Proceedings of the 2014 Federated Conference on Computer Science and Information Systems pp. 1539–1547
DOI: 10.15439/2014F287
ACSIS, Vol. 2

A New Intrusion Prevention System for Protecting Smart Grids from ICMPv6 Vulnerabilities

Manali Chakraborty, Nabendu Chaki
University of Calcutta
Kolkata, India
Email: manali4mkolkata@gmail.com
nabendu@ieee.org

Agostino Cortesi
DAIS
Universita Ca'
Foscari Venezia
Email: cortesi@unive.it

***Abstract*— Smart Grid is an integrated power grid with a. reliable, communication network running in parallel towards providing two way communications in the grid. It's trivial to mention that a network like this would connect a huge number of IP-enabled devices. IPv6 that offers 18-bit address space becomes an obvious choice in this context. In a smart grid, functionalities like neighborhood discovery, autonomic address configuration of a node or its router identification may often be invoked whenever newer equipments are introduced for capacity enhancement at some level of hierarchy. In IPv6, these basic functionalities like neighborhood discovery, autonomic address configuration of networking require to use Internet Control Message Protocol version 6 (ICMPv6). Such usage may lead to security breaches in the grid as a result of possible abuses of ICMPv6 protocol. In this paper, some potential newer attacks on Smart Grid have been discussed. Subsequently, intrusion prevention mechanisms for these attacks are proposed to plug-in the threats.**

I. Introduction

A SMART grid is an intelligent energy network that integrates the actions of all users connected to it and makes use of advanced information, control, and communication technologies to save energy, reduce cost and increase reliability and transparency [1].

The backbone of the Smart Grid will be its communication network. This network is to connect the different components of the Smart Grid together, and provide two-way communication. IPv6 is a new technology which gained a massive attention, as a supporting layer in smart grid communication. The huge address space of IPv6 supports the network architecture of the smart grid communications. Besides, features like stateless address auto configuration (SLAAC) and IPSec support makes IPv6 more suitable for smart grid. IPv6 also supports prioritization of messages and different Quality of Service models, which complements several smart grid applications [8]. However, with these new advancements in technology, IPv6 is also exposed to various attacks, such as header modification attack, fragmentation attacks , etc. [5], [6]. In this paper, we focus on some of the possible ICMPv6 attacks that are particularly relevant in the context of building networking infrastructure between Smart Meters (SM), Data Collection Units (DCU) and Meter Data Management System (MDMS). We would demonstrate how these could affect the Smart Grid before proposing appropriate Intrusion Prevention Systems (IPS) to protect the grid from such attacks.

IPv4 networks often filter ICMP messages to avoid security concerns. However, for IPv6, this is not possible. ICMPv6 is used for basic functionalities and used by other IPv6 protocols like Neighbor Detection Protocol (NDP). Neighbor Discovery Protocol (NDP) is a protocol used with IPv6 to perform various tasks like router discovery, auto address configuration of a node, neighbor discovery, Duplicate Address Detection, determining the Link Layer addresses of other nodes, address prefix discovery, and maintaining routing information about the paths to other active neighbor nodes [4]. Thus, the implementation of IPv6 in Smart Grid needs some serious care to protect from the security vulnerabilities of the ICMPv6 protocol. NDP uses five ICMPv6 messages. These are:

- Router Solicitation (RS) message: Hosts send RS message to enquire about a legitimate router on the link.
- Router Advertisement (RA) message: Routers send RA message, either periodically or in response to RS message.
- Neighbor Solicitation (NS) message: Hosts send NS message to determine the link layer address of a specific node, and also to verify whether an address is already present on link or not.
- Neighbor Advertisement (NA) message: Hosts send NA message in response to the NS message.
- Router Redirect (RR) message: Routers send RR message to inform a host about a better router on its link.

With higher degree of autonomic control and decision making, a smart grid also becomes subject to several security concerns. Smart grid is generally considered as a heterogeneous, backward compatible, static, self adapting and self healing network, with a large number of devices, where two way communications is provided between Smart Meters and a Supervisory Control and Data Acquisition (SCADA) system. This requires special QoSs, like high restriction on delay, failure and voltage quality [3]. In smart

978-83-60810-58-3/$25.00

grid, availability and integrity are typically considered more important than confidentiality [9]. Also the risk factor is quite high in smart grid as compared to traditional networks. Thus, the existing solutions for cyber security often fall short of the typical requirements for a smart grid.

Some work has been done to secure smart meters and communication network of Smart Grid or SCADA systems [10]. An IPv6 based moving target defense system is provided in [11] to secure the communication between hosts. Most of the network attacks target some specific addresses, so, moving the target address will prevent hosts from being located for an attack. [12], [13], [14] explains different techniques for IPv6 address configuration schemes for smart grid. However, security solutions for specific IPv6 problems, like ICMPv6 attacks, for Smart Grid environment are still need to be addressed. In [16], a distributive, trust based approach to detect attacks in Duplicate Address Detection (DAD) phase was proposed. However, this concentrates only on one type of attack in DAD. In [17], the requirements and practical needs for monitoring and intrusion detection in AMI is discussed. In [18], a layered combined signature and anomaly-based IDS for HAN was proposed. This IDS was designed for a ZigBee based HAN which works at the physical and medium access control (MAC) layers. However, the work only considers the HAN part of AMI. In [19], a specification-based IDS for AMI is proposed. While the solution in [19] relies on protocol specifications, security requirements and security policies to detect security violations, it would be expensive to deploy such IDS since it uses a separate sensor network to monitor the AMI.

