Proposed an Algorithm for Preventing IP Spoofing DoS Attack on Neighbor Discovery Protocol of IPv6 in Link Local Network


Abstract—Duplicate Address Detection (DAD) is one of the most interesting features in IPv6. It allows nodes to connect to a network by generating a unique IP address. It works on two Neighbor Discovery (ND) messages, namely, Neighbor Solicitation (NS) and Neighbor Advertisement (NA). To verify the uniqueness of generating IP, it sends that IP address via NS message to existing hosts. Any malicious node can receive NS message and can send a spoof reply, thereby initiates a DoS attack and prevents auto configuration process. In this manner, DAD is vulnerable to such DoS attack. This study aims to prevent those malicious nodes from sending spoof reply by securing both NS and NA messages. The proposed Advanced Bits Security (ABS) technique is based on Blake2 algorithm and introducing a creative option called ABS field that holds the hash value of tentative IP address and attached to both NA and NS message. We expect the ABS technique can prevent spoof reply during DAD procedure in link local network and can prevent DoS attack.


I. INTRODUCTION

IP address is used to uniquely identify every node in a network. Unlike IPv4, IPv6 operates a 128-bit address that Theoretically allowing 2^{128} or approximately 3.4×10^{38} addresses [1]. Google statistics on 25th may, 2019 shows the percentage of users reaching Google service over IPv6 28.25% compared with IPv4 [2].

IPv6 introduced simpler header format and novel mechanisms such as neighbor discovery concept and address auto configuration [3]. Neighbor Discovery Protocol (NDP) offers a number of functions such as address resolution, parameter discovery, address auto-configuration and duplicate address detection (DAD). NDP defines five Internet Control Message Protocol Version Six (ICMPv6) messages [3]. Router Solicitation (RS), Router Advertisement (RA), Neighbor Solicitation (NS), Neighbor Advertisement (NA) and Redirect message to perform its functions. DAD only relies on two of them, NS and NA messages. During address auto-configuration, any node on the same link can expose the DAD procedure to a DoS attack by responding to each NS [4].

Exchanging NDP messages between nodes, which are ICMPv6 messages, can be misused for performing attacks [5]. Request for Comment (RFC) 4861 recommended using IPSec and SeND [5] to protect NDP functions including DAD. However, research shows that they are not a solid mechanism, by reason of bootstrapping problem, complex algorithm, heavy computational problems and so on [4].

This study represents an extension of the previous work which aims to utilize Blake2 hashing function, introducing a creative field named ABS mechanism in both NS and NA, to secure tentative IP address during DAD procedure in link local network.

A. Neighbor Discovery Protocol (NDP)

Neighbor discovery protocol (NDP) used with IPv6, operates at the link layer of the Internet model [6], and is responsible for gathering various information required for internet communication. It also includes the configuration of local connections, domain name servers, and gateways used to communicate with more distant systems. Five types of ICMPv6 informational messages as explained in RFC 4861 [5] and shown below.

| TABLE I: NDP MESSAGE PROPERTIES |
|-------------------------------|-----------------|-----------------|-----------------|-----------------|
| Message name                  | Type            | Sender          | Receiver        | Properties      |
| Router solicitation (RS)      | 133             | Nodes           | All routers     | Sent from hosts |
|                               |                 |                 | multicast-      | asking router    |
|                               |                 |                 | address         | to send          |
|                               |                 |                 | (FF02:2)        | router           |
| Router advertisement (RA)     | 134             | Routes          | If RS is sent: |
|                               |                 |                 | sender of the   | Sent from        |
|                               |                 |                 | RS              | routers          |
|                               |                 |                 | Otherwise:      | periodically or, |
|                               |                 |                 | all-nodes       | in a response to |
|                               |                 |                 | multicast       | RS in order to   |
|                               |                 |                 | address         | advertise         |
|                               |                 |                 | (FF02:1)        | their presence   |
| Neighbor solicitation         | 135             | Nodes           | Solicited       | Sent by hosts    |
|                               |                 |                 | node or target  | to request       |

DOI: http://dx.doi.org/10.24018/ejers.2019.4.12.1644
B. DAD Security Vulnerabilities

Each host performs the DAD procedure before determining its IP address. The target node multicasts NS messages with a newly generated address to verify its uniqueness to the solicited-node multicast group (SNMA). All existing nodes will receive the NS message, and if a node is discovered on the same link and has the same IP address, it will reply via NA message as a response to the NS message.

