Review of Security Issues in IPv6 Router Discovery

Conference Paper · May 2017

Navaneethan C Arjuman
Malaysia University of Science and Technology (MUST)
6 PUBLICATIONS 41 CITATIONS
SEE PROFILE

Selvakumar Manickam
Universiti Sains Malaysia
311 PUBLICATIONS 2,472 CITATIONS
SEE PROFILE

Shankar Karuppayah
Universiti Sains Malaysia
69 PUBLICATIONS 980 CITATIONS
SEE PROFILE

Shafiq Ul Rehman
The Kingdom University
40 PUBLICATIONS 650 CITATIONS
SEE PROFILE

Review of Security Issues in IPv6 Router Discovery

Navaneethan C. Arjuman [1], Selvakumar Manickam [2,] Shankar Karuppayah [3], Shafiq Ul Rehman [4]

National Advanced IPv6 Centre (NAv6),
Universiti Sains Malaysia, Penang, Malaysia
(nava@nav6.usm.my , selva@usm.my, kshankar@usm.my, shafiq@nav6.usm.my)

Abstract: Router Discovery protocol is an important component of Neighbour Discovery Protocol for IPv6 Address assignment. Even though the IPv6 Router Discovery protocol provides significant advantages over IPv4 Router Discovery but it still possess some weaknesses in terms of the protocol design. The existing vulnerabilities within the Router Discovery protocol design become root cause of some attacks that take place during IPv6 address assignment in the IPv6 networks. In order to overcome these attacks, several prevention mechanisms have been proposed. The proposed mechanisms do provide solution to overcome some of the weaknesses within the Router Discovery Protocol but the mechanism itself has some weakness as well. The primary focus of this paper would be to identify all the relevant prevention techniques for the Router Discovery. At the same time discuss in details advantages and weakness these prevention techniques.

Keywords: Router Discovery, Router Solicitation, Router Advertisement, Router Discovery Attacks

1 Introduction

IPv6 was introduced to circumvent the shortage of global IPv4 address. In IPv6, ICMPv6 messages are used to manage assignment the IPv6 address unlike in the IPv4. The vulnerabilities in the ICMPv6 messages have led to various attacks in IPv6 networks [1]. Various mechanisms are available to assign IPv6 address to a particular host. This includes static, stateful and stateless approach. In the static scenario, a fixed IPv6 address can be assigned to a host by the user manually. In the stateful scenario, the IPv6 address is assigned by a server especially Dynamic Host Configuration Protocol version 6 (DHCPv6) Server [2]. But in the stateless scenario based on the Stateless Address Autoconfiguration (SLAAC) [3], the newly joining host will obtain the IPv6 address using Neighbour Discovery Protocol (NDP). NDP protocol in IPv6 consist of five Internet Control Message Protocol Version 6 (ICMPv6) messages types [4] that are Router Solicitation (RA), Router Advertisement (RA), Neighbour Solicitation (NS), Neighbour Advertisement (NA) and Router Redirect. ICMPv6 Router Discovery consists of RS and RA [5]. In the SLAAC scenario, the host obtained the lower 64 bits of IPv6 address known as Prefix using Router Discovery (RD) and the higher 64 bits address known as host Interface Identifier based on Neighbour Discovery (ND). The host will request for Prefix, Maximum Transmission Unit (MTU) [4, 5] and other relevant parameters by initiating RS to all the routers that attached to the local link and all routers will reply with the above mentioned parameters. The host will select the router that provides the nearest next hop and update the neighbor cache of the host.

When there are rogue routers attached to the network then the attacker will reply with RA with rogue router parameters to RS initiating host. The RA reply with highest priority preference by rogue router will be the default route for the host. Since the rogue router will become the default route and all the future communication of the victim host will be intercepted by the rogue router. This attack is known as a Router Advertisement Spoofing attack. The attacker can launch various attacks [6, 12] using spoofing information from the rogue router. Some of the known attacks are Man-In The Middle Attack, Denial of Service Attack, Replay Attack, and Phishing. Since there is no verification process implemented to authenticate legitimate router in the SLAAC before assigning the IPv6 address, the host will select the rogue router as default router which leads to these attacks. There are already proposed several mitigation techniques to overcome the above mentioned security vulnerabilities in the RD protocol. This paper is focused on to review the Router Discovery vulnerabilities issues, and discuss advantages and weakness of these existing mitigation techniques.

