International Journal of Security and Its Applications
Vol.9, No.11 (2015), pp.77-86
http://dx.doi.org/10.14257/ijsia.2015.9.11.08

Integrated Framework to Detect and Mitigate Denial of Service (DoS) Attacks on Duplicate Address Detection Process in IPv6 Link Local Communication

Shafiq Ul Rehman[1] and Selvakumar Manickam[1]

[*]*National Advanced IPv6 Centre (NAv6), Universiti Sains Malaysia*
shafiq@nav6.usm.my,
selva@usm.my

Abstract

In addition to addressing the scarcity of IP address space, Internet Protocol version 6 (IPv6) also addressed some of the shortcomings of Internet Protocol version 4(IPv4). These include neighbor discovery, address auto-configuration, and others. Many of this message exchange are done via the Internet Control Message Protocol (ICMP) and the use of this protocol in the IPv6 paradigm, i.e. ICMPv6 plays a bigger role compared to ICMPv4. One of the key process that is carried during neighbor discovery process is to check if the address generated already exists. This process is called the Duplicate Address Detection (DAD). Nevertheless, the design of this process has led to a severe security vulnerability allowing attackers to easily carry out Denial-of-Service (DoS) attack by causing every address generated to be a duplicate leading to new hosts unable to join the network. Various techniques and mechanisms have been introduced to address this vulnerability such as NDPMon, SeND, and SAVA. Nevertheless, these techniques are either not robust or have performance implications vis-à-vis with the DAD DoS detection and mitigation. In this paper, we put forward a novel framework that is able to detect, mitigate DoS attacks while being light-weight at the same time.

Keywords*: DoS, Intrusion Detection, Intrusion Prevention, IPv6 Security, DAD, Neighbor Discovery, Address autoconfiguration*

1. Introduction

IPv6 [1, 2] protocol provides many benefits apart from larger address space than its predecessor protocol IPv4 [3]. One of them is address auto-configuration [4] mechanism. This feature allows IPv6 compatible devices to configure IP addresses automatically without any intervention from service providers such as; DHCP server. However, generated IP address has to be unique in order to prevent the conflict of IP addresses among hosts in IPv6 link local communication. Therefore, there is a mechanism known as Duplicate Address Detection (DAD) [5] process to verify the uniqueness of self-generated IP address. In IPv6 network every host has to perform DAD process in order to obtain a unique valid IP address.

During neighbor discovery [6], IPv6 hosts use ICMPv6 [7] message types to communicate with each other. Such as; hosts use neighbor solicitation (NS) message to send a query to neighboring hosts on the same link and in response hosts send neighbor advertisement (NA) message. While performing DAD process, hosts send NS message to verify whether the self-generated IP address is already used by any existing host or not. If any existing host has already configured that IP address replies back with NA message that IP address is already in use.

Hence, new host generates a new IP address and perform the DAD process again. For instance, when a New-Host joins the IPv6 local network it generates fe80:1234::a as link

ISSN: 1738-9976 IJSIA

local address to make sure the generated IP address is unique it sends NS message to existing hosts on the same link. Here, Host-A has already configured the same IP addresses. Thus, it sends the reply via NA message that generated IP already in use. Hence, New-Host generates a new link local IP address such as; fe80:1234::d and performs the same DAD process again in order to verify its uniqueness. Since, there is no response from the neighboring hosts for its existence. Therefore, New-Host considers that generated IP address is unique and can configure it as a preferred IP address. Figure 1 depicts the Duplicate Address Detection process.

Figure 1. Duplicate Address Detection Process

In IPv6 link local communication, during neighbor discovery hosts are considered trustworthy therefore relies on the information being shared. However, any malicious host can take advantage of this phenomenon. Therefore, once joining the IPv6 local link an intruder can exploit the DAD process by disrupting the communication between hosts. Studies [8-10] have shown that DAD process is vulnerable to denial of Service attacks. During DoS on DAD attack, an attacker attempts that the victim host is unable to obtain a valid IP address by claiming the existence of self-generated IP address via sending fake NA messages in reply to its NS messages.

