Journal of Engineering Science and Technology
Vol. 13, No. 9 (2018) 2898 - 2915
© School of Engineering, Taylor's University

IMPLEMENTATION OF TRUST NEIGHBOR DISCOVERY ON SECURING IPv6 LINK LOCAL COMMUNICATION

SUPRIYANTO PRAPTODIYONO[1,*], TEGUH FIRMANSYAH[1],
IZNAN H. HASBULLAH[2], RAJA KUMAR MURUGESAN[3],
AZLAN OSMAN[4], CHONG YUNG WEY[2]

[1]Department of Electrical Engineering, Universitas Sultan Ageng Tirtayasa, Indonesia
[2]National Advanced IPv6 Centre (NAv6), Universiti Sains Malaysia
[3]School of Computing and IT, Taylor's University, Taylor's Lakeside Campus, Malaysia
[4]School of Computer Sciences, Universiti Sains Malaysia, Malaysia
[*]Corresponding Author: supriyanto@untirta.ac.id

Abstract

Neighbour Discovery Protocol is a core IPv6 protocol used within the local network to provide functionalities such as Router Discovery and Neighbour Discovery. However, the standard of the protocol does not specify any security mechanism but only recommends the use of either Internet Protocol Security (IPSec) or Secure Neighbor Discovery (SEND) that has drawbacks when used within IPv6 local network. Furthermore, neither is enabled by default in the IPv6 local network; leaving the protocol unsecured. This paper proposes Trust-ND with reduced complexity by combining hard security and soft security approaches to be implemented on securing IPv6 link-local communication. The experimentation results showed that Trust-ND managed to successfully secure the IPv6 Neighbour Discovery. Trust-ND significantly cuts down the time to process NDP messages up to 77.21 ms for solicitation message and 100.732 ms for advertisement message. It also provides additional benefit over regular NDP in terms of data integrity for all Trust-ND messages with the introduction of Trust Option.

Keywords: IPv6, Neighbor Discovery Protocol, Security, Trust Management, Vulnerability.

1. Introduction

Internet Protocol is one of the widely used technologies in the 21st century. The current version of Internet Protocol, IPv4, has grown exponentially since its inception in the 1970s until today. The growth of Internet user reaches 923.9% from 2000 until 2017 [1]. This is the root cause of the problem of IP address exhaustion facing IPv4. Fortunately, researchers had anticipated this problem in early to mid-90s and brought forth a new version of IP protocol called IPv6. IPv6 was created not only to solve the IP address exhaustion problem but also designed with many benefits compared to its predecessor such as simpler header format, extensibility and mobility support as well as introducing new concept such as Neighbour Discovery. Neighbour Discovery is realized within NDP, which a core protocol in IPv6 is. The NDP includes three main mechanisms: router discovery, Neighbour Discovery and address auto-configuration [2]. This paper focuses on link-local communication used to discover linked neighbours of an IPv6 node. Neighbours could be routers or hosts in the same subnet. The Neighbour Discovery mechanism includes Neighbour Unreachability Detection, duplicate address detection, next hop determination and address resolution.

As a new protocol, it is inevitable for IPv6 to have a number of security vulnerabilities as being reported in [3]. The vulnerabilities are found mainly in three new features of IPv6: flow label, IPv6 extension header and IPv6 Neighbour Discovery. Detail discussion on IPv6 link-local communication that employs Neighbour Discovery could be found in [4], which classify the security threats into either link layer threat or network layer security threat. Both security threats discussion involved Neighbour Discovery messages-RS, RA, NS, NA and redirect message. According to Narten et al. [2], the messages format and exchange could be seen in more detail.

However, the original standard of IPv6 Neighbour Discovery [2] did not define any security measure to protect Neighbour Discovery mechanisms. It only recommended using either SEND [5] or IPSec [6] without providing any detail explanation on how to implement it. Several studies [7-11] reported the drawbacks of both mechanisms. The main drawback is the processing overhead on IPv6 nodes due to heavy dependency on cryptography mechanism by SEND and IPSec. For IPSec, there is another serious problem-the bootstrapping process [9]. As a result, the adoption of either security mechanisms in real-world remains extremely low and no major Operating System provides a good level of support [8]. Software Engineering Institute [12] reported that the number of insider attacks is on a steady increase. Insider attacks are defined as threats originating from neighbouring nodes. The failure to address the lack of security in IPv6 Neighbour Discovery implementation could result not only in system failure but will also be difficult to recover.

This paper proposes an implementation of a new security mechanism for Neighbour Discovery, called Trust-ND, using trust-based mechanism from soft security approach and combines it with hard security approach to achieve a secure yet lightweight mechanism. The rest of this paper is organized as follows: Section 2 provides an overview of Neighbour Discovery in IPv6 and some well-known weaknesses in its implementation. Section 3 discusses related works on securing Neighbour Discovery, while Section 4 explains the design of the proposed solution. Section 5 provides experimentation setup followed by result and discussion in Section 6. The last section, Section 7 concludes this paper and presents some potential future research works.

2. Overview of Neighbor Discovery in IPv6

As specified by Narten et al. [2], Neighbour Discovery mechanism is part of NDP for IPv6. This mechanism plays a critical role in IPv6 operation. The operation of IPv6 will be impossible without NDP protocol. The protocol allows an IPv6 host to configure its own IPv6 address, set network parameter and link parameter as well as discover the status of another node in the same link.

2.1. IPv6 Neighbor Discovery mechanisms

There are four main mechanisms in IPv6 Neighbour Discovery. This section provides an overview of these mechanisms as follows: address resolution, next hop determination, Neighbour Unreachability Detection and duplicate address detection, as depicted in Fig. 1. Address resolution is used by an IPv6 node to discover neighbour's link-layer address when it needs to send a packet to a specific neighbour within the local network. In principle, it is similar to the ARP in IPv4. Even though nodes are directly connected, without knowing the neighbour's MAC address, an IPv6 node will not be able to communicate with its neighbours. The mechanism is also required when a node needs to send IPv6 packets to an external network via a router. The sender must first know the router's MAC address in order to send the packets.

