PROJECT REPORT

ON

"DETECTION AND MITIGATION OF NDP ATTACK FOR AMI DEVICES IN SMART GRID SYSTEM"

By

PURBASHA CHOWDHURY (T91/CSE/166002)
SONA SHAW (T91/CSE/164048)
PREMANSU KAR (T91/CSE/166006)

Under the guidance of

PROF. (DR.) NABENDU CHAKI
Department of Computer Science & Engineering
University of Calcutta,
West Bengal, India

CERTIFICATION

This is to certify that Ms. Purbasha Chowdhury, Mr. Sona Shaw and Mr. Premansu Kar is working under my guidance for preparing the project entitled **"Detection and Mitigation of NDP attack for AMI devices in Smart Grid System"** to be submitted to the University of Calcutta in partial fulfillment of the requirement for the Degree of B.Tech in Computer Science & Engineering.

Signature of HOD
Department of Computer Science & Engineering
University of Calcutta,
West Bengal, India

PROF. (DR) NABENDU CHAKI
Department of Computer Science & Engineering
University of Calcutta,
West Bengal, India

ACKNOWLEDGEMENTS

Before presenting the dissertation work, we find this occasion felicitous to voice sincere thanks to our project guide Prof. (Dr.) NABENDU CHAKI, Department of Computer Science & Engineering, University of Calcutta who not only provided us with his valuable suggestions and guidelines but also inculcated the spirit of independent work within us. Patience and cooperation shown by him cannot be expressed adequately enough in words.

PURBASHA CHOWDHURY

SONA SHAW

PREMANSU KAR

(Student, B.Tech in CSE-8th Semester-2019-20)
Department of Computer Science & Engineering
University of Calcutta,

CONTENTS

CHAPTER	PARTICULARS	PAGE
CHAPTER 1	**INTRODUCTION**	3
1.1	Smart Grid System	3
1.2	Smart Meter System	3
CHAPTER 2	**SMART METER NETWORK**	5
2.1	Classification of Smart Metering Network	5
CHAPTER 3	**Research on Smart Grid System & Attacks**	8
3.1	Vulnerabilities	8
3.2	Attack and types of attacks	8
3.3	More Attacks	9
3.4	Some attacks on SMN	9
3.5	Attacks on data	10
3.6	Some security requirements on Smart Metering Networks	11
CHAPTER 4	**IPV6 and ICMPV6 vulnerabilities and attacks**	13
4.1	IPV4 Header	13
4.2	IPV6 Header	14
4.3	IPV4 vs IPV6	14
	4.3.1 Similarities between IPv6 and IPv4 vulnerabilities	14
	4.3.2 Differences between IPv6 and IPv4 vulnerabilities	15
	4.3.3 Unique vulnerabilities to IPv6	15
4.4	ICMP Protocol	15
	4.4.1 ICMPv4	15
	4.4.2 ICMPv6	15
	4.4.3 ICMP Attacks	16
	4.4.4 Unique ICMPv6 Attacks	18
4.5	Neighbor Discovery Protocol(NDP)	18
4.6	Smart Meter communication through NDP	20
CHAPTER 5	**Proposed attack scenarios in AMI**	21
CHAPTER 6	**Proposed Mitigation Scheme**	22
6.1	Mitigation technique 1	23
6.2	Mitigation technique 2	25

CHAPTER 7	**Simulation**	28
7.1	Trial Network	28
7.2	Approach of Simulation	29
	7.2.1 Simulation of Step 1	29
INFERENCE		30
CONCLUSION		30
REFERENCE		31

List of Figures

Figure No.	Title	Page No.
1.1	Classification of Cyber Attacker Actions	4
2.1	Home Area Network (HAN)	6
2.2	Building Area Network (BAN)	6
2.3	Neighborhood Area Network (NAN)	7
2.4	Advanced Metering Infrastructure	7
3.1	Security requirement for SMNs	11
4.1	IPv4 Header Structure	13
4.2	IPv6 Header Structure	14
4.3	ICMPv4 Packet Format	15
4.4	ICMPv6 Packet Format	15
4.5	ICMP Sweep Attack	16
4.6	ICMP Route Redirect	17
4.7	ICMP Router Discovery Message Attack	17
4.8	MITM with spoofed ICMPv6 NA	18
4.9	RS message packet format	19
4.10	RA message packet format	19
4.11	NS message packet format	19
4.12	NA message packet format	20
4.13	RR message packet format	20
7.1	Network creation between border-router and udp-sender motes	28
7.2	Terminal Window output	28
7.3	Routing Table	29
7.4	Radio traffic between motes	29
7.5	Mote Output	30
7.6	Timeline Output	30

1. Introduction:

1.1 Smart Grid System:

The smart grid can be defined as an integration of power grid systems with communication systems. It is undeniable that the integration of communication systems into the power grid systems has improved the ways of managing and controlling the resources of power grid systems such as power flow and data management system[1]. This integration also enables a two-way communication between utility provider and energy consumers which also allows an efficient ways to manage and monitor data flow from a hierarchical structure of the smart grid systems.

The smart grid consists of two main components namely power grid systems and communication systems. Subsequently, power grid systems can be further divided into three major sections:

- Power Generation
- Power Transmission
- Power Distribution

These three sections are responsible for supplying electrical power to consumers' homes, factories and business buildings.
Smart grid's function is not only about adding communication systems; it also covers

- Sustainable energy system
- Efficient energy management
- Secures energy supply.

