scientific reports

OPEN

IPv6 addressing strategy with improved secure duplicate address detection to overcome denial of service and reconnaissance attacks

Gyanendra Kumar[1,6], Anil Gankotiya[2,6], Sur Singh Rawat[3,6], Balamurugan Balusamy[4,6] & Shitharth Selvarajan[5,6]✉

With technology development, the growing self-communicating devices in IoT networks require specific naming and identification, mainly provided by IPv6 addresses. The IPv6 address in the IoT network is generated by using the stateless auto address configuration (SLAAC) mechanism, and its uniqueness is ensured by the DAD protocol. Recent research suggests that IPv6 deployment can be a risky decision due to the existing SLAAC-based addressing scheme and the DAD protocol being prone to reconnaissance and denial of service (DoS) attacks. This research paper proposes a new IPv6 generation scheme with an improved secure DAD mechanism to address these problems. The proposed addressing scheme generates IPv6 addresses by taking a hybrid approach based on vendor id of medium access control (MAC) address, physical location, and arbitrary random numbers, which mitigates reconnaissance attacks by malicious nodes. To prevent the DAD process from DoS attacks, hybrid values of interface identifier (IID) are multicast instead of actual values. The proposed scheme is evaluated under reconnaissance and DoS attacks in the presence of malicious nodes. The evaluation results demonstrate that the proposed method effectively mitigates reconnaissance and DoS attacks, outperforming the EUI-64 and SEUI-64 schemes in terms of address success rate (ASR), energy consumption, and communication overhead. Specifically, the proposed method significantly reduces the average probing rate for scanning the existence of an IPv6 address, with only a 1% probing rate compared to SEUI-64's 5% and EUI-64's 100%. Furthermore, the additional communication overhead introduced by the proposed method is less than 13% and 11% compared to EUI-64 and SEUI-64, respectively. Additionally, the energy consumption required to assign an IPv6 address using the proposed method is lower by 12% and 5% when compared to EUI-64 and SEUI-64, respectively. These findings highlight the effectiveness of the proposed method in enhancing security and optimizing resource utilization in IPv6 addressing.

Small devices and the IoT have increased their stature in communication, creating opportunities for new dimensions of effective communication around the world. As is known, Internet communication devices and sensors require unique IPs to communicate with each other. Considering the problems of IPv4, IPv6 is defined in RFC 2460 as a better and more secure Internet protocol that is suitable for providing unique addresses of small devices and sensors in IoT networks. Additional functionality like IP security (IPSEC) in the IPv6 suite makes it more viable in an IoT environment[1].

The IPv6 protocol suite supports three types of address assignment: Manual, stateful auto address configuration, and SLAAC. In the manual configuration, the network administrator assigns the addresses to individual hosts and new network nodes. On the other hand, IPv6 stateful auto-configuration allows hosts to obtain interface addresses or configuration information and other parameters from servers called dynamic host configuration (DHCP) servers. Servers maintain a database that uniquely contains information about the

[1]Department of IoT and Intelligent Systems, Manipal University Jaipur, Jaipur 302034, India. [2]School of Computing Sciences and Engineering, Galgotias University, Greater Noida 203201, India. [3]Department of Computer Science and Engineering, J.S.S. Academy of Technical Education, Noida 201301, India. [4]Shiv Nadar University, Delhi-National Capital Region NCR, Delhi 201314, India. [5]School of Built Environment, Engineering and Computing, Leeds Beckett University, LS6 3QS Leeds, UK. [6]These authors contributed equally: Gyanendra Kumar, Anil Gankotiya, Sur Singh Rawat, Balamurugan Balusamy, and Shitharth Selvarajan. ✉email: shitharths@kdu.edu.et

various hosting IP addresses. In manual and stateful addressing, there is no requirement for verification of the uniqueness of the new address, as it is the responsibility of the administrator or servers[2].

The SLAAC process enables a host to assign addresses and is completed in two stages: first address generation and second uniqueness verification. In the literature, many stateless address-generation schemes are available. These stateless addressing schemes can be classified into three main classes: Extended Unique Identifier (EUI)-64[3], privacy addressing, and cryptography-generated addressing schemes[4]. The IPv6 address combines and contains two parts: a global prefix and a local prefix.

The global prefix of an address is obtained from the network router or coordinator, and it will be the same for all addresses in the network[5]. The local prefix, also known as the IID, is generated by the addressing scheme. The IID part must be unique inside a network, and it is ensured by DAD, which is a service provided by Neighbor Discovery Protocol (NDP)[6]. The EUI-64 address generation scheme is primarily used in IPv6 assignment but is accessible to reconnaissance attacks by attackers[7–9]. Reconnaissance attacks are conventional intelligence-gathering techniques that might be logistical or physical. These attacks gather information about the target network or system to attack it[10]. They collect threat intelligence from billions of vulnerable Internet-connected devices and use it to launch DoS attacks. A DoS attack is an attempt by the perpetrator to render a machine or network resource, such as a host linked to the Internet, inaccessible to users by disrupting services temporarily or indefinitely. The extended version of EUI-64, known as the Segment Extended Unique Identifier (SEUI-64), is introduced to mitigate reconnaissance attacks in the network. The standardized EUI-64 address generation scheme uses a 48-bit MAC address to form a 64-bit IID. The 64-bit IID is created by concatenating the first 24 bits of MAC, 16 bits as FEFF, and the last 24 bits of MAC. The problem is that the IID part of a device is permanently fixed across all links, which makes it vulnerable to reconnaissance attacks. An extended version, SEUI-64[11], is proposed to resolve this attack, which uses the part of the MAC address of the coordinator or gateway of the network to generate the IID of the first node joining the network and extends it by employing Fisher-Yates shuffle to generate other nodes' IIDs joining the same network link. The author claims that it mitigates the reconnaissance attack, but it does not follow the SLAAC configuration requirements for independent address generation. Many other IID generation schemes are available in the literature based on different methods and parameters. In[12,13], a coordinate-based strategy generates the unique address, but the coordinate-based IP address has some conflict issues when the two nodes are in the same device. Another method, Match-Prevention, is presented to protect the address resolution and DAD processes against DoS attacks while safeguarding the target address[14]. The P4DAD has been shown to secure the DAD process by filtering bogus NDP messages, masking the target node's address in the current network, and reliably responding with the (Neighbor Advertisement) NA message[15]. Keeping in mind a lightweight solution to prevent DAD from DoS attacks that use less bandwidth and processing time, the 64-bit Hash technique is described[16], which uses SHA-512 to secure the NA and Neighbor Solicitation (NS) messages by encrypting the new node's address and using hashed values of only 64 bits in the NA and NS messages.

The SLAAC-based addressing scheme uses the DAD process of NDP, which allows the node to configure a unique IP after verifying it with an existing host on the same link. Once the node generates the IID, it uses an NS message to multicast the IID or part of it into the network. The existing nodes of the network that have similar IIDs should reply using an NA message. If the new node does not receive any replies within the stipulated time, it will form an IP address by combining IID with a global routing prefix (GRP); otherwise, it will regenerate a new IID. The NDP has limitations on securing NS and NA messages. Any node acting as a single link in the conventional DAD approach can respond to each NS message multicast from the target host, exposing the DAD process to a DoS attack[17,18].One of the main problems encountered when using IPv6 in wearable and IoT devices is IPv6 address allocation privacy and security considerations[19]. Although the DAD function of the NDP certifies the validity of a self-generated IP address, there are issues with real bottlenecks affecting the DAD process when assigning the IP address for IoT devices[20]. The DoS attacks on the DAD are illustrated in Fig. 1. To ensure the uniqueness of the node address, It multicasts an NS message into the network, after which the attacking node on the other end responds with a fake NA claiming that the multicast IID is already in use. In the said situation, the new node will again regenerate the new IID and multicast it into the network; the attacker

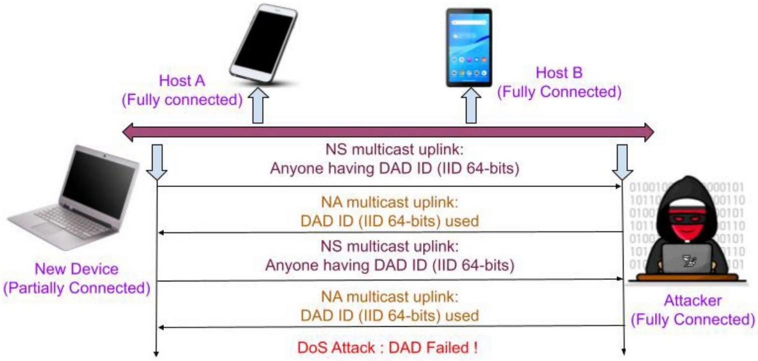

Fig. 1. A DoS attack on DAD. When a DAD is subjected to a DoS attack, the new device is prevented from configuring any address.

can continue the attack by sending another NA message indicating that the IID has already been used. As a result, the new device cannot identify any IPv6 addresses with which its interface may be configured. To improve the basic DAD, improve DAD[21], enhance DAD[22], secure DAD[23], P4-DAD[24] and DAD-h[25,26] are presented. In Improved DAD[21], the new node only multicasts a portion of the address so that the existing attacker does not get the multicast IID, but if the new node itself turns out to be an attacker, it can expose a challenge to the system.

In enhanced DAD[22], looped-back NS is detected when the two nodes are sending the same address, but after this, the network manager improves the network manually. In[24], a hash function is used in the DAD process to generate the address to the node without leaking the target DAD address, where DAD-h is to eliminate the DoS attack. To protect NDP, RFC 4861 suggested the IPSec[27] and SeND[28] algorithms in which IPsec suffers from bootstrapping and SeND loaded to complexity[29]. In the secure DAD, the address is divided into DAD ID, secret ID, and node ID, where DAD ID and node ID are used to multicast, and secret ID does not participate in the address generation process.

This research work proposed an improved secured DAD, which is based on the hybrid approach for address generation where encrypted hybrid ID is multicast into the network to address the reconnaissance and DoS attacks. The improved secure DAD, the DAD ID, and the secret ID are used to form an encrypted hybrid ID. This hybrid ID is multicast and in reply, the encrypted node ID is used, which mitigates DoS attacks and improves the latency along with reducing the addressing cost. The following are the main objectives and contributions of this paper:

Objectives

- To address the security vulnerabilities in the SLAAC mechanism of IPv6 networks.
- To address the security vulnerabilities in the DAD protocol of IPv6 networks.
- To develop a new IPv6 generation scheme with an improved secure DAD mechanism.
- To evaluate the effectiveness of the proposed scheme in mitigating DoS and reconnaissance attacks.

