Improved Secure Neighbor Discovery Protocol (ISEND) for New Wireless Networks Generations

Imen El Bouabidi[1], Salima Smaoui[1], Faouzi Zarai[1], Mohammad S. Obaidat[2] and Lotfi Kamoun[1]
LETI laboratory, University of Sfax, Sfax, Tunisia
[2]*Computer Science and Software Engineering Department, Monmouth University, NJ 07764, Monmouth, U.S.A.*

Keywords: Wireless Network, NDP Protocol, Send, Incompatibility, Delegation.

Abstract: In charge of several critical functionalities, the Neighbor Discovery Protocol (NDP) is used by IPv6 nodes to find out nodes on the link, to learn their link-layer addresses to discover routers, and to preserve reachability information about the paths to active neighbors. Given its important and multifaceted role, security and efficiency must be ensured. However, NDP is vulnerable to critical attacks such as spoofing address, denial-of-service (DoS) and reply attack. Thus, in order to protect the NDP protocol, the Secure Neighbor Discovery (SEND) was designed. Nevertheless, SEND's protection still suffers from numerous threats and it is currently incompatible with the context of mobility and especially with the proxy Neighbor Discovery function used in Mobile IPv6. To overcome these limitations, this paper defines a new protocol named Improved Secure Neighbor Discovery (ISEND) which adapt SEND protocol to the context of mobility and extend it to new functionalities. The proposed protocol (ISEND) has been modeled and verified using the Security Protocol ANimator software (SPAN) for the Automated Validation of Internet Security Protocols and Applications (AVISPA) which have proved that authentication goals are achieved. Hence, the scheme is safe and efficient when an intruder is present.

1 INTRODUCTION

Internet Protocol version 6 (IPv6) is a solution to the problem of the shortage of public IPv4 addresses that faces Internet. IPv6 adds many improvements to IPv4 in areas such as quality of service, routing and network auto-configuration. The introduction of IPv6 brings a set of new network protocols. One of these new protocols is the Neighbor Discovery Protocol (NDP) (Narten et al., 2007) which is part of the Internet Control Message Protocol Version (ICMPv6).

NDP operates in the network layer of the Internet network architecture. It is heavily used for several critical functionalities, such as determining link layer addresses, discovering other existing nodes on the same link, providing address auto-configuration of nodes, detecting duplicate addresses, finding routers and maintaining reachability information about paths to active neighbors and forward data.

However, NDP presents many security problems. It is vulnerable to many attacks (Nikander et al., 2004), for that reason the Internet Engineering Task Force (IETF) defined a secure version of that protocol, called Secure Neighbor Discovery (SEND) which is based on Cryptographically Generated Addresses (CGA). With SEND extensions, the node can prove CGA address ownership by signing messages with its private key, as well, SEND prevents functions that require a third party node to modify or emit NDP message. The Proxy Neighbor Discovery (Proxy ND), of the IPv6, can emit packets on behalf of the Mobile Node (MN), which enables the incompatibilities between the SEND protocol and the Proxy ND. In this context, our contribution consists to solve the problem of incompatibility between the Proxy ND and the SEND protocol.

The remainder of this paper is organized as follows: Section 2, presents NDP protocol. In the third section, the NDP vulnerabilities are cited, In Section 4, we present SEND and its limits for supporting mobility and in particular the incompatibility problem between SEND and Proxy ND

Related work is summarized in Section 5.

In Section 6 we detail the proposed solution to resolve the above mentioned incompatibility problem. Section 7 describes a simulation method of

El Bouabidi I., Smaoui S., Zarai F., Obaidat M. and Kamoun L..
Improved Secure Neighbor Discovery Protocol (ISEND) for New Wireless Networks Generations.
DOI: 10.5220/0005123300710077
In *Proceedings of the 11th International Conference on Wireless Information Networks and Systems* (WINSYS-2014), pages 71-77
ISBN: 978-989-758-047-5

our scheme by a model checking tool called AVISPA. Finally, we conclude the paper in Section 8.

2 NEIGHBOR DISCOVERY PROTOCOL

NDP solves a set of problems related to the nodes that are located on a same link, prefix discovery, router discovery, address auto-configuration, Duplicate Address Detection (DAD), Neighbor Unreachability Detection (NUD), and redirect.

