International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-8 Issue-4, November 2019

Address Autoconfiguration in IPv6 Networks: Challenges and Countermeasures

Rajula Angelin Samuel , D. Shalini Punithavathani

Abstract*: The demand for internet and its applications has eventually led to the depletion of the dominant IPv4 addresses. This has resulted in the inevitable need for the next generation Internet Protocol IPv6, which contains an enormous pool of IP addresses. Address Autoconfiguration, a remarkable feature of IPv6 enables a node connected in the network to automatically configure an IP address for its interface and instantly participate in network communications. The Internet Engineering Task Force (IETF) has classified autoconfiguration into Stateless and Stateful mechanisms. Several IPv6 protocols have been employed to achieve autoconfiguration of networks. However, in addition to the excellent competence of this feature, autoconfiguration certainly suffers in terms of security and optimization. This paper attempts to enlighten the need and merits of Address Autoconfiguration and finally highlights the challenges, open issues and countermeasures involved in achieving this in real time environment.

Keywords: **Autoconfiguration, DAD, CGA, ICMPv6, IETF, IPSec, IPv6, Neighbor Discovery Protocol, SeND, SLAAC**

I. INTRODUCTION

The Internet Protocol (IP) is the massively used communication protocol. Every host connected to the network requires a unique address for communicating with other devices in the network. IP is responsible for host addressing, packet fragmenting and routing datagrams between source and destination hosts. The dominant 32-bit Internet Protocol Version 4 (IPv4) with the limited 2^{32} addresses routes most of the current day internet traffic. The tremendous increase in the usage of internet applications in the recent years has originated the exhaustion of IPv4 addresses. This has paved the way for the successor, next generation Internet Protocol version 6 (IPv6).

Manuscript published on November 30, 2019.
* Correspondence Author
Rajula Angelin Samuel*, Department of Computer Science & Engineering, Government College of Engineering, Tirunelveli, Tamilnadu, India
D. Shalini Punithavathani, Department of Computer Science & Engineering, Government College of Engineering, Tirunelveli, Tamilnadu, India

The 128-bit IPv6 with massive 2^{128} addresses will certainly replace IPv4 in the future. At present, IPv4 and IPv6 coexists in the network layer and immediate transitioning is not feasible due to the incompatibility of the protocol structures. IETF, has suggested several transition mechanisms like Dual Stack, Translation and Tunneling to be incorporated in the network for smooth functioning in the coexistence phase. IPv6 surpasses IPv4 not only in terms of large address space but also has built-in Security (IPSec), end-to-end connectivity, improved Quality of Service and better mobility.This paper elucidates IPv6 autoconfiguration mechanisms discussing the necessity and advantage of this significant feature and finally summarizes the challenges along with countermeasures that will direct the perspective of future analysts. The paper is structured as follows: Section II portrays the procedure of autoconfiguration and Section III explains Stateless and Stateful autoconfiguration types, wherein autoconfiguration of networks is achieved with/without third-party intervention. Section IV sheds light on IPv6 Neighbor Discovery Protocols (NDP) which is a key to achieve address autoconfiguration and in Section V the attacks encountered during autoconfiguration is discussed. Section VI deals with the review of prominent research work and their implications. Finally, the last section highlights the challenges and countermeasures involved in achieving autoconfiguration.

II. IPV6 ADDRESSING

The 128-bit long IPv6 addresses are assigned to single or a group of interfaces. Due to the large addressing capability, a single interface can be assigned with multiple IPv6 addresses.

A. Addressing Format

IPv6 addresses are alphanumeric strings segregated into 8 groups using colons, each of which is 16 bits. Each group is denoted using four hexadecimal digits. The 128-bit IPv6 address is split into two variable length parts. The first being the network id is used for routing and the latter is the interface id used to identify the address of the interface. The upper bit section of the network component is used for global network address and the lower bit section is used for subnets on the internal network. The interface Id can be derived from MAC address using IEEE's EUI-64 conversion format or random generation methods.

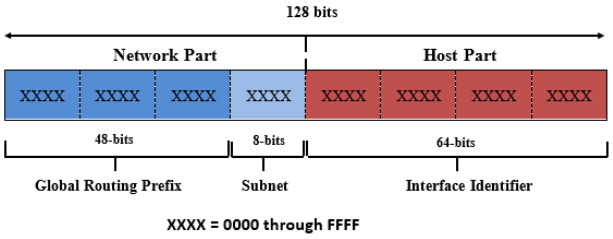

Fig. 1.IPv6 Address Format

B. Addressing Types

The IPv6 addresses are classified as unicast, anycast and multicast addresses. The leading bits of the address (prefix) specifies the type of address.

- **Unicast addresses** are identifiers for an individual interface. Unicast address can be global, site-local, link-local and IPv4-compatible IPv6 address. Global addresses have global-scope and are used for communication across networks whereas site-local and link-local addresses have local-scope and are used for single link or single site communications. IPv4-compatible IPv6 addresses are designed to be used during the transitioning (IPv4 to IPv6) phase where these addresses are used as tunnel endpoints when IPv6 packets are tunneled over an IPv4 only network.
- **Anycast addresses** are assigned to more than one interface. Packets sent to an anycast address is delivered to the nearest interface identified by that address. Anycast addresses are identical to unicast addresses, when a single unicast address is assigned to more than one interface it is termed as an anycast address.
- **Multicast address** is an identifier for a set of interfaces. A single interface can be linked to any number of multicast groups. A packet destined to a multicast address is routed to all interfaces identified by that address. Routers in the link joins the all-routers (FF02::2) multicast address and the nodes in the link joins all-nodes (FF02::1) multicast address automatically. Solicited-node multicast addresses are addresses with link-local scope derived from the target node's address. Target addresses that vary only in the most significant bit will join the same solicited-node multicast address.