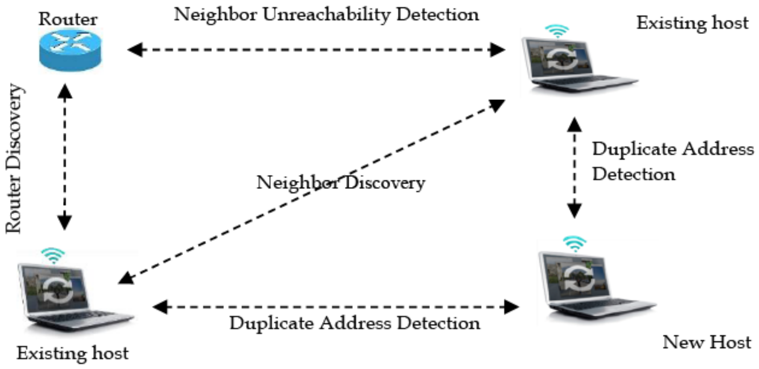

Router
Neighbor Unreachability Detection
Existing host
Router Discovery
Duplicate Address Detection
Neighbor Discovery
Duplicate Address Detection
Existing host
New Host

Fig. 1. Neighbour Discovery mechanisms.

NUD is a mechanism to discover the reachability status of other nodes in the same link. Status of a neighbour is important when a node wants to send an IPv6 packet. If the packet is sent to the external network, the sending node has to know the status of the default router since it will forward the packet [13]. The inactive router could make the packet fail to reach its destination. In case, the IPv6 node has more than one default routers in the link, the NUD can help to identify an inactive router and switch to an active default router. Without NUD, an IPv6 node could potentially send packets to an inactive router, which may cause packets to be lost. By examining the neighbour states, an IPv6 node could send or forward IP packet by just looking at its neighbour cache table.

DAD is a method to ensure the uniqueness of an IPv6 address. It is usually used by a new IPv6 node when running SLAAC mechanism [14]. It is done by sending a multicast message to neighbours announcing its tentative address. If there is no reply to the message within a stipulated time, the tentative address is considered unique within the local network and can be assigned to the sender’s interface. Otherwise, a duplicate address is detected and IP operation on the interface should be disabled [14]. Furthermore, the node is not able to send any IP packets from the interface and silently drop any IP packets received on the interface.

2.2. Threats in IPv6 Neighbour Discovery

The existence of threats and vulnerabilities in NDP, a core protocol in IPv6 implementation as evidenced by many research and studies conducted as well as many solutions proposed. According to Nikander et al. [15], RFC 3756 is the first document that modelled trust in Neighbour Discovery with a list of potential threats. It was referenced by a number of researchers and reported in [4, 8, 16-18]. The threats are summarized in Table 1.

Table 1. Summary of threats on Neighbour Discovery.

Threats	Attacking methods	Impacts
ND DoS attack	Sending thousands of NS and NA messages	The victim is forced to process the NS messages and continuously update its cache table
Neighbour cache poisoning	Poisoning the target node’s neighbour cache	Communication failure for the host
NS/NA spoofing	NS and NA messages	An attacker could perform several malicious activities by modifying one or more fields in the NDP message
NUD failure	A malicious node replies by fabricating the NA message	This is a failure on NUD mechanism, which results in lost packet
DAD DoS attack	An attacking node crafts an NA message as a reply to the NS on DAD process	The node will not be able to configure its own IPv6 address and thus will be denied using networking services
Replay attacks	Intercepting NDP messages and retransmitting them	The victim processes unintended messages that resulting in waste resources

3. Related Works

Since IPv6 is an ultimate technology that would be used by Internet users over the world, attention to its security should be taken seriously. All threats listed in Section 2 also present in IPv4; however, it is more dangerous within IPv6 realm due to its critical reliance on NDP within the local network. Blocking off ICMPv6 messages, which is used by NDP, are not an option when using stateless auto configuration. Researchers attempt to prevent the threats by proposing numbers of the method. This section discusses the related works on securing ND in IPv6.

3.1. Secure Neighbour Discovery

SEND was standardized in [5] with the addition of four new NDP options to prevent NDP messages exploitation and address spoofing. The new options are CGA option, RSA signature option, nonce option and timestamp option. The CGA option uses the cryptographic method on the IPv6 address to prevent any form of address spoofing and stealing [19]. A number of papers evaluated the effectiveness of the CGA option such as [20-23]. All authors reached the same conclusion that the process to generate CGA is costly and has heavy calculation especially when high sec value is used. It can take years to generate an IPv6 address [24]. RSA signature option was introduced to provide message integrity and authenticate the sender. It is very effective in protecting data, but in local networking, the use of RSA requires unnecessary effort as reported in [7]. The RSA introduced 99 percent overhead on SEND operation.

Nonce option and time stamp option were added to prevent a replay attack. When the size of all new NDP options was taken into consideration, a problem on bandwidth consumption would become apparent. The cumulative size of all SEND options is 368 bytes compared to a mere 80 bytes for the original RA message, which is the largest of NDP message [25]. Those are the reasons why major OS vendors are reluctant to implement SEND in their products [8].

3.2. Compact Neighbour Discovery

Compact ND [26] focus is on preventing ND DoS attack from flooding attack, ND message spoofing or neighbour cache poisoning. These attacks could consume the bandwidth of the entire network. Compact ND used bloom filter [27] concept to filter NS messages in the queue of an access router. The bloom size determination is important to obtain an optimal size of hash calculation in addition to the target address in NS message. The bloom size would direct all incoming IP packets through a tunnel queuing before reaching the access router. This scheme prevents ND DoS attack by dropping packets with the unknown destination address. However, since the task of dropping packet is handled by the access router, this would add an extra burden for the router. In addition, the bloom filter uses the MD5 hash algorithm [28], which has been broken by a few documented attacks [29, 30].

3.3. Controlling abnormal ND messages

This scheme [31] is used to prevent ND DoS attack by differentiating normal packets from abnormal one since this type of attack employs abnormal packet with fictitious IP address. The scheme checks the destination IP field of every incoming packet into LAN for bogus entry. If the destination IP exist, then the packet is considered as a normal packet; otherwise, it is considered as abnormal and will be put in the low priority queue but not discarded. A similar scheme, IP labeling and packet marking [32] was proposed to protect IPv6 LAN from ND-DoS attack originating from both outside and inside the local network. Access router has to check all ingress traffic to determine whether the destination IP addresses exist within the LAN or not. If the IP address is valid, it will be forwarded to the destination and labelled as a high priority. Otherwise, the packet will be marked as low priority.

Egress IPv6 traffic will be checked on its source IP address based on active and inactive IP address. Packets originating from the host with an active IPv6 address will be labelled high priority. Otherwise, the packet will be marked as suspicious, which would either be discarded or forwarded as low priority. These two schemes introduce additional tasks for the access router that would reduce the forwarding capability as the main task of the router.