We have proposed a new Intrusion Prevention System for providing security against ICMPv6 attacks in smart grid networks. The structure of the paper is as follows. First, we discuss three important functionalities for a Smart Meter: Router Discovery, Duplicate Address Detection and Neighbor Discovery, using NDP and various ICMPv6 messages. Possible attacks and the effects of those attacks on smart grid are analyzed for each function. Finally, we propose an Intrusion Prevention System (IPS) to prevent the attacks in the Router Discovery phase and detect the attacks in the Duplicate Address Detection and Neighbor Discovery phase.

Notice that we do not claim that using NDP or ICMPv6 is the only option for realizing functionalities like router discovery or address configuration in a smart grid. As for example, instead of having an auto configurable addressing scheme, smart grids may also have independent Certifying Authority (CA) for providing addresses to newly installed SMs. However, the cost of installation and maintenance of such centrally controlled architecture may be avoided using auto configurable SMs. This paper aims to expose the security threats there and to propose suitable intrusion prevention mechanisms to safeguard smart grids from ICMPv6 misuses.

II. Smart Grid And ICMPv6 Abuses

Figure 1 shows the communication architecture of Smart Grid. Smart Energy Utility Network (SUN) hierarchically consists of three components: Home Area Network (HAN), Neighborhood Area Network (NAN), and Wide Area Network (WAN) [15]. The HAN provides the communication between the Smart Meters in a home and other appliances in that home. The NAN connects SMs to the Data Collection Units (DCUs), and WAN provides access between the DCUs and Meter Data Management System (MDMS). DCU collects data from hundreds of SMs and sends them to the MDMS. At the lowest level, the smart meters act as hosts in a network and DCUs are the routers of the network. We assume that

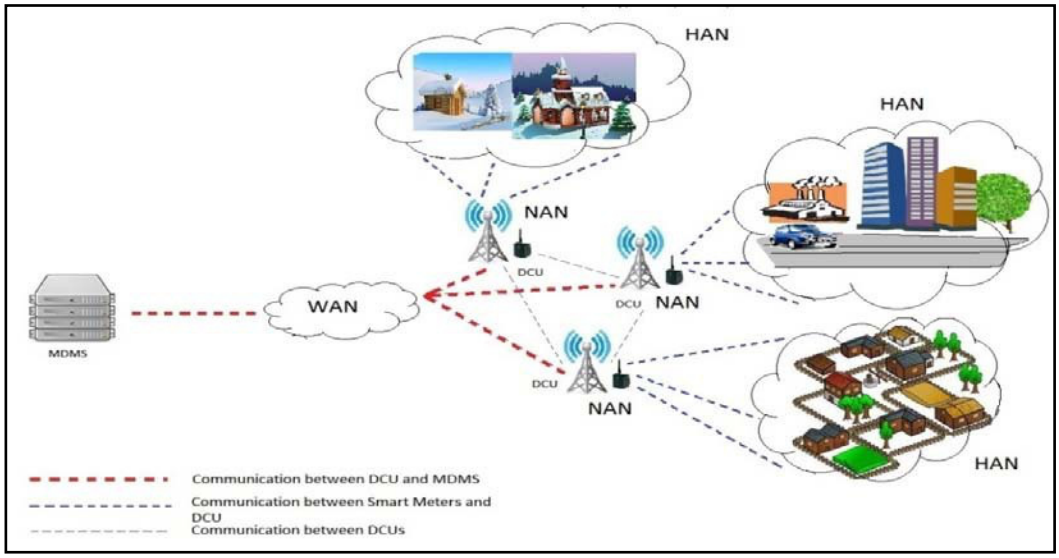

Fig. 1: Communication Architecture of Smart Grid

- Smart Meters are managed by DCUs. When a SM X is installed in a subnet, it should find a DCU, say R, to bind with. X will continue to communicate through DCU R,

until it receives any ICMPv6 Router Redirect (RR) message from R.

- Each DCU keeps a neighbor cache, storing the addresses of all DCUs in its neighborhood.
- Each subnet has a different and unique 64 bit prefix address for addressing SMs within the subnet.
- Each DCU communicates with the SMs within its subnet, and then transmits the aggregated data to DCU.
- Every SM keeps a neighbor cache to store addresses of all its one hop neighbors

A. Router Discovery

When a SM X is installed in a subnet, it should find a DCU to bind with. The Smart Meter X will continue to communicate through that DCU, until it receives any ICMPv6 Router Redirect (RR) message from the previous DCU.

Normal Procedure for Router Discovery

Normally Smart Meters discover their router or DCU through the following steps,

- First, X sends an ICMPv6 Router Solicitation (RS) message to locate a DCU in its local link.
- A legitimate DCU then responds with an ICMPv6 Router Advertisement (RA) message, with a 64 bit prefix address for its subnet.
- Then X registers that DCU as its default router in the link, and auto-configures a global unicast address based on the received prefix.

Attacks in Router Discovery phase

The most prominent attack in this phase occurs if an attacker falsely claims to be a DCU. It can spoof an RA message from a legitimate DCU and send it to the Smart Meter, with or without altering the prefix address for that subnet. In either case, the newly installed Smart Meter registers the attacker as its DCU. If the adversary alters the prefix address, then the Smart Meter will auto-configure its global address based on a wrong prefix. As a result, the Smart Meter will get blocked in the subnet and will not be able to communicate with any other Smart Meter or DCU except the attacker. The situation becomes a bit more complex when the adversary sends the RA message without changing the prefix. In this situation, the Smart Meter can communicate within its subnet. However, it becomes quite impossible for the Smart Meter to communicate beyond its subnet as the registered DCU for the Smart Meter is an attacker who is not recognized by other Smart Meters in the Neighborhood Area Network.