Contributions

1. Conducted a background study and literature review about the IPv6 address generation scheme, DoS attacks on the IPv6 addressing process, and Reconnaissance attacks such as identity revealing, location tracking, correlation of activity, etc.
2. Proposal of a novel hybrid IPv6 address generation scheme that combines the MAC address, physical location, and arbitrary random numbers. This scheme mitigates address prediction and secures device information from reconnaissance attacks by malicious nodes.
3. Development of an improved secure DAD mechanism to enhance security against reconnaissance and DoS attacks.
4. Performs extensive evaluation of proposed addressing and DAD process under the presence of malicious nodes, and results reveal the following outcome:

   (a) The proposed scheme and DAD process successfully mitigate the reconnaissance and DoS attack.
   (b) Successfully assigns IPv6 addresses to all nodes without addressing conflict.
   (c) The proposed work outperforms existing EUI-64 and SEUI-64 in terms of successful scanning of IPv6, ASR, communication overhead, and energy consumption.The rest of the research work is organized as follows. "Literature review" reveals the existing literature work and the proposed addressing and DAD scheme is described in "Proposed FEUI-64 scheme and improved secure DAD". The mathematical analysis is presented in "Analysis", whereas the experimental evaluation under reconnaissance and DoS attacks of the proposed work is presented in "Experimentation, results and discussion". Finally, the conclusion is presented in "Conclusion and future scope".

Literature review

The proposed methodology is built upon a comprehensive review of existing research in the field. The following papers have been considered as the foundation for the design of the proposed methodology:

In the SLAAC-based IPv6 addressing EUI-64 is primarily used to generate tentative address and the DAD process verifies the uniqueness and after verification address is made as assigned. However, the address generated by EUI-64 remains unchanged across the different networks, making it vulnerable to different reconnaissance attacks. The design flaws of the DAD process also suffer from DoS attacks which make the IPv6 assignment process fail[2,19]. To address these issues there are many works already available in literature and some key works are described in the following paragraphs.

Abdullah[11] 2019, proposes the SEUI-64 addressing strategy as a solution to mitigate reconnaissance attacks in IPv6 networks. The novelty of the proposed method lies in its utilization of the MAC address of coordinator nodes, followed by address shuffling, to generate IPv6 addresses. The results indicate that SEUI-64 provides improved resistance against reconnaissance attacks compared to existing addressing schemes.

Asati et al.[7] 2015, presents the RFC 7527, which introduces an enhanced DAD mechanism for IPv6 networks. The proposed method enhances the existing DAD protocol by introducing additional checks and optimizations to improve address uniqueness and mitigate potential address conflicts. The novelty of this work lies in the enhanced DAD mechanism, which ensures the uniqueness of IPv6 addresses and improves network reliability.

Al-Ani et al.[17,20] 2018, 2019, introduces a security technique called DAD-match to prevent DoS attacks on the DAD process in IPv6 link-local networks. The proposed technique enhances the security of the DAD process by introducing additional checks and mechanisms to detect and mitigate potential DoS attacks. The novelty of this work lies in the DAD-match technique, which ensures the integrity and availability of the DAD process in IPv6 networks.

Ahmed et al.[4] 2021, investigate the use of cryptographically generated addresses (CGA) in IPv6 networks and analyze their effectiveness in terms of security, optimization, and protection. They discuss the design and implementation of CGA and evaluate its performance and security features through experimental analysis. The paper highlights the advantages of using CGA in mitigating security threats such as address spoofing and DoS attacks. Additionally, the authors propose optimizations to enhance the efficiency and practicality of CGA deployment.

He et al.[24] 2021, present a novel approach for securing DAD using the P4 (Programming Protocol-Independent Packet Processors) language. Their research focuses on enhancing the security of DAD, a critical process in IPv6 networks, by leveraging programmable data planes. The authors propose a secure DAD framework that utilizes P4-based switches to perform efficient and reliable address verification. Through extensive experiments and evaluations, they demonstrate the effectiveness of their approach in preventing address spoofing attacks and ensuring the integrity of DAD.

Dou et al.[12] 2019, propose a coordinate-based addressing scheme for Mobile Ad hoc Networks (MANETs) to enhance the efficiency and scalability of address assignment. Their research addresses the challenges of address management in MANETs by utilizing geographic coordinates as identifiers for network nodes. The authors develop a hierarchical addressing structure that allows for efficient routing and location-based services in MANETs. Through simulations and comparisons with traditional addressing schemes, they demonstrate the advantages of their approach in terms of reducing address overhead and improving the overall network performance.

Kumar et al.[23,30,31], present an IPv6 addressing scheme that incorporates a secure DAD mechanism. Their research focuses on mitigating the risks associated with duplicate addresses in IPv6 networks by enhancing the traditional DAD process. The proposed scheme employs partial multicasting of IID to ensure the uniqueness of assigned addresses and protect against address conflicts. Through simulations and analysis, the authors demonstrate the effectiveness of their approach in preventing address duplication and improving the overall security of IPv6 networks. This study contributes to the ongoing efforts in developing secure addressing schemes for IPv6 deployment.

Song and Ji[25] 2016, propose a novel approach for DAD in IPv6 networks using a hash function. Their research focuses on improving the efficiency and accuracy of the DAD process by introducing a hash-based algorithm. The proposed method leverages the properties of hash functions to generate unique identifiers for IPv6 addresses, eliminating the need for additional communication overhead during address assignment. Through extensive experiments and analysis, the authors demonstrate the effectiveness of their approach in detecting and preventing duplicate addresses reliably and efficiently. This study contributes to the advancement of DAD techniques in IPv6 networks, providing a promising solution for addressing conflict resolution.

Mavani and Asawa[26] 2018, present a privacy-preserving approach for IPv6 address auto-configuration in the context of the IoT. Their work addresses the privacy concerns associated with the traditional SLAAC mechanism by introducing a novel privacy-preserving scheme. The proposed scheme aims to protect the privacy of IoT devices by preventing the exposure of their network identifiers during the auto-configuration process. By leveraging cryptographic techniques and anonymous identifiers, the authors demonstrate how the proposed scheme can effectively mitigate the potential risks of address-based tracking and profiling in IoT deployments.

Kumar and Tomar[17] 2021, propose a stateless spatial IPv6 address configuration scheme specifically designed for IoT applications. The scheme aims to provide efficient and scalable address auto-configuration while considering the spatial characteristics of IoT devices. By utilizing the geographic information of devices and leveraging spatial algorithms, the proposed scheme enables the automatic assignment of unique IPv6 addresses to IoT devices without relying on centralized servers or stateful protocols. The research, presents the design, implementation, and evaluation of the proposed scheme, showcasing its effectiveness in supporting large-scale IoT deployments with reduced communication overhead and enhanced address uniqueness. The work contributes to the field of IoT address configuration by offering a spatially-aware and stateless approach to address assignment in IoT networks.

Ibrahim et al.[32] 2022, presents a novel concept for DAD processes in IPv6 link-local networks. The authors address the limitations of existing DAD mechanisms in scenarios where multiple devices attempt to configure the same address simultaneously. The proposed concept introduces a modified DAD algorithm that combines local uniqueness and network-wide uniqueness checks to ensure the uniqueness of IPv6 addresses in the link-local network. The paper elaborates on the design and implementation of the proposed concept, providing detailed insights into its operation and performance evaluation. The novelty of the research lies in the innovative approach to address conflicts and enhance the reliability of address assignments in link-local environments.

Song et al.[33] 2022, proposes an anti-DoS DAD model. The authors address the vulnerability of DAD processes to DoS attacks, where malicious entities flood the network with duplicate address claims, leading to service disruption. The proposed model introduces enhanced security measures to mitigate such attacks and ensure the integrity and availability of address assignments in IPv6 networks. The paper presents the design and implementation details of the anti-DoS DAD model, highlighting the key features and mechanisms employed for attack detection and prevention. The experimental results demonstrate the effectiveness of the proposed model in mitigating DoS attacks and improving the overall reliability of DAD processes.

Li et al.[34] 2022, presents a novel approach called P4-NSAF for defending IPv6 networks against ICMPv6 (Internet Control Message Protocol version 6) DoS and Distributed Denial of Service (DDoS) attacks. The authors address the vulnerability of IPv6 networks to such attacks, which can cause service disruption and network congestion. The proposed P4-NSAF utilizes the programmability of the P4 language to enhance the network's ability to detect and mitigate ICMPv6-based DoS and DDoS attacks. The paper discusses the design and implementation of P4-NSAF, highlighting the key mechanisms and algorithms used for attack detection and mitigation. Experimental results demonstrate the effectiveness of P4-NSAF in defending against ICMPv6 DoS and DDoS attacks, providing improved network security and stability. The research contributes to the field of network security by leveraging P4 programmability to enhance the resilience of IPv6 networks against ICMPv6-based attacks.

Seth et al.[35] 2023, propose a novel approach called DADCNF for diagnosing the threat of DAD in networks using Conjunctive Normal Form (CNF). The authors address the challenges of identifying and mitigating DAD-related issues, which can lead to address conflicts and disruptions in network operations. The DADCNF approach leverages CNF, a logical representation format, to analyze the conditions and rules associated with DAD processes and identify potential threats. The paper discusses the design and implementation of DADCNF, highlighting the use of CNF-based diagnosis techniques to identify vulnerabilities and propose mitigation strategies. Experimental results demonstrate the effectiveness of DADCNF in accurately diagnosing DAD threats and facilitating prompt action to prevent address conflicts.

Guangjia et al.[36] 2019, propose a method to prevent DoS attacks in IPv6 networks by utilizing multi-address generation and DAD. The authors address the vulnerability of DAD processes to DoS attacks, which can disrupt network operations and compromise network availability. The proposed method involves generating multiple addresses for a device and conducting DAD for each address independently. By implementing this approach, the authors aim to distribute the impact of DoS attacks across multiple addresses, thereby reducing the potential for a successful attack. The paper presents the design and implementation details of the multi-address generation and DAD scheme, highlighting its effectiveness in preventing DoS attacks. Experimental results demonstrate the improved resilience of the proposed method compared to traditional DAD approaches.