Hence, victim host is unable to verify the uniqueness of self-generated IP address. Thus, cannot obtain a valid IP address due to DAD process failure. For example, while host performs DAD process in order to verify the uniqueness of self-generated IP address such as; fe80:1234::c it sends NS message to existing hosts. In this case, an Attacker responds back by claiming the generated IP address via fake NA message. During DAD process, New-Host generates an IP address such as; fe80:1234::d and sends NS message to existing hosts for verification purpose, again an Attacker claims the IP address via NA message. Therefore, New-Host is unable to configure its tentative IP address due to DAD process failure. Thus, New-Host would be unable to configure valid unique IPv6 link local address. Figure 2 illustrates the DoS on DAD attack.

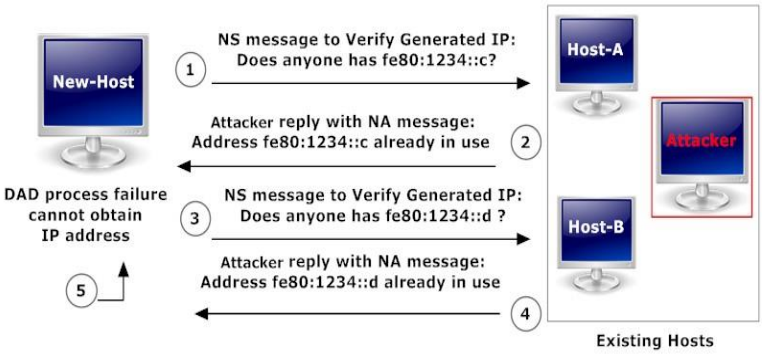

Figure 2. DoS Attack During DAD Process

2. Related Works

In order to address the security issue in DAD process as discussed in Section I. Over the years, a number of security mechanisms have been proposed to secure neighbor discovery in IPv6 link local communication. With different approaches being proposed to deal with the security threats in IPv6 LLC. Generally, these existing schemes can be categorized into detection and mitigation mechanisms, respectively. In this paper, we have mentioned some of these existing mechanisms as follows:

2.1 Existing Detection Mechanisms

Some of the existing detection mechanisms for neighbor discovery in IPv6 LLC are; Neighbor Discovery Protocol monitor (NDPmon) [11], was proposed to deploy and configure on IPv6 link local network, in order to detect the anomalies during hosts neighbor discovery in IPv6 LLC. This mechanism detects the anomalies based on behavioral changes in the hosts (IP and MAC addresses). However, the drawback with behavior based detection mechanism is that if genuine changes takes places in the network it still considers them anomalies [12]. Since, this mechanism is unable to distinguish between the normal and abnormal traffic changes in IPv6 network. Therefore, NDPmon is not an ideal option for address autoconfiguration due to its dynamic nature. Neighbor Discovery- Shield [13], was proposed to filter ND messages containing malicious information during neighbor discovery in IPv6 LLC. However, the study [14] has shown that the ND- Shield is vulnerable to Denial of service (DoS) and fragmentation attacks during neighbor discovery in IPv6 LLC.

In recent attempts, an Active detection mechanism [12] was proposed to detect the attacks against NDP Protocol. This proposed mechanism is probing based (IDS). In order to perform intrusion detection it sends probes or verification messages upon receiving NS and NA messages to confirm their uniqueness. The developers of the proposed mechanism claim that proposed mechanism is easy to deploy and compatible with the standard NDP protocol. In addition to that, it claimed to be interoperable with major Operating Systems. Nevertheless, due to its probing nature increases CPU utilization and require larger bandwidth [12]. Thus, can raise the complexity issues during DAD process in IPv6 LLC.