Once an adversary successfully convinces a newly installed Smart Meter of being its valid DCU, it can launch a myriad of conventional network attacks on the Smart Grid. It can launch a man-in-the-middle attack by intercepting packets from the Smart Meters or from the DCUs and suitable changing the Source and Destination address fields such that neither of these two entities are aware of the presence of an attacker in between. The attacker can also tweak the data contained in the intercepted packets. Another traditional network attack is the Denial-of-Service attack. The attacker can overload the network resources by generating spurious packets having the newly installed Smart Meter address as the Source Address.

B. Duplicate Address Detection

After auto configuring the address for itself, the Smart Meter X will want to know whether the address is available for use.

Normal Procedure for Duplicate Address Detection

The following steps are used for duplicated address detection.

- Smart Meter X, sends an ICMPv6 Neighbor Solicitation message for the address it wants to claim.
- If any Smart Meter on that subnet already has that address, then it sends an ICMPv6 Neighbor Advertisement message.
- If X does not receive any NA messages stating that the address has been taken, then X is able to use that address.

Attacks in Duplicate Address Detection phase

An intruder can prevent a Smart Meter from acquiring any auto-configured address, by sending an NA for the corresponding address in every NS message sent out by the Smart Meter. As a result, the Smart Meter will not be able to communicate within the network. Besides, an intruder can block a NA message from an authentic SM. This results in two or more SMs using the same address within a network. As a result of this attack, a legitimate SM can be accused of identity spoofing. Also, more than one assignment of the same address within a network can cause improper functioning during the routing phase.

In order to detect these kinds of attacks, we propose a modified version of the Duplicate Address Detection phase,

- SM X sends an ICMPv6 NS message for the address it wants to acquire.
- On receiving the NS message, every Smart Meter scans its neighbor cache information for that address. If they find the address in their cache, then they send a reply to the X.
- If any Smart Meter on that subnet already has that address, then it sends an ICMPv6 NA message.
- If the X receives neither any NA messages stating that the address has been taken nor receives any messages from its neighbors stating that the address is present in their cache, then X is able to use that address.

If X receives only the NA message from another Smart Meter but no neighborhood information about that address is received, it implies that such an address is not in existence within the subnet and some attacker is trying to prevent X from acquiring that address. If X does not receive any NA message, but its neighbors reply with their cache information stating that the address is present in their neighborhood, then the X concludes that an attacker has intercepted the NA message from the target Smart Meter and has dropped it.

Thus, X is able to use an address only when it neither receives the NA nor any neighborhood cache information from its neighbors.

If the attacker is intelligent enough, it can send both the NA message and also spoof some reply messages from other Smart Meters and change their contents. In that case, SM X will not be able to detect the attack. So, to detect this kind of attack, if a Smart Meter exists with the same address, it not only replies with an NA message but also sends its neighborhood information to X. SM X then sends unicast queries to each of the neighbors found in the reply message to verify the existence of such a Smart Meter. In this way, X can be assured whether he is being duped or whether the particular address is really being used within the subnet. However, since the reply message can also be intercepted by the attacker, it must be broadcast within the network. This will assure the delivery of the reply message to X.

C. Neighbor Discovery

Once the Smart Meter acquires a unique global address, then it can start communication through the DCU. It can also communicate with the other Smart Meters, both in its subnet and in other subnets. Smart Meters on the same subnet can communicate directly with each other without using any router or gateway when a SM has link layer addresses of other neighboring SMs. Thus it is important to store the link layer addresses of the neighboring SMs in the local cache of every SM. Neighbor Discovery facilitates the same.

Normal Procedure for Neighbor Discovery

In order to communicate with a SM B on its own subnet, a Smart Meter A has to perform the following steps,

- First, the SM A sends an ICMPv6 NS message requesting the link-layer address of B.
- If B is present in that subnet, then it replies with an ICMPv6 NA message. SM A knows the MAC address of B from this NA message.
- SM A then creates a neighbor cache entry for B that binds the MAC address of B to its IPv6 address.

Attacks in Neighbor Discovery phase

The attacks of this phase are similar to the attacks of the Duplicate Address Detection phase. Here also an intruder can try to impersonate B, and intercept all packets that are destined to B, or an intruder can block a NA reply from B so that A thinks that B is not present in the network.

III. Proposed IPS to Handle ICMPv6 Threats in Smart Grid

In section 2, we have seen three possible security breaches in Smart Grid for Router Discovery, Duplicate Address Detection and for Neighbor Discovery in sub-sections II.A, II.B and in II.C respectively. The Intrusion Prevention Systems (IPS) against each of these three attacks due to ICMPv6 vulnerabilities have been proposed in the following sub-sections.

