International Journal of Computing and Digital Systems
ISSN (2210-142X)
Int. J. Com. Dig. Sys. 8, No.2 (Mar-2019)
http://dx.doi.org/10.12785/ijcds/080209

# Lightweight Secure Router Discovery Mechanism To Overcome DOS Attack In IPv6 Network

**Navaneethan C. Arjuman [1], Selvakumar Manickam [2], Shankar Karuppayah [3] and Balasubramanian Nathan [4]**

[1234]*National Advanced IPv6 Centre (NAv6), Universiti Sains Malaysia, Penang, Malaysia*

*Received 9 Nov. 2018, Revised 20 Dec. 2018, Accepted 29 Dec. 2018, Published 1 Mar. 2019*

**Abstract:** Router Discovery (RD) which is the core component of Neighbour Discovery Protocols (NDP) plays key role in the IPv6 address assignment in the IPv6 network. Weakness in the standard Router Discovery protocol leads to several attacks in the IPv6 network. More and more attacks are initiated within network due to the existing vulnerabilities. Even though there are several detection, mitigation and prevention mechanism are already available but these mechanisms itself have issues such as highly complex, high cost and faces several other issues within the design itself. This paper proposed an improved Secure Router Discovery prevention mechanism that is lightweight, integrated and self-regulated that will overcome the issues with the existing prevention techniques. The primary focus of this paper would be discussion on the assumptions, threat model and design goals of the proposed mechanism. It also explains the proposed architecture, components of the building blocks of the architecture and the operation of this lightweight mechanism.

**Keywords:** Router Discovery Vulnerabilities, Router Solicitation, Router Advertisement, Router Discovery Attacks, Secure Router Discovery Prevention Mechanism.

## 1. INTRODUCTION

In the IPv6 network, ICMPv6 message are used to assign the IPv6 address unlike in IPv4 network [1]. The IPv6 address assignment categorised either as stateful or stateless [2]. In Stateless Address Auto configuration (SLAAC), Neighbour Discovery Protocol (NDP) plays a pivotal role in the address assignment [3].

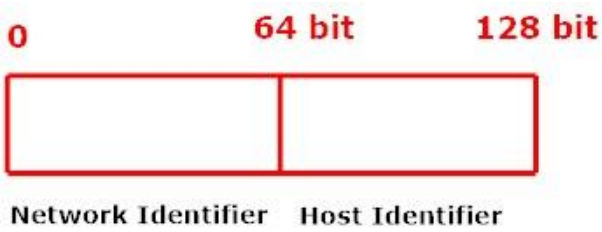



Figure 1. 128 Bit IPv6 Address

NDP protocol in IPv6 consist of five Internet Control Message Protocol Version 6 (ICMPv6) messages types that are Router Solicitation (RA), Router Advertisement (RA), Neighbour Solicitation (NS), Neighbour Advertisement (NA) and Router Redirect [4]. ICMPv6 Router Discovery consists of RS and RA [2,7].

In Figure 1, the host obtained the lower 64 bits of IPv6 address known as Prefix using Router Discovery and the higher 64 bits address known as host Interface Identifier based on Neighbour Discovery (ND) [2,7].

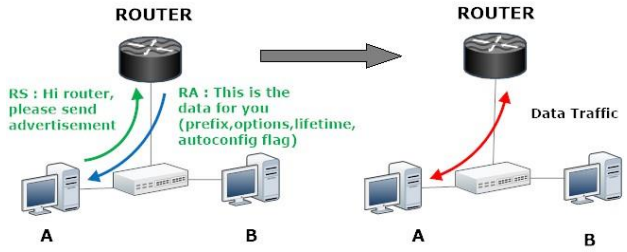



Figure 2. Router Discovery Process

Refer the above Figure 2, in the standard design process, a new host will send RS to all the active routers on the link and all the routers will reply with RA together with information such as prefix, options, lifetime and autoconfiguration flag [5,7]. The host will the select the gateway router based on highest priority and nearest next hop [7].

*E-mail: nava@nav6.usm.my , selva@usm.my, kshankar@usm.my, balasubramanian@nav6.usm.my*

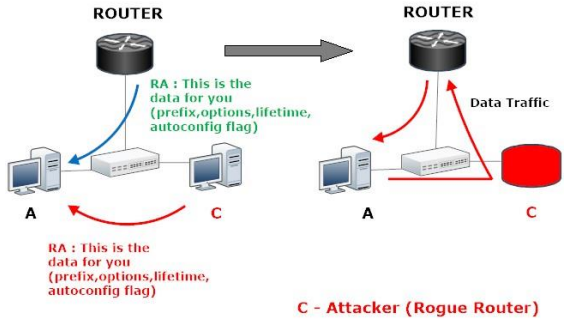



Figure 3 . Router Discovery Process Vulnerabilities

In the IPv6 network, the existing legitimate node can turn to be become rogue router and the rogue router who is the attacker can compromise the existing legitimate router [6]. By sending the lifetime equal to zero, the legitimate would be no longer available [8,9] and the rogue router will send its configuration to the existing host to be configured as new gateway. So, all the future communication will go through via attacker's gateway.