2.2 Existing Mitigation Mechanisms

Some of the existing mitigation mechanisms for neighbor discovery in IPv6 LLC are; Secure Neighbor Discovery Protocol (SeND) [15, 16], was proposed to address the security concerns with the NDP. Although SeND mitigates major security vulnerabilities such as: address spoofing, replay attack *etc*. against NDP in IPv6 LLC. However, studies [14, 17] have proven that SeND lacks confidentiality and source address validation. In addition, due to its complex mechanism, it increases higher complexity while address configuration in IPv6 LLC. Source Address Validation Architecture (SAVA) [18] mechanism, was proposed to validate the source address so that to counter the spoofing attacks. However, the study [14] has shown that SAVA is unable to prevent DoS attacks during DAD process. Also, Windows Secure Neighbor Discovery (WinSeND) [13] was proposed to implement the SeND mechanism on Windows platform, in order to secure the hosts address auto-configuration in IPv6 LLC. WinSeND is application software based mechanism developed in Microsoft.Net. WinSeND has same security issue like SeND mechanism. Apart from being platform dependent, it also requires regular patching [12]. Thus, due to these limitations WinSeND mechanism is not appropriate for securing DAD process in IPv6 LLC.

Meantime, other mechanisms were proposed by the researchers to enhance the DAD process in IPv6 LLC such as; Optimistic Duplicate Address detection (DAD) RFC 4429 [5] attempts to reduce delay and disruptions in DAD process during address auto-

configuration in IPv6 LLC. However, it does not mitigate DoS attacks on DAD process during address auto-configuration. Later, Pull Model [19] was proposed to improve and secure the DAD process during address auto-configuration in IPv6 LLC. Although, it claims enhancement and flexibility in DAD process during address auto-configuration. However, the study [19] has also shown that it is susceptible to brute force and inverting attacks. Recently, Enhanced Duplicate Address Detection RFC 7527 [20] was proposed to enhance the DAD algorithm; in order to detect and mitigate the loop backed message issue in DAD process during address auto-configuration in IPv6 LLC. However, the mechanism does not improve the security posture of DAD process, for example; it does not mitigate a DoS attack on DAD process in IPv6 LLC.

Thus, from the existing mechanisms it is clear that there have been attempts to enhance the security mechanism in IPv6 LLC. However, studies have also proven that there is no such mechanism which can detect and mitigate the DoS attack on DAD process during address auto-configuration in IPv6 LLC. Even though, some schemes claim to improve the security in DAD mechanism while others enhancing DAD algorithm itself. However, these mechanisms are either complex, platform specific or vulnerable to DoS attacks. Currently, there is no suitable mechanism which can address the issue of DoS attacks on DAD process. Therefore, an integrated mechanism is required to detect as well as mitigate the Denial of service attack on duplicate address detection in IPv6 link local communication.

3. Proposed Scheme

Integrated Framework has been proposed to detect and mitigate the Denial of Service (DoS) attacks on duplicate address detection process in IPv6 Link Local Communication. Beginning with assumptions, this section describes the architecture of the proposed Framework, and the mechanisms to detect and mitigate the DoS attacks while performing DAD process in IPv6 LLC.

3.1 Assumptions

Proposed Framework relies on the assumptions mentioned as under:

1. All joining hosts are enabled IPv6 address auto-configuration mechanism.
2. The Access router has static IPv6 address configured to provide a network prefix required by the hosts in order to perform address auto-configuration on the local link.
3. The Integrated Framework machine is a trusted machine and has static IPv6 address configured.
4. Integrated Framework machine obtains the information of all existing hosts on IPv6 local link including the Access router.

3.2 Design of Integrated Framework

In order to design an Integrated Framework, a rule based system [21, 22] has been employed to detect and mitigate the denial of service attack on DAD process during address auto-configuration in IPv6 link local communication. Rule-based mechanism has been applied in a manner to store and update the existing hosts IP addresses in order to interpret the information in an efficient way. They are often utilized in artificial intelligence based applications and research. To control the decision making in address auto-configuration is a challenging task due to its dynamic nature. Therefore, the concept of Rule-Based system has been applied to deal with this issue during address auto-configuration in IPv6 link local communication.