Wang et al.[21] 2016, propose an improved DAD mechanism for 6LoWPAN networks. The authors address the limitations of the traditional DAD process in 6LoWPAN, which can lead to increased communication overhead and delays in address assignment. The proposed method introduces an optimized DAD algorithm that reduces the number of DAD messages exchanged and minimizes the time required for address verification. By optimizing the DAD process, the authors aim to improve the efficiency and scalability of address assignment in 6LoWPAN networks. The paper presents the design and implementation details of the improved DAD mechanism and evaluates its performance through simulations. The results demonstrate the effectiveness of the proposed approach in reducing communication overhead and enhancing the address assignment process in 6LoWPAN networks. The research contributes to the advancement of addressing mechanisms in 6LoWPAN, enabling more efficient and reliable communication in resource-constrained IoT environments. Table 1 presents the key IPv6 addressing strategy with the DAD method, which outlines respective advantages and disadvantages.

Method	Advantages	Disadvantages
EUI-64[3]	EUI-64 provides a vast 64-bit address space, reducing address conflicts and simplifying IPv6 address creation from MAC addresses. Its IEEE standardization ensures compatibility across various devices.	EUI-64 can raise privacy concerns by revealing device MAC addresses. Prone to reconnaissance attacks, fixed format may not suit all network scenarios, and its limited flexibility can be a drawback for custom address management
Basic DAD[2]	Protect Duplicacy of the address of the nodes, Simple and Lightweight.	Multicast Full IID, Any malicious node inside the network can claim to have the same address as the new node, Prone to DoS attacks, Privacy of address, and a new malicious node can join with a conflicting address
Modified EUI-64[37]	Enhances privacy by obscuring the direct mapping of MAC addresses to IPv6 addresses, reducing tracking and privacy breaches, and less predictable, mitigating reconnaissance attacks	Additional computational overhead, does not entirely eliminate privacy and security risks, may require updates to existing systems, and prone to reconnaissance attacks
SEUI-64[11]	Improved resistance against reconnaissance attacks compared to existing addressing schemes	Low ASR, stateful addressing, high computational overhead, the possibility of reconnaissance attacks
Enhanced DAD[7]	Mitigates the loopback of NS DAD message by adding a nonce	Security issues of Basic DAD still exist
DAD-Match[17,20]	provides a simple, light security system to prevent external DoS attacks during the DAD operation in an IPv6 link-local network	Only protects from outsider attacks but fails when an internal node is an attacker
CGA-Lighter[4]	Uses MD5 instead of Hashing, Lightweight, Protect from external attacks	High Computation, Does not protect from internal attacks
P4DAD[24]	Block fake NDP messages inside the network to protect DAD against denial-of-service attacks	It does not stop malicious nodes from performing attacks; instead detects and defends them
Improved DAD[21]	Protect Duplicity of the address of the nodes, Simple and Lightweight. Partial Privacy of address is ensured; existing malicious nodes cannot spoof tentative addresses.	IID of existing nodes exposed to the new node. A malicious node can join with the conflicting IPv6.
Secure DAD[23,30,31]	mitigate the DoS attacks, Lightweight, preserve the privacy of address	Issue in standard compliance, Partially preserve privacy, Enhancement required to overcome overhead, energy consumption
DAD-h[25]	High ASR under attack, does not need external hardware or a lot of computer power, and lightweight security solution.	It doesn't protect address privacy from existing nodes; hence vulnerability of claiming tentative IID
EPUI[18]	Unpredictable IPv6 generation, Lightweight, Mitigates reconnaissance attacks	Does not protect from DoS attacks.
FDIPA[13]	High ASR, low overhead and energy consumption, compatible with geographical routing	No protection against DoS attacks, Technological limitations
Ibrahim et al.[32]	Simple verification will indicate the presence of neighbors	It protects only sending NS messages by illegitimate node
P4-NSAF[34]	Defend against flooding attacks and source address spoofing attacks	It doesn't prevent the attacks of internal malicious nodes
DADCNF[35]	Simple, with low overhead, no change in protocol needed, minimal resource consumption, less processing time	Detection is required, which adds extra burden, Detect and defend; does not prevent

Table 1. A summary of key IPv6 addressing and DAD methods to handle the different kinds of attack.

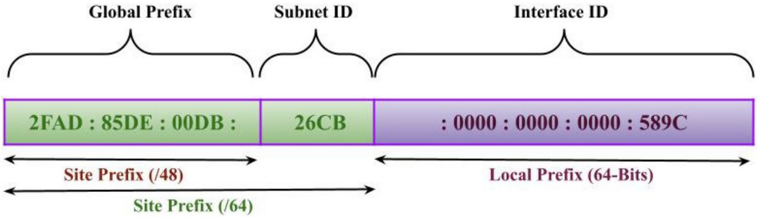

Fig. 2. Global unicast IPv6 address.

Part	Name	Length	Sourcs
1	CVTag	3 Bytes	Coordinate Value Tag: x y z coordinate values set
2	VID	3 Bytes	Vendor identifier part is the network interface's MAC address XOR with time-stamp at IID generation
3	RID	2 Bytes	Randomly generated ID

Table 2. Interface ID parts.

Despite the valuable contributions made by these studies, there remains a research gap regarding the reconnaissance and DoS attacks in the context of IPv6 addressing. Specifically, more attention could be given to identifying and mitigating potential reconnaissance attacks targeting the EUI-64-based addresses and the DAD process. Existing Secure DAD methods are primarily focused on preventing external attacks and do not adequately address internal attacks that occur during the matching process of the multicast IID with the existing node's IID. Normal matching can reveal the multicast IID to the existing node even if it is encrypted, allowing the existing node to spoof the new node with a misleading match response. Other types of DAD methods that work based on detection and defense are costly in terms of both resources and efficiency. Some methods use partial IID information and do not rely on matching information from existing nodes. While these methods offer partial protection from internal attacks, there is still significant room for improvement in ensuring comprehensive security Additionally, further research is needed to develop robust mechanisms to defend against sophisticated DoS attacks that specifically target the DAD process, ensuring uninterrupted address assignment and network operation. Addressing these research gaps will contribute to the development of more secure and resilient IPv6 addressing schemes, ensuring lower communication overhead and energy consumption for efficient network services.

Proposed FEUI-64 scheme and improved secure DAD

Proposed Ipv6 addressing scheme

This section proposes a new Fragmented Extended Unique Identifier FEUI-64 addressing scheme that mitigates the limitations of the SEUI-64 and EUI-64 addressing approaches. Its primary goal is to generate IPv6 addresses for nodes attached to the network interfaces so that an attacker should not correlate the different activities of a node with the generated address without violating specified standards of SLAAC.

Description of the autoconfiguration

The literature analysis of the SLAAC method proved that it performed well in resource-constrained networks. It uses NDP to perform different auto configuration activities when a node is connected to the network. The objective of the proposed auto-configuration scheme is to assign a unique IPv6-this requires several improvements, including link-local IPv6 address design and global unicast IPv6 addressing. The general address format of IPv6 is illustrated in Fig. 2, where it is divided into two sections which are global and local prefixes.

The proposed FEUI-64 to create the IPv6 addressing and connect it to another node are discussed following steps.

1. In the first step, prepare the IID using the FEUI-64 addressing scheme for producing a link-local IPv6 address.
2. In the second step, a Neighbor Solicitation (NS) message is multicast to determine the uniqueness of the address using the proposed improved secure DAD process.
3. In the last steps, theIPv6 address will be formed by combining GRP and IID for the interface if it is unique.

The proposed FEUI-64 scheme is recommended as an improved version of the existing approach of EUI-64 and SEUI-64 to mitigate the reconnaissance attack. This solution avoids the attacker's discovery of easily observed MAC address-based IID construction. Therefore, the proposed IID is based on coordinate values, modified MAC values using a time-stamp, and randomly generated ID, which help to create unique addresses and reduce address scanning, correlation of device activities, and tracking. It is started mainly by a node generating an IID, which would be used to create the unique link-local and global unicast IPv6 addresses-stimulating FEUI-64 just before starting SLAAC guarantees optimum execution efficiency and randomization, including link-local and global IPv6 addresses.

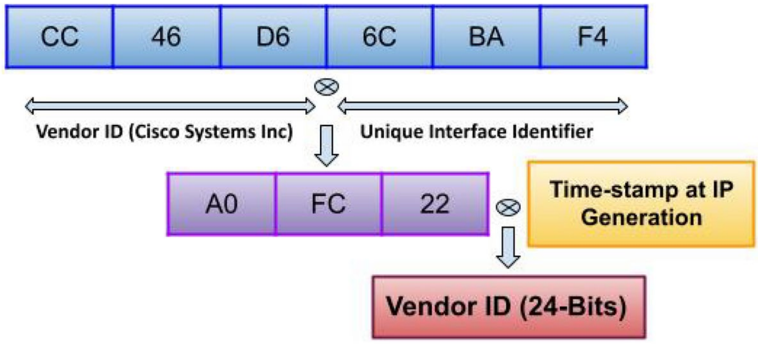
CC
46
D6
6C
BA
F4
Vendor ID (Cisco Systems Inc)
Unique Interface Identifier
A0
FC
22
Time-stamp at IP Generation
Vendor ID (24-Bits)

Fig. 3. Vendor ID generation using unique MAC address.

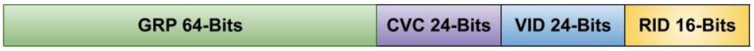

Fig. 4. FEUI IPv6 address format.

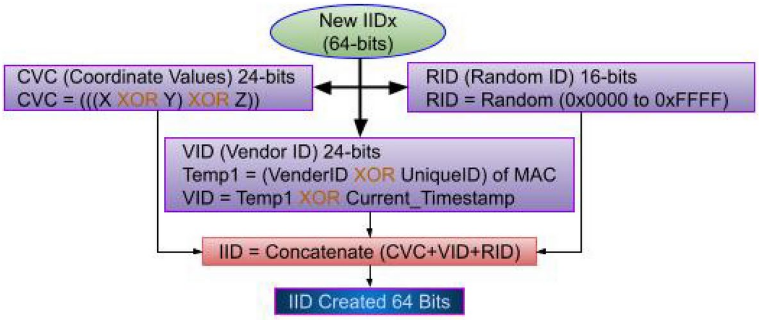
New IIDx
(64-bits)
CVC (Coordinate Values) 24-bits
CVC = (((X XOR Y) XOR Z))
RID (Random ID) 16-bits
RID = Random (0x0000 to 0xFFFF)
VID (Vendor ID) 24-bits
Temp1 = (VenderID XOR UniqueID) of MAC
VID = Temp1 XOR Current_Timestamp
IID = Concatenate (CVC+VID+RID)
IID Created 64 Bits

Fig. 5. Phase -1 IID creation.

Class	Context	Multicast	Address type
0	GRP	AR or Fully connected	Interface address
1	XOR value	Partially connected	Tentative address

Table 3. Beacon frames expansion.