Section 2 covers the background how a newly joining host gets IPv6 Prefix and related parameters. Section 3 discusses vulnerabilities within RD protocol. Section 4 and 5 explains the existing mitigation techniques to overcome the weakness within RD protocol. Section 5 provides conclusion and discuss future work.

2 Background

In this section, it has been assumed that the reader has basic knowledge about IPv6 address and ICMPv6 messages structure.

The 128 bit IPv6 address assignment for newly joining host in the network implemented based on RD for the lower 64 bits and ND for higher 64 bits. The RD process implemented using both RS (Type 133) and RA (Type 134) messages as depicts by Figure 1.

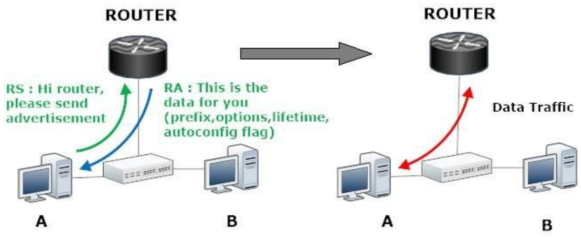
ROUTER
ROUTER
RS : Hi router, please send advertisement
RA : This is the data for you (prefix,options,lifetime, autoconfig flag)
Data Traffic
A
B
A
B

Figure 1: Process Flow of Router Discovery [19]

When Host A first joints the IPv6 link, it will multicast RS message to all the neigbour routers on the link to get the IPv6 Prefix and related parameters such as Maximum Transmission Unit (MTU) and Domain Name Service (DNS) details. The source address will be the IP address of the sending interface or it could be unspecified address if there is no address on the sending interface [4] of the host. The typical destination address will be the all routers multicast address ff02::2.

Upon receiving the RS message from the Host A, all the active routers such as Router A and Router B on the link will response to the RS message with RA message as depicts in the Figure 1. Router usually sends out RA message in the unsolicited scenario periodically and solicited scenario upon receiving RS from the host [4]. The source address will be the link layer address of the sending router interface. The typical destination address will be the source address of requesting host or all-nodes multicast address ff02::1. The host will configure it's default gateway based on nearest next hop router and also based on the following conditions.

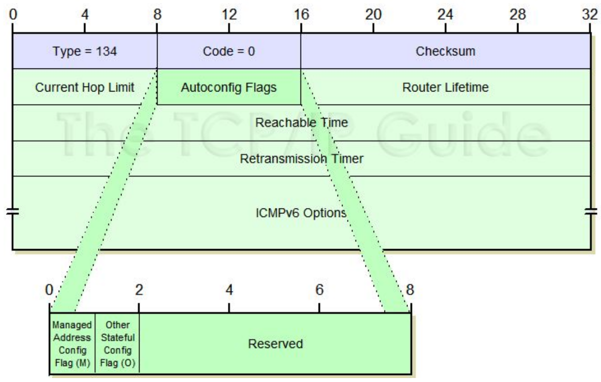

Figure 2: RA Message Format
(Source: http://www.tcpipguide.com/)

Figure 2 depicts RA message format. When the Managed Address Config Flag M bit under the Autoconfig Flags is enabled means the Prefix assignment will be from DHCPv6 server. When M bit set and the O bit is not set then O bit will redundant and can be ignored because all the information will be provided by the DHCPv6 server [4]. Disable the M bit and enable O bit allows the global unicast prefix assignment from RA and the ND configuration from a DHCPv6 Server. Enabling O bit means the other configuration such as DNS related information or other servers information are from the DHCPv6 server.