A. Intrusion Prevention Mechanism in Router Discovery and Updation phase

In order to prevent these possible security threats, we propose a modified Router Discovery phase as follows,

- First, SM X sends an ICMPv6 RS message to locate a DCU in its local link.
- X receives an ICMPv6 RA message with a 64 bit prefix address for its subnet.
- On receiving the RA message, X extracts the DCU's address from the packet.
- X then broadcasts an ICMPv6 Echo Request message on its subnet.
- Receivers of the ICMPv6 Echo Request message will communicate with their DCU. If a new valid DCU is installed in the subnet, then the other DCUs will have information about the new DCU. If receivers of ICMPv6 Echo Request message receive Router Redirect message (RR) from their current DCU, then they reply with an ICMPv6 Echo Reply message with the address of the new DCU.
- Otherwise, Echo Reply message contains the address of the existing DCUs.
- If the DCU address in the RA message received by SM X matches with a majority of the neighbors' default routers address, then SM X concludes that the DCU is authentic. Consequently, X installs this DCU as its default router in the link, and auto-configures a global unicast address based on the received subnet prefix.
- If the received DCU's address does not match with the address of the default router of the majority of the neighbors, say C, then X concludes that it has been attacked by some adversary and C is the original DCU of that subnet.
- Subsequently, X installs C as its default router in the subnet and auto-configures a global unicast address based on the prefix of C.
- If X does not receive any Echo Reply message within a certain time, then it concludes that it has been blocked by some attacker and sends an SMS alert to the registered mobile number.

Router Updation Phase

DCUs in the Smart Grid network periodically broadcast RA messages to advertise themselves on the subnet. If a Smart Meter receives a RA from a DCU, then they change their existing DCU and register the new DCU as a router in its routing information table.

In this situation an attacker may spoof a RA message and send it to some Smart Meters. On receiving a RA message, Smart Meters then register the attacker as a router. In order to detect this kind of attacks we propose an intrusion prevention mechanism as follows,

- DCUs periodically broadcast RA message.
- On receiving a RA message with new DCU information, every Smart Meter sends a RS message to its existing DCU.

- The existing DCU, on receiving a RS message, checks whether a new DCU with higher priority is available for the subnet.
- If such a DCU exists, it sends a RR message to the SMs with the information of the new DCU. Otherwise, it advertises itself again with a RA message.
- A SM resets its DCU information if and only if it receives a RR message and the DCU information contained within the RR message matches with the previously received RA message. Otherwise, it discards the RA message.

Figure 2 shows a high level view of intrusion detection in Router Discovery and Updation phase, when an attacker spoofs a RA message from DCU and sends it to a Smart Meter X without changing the 64 bit prefix address. In the first half of the figure, an attacker spoofs a RA message and sends it to the newly installed Smart Meter X. In the second half of the figure, an attacker broadcasts a RA message to all the working Smart Meters.

The proposed IPS apparently comes with a boot-strapping limitation. It will not work properly when a new Smart Meter is installed under a new subnet. If Smart Meter X is the first meter in the subnet, then it can't consult with its neighbors to authenticate a legitimate DCU. However, in practice when a new DCU, say K, is to be introduced in a layer just on top of the SMs, some of the SMs under a neighboring DCU will be allocated under K by using RR messages from the current DCU of the respective SMs. The

