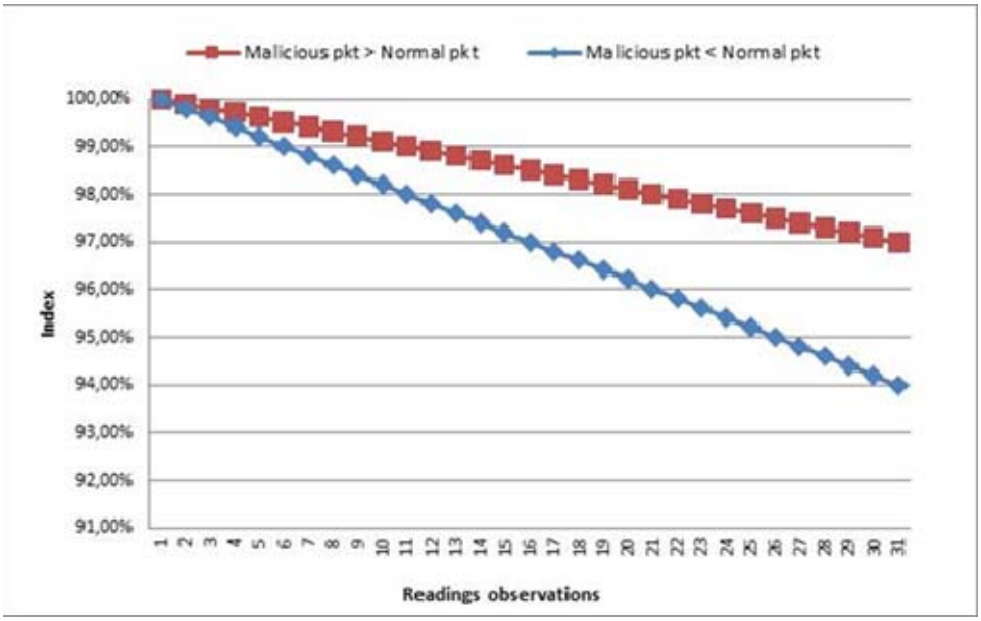

Figure 6. Accuracy of the Proposed Algorithm on RH0 Based on 31 Observations

The extended algorithm has a high accuracy in protecting the home network and handles suspicious packets containing multi-hops of RH IP addresses. Compared to no multi-hop algorithm, the multi-hop algorithm has accuracy of 97% with a difference of 2%. Figure 7 shows the accuracy of the proposed algorithm with multi-hop and no multi-hop addresses handling.

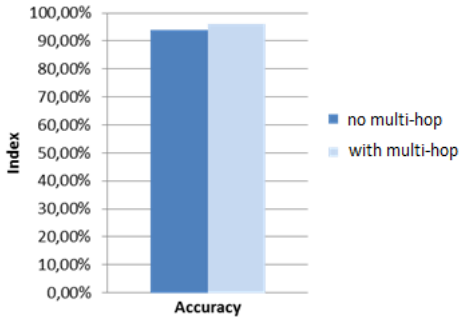

Figure 7. Accuracy of the Proposed Algorithm on RH2 Packets

Two trials (with 31 observations each) are conducted to verify the significance of the experimental results. The Mean and Standard Deviation of the first and the second trial are (0.97000; 0.018619) and (0.98500;0.009092), respectively.

The results of the t-test shown in Table 2 present that the proposed algorithm has a significant effect on the effectiveness of packet filtration. It is clearly seen that there is a significant difference in Mean between trial one and two. The t-test result also indicates a high significance for the developed algorithm at (sig = 0.000 < 0.01), i.e. the confidence is greater than 95% [13].

Table 2. t-Test For Results Significance

Trial	Levene's test for equality of variances		t-test of equality of Means					95% confidence interval of the diff.	
	F	Sig.	T	df	Sig. (2-tailed)	Means diff.	Std. Err. Diff.	Lower	Upper
Equal variant assumed	15.528	0.000	-4.031	60	0.000	-0.015	0.003721	-0.022414	-0.007556
Not assumed			-4.031	43.538	0.000	-0.015	0.003721	-0.022502	- 0.007498

4. Conclusion

An algorithm for securing home agent network in a mobile IPv4/IPv6 mixed network from IPv6 routing header vulnerability has been proposed. The proposed algorithm is incorporated into the Home Agent of a NATed IPv4 network. Testbed experimental results show that the proposed algorithm accurately filter malicious packets coming into the NATed IPv4 network without significance delay on filtering process.

This paper focuses only the routing header type 0 and type 2. In future, other vulnerabilities in mixed IP network will be considered with the intention of providing seamless and secure handover process.

References

[1] Ahmadi, SM. Analysis Towards Mobile IPv4 and Mobile IPv6 in Computer Networks. *International Journal of Intelligent Systems and Applications (IJISA)*. 2012; 4(4): 33-51.

[2] Hong, LX. *The Research of Network Transitional Technology from IPv4 to IPv6*. Proceedings of the 4th IEEE International Conference on Digital Manufacturing and Automation (ICDMA). Shandong. 2013: 1507-1509.

[3] Lee, KH., Jung, HK., Lee, HW., Lee, SK., Han, YH. A Network-Based IP Mobility Management Scheme with IPv4/IPv6 Dual Stack Support. In: H-K Jung et. al. *Editors*. *Lecture Notes in Electrical Engineering: Future Information Communication Technology and Applications (ICFICE 2013)*. Berlin:Springer. 2013: 199-216.

[4] Jun Zhang, Hai Zhao, Bo Yang, Si-yuan Jia. Fractals on IPv6 Network Topology. *TELKOMNIKA Indonesian Journal of Electrical Engineering*. 2013; 11(2): 577-582.

[5] Durdağı, E., Buldu, A. IPv4/IPv6 Security and Threat Comparisons. *Procedia-Social and Behavioral Sciences*. 2010; 2(2): 5285-5291.

[6] La Polla, M., Martinelli, F., Sgandurra, D. A Survey on Security for Mobile Devices. *IEEE Communications Surveys & Tutorials*. 2013; 15(1): 446 - 471.

[7] Zagar, D., Grgic, K., Rimac-Drlje, S. Security Aspects in IPv6 Networks-Implementation and Testing. *Computers & Electrical Engineering*. 2007; 33(5-6): 425-437.

[8] Al-Tamimi, BN., Budiarto, R., Omar, MA., Alhendawi, MK. Exploiting IPv6 Routing Headers Type 0/2 in Different IP Wireless Networks: Attack Scenario & Analysis. *Journal of Theoretical and Applied Information Technology*. 2014; 59(2): 372-378.

[9] Karthikeyan, V., Prittopaul.P. A Survey on Vulnerability of Type 0 Routing Header in IPv6. *International Journal of Computer Science and Management Research*. 2013; 2(2): 1671-1676.

[10] Wadhwa, M., Khari, M. Security Holes in Contrast to the New Features Emerging in the Next Generation Protocol. *International Journal of Computer Applications*. 2011; 20(3): 35-39.

[11] Dac-Nhuong Le. DDoS Attack Defense in Next Generation Networks using Private Security Policy. *International Journal of Information and Networks Security (IJINS)*. 2014; 3(3): DOI:10.11591/ijins.v3i3.6340.

[12] Field, A. *Discovering Statistics Using SPSS*. Third Edition. London: Sage Publications. 2009.

[13] Hair, JF., Black, WC., Babin, BJ., Anderson, RE. Multivariate Data Analysis: A Global Perspective. Seventh Edition. New Jersey: Pearson Prentice Hall. 2010.