The higher 64 bit assignment of the IPv6 address will be completed using Neighbour Discovery using both NS and NA messages. The completion of Duplicate Address Detection (DAD) process [4] allows the host to have legitimate address to communicate within link local and global communication.

3 ROUTER DISCOVERY VULNERABILITIES

The above IPv6 address assignment is vulnerable to attacks because there are weakness exist in the Router Discovery process. The presence of rogue routers in the network can lead to host receiving fake router RA information.

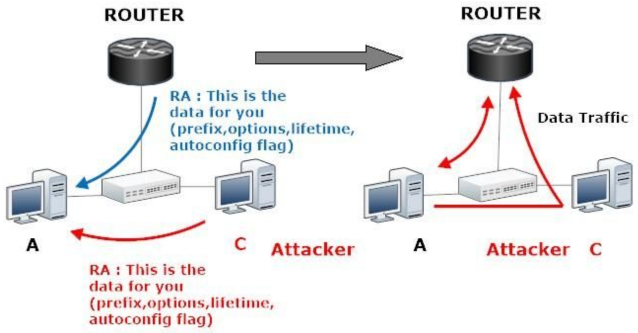
ROUTER
ROUTER
RA : This is the data for you (prefix,options,lifetime, autoconfig flag)
Data Traffic
A
C
Attacker
A
Attacker
C
RA : This is the data for you (prefix,options,lifetime, autoconfig flag)

Figure 3: Router Advertisement Spoofing Attack [19]

When the Host A sends out RS message to all the active routers on the link, the Attacker C will also receive the same message. The Attacker C whom act as rogue router will send RA messages with higher priority so that Host A will configured it's default gateway with rogue router prefix. The nature of selection of router is based on nearest next hop. So the attacker can craft the RA packet with highest priority and the nearest next hop value so that host will configured with rogue router information as default router. Once the data transmission takes place, all the packets will be routed through the rogue router before it reach the actual destination. The attacker able to sniff the information that passed through the victim host to the destination. This attack is known as Router Advertisement Spoofing [17]. Using the spoofed information from the rogue router, the attacker also can initiate various other attacks [16] such as Man-In The Middle Attack, Denial of Service (DoS) attack, Replay attack, Re-direction attack, phishing etc. Router Advertisement flooding attacks also can be initiated using multiple RA announcements and freeze the local network communications as well [17] due to the weakness within the RA protocol.

The above mentioned attacks are possible because there is no security mechanism in place to verify the legitimacy of the default router within the RD protocol. There is several security mechanisms have been proposed to mitigate the above issues. This paper will cover on the implemented techniques that focus on how to mitigate issues related to Router Discovery issues only. Some of the implemented related mitigation techniques that mainly focused on RD are SeND's Authorisation Delegation Discovery [7], Trust Router Discovery Protocol [8] and Router Advertisement Guard [9].

This paper also review alternative related works that includes RD mitigation techniques such as Candidate Access Router Discovery [10], Trust ND [11], Trust Based Security Enhancement Mechanism For Neighbor Discovery Protocol In IPv6 [12], Dynamic IPv6 Activation based Defense for IPv6 Router Advertisement Flooding (DoS) Attack [13] and Secure Duplicate Address Detection [14]. The following sections will review in details the above mitigation mechanism.

4 PREVENTION MECHANISM

4.1 SeND's Authorisation Delegation Discovery (ADD)

The ADD mechanism is part of SeND standard. IPv6 host can verify the authenticity of the legitimate router based on the trusted electronic certificate that issued by Certificate Authority. This mecahism has introduced two new ICMPv6 messages namely Certificate Path Solicitations (CPS) and Certificate Path Advertisment (CPA) [7].