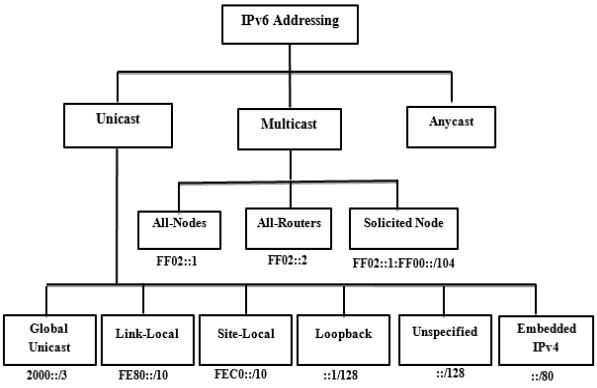

Fig. 2.IPv6 Address Types

C. Addressing States

Each address assigned to an interface has a lifetime component with it, which indicates the time period the address is bound to that corresponding interface. The address is usually in preferred state when it is assigned to an interface and when the lifetime expires, the address becomes invalid and the state changes from preferred to deprecated.

Table - I: List of IPv6 Address States

State	*Description*
Tentative	Address uniqueness being verified, before assigning to an interface
Preferred	Address assigned to an interface, use is unrestricted
Deprecated	Address assigned to an interface, cannot be used for new communication
Valid	Preferred or Deprecated address
Invalid	Lifetime expired addresses, cannot be used as source or destination addresses

D. Addressing Merits

IPv6 addresses encompass a bundle of advantages compared to its predecessor.

- Scalability – Large addressing capability facilitating unique address to every interface in the network.
- Efficient Routing - Smaller routing tables with simplified packet header and prefix aggregation.
- Autoconfiguration – Stateless autoconfiguration of host when enabled on an IPv6 network.
- Built-in-Security (IPSec) - Security protocol which authenticates and encrypts the data transmitted.
- Efficient Data Flow – Improving performance by transmitting jumbograms (packets exceeding MTU).
- Multicasting – Promotes sending packets to multiple destinations in a single operation.

III. ADDRESS AUTOCONFIGURATION IN IPv6

Autoconfiguration of networks is crucial to lessen the overall operational cost and enhance network design leading to a plug and play architecture. By autoconfiguration, any node enabled on the link generates its own address for communication within the network with minimal or no external support. Autoconfiguration is possible only on multicast enabled interfaces.

A. Autoconfiguration Types

- **Stateful Address Autoconfiguration** is a mechanism by which a host obtains the 128-bit address and other network configuration parameters from a DHCPv6 server. In this type of configuration, a third-party device is a prerequisite for a host/interface to be enabled on the network.
- **Stateless Address Autoconfiguration (SLAAC)**, an exclusive aspect of IPv6 facilitates a host to dynamically generate its own IPv6 address and participate in network communications with no manual configurations.

Stateful configuration is recommended when the site requires strict control over the address assignments whereas stateless approach is advised when site is not concerned with the exact number of address assignments. Both the approaches can be used simultaneously in the same network. The administrator of the site specifies the autoconfiguration type by setting the Managed Address Configuration Flag (M Flag) and Other Stateful Configuration Flag (O Flag) in the messages advertised by the routers to all the nodes in the network.

Retrieval Number: D9178118419/2019©BEIESP
DOI:10.35940/ijrte.D9178.118419
Journal Website: www.ijrte.org

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

Table - II: Address Allocation Types

Address Allocation Mechanisms	*O FLAG [Other Stateful configuration Flag]*	*M FLAG [Managed Address Configuration Flag]*
SLAAC (No DHCPv6) Stateless Autoconfiguration	0	0
SLAAC + DHCPv6 Stateless Autoconfiguration	1	0
DHCPv6 Stateful Autoconfiguration	0	1
DHCPv6 + Stateless Stateful	1	1

B. Autoconfiguration Process

A node performs sequence of steps to automatically configure its interface in an IPv6 network. First, the node evaluates the M and O flag to determine the type of configuration: stateless, stateful or hybrid. Every interface enabled on the link has atleast two IPv6 addresses. The link-local addresses for data exchange within the network and the routable global address for communication across networks. The process of generating link-local and global addresses via stateless mechanisms are presented in this section.

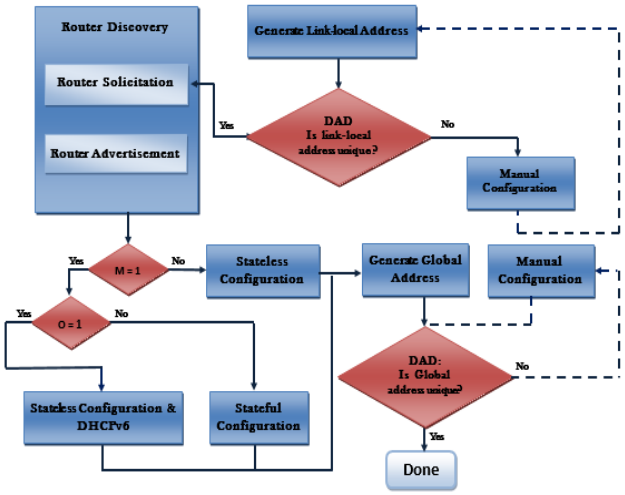

Fig. 3.Address Autoconfiguration Process

- **Link-Local Address Generation:** When an interface with multicast capability is enabled in the link, the nodes (hosts and routers) begin the autoconfiguration process. First, link-local address for the interface is generated. An interface may be enabled during system startup time, reinitialized after failure or while attaching to a link for the first time. The link-local address is formed by combining the interface id of the node with the link-local prefix FE80::0. The node verifies the uniqueness of the tentatively generated link-local address by validating that the generated address is not assigned to any other node in the link before configuring it for itself.
- **Duplicate Address Detection:** To certify that all newly the addresses are different on the link, every node does a duplicate address detection (DAD) check on the addresses. This check is done prior to assigning the address to any interface. DAD check is done on all unicast addresses configured via stateless approach or DHCPv6. The address on which DAD procedure is initiated will be in "tentative" state, once the address is identified to be unique the state changes from "tentative" to "preferred". An address should be in preferred state to be used for communication in the network. The procedure for detecting duplicate address is discussed in section IV. If the newly generated address is discovered to be duplicate, it cannot be assigned to the interface and a new interface id has to be assigned or all IP address for that interface should be manually configured.
- **Global Address Generation** The global address is formed by combining the interface id with a prefix advertised by the router in the link. Router Advertisements containing prefix-information options are sent at regular intervals by routers in the link to the all-nodes multicast address. The nodes in the link can send Router Solicitation messages to all-router multicast address to intimate the routers to send Router Advertisement messages. The global addresses are routable on the internet and are used for communication across networks. Like Link-local address, global address is also verified for uniqueness via DAD procedure as depicted in Fig.3.