In standard design operation, there is no mechanism to verify the legitimate router [8] and this vulnerability will lead to several attacks such as Denial of Service (DOS) attack, Man In Middle Attack and Flooding Attack.

There are several detection, mitigation and prevention techniques already available to overcome these issues. But this research would only focus on prevention techniques only. Even though these existing techniques able to overcome the above-mentioned security vulnerabilities but these techniques face issues such as highly complex, high cost and faces other vulnerabilities that will be discussed in the following section. This paper is focused on designing a lightweight mechanism for Secure Router Discovery process which is lightweight, integrated and self-regulated.

Section 2 covers summary of related secure RD prevention techniques. Section 3 discusses assumptions, threat model and design goals of the proposed mechanism. Section 4, 5 and 6 respectively explains the proposed architecture, components in each building blocks and the operation of the proposed mechanism. Section 7 provides conclusion and discuss future work

## 2. RELATED WORK

There are several secure Router Discovery prevention techniques have been proposed in the past such as SeND's Authorisation Delegation Discovery [10], Trust Router Discovery Protocol [11], Router Advertisement Guard [12] and Trust Neighbour Discovery (Trust ND) [13]. But these techniques also face several issues as summarized in the following Table 1.

TABLE 1. SUMMARY OF RELATED WORKS ON SECURE ROUTER DISCOVERY

| No | Mechanism | Implementation and security issues in the IPv6 Network |
|---|---|---|
| 1 | SeND's ADD [10] | 1. Lengthy certificate authentication process<br>2. Multiple certificate request can lead to DOS attacks<br>3. The computational cost is very high<br>4. The computation is highly complex<br>5. Increase network overhead and bandwidth consumption |
| 2. | TRDP [11] | 1. More complex because additional ICMPv6 messages required<br>2. Required intermediate router for authentication<br>3. High implementation cost |
| 3. | RA-Guard [12] | 1. Does not able to block RA messages that are communicate directly<br>2. Unable to block RA messages that are channelled through tunnelled traffic<br>3. Only configured and support ingress RA message<br>4. Unable to support on trunks ports with merge mode<br>5. Unable to configure in the network that uses ACL ICMPv6 optimization' |
| 4. | Trust-ND [13] | 1. The SHA-1 hashing algorithm is very vulnerable to high collision attack<br>2. Unreliable Trust Tag value generations<br>3. Complex processing overhead |

Even though the above researchers have proposed the above prevention mechanism to overcome the RD issues, but these techniques do faces problems such as highly complex, high cost and other issues as explained in the above table [14]. So, there is real need to propose an improved mechanism that are lightweight, integrated and self-regulated.

## 3. DRAWBACK OF EXISTING SECURE ROUTER DISCOVERY MECHANISM

The drawbacks of the above-mentioned existing mechanism can be categories into three main causes as follows:

### *A. High complexity and high cost*

The complexity level of any mechanism can be measured by noticing the executions of its operations [21]. If the process is more complex, then more

resources would be required, and the processing time will much longer for the operations. So, the implementation cost also would be very high as well. The cost not only include the resource but the time as well. The study by Praptodiyono [13] shows that the existing mechanism ADD and TRDP have high complexity and high cost since the router verifications required more processing time because of the lengthy router certificate process. So, any malicious router can provide bogus parameters to the host and the certificate process will be continually repeated forever for the router discovery process. Multiple certificate verification also would lead to high volume of traffics in the IPv6 network and eventually lead into DoS attack in the IPv6 link local communication.

### *B. Partial Protection*

Although the existing Trust-ND mechanism able to address the complexity issue by introducing lightweight solution using hashing technique but this hashing technique introduced new vulnerabilities such as hash collision attack [22]. The verification process of the RS and RA message can be exploited by attacker using this attack during the RD process.

### *C. Third party service requirement*

The existing ADD and TRDP required third party services such as Trust Anchor (TA) finally to verify the certificate in the secure RD process. Reliance on third party would increase the length of certification process and eventually lead to DoS attack.

## 4. PROPOSED MECHANISM APPROACH

To fulfill the above design objective, that is to design a secure router discovery mechanism that is lightweight, integrated and self-regulated. This mechanism will be known as SecMac Secure Router Discovery (SecMac-SRD) mechanism. The following sections discuss in detail the assumptions, threat model, design goal and overall architecture of the design.

