International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 7 July 2021, pp: 2506-2512 www.ijaem.net ISSN: 2395-5252

Intelligent and SecureNetwork for Smart Power Grid

Neeraj[*1], Rajiv[*2], Mukesh Singla[*3]

[*1]*M.Tech Student, Department of Computer Science and Engineering, Shri Baba Mastnath Engineering College,Rohtak, Haryana, India*

[*2]*Assistant Professor, Department of Computer Science and Engineering, Shri Baba Mastnath Engineering College,Rohtak, Haryana, India*

[*3]*Professor, Department of Computer Science and Engineering, Shri Baba Mastnath Engineering College,Rohtak, Haryana, India*

Submitted: 05-07-2021 Revised: 17-07-2021 Accepted: 20-07-2021

ABSTRACT

Smart Grid (SG) is an insightful and versatile energy conveyance network that joins the conventional force framework and IT correspondence organization. It means to give more proficient, better deficiency versatile and solid energy support. Powerful correspondence design is the key that separates Smart Grid from the customary energy conveyance framework. The foundation of the Smart Grid will be its correspondence organization. This organization is to associate the various parts of the Smart Grid together, and give two-way correspondence. IP empowered gadgets are important to assemble such organization spread over a huge geographic district and interfacing gadgets beginning from normal family electrical apparatuses up to control age units. With the immense number of gadgets including the keen electrical apparatuses, progressively being utilized in homes, IPv6 become a conspicuous decision for Smart Grid for its data transfer capacity. IPv6 is another innovation which acquired an enormous consideration, as a supporting layer in keen network correspondences. The immense location space of IPv6 upholds the organization design of the shrewd network correspondences. Moreover, highlights like stateless location auto setup (SLAAC) and IPSec support makes IPv6 more appropriate for savvy network. IPv6 likewise upholds prioritization of messages and distinctive Quality of Service models, which Complements a few savvy lattice applications.

Notwithstanding, similar to any new innovation, IPv6 also accompanies a lot of issues on which more work should be finished. In this we have centered our examination towards the execution of Smart Grid correspondence network utilizing IPv6.

Keywords: Analysis, smart grid, communication, IPV6.

I. INTRODUCTION

Theconventionalelectricalpowergridthathasbeenusedoverdecadeshasmetourneeds in the past. However, as the society advances technologically so does the expectations from various infrastructures surrounding us. Smart Grid (SG)isanintelligentelectricitynetworkthatintegratestheactionsofallusersconnected toitandmakesuseofadvancedinformation,control,anddcommunicationtechnologies to save energy, reduce cost and increase reliability and transparency.

A typical Smart Grid should consist of six basic sub-systems: Power Generation System,DistributionSystem,TransmissionNetwork, DataManagementandProcessing System, Smart Metering System and a Data Communication System connecting all the other systems to provide a two way communication. The first sub-system is the power generation that takes place in large power plants or renewables power plants; the second sub-system is the transmission that transports energy to the areas where it will be consumed; the third sub-system is the distribution that delivered energy to the end user; smart metering system monitors, measures and collects the end user data. In order to support the Smart Grid operation, Data Communication systems are needed forintegratingalltheothersubsystemswithDataManagementandProcessingsystem. The communication architecture of Smart Grid has three hierarchical layers: Home AreaNetwork(HAN),NeighborhoodAreaNetwork(NAN),andWideAreaNetwork.

Smart Grid is meant to modernize traditional power grids with the two-way data communication along with energy supply. In order to enhance the

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 7 July 2021, pp: 2506-2512 www.ijaem.net ISSN: 2395-5252

functionalities of the network, Smart Grid offers several applications to help both customers and utilities to optimize the energy usage and billing. Advanced Metering Infrastructure or AMI is one of the most important features of Smart Grid. It establishes a direct communication between customers and utilities, including, meter readings at periodic intervals (sometimes on demand) to the Data Collection Units or DCUs, updated electricity tariffs at regular intervals to smart meters, electricity outage alert messages and sometimes it upgrades the meter firmware.