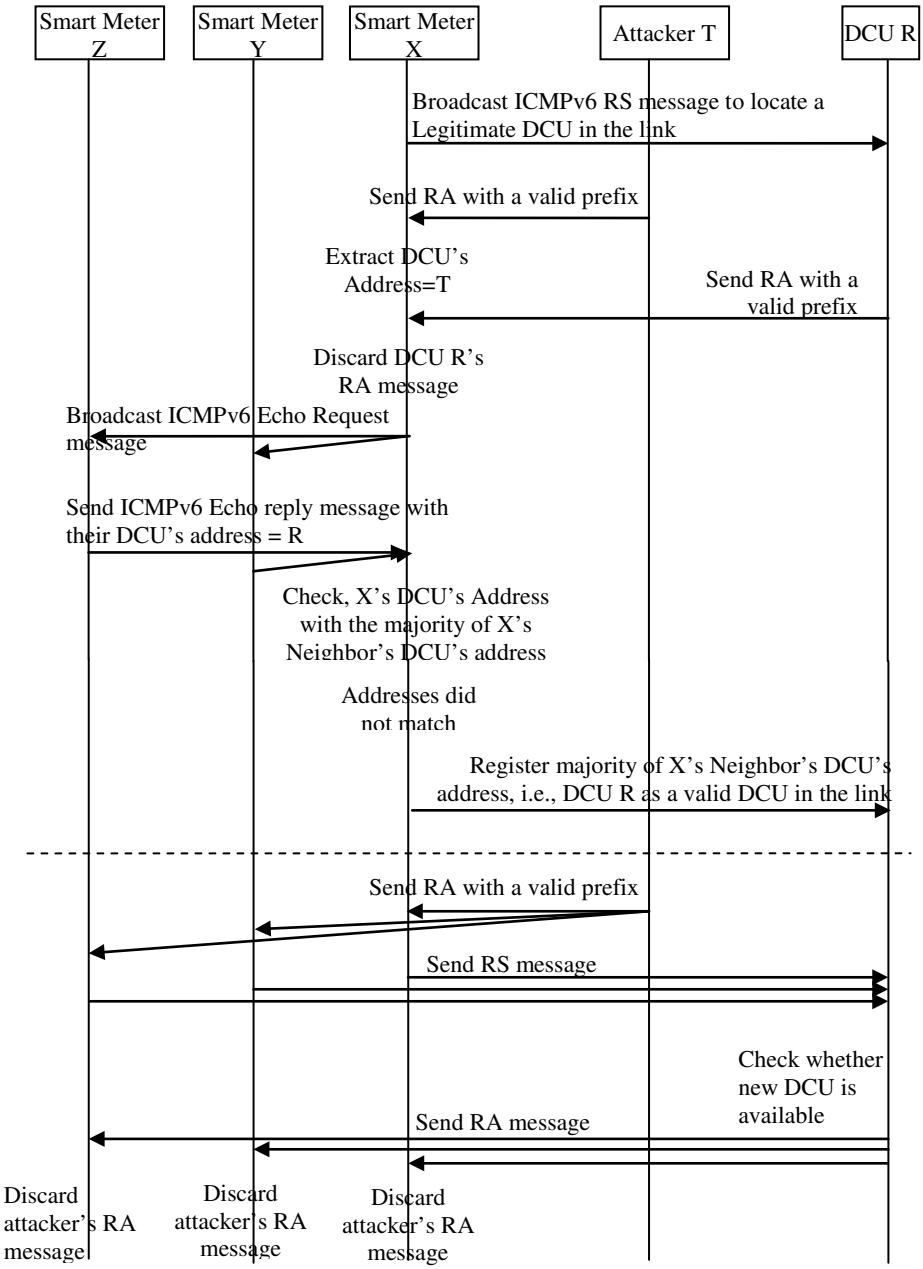

Fig. 2: High level view of Intrusion Prevention in Router Discovery and Updation phase

same is applicable for the entire Smart Grid when a new DCU is to be introduced at any higher level. Thus, the bootstrapping problem as mentioned above will not be an actual bottleneck in the context of smart grid.

B. Intrusion Prevention Mechanism in Duplicate Address Detection

In order to secure Duplicate Address Detection, the following steps are performed,

- SM X sends an ICMPv6 NS message for the address it wants to acquire, say Z.
- If Z already exists in the same subnet, then it broadcasts an ICMPv6 NA message along with the address of all neighbors in its neighbor cache.
- If Z exists, then its one-hop neighbors have Z in their neighborhood cache. These neighbors, on receiving the NS message, reply with a confirmation message.
- X builds the neighbor list of Z from the unicast confirmation messages received from Z's neighbors and verifies it with the neighborhood data sent by the node Z itself.
- If majority of the neighbors confirm the existence of Z, then X concludes that it cannot use Z. Otherwise, X sends unicast queries to those neighbors of Z from which it did not receive any confirmation message.
- Each neighbor N broadcasts Hello message to update its Neighbors. If N finds Z as a neighbor, then it sends a reply confirming existence of Z or remains silent.
- SM X continues sending these queries until either it has a majority decision or all neighbors of Z have been exhaustively queried.
- If X receives both NA message from Z and majority confirmation messages from Z's one-hop neighbors, then it repeats the process with some other auto configured address P. Otherwise, X can use the address Z.

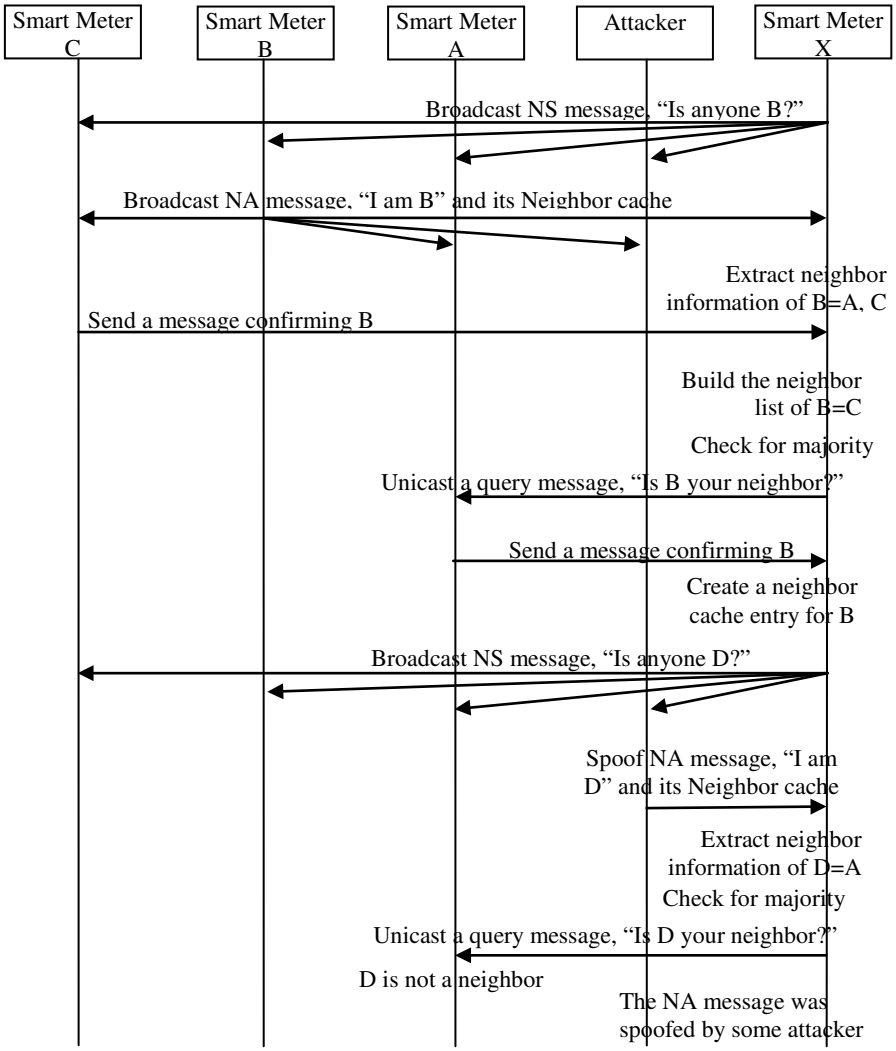

Fig. 3: High level view of Intrusion Prevention in Duplicate Address Detection phase

Figure 3 shows a high level view of intrusion detection in Duplicate Address Detection phase, when X wants to acquire address B. However, in this case, B is already present in the subnet. X verifies the presence of another SM in the subnet, with same address, i.e. B, with the help of B's neighbor list: C, A. Consequently, A wants to acquire

address D. This time an attacker falsely claims himself to be D. X successfully detects this attack.