### *A. Assumptions*

The design of the above mentioned SecMac-SRD mechanisms is based on the following assumptions

1) The IPv6 local network consist of one gateway router, router authentication server, one ethernet switch, a new host, two existing hosts, an attacker and one network monitoring host.
2) All devices in the IPv6 network will obtain IPv6 addressing based SLAAC scheme.
3) Every new host will be installed with SecMac Host Enabler Module.
4) Every router will be installed with SecMac Router Enabler Module.
5) The Network monitoring host to monitor and analyse the RS and RA messages.

The following Figure 4 depicts the setup of test bed environment based on the above-mentioned assumptions.

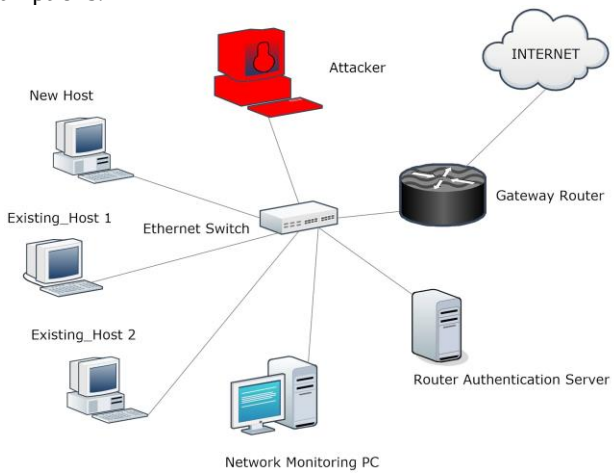



Figure 4. Test Bed Environment

### *B. Threat Model*

Based on the above-mentioned assumptions, the following section discussed the threat model of the test bed environment

1) The attacker will compromise the existing legitimate router by modifying some of the parameters. For an example, the attacker can make lifetime option as zero so that the existing default router no longer valid.
2) Then the rogue router will send fake RA message with its own configuration to the new host.
3) The new host will configure the rogue router as new default router then will deny the services.

### *C. Design Goal*

To fulfill the design goal of the newly proposed secure router mechanism, there are three requirement that needs to be considered that are lightweight, integrated and self-regulated. So, to achieve the above goals, the main goal has been broken to the following sub-goals.

1) In order reduce the high complexity and high cost issue in the secure RD process that discussed in Section 3, a lightweight RD messages verification will fulfill this goal. Since ADD and TRDP has lengthy certification verification process and eventually lead to DoS attacks due to lengthy and multiple certificate requesting. Thus, reducing the complexity on secure RD mechanism means less processing time require for the RD messages verification and avoid DoS attack. The Universal Message Authentication Code (UMAC) hashing technique and Lightweight Router Authentication Server would able to provide lightweight requirement of the new SecMac-

SRD mechanism. UMAC uses only 64 bits message digest compare to SHA-1 which use 160 bits that was used in Trust-ND. Lightweight Router Authentication Server would provide another level lightweight protection for the secure RD.

2) The partial protection drawback in the secure RD mechanism such as Trust-ND could be address by introducing the integrated feature in the newly proposed SecMac-SRD mechanism. This feature would overcome the DoS attack issue related hash collision attacks. The UMAC hashing technique would able to provide integrated requirement of the new SecMac-SRD mechanism. The UMAC hashing algorithm is not susceptible to hashing collision attack.

3) The design goal to overcome the reliance of third party for the certificate verification can be resolved by introducing the self-regulated feature of the newly proposed SecMac-SRD mechanism. The ADD and TRDP must finally rely on third party Trust Anchor to complete the certification verification process. The process will be lengthy and eventually lead to DoS attacks. The self-regulated feature in the newly proposed SecMac-SRD mechanism would cut down the verification process tremendously. The UMAC hashing technique would able to provide self-regulated requirement of the new SecMac-SRD mechanism.

### *D. Contributions*

In the earlier sections, the role of the router discovery process in IP address assignment has been discussed briefly. To overcome issues with router discovery, previously researchers have proposed several security mechanisms. Even though these mechanisms able to address the router discovery issue but due to vulnerabilities in the design of these mechanisms, these mechanisms still faced issues as discussed in Section 2. To overcome the shortcomings of the mechanism, this research has proposed a new mechanism to ensure lightweight secure communications of the router discovery in the IPv6 network. The proposed mechanism would secure the router discovery messages such as Router Solicitation (RS) and Router Advertisement (RA) message from any exploitation and overcome any DoS attack during router discovery process. In order to achieve the above research goal, the IPv6 test-bed has been setup to evaluate the proposed SecMac-SRD mechanism. Following are the contributions of this research work

1. The key contribution of this research would be test-bed development of lightweight secure router discovery (SecMac-SRD) mechanism to prevent the DoS attack during the router discovery process in the IPv6 network.
2. Redesign the RS and RA messages with SecMac Tag options.
3. Design IPv6 test-bed to carry out attack using this new mechanism.
4. The other sub contribution would be Lightweight Router Authentication Server.