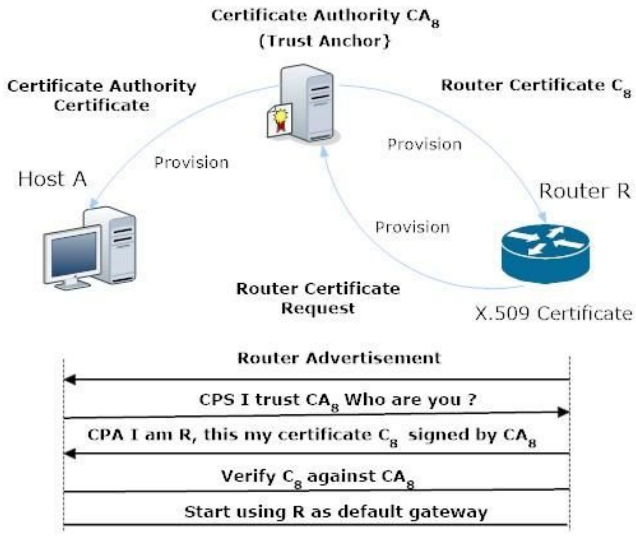
Certificate Authority CA_8
(Trust Anchor)
Certificate Authority Certificate
Router Certificate C_8
Provision
Provision
Host A
Router R
Provision
Router Certificate Request
X.509 Certificate
Router Advertisement
CPS I trust CA_8 Who are you ?
CPA I am R, this my certificate C_8 signed by CA_8
Verify C_8 against CA_8
Start using R as default gateway

Figure 4 : Router Authorization Process [15]

Figure 4 depicts how the ADD process implemented during the legitime router authorisation process in a typical IPv6 network. Based on this mechanism when Host A first joining the network, it will multicast RS to all the routers on the link and all the active routers will reply with RA. In order to verify whether the RA is from the legitimate router, Host A will send out CPS to request for the certification path to verify the Certificate Authority (CA_8) that trusted by the Host A . Upon the receiving the CPS, the Router R required to reply with CPA informing Host A that the router identity and provide certificate such as X.509v3 that was signed by the CA_8 [15]. The Host A will verify the certificate provided by Router R and if the certificate is valid then the host will accept the Router R as the default router. If not valid then the process will be repeated again.

This mechanism also have some weakness that leads to DOS attack during the certificate path verification process. The attacker will keep sending unneccessary CPAs to Host A so that Host A is required to certify the path again and again [15]. This will occupy the host to perform many unnecessary computation task to validate the CA. In this scenario, even though there is no specific attack take place but the host has to verify the whole certificate chain obtained from the router. This process resulting lengthy certificate verifications and it will be costly especially in mobile nodes where immediate switching required from one cell to another cell. Also this mechansim also has limitation for configuring using static IPv6 address and SLAAC using fixed interface identifier . Also ADD does not specify how to use trust anchor between nodes with dynamically changing address such as privacy address configuration.

4.2 Trust Router Discovery Protocol (TRDP)

TRDP try to address the limitation of ADD. ADD CA verification is very lengthy and consume high computation process compare to TRDP.

Figure 5 depicts A Colored Petri Net decriptions that analyse the process flow of the TRDP process. In the TRDP process, newly joining host can verify legitimate Access Router (AR) based on the Router Access Passport (RAP) [8]. RAP are issued to AR by upper intermediate router that linked to trust anchors unlike in the ADD process where the host to verify the whole certification path to trust the anchors. TRDP introduce two pair ICMPv6 messages known as TRPS/TRPA (Trusted Router Passport Solicitation/Trusted Router Passport Advertisment) and TR^{2}PS/TR^{2}PA (Trusted Router-Router Passport Solicitation/Trusted Router-Router Passport Advertisment) [8].

The newly joining host will send out RS, the AR will reply with RA. Upon receiving the RA, the host will send out the TRPS with Nonce and list of Trust Anchors (TA) to verify legitimacy of the AR. The AR will reply with the Nonce, TA and RAP with signed by the TA. Upon receiving the TRPA with valid RAP, host will set the AR as the default router. The TRPA is send in the encrypted form to avoid unneccessary interception by the attackers.