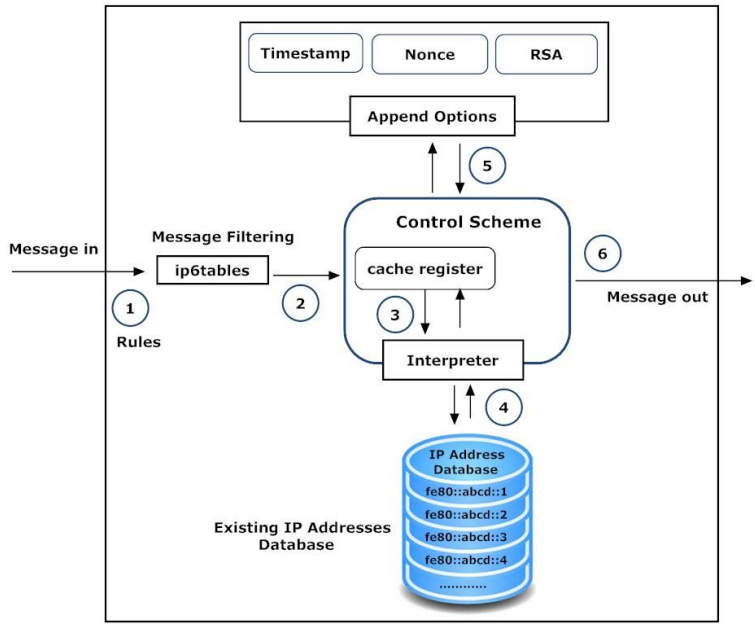

Figure 3. Architecture of an Integrated Framework

3.3 Elements of Proposed Framework

The Proposed Framework has four main elements such as; ip6tables [23], Control Scheme, IP address database and Append options. As shown in Figure 3.

1. *ip6tables* are used to manage the traffic flow, ip6tables rules have been applied to filter out the incoming messages in the framework it acts like a firewall. For example, if the incoming message is NS / NA messages, then allow the message otherwise, discard the message in order to restrain the undesirable incoming traffic.
2. *Control Scheme* is the main element of the framework, it performs the verification operation and mitigation process of the IP address. It has two sub components; *cache registry* and *interpreter*. *Cache registry* is the temporary repository for the incoming message, and the *interpreter* does the operations of matching the incoming IP address with the existing address database. If the match of the IP is detected, then it generates a message "duplicate IP found"or if no matching occurs it replies with "unique IP found".
3. *IP Address Database* is the repository of IP addresses, which are already configured by the existing hosts on the same link. Once the duplicate address detection, verification of new host IP address is done; it is stored in the existing database in order to keep the records updated.
4. *Append Options* are security options such as; *Timestamp, Nonce, and RSA*, which can be used to prevent an intruder to disrupt the communication between existing hosts in IPv6 LLC. Study [24] has shown that options like *Timestamp,* can be used to protect the attacks like replay attack, DoS attack, and DAD attack. *Nonce* option, can be used to secure solicited advertisement and *RSA* signature option, can be used to authenticate the hosts. Thus, after these options are appended to the message can ensure secure information exchange between hosts in IPv6 link local network.

3.4 Proposed Framework Scheme

In order to describe the mechanism of the proposed framework, a scenario has been presented where a host wants to join the IPv6 local network and generates a tentative IP address. After address generation, DAD Process has to be performed in order to verify its

uniqueness on the same link. The proposed scheme ensures DAD process is being performed without any disruption from the intruders. Thus, a host can obtain the preferred IP address and can communicate with neighboring hosts on the same link. Moreover, proposed scheme determines a secure link local communication in IPv6 local network. The entire process is explained as follows:

1. The Host sends NS message to solicit node multicast address (SNMA) group, to verify the uniqueness of its generated tentative IP address. All existing Hosts including the proposed framework scheme (PFS) on the same link receives the NS message. Upon receiving the NS message, PFS filter the incoming messages in order to manage the traffic flow. For instance, if the incoming message is NS/NA message, then it entertains the message else message is being discarded.
2. While Host performs DAD process, proposed framework scheme (PFS) verifies the generated IP address for its uniqueness. The control scheme of the PFS matches the generated IP with the existing IP address database, which is the repository of the IP addresses of existing Hosts on the local link. If no matching of IP address is found, it consider that generated IP address is unique on the local link. Since, it is a unique IP address security options such as; Timestamp, Nonce, and RSA are added to the NA message to ensure secure link local communication. Afterwards, PFS sends reply to the Host with NA message "Unique IP found". Moreover, the information is being stored in an existing IP address database in order to maintain and update the IP address database. Since, the PFS has verified the generated tentative IP address is unique on the same link. Thus, a host can use it as a preferred IP address.
3. However, if a match of generated IP address is found in the existing IP address database; PFS replies with the NA message "Duplicate IP address detected". As duplicate address detection has been confirmed on local link. Thus, the Host can generate a new tentative IP address and proceed with a new DAD process. Therefore, the Host can determine whether the generated IP address is unique or duplicate on the same link.
4. In case of the DoS attack attempt on DAD process, a Host can receive fake NA replies from an attacker which can disrupt its communication with neighboring hosts as already mentioned in section I. Thus, it can cause DAD process failure, which leads to no address generation. In order to counter such DoS attack, our proposed framework scheme (PFS) assures that Host accepts only the verified NA replies from the PFS machine while ignore other NA reply messages which are not verified or certified by the PFS machine itself. Hence, the Host can complete DAD process and obtain its preferred IP address. Since, PFS machine is trusted machine on the local link and contains all information about existing host on the local network. Thus, can detect any attempt of DoS on DAD process in IPv6 LLC.
5. In order to mitigate the DoS attack attempts on DAD process, PFS ascertains that every existing host on the local link exchanges its information with PFS periodically; in order to maintain and update the existing IP address database. Thus, PFS can make sure that intruders are unable to disrupt the communication during DAD process.

Thus, our proposed framework scheme can ensure secure link local communication in IPv6 link local network. Figure 4 describes the process of proposed framework scheme (PFS).