## 5. SECURE ROUTER MECHANISM ARCHITECTURE

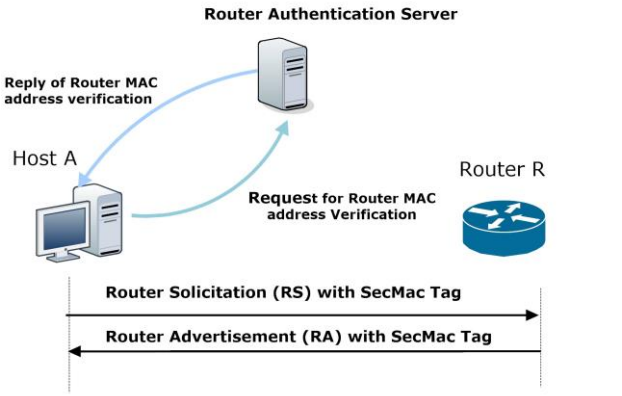



Figure 5 . SecMac Secure Router Discovery Mechanism

To fulfill the requirement of the secure router discovery mechanism that are lightweight, integrated and self-regulated, the SecMac Secure Router Discovery Mechanism has designed to secure the router discovery process in the IPv6 network. The above Figure 5 shows the overall operation how the proposed new secure RD mechanism works.

The following section describes in detail the components of the proposed mechanism, its building blocks and its operation in the respective in building blocks. The following are the key components of the mechanism

1. SecMac Host Enabler
2. SecMac Router Enabler
3. SecMac Router Authentication Server

### *A. SecMac Host Enabler*

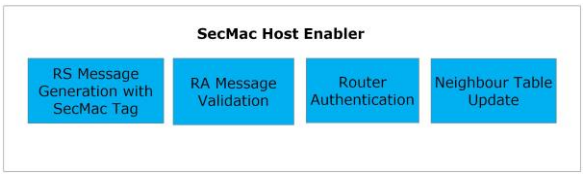



Figure 6. SecMac Host Enabler Structure

The SecMac Host Enabler would be a Rule Based Enabler that is designed to conduct several operations within the host. Rule Based System [19,20] has been used in the artificial intelligent application and research

in the past. It also has been used in detection and mitigation techniques.

The Host Enabler has four key components as depicts in Figure 6 that are RS Message Generation with SecMac Tag, RA Message Validation, Router Authentication, Neighbour Cache Table.

1) RS Message Generation with SecMac Tag is responsible for generating RS Message with the hashed MAC, Nonce and Time Stamp that will be send out to all the routers on link.
2) RA Message Validation is assigned to verify the RA Message that received from the routers whether it is valid RA.
3) Router Authentication module responsible for to verify the Router MAC Address with the Authentication server upon receiving the RA.
4) Neighbour Cache Table is the repository of existing IP addresses currently allocated to the existing host including router on the same link. After the verification of RD process, its information is stored in the existing database to keep records.

### *B. SecMac Router Enabler*

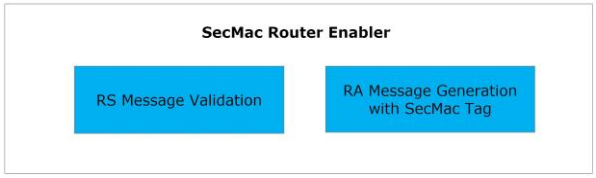



Figure 7. SecMac Router Enabler Structure

The SecMac Router Enabler as depicts in Figure 7 would be Rule Based enabler that is designed to conduct several operations within the router. It will have two key components that is RS Message Validation and RA Message Generation with SecMac Tag.

1) RS Message Validation is assigned to verify the RS Message that received from the host whether it is a valid RS.
2) RA Message Generation will be attached the hashed MAC, Time Stamp and Nonce that will be attached as RA options in the RA messages.

### *C. SecMac Router Authentication Server*

The SecMac Router Authentication Server would maintain the simple database of the valid routers on the link. All the update to the server will be done by the network administrator manually. Upon completion of the hashing extraction process, the host will send a request to the router to verify the newly received router is a valid router. It will reply YES to host when the router is a valid router. It will reply NO when there no entry in the database. Then the host will drop the router entry in the Neighbour Cache Table

## 6. MESSAGE AUTHENTICATION MODEL

To secure the RS and RA message exchange between the host and router in IPv6 local network, the use of message authentication is recommended to authenticate the message content. The integrity of the NDP message exchange will be maintain in this process. This is the key purpose of the proposed mechanism. This will protect the RS and RA messages from several types of attacks such as; masquerade, content modification sequence modification and timing modification which are the main causes of launching a DoS attack.