It uses five messages provided by ICMPv6 such as:

- Router Solicitation (RS): messages issued by a host to cause local routers to transmit information.
- Router Advertisement (RA): RA is sent periodically by IPv6 routers or in response to a RS message.
- Neighbor Solicitation (NS): NS messages are originated by the nodes to ask the link layer address of another node, also it used for DAD and neighbor unreachability detection.
- Neighbor Advertisement (NA): NA messages are always sent in response to a NS message from a node, it can be sent by a node when its link layer address is changed.
    - Redirect: Redirect messages are always sent by the router to a host asking "it" the host to update its routing information. The router can send Redirect message back to the host when a router knows that the best path for that host to reach the destination is another.

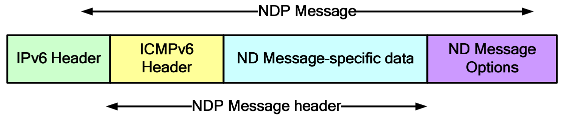


Figure 1: The NDP Message Format.

3 VULNERABILITIES OF NDP

NDP uses simple mechanisms to secure messages by accepting messages from the same local link, or nodes with either unspecified or link local IPv6 addresses and with hop limit, but this is not enough security and makes NDP vulnerable to several attacks such as:

- Spoofing: In a spoofing attack a malicious node uses another node's address or identity. Attackers can send a fake message in the aim to associate its Medium Access Control (MAC) address with the IP address of another host falsify data and thereby gaining an illegitimate…, so attackers can use spoofs to leverage man-in-the-middle (MITM) attacks, create DoS (Denial of Service) attacks.

  DoS: This attack prevents communication between the legitimate node and other nodes. Attackers can be practiced to prevent a node to get a new IPv6 address by generation DoS en DAD (when the legitimate node is currently checking whether an address is already in use or not)

  Indeed, DAD allows duplicate address detection, however an attacker can always responding to each DAD massage "I have this address". Thus, the legitimate node won't be able to configure an IPv6 address to access the network.
- Redirect: type of attacks in which an attacker redirects packets away from the legitimate receiver to another node on the link.
- Attacker can intercept a message NS and changes the source link layer address option, acting as an MITM between the two nodes.
- Replay: In replay attacks, attackers capture and change messages from a different context into the intended context, thereby fooling the legitimate participant(s) into thinking they have successfully completed the protocol run.

4 SECURE NEIGHBOR DISCOVERY (SEND)

SEND is a security extension of the ND protocol. It provides the address ownership and ensures message authenticity, integrity and freshness. Its protection is twofold: it protects the node from address spoofing and provides to the host a mechanism to authenticate its Access Router (AR).

To achieve these enhancements, SEND introduces four new options: CGA, RSA Signature, Nonce and Timestamp options, and two ICMPv6 messages for identifying the router authorization process

- CGA Option: It encapsulates the CGA Parameters in a NDP message. CGAs are used to make sure that the sender of a neighbor discovery message is the owner of the claimed address. A public-private key pair is generated by all nodes before they can claim an address. The CGA option is used to carry the public key and associated parameters. The messages are signed with the corresponding private key. Only if the source address and the public key are known can the verifier authenticate the message from that corresponding sender.

- RSA option: The RSA Signature option is used to authenticate the identity of the sender and to protect all messages relating to Neighbor and Router Discovery. The message which is sent from CGA address is signed with the address owner private key and the public key is used to verify the signature.
- Nonce Option: This option provides anti-replay protection, and ensures that an advertisement is a fresh response to a solicitation which is sent earlier by the node.
- Timestamp option: the Timestamp make sure that redirects and unsolicited advertisements have not been replayed.
- Certificate Path Solicitation (CPS): is sent by hosts during the Authorization Delegation Discovery (ADD) process to request a certification path between a router and one of the host's trust anchors.
- Certificate Path Advertisement (CPA): the CPA message contains the router certificate, it is sent in reply to the CPS message.