II. METHODOLOGY

ICMPv6Vulnerabilities

We center on a portion of the conceivable ICMPv6 assaults that are especially significant with regards to building organizing foundation between Smart Meters (SM), Data Collection Units (DCU) and Meter Data Management System (MDMS). Three fundamental elements of NDP: Router Discovery, Duplicate Address Detection and Neighbor Discovery are talked about regarding Smart Grid climate. We initially think about the typical technique for executing each stage, and afterward examine the potential assaults. At last an anticipation technique is given to get the framework. The proposed work considers numerous securities penetrates on Smart Grid and gives an IPS to forestall these assaults in Router Discovery and Updating stage just as in Neighbor Discovery and DAD stage. This, thusly, helps forestalling a few assaults on ICMPv6 convention, similar to DoS, man-in-the center assault, parodying assaults productively. It is additionally light weight and doesn't trouble the framework with pointless bundle overhead.

IPv4 networks regularly channel ICMP messages to keep away from security concerns. In any case, for IPv6, this is unimaginable. ICMPv6 is utilized for essential functionalities and utilized by other IPv6 conventions like Neighbor Detection Protocol (NDP). Neighbor Discovery Protocol (NDP) is a convention utilized with IPv6 to perform different assignments like switch disclosure, auto location design of a hub, neighbor revelation, Duplicate Address Detection, deciding the Link Layer locations of different hubs, address prefix disclosure, and keeping up with directing data about the ways to other dynamic neighbor hubs [149]. Subsequently, the execution of IPv6 in Smart Grid needs some genuine consideration to shield from the security weaknesses of the ICMPv6 convention. NDP utilizes five ICMPv6 messages. These are:

- Router Solicitation (RS) message: Hosts send RS message to inquire about a genuine switch on the connection.
- Router Advertisement (RA) message: Routers send RA message, either intermittent partner or because of RS message.
- Neighbor Solicitation (NS) message: Hosts send NS message to decide the connection layer address of a particular hub, and furthermore to confirm if a location is now present on interface.
- Neighbor Advertisement (NA) message: Hosts send NA message in light of the NS message.
- Router Redirect (RR) message: Routers send RR message to educate a host about a superior switch on its connection.

1. Router Discovery

At the point when a SM X is introduced in a subnet, it's anything but a DCU to tie with. The Smart Meter X will keep on imparting through that DCU, until it gets any ICMPv6 Router Redirect (RR) message from the past DCU.

1.1. Normal Procedure for Router Discovery

Regularly Smart Meters find their switch or DCU through the accompanying advances,

- First, X sends an ICMPv6 Router Solicitation (RS) message to find a DCU in its nearby connection.
- An authentic DCU then, at that point reacts with an ICMPv6 Router Advertisement (RA) message, with a 64 bit prefix address for its subnet.
- Then X registers that DCU as its default switch in the connection, and auto-arranges a worldwide unicast address dependent on the got prefix.

1.2. Attacks in Router Discovery stage

The most conspicuous assault in this stage happens if an assailant dishonestly claims to be a DCU. It's anything but a RA message from a real DCU and sends it to the Smart Meter, with or without changing the prefix address for that subnet. Regardless, the recently introduced Smart Meter enlists the assailant as its DCU. In the event that the enemy changes the prefix address, the Smart Meter will auto-arrange its worldwide location dependent on an off-base prefix. Therefore, the Smart Meter will get impeded in the subnet and won't speak with some other Smart Meter or DCU aside from the aggressor. The circumstance turns into a touch more unpredictable when the enemy sends the RA message without changing the prefix. In the present circumstance, the Smart Meter can convey inside its subnet. Nonetheless, it turns out

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 7 July 2021, pp: 2506-2512 www.ijaem.net ISSN: 2395-5252

to be very inconceivable for the Smart Meter to impart past its subnet as the enrolled DCU for the Smart Meter is an aggressor who isn't perceived by other Smart Meters in the Neighborhood Area Network.