Hashing usually used for checking performance improvement, error checking, authentication, and encryption [15]. Study [16] has shown that hash function is more suitable mechanism to authenticate NDP messages compare to the encryption mechanism because it does less computation. Studies [16,17] suggested that Universal Hashing approach can be used to authenticate messages and do search operation etc on contemporary machines. Furthermore, the study [17] shows that UMAC is the faster compare to the current practice of hashing function HMAC-SHA1 [18], as a practical algorithm. For example, the UMAC able to achieves peak performance of 5.6 Gbits/sec (0.51 cycles/byte) as compared to SHA-1 implementation runs at 12.6 cycles/byte [14,17].

Study [17] also shows that when UMAC is implemented in the parallelizable scenario will have even faster implementation speed. This will provide faster integrity checks for the RS and RA message communication. Besides the integrity checks to avoid multiple request and reply scenarios, filtering mechanism can be applied for the receiving messages. Since the RD messages are in the form of request and response scenario, so the using sequence number or nonce will make sure that the reply of every messages are based on corresponding solicitation only. Also, to limit the receiving responses, there is need to store message generation time (Timestamp) of the sender as well. This predefined time can used to prevent the DOS attack during RD process. So, the new authentication model using SecMac Tag would have hashed MAC value with message generation time (Timestamp) and nonce as shown in Figure 8 below.

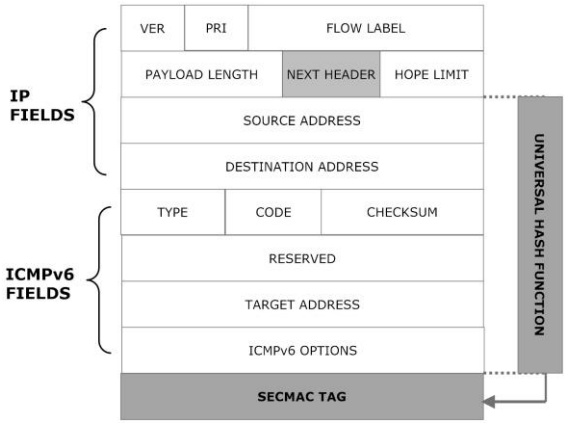



Figure 8. Message Authentication Model

### A. SecMac Tag

In the default Router Discovery operation, it was assumed all the routers are considered trustworthy. Since there are more and more insider DOS attacks are taking place, so the insider nodes whom are initial trusted then later can turn to be a bad router and will launch DOS attacks in the IPv6 network. So, to differentiate a legitimate router, there are real needs to apply a security mechanism during the RD process.

The RS and RA messages can be redesigned to add the ICMPv6 Options with "SecMac Tag". So, the host and routers that has this option only will be allowed to communicate in the IPv6 network. "SecMac Tag" is options that consist of message authentication algorithm to differentiate the valid messages from the bogus ones. Any new host will send the RS messages with "SecMac Tag" and the valid router with reply with RA with "SecMac Tag". If the secure tag is matched, then the host will consider the router as the default gateway. But the host will only configure the default gateway upon router verification from the Router Authentication Server for the initial stage. The following communications do not require the server authentication. If there are RA messages received without SecMac Tag or there any changes in SecMac Tag, then the host will drop the RA messages. The RS and RA SecMac Tag generation and matching process is shown in Figure 9 and Figure 10.

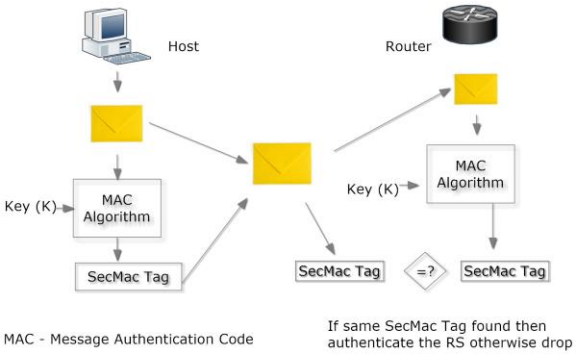



Figure 9. RS SecMac Tag Validation Process

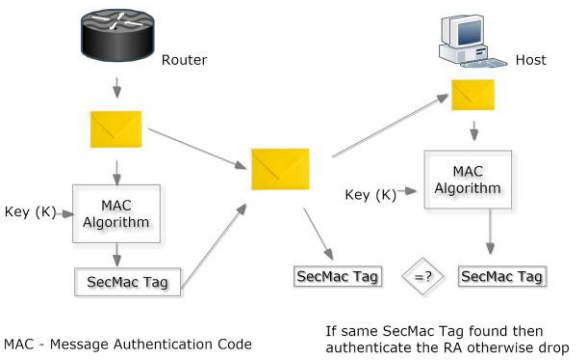



Figure 10. RA SecMac Tag Validation Process

### B. SecMac Tag Format

To ensure the secure router discovery process, the host will only except the valid RA messages that appended with "SecMac Tag". As specified in the Message Authentication Model, the new security would have at least three components such as message authentication code, nonce and timestamp. Upon assigning the "SecMac Tag", the respective RS and RA messages would know as SecMac-RS and SecMac-RA. Figure 11 shows fields in the newly proposed SecMac Tag.