3.4. NS/NA spoofing detection

Barbhuiya et al. [33] had devised a method to detect NS/NA spoofing attack by ensuring the genuineness of the IP-MAC binding using an active verification mechanism. They assumed that all hosts use SLAAC to generate IPv6 address and that the access router has statically assigned an IPv6 address. The method uses IDS

(Intrusion Detection System) as a trusted machine with static IP-MAC binding and two interfaces for port mirroring as well as NS/NA handling. It sends a verification message (NS probe request) upon receiving NS or NA message. To differentiate between a genuine and a spoofed message, the NS probe request, NA and NS messages are kept in cache tables. It checks an NS message by inspecting the immutable fields of the packet header and MAC address consistency (ICMPv6 and IPv6) header. Comparing the packet with the authenticated binding table, if there is a match, then the packet has a genuine IP-MAC pair, otherwise, the message is considered as spoofed and will be logged. The weakness of this method is it requires too many tables, which would consume more memories.

The weaknesses of all related works studied are summarized in Table 2. From the earlier discussion and the information presented in the table, we can conclude that the existing security mechanism for IPv6 link-local communication has issued such as high complexity and partial coverage. Some of the mechanism introduced high network overhead and heavy calculation. They also add an additional burden on the router for checking abnormal packets from an external network; whereas IPv6 local communication is mainly constrained to within internal nodes. As a result, most OS vendors are reluctant to adopt them in their products and this is the reason why the most IPv6 local network is still left unsecured and vulnerable. Based on the aforementioned issues, a new security mechanism for IPv6 Neighbour Discovery is needed with low complexity and covers the whole NDP processes. The next section presents the proposed security mechanism for IPv6 Neighbour Discovery.

Table 2. Summary of related works.

Security mechanism	Weaknesses
Router Advertisement	1. It needs high cost to compute CGA and RSA options 2. It is not able to identify if CGA is used by legitimate node or not 3. Static address configuration cannot use CGA address 4. It runs some algorithm with high complexity 5. It offers an increasing network overhead as well as higher bandwidth
Compact neighbor discovery	1. It is focused on reducing bandwidth consumption rather than security 2. It adds computation cost in access router 3. It requires additional Bloom Filter mechanism to compact NS message 4. It does not address issues on normal packet congestion
Controlling abnormal ND messages	1. It protects ingress filtering only 2. It is unable to prevent insider attack 3. It adds tasks for the access router to check every packet received 4. It still allows receiving abnormal packet that is potentially harmful
NS/NA spoofing detection	1. It requires more tables, which need more memory and CPU resources 2. It unable to prevent RA based attacks 3. The host requires more time to process and build tables

4. Trust Neighbor Discovery

In this paper, we attempt to fill the security gap discussed in Sections 2 and 3 by proposing an integration between hard security and soft security [34]. The heavy calculation of SEND is due to the use of highly complex encryption method such as RSA signature, which is typically used in the data security field. As stated by Kartalopoulos [35], network security requirement is different from data security. Network security's main aim is to protect information during transmission. It concerns message integrity as well as availability. Therefore, as long as the message integrity and availability can be assured, the use of less complex encryption method with lesser complexity is sufficient. Thus, we propose a Trust-ND mechanism that provides message integrity, which is lacking in standard NDP, but with less demand on cryptography calculation. It adopts the concept of distributed trust management [36].

4.1. Trust-ND concept

Trust-ND combines data integrity and availability features provided by cryptography-based hard security and reliability as well as the quality of information supported by trust-based soft security service [37]. This approach is a candidate for devising an alternative security mechanism in the IPv6 local network. Trust-ND appears in the form of Trust Option of an NDP message. The Trust Option format can be found in [38].

Trust-ND consists of six fields begin with three common fields: TYPE, LENGTH and RESERVED. TYPE is a 1-byte field that indicates the type of NDP option with a value of 253. This value was assigned and reserved by IANA for the purpose of experimentation and testing [39]. LENGTH indicates the total size in bytes of the Trust Option including TYPE, LENGTH and RESERVED fields. The Trust Option length is 32 bytes, which is a multiple of 8 octets as required by NDP standard. The RESERVED field is for future use. The other three fields are the proposed fields with the following considerations:

- Message Generation Time is a 4 bytes field that is intended to inform the receiver the time the message was generated at the sender. This is similar to the timestamp that could be used by the receiver to justify whether the message was recently generated. It could also be used by the receiver to prevent a DoS attack by discarding any messages arriving before or after the stated interval time.
- Nonce is a 4 bytes field indicating the uniqueness of each NDP message. It can be differentiated from other messages in the local network. It is proposed to prevent a replay attack. The receiver can discard any messages with identical nonce value. It could also be used by a sender to ensure a received advertisement message is a reply to a correct solicitation message.
- Message Authentication Data (MAD) is a 20 bytes field that contains the output of hash function operation to provide message integrity. This can protect the message from any content modification. According to Saleem et al. [40], the use of the hash function is based on the study.

The Trust Option is then attached to each of the five NDP messages. The IPv6 packet with Trust-ND message is transmitted between IPv6 neighbouring nodes strictly following the standard NDP mechanism.

4.2. Operation of Trust-ND

The operation of Trust-ND consists of four main tasks: message generation, message verification, trust calculation and trust neighbour cache updating as illustrated in Fig. 2. A sending node generates Trust-ND messages following the standard IPv6 packet generation process with the Next Header value of 58 and the Hop Limit value of 255. The Trust Option is then attached to each of the Trust-ND messages. The sender then stores the generation time before sending the message to its destination.

The receiving nodes verify the message and then calculate the trust value of neighbouring nodes based on the Trust Option and other information in the message. The verification is done by looking up the availability of the neighbour's identity in trust table. The trust value obtained from the calculation would then be used to update the node's trust table. The trust table is a modification of the current neighbour cache. It adds the trust value of neighbouring nodes in line with neighbour's IP and MAC address. When the receiver gets an ICMPv6 message from its NIC (network interface card), it first checks the NDP option for TYPE field with a value 253 indicating the presence of Trust Option. If there is no Trust Option, the message is considered as distrusted and the receiver will update its cache table for the message sender. If the message has a Trust Option, the nonce number will be checked. If the number is unique (compared to the nonce number of previous messages), the MAD will be extracted. Otherwise, the message will be discarded because it is considered as a replay attack. Hash operation (SHA-1) will be performed on the extracted message in order to obtain a new authentication data (MAD') value. MAD' will be compared to the original MAD to determine whether the message is trusted or not.