Class	Context	Unicast	Address type
0xE	Node ID	Fully connected	Interface address
0xF	Node ID	Partially connected	Tentative address

Table 4. Command frames expansion.

IID generation

In this proposed scheme, the IPv6 address is generated by the combination of multiple IDs, which is based on the Coordinate Value Code (CVC), Vendor Identifier (VID), and random ID (RID), as depicted in Fig. 4 and Table 2 where the IID generation flow chart is illustrated in Fig. 5. The FEUI-64 algorithm picks CVC based on node physical location and Vendor Identification part of MAC, whereas the remaining bits are randomly generated ID. This IID part focused on unpredictable value and unique address representation. All of these components are explained in Table 2. The CVC, which is three bytes long, is the first portion, where the x, y, and z coordinate value set is the physical location value. As the physical location of any device does not remain the same, therefore, XOR values of x,y, and z coordinates represent the 3-bytes values. The attacker could not predetermine them. The XOR value of x,y, and z is calculated, and 3 Byte LSB values are considered CVC. The 3

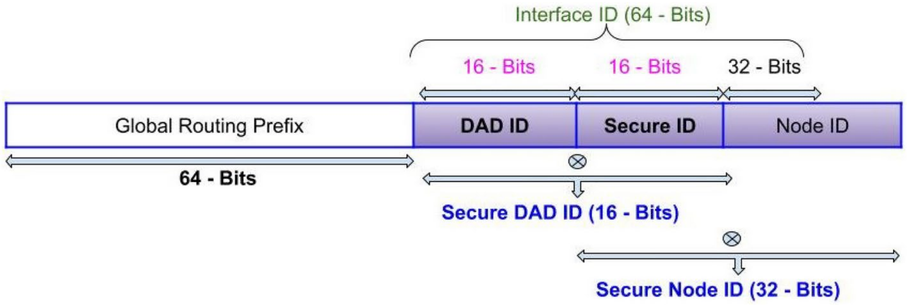

Fig. 6. IID format for DAD.

bytes VID are generated in two steps where the first step is evaluated through the first three bytes of a network interface's MAC address with XOR of the last three bytes of the MAC address. In the second step, this value is XOR with the current time-stamp to generate the VID, as depicted in Fig. 3. The final part is 2 bytes randomly generated ID (RID) limited to arbitrary bytes. The randomly generated ID is a 16-bit (2-byte) string that is chosen at random each time when a new interface ID is created. The whole process of FEUI-64 IID generation is explained in Algorithm 1.

```
Input:Device Location, MAC Address, IID Generation
Timespam
FEUI64(Device_Location, MAC_Address)
$X \leftarrow XCoordinate\_Values(Location)$
$Y \leftarrow YCoordinate\_Values(Location)$
$Z \leftarrow ZCoordinate\_Values(Location)$
$CVC \leftarrow (((X\ XOR\ Y)\ XOR\ Z))$
$Temp1 \leftarrow ((VendorID\ XOR\ UniqueID)\ ofMAC$
$VID \leftarrow ((Temp1\ XOR\ Current\_Timestamp)$
$RID \leftarrow Random(0x0000, 0xFFFF)$
$IID \leftarrow Concatenate(CVC, VID, RID)$
```

Algorithm 1. IID Creation using FEUI - 64

Flow chart of FEUI-64 addressing scheme

The proposed IPv6 allocation scheme is elaborated in different phases using the flowchart as shown in Fig. 5. In phase-1, the IID creation is divided into three parts CVC (3 bytes), VID (3 bytes), and RID (2 bytes), which is obtained through the XOR value of the variables in different regions to provide uniqueness in IID construction. This makes the created IID unpredictable as compared to EUI-64 and SEUI-64. This process makes it novel and unique.

The proposed improved secure DAD

In this paper, the improved secure DAD is also proposed to mitigate the DoS attack. After the IID generation, the new node completes the DAD process in three steps. The proposed improved secure DAD scheme method is based on the IoT, wearable, WSN, and portable nodes in the network in which there may be three types of nodes: fully connected, partially connected, and new. The AR is used to connect these nodes to the IPv6 network. The fully connected node has completed its DAD process and is assigned with a unique IPv6, whereas the partially connected node has recently begun the DAD process and the new node. Just so you know - the process was completed with the expended beacon frames[21] illustrated in Tables 3 and 4. The detailed description of the proposed DAD process is explained in the following sub-sections.

```
Input:GRP, BC_DADID, AS_Category, Node_Class,IP,NFR, BC_DADID_list, NSFB, F_Class, DAD_Counter
Step 1:
IPv6_Creation(GRP, BC_DADID, AS_Category, Node_Class)
$Node\_Class \leftarrow Partially\_Connected$
if $(AS\_Category == x)$ then
    $IID \leftarrow FEUI64(DeviceLocation, MACAddress)$;

else
    $IID \leftarrow Any\_other\_address\_scheme()$;
end
$DADID \leftarrow substring(IID, 0, 15)\ XOR\ substring(IID, 16, 31)$
if $(compare(DADID, BC\_DADID\_list))$ then
    Goto Step 1:
else
    if $(NSFB == Class\_1)$ then
        NS Frame Multicast (Table-1)
    end
    while $(Time\_Out \neq True)$ do
        if $(NFR == True)$ then
            if $(F\_Class == 0xF1\ and\ RID == RID\_Res)$ then
                $RID = Distinct\_Random\_Value(RID\_Res)$  $IID = Merge(substring(IID, 0, 15),$
                $substring(IID, 16, 31), RID)$
            else
                if $(F\_Class == 0xE1\ and\ RID == RID\_Res)$ then
                    $IncreaseDAD\_Counter$
                    if $(DAD\_Counter < Max\_DAD)$ then
                        Goto Step 3:
                    else
                        Record IP Creation Fault
                    end
                end
            end
        end
    end
end
$IP = Merge(GRP, IID)$
$Node\_Class = Fully\_Connected$
$ReturnNode\_Class$
```

Algorithm 2. Proposed DAD process for Unique IP

Improved secure DAD

In improved secure DAD, it is assumed that a new node attempts to join the existing network. It first gets GRP by sending Class-0 beacons frame to access router (AR), then constructs IID and deploys a unique address using the proposed DAD method, which is elaborated below:

Step-1: A new node creates a 64-bit IID using the FEUI-64 addressing scheme and then divides the generated IID into three components, 16-bit DAD ID, 16-bit Secure ID, and 32-bit Node ID, as shown in Fig. 6. Then, in a class-1 message, it multicasts the XOR value of DAD ID with Secure ID and assigns a temporary link address (TLA) as a source address and designates itself a partially-connected node. Before multicasting a class-1 frame, the following needs must be fulfilled.

Case 1: The newly formed DAD ID should not be identical to DAD IDs obtained by the class-1 beacon.

Case 2: The new node can run the DAD process as many times as allowed; otherwise, it will record a configuration error.

Step-2: If the XOR value of DAD ID with Secure ID of the fully and partially connected nodes on the network is the same as the XOR value of the received Class-1 frame that was multicasted by the new node, then both types of nodes will unicast their XoR of Secure ID and Node ID to the new node via the Class-0xE and 0xF frame.

Step-3: If the new node does not receive class-0xE or 0xF frames within an allotted period, it proceeds to step 4. Otherwise, it will work according to the following guidelines:

Action 1: If the node-ID of the new node does not match any of the node IDs obtained in the Class-0xE frame (XoR values), it is recommended to proceed to step 4.
Action 2: If the Node-ID of the new node is different from the Node-ID of any partially connected node but the same as the Node-ID of the fully connected node, the new node creates another distinct new Node-ID and proceeds to step 4.
Action 3: If the new node's Node ID is the same as any of the partially-connected nodes, then the process returns to step 1.

Step-4: By integrating GRP with IID, a new node announces itself as fully-connected and starts using an IPv6 address for further communication in the network.The proposed improved secure DAD process is explained using Algorithm 2 and Algorithm 3. Algorithm 2 is used by the new node to multicast part of the newly generated IID, and Algorithm 3 is used by the existing node to verify the uniqueness of the IID.

```
Input:NSFR, IPv6_addresses, Node_Class
Validation_Frame (NSFR, IPv6_addresses, Node_Class)
if $(NSFR == Class\_1)$ then
    while $(IPv6\_addresses! = Null)$ do
        $IPx = Address\ Extracted\ from\ IPv6\_addresses$
        $DAD\_IDx = substring(IID, 0, 15)\ XOR\ substring(IID, 16, 31)$
        $RID1 = (substring(IIDx, 32, 47)\ XoR\ sbstring(IIDx, 16, 31)$
        $RID2 = substring(IIDx, 48, 63)\ XoR\ substring(IIDx, 16, 31)$
        RID = RID1 concatenate RID2
        if $(DAD\_IDx == DADID\_Res)$ then
            if $(Node\_Class == Fully\_Connected)$ then
                Acknowledge NA Frame_Class as 0xF1 with RID
            else
                Acknowledge NA Frame_Class as 0xE1 with RID
            end
        end
    end
    $Return\ Frame\ Validated$
else
    $Ignore\ NS\ Frame$
end
```

Algorithm 3. Validation using NS and NA Frames

Flow Chart of Proposed DAD process
The flow chart of the proposed DAD protocol is shown in Figures 7 and 8. Figure 7 is the flow of different steps to send NS frame along with XOR value of DAD ID and Secure ID of IID, and waiting for a response from the existing node for IPv6 assignment. In Figure 8, the steps performed by the existing node are shown.

The complexity of proposed method

The running complexity of the proposed work in assigning a unique address to a node depends upon the severity of the DoS attack and the uniqueness of generated tentative IPv6. The worst-case complexity of the algorithm is O(Dn), and the best case complexity is O(1). Here Dn is the number of times the DAD process is repeated to assign unique IP. The proposed method mitigates the reconnaissance and DoS attack; hence it maximizes the chance to assign IP in the first attempt to achieve best-case complexity.

Analysis

This paper has analyzed the performance of the proposed addressing scheme and DAD process based on four metrics, i.e., ASR under DoS attack, Reconnaissance attack, Added Communication overhead, and Energy consumption. The proposed addressing and DAD scheme is analyzed according to the metrics in WSN, IoT, and Mesh Network, whereas evaluation is performed in the next section.

Address success rate (ASR) DoS attack

The ASR of an addressing scheme is defined as the ratio of the number of successful allocations of IPv6 addresses to all nodes in the network to the total number of attempts for allocations, i.e., the sum of successful and unsuccessful allocations.