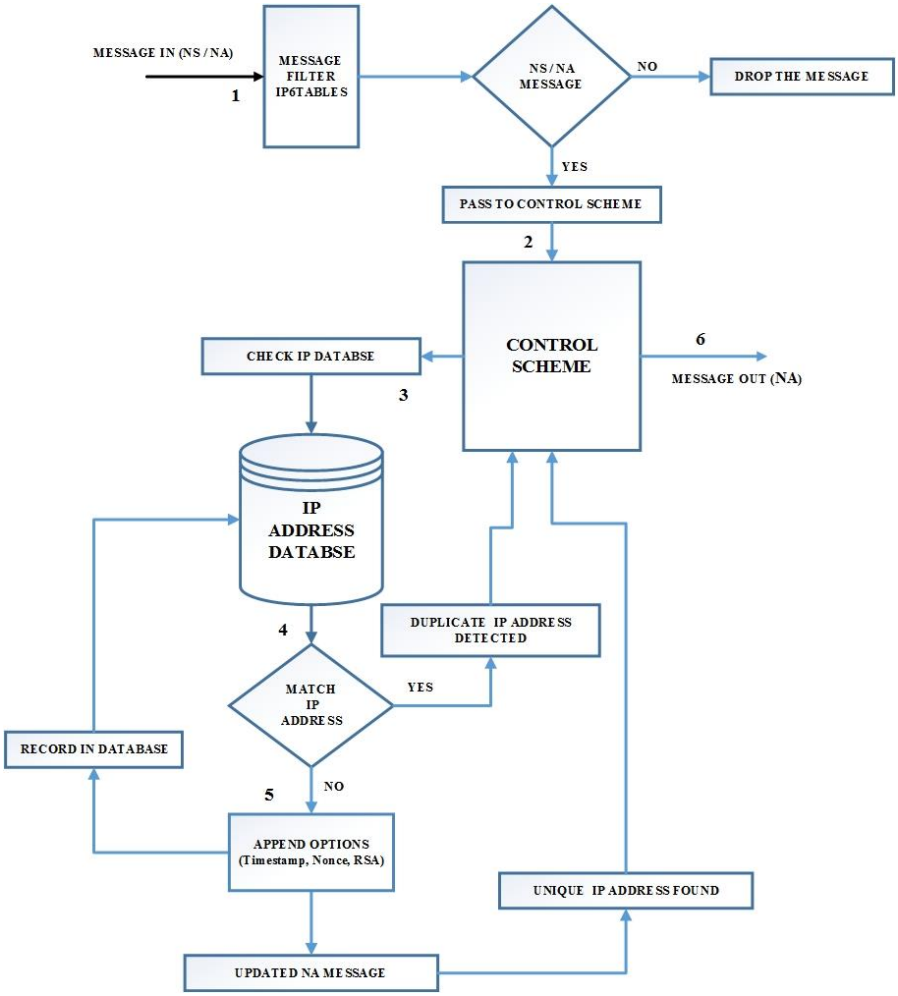

Figure 4. Proposed Framework Scheme

5. Conclusion and Future Work

In this paper, an Integrated Framework to detect and mitigate denial of service (DoS) attacks on duplicate address detection process in IPv6 link local communication has been proposed. The proposed scheme uses rules based mechanism to verify the uniqueness of self-generated IP address. While matching its existing with IP address database, to detect and mitigate the DoS attacks against DAD process during address auto-configuration in IPv6 local network. Moreover, it uses a simple approach as the operational rules are normal queries to verify the existence of generated IP address. Also, it does not require any modification in Neighbor Discovery process and being a centralize based scheme which is easy to manage. Thus, with these features the proposed framework scheme can provide a secure and reliable link local communication between hosts in IPv6 local network.

At present, an integrated framework has been proposed. In order to test and validate the proposed scheme, our future work will be to implement the proposed framework in IPv6 link local environment at the National Advanced IPv6 Centre (NAV6) research institute. Thus,can ensure a secure address autoconfiguration and reliable link local communication in IPv6 network.

Acknowledgments

This research was supported by the Ministry of Higher Education Malaysia, in collaboration with the National Advanced IPv6 Centre, Universiti Sains Malaysia.