IV. ADDRESS AUTOCONFIGURATION PROTOCOLS

Autoconfiguration of a node is achieved using the Neighbor Discovery Protocol (NDP). NDP uses 5 messages of Internet Control Message Protocol version 6 (ICMPv6) shown in Table-IV to complete the role of autoconfiguration. The integral functions of NDP are IP address generation in SLAAC, checking the uniqueness of the generated address through the DAD process, establishing connection with adjacent nodes and redirecting traffic path from one to another. NDP [2] in IPv6 provides horde of enhancements compared to IPv4 and it is considered as a replacement for IPv4 protocols like Address Resolution Protocol (ARP), ICMP Router Discovery (RDISC) and ICMP Redirect (ICMPv4).

A. Router Solicitation (RS)

When an interface is enabled in a link, the new node issues Router Solicitation message with unspecified address (::) as source to all-routers multicast address to intimate the routers in the link to send Router Advertisement immediately rather than sending it during the next scheduled time. This request is sent to obtain the network prefix to configure the global address for communication across networks.

B. Router Advertisement (RA)

Routers in the link periodically/upon request multicasts Router Advertisement messages to all-nodes multicast address to inform its availability in the network. The advertised message contain network parameters like prefix list, flags, MTU and hop limit. The flags specify whether the node has to use stateless or DHCPv6 method for address configuration. The prefix advertised are used for global address generation.

C. Neighbor Solicitation (NS)

The nodes send out Neighbor Solicitation messages to find out the link-layer address of the neighbors. NS messages are also sent to verify the reachability of a neighbor. During duplicate address detection procedure, NS messages are used to determine if the generated unicast address is duplicate. The tentatively generated ipv6 address is sent in the target address field of the NS message to solicited-nodes multicast address to verify its uniqueness using the unspecified address (::) as source.

D. Neighbor Advertisement (NA)

Neighbor Advertisements are dispatched as response to NS messages to the link-layer address of the invoking interface or to all-nodes multicast address if the source address is unspecified. A node may send NA messages to inform link-layer address change or during duplicate address detection procedure, if the tentative address sent in the NS message is duplicate the nodes in the link respond back with a NA message.

Table- III: List of Autoconfiguration Protocols

Message Type	Function	Source Address	Destination Address	Information [Sent/Requested]	ICMP Type	Code
Router Solicitation (RS)	Router Discovery	Interface address if assigned or :: if not assigned	all-routers Multicast address (FE02::2)	Sent by hosts to intimate routers to send RAs quickly	133	0
Router Advertisement (RA)	Router Presence	Router's Link-local address	Source address of invoking host or all-nodes multicast address (FE02::1)	Sent by routers - Prefix information, hop limit, MTU	134	0
Neighbor Solicitation (NS)	Neighbor Discovery	Interface address if assigned or :: if not assigned	Solicited-node multicast address or the target address of a node	Sent by host to request link layer address of target node or to check the uniqueness of the target address (DAD)	135	0
Neighbor Advertisement (NA)	Neighbor Presence	Interface address of the neighboring host	Source address of invoking host or all-nodes multicast address (FE02::1)	Sent by neighboring host to intimate change in link-layer address or duplicate address during DAD	136	0
Redirect	Better First-Hop node	Link-local address of originating interface	Sent to the node that triggered the redirect.	Sent by routers to intimate the better first-hop node in the destination path.	137	0

V. THREATS ON AUTOCONFIGURATION

Neighbor Discovery Protocol (NDP) which plays a key role in autoconfiguration of a node is exposed to several network-based attacks. The main devices that take part in autoconfiguration are hosts and routers. The most common attacks on the NDP messages are classified as Host-Related and Router-Related threats and are discussed below.

A. Host-Related Threats

- **Neighbor Solicitation/Advertisement - Spoofing**

The attacker node pretends to use a legitimate address and transmit packets destined to a particular interface to a different link layer address. In IPv6, the NDP messages used by an interface to discover the presence of neighbors are attacked and counterfeit addresses are updated in the neighbor cache [14]. The packets gets routed to the spoofed fake address in the cache resulting in a denial of service to the original destination. Sniffing and Man-in-the-Middle attacks are common examples of address spoofing.

- **DAD – Denial of Service (DoS) Attack**

When the target address sent in the DAD request is continuously claimed by an attacker [11] in the network, that address can never be acquired by the interface initiating the request. Hence, the interface trying to get enabled on the link using SLAAC fails resulting in Denial of Service (DoS) attack [7]. The address can be claimed by the attacker by sending fake NA messages in response to NS indicating the target address is already owned by the attacker.

- **Neighbor Unreachability Detection (NUD) Failure**

The nodes on the link send NS to determine the reachability of peer nodes. The reachable peer nodes respond back with a NA. If the soliciting node does not receive a reply from the peer node, it resends the NS message few times and ultimately the neighbor cache entry of the unreachable node is deleted. When a malicious node in the link sends formulated NA [15] in response to the neighbor reachability NS message, it results in a situation where the originally targeted destination is inaccessible leading to NUD failure.

B. Router-Related Threats

- **Malicious Last-Hop Router Attack**

By multicasting legal Router Advertisements or sending RAs in response to RS messages, an attacker node in the link impersonates itself as a last hop router. A node trying to discover a last hop router selects the illegitimate node as its default router. This makes the host to deceitfully believe that an accessible router is unable to route traffic resulting in a DoS attack.