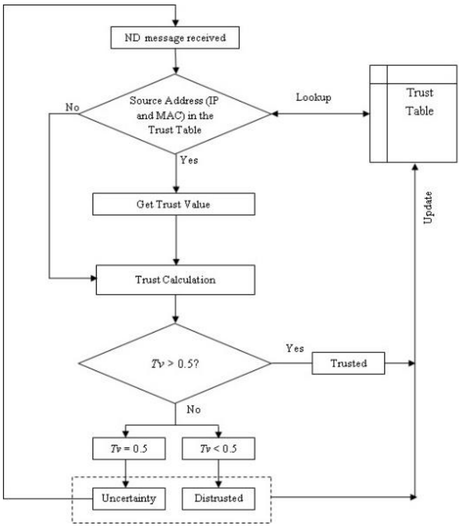


Fig. 2. Trust-ND verification.

4.3. Trust calculation in Trust-ND

The main contribution of the soft security in the proposed Trust-ND is the trust calculation at the receiver. After the message verification is done, the receiver performs trust calculation based on two trust considerations, which are Direct Trust and Knowledge Value [41-44]. The calculation of DT uses Eq. (1) and KV is taken from the existing trust table.

$$DT = \frac{\sum Valid\ Trust{-}ND\ messages}{\sum ND\ messages} \tag{1}$$

Direct Trust is a comparison between the total of Valid Trust-ND messages and the total of ND messages received. The Total Trust value is the addition of Direct Trust and with a Confidence Factor as formulated in Eq. (2). The Confidence Factor is calculated using Eq. (3). The NOM in Eq. (3) is the number of messages received by the receiver node.

$$TT = (Conf\ x\ DT) + ((1 - Conf)\ x\ KV) \tag{2}$$

$$Conf = \frac{nom}{nom+1} \tag{3}$$

The KV is the existing value of trust value obtained during the previous calculation. The KV is taken from the trust value column inside the trust table. In the case for the first ND message, the KV is zero meaning there is no prior knowledge for a particular neighbour. The TT will be a value between 0 and 1. The minimum value of 0 represents a distrusted state of sender while the value of 1 represents a trusted sender. A value of 0.5 is considered uncertainty. When the value state is uncertainty, the receiver requests retransmission to get other information from the particular sender. The Total Trust $0 \leq TT < 0.5$ is categorized as distrusted. Otherwise, the trusted sender value can take any number within $0.5 < TT \leq 1$. The sender ID including IP address and MAC address is stored with the Total Trust value in the receiver's trust table.

5. Experimental Setup

The proposed Trust-ND has been implemented on an IPv6 local network with five nodes representing a router, an attacker, a new host and two existing hosts as shown in Fig. 3. The topology represents a typical IPv6 LAN that runs IPv6 NDP mechanism. There are two existing nodes connected via an Ethernet connection and a new host connected via a wireless medium. Since this is a public network setting, the attacker node may connect to the network any time via a wireless connection.

Table 3 lists hardware specification for hosts and attacker used in Fig. 3. All the hosts and attacker use the Fast Ethernet as layer 2 technology. All the nodes are connected to a layer of 2 switch TO-Link 16 Port 10/100 Mbps. All nodes (except the attacker) are installed with Trust-ND packet processing program developed in JAVA language. The attacker's machine uses BackTrack 5 R3 Operating System bundled with THC IPv6 attack toolkit and a packet crafter tool, scapy. The attacker has the capability to launch NDP threats listed in Section 2 using the tools included in BackTrack 5. The experiments were conducted under normal condition and repeated again with the network under attack. For comparison purpose, the experiments were performed for the original NDP, Trust-ND and SEND mechanism.

Target victim of the attack could be the router, one of the existing hosts or the new host with either a sender or a receiver role. The experiments were done to understand the behaviour of the receiver on processing the original NDP, SEND mechanism and Trust-ND messages. The processing time, bandwidth consumption and functionality were measured to justify the performance of Trust-ND. The results would confirm whether the proposed security mechanism could satisfy the requirements.

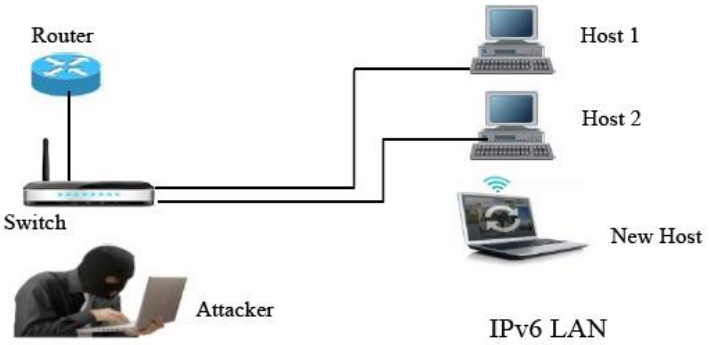


Fig. 3. Experimentation topology.

Table 3. Hardware specification.

Nodes	CPU	Memory	OS
Host 1	Intel (R) Core (TM)2 Duo CPU E6750 @2.66GHz	0.98 GB	Windows XP
Host 2	Intel (R) Core(TM)2 Duo CPU E7500 @2.93GHz	4 GB	Windows 7
New host	Intel (R) Core(TM)2 Duo CPU T5850 @2.16GHz	3 GB	Windows 7
Attacker	Intel (R) Core (TM)2 Duo CPU E6750 @2.66GHz	0.98 GB	Backtrack 5

6. Results and Discussion

Experiments were conducted according to the procedure of standard NDP mechanism to carry Trust-ND message as well as SEND message. Operation of Trust-ND under normal condition would generate ND message with Trust Option. The value of KV that actually the existing trust value is variable. For the first received Trust-ND message, the KV is zero indicating there is no prior communication with the sender. Figure 4 shows an example of Trust-RA message.

The last option in the trust-RA is the trust option with the size of 32 bytes. Based on Fig. 4, the data of trust option can be listed as follows:

Type	: fd
Length	: 04
Reserved	: 00 00
Management	: 0f 2c 00 32
Nonce	: 00 4f 24 37
MAD	: 91 20 5c a3 95 46 67 c1 40 53 39 a9 1d a8 f7 1f 61 b2 b0 d3

There are two processes on the ND message, the sender generates ND message and receiver verifies the ND message. Measurement taken on the processing time for the operation of three NDP mechanisms (original NDP, Trust-ND and SEND) yielded result as shown in Table 4.