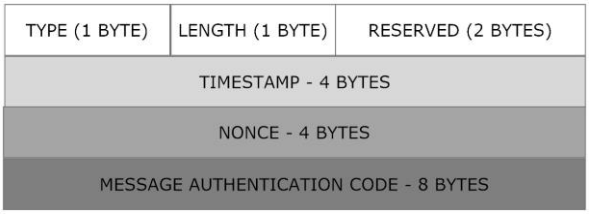



Figure 11. SecMac Tag Format

The format of the *SecMac Tag* option as shown in Figure 11 follows the option format of RFC 4861 [4]; all NDP options should include type and length. The length of NDP option should be minimum 8 bytes (64 bit); otherwise the option must be padded. Further, the secure tag consists of 20 bytes size divided into six fields as follows:

Type : 1 byte size identifier that indicates the option type carrying by the NDP message. The SecMac Tag type defined is 253 since this option is under experimentation.

Length : 1 byte field to indicate the total length of the SecMac Tag option including the type and length fields in unit of 8 bytes. The total length of the SecMac tag option is 20 bytes and thus the value of the Length field is 3 bytes.

Reserved : 2 bytes unused field that is purported for future improvement of the SecMac Tag. RFC 4861 mandates the minimum NDP option is 64 bits and its length is multiple 8 bytes. Thus, reserved field is padded to meet the minimum size of NDP options.

Timestamp : 4 bytes size is the message generation time that indicates when the NDP messages with secure tag are generated by the sender. This field contains the hex format of the date time format, including: hour, min, second and millisecond.

Nonce : 4 bytes field that is intended to provide uniqueness of RS/RA messages on IPv6 RD process to prevent replay attack. This field contains a random number generated by sender of solicitation message or unsolicited advertisement.

MAC : 8 bytes size is the message authentication data as the output of the universal hash function operation used for hashing of sender information. This field is the main field of the SecMac Tag Options of providing the key information to the receiver. This will examine whether the message contains any alteration.

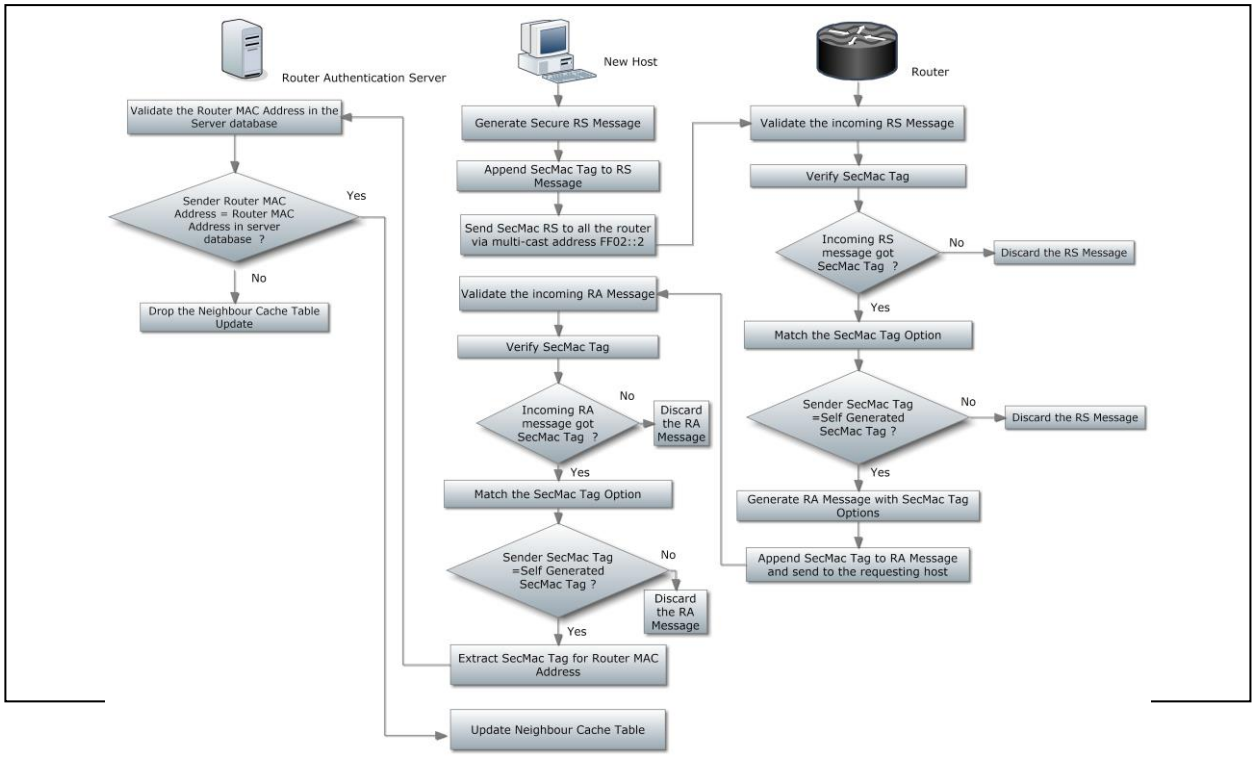
## 7. SECURE ROUTER DISCOVERY MECHANISM PROCESS FLOW