- **Bogus Address Configuration**

A bogus prefix is attached in the RA formulated by the attacker and multicasted to the node on the link. During SLACC the nodes use the bogus information to frame the global address. The address generated cannot be used for communicating across network due to illegal prefix leading to denial of service to the victim node.

- **Bogus on-link prefix**

An attacking node on the link sends a fabricated RA with a prefix of arbitrary length. When a sending host believes a prefix to be on the network, the host will never send packets for that prefix to the router rather it performs an address resolution by sending NS messages, but response would be denied [18] causing a DoS leading to flooding of routing table.

- **Default Router is killed**

By launching DoS attack on the router, the malicious node on the link makes the router unresponsive. As a result of this the default routers list of a node becomes empty moving the routers in the link to a dead state. Assuming there are no routers in the link the nodes use the Neighbor Discovery messages to send packets to other nodes. The attacker in the link can easily spoof the NS/NA packets exchanged.

- **Parameter Spoofing**

The attackers can spoof and send valid-seeming RAs by altering the configuration parameters [46] that indicate the type of configuration of the node in the link (Stateless or Stateful). The manipulation of additional parameters can create an impact on enabling the interface on the network.

Table- IV: Neighbor/Router Discovery Protocol Threats

Type of Attack	*Attack Name*	*ND[a]/RD[b]*	*Messages*
Host-Related Attacks	NS/NA Spoofing	ND	NS/NA
	DAD – DoS	ND	NS/NA
	NUD Failure	ND	NS/NA
Router-Related Attacks	Malicious Last-Hop Router	RD	RS/RA
	Bogus address configutaion	RD	RA
	Bogus on-link prefix	RD	RA
	Default router killed	RD	RA
	Parameter Spoofing	RD	RA

[a] Neighbor Discovery, [b] Router Discovery

VI. ANALYSIS AND DISCUSSIONS

Duplicate Address Detection (DAD) procedure is considered to be one of the crucial steps in the autoconfiguration process, as autoconfiguration of a node solely lies on the success of DAD process. Unfortunately, DAD is subjected to several attacks and [5], [10], [11] has emphasized that DAD to a greater extent is exposed to Denial of Service (DoS) attacks. In [6], DoS-on-DAD can prevent a node from obtaining the target address by continuously replying NA messages indicating that the address is not unique. Due to DAD failure, the interface will never be enabled on the link. To address security issues in NDP messages, IETF the originator of IPv6 itself has formulated enhancements like IPSec [22], SeND [13] and CGA [25]. It is also inferred after keen analysis that several techniques have been proposed by researchers with the intension to secure DAD process to enable autoconfiguration by enhancing the standards provided by IETF. The findings have been classified under three broad categories: Securing Address Generation, Monitoring Address Configuration and Securing Address Configuration. Relevant methods and their advantages and drawbacks are critically analyzed in this section.

A. Securing Address Generation

The following methods discussed have been suggested by researchers to secure the address generation process to prevent DoS attacks during DAD.

Cryptographically Generated Addresses (CGA) [25] are IPv6 addresses in which the rightmost 64 bits (Interface Id) of the 128-bit address framed from random generation methods is computed from a cryptographic hash function of the owner's public key. As the public key is bound to CGA the address holder can use the matching private key to claim ownership and sign the message while sending. The 3-bit security parameter (Sec) of CGA determines the level of security against attacks and it is encoded at the leading 3 bits of the host Id [26]. CGAs are rigid forbidding attackers from spoofing and address stealing without depending on any trust authority. Since there is no mechanism to prove address individuality in CGA, an illegal node can create a new address from a random subnet and claim it to be a CGA. Moreover CGA computations cost is extremely high and hence frequently changing the address is not possible yielding to address stealth.

A substitute protocol to CGA called CGA++ suggested in [28] as an enhancement to CGA to overcome the shortcomings of standard CGA and boosts the overall security. To address the authentication issue in the original CGA, CGA++ uses an additional digital signatures component for address verification. It resolves the global time-memory trade-off attack existing in CGA. But the usage of digital signatures has further added to the computational cost of generation and verification of CGA leading to increased address renewal cost.

Time-Based CGA (TB-CGA) [27], a modification to CGA was proposed to limit the time taken to generate CGA and increase the probability to have a better Sec value. A time parameter is introduced to ensure termination of CGA generation at a certain point. To automatically get an optimal sec value, granularity is changed from 16 to 8 and the number of iterations to generate CGA is reduced. TB-CGA has better computational results compared to standard CGA.

In [40], another approach to improve the performance of CGA is proposed, and two major changes are implemented. First, replacing RSA and incorporating ECC and ECDSA (Digital Signature) for faster computation speed and second, using General Purpose Computing on Graphical Processing Unit (GPGPU) to reduce the generation time when a high Sec value is used. It has been proved that replacing RSA with ECC has drastically improved CGA performance. Finally, the impact of several hash functions were evaluated, recommending the use of SHA-2 for future implementations.

B. Monitoring Address configuration

The mechanisms proposed by analysts to monitor, mitigate and manage the protocols responsible for address configuration are reviewed in this section.

NDPMon [44] designed to monitor Neighbor discovery packets is an IPv6 version of ArpWatch with added functionalities. NDPMon deploys a third party tool on the network to monitor ND packets with an updated neighbor cache with timestamp. The ND packets are captured and analyzed with the entries in the monitoring database and incase of discrepancies or suspicious activities, alerts are raised and the report summary is sent to a preconfigured email address. Maintaining a third-party database and securing it against network vulnerabilities is a major setback offunctionality.