If a new host does not receive any response NA to its NS messages from the neighboring nodes, then it is considered that the newly generated address is unique. Moreover, if three seconds have passed and no NA message is received, then the target node considers that the generated IP address is unique and no other remaining nodes on the same link use the address. After three tries [7] the new host stops the DAD process.

The attacker node can disturb the DAD procedure and can initiate a DoS attack. Studies [4], [7] have shown that the DAD process is exposed to Denial of Service (DoS) attacks. In a DoS attack, an attacker causes the new host to be unable to assign an IP address by delivering a fake NA message in reply to NS messages. Thus, the victim host cannot verify the uniqueness of the generated IP address.

C. Existing Security and Their Vulnerabilities

RFC (Request for comment) 4861 recommends using IPSec and SeND to protect NDP mechanisms including DAD [5]. IPSec suffers from bootstrapping problems when handled for NDP. While SeND mechanism relies on a complex algorithm that requires heavy computation that results in high consumption of both time and resources [8].

The SAVI (Source Address Validation Improvement) principle is built around the concept of maintaining track of anchor information containing trusted information such as port and MAC (Medium Access Control) address of IPv6 host [8].

In RFC 6959 [9], some possible threats, as well as the challenges in its implementation, are described. Applying SAVI on an access network could create a problem on dynamic address configuration such as Stateless Address Auto Configuration (SLAAC) and Dynamic Host Control Protocol Version Six (DHCPv6). This is due to the difficulty to constitute and maintain the binding of anchor information due to the dynamically changing nature of IP address in that particular setting.

II. RELATED WORKS

A. Trust Neighbor Discovery (Trust-ND)

In this mechanism, the authors proposed a checking algorithm based on modified NS and NA messages format. They introduced them as Trust-NS and Trust-NA messages, both of them containing Trust Option [7].

Because of the use of less complex algorithms, Trust-ND message processing is much faster than SeND mechanism [7]. In addition, the small size of Trust Option also consumes less bandwidth. It significantly has less bandwidth consumption compared to SeND [7].

But Trust ND used the SHA-1 hashing algorithm, and SHA-1 is not perfect for encrypting data, research [10] shows the SHA-1 algorithm is vulnerable to hash collision attacks, and hash collision vulnerability can be easily used to perform DoS attack. Because of its design method, Trust-ND is not a suitable security means for the IPv6 DAD procedure.

B. Push vs. Pull

In the sender-push model, the sender knows the identity of a receiver in advance and pushes the message in an asynchronous manner to the receiver [11]. In the receiver-pull model, it is the receiver who initiates the message transfer by explicitly contacting the sender.

The principle disadvantages of such model are that the sender needs to store outgoing messages and keep them available at least till the intended receivers are willing to retrieve them, moreover, the sender needs to store outgoing messages and keep them available at least till the intended receivers are willing to retrieve them.

Furthermore, this model utilizes MD5 hash computation to authenticate the IP address with existing hosts on the same link. If the hash function is too short, then it is vulnerable to a brute force attack. However, if the hash value is found too long, then it facilitates possible inverting attacks [12].

C. DAD-h

In this paper, the authors planned to modify NS and NA messages similar to the Trust ND discovery technique. They proposed to replaces the traditional NS and NA messages by NS_{DAD-h} and NA_{DAD-h}, respectively [13].

DAD-h includes an experimental field that stores bits of the hash value of tentative IP address. Next, send it to the neighboring hosts in the link-local network for checking the address. The host who finds that the portion is duplicated then it must respond with the other portion to verify. This procedure prevents the attacker to generate fake NA message on replying to the NS, as NA containing only a portion of the generated address.