Table 4 listed the average processing time of NDP messages for the three NDP mechanisms for both sender and receiver. It also displays the standard deviation and overhead for each mechanism. The original NDP mechanism is the fastest as expected since it does not perform any security verification. The processing time is

0.072 ms for NS message and 0.073 ms for NA message. Since the original NDP mechanism is the existing NDP implementation, it becomes the baseline for the purpose of comparison in this paper. Based on this baseline, the performance of the proposed Trust-ND and SEND mechanism is evaluated.

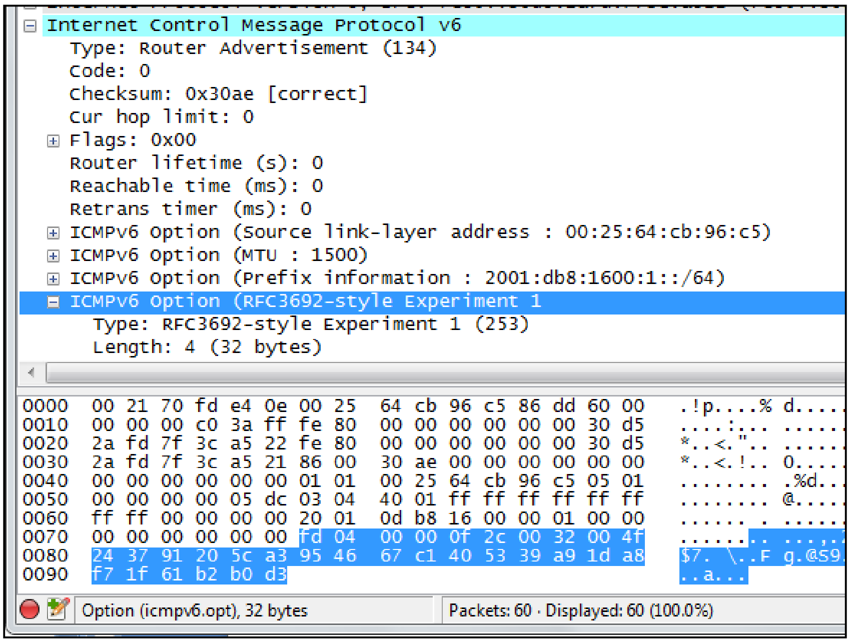
In terms of processing time, the result showed that SEND mechanism took a very long time to process each SEND message. It took an average of 77.347 ms and 100.86 ms to process NS and NA message respectively. A similar result was obtained by another researcher [7] who also measured the processing time of SEND. The high processing time of SEND is due to the complexity of its mechanism and also its message size. On contrary, the proposed Trust-ND only took 0.137 ms to process Trust-NS and 0.134 ms for Trust-NA. The result clearly showed that the Trust-ND has a significantly decrease the network overhead up to 77.21 ms for NS message and 100.73 ms for NA message.

The processing time overhead for each type of message was calculated by comparing the average processing time to the baseline. SEND has a very high overhead, as high as 77.27 ms and 100.79 ms for NS message and NA message respectively. The Trust-ND, on the other hand, has much smaller overhead-0.065 ms for Trust-NS message and 0.061 ms for Trust-NA message. This implies that Trust-ND can decrease the overhead up to 99% for both NS message and NA message. In addition, the standard deviation of Trust-ND message is very small (0.005854 ms), which indicates that the processing of Trust-ND message is more stable and predictable compared to SEND mechanism. The standard deviation of SEND is 11.301 ms.

The Trust-ND implementation also resulted in a reduction in bandwidth consumption compared to SEND mechanism. Based on Praptodiyono et al. [45] observation, NDP messages from the bulk of IPv6 local traffic is in a dual-stack environment. It can reach up to 84% of all ICMPv6 messages in a local network. This clearly implies that NDP message exchanges would affect the amount of available bandwidth in a local network. Table 5 shows the bandwidth consumed by each NDP message for standard NDP, SEND and Trust-ND. Since NDP messages are transmitted locally, the bandwidth consumption has a direct correlation to the message size. The bigger the message size, the higher the bandwidth consumption it would be.

The bandwidth consumption listed in Table 5 justifies the effect of Trust-ND implementation. Trust-ND introduces additional bandwidth consumption of around 30% compared to the existing NDP. In contrast, the SEND has much higher bandwidth consumption, which is 339% increase compared to the existing NDP. Furthermore, Trust-ND can decrease the bandwidth consumption of SEND mechanism up to 309%. Each of the NDP processes has different bandwidth consumption. However, the experiments showed that for all processes, SEND consumed the highest bandwidth as listed in Table 6.

The main problem of SEND is the heavy calculation, which causes high processing time. Since the source of heavy calculation in SEND is the use of complex cryptography, eliminating cryptography will remove the problem. However, omitting cryptography entirely would render NDP to be insecure. Trust-ND proposes a new approach to address this problem by using distributed trust management concept from the soft security approach to complement a less complex cryptography method of hard security approach. The experiment results showed that Trust-ND is able to reduce the processing time.



```
⊟ Internet Control Message Protocol v6
    Type: Router Advertisement (134)
    Code: 0
    Checksum: 0x30ae [correct]
    Cur hop limit: 0
  ⊞ Flags: 0x00
    Router lifetime (s): 0
    Reachable time (ms): 0
    Retrans timer (ms): 0
  ⊞ ICMPv6 Option (Source link-layer address : 00:25:64:cb:96:c5)
  ⊞ ICMPv6 Option (MTU : 1500)
  ⊞ ICMPv6 Option (Prefix information : 2001:db8:1600:1::/64)
  ⊟ ICMPv6 Option (RFC3692-style Experiment 1
      Type: RFC3692-style Experiment 1 (253)
      Length: 4 (32 bytes)

0000  00 21 70 fd e4 0e 00 25  64 cb 96 c5 86 dd 60 00   .!p....% d.....
0010  00 00 00 c0 3a ff fe 80  00 00 00 00 00 00 30 d5   ....:... ......
0020  2a fd 7f 3c a5 22 fe 80  00 00 00 00 00 00 30 d5   *..<."..  ......
0030  2a fd 7f 3c a5 21 86 00  30 ae 00 00 00 00 00 00   *..<.!.. 0.....
0040  00 00 00 00 00 00 01 01  00 25 64 cb 96 c5 05 01   ........ .%d...
0050  00 00 00 00 05 dc 03 04  40 01 ff ff ff ff ff ff   ........ @.....
0060  ff ff 00 00 00 00 20 01  0d b8 16 00 00 01 00 00   ...... . ......
0070  00 00 00 00 00 00 fd 04  00 00 0f 2c 00 32 00 4f   ........ ...,..
0080  24 37 91 20 5c a3 95 46  67 c1 40 53 39 a9 1d a8   $7. \..F g.@S9.
0090  f7 1f 61 b2 b0 d3                                  ..a...

Option (icmpv6.opt), 32 bytes    Packets: 60 · Displayed: 60 (100.0%)
```

Fig. 4. Trust-RA message.