Although, SEND was designed to enhance the security of the NDP protocol, it still suffers from numerous vulnerabilities. On one hand, there is an incompatibility between Anycast addresses and SEND. Indeed, in the case of NDP signaling SEND authorizes only the owner of the address. On the other hand, the procedure of the CGA verification used in SEND can launch DoS attack (Gelogo et al., 2011). Finally, SEND (Arkko et al., 2005) ensures that only the owner of the address is enabled to send message with its source address. Therefore, the message's integrity is valid through the CGA verification and the RSA Signature option protection.

As well, the proxy ND can intercept and modifies messages on behalf of the mobile nodes. As such, Proxy ND and SEND are incompatible. This context presents our interest.

5 RELATED WORK

Although the literature carries a multitude of ND security protocols addressing a number of problems related to security and mobility, there are no lightweight, robust solutions ND Proxy that can operate autonomously in an open environment without use an incompatibilities problems between ND proxy and SEND. This section details some related work focused to resolves incompatibilities between SEND and Proxy ND. Among them, Krishnan et al. present in (Krishnan et al., 2012) a certificate based solution. The router's certificate is extended to support a new Extended Key Usage (EKU) field that indicates whether the router assumes a proxy role. Then, whenever it issues or modifies ND messages and signs with its public key. Neighboring nodes learn, during the Authorization Delegation Discovery, that the router is also authorized to act as a proxy for this subnet prefix or not, therefore they will trust all messages coming from this proxy.

In document (Combes et al., 2010) and (Nikander et al., 2002), Nikander and Arkko, propose a solution which empowers the nodes to determine if a router is trusted enough to be a proxy and to issue a certificate to authorize it to act as such. But, this solution fails to identify the real overhead due to the certificate exchange mechanism.

In (Cheneau et al., 2011), the author's claim their solution is especially important to resolve incompatibilities between SEND and Proxy ND, which is based on Signature Algorithm Agility. In this paper, the author's propose modifications to the CGA addresses and the SEND protocol to support Signature Algorithm Agility and present the MCGA addresses. Then they extend the MCGA addresses to store public keys of different nodes, therefore enabling a secure address sharing and to solve incompatibilities between the Proxy ND and the SEND protocol. With the novel solution-based certification mechanism, and the introduction of new addresses, the proposed solution achieves defending against many attacks successfully and efficient.

6 IMPROVED SECURE NEIGHBOR DISCOVERY PROTOCOL

The principle operation of NDP is the neighbor discovery. Indeed, when a mobile sends an NS requesting some information to another neighbor node in the same network, it will respond with an NA. But the problem is when the MN leaves its home network as illustrated in the Figure 2.

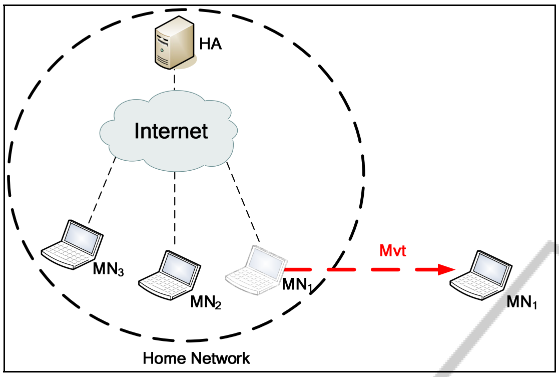


Figure 2: Network architecture.

Our contribution is an improvement of the SEND protocol to solve the problem of incompatibilities between the Proxy ND and the SEND protocol. Indeed our solution consists of three steps:

6.1 Router- Delegation

The first step of our proposed scheme named Router- Delegation. When the MN_1 leaves its home network (regardless it is still transmitting or not), it delegates its NDP responsibilities to the Home Agent (HA). With this delegation, the latter acts as a proxy and can sign and send the secured NA messages.

The delegation is sent to the HA in the Binding Update (BU) message. Once the router receives this message, it responds with a Binding Update Acknowledgment (BACK) affirming the acceptance of this delegation.