However, research [14] shows that the MD5 hash function has issues with IPv6 protocol during data transmission. Even in using the MD5 in IPv6 include the higher latency cost compared to the value used and the processor occupied entirely by the computation of the MD5 algorithm. Moreover, MD5 is vulnerable to a hash collision attack. So, MD5 hash function not only just has performance issues with IPv6 protocol but is equally vulnerable to security threats.
D. DAD-match

In this paper, the authors [15] modified and improved the DAD-h technique. The proposed security DAD-match technique builds on SHA-3 hash function by proposing an alternative option called DAD-match, which contains the hash value of tentative IP address and attaches to NS and NA messages to become NS-match and NA-match messages. DAD-match technique can provide less complex lightweight. However, they implemented SHA-3 algorithm for hashing the IP address. SHA-3 is the latest among SHA family, but it has a speed issue as stated from research [14].

III. PROPOSED ADVANCED BITS SECURITY (ABS) TECHNIQUE

As the earlier proposals (Trust-ND, Push vs. Pull, DAD-h, and DAD-match) are unable to properly secure the NS and NA messages to prevent the IP spoofing DoS attack during the DAD procedure completely, we are offering a novel method named as ABS mechanism. In this study of the development, our research aims to propose a technique by introducing some changes in the original NS and NA messages format design.

Main Stages of ABS technique:

The main target of our proposing plan is to secure the NS and NA messages during the DAD procedure to hide the generated IP address from the attacker, so that the Dos attack can be avoided.

For a simplified explanation, we divided our procedure into three steps.

A. Utilizing Blake2b Hashing Technique

Blake2b is considered stronger and flexible among the traditionally used hashing function. In the previous related works, hashing functions used in the purpose of reducing the total bit size. But instead of reducing bit size, we propose to further increase it. Blake2b offers increasing the bit size from64bits to 224 bits, 256 bits, 384 bits or 512 bits. In other cases of encryption, a larger bit size does affect a heavy calculative matter. But in our advanced and slightly different techniques, it will not be affected by taking the larger size.

The workflow of the proposed technique is summarized in the following steps:

- When a new node wants to join the link local network, it generates an IPv6 address as a tentative IP address.
- The target host selects the first 64bit of tentative IP address. Using Blake2b algorithm hashes the selected bits and inserts them into the ABS field of NS message format.
- The target host send the NS to the SNMA address based on the last 24-bit of the tentative IP address. All existing hosts on the same IPv6 link that have the same SNMA address receive the message.
- After receiving NS message, the existing hosts first check for the ABS field, if it is not existing then discard the message, otherwise receiver run a query if it matches with its own first 64bit hashes values.
- If it does not match with received 64-bit hash values, then the host discard the message, otherwise if matches found subsequently it recalls hash values of its own IP from cache and send a NA message as a reply with next 32-bits and last 32-bits.
- Upon receiving the NA message, the target host first checks for ABS field, if it is not found then discard it, otherwise check for both next 32-bits and last 32-bits that sent from one of existing hosts.
- If matches not found then it is considered that the

We consider using the 512-bit the variation for highest security in this perspective. Besides this, anyone can choose other variations between 224 bits, 256 bits or 384 bits simultaneously. But we recommend considering 512bits, as larger sizes ensure higher security.

As larger hashing bits require higher computational times and resources, so it is almost impossible for the attacker to decrypt it in time. But in our algorithm, we proposed several steps that only needed to compare the hash values. So, it is not required to decrypt it at all. That’s why it is better to choose larger bits to ensure higher security.

B. Control Shifting Procedure

In the core design of NS and NA messages of IPv6 duplicate address verification, control was with NA message only. So, there is a distinct possibility that the received NA message can be generated from the unknown attacker, thus it can be causing spoofing DoS attack within the NDP protocol of IPv6 in the link-local network. But in this ABS procedure spoofing detection control is shifted to the host (sender), who is willing to join to a link-local network, with a tentative interface address.