Table 4. Average processing time.

NDP	Original NDP (ms)		Trust-ND (ms)		SEND (ms)	
NDP Message	**NS**	**NA**	**Trust-NS**	**Trust-NA**	**SEND NS**	**SEND NA**
Sender	0.053	0.053	0.066	0.067	54.563	76.441
Receiver	0.019	0.020	0.071	0.067	22.784	24.425
Total	0.072	0.073	0.137	0.134	77.347	100.866
Standard deviation	0.0041	0.0069	0.0076	0.0059	11.478	11.1247
Overhead	Baseline		0.065	0.061	77.275	100.793

Table 5. Bandwidth consumed by NDP messages.

NDP Message Type	Bandwidth (Kbps)		
	NDP	Trust-ND	SEND
RS	0.56	0.816	3.504
RA	0.944	1.2	3.888
NS	0.688	0.944	3.632
NA	0.688	0.944	3.632
Redirect	1.456	1.712	4.400

Table 6. Average bandwidth consumption.

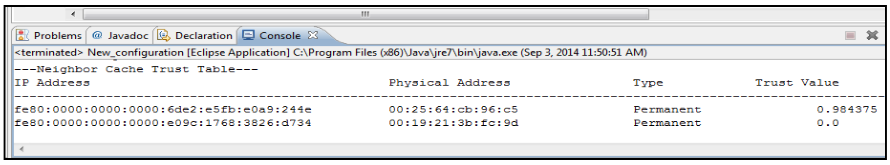
NDP Process	Bandwidth (Kbps)		
	NDP	Trust-ND	SEND
Router discovery	4.336	5.616	19.056
Address configuration	8.384	11.456	43.712
Address resolution	3.44	4.72	18.16
Neighbor unreachability detection	1.376	1.888	7.264
Duplicate address detection	5.504	7.552	29.056
Redirection	2.736	2.992	5.072

Furthermore, the integration between less complex cryptography with soft security approach reduced the NDP option size. The hard security function is combined in one NDP option, named Trust Option while the trust calculation is done in each node. Hence, the Total Trust Option size is only 32 bytes compared to 368 bytes for SEND mechanism. The smaller NDP option size not only decreases the processing time but also reduces bandwidth consumption.

The last measurement is the functionality of Trust-ND, which means measuring how Trust-ND could satisfy the objectives of security. The main focus of NDP security is to assure the integrity of NDP messages as well as to prolong service availability for IPv6 nodes. In order to test the capability of Trust-ND to provide message integrity, experiments have been conducted using parasite 6 tools to perform NS and NA spoofing attack. The result showed Trust-ND node successfully detected all spoofed messages. When the attacker does not implement Trust-ND, the spoofed NDP messages would not carry Trust Option. It is a simple matter for the receiver to detect and discard NDP messages without a Trust Option. Hence, the receiver would not process the message further and any attempt to falsify the information would be thwarted. The receiver then calculates the trust value for the spoofed message sender. The calculation using Eqs. (1) to (4) will update the Trust Neighbor Cache (Trust-NC) information. The second entry on Fig. 5 is the spoofed message from a malicious sender (the IP address belongs to host 2 but the MAC address belongs to the attacker). As a victim, Host 1 is able to detect the attacker's message and treated it as the distrusted sender (Trust Value = 0). This showed that Trust-ND is able to assure the integrity of Trust-ND message.

Another type of attack on NDP, DoS attack, can be carried out by flooding the victim with an enormous amount of NDP messages. Figure 6 demonstrates the experiment result of the flooding attack on SEND mechanism as well as the Trust-ND. Flooding attack experiment was conducted by generating and transmitting a large number of SEND messages at a rate of 300,000 packets per second to a machine that runs SEND mechanism. The SEND machine can process, on average, just 442 NS messages for an average duration of 1.43 seconds before it crashed.

The same experiment was repeated several times for Trust-ND as in SEND mechanism. Up to 100,000 Trust-NS messages were generated and sent to the target host at the rate of 325,000 packets per second with the purpose of crashing the receiver machine. However, such an attempt failed to make the machine crash. It can still process all NS messages without any disruption. This is an evidence that the Trust-ND process is lightweight due to the use of less complex encryption method and having smaller message size, thus allowing it to process a larger number of messages without crashing compared to SEND. This means Trust-ND is more resilient than SEND mechanism in handling flooding attack.



```
<terminated> New_configuration [Eclipse Application] C:\Program Files (x86)\Java\jre7\bin\java.exe (Sep 3, 2014 11:50:51 AM)
---Neighbor Cache Trust Table---
IP Address                                Physical Address           Type         Trust Value
-------------------------------------------------------------------------------------------------
fe80:0000:0000:0000:6de2:e5fb:e0a9:244e   00:25:64:cb:96:c5          Permanent       0.984375
fe80:0000:0000:0000:e09c:1768:3826:d734   00:19:21:3b:fc:9d          Permanent       0.0
```

Fig. 5. Trust neighbor cache.

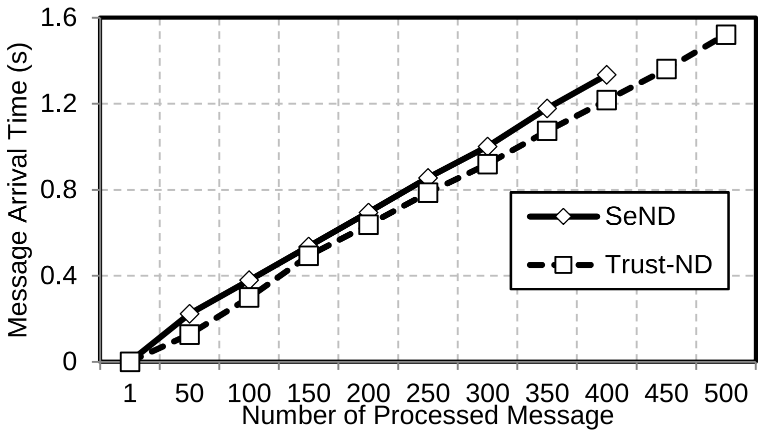


Fig. 6. Flooding attacks.

7. Conclusion

The development of IPv6 as the successor of IPv4 brought not only benefits but also vulnerabilities. Due to the decision of the designers not to secure the newly introduced NDP, the IPv6 local network is left exposed and vulnerable to various threats from insider attacks.