When an enemy effectively persuades a recently introduced Smart Meter of being its substantial DCU, it's anything but a heap of traditional organization assaults on the Smart Grid. It's anything but a man-in-the-center assault by capturing parcels from the Smart Meters or from the DCUs and appropriate changing the Source and Destination address fields to such an extent that neither of these two substances know about the presence of an aggressor in the middle. The aggressor can likewise change the information contained in the captured bundles. Another conventional organization assault is the Denial-of-Service assault. The assailant can over-burden the organization assets by creating false bundles having the recently introduced Smart Meter address as the Source Address.

2. Duplicate Address Detection

After auto designing the location for it, the Smart Meter X will need to know whether the location is accessible for use. The accompanying advances are utilized for copied address recognition.

- Smart Meter X, sends an ICMPv6 Neighbor Solicitation message for the location it needs to guarantee.
- If any Smart Meter on that subnet as of now has that location, then, at that point it sends an ICMPv6 Neighbor Advertisement message.
- If X doesn't get any NA messages expressing that the location has been taken, then, at that point X can utilize that location.

2.1. Attacks in Duplicate Address Detection stage

A gatecrasher can keep a Smart Meter from getting any auto-arranged location, by sending a NA for the relating address in each NS message conveyed by the Smart Meter. Therefore, the Smart Meter won't impart inside the organization. Moreover, an interloper can impede a NA message from a valid SM. These outcomes in at least two SMs utilizing a similar location inside an organization. Because of this assault, an authentic SM can be blamed for personality mocking. Additionally, more than one task of a similar location inside an organization can cause ill-advised working during the steering stage. To identify these sorts of assaults, we propose an adjusted rendition of the Duplicate Address Detection stage,

- SM X sends an ICMPv6 NS message for the location it needs to procure.
- On getting the NS message, each Smart Meter examines its neighbor reserve data for that location. In the event that they discover the location in their store, they send an answer to the X.
- If any Smart Meter on that subnet as of now has that location, then, at that point it sends an ICMPv6 NA message.
- If the X gets neither any NA messages expressing that the location is been taken nor gets any messages from its neighbors expressing that the location is available in their store, then, at that point X can utilize that location.

In the event that X gets just the NA message from another Smart Meter however no local data about that address is gotten, it infers that such a location the location isn't in presence inside the subnet and some aggressor is attempting to keep X from procuring that location. On the off chance that X doesn't get any NA message, yet its neighbors answer with their reserve data expressing that the location is available in their area, then, at that point the X reasons that an aggressor has caught the NA message from the objective Smart Meter and has dropped it. Along these lines, X can utilize a location just when it neither gets the NA nor any local store data from its neighbors.

In the event that the assailant is savvy enough, it can send both the NA message and furthermore parody some answer messages from other Smart Meters and change their substance. All things considered, SM X won't recognize the assault. Thus, to distinguish this sort of assault, if a Smart Meter exists with a similar location, it's difficult answers with a NA message yet in addition sends its local data to X. SM X then, at that point sends unicast inquiries to every one of the neighbors found in the answer message to check the presence of a particularly Smart Meter. Thusly, X can be guaranteed whether he is being tricked or regardless of whether the specific location is truly being utilized inside the subnet. Be that as it may, since the answer message can likewise be blocked by the aggressor, it should be communicated inside the organization. This will guarantee the conveyance of the answer message to X.

3. Neighbor Discovery

When the Smart Meter secures a special worldwide location, then, at that point it can begin correspondence through the DCU. It can likewise speak with the other Smart Meters, both in its

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 7 July 2021, pp: 2506-2512 www.ijaem.net ISSN: 2395-5252

subnet and in other subnets. Savvy Meters on the equivalent subnet can discuss straightforwardly with one another without utilizing any switch or door when a SM has interface layer locations of other adjoining SMs. In this way store the connection layer locations of the adjoining SMs in the nearby reserve of each SM. Neighbor Discovery works with something very similar.

3.1. Normal Procedure for Neighbor Discovery

To speak with a SM B on all alone subnet, a Smart Meter A needs to play out the accompanying advances,

- First, the SM A sends an ICMPv6 NS message mentioning the connection layer address of B.
- If B is available in that subnet, then, at that point it's anything but an ICMPv6 NA message. SM A realizes the MAC address of B from this NA message.
- SM A then, at that point makes a neighbor reserve section for B that ties the MAC address of B to its IPv6 address.