C. Intrusion Prevention in Neighbor Discovery phase

The detection procedure is quite similar to the Duplicate Address Detection phase as discussed to section III.B. At first, SM X sends an ICMPv6 NS message requesting the link-layer address of Z. On receiving the NS message, every Smart Meter scans its neighbor cache information for that address. If they find the address of Z in their cache, then they send the address of all neighbors of its neighbor cache to X. If node Z is present in that subnet, then it replies with an ICMPv6 NA message and sends the addresses of all neighbors of its neighbor cache. From that NA message, SM X knows the MAC address of Z.

Subsequently, SM X sends unicast queries to each of the neighbors found in the reply message to verify the existence of Z. Every neighbor will broadcast their replies. If X receives a NA messages from Z and majority of reply messages from the neighbors assuring the existence of Z, then SM X creates a neighbor cache entry for Z that binds the MAC address of Z to its IPv6 address. Figure 4 shows a high level view of intrusion detection that may occur during the Neighbor Discovery phase. Here, DCU X wants to communicate with SM Z, but attacker node tries to impersonate Z.

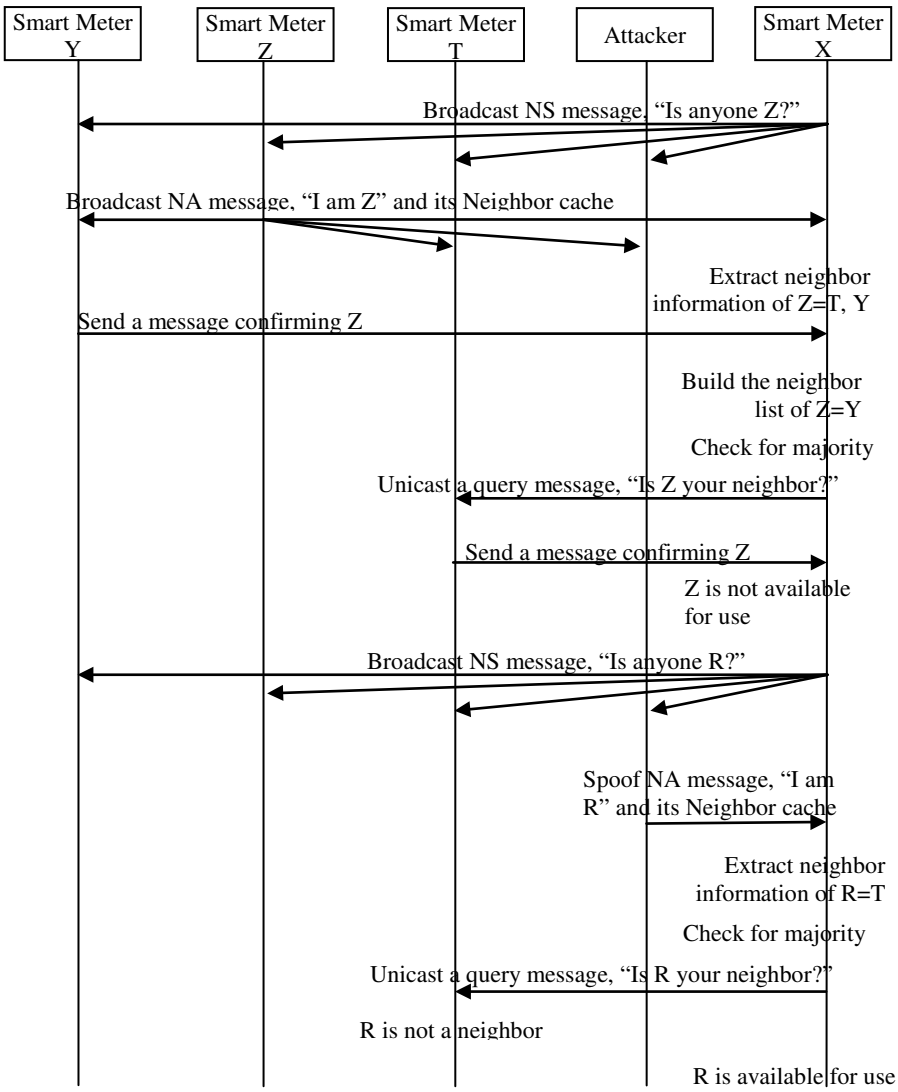

Fig. 4: High level view of Intrusion Detection in Neighbor Discovery phase

IV. Simulation Results

In order to access the performance of ICMPv6 in absence of the proposed IPS and in its presence, we have simulated an environment using Qualnet simulator software. In order to evaluate the performance of the proposed approach, two of the most important performance metrics have been considered. These are false negatives and jitter. *False negative* is measured with respect to both node density and fake router density. Jitter is compared for ICMPv6, with and without our proposed algorithm. The simulation scenario and settings are described in Table I below.