The security mechanisms recommended for IPv6 NDP such as IPSec and SEND are not trivial to be implemented due to their high complexity. This research proposes Trust-ND to address the problems faced by existing security mechanism for IPv6 NDP. This research focuses on securing NDP in an IPv6 public network utilizing the concept of distributed trust management from soft security approach to complement a less complex cryptography method of hard security approach. Trust Option is added as a new NDP option to assure the integrity of NDP messages. In addition, a Trust Neighbor Cache table is introduced to store the trust state of a particular sender. The entries would be updated based on the result of trust calculation. Experiments were done to validate the operation of Trust-ND and its functionality. The result clearly shows that Trust-ND has significantly less processing time and bandwidth consumption compared to SEND mechanism.

The proposed Trust-ND has been demonstrated to be able to assure message integrity as well as prolong service availability. Further research can be done by extending the scope to include a larger network as well as other network model such as ad hoc network. Since Trust-ND is a mechanism based on distributed trust management, its performance against threats specifically targeted at trust-based security mechanisms such as Sybil and bad-mouthing attacks needs to be further explored. Last but not least, the behaviour of Trust-ND mechanism in a mixed environment, where not all hosts implement Trust-ND, also needs to be investigated.

Acknowledgement

This research was supported by the Directorate General of Higher Education, Ministry of Research, Technology and Higher Education, the Republic of Indonesia in collaboration with Universiti Sains Malaysia and School of Computing and IT, Taylor's University.

This research was supported by the Directorate General of Higher Education, Ministry of Research, Technology and Higher Education, the Republic of Indonesia in collaboration with University Sains Malaysia and the School of Computing and IT, Taylor's University.

Abbreviations

ARP	Address Resolution Protocol
CERT	Computer Emergency Readiness Team
CGA	Cryptographically Generated Address
CONF	Confidence Factor
DAD	Duplicate Address Detection
DoS	Denial of Service
DT	Direct Trust
ICMPv6	Internet Control Message Protocol version 6
IPSec	Internet Protocol Security
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
KV	Knowledge Value
LAN	Local Area Network
MAC	Media Access Control
MAD	Message Authentication Data
MD5	Message Digest 5
NA	Neighbour Advertisement
ND	Neighbour Discovery
NDP	Neighbour Discovery Protocol
NOM	Nominal (number of message)
NS	Neighbour Solicitation
NUD	Neighbour Unreachability Detection
OS	Operating System
RA	Router Advertisement
RFC	Request for Comment
RS	Router Solicitation
RSA	Rivest Shamir Adelman
SEND	Secure Neighbor Discovery
SHA-1	Secure Hash Algorithm 1
SLAAC	Stateless Address Auto-Configuration
Trust-N	Trust Neighbor Cache
Trust-ND	Trust Neighbor Discovery
TT	Total Trust

References

1. Internet World Stats. (2017). Usage and population statistic. Retrieved March 14, 2017, from http://www.internetworldstats.com/.
2. Narten, T.; Nordmark, E.; Simpson, W.; and Soliman, H. (2007). Neighbor discovery for IP version 6 (IPv6), RFC 4861. Retrieved December 13, 2017, from https://tools.ietf.org/html/rfc4861.

3. Supriyanto; R.; Murugesan, R.K.; and Ramadass, S. (2012). Review on IPv6 security vulnerability issues and mitigation methods. *International Journal of Network Security & Its Applications(IJNSA),* 4(6), 173-185.
4. Supriyanto; Hasbullah, I.H.; Murugesan, R.K.; and Ramadass, S. (2013). Survey of internet protocol version 6 link local communication security vulnerability and mitigation methods. *IETE Technical Review*, 30(1)**,** 64-71.
5. Arkko, J.; Kempf, E.; Zill, B.; and Nikander, P. (2005). SEcure neighbor discovery (SEND). RFC 3971. Retrieved December 13, 2017, from https://tools.ietf.org/html/rfc3971.
6. Stockebrand, B. (2007). IPv6 in practice. Retrieved September 28, 2018 from https://www.springer.com/la/book/9783540245247.
7. An, G.; Kim, K.; Jang, J.; and Jeon, Y. (2007). Analysis of SEND protocol through implementation and simulation. *Proceedings of the International Conference on Convergence Information Technology (ICCIT 2017).* Gyeongju, South Korea, 670-676.
8. AlSa'deh, A.; and Meinel, C. (2012). Secure neighbor discovery: Review, challenges, perspectives, and recommendations. *IEEE Security & Privacy,* 10(4), 26-34.
9. Arkko, J.; and Nikander, P. (2005). Limitations of IPsec policy mechanisms. Security protocols. *Lecture Notes in Computer Science*, 3364, 241-251.
10. Wen, X.; Xu, C.; Guan, J.; Su, W.; and Zhang, H. (2010). Performance investigation of IPSEC protocol over IPv6 network. *Proceedings of the International Conference on Advanced Intelligence and Awareness Internet (AIAI 2010).* Beijing, China, 174-177.
11. Arkko, J.; Aura, T.; Kempf, J.; Mantyla, V.-M.; Nikander, P.; and Roe, M. (2002). Securing IPv6 neighbor and router discovery. *Proceedings of the 1st ACM Workshop on Wireless Security (Wise '02).* Atlanta, Georgia, United States of America, 77-86.
12. Software Engineering Institute (2013). How bad is the insider threat? *US State of Cybercrime Survey*. Carnegie Mellon University.
13. Blanchet, M. (2006). *Migrating to IPv6: A practical guide to implementing IPv6 in mobile and fixed networks*. Quebec, Canada: John Wiley & Sons Ltd.
14. Thomson, S.; Narten, T.; and Jinmei, T. (2007). IPv6 stateless address autoconfiguration. RFC 4862. Retrieved December 13, 2017 from https://tools.ietf.org/html/rfc4862.
15. Nikander, P.; Kempf, J.; and Nordmark, E. (2007). IPv6 neighbor discovery (ND) trust models and threats. RFC 3756. Retrieved December 13, 2017 from https://tools.ietf.org/html/rfc3756.
16. Gelogo, Y.E.; Caytiles, R.D.; and Park, B. (2011). Threats and security analysis for enhanced secure neighbor discovery protocol (SEND) of IPv6 NDP security. *International Journal of Control and Automation,* 4(4), 179-184.
17. Kukec, A.; Krishnan, S.; and Jiang, S. (2011). The secure neighbor discovery (SEND) hash threat analysis. RFC 6273. Retrieved December 13, 2017 from https://tools.ietf.org/html/rfc6273.