In the scenario where the AR do not have the RAP with the signed by appropriate TA which address by host then the AR will initiate TR^{2}PS message to the upper AR to request for the RAP. The upper AR required to respond with TR^{2}PA with the RAP. If the upper router also do not have the RAP requested by the host then the process will repeated to upper routers step by step until reach the TA. The above TR^{2}PS and TR^{2}PA are carried out in the encypted manner to avoid interception by the attackers.

Even though TRDP improves the performance Router Discovery compare to ADD but the process still lengthy compare to RA-Guard and provide loop holes for DoS attacks to take place in the process of acquiring RAP.

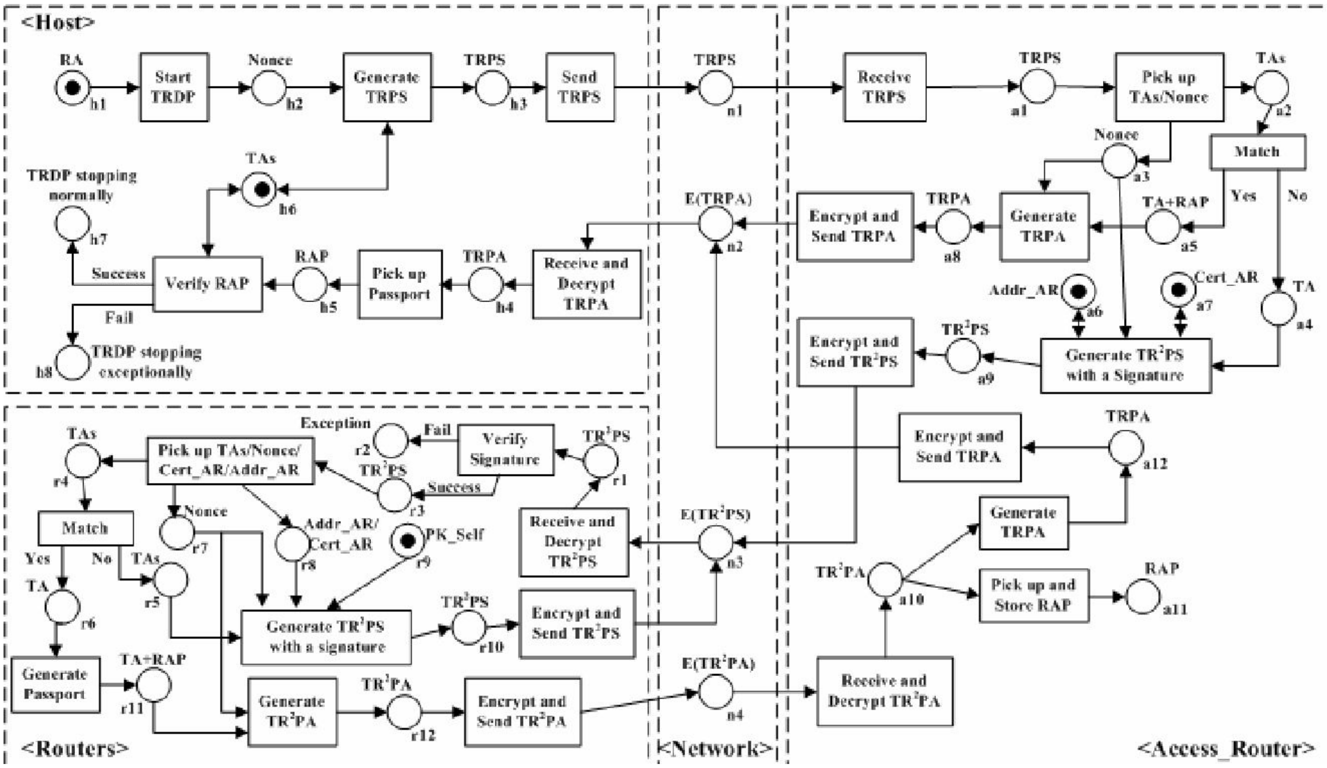

Figure 5 : A Colored Petri Net Descriptions for TRDP [8]

4.3 *Router Advertisement Guard (RA-Guard)*

Unlike ADD and TRDP, RA-Guard provide protection against rogue router attacks in the shared Layer 2 in the network segment. This mechanism can be implemented complement with SeND. This mechanism will filter the RA messages that not from the authorised source [9].