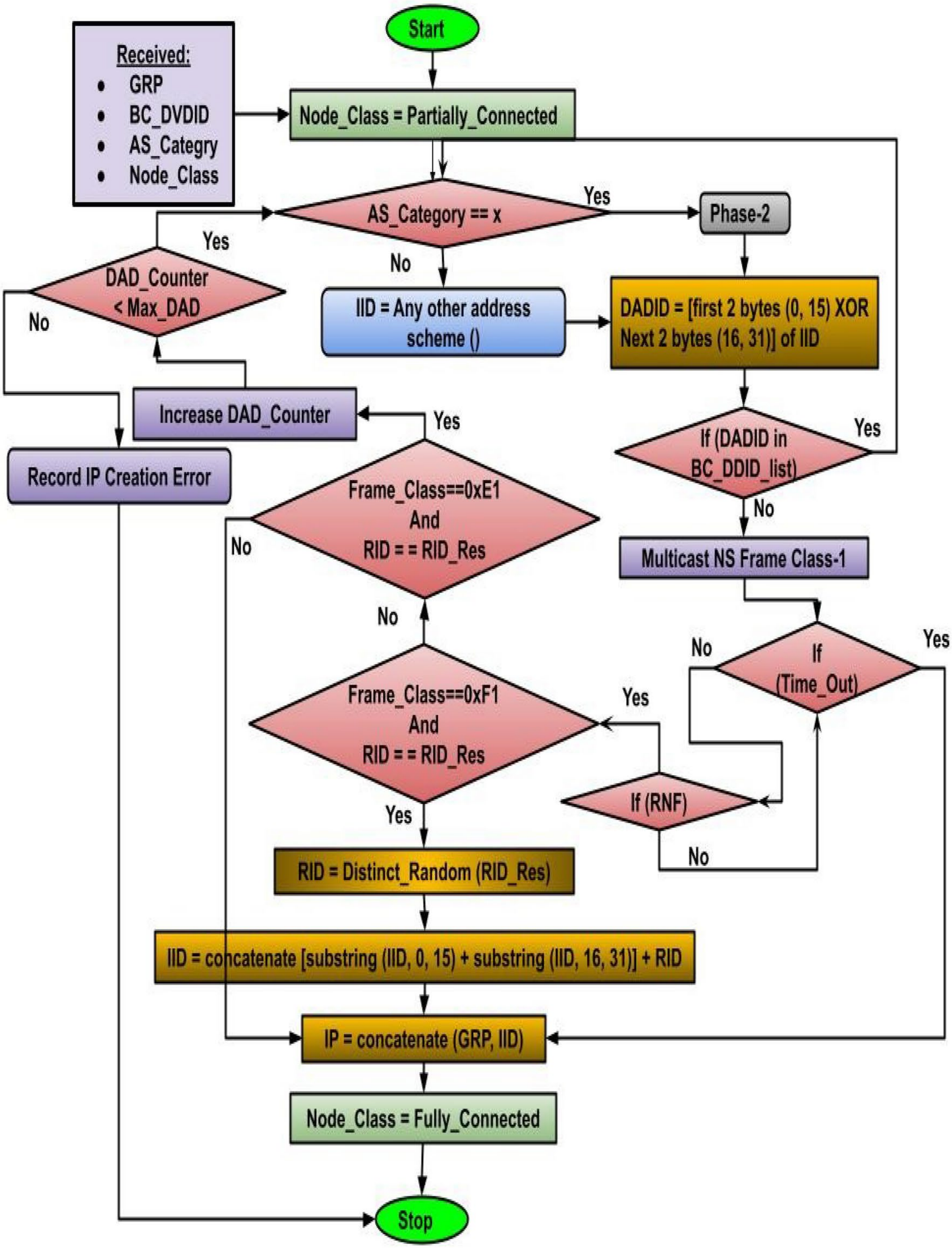
Start
Received:
GRP
BC_DVDID
AS_Categry
Node_Class
Node_Class = Partially_Connected
AS_Category == x
Yes
Phase-2
No
IID = Any other address scheme ()
DADID = [first 2 bytes (0, 15) XOR Next 2 bytes (16, 31)] of IID
DAD_Counter < Max_DAD
Yes
No
Increase DAD_Counter
Yes
Record IP Creation Error
If (DADID in BC_DDID_list)
Yes
No
Multicast NS Frame Class-1
Frame_Class==0xE1 And RID = = RID_Res
No
No
If (Time_Out)
No
Yes
Frame_Class==0xF1 And RID = = RID_Res
Yes
If (RNF)
Yes
No
RID = Distinct_Random (RID_Res)
IID = concatenate [substring (IID, 0, 15) + substring (IID, 16, 31)] + RID
IP = concatenate (GRP, IID)
Node_Class = Fully_Connected
Stop

Fig. 7. Phase-2 Improved DAD process.

$$ASR = S/(T) \tag{1}$$

Here S represents successful allocations, and T represents the total number of attempts for allocation.

General address configuration cost

The total cost of address configuration is evaluated using IID generation cost and DAD process costs, as defined in Eq. (2), where Dn is the number of repeated DAD operations for generating the unique node address. The cost of IID generation is calculated through Eq. (3) which includes the cost of generating CVC, VID, and RID. The

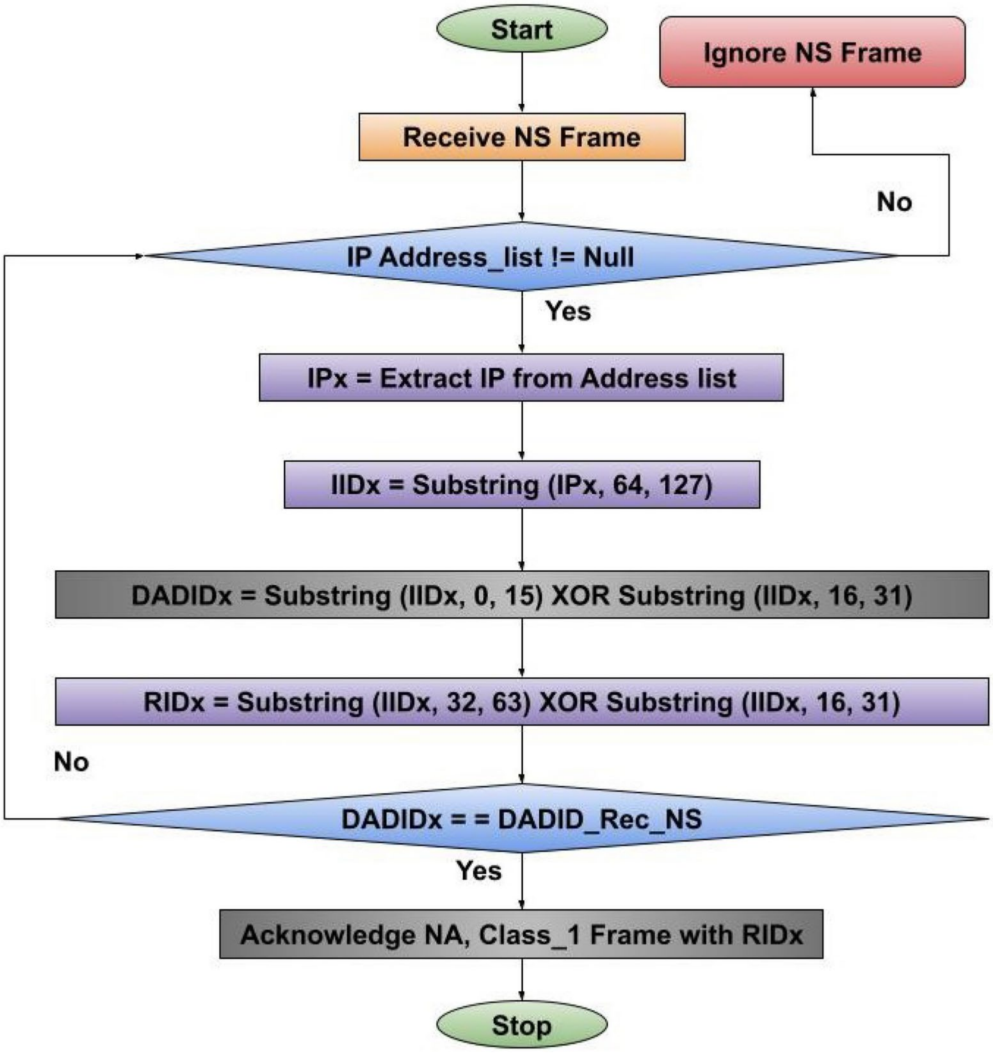
Start
Ignore NS Frame
Receive NS Frame
No
IP Address_list != Null
Yes
IPx = Extract IP from Address list
IIDx = Substring (IPx, 64, 127)
DADIDx = Substring (IIDx, 0, 15) XOR Substring (IIDx, 16, 31)
RIDx = Substring (IIDx, 32, 63) XOR Substring (IIDx, 16, 31)
No
DADIDx = = DADID_Rec_NS
Yes
Acknowledge NA, Class_1 Frame with RIDx
Stop

Fig. 8. Phase-3 (Validation of Received NS Frame).

Variables	Explanation	Unit
Emul	Energy consumption of multiply operator	nJ/bit
Esht	Energy consumption of shift operator	nJ/bit
D	Range of transmission	M
L	Length of data	Bits
Edis_r_ratio	Energy dissipation rate to run the radio	nJ/bit
Edis_r_amp	Energy dissipation rate to transmit amplifier	pJ/bit/m^2
N	Total nodes within the network	Number
Na	Fully connected nodes	Number
Nb	Partially connected nodes	Number
Fsize_1	Class-1 frame size	Bits
Fsize_2	Class-0xE frame size	Bits

Table 5. Specifications of network model parameters.

Variables	Explanation	Unit
[X, Y]	Network reach range	400 × 400 m^2
N	Nodes (Total)	[50,500]
D	Transmission range of individual nodes	2 3m
i, j, k	Size of DAD ID, Secrete ID, and Node ID	16, 16, 32 bits
L	Packet length	320 bits
Edis_r_ratio	Energy dissipation rate to run the radio	50 nJ/bit
Edis_r_amp	Energy dissipation rate to transmit amplifier	100 pJ/bit/m^2
Esht	Energy consumption of shift operator	4.26 nJ/bit
Emul	The energy consumption of multiply operator	6.39 nJ/bit

Table 6. Simulation setting and environment.

Nodes	FEUI	SEUI	EUI
10	1	0.012	0.006
20	1	0.025	0.004
30	1	0.027	0.012
40	1	0.024	0.009
50	1	0.08	0.007
60	1	0.061	0.021
70	1	0.085	0.019
80	1	0.12	0.01

Table 7. Successful scanning rate.