3.2. Attacks in Neighbor Discovery stage

The assaults of this stage are like the assaults of the Duplicate Address Detection stage. Here likewise an interloper can attempt to mimic B, and capture all parcels that are bound to B, or a gatecrasher can obstruct a NA answer from B so A thinks that B is absent in the organization.

4. Proposed Intrusion Prevention System

Figure 1 show a general perspective on interruption recognition in Router Discovery and Updating stage, when an assailant parodies a RA message from DCU and sends it to a Smart Meter X without changing the 64 cycle prefix address. In the principal half of the figure, an assailant parodies a RA message and sends it to the recently introduced Smart Meter X. In the second 50% of the figure, an aggressor communicates a RA message to every one of the functioning Smart Meters. Figure 2shows a general perspective on interruption identification in Duplicate Address Detection stage, when X checks the presence of another SM in the subnet, with same location. An aggressor impedes a NA message from a legitimate SM X. Figure 3shows a general perspective on interruption identification in Neighbor Discovery stage, when DCU X needs to speak with Z, however aggressor attempts to mimic Z.

III. RESULTS

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 6 shows that there are no false negative for 2, 4, or 6 malicious nodes out of 50 nodes. The false negative increases with increasing number of malicious nodes. Figure 4 and 5 show the effect on false negatives with a linear percentage of malicious nodes. The experimental results are in line with reality where any IPS system fails when majority of nodes become compromised.

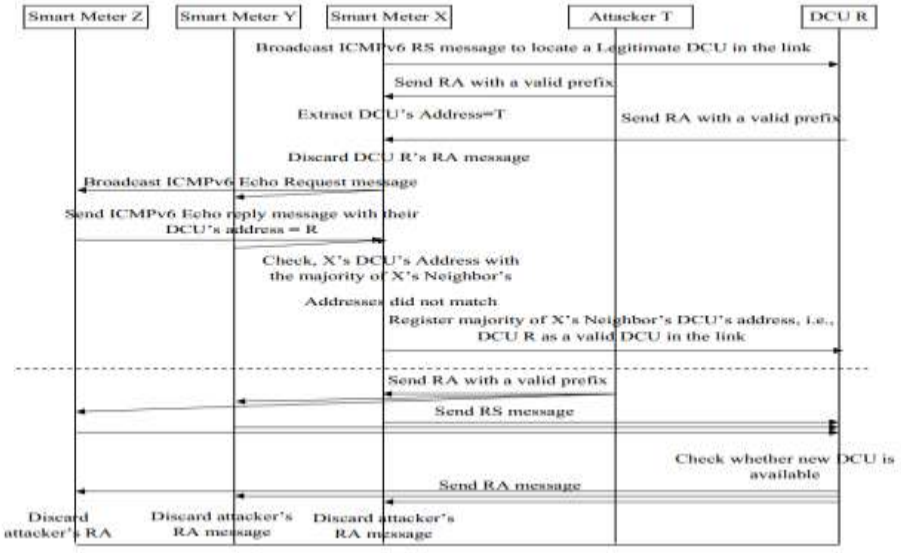

Figure 1: High level view of IPS in Router Discovery and Updating phase.

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 7 July 2021, pp: 2506-2512 www.ijaem.net ISSN: 2395-5252