![Fig. 2. Workflow of our proposed algorithm.](image-url)
generated IP address is unique. Otherwise, the target host will generate another IP address and repeat the whole algorithm from beginning. And if the host is not found a unique IP within three tries then it will stop the whole generating process.

This algorithm clarifies that all controls and checking are shifted to the new hosts, who are willing to connect to the network, via assigning a new interface address for link-local connections.

C. Advanced Bit Shifting Mechanism

According to RFC 4861 [5], Future versions of NS and NA messages format can define new option types. Therefore, we redesigned the traditional NDP message NS and NA format (shown in Fig. 3(a) and Fig. 4(a) respectively) and included a secondary option to the NS and NA core messages format [5], Named as the ABS (Advanced Bits Security) mechanism. The NS and NA redesigned format are shown in Fig. 3(b) and Fig. 4(b) respectively.

![Fig. 3(a). NDP Neighbor Solicitation (NS) message.](image)

![Fig. 3(b). Redesigned NS format with ABS mechanism.](image)

![Fig. 4(a). NDP Neighbor Advertisement (NA) message.](image)

![Fig. 4(b). Redesigned NA format with ABS mechanism.](image)

Though we generated 512 bits of hash values from the blake2b algorithm. But we do not utilize all of it at the same time. In the ‘ABS Mechanism’ field of NS message format, we use only the first 64 bits of total hash values. Next 32 bits and the last 32 bits are stored in the register during the DAD process.

When other hosts of the same network receive the NS message during the DAD procedure, they check for the ABS field, if it is not existing then discard it otherwise open the ‘ABS mechanism’ field to obtain the sender’s first 64 bits. Then check those bits with its own first 64 bits of hash interface address, whether they are matched or not. If it is not matched, then no NA will be sent over.

![Fig. 5. ABS bit division procedure.](image)

But if the bits are found equal, an NA message will be sent included ‘ABS mechanism’ field which contains the next 32 bits and the last 32 bits of the total hash values. But even the existing attacker host sent a false reply with 32bits, (though the bits are not matched) then it can be easily detected and the system is alerted that someone is trying to perform spoofing DoS attack in the link-local network. Otherwise if the next 32 bits and the last 32 bits matched, then the new host will generate a new interface address and hash it again.

If the attacker wants to attack the link-local network, they need the whole address. As the addresses are in hash values so they have to perform a lot heavier calculation (512 bits sequence to attack) compared to the previous related techniques. This process can also be applied in other variations of blake2b (224 bits, 256 bits or 384 bits) without changing the algorithm.

IV. DISCUSSION

This part objectively compares our attempt to the previous ones and finds out the improvement of our proposed procedure among others.

A. Comparing Hashing Functions

Most popular hashing algorithms are MD5, and different version of SHA. To choose our hashing algorithm, we did study several documents. Research [14] presents several comparisons between different hashing algorithms.

Among MD5, SHA-1, SHA-2 and SHA-3, they consider SHA-2 is comparatively better than any other hashing function [16], though SHA-3 is the latest among them. Furthermore, the study shows SHA-2 has some speed issues [17], as it is not fast enough compared to other hashing algorithms. Therefore, we preferred another hashing algorithm BLAKE2.

![Fig. 6. Comparison of the hash functions in terms of speed.](image)

BLAKE2 is a cryptographic hashing function, faster than MD5, SHA-1, SHA-2, and SHA-3 [17], additionally is at least as secure as the latest standard SHA-3. BLAKE2 has been adopted by many projects due to its incredible speed and security.

Blake2 is specified in RFC 7693 [18], and their code and test vectors are available on GitHub [19], licensed under CC0 (public domain-like). Blake2 is also described in the 2015 book titled ‘Hash Function Blake’ [20]. BLAKE2 comes in two flavors; Blake2b and Blake2s.