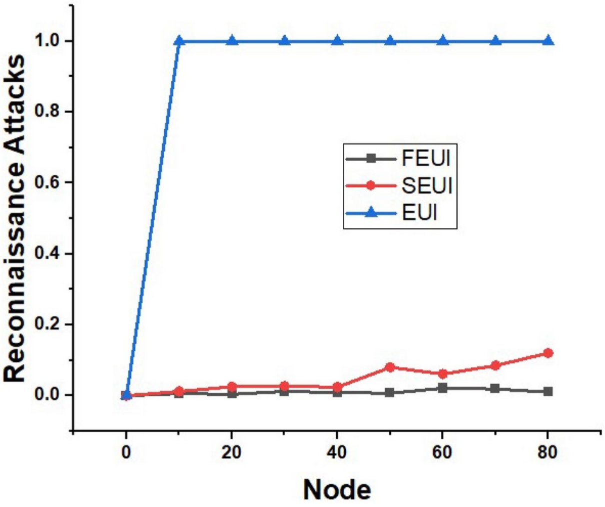

Fig. 9. Reconnaissance attack.

DAD process cost is evaluated by using Eqs. (4), (5), and (6); it includes the NS multicast cost and NA response cost of matching the IID of existing nodes.

$$TC_{address-cost} = \sum_{x=1}^{D_n} (IID_{gen-cost} + DAD_{cost}) \tag{2}$$

$$IID_{gen-cost} = CVC_{cost} + VID_{cost} + RID_{cost} \tag{3}$$

$$DAD_{cost} = multicast_{cost} + Response_{cost} \tag{4}$$

$$multicast_{cost} = (N-1) * F_{size-1} \tag{5}$$

$$Response_{cost} = (n_a + n_b) * F_{size-2} \tag{6}$$

Energy consumption (EC)

The total Energy Consumption for Address Allocation is evaluated using Eq. (7). The ECIID-generation defines the consumption of energy in generating bits of IID, ECDAD is the total energy consumed for the proposed DAD process, and ECduplicity is the consumption of the energy for resolving the duplicity, which is evaluated using Eqs. (8), (9), and (10) respectively. The equation NAavg-neighbour defines the average number of neighbors for each node. The Etransmit(d,m), Ereceive(d,m), and Eforward(d,m) are the energy consumptions for transmitting, receiving, and forwarding the bits into the network using Eqs. (12), (14), and (15) respectively where d denotes the distance in meters, m denotes the bit of data sending to a node. The remaining constant parameters used for evaluating energy consumption were defined in Table . 4 of the specification of the first-order radio network.

$$EC_{(T-energy)} = (EC_{IID-gen} + EC_{DAD} + EC_{dup}) \tag{7}$$

$$\begin{aligned} EC_{IID-gen} = {} & [(EC_{CVC-pr}) + (EC_{VID-pr}) + (EC_{RID-pr})] \cdot EC_{mul} + \\ & EC_{sht} \end{aligned} \tag{8}$$

$$EC_{DAD} = \sum_{i=0}^{N-1} [EC_{transmit}(d,m) + NA_{avg-neighbor} + EC_{receive}(d,m)] \tag{9}$$

$$EC_{dup} = \sum_{x=1}^{D_n} (EC_{IID-gen} + EC_{DAD} + EC_{net-receive}) \tag{10}$$

$$\begin{aligned} EC_{node-receive} = (n_a + n_b) * F_{size-2} * [E_{tmt}(d,m) + \\ E_{fwd}(d,m) * Hop_{cnt-avg}] \end{aligned} \tag{11}$$

$$E_{transmit}(d,m) = E_{tran-unit} + E_{multi-path-unit} \tag{12}$$

$$E_{trt}(d,m) = [m * (E_{dis-r-ratio} + E_{dis-r-amp})] * d^2 \tag{13}$$

$$E_{receive}(d,m) = m * E_{dissipation-rate-ratio} \tag{14}$$

$$E_{forward}(d,m) = E_{transmit}(d,m) + E_{receive}(d,m) \tag{15}$$

Communication overhead (CO)

The Overhead Communication cost is evaluated through Eq. (16) using multicast and response message costs.

$$CO_{cost} = multicast_{msg-cost} + Response_{msg-cost} \tag{16}$$

$$multicast_{msg-cost} = (N-1) * F_{size-1} \tag{17}$$

$$Response_{msg-cost} = (n_a + n_b) * F_{size-2} \tag{18}$$

Experimentation, results and discussion

This section presents the evaluation of the proposed algorithm under the reconnaissance and DoS attack in the presence of malicious or attacker nodes in the network. We have compared our proposed method, FEUI-64, with the IEEE standardized EUI-64[3] and the recent SEUI-64[11] because all these methods utilize MAC information with varying advancements aimed at enhancing address security. The comparison is relevant as these mechanisms aim to maximize the ASR and minimize predictability, thereby mitigating reconnaissance attacks. The performance in terms of ASR, energy consumption, and communication overhead is evaluated using the parameters described in Table 5 and the simulation environment, as described in Table 6. The proposed FEUI-64 method is evaluated in Python 3.9.0 on a Windows 7 platform with a Core-i3 processor running at 3.6GHz and 4GB of RAM.

Results

Reconnaissance attack

The reconnaissance attack is tested to perform sequential scanning by the attacker of generated address to identify the nodes. The reconnaissance attack can be mitigated if the attacker fails to recognize the generated address. It can be represented as the ratio of successful scans to the total number of scans.

Reconnaissance attack = Successful scan/Total scan

Here successful scan means the attacker can identify generated address. So to make the addressing scheme attack-proof, successful scan should be minimized to zero.

An attack program was developed to evaluate the performance of the proposed FEUI-64 addressing scheme compared to EUI-64 and SEUI-64 schemes. The scanning program examined the addresses of nodes ranging from 10 to 80 within the network. The results of the scanning attacks, as shown in Table 7 and Fig. 9, provide insights into the effectiveness of the different addressing schemes, including FEUI, SEUI, and EUI. The table and figure illustrates the percentage of nodes that were successfully identified by the scanning program for each addressing scheme. In the FEUI-64 scheme, all the nodes almost undetected, indicating its robustness against scanning attacks. On the other hand, the EUI-64 scheme, which generates addresses based on the MAC address of the node, showed a higher rate of successful identification by the scanning program. The SEUI-64 scheme, which incorporates shuffling to generate addresses, also exhibited some vulnerability to scanning attacks, with a moderate number of nodes being identified.

These results highlight the superiority of the proposed FEUI-64 scheme in preventing scanning attacks compared to the EUI-64 and SEUI-64 schemes. The FEUI-64 scheme offers a significantly higher level of address obfuscation, making it extremely difficult for an attacker to identify the generated addresses. The data presented in Table 7 confirms that the proposed FEUI-64 addressing scheme provides enhanced security against scanning attacks, reinforcing its effectiveness in safeguarding IPv6 addresses in IoT networks.

ASR under DoS attack

In this evaluation, the ability to mitigate of DoS attack in the presence of a malicious node is tested. The proposed work, along with EUI-64 and SEUI-64, is evaluated in three different scenarios to check whether it successfully assign an IPv6 address to all nodes for different size of network or fails.

In the first scenario, it is considered that there is no malicious node present in the network. In this case, all three methods successfully assigned addresses to all network nodes. In other words, it can be said that they achieved a 100 percent success rate. The observed result is shown in Fig. 10, and it clearly shows that all three methods' ASR is 1(100 percent success).

In the second scenario, the ASR is evaluated under the presence of a malicious node inside the network. In this case, the proposed work succeeds in IPv6 assignment while the EUI-64 and SEUI-64 fail. The reason behind this is the DoS attack by the malicious node, which attacks by false reply to all requests of IID verification by the new node. The simulation illustrated in Fig. 11 reveals that the proposed work achieves 100 percent ASR while EUI and SEUI fail.

In the third scenario existing as well as new nodes both are malicious, which is illustrated in Fig. 12, where the proposed work succeeds in assigning an IP address to the node while the EUI and SEUI fail.

Communication overhead

The evaluation criterion of added communication overhead, measured in terms of the number of bytes, was considered in this research. To assess this criterion, simulations were conducted on networks of varying sizes. The results obtained were used to plot Fig. 13, which visualizes the communication overhead of the proposed FEUI, SEUI, and EUI schemes. Additionally, the specific data for different network sizes is summarized in Table 8.

The results presented in Table 8 and depicted in Fig. 13 indicate that the proposed FEUI scheme introduces less communication overhead compared to the EUI and SEUI schemes. The FEUI addresses, which are generated using a hybrid approach, significantly reduce the number of bytes required for communication. As shown in the table, the FEUI scheme consistently exhibits a lower communication overhead across all network sizes, outperforming both the EUI and SEUI schemes.

The observed reduction in communication overhead can be attributed to the utilization of a smaller number of bits in the IID during the DAD multicasting process. By minimizing the repetition of the DAD process, the proposed FEUI scheme effectively mitigates DoS and reconnaissance attacks, resulting in a more efficient utilization of network resources.

Additionally, the average communication overhead, computed over ten simulation runs and presented with 95% confidence intervals, is as follows: EUI (18684 ± 8251), SEUI (18398 ± 8001), and FEUI (16481 ± 7168). These results are illustrated in Fig. 14.

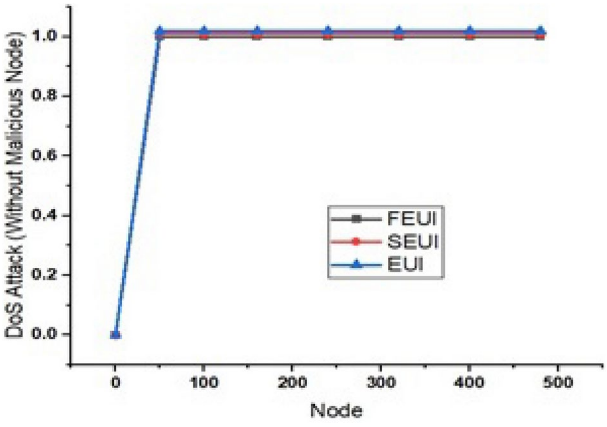

Fig. 10. ASR without attack.