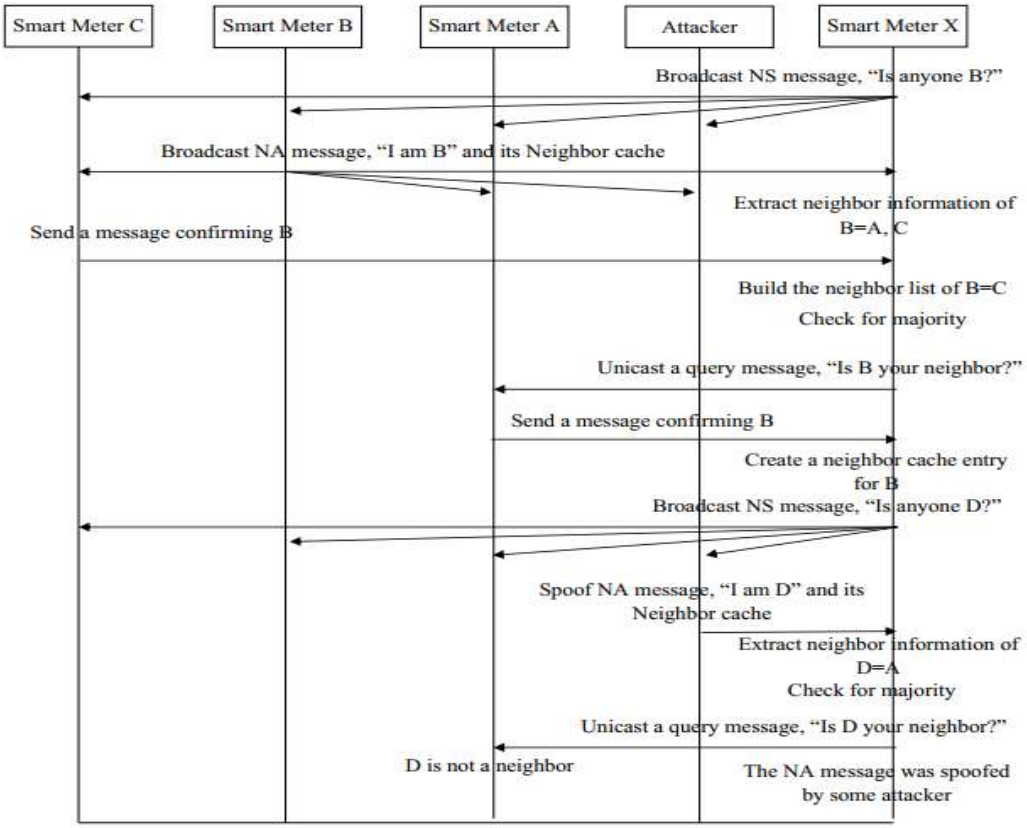

Figure 2: High level view of IPS in Duplicate Address Detection phase.

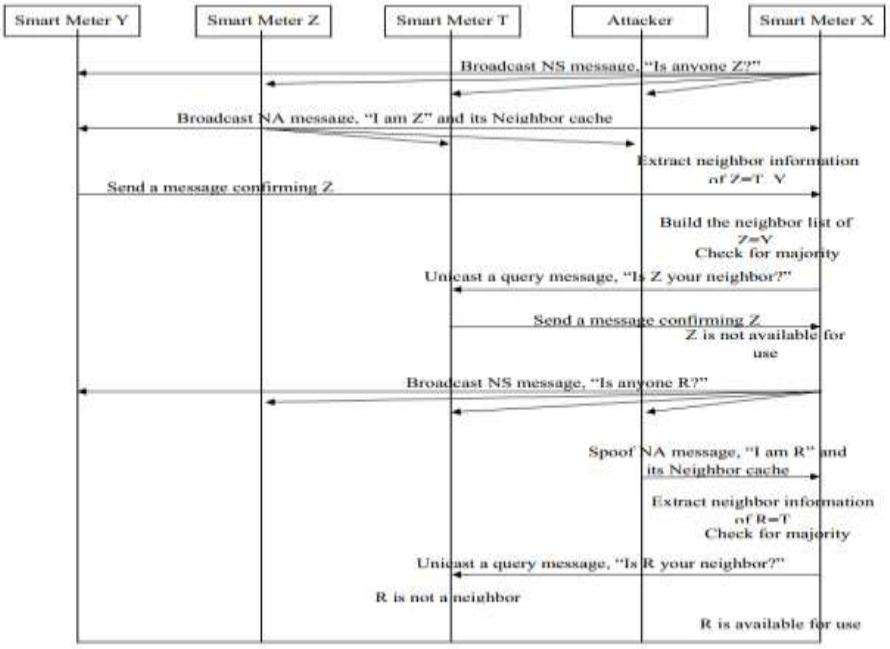

Figure 3: High level view of IDS in Neighbor Discovery phase.