INDPMon (Intelligent Neighbor Discovery protocol Monitoring) [45] uses Extended Finite State Machines (EFSM) to detect anomalies in ND packets. A strict anomaly detection technique is deployed to monitor and investigate the behavior of NDP. Failure states are maintained in EFSM and contraventions to the normal behavior of the protocol arising due to misconfiguration or NDP attacks like DAD and flooding are reported. The major drawback of this approach is the it can only identify attacks that contradict the protocol constraints and other attacks dealing with illegitimate or spoofed IP address cannot be reported.

6MoN [47] is a plug and play network monitoring tool, used to automatically monitor and mitigate RAs. It monitors the RA messages sent by routers by inspecting and detecting advertisements sent by rogue routers with minimal configuration in the network.

C. Securing Address configuration

NDP plays a vital role in address transmission during the DAD process. Considerable research has been conducted by researchers to secure NDP either by adding new NDP options or by extending the NDP header. Below are the methods appropriate to autoconfiguration.

Secure Neighbor Discovery Protocol (SeND) [13], a security enhancement of NDP which adds a set of ND options to the standard ND protocol. Proof of address ownership, authorization of router and RSA signature options are added to protect NDP messages. RSA Signature option was introduced to protect ND and RD messages. Two more supplemental options Timestamps and Nonce are to prevent replay attacks. SeND implementers in [34] have proved that it is still exposed to DoS attacks and has rigid deployment complexities and high bandwidth consumption.

Internet Security Protocol (IPSec) [22] an innate protocol of IPv6 was devised to secure data transmitted in the IP layer. It extends the IPv6 header to include Encapsulating Security payload Header (ESP) and the Authentication Header (AH) to provide data integrity and confidentiality by authenticating and encrypting the data packets. In [35], the authors have conferred the shortcomings of IPSec policy mechanisms and concluded it to be inadequate especially in the context of authorization and has further suggested modifications to the existing facility.

Simple Secure Addressing Scheme (SSAS) [38] – SSAS was designed as an enhancement of SeND. RSA is replaced with Elliptic Curve Cryptography (ECC) algorithm for the address configuration. Signature and Timestamps options were included to block spoofing. Though SAAS method is lightweight and has curtailed processing time compared to SeND, the use of signatures and key exchange make it complex [39] subjecting it to DoS attack on DAD process due to the increased address configuration latency.

Duplicate Address Detection – Hash Function (DAD-h) [36] proposed has suggested to mask the target address during the DAD process to eliminate DoS attack and increase address autoconfiguration success rate. In the standard DAD process, the tentative address sent to verify uniqueness is multicasted in the network providing an ease for attacks. An attacker can send a spoofed reply and deny autoconfiguration of a node. In DAD-h, MD5 hashing is applied to the 128-bit tentatively generted address and the rightmost 64-bits are stored in a field called Hash_64. The Hashed target is multicasted and the original target is hidden. Studies have shown that MD5 Hash has high latency and is vulnerable to collision attack [37], [38].

Trust – Neighbor Discovery (Trust-ND) [30] reduces the processing time to secure DAD compared to the standard SeND. Trust-ND recommends new trust options containing Message Generation Time, Nonce and Message Authentication Data to be added in all NDP messages. It combines hashing function SHA-1 and trust options to ensure data integrity. In SeND the processing time at the sender end is high compared to the processing time at the receiver due to RSA signing at the sender. Trust-ND is considered as a lightweight security model as it not only reduces the computation time at the sending and receiving end but also consumes very less bandwidth. Researchers have justified that SHA-1 is sensitive to hash collision attacks [6], [31], [32] and since Turst-ND uses SHA-1 hashing for security it is considered to suffer from collision attacks.

Hash – Secure Target Address in DAD [33] (HSEC-Target-DAD) technique uses hybrid SHA-512 hashing and symmetric encryption (RSA). Each sending node generates public-private key pairs and hashed tentative address. The last 64-bits of the hash is embedded into the HASH-TARGET-64 option and tied to the NDP messages. The receiving node decrypts and compares the hash thereby eliminating unauthorized NA messages.

Duplicate Address Detection Match (DAD-Match) [6] has been suggested to secure the NS and NA of NDP during DAD process and identify whether the messages are initiated from legitimate users or not. A new option called DADmatch is incorporated to accomplish this. It comprises of Type, Length, Nonce, Random Integer and IPhash. It overcomes the drawbacks of Trust-NS [30] by using SHA-3 hashing and when compared to SeND and Trust-ND, DADmatch is more efficient and consumes less time.

Secure – Duplicate Address Detection (Secure-DAD) [10] was constructed to counter DoS attacks in DAD by overcoming the complexities of SeND, SSAS and Trust-ND. Secure-DAD is constructed on Universal hashing (UMAC) algorithm and recommends the addition of a secure tag option in NS and NA reciprocated during DAD. The secure tag contains a code to segregate the legitimate NS and NA messages from the fake ones.