18. Martin, C.E.; and Dunn, J.H. (2007). Internet protocol version 6 (IPv6) protocol security assessment. *Proceedings of the IEEE Military Communications Conference (MILCOM 2007).* Orlondo, Florida, United States of America, 1-7.
19. Aura, T. (2005). Cryptographically generated addresses (CGA). RFC 3972. Retrieved December 13, 2017, from https://tools.ietf.org/html/rfc3972.
20. Bos, J.; and Ozen, O. (2009). Analysis and optimization of cryptographically generated addresses (CGA). *Project Report of Security and Cooperation in Wireless Network*. 44 pages.
21. Cheneau, T.; Boudguiga, A.; and Laurent, M. (2010). Significantly improved performances of the cryptographically generated addresses thanks to ECC and GPGPU. *Journal Computers and Security*, 29(4), 419-431.
22. Qadir, S.; and Siddiqi, M.U. (2011). Cryptographically generated addresses (CGAs): A survey and an analysis of performance for use in mobile environment. *International Journal of Computer Science and Network Security*, 11(2), 24-31.
23. Alsa'deh, A.; Rafiee, H.; and Meinel, C. (2012). Stopping time condition for practical IPv6 cryptographically generated addresses. *Proceedings of the International Conference on Information Networking*. Bali, Indonesia, 257-262.
24. Rafiee H.; and Meinel, C. (2013). SSAS: A simple secure addressing scheme for IPv6 autoconfiguration. *Proceedings of the Eleventh Annual International Conference on Privacy, Security and Trust (PST).* Tarragona, Spain, 275-282.
25. Supriyanto; Murugesan, R.K.; Osman, A.; and Ramadass, S. (2013). Security mechanism for IPv6 router discovery based on distributed trust management. *Proceedings of the IEEE International Conference on RFID Technologies and Applications (RFID-TA)*. Johor Bahru, Malaysia, 1-6.
26. Mutaf, P.; and Castelluccia, C. (2005). Compact neighbor discovery: a bandwidth defense through bandwidth optimization. *Proceedings of the IEEE 24th Annual Joint Conference on Computer and Communications Societies*. Miami, Florida, United States of America, 2711-2719.
27. Bloom, B.H. (1970). Space/time trade-offs in hash coding with allowable errors. *Communications of the ACM*, 13(7), 422-426.
28. Rivest, R. (1992). The MD5 message-digest algorithm. RFC 1321. Retrieved December 13, 2017, from https://tools.ietf.org/html/rfc1321.
29. Touch, J.D. (1995). Performance analysis of MD5. *Proceedings of the Applications, Technologies, Architectures, and Protocols for Computer Communications.* Massachusetts, United States of America, 77-86.
30. Barchett, L.D.; Banerji, A.; Tracey, J.M.; and Cohn, D.L. (1996). Problems using MD5 with IPv6. *Journal of Performance Evaluation*, 27-28, 507-518.
31. An, G.; and Nah, J. (2006). Effective control of abnormal neighbor discovery congestion on IPv6 local area network. Ubiquitous intelligence and computing. *Lecture Notes on Computer Science*, 4159, 966-976.
32. An, G.; and Kim, K. (2008). Real-time IP checking and packet marking for preventing ND-DoS attack employing fake source IP in IPv6 LAN. Autonomic and trusted computing. *Lecture Notes on Computer Science*, 5060, 36-46.
33. Barbhuiya, F.A.; Biswas, S.; and Nandi, S. (2011). Detection of neighbor solicitation and advertisement spoofing in IPv6 neighbor discovery protocol.

Proceedings of the 4th International Conference on Security of Information and Networks. Sydney, Australia, 111-118.

34. Josang, A. (2007). Trust and reputation systems. Foundations of security analysis and design IV. *Lecture Notes of Computer Science*, 4677, 209-245.
35. Kartalopoulos, S.V. (2008). Differentiating data security and network security. *Proceedings of the IEEE International Conference on Communications*. Beijing, China, 1469-1473.
36. Blaze, M.; Feigenbaum, J.; and Lacy, J. (1996). Decentralized trust management. *Proceedings of the IEEE Symposium on Security and Privacy*. Oakland, California, United States of America, 164-173.
37. Govindan, K.; and Mohapatra, P. (2012). Trust computations and trust dynamics in mobile adhoc networks: A survey. *IEEE Communications Surveys & Tutorials*, 14(2), 279-298.
38. Praptodiyono, S.; Hasbullah, I.H.; Anbar, M.; Murugesan, R.K.; and Osman, A. (2015). Improvement of address resolution security in IPv6 local network using trust-ND. *TELKOMNIKA Indonesian Journal of Electrical Engineering,* 13(1), 195-202.
39. Fenner, B. (2006). Experimental values in IPv4, IPv6, ICMPv4, ICMPv6, UDP, and TCP headers. RFC 4727. Retrieved December 13, 2017, from https://tools.ietf.org/html/rfc4727.
40. Saleem, S.; Popov, O.; and Dahman, R. (2011). Evaluation of security methods for ensuring the integrity of digital evidence. *Proceedings of the International Conference on Innovations in Information Technology*. Abu Dhabi, United Arab Emirates, 220-225.
41. Sabater, J.; and Sierra, C. (2005). Review on computational trust and reputation models. *Artificial Intelligence Review*, 24(1), 33-60.
42. Esfandiari, B.; and Chandrasekharan, S. (2001). On how agents make friends: Mechanisms for trust acquisition. *Proceedings of the Fourth Workshop on Deception, Fraud and Trust in Agent Societies*. Montreal, Canada, 27-34.
43. Zahariadis, T.; Trakadas, P.; Leligou, H.C.; Maniatis, S.; and Karkazis, P. (2012). A novel trust-aware geographical routing scheme for wireless sensor networks. *Wireless Personal Communications,* 69(2), 805-826.
44. Almenarez, F.; Marin, A.; Campo, C.; and Garcia, C. (2004). PTM: A pervasive trust management model for dynamic open environments. *Proceedings of the First Workshop on Pervasive Security, Privacy and Trust in Conjunction with Mobiquitous*. Boston, Massachusetts, United States of America, 8 pages.
45. Praptodiyono, S.; Hasbullah, I.H.; Anbar, M.; Murugesan, R.K.; and Osman, A. (2014). Risk analysis of the implementation of IPv6 neighbor discovery in public network. *Proceedings of the International Conference on Electrical Engineering, Computer Science and Informatics*. Yogyakarta, Indonesia, 275-279.