Figure 12 shows that the new host will send the redesigned RS message with SecMac Tag to all the routers in the network and the valid routers will reply with redesigned RA message with SecMac Tag. If the SecMac tag matched, then requesting host will extract the Router MAC Address and verify with the Router Authentication Server. If the extracted new router is valid then the Neighbour Cache Table will be updated with this valid router. The host will use this router as the default gateway.

The proposed mechanism provides protection against fake RA messages that can lead to DOS attack in the IPv6 network. Once the host accepted the configure the fake RA message and the attacker can deny legitimate service to the host which lead into DOS attacks. In the proposed SecMac mechanism, the standard RS and RA messages will be redesigned by appending the SecMac Tag options. The SecMac tag options will provide integrity checking on the router whether it is legitimate router or rogue router. If it is a rogue router then this mechanism would not allow the rogue router to be configured as default gateway,

This section provides details description how the SecMac Secure Router Discovery functions works.

1. The new host will generate redesigned RS Message with SecMac Tag. The SecMac options consist of Timestamp, Nonce and MAC
2. The new host will send out the redesigned RS message to all the router on the link via multicast address FF02::2.
3. Upon receiving the SecMac RS Message, the router will validate whether the RS message got valid SecMac Tag. If yes, then it will proceed to next level to verify the Timestamp, Nonce and MAC. If the validation is valid then the router will generate redesigned RA Message. Otherwise it will drop the request.
4. Then the router will generate SecMac Tag and append to the RA message.
5. The generate SecMac RA message will be sending to the requesting host.
6. Upon receiving the SecMac RA message, the requesting host will validate whether the RA message received are from the valid router.
7. First the host will verify whether RA has SecMac tag option. Later it will verify the Timestamp, Nonce and MAC.
8. Once the Timestamp, Nonce and MAC is verified, if valid then the host will check the MAC address of the router with the Router Authentication Server otherwise the RA message will be dropped.



9. The host will send a request to the Router Authentication Server to check whether the router MAC address is available in the server's database. If yes, then the router information will be updated in the Neighbour Cache Table.
10. The router will be the default gateway for the host.
11. If no, then the router information would not be updated in Neighbour Cache Table.

## 8. CONCLUSION AND FUTURE WORK

This paper explained the newly proposed secure router discovery mechanism that overcome the DOS attack in the IPv6 network. This mechanism expected to overcome the shortfalls of the existing prevention mechanisms that was discussed in the related work section. This mechanism provided secure router discovery which is lightweight, integrated and self-regulated. Both RS and RA message has been redesigned and appended with SecMac tag that provide integrity of the both messages. Furthermore, the valid router is checked again with Router Authentication Server. This mechanism allows the host to configure a valid gateway router and eventually prevents DoS attacks. The future work would involve test and evaluate the proposed mechanism in terms of effectiveness and performance in terms of time and computation. This will mechanism will be tested using a closed IPv6 network test-bed.

## References


[1] Arjuman N, S Manickam,"Review on ICMPv6 Vunerabilities and its Mitigation Techniques: Classifications and Art" in Computer, Communications, and Control Technology (I4CT), 2015 International Conference, 2015, pp 323-327.

[2] Arjuman N, S Manickam, S Karuppayah and S U Rehman "Review of Security Issues in IPv6 Router Discovery" in Conference: 4th International Conference on Mathematical Sciences and Computer Engineering (ICMSCE), 2017, pp 125-131.

[3] Thomson, S. T. Narten, and T. Jinmei, "IPv6 Stateless Address Autoconfiguration", in Request for Comments 4862, 2007, Internet Engineering Task Force.

[4] Narten. T, et al., "Neighbor Discovery for IP Version 6 (IPV6)", in Request for Comments 4861, 2007, Internet Engineering Task Force.