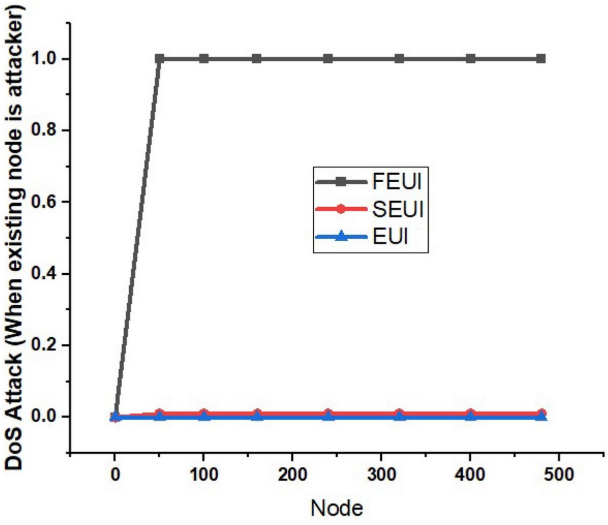

Fig. 11. ASR: when an existing node is malicious.

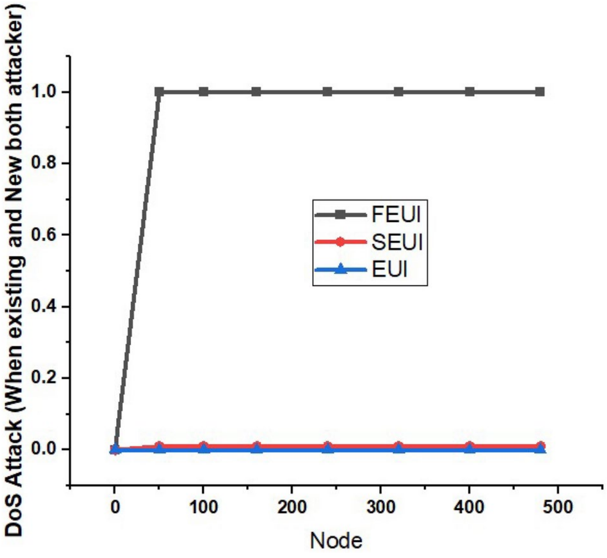

Fig. 12. ASR: when existing and new nodes are both malicious.

Energy consumption

The evaluation criterion of total energy consumption for assigning a unique IPv6 address to a new node, considering the verification process by the DAD protocol, was investigated as the fourth criterion. Figure 15 presents the energy consumption results for the proposed FEUI scheme compared to the EUI and SEUI schemes across different node distributions. Moreover, Table 9 provides detailed data on energy consumption for each scheme at various network sizes.

From the results depicted in Fig. 15 and presented in Table 9, it is evident that the proposed FEUI scheme surpasses both the EUI and SEUI schemes in terms of energy consumption across different node distributions. This improvement can be attributed to the utilization of a reduced number of multicast bits during the DAD process. By minimizing the energy-intensive aspects of the addressing process, the proposed scheme effectively reduces energy consumption without compromising security.

As shown in Table 9, the FEUI scheme consistently exhibits lower energy consumption values compared to the EUI and SEUI schemes for each network size. This reduction in energy consumption is significant, as it enables more energy-efficient operation of IoT devices while ensuring secure and unique IPv6 addressing. The proposed FEUI scheme proves to be a more sustainable and energy-conscious choice for IoT deployments, contributing to overall energy savings and prolonging the operational lifespan of battery-powered devices.

Moreover, the simulation for energy consumption was repeated ten times to ensure reliable results at a 95% confidence level. Figure 16 presents the average energy consumption along with the standard deviation and a

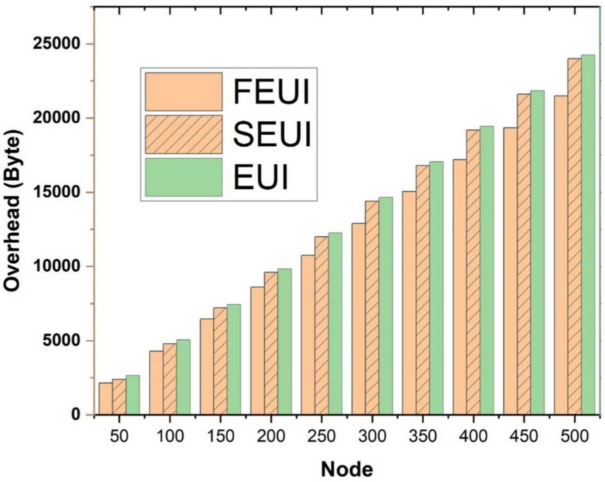

Fig. 13. Overhead analysis.

Nodes	FEUI	SEUI	EUI
50	2150	2650	2400
100	4300	5050	4800
150	6450	7450	7200
200	8600	9850	9600
250	10750	12250	12000
300	12900	14650	14400
350	15050	17050	16800
400	17200	19450	19200
450	19350	21850	21600
500	21500	24250	24000

Table 8. Communication overhead in byte.

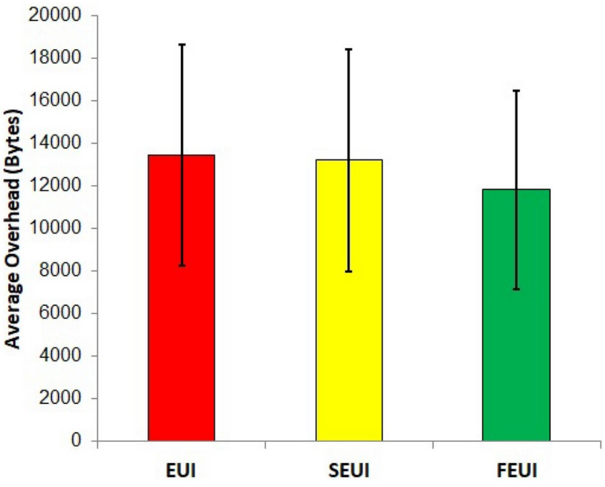

Fig. 14. Overhead analysis with 95% confidence intervals.

95% confidence interval, offering a thorough assessment. The plots in Fig. 16 display the average values obtained from the simulations.

Discussion

The simulation results reveal several significant outcomes:

Nodes	FEUI	SEUI	EUI
50	10.7	11.21	12.23
100	21.63	22.6	24.72
160	34.74	36.4	39.71
240	52.23	54.73	59.68
320	69.74	73.24	79.72
400	87.21	91.35	99.67
480	104.67	109.66	119.65

Table 9. Energy consumption in mJ.

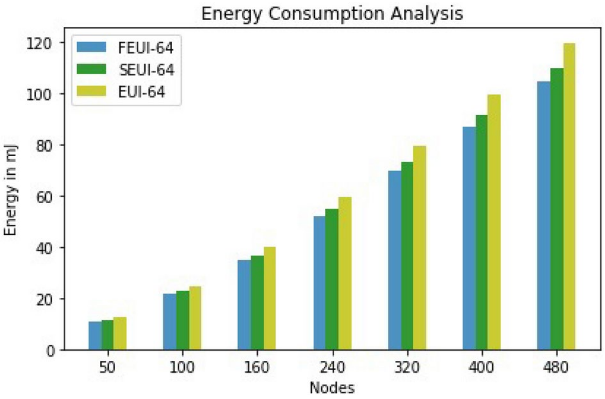

Fig. 15. Energy consumption.

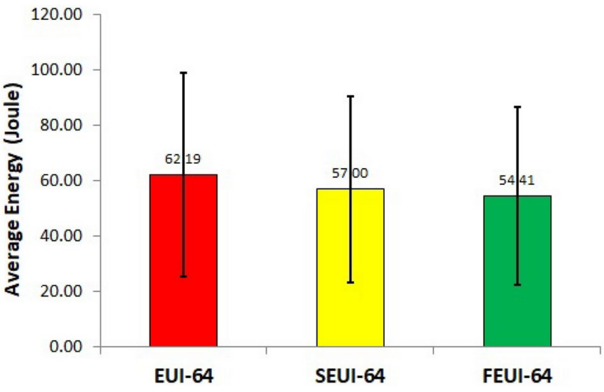

Fig. 16. Energy consumption with 95% confidence intervals.

(a) The proposed FEUI-64 scheme effectively mitigates reconnaissance attacks by malicious nodes. Unlike the EUI and SEUI schemes that rely on pre-existing parameters such as the MAC address, the FEUI-64 scheme generates IPv6 addresses without any pre-known information. This characteristic makes it extremely challenging for attackers to identify and probe the addresses of nodes, ensuring a higher level of security.

(b) The utilization of the XOR value of the DAD ID and Secure ID in the proposed scheme enhances the security of the DAD process. By incorporating this improved secure DAD mechanism, the proposed scheme significantly reduces the susceptibility to DoS attacks from both existing and new malicious nodes. The complexity introduced by the XOR operation makes it highly difficult for attackers to disrupt the address assignment process.

(c) The proposed FEUI-64 scheme is designed to generate unpredictable IPv6 addresses to mitigate reconnaissance attacks without compromising ASR. The uniqueness of these generated IPv6 addresses is verified through the DAD method. In the proposed DAD method, only a portion of the IID is multicast into the network, while the existing nodes unicast the remaining part. By mitigating DoS attacks and increased ASR, the proposed work typically completes DAD in one round. In contrast, traditional methods often require multiple rounds of the DAD process, especially under attack conditions and poor ASR, leading to increased NS message overhead in the network. Thus, the proposed method achieves reduced overhead for three main reasons: firstly, no compromise with ASR, fewer IID bits are used during multicast, and finally, the DAD process is often completed in fewer rounds.Overall, the simulation results demonstrate that the proposed FEUI-64 scheme offers enhanced security and improved performance compared to the conventional EUI and SEUI schemes. It effectively addresses the vulnerabilities associated with reconnaissance attacks and DoS attacks, while also optimizing communication overhead and energy consumption. These findings validate the effectiveness and practicality of the proposed scheme for secure IPv6 addressing in IoT networks.

Conclusion and future scope

The proposed research presents a novel approach to address the vulnerabilities of existing SLAAC-based designs and DAD protocols, specifically in the context of reconnaissance and DoS attacks. The FEUI-64 scheme, combined with an improved secure DAD mechanism, offers a robust solution to enhance the security and performance of IPv6 addressing in IoT networks. The key contributions of this research lie in the proposed FEUI-64 scheme, which incorporates a hybrid IID generation strategy. The FEUI-64 scheme combines the CVC part, the Vendor Identification part derived from the MAC address with a timestamp, and the remaining bits generated randomly. By leveraging this approach, the FEUI-64 scheme significantly reduces the probability of successful reconnaissance attacks, as it eliminates the reliance on pre-existing parameters and introduces a higher degree of randomness in address generation.