Table – V: Summary of Proposed Mechanisms

Proposed Mechanisms	Year	Function	Additions/Modifications	Merits	Demerits
Cryptographically Generated Address (CGA)	2005	Binding public signature key to an IPv6 address to attain address ownership	Cryptographic hash function and 3-bit sec parameter to set security level of the address	Malicious node spoofing and address stealing more challenging	Not certified with very high computational cost especially when sec value increases and not feasible to replace address due to cost.
CGA++	2009	Enhancement to CGA to overcome its shortcomings and address security issues	Digital signature component added to resolve authentication issue	Authentication during address verification and prevention of time-memory trade-off attack	Increased computational cost during address generation and address renewal.
CGA with ECC + ESDSA & GPGPU	2010	Replace RSA to enhance performance of CGA generation	ECC + ESDSA and General Purpose Graphical Processing Unit	Faster computation speed and reduced generation time	Redesigning the standard CGA generation process
Time-Based CGA	2012	Limit time taken to generate CGA	Granularity changed to 8, Time parameter added to terminate CGA generation	No. of iterations of CGA generation reduced increasing speed	CGA verification still remains as standard CGA
Neighbor Discovery Monitoring (NDPMon)	2007	Monitoring NDP messages by capturing and inspecting	Third-party database to monitor NDP packets transmitted	Alerts raised and report generated for suspicious activity	Rely on a database server-single point of failure
6MoN	2012	Network tool to monitor and mitigate RAs	Minimal configuration in the network	Detecting RAs sent by rogue routers	Scope of monitoring is limited to routers.
Intelligent Neighbor Discovery Monitoring (NDPMon)	2015	Detecting anomalies in NDP messages by	Extended Finite state machines to detect anomalies	Detect messages contradicting to the normal behaviour	Vulnerable to address spoofing
Internet Protocol Security (IPSec)	1998	Securing data transmitted in the Internet layer	Extends header to include Encapsulating Security payload Header (ESP) and the Authentication Header (AH)	Data Integrity and Confidentiality by authentication and encryption	Lack of authorization and inadequate security
Secure Neighbor Discovery (SeND)	2005	Industry standard to Secure the Neighbor Discovery	Extended header with ND options like address ownership, router authorization, RSA signature, Timestamp, Nonce	Counteract Neighbor discovery message threats like DoS, Spoofing, authentication and authorization	Deployment Challenges and high computational cost, increased bandwidth consumption and security
Simple Secure Addressing Scheme (SSAS)	2013	Improve the standard SeND protocol	RSA replaced with Elliptic Curve Cryptography (ECC)	Lightweight with reduced processing time	Complexity due to signatures and key exchange mechanisms
Duplicate Address Detection – Hash Function (DAD-h)	2016	Hiding the target address sent in the ND message	MD5 hashing and Hash_64 field	Increased autoconfiguration success rate	High Latency and subjected to collision attack
Trust-Neighbor Discovery (Trust-ND)	2016	Improving and securing standard ND by using trust options	SHA-1 and Trust option with message generation time, Nonce and authentication data	Lightweight security model that ensures data integrity	Susceptible to collision attack due to the usage of SHA-1
Duplicate Address Detection Match (DAD-match)	2017	Securing DAD by identifying NDP message authenticity	DADmatch option with Type, Length, Nonce, Random Integer and IPhash	Efficient and less time consuming compared to SeND	Router related messages of NDP are still at risk of attacks
Secure Duplicate Address Detection (Secure-DAD)	2017	Segregating legitimate and fake NDP messages	Universal hashing UMAC and Secure tag option	Ability to secure DAD and segregate legitimate messages from fake messages	Processing overheads and bandwidth utilization in address verification
Hash-Secure-Target in DAD (Hash-Target-DAD)	2018	Secure Target address during DAD process	Hash-Target-64 option with SHA-512 hashing and RSA (Symmetric Encryption)	Hybrid encryption with tight security levels	Lengthy keys are required for increased security

VII. CHALLENGES AND COUNTERMEASURES

The demand in usage on internet has become a growing concern as it has resulted in the lack of trust among the internet user. The liberation of attacks and the demerits of the defensive mechanisms have made adapting to new technologies improbable. Stateless autoconfiguration grants a node to attach itself to a link, autoconfigure an address and initiate communication with peers without any registration or authentication at the site end. In spite of the several available methods to guarantee autoconfiguration, the challenges and vulnerabilities associated with it still remain and are subjected to profound research. The two major areas that remains as challenge in autoconfiguration are Security and Optimization. The challenges and the appropriate countermeasures are discussed in this section.

A. Stateless Autoconfiguration Security

Autoconfiguration imposes huge vulnerability threats in many situations especially during the address verification (DAD) process. Several researchers have generalized that the major cause for autoconfiguration failure in genuine situation is lack of authentic security during NDP message transmission, leading to DoS attack.

The systematically planned security defender SeND with CGA is unfortunately exposed to ruthless attacks during CGA verification and configuration process. The high computation complexity in generating CGA makes it impractical for address replacement which eventually results in privacy related attacks. The current methods have soaring communication overheads and elevated network bandwidth and resource consumption are the major root causes for the lack of awareness and support for SeND implementation is many operating systems. The survey conducted across the world-wide by [41] has concluded that predominant security attacks are in IPv6 networks compared to the others. Modification to the existing or constructing a new solution to secure NDP and defend it against attacks are in high demand and this has created scope for further research among the networking society.

B. Stateless Autoconfiguration Optimization

One of the major challenges in autoconfiguration is to optimize and improve the performance of the existing autoconfiguration process. Overall time taken for stateless address generation and verification (DAD), computation cost and bandwidth consumed are the factors that affect the performance of the system. An ideal autoconfiguration system is one that enables an interface on the link in a stateless manner within the stipulated time and limited resources. Most of the proposed solutions have severe performance degradation due to the nature of security rules applied. It is inferred from the literature that, security is inversely proportional to performance. When strict security is incorporated, the system performance is curtailed and when security is relaxed, optimal performance can be achieved.

C. Countermeasures

Based on the review of several mechanisms proposed by researchers and further analysis of the merits and demerits, autoconfiguration of a node/interface in an IPv6 network still remains at risk especially in terms of DoS attack. DoS attack, considered as the major threat to autoconfiguration, when mishandled would leave the autoconfiguration process unaccomplished. In order to guarantee autoconfiguration, two main areas are to be considered:

- First, securing the autoconfiguration procedure to allow eligible and legitimate interfaces to be enabled on the link.
- Second, optimizing the autoconfiguration process to increase the performance by reducing the computational cost and bandwidth consumption.

For securing the autoconfiguration process, the DoS attack during DAD has to be eliminated. The research society could combine the strengths of appropriately proposed DoS defensive mechanisms to construct a hybrid framework to secure DAD. The NDP messages transmitted during autoconfiguration should be monitored and secured using a lightweight encryption system and a collision free hashing technique. For optimization, the DAD process has to be quickened by shifting the scope of DAD check at the interface end to the router end, thereby tightening the security at the router and relaxing the security at the interface and ruling out DoS attack, computational overheads and bandwidth consumption.