The RA-Guard can be enabled in the Layer 2 networking devices such as switch as the router authorization proxy. RA-Guard and can be implemented both on the stateful and stateless scenarioes.

In the stateless scenario, the decision to allow the RA traffic is based on the source link layer address, source port where the frame is received from, IP address of the source and prefix list [9]. Based on the above information the Layer 2 device either allow or disallow the RA traffic. The above decision to allow and not allow also is based on router priority as well. The above stateless setup can be configured using small L2 switch which one interface statically connected to a router and others are connected non-router devices. With this setup the only allowing RA to interface that connected to router and the other interfaces will block the RA traffics as per Figure 6.

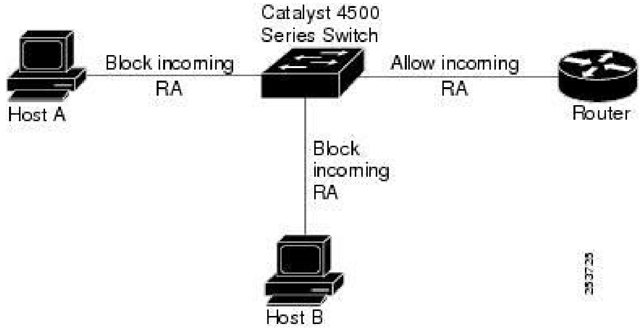

Figure 6 : Stateless RA Implementation
(Source : http://www.cisco.com)

In the stateful scenario, RA-Guard dynamically will learn about senders legistimate RA and stores information for subsequent RA forwarding [9]. In this secnario RA Guard works in four different states as mentioned below.

State 1 – OFF
RA-Guard not available on the interface

State 2 – LEARNING
The device actively learn the information about IPv6 routing devices that connected to this interface.This process take place over predefined period or triggered by event. End of the period, the RA-Guard enabled interface either block the RA Message until the source is validated or forward to destination once source is validated.

State 3 – BLOCKING
RA-Guard enabled interface block all the ingress RA message. L2 device operator can manually change the status from BLOCKING to FORWARDING.

State 4 – FORWARDING
RA-Guard will forward all the ingress RA message to the destination. L2 device operator can manually change the status from FORWARDING to BLOCKING.

The stateful RA-Guard will work as well with SeND. In this scenario blocking and forwarding of ingress RA messages are based on SeND configurations. Upon capturing the RA messages, the devices will verify agaisnt the Crytographically Generated Address (CGA) and the RSA (Rivest, Shamir, and Adleman algorithm for public-key cryptography) Signature. It will drop the RA message if the verification failed. The L2 device will attempt to retrieve valid certificate from cache from public key infrastructure. If found the certificate then RA message will be delivered to the destination. If not found the L2 device will initiate CPS to locate the CA. It will capture the CPA in order to verify the certificate chain. Failure to validate the certificate chain will result the RA will be dropped. Upon successful validation the RA message will be forwarded to destination and the certificate will be cache in the router [9].

But the implementation of the RA-Guard also comes with the following shortcomings

1. RA-Guard unable to block rogue RA messages that does not communicate via RA-Guard enabled devices.
2. RA-Guard unable to block the RA messages that are channel through tunneled traffic.
3. RA-Guard can be only configured and supported for rogue ingress RA messages only and not egress RA Messages.
4. Unable to configured RA-Guard in the devices that already configured with ACL ICMPv6 optimization.
5. The RA-Guard feature is not supported on trunks ports with merge mode.

Also there are methods based on evasion techniques to circumvent RA-Guard implementation by employing IPv6 extensions headers [18]. The RA-Guard is unable to drop if the forged RA packets are fragmented. So the above mentioned limitations are needed to eliminate for wider implementation.