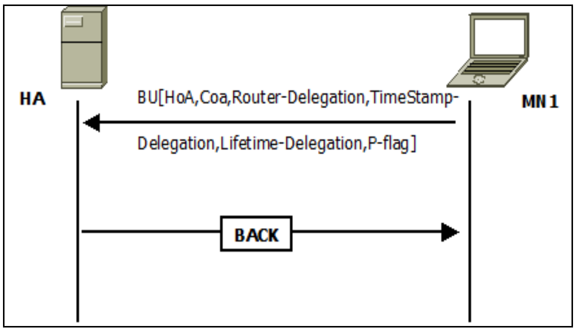

HA
MN1
BU[HoA,Coa,Router-Delegation,TimeStamp-
Delegation,Lifetime-Delegation,P-flag]
BACK

Figure 3: Router-Delegation

To achieve this goal, we are served of the format of the BU message (as shown Figure 4) which contains an extension field that we have used to include the R-delegation parameters. The MN_1 sends a combined Binding Update message with the router delegation. The R- delegation corresponds to a signature with the private key of MN_1 of a HA MAC address that the HA gives it to the MN_1 since its initial access. This signature of the MAC Address (16 bytes) is inserted later in the BU with the “TimeStamp-Delegation” and “Lifetime-Delegation”.

- TimeStamp-Delegation: This field specifies the start time of delegation.
- nguish a simple and a modified BU, a new flag P is added to the header of theLifetime-Delegation: This field indicates the lifetime of MAC-Address-Delegation starting from timestamp-delegation.

To enable the HA to disti BU message (see Figure 4). The HA receiving the modified BU with the flag set, will be notified that the BU request corresponds to a registration with router delegation sent by the MN_1.

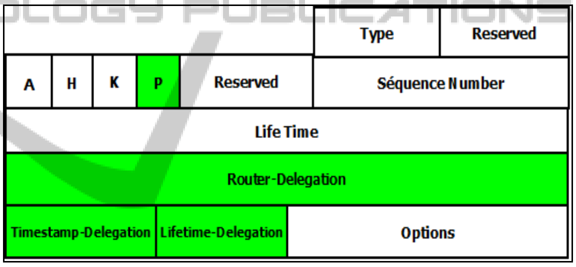


Figure 4: Modified BU format.

6.2 Router- Delegation Checking

The second step is called Router-Delegation Checking. After receiving the modified BU message from MN_1, the HA registers the delegation in the database registration. When the HA receives the NS message from other node (MN_2) (to request the link layer address of another node) whose destination is MN_1, it consults its registration database to find a delegation for the MN_1. If it finds an appropriate delegation, it generates and signs the NA instead of MN_1 then sends it to the MN_2. If it does not find an appropriate registration, it drops or treats with unsecured manner the packet NS. The NA messages can also be sent by HA when it receives the BU message with the P flag set; link-layer address is changed.

Upon receiving a NA message in response to an NS message from a HA with the P flag set, MN_2 checks the NA message. If the router delegation verification is successful, the neighbor cache should be updated.

With these options, the router proves that he is delegated from MN_1 and it can answer to all NS messages through the modified NA message.

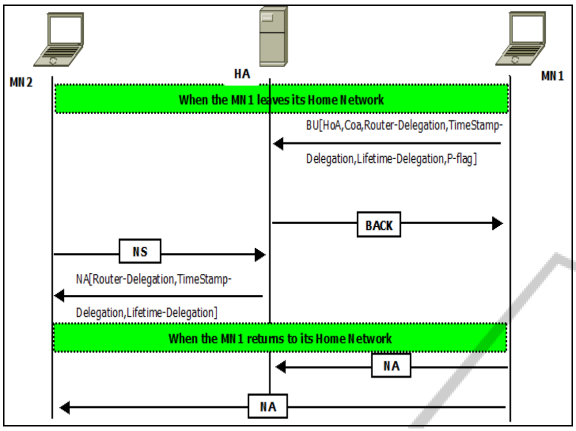

MN2
HA
MN1
When the MN1 leaves its Home Network
BU[HoA,Coa,Router-Delegation,TimeStamp-Delegation,Lifetime-Delegation,P-flag]
BACK
NS
NA[Router-Delegation,TimeStamp-Delegation,Lifetime-Delegation]
When the MN1 returns to its Home Network
NA
NA

Figure 5: Improved Secure Neighbor Discovery message flow.