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 7 July 2021, pp: 2506-2512 www.ijaem.net ISSN: 2395-5252

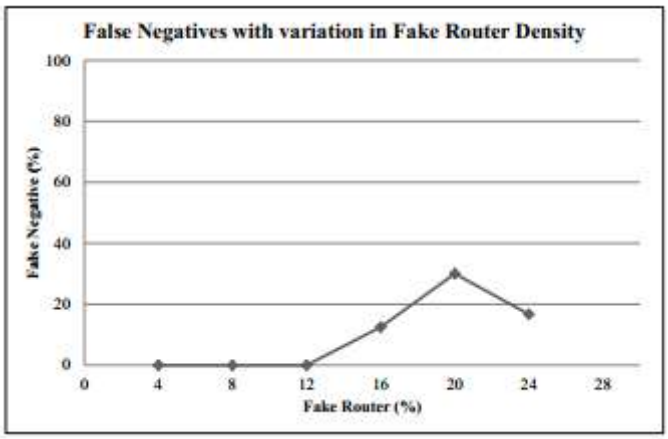

Figure 4: False Negative vs. Number of Malicious DCUs.

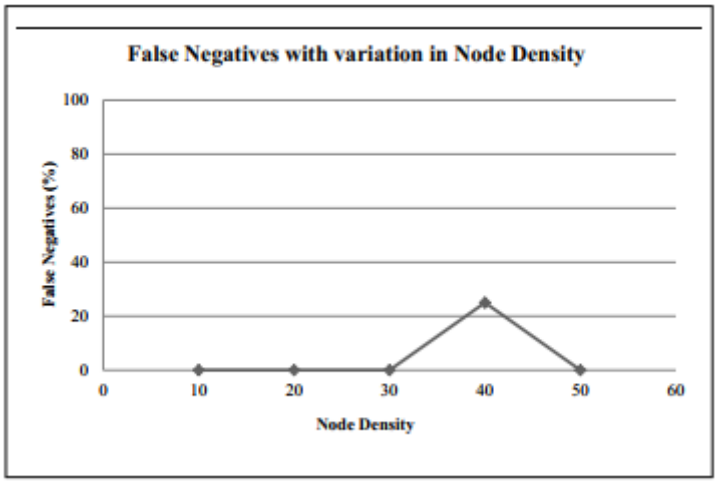

Figure 5: False Negative vs. Node density.

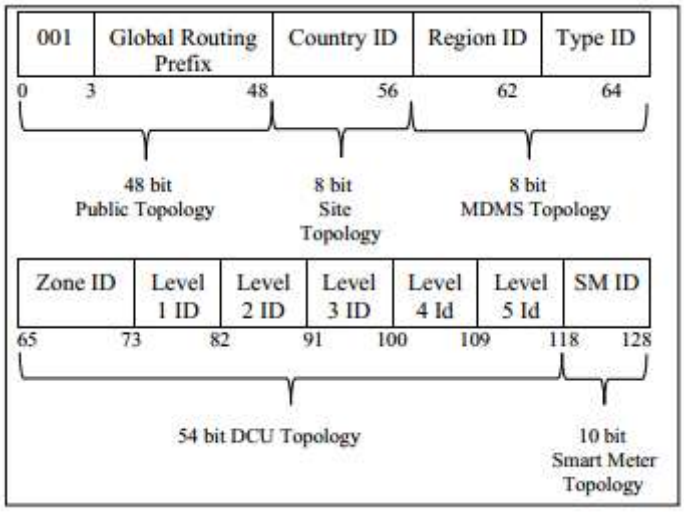

Figure 6: Proposed IPv6 addressing structure.