[5] Atik Pilihanto, "A Complete Guide on IPv6 Attack and Defense", SANS Institute, 2011

[6] T. Chown, S. Venaas, "Rogue IPv6 Router Advertisement Problem Statement", in Request for Comments 6104, 2011, Internet Engineering Task Force.

[7] Deering, S., "ICMP Router Discovery Messages" in Request for Comments, 1256, 1991, Internet Engineering Task Force.

[8] Nikander, P., Kempf, J., & Nordmark, E., "IPv6 neighbor discovery (ND) trust models and threats" in Request for Comments, 3756, 2004, Internet Engineering Task Force

[9] Thomson, S., "IPv6 stateless address autoconfiguration", Request for Comments, 2462,1998, Internet Engineering Task Force

[10] Arkko J., et al., "Secure neighbor discovery (SEND)", 2005, in Request for Comments 3971, Internet Engineering Task Force

[11] Zhang, J., et al, "TRDP: A Trusted Router Discovery Protocol", in International Symposium on Communications and Information Technologies (ISCIT), 2007, pp. 600-605.

[12] Levy-Abegnoli, E et al, "IPv6 router advertisement guard", 2011, in Request for Comments 6105, Internet Engineering Task Force.

[13] Praptodiyono, S.,"Security mechanism for IPv6 stateless address autoconfiguration" in International Conference on Automation, Cognitive Science, Optics, Micro Electro-Mechanical System, and Information Technology (ICACOMIT), 2015, pp. 31-35.

[14] Rehman, S. U., & Manickam, S, "Novel Mechanism to Prevent Denial of Service (DoS) Attacks in IPv6 Duplicate Address Detection Process" in International Journal of Security and Its Applications,2016, 10(4), pp. 143-154.

[15] Henson, V., "An Analysis of Compare-by-hash" in HotOS, 2003, pp 13-18

[16] V. Shoup, "On fast and provably secure message authentication based on universal hashing", in Advances in Cryptology—CRYPTO'96, Springer Berlin Heidelberg, January (1996), pp. 313-328.

[17] T. Krovetz, "UMAC: Message authentication code using universal hashing", (RFC 4418), March, (2006).

[18] Krawczyk, Hugo, Ran Canetti, and Mihir Bellare. "HMAC: Keyed-hashing for message authentication." (RFC 2104), January (1997).

[19] B.G. Buchanan, and E.H Shortliffe, "Rule-based expert systems", Addison-Wesley Reading, MA, (1984).

[20] J.A. Bernard, "Use of a rule-based system for process control", International Society for Optics and Photonics, (1987), pp. 835-849.

[21] Flood. R. L., & Carson, E., "Dealing with complexcity: An introduction to the theory and applications of system. Springer, Science & Business Media, (2013).

[22] Bhargavan, K., & Laurent, G., "Transcript collision attacks: Breaking authentication in TLS, IKE, and SSH. NDSS'16, February (2016).


Navaneethan C. Arjuman is currently the PhD Research Fellow at National Advanced IPv6 Centre (NAv6) in Universiti Sains Malaysia (USM). He received his Bachelor of Engineering in Communication and Signal processing from Staffordshire University, United Kingdom. He is currently the Co-chair of IPv6 Working Group of Asia Pacific Advanced Network (APAN). His research interests are IPv6 Technology, Internet security and Internet of Things (IOT).

**Dr Selvakumar Manickam** is currently 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 the Head of Internet

Security Working Group under Malaysian Research and Education Network (MyREN).

Dr. Shankar Karuppayah is currently Senior Lecturer and researcher at National Advanced IPv6 Centre (NAv6), Universiti Sains Malaysia. He received his Bachelor of Computer Science in 2009 and his M.Sc. in Engineering (Software Systems Engineering) from King Mongkut's University of Technology North Bangkok in 2011 which is based on the RWTH Aachen University Model syllabus. He obtained his PhD in 2016 from Technische Universität Darmstadt. His main research interest is Cyber Security and P2P Botnets. To date, he has authored and co-authored more than 10 articles in journals, workshops, and conference proceedings.

Balasubramanian Nathan is currently the PhD Research Fellow at National Advanced IPv6 Centre (NAv6) in Universiti Sains Malaysia (USM). He received his Bachelor of Physics and Master of Computer Applications in 1995 and 1998. He obtained his M.Phil(Computer Science) in 2008. His research interest are Software Defined Networks and Routing Algorithms.

International Journal of Computing and Digital Systems
ISSN (2210-142X)
Int. J. Com. Dig. Sys. 8, No.2 (Mar-2019)

*E-mail: nava@nav6.usm.my , selva@usm.my, kshankar@usm.my, balasubramanian@nav6.usm.my*