<table>
<tr><td colspan="3">Type</td><td colspan="2">Code</td><td colspan="2">Checksum</td></tr>
<tr><td>R</td><td>S</td><td>O</td><td colspan="4">Reserved</td></tr>
<tr><td colspan="7">Target Address</td></tr>
<tr><td colspan="7">Router-Delegation</td></tr>
<tr><td colspan="3">Timestamp-Delegation</td><td colspan="2">Lifetime-Delegation</td><td colspan="2">Options</td></tr>
</table>

Figure 6: Modified NA message format.

6.3 Router-Delegation Revocation

The third step named Router-Delegation Revocation is dedicated when the MN_1 returns to its home network. Therefore, it sends a NA message to all network nodes (Destination address FF02::1) with the following falgs:

- R and S flags are not set.
- O flag is set.

The override flag (o) is set to indicate that the information in this NA should override any existing neighbor cache entry and update the link layer address.

7 ANALYSIS AND VERIFICATION OF THE PROPOSED SCHEME

7.1 Security Analysis

Our objective is to overcome the limitation of the incompatibility of SEND protocol with the context of mobility and especially with the proxy Neighbor Discovery in a secure way. In this subsection, we will enumerate the covered security requirements by our proposed scheme.

1) Authentication

In order to minimize spoofing attack, our proposed scheme guarantees authentication between:

- HA and MN1: When the MN1 leaves its home network, authentication is done through the modified BU message.
- MN2 and HA: When the HA emit NA message on behalf of MN1, the authentication is effected through the modified NA message
- HA/MN2 and MN1: When the MN1 returns to its home network, this authentication is done through the NA message.

2) Anti Replay Attack:

To prevent reply attack, we add the following fields:

- **TimeStamp-Delegation:** When communication node receives message, it will further deal with the message only if the TimeStamp-Delegation is in a reasonable range.
- **Lifetime-Delegation:** is used to eliminate a long term Router-Delegation.

7.2 Automated Formal Security Analysis

To verify the security of *ISEND* protocol, we have used the Security Protocol Animator Software (SPAN) for the Automated Validation of Internet Security Protocols and Applications (AVISPA project).

SPAN integrates four automatic security analysis and verification back-end: “On-the-Fly Model-Checker” (OFMC), “Constraint Logic-based Attack Searcher” (Cl-AtSe), SAT-based Model-Checker (SATMC) and Tree Automata based Automatic Approximations for the Analysis of Security Protocols (TA4SP).

The first step of the verification consists of modeling our solution using HLPSL formal language of AVISPA. Generally, any HLPSL code in AVISPA consists of role, session, environment and goal sections. In our HLPSL specification, we defined three basic roles: the MN_1, HA and MN_2. Each of these roles implements its related part of Secure ISEND.

SPAN can only deal with the authentication and confidentiality properties. So, we can verify authentication of agents on certain parameters. An authentication security goal consists of witness and request events used to check this property. The first authentication to be checked is between the HA and MN$_1$. We specify this goal as follow:

- The HA authenticates the MN1with {Mac'}_inv(K)
  In the transition of HA, we add the following line:

  request(HA, MN$_1$auth_1, {Mac'}_inv(K))

  And in the transition of MN1, we add the following line

  witness(MN$_1$,HA,auth_1, {Mac'}_inv(K))

The second authentication to be checked is between the HA and MN$_2$. We specify this goal as follow:

- The MN2 authenticates the HA with {Mac'}_inv(K)
  In the transition of MN2, we add the following line:

  request(MN$_2$,HA,auth_2, {Mac'}_inv(K))

  And in the transition of HA, we add the following line

  witness(HA, MN$_2$,auth_2, {Mac'}_inv(K))

- The other authentication should be checked when the MN1 returns to its home network. This authentication is done through the NA message transmit by MN1 to all neighbors nodes.
  In the transition of HA, we add the following line:

  request(HA,MN$_1$,auth_3,na({{Mac'} _inv(K).tmp.lifetime_inv(k)))

In the transition of MN$_2$, we add this line:

request(MN2,MN$_1$,auth_4,na({{Mac'} _inv(K).tmp.lifetime_inv(k)))