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 7 July 2021, pp: 2506-2512 www.ijaem.net ISSN: 2395-5252

IV. CONCLUSION

Incorporating IPv6 with Smart Grid is very normal, as just IPv6 could coordinate with the size of Smart Grid organization. The enormous location space, auto arrangement of addresses, QoS support innovation helps Smart matrix to build a huge organization with a remarkable location indicated for every single gadget, productive steering, start to finish security. Notwithstanding, keen framework has extremely high security request that should be considered prior to sending IPv6 towards building Smart Grid. In this section, the issues of utilizing ICMPv6 in NDP and the potential impacts of these issues on Smart Grid are thought of. Plus, another location arrangement of IPv6 Global Unicast tending to towards supporting the powerful various leveled correspondence design of Smart Grid Network and address setup techniques for both Smart Meters and DCUs are proposed.

Three primary elements of NDP: Router Discovery, Duplicate Address Detection and Neighbor Discovery are examined regarding Smart Grid climate. We initially think about the typical method for executing each stage, and afterward we examine the potential assaults. At last an avoidance strategy is given to get the framework. This interruption anticipation framework helps forestalling a few assaults on ICMPv6 convention, similar to DoS, man-in-the-center assault, satirizing assaults effectively. It is additionally light weight and doesn't trouble the framework with superfluous bundle overhead. The proposed work considers various security penetrates on Smart Grid and gives an IPS to forestall these assaults in Router Discovery and Updating stage just as in Neighbor Discovery and DAD stage.

The proposed tending to composition is superior to the overall IPv6 tending to structure, as far as better use of address space and supporting the powerful various leveled engineering of Smart Grid. Furthermore, it likewise assists Smart Grid with getting more adaptable. This strategy diminishes the location design delay, as the setup cycle done locally. Other than it likewise decreases the weight of MDMS for arranging the location of each DCU under it. in this strategy each DCU can design the location of its kids DCUs. The proposed approach assembles the establishment for a few significant expansions in future. In continuation to the proposed work, it is intriguing to foster another directing convention for the last mile correspondence in Smart Grid.

REFERENCES

[1] U.S Energy Information Administration, “International Energy Outlook 2017”, September,2017.

[2] A White Paper by United States Agency for International Development, USAID India, “The smart grid vision for India’s power sector”, March2010.

[3] “Study of Security Attributes of Smart Grid—Current Cyber Security Issues”, DepartmentofEnergyOfficeofElectricityDeliveryandEnergyReliability,National SCADA Test Bed, April2009.

[4] NIST Special Publication 1108R2, “NIST Framework and Roadmap for Smart Grid Interoperability Standards”, Release 2.0, National Institute of Standards and Technology (NIST) Std., February2012.

[5] S.Bera,S.Misra,J.J.P.C.Rodrigues,“CLoudComputingApplicationsforSmart Grid: A Survey”, IEEE Transactions on Parallel and Distributed Systems, Vol. 26, No. 5, pp. 1477-1494,2015.

[6] S. Bera, S. Misra, D. Chatterjee, “C2C: Community-Based Cooperative Energy Consumption in Smart Grid”, IEEE Transactions in Smart Grid, Vol. 9, No. 5, pp. 4262-4269,2018.

[7] Mondal,S.Misra,L.S.Patel,S.K.Pal,M.S.Obaidat,“DEMANDS:Distributed EnergyManagementUsingNoncooperativeSchedulinginSmartGrid”,IEEESystems Journal, Vol. 12, No. 3, pp. 2645-2653,2018.

[8] R.Berthier,W.H.Sanders,“Specification-BasedIntrusionDetectionforAdvanced Metering Infrastructures”, IEEE 17th Pacific Rim Int’l Symp. on Dependable Computing, pp. 184-193,2011.

[9] D.Mashima,A.A.C´ardenas,“Evaluatingelectricitytheftdetectorsinsmartgrid networks”, Research in Attacks, Intrusions, and Defenses (RAID), LNCS 7462,pp. 210–229,2012.

[10] J.Nagi,K.S. Yap,S.K.Tiong,S.K.Ahmed,M.Mohamad,“Nontechnicalloss detection for metered customers in power utility using support vector machines”, IEEE Transactions on Power Delivery, vol. 25, no. 2, pp. 1162-1171,2010.