References

[1] S. Hagen, "IPv6 Essentials, O'Reilly: Second Edition", **(2006)**.
[2] S. E. Deering, "Internet protocol version 6 (IPv6) specification", **(1998)**.
[3] E. Durdağı, and A. Buldu, "IPV4/IPV6 security and threat comparisons", "Procedia-Social and Behavioral Sciences", vol. 2, no.2, **(2010)**, pp. 5285-5291.
[4] S. Thomson, "IPv6 stateless Address Autoconfiguration", **(1998)**.
[5] N. Moore,"Optimistic duplicate address detection (DAD) for IPv6", **(2006)**.
[6] T. Narten, W.A. Simpson, E. Nordmark, and H. Soliman,"Neighbor discovery for IP version 6 (IPv6)", **(2007)**.
[7] A. Conta, and M. Gupta, "Internet control message protocol (icmpv6) for the internet protocol version 6 (ipv6) specification", **(2006)**.
[8] X.Yang, T. Ma, and Y. Shi,"Typical dos/ddos threats under ipv6 ",IEEE, **(2007)**, pp. 55-55.
[9] Supriyanto, I. H. Hasbullah, R. K. Murugesan, and S. Ramadass, "Survey of Internet Protocol Version 6 Link Local Communication Security Vulnerability and Mitigation Methods", IETE Technical Review, vol. 30, no. 1, **(2013)**, pp. 64-71.
[10] A. AlSa'deh, H. Rafiee, and C. Meinel, "IPv6 Stateless Address Autoconfiguration: Balancing Between Security, Privacy and Usability", Foundations and Practice of Security, Springer, **(2013)**, pp. 149-161.
[11] F**.** Beck, T. Cholez, O. Festor, and I. Chrisment, "Monitoring the Neighbor Discovery Protocol", Monitoring the Neighbor Discovery Protocol **(2007)**.
[12] F. A. Barbhuiya, G. Bansal, N. Kumar, S. Biswas, and S. Nandi, "Detection of Neighbor Discovery Protocol Based Attacks in IPv6 network", Networking Science, vol. 2, no. 3-4, **(2013)**, pp. 91-113.
[13] H. Rafiee, A. Alsa'deh, and C. Meinel, " Winsend: Windows Secure Neighbor Discovery", ACM, **(2011)**, pp. 243-246.
[14] R. K. Murugesan, and S. Ramadass, "REVIEW ON IPV6 SECURITY VULNERABILITY ISSUES AND MITIGATION METHODS", International Journal of Network Security & Its Applications, vol. 4, no. 6 **(2012)**.
[15] R. K. Murugesan, and S. Ramadass, "REVIEW ON IPV6 SECURITY VULNERABILITY ISSUES AND MITIGATION METHODS", International Journal of Network Security & Its Applications, vol. 4, no. 6 **(2012)**.
[16] S. Chiu, and E. Gamess, "Easy-SEND: A Didactic Implementation of the Secure Neighbor Discovery Protocol for IPv6", **(2009)**.
[17] A. AlSa'deh, and C. Meinel, "Secure neighbor discovery: Review, challenges, perspectives, and recommendations", Security & Privacy, IEEE, vol.10, no. 4, **(2012)**, pp. 26-34.
[18] J. Wu, G. Ren, and X. Li, "Source address validation: Architecture and protocol design", IEEE, **(2007)**, pp. 276-283.
[19] G. Yao, J. Bi, S. Wang, Y. Zhang, and Y. Li, "A pull model IPv6 Duplicate Address Detection", IEEE, **(2010)**, pp. 372-375.
[20] W. George, and T.W. Cable, "Enhanced Duplicate Address Detection", **(2015)**.
[21] B.G. Buchanan, and E.H Shortliffe, "Rule-based expert systems", Addison-Wesley Reading, MA, **(1984)**.
[22] J.A. Bernard, "Use of a rule-based system for process control", International Society for Optics and Photonics, **(1987)**, pp. 835-849.
[23] R. Kabila, "Network Based Intrusion Detection and Prevention Systems in IP-Level Security Protocols", network security, vol.7, **(2008)**, pp. 11.
[24] M.S.Chavan, M.P. Mandge, M.S. Ghogare, and M.M. Pavaskar, "Implemantation Of Securing Ipv6 Infrastructure Using CGA, RSA, Timestamp And Nonce", vol.2, no.5, **(2013)**, pp.608-620.

Authors

Shafiq Ul Rehman, he has B.Sc. degree in Computer Science and has received his M.Sc. degree in Network Technology & Management from Amity University (India) in 2012. He has worked on various research projects related to Network Security and Internet Technologies. Currently, he is a PhD research fellow in National Advanced IPv6 Centre (NAV6), Universiti

Sains Malaysia (USM). His research interest includes Networking, IPv6, Security, Open Source Technology, Ubiquitous Computing and Cloud Computing.

Selvakumar Manickam, he is the senior lecturer at National Advanced IPv6 Centre (NAv6), Universiti Sains Malaysia. He received his Bachelor of Computer Science and Master of Computer Science in 1999 and 2002, respectively. He obtained his Ph.D. from Universiti Sains Malaysia (USM) in 2013. His research interests are Internet security, cloud computing, Android and open source technology. He is an Executive Council member of Internet Society (ISOC), Malaysian Chapter and also the Head of Internet Security Working Group under Malaysian Research and Education Network (MyREN).