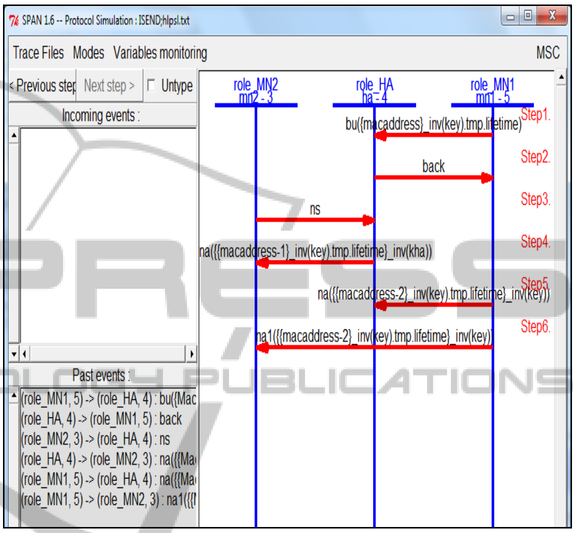
And in the transition of MN1, we add these following lines

witness(MN$_1$,HA,auth_3,na({{Mac'} _inv(K).tmp.lifetime_inv(k)))
witness(MN1,MN2,auth_4,na({{Mac'} _inv(K).tmp.lifetime_inv(k)))

Finally, in the goal section, we add the following line:

authentication on auth_1,auth_2,auth_3,auth_4

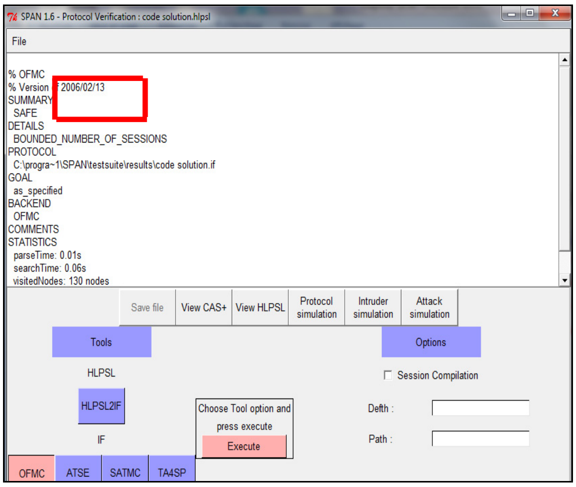
When *auth_1*, *auth_2*, *auth_3* and *auth_4* are declared as *protocol_id.*
The animation of the HLPSL specification with SPAN is illustrated in the figure 7.


SPAN 1.6 -- Protocol Simulation : ISEND;hlpsl.txt
Trace Files
Modes
Variables monitoring
MSC
< Previous step
Next step >
□ Untype
Incoming events :
Past events :
role_MN2
mn2 - 3
role_HA
ha - 4
role_MN1
mn1 - 5
Step1.
bu({macaddress}_inv(key).tmp.lifetime)
Step2.
back
Step3.
ns
Step4.
na({{macaddress-1}_inv(key).tmp.lifetime}_inv(kha))
Step5.
na({{macaddress-2}_inv(key).tmp.lifetime}_inv(key))
Step6.
na1({{macaddress-2}_inv(key).tmp.lifetime}_inv(key))

```
(role_MN1, 5) -> (role_HA, 4) : bu({Mac
(role_HA, 4) -> (role_MN1, 5) : back
(role_MN2, 3) -> (role_HA, 4) : ns
(role_HA, 4) -> (role_MN2, 3) : na({{Ma
(role_MN1, 5) -> (role_HA, 4) : na({{Ma
(role_MN1, 5) -> (role_MN2, 3) : na1({{I
```

Figure 7: Exchange messages of ISEND with SPAN.