VIII. CONCLUSION

Address autoconfiguration procedure in IPv6 networks, the challenges and threats encountered during the process have been showcased in this paper. NDP uses ICMPv6 messages to achieve autoconfiguration, the insecure nature of NDP exposes several vulnerabilities which are inevitable. This paper highlights the defensive mechanisms proposed by researchers against the Denial of Service (DoS) attacks which is thought-out as a major milestone for autoconfiguration. Though IETF has suggested enhancements like IPSec, SeND and CGA to secure the existing functionality, the intensive computational cost, bandwidth and deployment challenges involved in adapting to the new features are impractical. Before the full-fledged implementation of IPv6 protocol stack, NDP security attacks must be considered and hence the drawbacks and challenges in the current system have been meticulously investigated and authentic countermeasures have been recommended to frame a secured and optimized autoconfiguration process by extending the scope for further research in this field.

REFERENCES

1. S. Groat, M. Dunlop, R. Marchany, and J. Tront, “The privacy implications of stateless IPv6 addressing”, Proceedings of the Sixth AnnualWorkshop on Cyber Security and Information Intelligence Research, 2010, pp. 52.
2. A. S. Ahmed, R. Hassan and N. E. Othman, “IPv6 Neighbor Discovery Protocol Specifications, Threats and Countermeasures: A Survey”,
3. A. S. Ahmed, R. Hassan, N. I. A. Azami and N. E. Othman, “Impacts Evaluation of DoS Attacks Over IPv6 Neighbor Discovery Protocol”, Journal of Computer Science, 2019, pp. 702-727.
4. Anbar M, Abdullah R, Saad RMA, Hasbullah IH. Review of preventive security mechanisms for neighbour discovery protocol. Adv Sci Lett [Internet]. 2017 [cited 2018 Dec 7];
5. Al-Ani, AK, Anbar, M, Manickam, S & Al-Ani, A 2019, “DAD-match; Security technique to prevent denial of service attack on duplicate address detection process in IPv6 link-local network”, 2019.
6. Al-Ani AK, Anbar M, Manickam S, Al-Ani A and Leau Y-B, “DAD-match Security Technique based on Hash Function to Secure Duplicate Address Detection in IPv6 Link-local Network. dl.acm.org [Internet], 2017
7. S. U. Rehman and S. Manickam, “Significance of duplicate address detection mechanism in IPv6 and its security issues: A survey”, Indian J. Sci. Technol., 2015, vol. 8, no. 30, pp. 1-8.
9. E. Mahmood, A. H. Adhab and A. Al-Ani, “Review paper on neighbour discovery protocol in IPv6 link-local network”, “International Journal of Services Operations and Informatics”, Jan 2019
10. S. Ul. Rehman, S. Manickam, “Improved Mechanism to Prevent Denial of Service Attack in IPv6 Duplicate Address Detection Process”, International Journal of Advanced Computer Science and Applications”, Vol.8. (No.2), 2017; pp. 63–70.
11. A. Alsa’deh, H. Rafiee, and C. Meinel, “IPv6 stateless address autoconfiguration: Balancing between security, privacy and usability”, Foundations and Practice of Security (Lecture Notes in Computer Science), Berlin, Germany, Springer 2013, pp. 149-161.
13. Arkko J, Kempf J, Zill B and Nikander “RFC 3971 - Secure neighbor discovery (SeND)”, 2005
14. R. Hassan, A. S. Ahmed, and N. E. Osman, “Enhancing security for IPv6 neighbor discovery protocol using cryptography”, in Amer. J. Appl. Sci., vol. 11, no. 9, 2014, pp. 1472 - 1479.
15. X. Yang, T. Ma, and Y. Shi, “Typical DoS/DDoS threats under IPv6”, in Proc. Int. Multi-Conf. Comput. Global Inf. Technol. (ICCGI), 2007, pp.55.