TABLE I.
SIMULATOR PARAMETER SETTINGS

Parameter	Value
Terrain area	1500X1500 m2
Simulation time	100 sec
Mac Layer protocol	DCF of IEEE 802.11b standard
Traffic Model	CBR (Constant Bit Rate)
No. of CBR applications	10 % of the number of nodes
Routing Protocol	AODV
DCU: Smart Meter	1:5

A. False Negative

False Negative occurs when a system cannot detect an attack. False negatives are often a greater threat than false positives. If there wasn't an attack and the system makes a false detection, it can affect the throughput at most. However, if there was an attack and the system is not able to detect it, then it may be disastrous. However, in our proposed IPS, there are no false positives for relatively smaller number of intruders. However, the IPS suffers from false negatives with increasing percentage of malicious nodes. Figure 5 shows that there are no false negative for 2, 4, or 6 malicious nodes out of 50 nodes. The fake router percentage represents the increasing number of fake routers or malicious nodes in a fixed number of nodes. For this experiment we take, 2, 4, 6, 8, 10, 12 fake routers in 50 nodes, with 4, 8, 12, 16, 20, 24 percentages respectively. The false negative increases with increasing number of malicious nodes. Figure 6 shows the effect on false negatives with a linear percentage of malicious nodes, i.e. a fixed percentage of fake routers or malicious nodes in an increasing number of total nodes. We carry out this experiment with 10, 20, 30, 40 and 50 nodes and 20% malicious nodes for each data set. There were no false negatives for 10, 20, 30 and 50 nodes with 20% malicious nodes. The experimental results are in line with reality where any IPS system fails when majority of nodes become compromised.

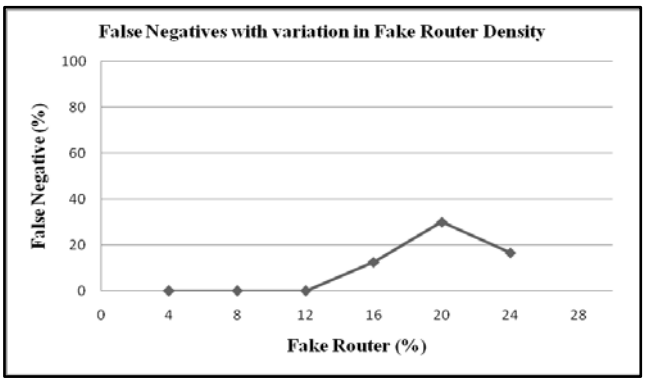

Fig. 5: False Negative vs. Number of Malicious DCUs

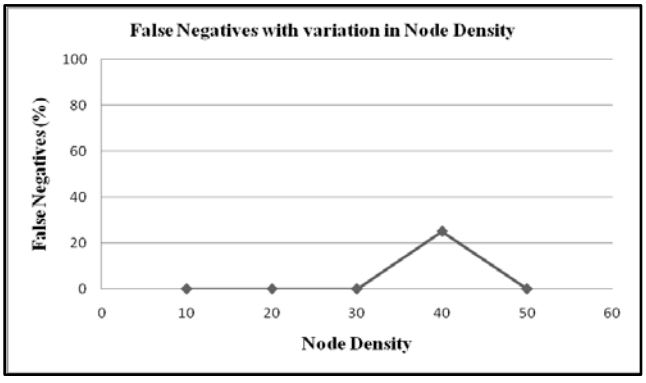

Fig. 6: False Negative vs. Node Density

B. Jitter

Jitter is expressed as an average of the deviation from the network mean latency. We measure both the Jitter for normal ICMPv6 and that with our proposed IPS for ICMPv6. Figure 7 illustrates that the proposed IPS reduces the Jitter.

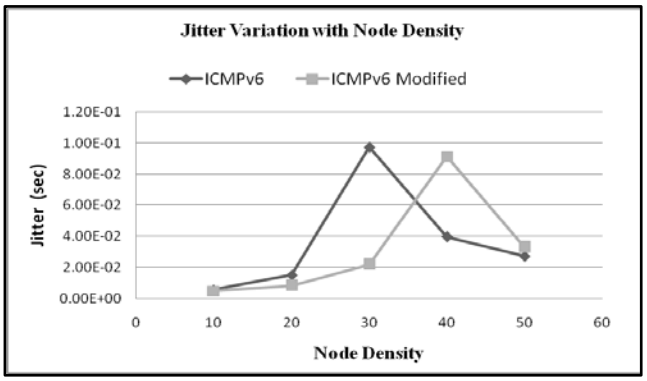

Fig 7: Jitter Vs Node Density for ICMPv6 and Modified ICMPv6

V. CONCLUSION

Integrating IPv6 with Smart Grid is quite natural, as only IPv6 could match the size of Smart Grid network. The large address space, auto configuration of addresses, QoS support technology helps Smart grid to construct a large network with a unique address specified for each and every device, efficient routing, end-to-end security. However, smart grid has very high security demand that needs to be considered before deploying IPv6 towards building Smart Grid. In this paper, the problems of using ICMPv6 in NDP and the possible effects of these problems on Smart Grid are considered. Three main functions of NDP: Router Discovery, Duplicate Address Detection and Neighbor Discovery are discussed with respect to Smart Grid environment. We first consider the normal procedure for executing each phase, and then discuss the possible attacks. Finally a prevention procedure is given to secure the system. The proposed work considers multiple security breaches on Smart Grid and provides an IPS to prevent these attacks in Router Discovery and Updation phase as well as in Neighbor Discovery and DAD phase. This, in turn, helps preventing several attacks on ICMPv6 protocol, like DoS, man-in-the-middle attack, spoofing attacks efficiently. It is also light weight and does not burden the system with unnecessary packet overhead.