On an Intel Core i5-6600 (Skylake microarchitecture, 3310MHz), Blake2b can process 1 gigabyte per second (or a speed rate of 3.08 cycles per byte) [17].

The Fig. 6 shows how Blake2 outperforms MD5, SHA-1, SHA-2, and SHA-3 on a Skylake Intel CPU.
B. Reasons for Choosing Larger Bit Size

In earlier proposals, authors used 32 or 64 bits to secure the message. But we used blake2b, in which the lowest variation is 224 bits and the highest variation is 512 bits, and we recommended 512 bits to be used. Larger bit size ensures higher security. As larger hashing bits require higher computational times and resources, so it is practically impossible for the attacker to decrypt it in a short period (as the default timer is three seconds only). And also, the variation will not be affecting our algorithm for further calculation. It is behind the reason preferring 512-bit variation.

C. Comparing Bit Division Mechanism

In earlier proposals, authors proposed to divide the core 64 bits tentative IP address into two parts. But in our algorithm, we divide the hashing 512 bits into three parts. First 64 bits, next 32 bits, and last 32 bits.

The first 64 bits are sent with NS to the connected hosts. Later on, the next 32 bits and last 32 bits are attached to the NA message as a reply to the previous NS. As we discussed earlier, higher bits offer more security, so our algorithm comparatively more secured than others.

D. Control Shifting

In earlier proposals, almost all of them preferred to shift the control of the decision making to the new host. We use a similar mechanism to build our own algorithm. So, it would be easier to typically prevent various possible security threats as well as make it a lot harder for the potential attacker to attack.

V. CONCLUSION

This study was particularly aimed to propose a new security technique called Advanced Bits Security (ABS), for securing the spoofing detection from IP spoofing DoS attacks in IPv6 link-local network. The proposed technique aims to overcome the limitations of the current existing mechanisms (Trust-ND, Push-Pull, DAD-h, and DAD-match) and improve the prevention of DoS-on-DAD attacks in terms of processing time and complexity. The ABS is based on the blake2b hash function to secure a tentative IP address exchange among hosts during the spoofing detection procedure. As a result, new hosts can connect the IPv6 network effectively. Further research can be carried out on the larger sized network to implement and evaluate its scalability performance.

REFERENCES


Md. Mostafizur Rahman
Affiliation:
Student and Researcher, Department of Electronics and Communication Engineering, Hajee Mohammad Danesh Science and Technology University, Dinajpur, Bangladesh.
E-mail: mostafizur.rahman.mce@gmail.com
Research interest:
1. Network Security
2. Wireless sensor network

Md. Mostafizur Rahman
Affiliation:
Student and Researcher, Department of Electronics and Communication Engineering, Hajee Mohammad Danesh Science and Technology University, Dinajpur, Bangladesh.
E-mail: mostafizur.rahman.mce@gmail.com
Research interest:
1. Network Security
2. Biomedical Engineering

Saif Ibn Reza
Affiliation:
Student and Researcher, Department of Electronics and Communication Engineering, Hajee Mohammad Danesh Science and Technology University, Dinajpur, Bangladesh.
E-mail: saifir.arup@gmail.com
Research interest:
1. Network Security
2. Biomedical Engineering
Sumonto Sarker
Affiliation:
Assistant Professor, Department of Electronics and Communication Engineering, Hajee Mohammad Danesh Science and Technology University, Dinajpur, Bangladesh.
Brief Biographical History:
Bsc in Telecommunication and Electronic Engineering, Ms in Information Tecnology
E-mail: sumonto@hstu.ac.bd
Research interest:
1. Network Security
2. Design new routing protocol
3. Wireless sensor network

Md. Mehedi Islam
Affiliation:
Associate Professor, Faculty of Electronics and Communication Engineering, Hajee Mohammad Danesh Science and Technology University, Dinajpur, Bangladesh.
Brief Biographical History:
Bsc in Applied Physics
Msc in Applied Physics
E-mail: mehedi@hstu.ac.bd
Research interest:
1. Network Security
2. Renewable Energy
3. Biomedical Engineering