5 Other Related work

This section discuss some of the other related work that covers RD protocol.

5.1 *Candidate Access Router Discovery (CARD)*

CARD propose allows seamless handover of mobile node (MN) from one access router to another [10]. Prior to handover the MN needs verify identities and capabilities of the Candidate Access Router (CAR) before initiating the handover. The CARD process of involves two key steps that are identifying the IP Addresses of CAR and finding their capabilities. But this implementation of RD more focused on router to router handover in the mobile networks. This mechanism does not cover RD by host.

5.2 *Neighbour Discovery Trust (Trust-ND)*

The Trust-ND implementation primarly focused on Secure Neighbour Discovery. But the authors suggested also can be implemented Router Discovery as part of future work [11]. Even though the performance better then SeND but this technique has not been tested for RD. This technique also has some weakness especially in the assignment of initial trust value and also no resistance against hashing collision attacks.

5.3 *Trust Based Security Enhancement Mechanism For Neighbour Discovery Protocol In Ipv6 (T-NDP)*

Unlike Trust-ND, T-NDP has implemented for Router Discovery. The primary focus of this mechanism is for router to router discovery in Mobile IPv6 environment [12]. Even though this mechanism claim better then SeND and Trust-ND but this technique also has weakness especially in the assignment of initial Trust State value. Furthermore this mechanism does not cover RD for host.

5.4 Dynamic IPv6 Activation based Defense for IPv6 Router Advertisement Flooding (DoS) Attack

The technique focus on turning off IPv6 connectivity when there is RA flooding attacks and turn on IPv6 connectivity if attack subside [13]. But this technique would not be effective when there is real time IPv6 applications running on the network.

5.5 Secure Duplicate Address Detection (Secure DAD)

Similar to Trust-ND, Security Tag also primarily focused on secure Neighbour Discovery with better performance. But the authors suggested also can be implemented on Router Discovery as part of future work [14]. Secure DAD is not tested for RD for now and also has weakness especially in the assignment of initial value for the security value.

6 Conclusion

This primary objective of this paper would be to review the existing prevention techniques to overcome RD protocol vulnerabilities. Based on the above review, all the existing mechanism does provide solution to overcome the weakness of RD vulnerabilities. But at the same time the existing mechanisms also have it own shortfalls that required to be fixed in order to provide more efficient secure Router Discovery. So the proposed future work would be looking into to improve the existing mechanism so that can provide more secure RD.

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] Droms, R., Bound, J., Volz, B., Lemon, T., Perkins, C., & Carney, M., "Dynamic host configuration protocol for IPv6 (DHCPv6), in Request for Commnets 3315, 2003, Internet Engineering Task Force

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

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

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

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

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

[10] Liebsch, M., "Candidate access router discovery (CARD)", 2005, in Request for Comments 6105, Internet Engineering Task Force.

[11] 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.

[12] Perumal, K., & Priya, M. M. J. P. J. "Trust Based Security Enhancement Mechanism For Neighbor Discovery Protocol In IPV6" in International Journal of Applied Engineering Research, 2016, 11(7), pp 4787-4796.

[13] Goel, J. N., & Mehtre, B., "Dynamic IPv6 activation based defense for IPv6 router advertisement flooding (DoS) attack", in Computational Intelligence and Computing Research (ICCIC), 2014 IEEE International Conference, 2014, pp 1-5.

[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] AlSa'deh, A. and C. Meinel, "Secure neighbor discovery: Review, challenges, perspectives, and recommendations", Security & Privacy, IEEE, 2012, 10(4): pp. 26-34

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

[17] Ullrich, J., Krombholz, K., Hobel, H., Dabrowski, A., & Weippl, E., "IPv6 security: attacks and countermeasures in a nutshell", in 8th USENIX Workshop on Offensive Technologies (WOOT 14), 2014,pp 5-16.

[18] Gont, F.," Implementation Advice for IPv6 Router Advertisement Guard (RA-Guard)" in Request for

Comments 7113, 2014, Internet Engineering Task Force.

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