16. F. Najjar, M. Kadhum and H. El-Taj, "Detecting Neighbor Discovery Protocol-Based Flooding Attack Using Machine Learning Techniques", Advances in Machine Learning and signal processing, Lecture Notes in Electrical Engineering, vol 387. Springer 2016, pp.129-139
17. A. S. Ahmed, R. Hassan and N. E. Othman, "Secure neighbor discovery (SeND): Attacks and challenges", IEEE, International Conference on Electrical Engineering and Informatics (ICEEI), 2017
18. A. S. Ahmed, R. Hassan, and N. E. Othman, "Improving security for IPv6 neighbor discovery," in Proc. Int. Conf. Elect. Eng. Inf. (ICEEI), 2015, pp. 271_274.
19. X. Yang, T. Ma, and Y. Shi, "Typical DoS/DDoS threats under IPv6," in Proc. Int. Multi-Conf. Comput. Global Inf. Technol. (ICCGI), 2007, p. 55.
20. A. M. Radwan, ``Using IPSec in IPv6 security," in Proc. 4th Int. MultiConf. Comput. Sci. Inf. Technol. (SIT), 2005, pp. 471_474.
21. "IPsec and its use in IPv6 environments", in Security in an IPv6 Environment. 2008, pp. 207_223.
22. S. Kent and R. Atkinson, "RFC 4301 - Security Architecture for the Internet Protocol", 1998.
23. R. Hassan, A. S. Ahmed, N. E. Othman, and S. Sami, "Enhanced encapsulated security payload a new mechanism to secure Internet protocol version 6 over Internet protocol version 4", Journal of Computer Science, vol. 10, no. 7, 2014, pp. 1344 - 1354.
24. S. Kent and R. Atkinson, "RFC 4301- Security Architecture for the Internet Protocol", 1998.
25. T. Aura, "RFC 3972 - Cryptographically Generated Addresses (CGA)", 2005.
26. M. Bagnulo and J. Arkko, "RFC 4581- Cryptographically Generated Addresses (CGA) Extension Field Format", 2006.
27. A. Alsa'deh, H. Ra_ee, and C. Meinel, "Stopping time condition for practical IPv6 cryptographically generated addresses," in Proc. Int. Conf. Inf. Netw., 2012, pp. 257_262.
28. J. W. Bos, O. Özen, and J. P. Hubaux, "Analysis and optimization of cryptographically generated addresses," in Information Security Berlin, Germany, Springer, 2009, pp. 17 - 32.
29. J. L. Shah & J. Parvez 2015, "Optimizing Security and Address Configuration in IPv6 SLAAC", Procedia Computer Science, Vol. 54, pp. 177-185.
30. Praptodiyono, S. Hasbullah, I. H. Kadhum, M. M. Wey, C.Y. Murugesan, R. K. Osman, "Securing duplicate address detection on IPv6 using distributed trust mechanism", International Journal of Simulation: Systems, Science and Technology, 17(26), 2016
31. Andreeva, E. Mennink, B. Preneel, "Open problems in hash function security", Designs, Codes and Cryptography. **77**(2–3), 2015, 611–631
32. T. Polk, L. Chen, S. Turner, P. Hoffman, "RFC – 6194 Security considerations for the SHA-0 and SHA-1 message-digest algorithms",2011
33. A. El Ksimi and C. Leghris, "Towards a new algorithm to optimize IPv6 neighbor discovery security for small objects networks", Security and Communication Networks" 2018.
34. A. S. Ahmed, R. Hassan, N. I. A. Azami and N. E. Othman, "Secure neighbor discovery (SeND): Attacks and challenges" International Conference on Electrical Engineering and Informatics, IEEE, 2017.
35. J. Arkko and P. Nikander, "Limitations of IPSec Policy Mechanisms", 11th International Workshop on Security Protocols, Cambridge, UK, 2003, pp. 241-251.
36. G. Song and Z. Ji, "Novel Duplicate Address Detection with Hash Function", PLoS ONE, 11(3), 2016.
37. Xie, T.; Liu, F.; Feng, D.: Fast collision attack on MD5. IACR Cryptol. ePrint Arch. 2013, 170 (2013)
38. H. Rafiee, and C. Meinel, "SSAS: A simple secure addressing scheme for IPv6 autoconfiguration", Eleventh Annual IEEE International Conference on Privacy, Security and Trust (PST), 2013, pp. 275-282
39. S. Praptodiyono, R. K. Murugesan, IH. Hasbullah, CY. Wey, MM. Kadhum and A. Osman, "Security mechanism for IPv6 stateless address autoconfiguration", IEEE International Conference on Automation, Cognitive Science, Optics, Micro Electro-Mechanical System, and Information Technology (ICACOMIT), 2015, pp. 31-36, 2015
40. T. Cheneau, A. Boudguiga and M. Laurent "Significantly improved performances of the cryptographically generated addresses thanks to ECC and GPGPU", Computers and Security, Elsevier, 2010, 29 (4), pp.419 - 431.
41. D. Anstee, C. F. Chui, P. Bowen, and G. Sockrider, "Worldwide Infrastructure Security Report", Burlington, MA, USA, Arbor Networks, 2013, vol. 11.
42. S. Guangxue, W. Wendong, G. Xiangyang, Q. Xirong, J. Sheng, and G. Xuesong, ``A quick CGA generation method," in Proc. 2nd Int. Conf. Future Comput. Commun. 2010, pp. V1-769_V1-773.
43. M. Moslehpour and S. Khorsandi, ``Improving cryptographically generated address algorithm in IPv6 secure neighbor discovery protocol through trust management," in Proc. 18th Int. Conf. Inf. Commun. Secur. (ICICS), 2016, pp. 1_5.
44. F. Beck, T. Cholez, 0. Fester, I.Chrisment, "Monitoring the Neighbor Discovery Protocol", IEEE Xplore, International Multi-Conference on Computing in the Global Information Technology, 2007.
45. F. Najjar, M. Kadhum and H. El-Taj, "Neighbor discovery protocol anomaly detection using finite state machine and strict anomaly detection", Proceedings of the 4th International Conference on Internet Applications, Protocols and Services (NETAPPS2015), 2015, pp. 967–978
46. P. Nikander, J. Kempf and E. Nordmark "RFC 3756 – IPv6 Neighbor Discovery (ND) Trust Models and Threats", 2004.
47. A. Gebrehiwot, M. Sommani, A. D. Vita and A.Manchini, "6MON: Rogue ipv6 router advertisement detection and mitigation and ipv6 address utilization Network monitoring tool", Terena networking Conference, 2012.
48. S. Hogg, "Securely Enabling ICMPv6 Router Advertisements on Your IPv6 Network",
49. M. Hollick, C. Nita-Rotaru, P. Papadimitratos, A. Perrig and S. Schmid, "Toward a taxonomy and attacker model for secure routing protocols", Computer Communication Review, 47(1), 2017, pp.43-48.
50. T. Chown and S. Venaas, "RFC 6104 - Rogue IPv6 Router Advertisement Problem Statement", 2011.

AUTHORS PROFILE

Rajula Angelin Samuel obtained her Bachelor of Engineering in Information Technology from Government College of Technology, affiliated to Anna University, Chennai, India. Then she obtained her M.Tech. in Computer and Information Technology from Manonmaniam Sundaranar University, Tirunelveli, India. Currently, she is a Full Time – Research Scholar in the Faculty of Information & Communication Engineering, at Anna University, Chennai. Her research interests include Computer Networks, Network Security Mobile Computing, Machine Learning and Data Mining.

D. Shalini Punithavathani is the Principal of Government College of Engineering, Tirunelveli, India. She received her B.Sc. in 1979 from Sarah Tucker College, affiliated to Madurai Kamarajar University, India, B.Tech. in Electronics in 1982 from Madras Institute of Technology, affiliated to Anna University, Chennai, India and M.E. in Computer Science and Engineering in 1990 from Government College of Technology, affiliated to Bharathiar University, Coimbatore, India. She got her Ph.D. entitled "Study and Implementation of IPv4 to IPv6 translation techniques" in 2010 from Anna University, Chennai, India. Her research interests include Computer Networks, Mobile Computing, Network Security and Data Mining.