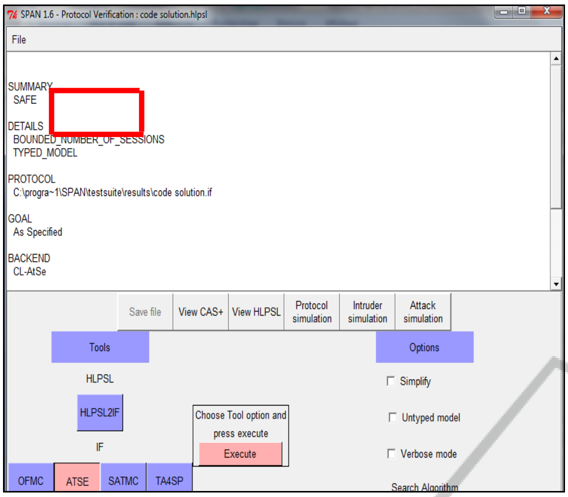
The result of the simulation of *ISEND* using SPAN has proved that defined goals are achieved, and it found to be a safe scheme. Figures 8 and 9 show the messages returned by OFMC and Cl-AtSe respectively. No discovered attacks were found, and the security goals are reached.



```
% OFMC
% Version of 2006/02/13
SUMMARY
  SAFE
DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
  C:\progra~1\SPAN\testsuite\results\code solution.if
GOAL
  as_specified
BACKEND
  OFMC
COMMENTS
STATISTICS
  parseTime: 0.01s
  searchTime: 0.06s
  visitedNodes: 130 nodes
```

□ Session Compilation
Defth :
Path :

Figure 8: OFMC performance analysis results.



```
SUMMARY
  SAFE

DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
  TYPED_MODEL

PROTOCOL
  C:\progra~1\SPAN\testsuite\results\code solution.if

GOAL
  As Specified

BACKEND
  CL-AtSe
```

Figure 9: Cl-ATSE performance analysis results.

8 CONCLUSION

Due to the rapid growth of wireless networks, it is necessary to deal with new requirements and challenges of security. Among the most interesting protocols in the IPv6 suite, which are prone to various threats in case of mobility events, we investigate the NDP protocol suffering from spoofing address and Denial of service attacks. These limitations lead to the appearance of the SEND protocol. Although, it was designed to enhance the security of the NDP protocol, SEND still suffers from numerous vulnerabilities. Therefore, to enhance security of SEND and to overcome these limitations, we investigate in this paper the problem of incompatibility with the proxy Neighbor Discovery function used in Mobile IPv6. Towards this objective, this paper describes the proposed protocol named Improved Secure Neighbor Discovery (ISEND) which adapts SEND protocol to the context of mobility and extends it to new functionalities. *ISEND* has been modeled and verified using SPAN which has proved that authentication goals are achieved. Hence, the scheme is safe and efficient when an intruder is present.

Future works will be focused on resolving the incompatibilities between Anycast addresses and SEND, as well as problems related to the Cryptographically Generated Addresses.

REFERENCES

T. Narten et al., “Neighbor Discovery for IP Version 6 (IPv6),” RFC 4861, Sept. 2007; http://tools.ietf.org/html/rfc4861.

P. Nikander, ed., J. Kempf, and E. Nordmark, “IPv6 Neighbor Discovery (ND) Trust Models and Threats”, IETF, RFC 3756, May 2004. http://tools.ietf.org/html/rfc3765.

YE. Gelogo, RD. Caytiles, and B. Park, “Threats and Security Analysis for Enhanced Secure Neighbor Discovery Protocol (SEND) of IPv6 NDP Security” International Journal of Control and Automation Vol. 4, No. 4, December, 2011.

J. Arkko, J. Kempf, B. Zill, and P. Nikander, “SEcure Neighbor Discovery (SEND),” IETF, RFC 3971, March 2005. http://tools.ietf.org/html/rfc3971.

S. Krishnan, J. Laganier, M. Bonola, and A. Garcia-Martinez, “Secure Proxy ND Support for SEND”, IETF, RFC 6496, February 2012. http://tools.ietf.org/html/rfc6496.

J.-M. Combes, S. Krishnan, and G. Daley, “Securing Neighbor Discovery Proxy: Problem Statement,” IETF, RFC 5909, July 2010. http://tools.ietf.org/html/rfc5909

P. Nikander and J. Arkko, “Delegation of Signalling Rights”, In Proceeding of the Security Protocols, 10th International Workshop, Cambridge, UK, April 16-19, 2002, LNCS 2845, pp. 203-212, Springer, 2003.

T. Cheneau, M. Laurent Network, “Using SEND Signature Algorithm Agility and Multiple-Key CGA to Secure Proxy Neighbor Discovery and Anycast Addressing”, In 6th Conference on Network Architectures and Information Systems Security (SAR-SSI), 2011, pp. 1 – 7

The avispa project. http://www.avispaproject.org/