A possible bootstrap problem of the proposed IPS system

has been considered and found insignificant in section III.A. The proposed methodology builds the foundation for several meaningful extensions in future. In future, we want to extend this work to detect collaborative attacks on smart grid.

ACKNOWLEDGEMENT

This work is a part of the Ph.D. work of Manali Chakraborty, a Senior Research Fellow of Council of Scientific & Industrial Research (CSIR), Government of India. We would like to acknowledge CSIR, for providing the support required for carrying out the research work. We would also like to acknowledge Jeeyan Sanyal, a student of the Masters program with Department of Computer Science and Engineering, University of Calcutta, for his contribution in the simulation process.

The work is partially supported by the PRIN "Security Horizons" project.

REFERENCES

[1] S. M. Amin, B. F. Wollenberg, " Toward a smart grid: power delivery for the 21st century." IEEE Power and Energy Mag. Vol.3. No.5. Sept.-Oct (2005) 34-41. DOI: 10.1109/MPAE.2005.1507024

[2] "Study of Security Attributes of Smart Grid Systems – Current Cyber Security Issues." Department of Energy Office of Electricity Delivery and Energy Reliability, National SCADA Test Bed, April (2009).

[3] M. R. Asghar, D. Miorandi, " A Holistic View of Security and Privacy Issues in Smart Grids." SmartGridSec, Lecture Notes in Computer Science. Vol. 7823. (2013) 58-71. DOI: 10.1007/978-3-642-38030-3_4

[4] T. Narten et al, "RFC 4861-Neighbor Discovery protocol for IPv6", september, 2007.

[5] M. A. Saad, S. Ramadass, S. Manickam, "A Study on Detecting ICMPv6 Flooding Attack based on IDS", Australian Journal of Basic and Applied Sciences, Vol.7. (2013) 175-181.

[6] S. Hogg, E. Vyncke, "IPv6 Security". 1st Edition, Cisco Press, Dec. ISBN: 978-1587055942 (2008).

[7] "The smart grid vision for India's power sector." White Paper by United States Agency for International Development, USAID India. March (2010).

[8] T. Zseby, " Is IPv6 Ready for the Smart Grid?" CYBERSECURITY '12 Proceedings of the 2012 International Conference on Cyber Security. (2012) 157-164. DOI: 10.1109/CyberSecurity.2012.27

[9] J. Liu, Y. Xiao, S. Li, W. Liang, C. L. P Chen, " Cyber Security and Privacy Issues in Smart Grids". IEEE Communications Surveys & Tutorials. Vol. 14, No. 4, 4th Quarter. (2012). DOI: 10.1109/SURV.2011.122111.00145

[10] T. Baumeister," Literature review on smart grid cyber security. "Tech. rep., Collaborative Software Development Laboratory, Department of Information and Computer Sciences, University of Hawaii, December (2010).

[11] S. Groat, M. Dunlop,W. Urbanksi,R. Marchany, J. Tront, "Using an IPv6 Moving Target Defense to Protect the Smart Grid." Innovative Smart Grid Technologies (ISGT), IEEE PES, (2012) 1-7. DOI: 10.1109/ISGT.2012.6175633

[12] C. Y. Cheng, C. C. Chuang, R. I. Chang, " Three-dimensional Location-based IPv6 Addressing for Wireless Sensor Networks in Smart Grid". 26th IEEE International Conference on Advanced Information Networking and Applications. (2012) 824-831. DOI: 10.1109/AINA.2012.42

[13] C. Y. Cheng, C. C. Chuang, R. I. Chang, " Lightweight Spatial IP address Configuration for IPv6-based Wireless Sensor Networks in Smart Grid." SENSORS 2012, IEEE. (2012) 1-4. DOI: 10.1109/ICSENS.2012.6411205

[14] A. P. Castellani, G. Ministeri, M. Rotoloni,L. Vangelista, M. Zorzi, " Interoperable and globally interconnected Smart Grid using IPv6 and 6LoWPAN." 3rd IEEE International Workshop on SmArt COmmunications in NEtwork Technologies, 10-15th June (2012) 6473-6478. DOI: 10.1109/ICC.2012.6364813

[15] M. Kim, "A Survey on Guaranteeing Availability in Smart Grid Communications". Advanced Communication Technology (ICACT). (2012) 314-317.

[16] Z. A. Baig, S. C. Adeniye, "A trust-based mechanism for protecting IPv6 networks against stateless address auto-configuration attacks". 17th IEEE International Conference on Networks. Singapore (2011). 171-176. DOI: 10.1109/ICON.2011.6168470

[17] R. Berthier,W. H. Sanders, H. Khurana, "Intrusion detection for advanced metering infrastructures: Requirements and architectural directions" In First IEEE International Conference on Smart Grid Communications (SmartGridComm), Oct. (2010). 350–355. DOI: 10.1109/SMARTGRID.2010.5622068

[18] P. Jokar, H. Nicanfar, V. Leung, "Specification-based intrusion detection for home area networks in smart grids". In IEEE International Conference on Smart Grid Communications (SmartGridComm), Oct. (2011).208–213. DOI: 10.1109/SmartGridComm.2011.6102320

[19] R. Berthier, W. H. Sanders, "Specification-based intrusion detection for advanced metering infrastructures." In IEEE 17th Pacific Rim International Symposium on Dependable Computing (PRDC), Dec. (2011). 184–193. DOI: 10.1109/PRDC.2011.30