Furthermore, the research focuses on enhancing the security of the DAD process by introducing an improved secure DAD mechanism. This mechanism employs XOR operations on the DAD ID and Secure ID to strengthen the resistance against DoS attacks from both existing and new malicious nodes. The enhanced secure DAD contributes to a more reliable and secure address assignment process.The experimental results validate the efficacy of the proposed FEUI-64 scheme and improved secur e DAD mechanism. The evaluations demonstrate a significant reduction in the success rate of reconnaissance attacks compared to existing EUI and SEUI schemes. Additionally, the proposed scheme exhibits lower communication overhead and energy consumption, thereby improving the overall efficiency of the addressing process.

While the proposed methodology showcases promising results, certain limitations should be acknowledged. One limitation is the reliance on specific network configurations and scenarios for evaluation. The performance of the proposed scheme may vary in different network environments or under diverse attack scenarios. Additionally, the research primarily focuses on mitigating reconnaissance and DoS attacks, and further exploration is needed to address other potential security threats. Looking ahead, there are several avenues for future research. Firstly, investigating the scalability of the proposed scheme to larger IoT networks with a higher number of nodes would provide valuable insights into its performance and efficiency. Secondly, exploring the integration of additional security mechanisms, such as anomaly detection or intrusion prevention techniques, could further fortify the overall security posture. Finally, exploring the applicability of the proposed scheme in other wireless network paradigms, such as Wireless Sensor Networks (WSNs) and Wireless Mesh Networks (WMNs), would expand its potential impact.

In conclusion, the proposed FEUI-64 scheme with improved secure DAD offers a robust and secure solution for mitigating reconnaissance and DoS attacks in IPv6 addressing. The novel hybrid IID generation and enhanced secure DAD mechanism contribute to improved security, reduced communication overhead, and energy efficiency. While further research is warranted to address potential limitations and explore additional security measures, the proposed scheme holds promise for IoT, WSN, WMN, and other wireless applications.

Data availability

Authors declare that all the data being used in the design and production cum layout of the manuscript is declared in the manuscript.

Received: 27 May 2024; Accepted: 18 October 2024
Published online: 24 October 2024

References

1. Deering, S. & Hinden, R. Internet protocol, version 6 (IPv6) specification. *IETF*, RFC 8200. http://www.rfc-editor.org/rfc/pdfrfc/rfc8200.txt.pdf (Accessed 22 July 2024).
2. Narten, D. T., Jinmei, T. & Thomson, D. S. IPv6 Stateless Address Autoconfiguration. *RFC 4862* (2007).
3. IEEE. Guidelines for 64-bit Global Identifier (EUI-64) Registration Authority. http://standards.ieee.org/regauth/oui/tutorials/EUI64.html (1997).
4. Ahmed, A. S., Hassan, R., Qamar, F. & Malik, M. IPv6 cryptographically generated address: Analysis, optimization and protection. *CMC-Comput. Mater. Continua* **68**, 247–265 (2021).
5. Kumar, G. & Tomar, P. A survey of IPv6 addressing schemes for Internet of Things. *Int. J. Hyperconnect. Internet Things (IJHIoT)* **2**, 43–57. https://doi.org/10.4018/IJHIoT.2018070104 (2018).
6. Gont, F., Cooper, A., Thaler, D. & Liu, W. Recommendation on stable IPv6 interface identifiers. *IETF, RFC 8064*.
7. Asati, R. et al. Enhanced duplicate address detection. *IETF, RFC 7527*.
8. Haddad, W., Nordmark, E., Dupont, F. & Bagnulo, M. & Patil, B. Privacy for mobile and multi-homed nodes: MoMiPriv problem statement. Internet Draft (2005).
9. Koodli, R. IP address location privacy and mobile IPv6: Problem statement. *IETF, RFC 4882*.
10. Verma, S., Kawamoto, Y. & Kato, N. A network-aware Internet-wide scan for security maximization of IPV6-enabled WLAN IoT devices. *IEEE Internet Things J.* **8**, 8411–8422. https://doi.org/10.1109/JIOT.2020.3045733 (2020).
11. Abdullah, S. A. SEUI-64, bits an IPv6 addressing strategy to mitigate reconnaissance attacks. *Eng. Sci. Technol. Int. J.* **22**, 667–672. https://doi.org/10.1016/j.jestch.2018.11.012 (2019).

12. Dou, Z., Wang, X. & Li, Y. Coordinate-based addressing for MANET. *Telecommun. Syst.* **71**, 121–139. https://doi.org/10.1007/s11235-018-0499-0 (2019).
13. Kumar, G. & Tomar, P. A stateless spatial IPv6 address configuration scheme for internet of things. IETE J. Res. 1-14 (2021). https://doi.org/10.1080/03772063.2021.1994037.
14. Al-Ani, A. K., Anbar, M., Al-Ani, A. & Ibrahim, D. R. Match-prevention technique against denial-of-service attack on address resolution and duplicate address detection processes in IPv6 link-local network. *IEEE Access* **8**, 27122–27138. https://doi.org/10.1109/ACCESS.2020.2970787 (2020).
15. He, L., Kuang, P., Liu, Y., Ren, G. & Yang, J. Towards securing duplicate address detection using P4. *Comput. Netw.* **198**, 108323. https://doi.org/10.1016/j.comnet.2021.108323 (2021).
16. Usman, M., Kamboh, U. R., Taqdees, M. D., Waheed, Z., Shehzad, M. N. & Zafar, H. Enhance neighbor discovery protocol security by using secure hash algorithm. In *2021 International Conference on Innovative Computing (ICIC)-IEEE* 1–8. https://doi.org/10.1109/ICIC53490.2021.9693085 (IEEE, 2021).
17. Al-Ani, A. K., Anbar, M., Manickam, S. & Al-Ani, A. DAD-match: Technique to prevent DoS attack on duplicate address detection process in IPv6 link-local network. *J. Commun.* **13**, 6.
18. Kumar, B. & Pragya. IPv6 addressing scheme to enhance the performance by mitigating reconnaissance attack. *Internet Technol. Lett.*[SPACE]https://doi.org/10.1002/itl2.493 (2023).
19. Cooper, A., Gont, F. & Thaler, D. Security and privacy considerations for IPv6 address generation mechanisms. *IETF, RFC 7721*. https://www.rfc-editor.org/rfc/pdfrfc/rfc7721.txt.pdf (accessed 22 July 2024).
20. Al-Ani, A. K., Anbar, M., Manickam, S. & Al-Ani, A. DAD-match: Security technique to prevent denial of service attack on duplicate address detection process in IPv6 link-local network. *PLoS One* **14**, e0214518. https://doi.org/10.1371/journal.pone.0214518 (2019).
21. Wang, X., Cheng, H. & Yao, Y. Addressing with an improved DAD for 6LoWPAN. *IEEE Commun. Lett.* **20**, 73–76. https://doi.org/10.1109/LCOMM.2015.2499250 (2015).
22. George, W. & Cable, T. W. Enhanced duplicate address detection. IETF, RFC 7527.
23. Kumar, G. & Tomar, P. IPv6 addressing scheme with a secured duplicate address detection. *IETE J. Res.* **68**(5), 3371–3378. https://doi.org/10.1080/03772063.2020.1756938 (2022).
24. He, L., Kuang, P., Liu, Y., Ren, G. & Yang, J. Towards securing duplicate address detection using P4. *Comput. Netw.* **198**, 108323. https://doi.org/10.1016/j.comnet.2021.108323 (2021).
25. Song, G. & Ji, Z. Novel duplicate address detection with hash function. *PLoS One* **11**(3), e0151612. https://doi.org/10.1371/journal.pone.0151612 (2016).
26. Mavani, M. & Asawa, K. Privacy preserving IPv6 address auto-configuration for Internet of Things. In *Intelligent Communication and Computational Technologies: Proceedings of Internet of Things for Technological Development*, vol. IoT4TD 2017, 3–14 (Springer, 2018) https://doi.org/10.1007/978-981-10-5523-21.
27. Stallings, W. IP security. *Internet Protoc. J.* **3**, 11–26 (2002).
28. Arkko, J., Kempf, J., Zill, B. & Nikander, P. Secure neighbor discovery (SEND). *IETF, RFC 3971*.
29. Ahmed, A. S. A. M. S., Hassan, R. & Othman, N. E. IPv6 neighbor discovery protocol specifications, threats and countermeasures: a survey. *IEEE Access* **5**, 18187–18210. https://doi.org/10.1109/ACCESS.2017.2737524 (2017).
30. Kumar, G. & Pragya. IPv6 addressing with hidden duplicate address detection to mitigate denial of service attacks in the internet of drone. *Concurr. Comput. Pract. Exp.* e8131 (2024) https://doi.org/10.1002/cpe.8131.
31. Pragya, Kumar, B. & Kumar, G. Optimized duplicate address detection for the prevention of denial-of-service attacks in IPv6 network. *IETE J. Res.* 1–26. https://doi.org/10.1080/03772063.2024.2350931 (2024).
32. Ibrahim, A. A., Abdulghafor, R. A. A. & Wani, S. A new concept of duplicate address detection processes in IPv6 link-local network. *Int. J. Innov. Comput.* **12**(2), 9–16 (2022).
33. Song, G., Hu, J. & Wang, H. An anti-DoS duplicate address detection model. *Eng. Lett.* **30**(2) (2022).
34. Li, Y., Yang, W., Zhou, Z., Liu, Q., Li, Z. & Li, S. P4-NSAF: defending IPv6 networks against ICMPv6 DoS and DDoS attacks with P4. In *ICC 2022-IEEE international conference on communications* 5005–5010 (IEEE, 2022).
35. Seth, A. D., Biswas, S. & Dhar, A. K. DADCNF: Diagnoser design for duplicate address detection threat using conjunctive normal form. *Comput. Netw.* **1**(222), 109539 (2023).
36. Guangjia, S., Hui, W. & Hangjun, W. Using multi-address generation and duplicate address detection to prevent DoS in IPv6. *IET Commun.* **13**(10), 1390–1396 (2019).
37. Hinden, R. & Deering, S. RFC 4291: IP version 6 addressing architecture. (2006).

Author contributions

All authors contribute equally. All the authors have consented the Journal to publish this paper.

Funding

The authors received no specific funding for this study.

Declarations

Ethics Approval

No Human subject or animals are involved in the research.

Consent to Participate:

All authors have mutually consented to participate.

Competing interest

The authors declare that they have no conflicts of interest to report regarding the present study.

Additional information

Correspondence and requests for materials should be addressed to S.S.

Reprints and permissions information is available at www.nature.com/reprints.

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.