1.1.1 Features of Smart Grid

Smart grid has several positive features that give direct benefit to consumers:

- Real time monitoring.
- Automated outage management and faster restoration.
- Dynamic pricing mechanisms.
- Incentivize consumers to alter usage during different times of day based on pricing signals.
- Better energy management.
- In-house displays.
- Web portals and mobile apps.
- Track and manage energy usage.
- Opportunities to reduce and conserve electricity etc.

1.2 Smart Meter System:

- A smart meter is a digital device that provides advanced functionalities of remote meter reading for collecting smart meter data. This includes sending and executing control commands such as remote connect or disconnect.

- A smart grid electric power system delivers electricity from producers to consumers using two-way **Smart Meter** technology that can remotely control consumer electricity use[3]. This can help utilities to conserve energy, reduce costs, increase reliability and transparency, and make processes more efficient.

- However, the increasing use of IT based electric power systems increases cyber security vulnerabilities, and this increases the importance of **Cyber Security.**

Cyber Security Threats:

- Availability
- Integrity
- Confidentiality
- Timeliness
- Human Machine Interface
- Software Vulnerabilities
- Authentication

Types of cyber-attacker actions:

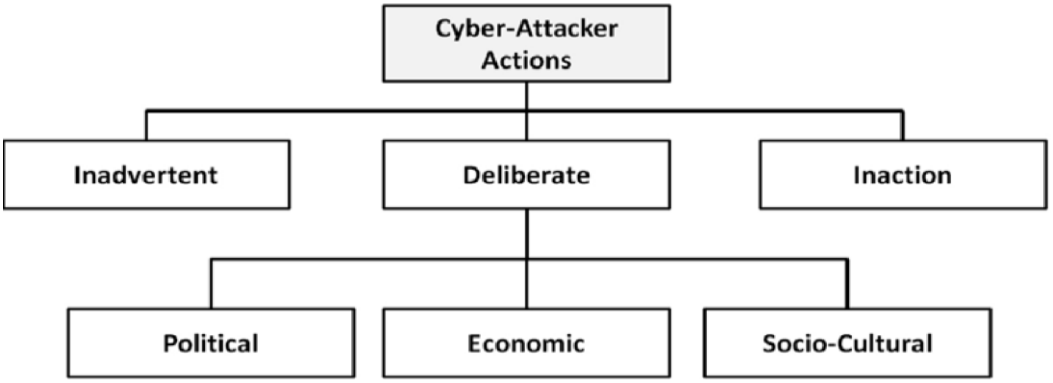

Fig 1.1: Classification of Cyber Attacker Actions

1.2.1 Difference between Meter and Smart Meter:

Electric Meters measure the amount of electricity used in a commercial or residential building. They can be either analogue meters or digital meters, which are also known as smart meters. Both types of meters provide the data on the electricity consumed to run heating and cooling systems, lights, appliances, and other devices that run on electricity[5].

Smart Meters, on the other hand, are much more interactive and multifunctional than the analogue meters. They can record the electricity use on a daily basis and share this information between the electricity suppliers and the consumers over wireless frequency networks. Smart meters, therefore, make for a home energy management system.

2. Smart Meter Network:

By communicating with other smart meters, a network of smart meters called **Smart Metering Networks (SMNs)** is formed. This network is also known as **Advanced Metering Infrastructure (AMI)**. The communication systems comprise of different network topologies such as:

- Wide Area Network (WAN)
- Neighborhood Area Network (NAN)
- Building Area Network (BAN)
- Home Area Network (HAN) (private network)

These four network topologies are the core networks that allow data exchange between utility provider and consumers. It is part of the smart grid communication systems that is responsible for managing and delivering smart meter information such as

- billing data
- command data
- request data
- Demand-response (DR) data

These data will be sent to the nearest utility provider office as well as consumers for analysis and billing process. With these abilities, a smart meter is not only can provide effective communication but also enable consumers to efficiently manage and monitor their own energy usage through DR programs such as incentive-based or time-based programs[7]. The growing dependability of smart meter communications on Internet-based communication has increased the vulnerabilities of smart metering networks to Internet-based attacks such as:

- Eavesdropping
- False data injection
- Denial of service (DoS)
- Impersonation
- Replay
- Repudiation

These attacks are dangerous to the smart grid systems in the sense that it can cause problems like power instability and huge financial losses. Nowadays, many security solutions have been proposed to secure data transmission in wired and wireless networks. Smart meter data will be recorded and transmitted to utility servers and as such there is vast amount of data will be exchanged between utility provider server and consumers. These frequent data collection of smart meters have increased the risk of violating human privacy such as information theft and profiling human behavioral patterns[8].

2.1 Classification of the Smart Metering Networks:

1. Home Area Network (HAN): HAN is a dedicated network connecting all smart devices that operate within a home network. To enable communication in HAN, a wireless smart meter is placed within consumer's home which is then acts as a HAN gateway that is responsible to manage all the data communication involved. Through this network, consumer can control and

monitor energy consumptions and data flow between home appliances such as thermostats, air conditioners, fridges, washers, dryers and stoves[4].

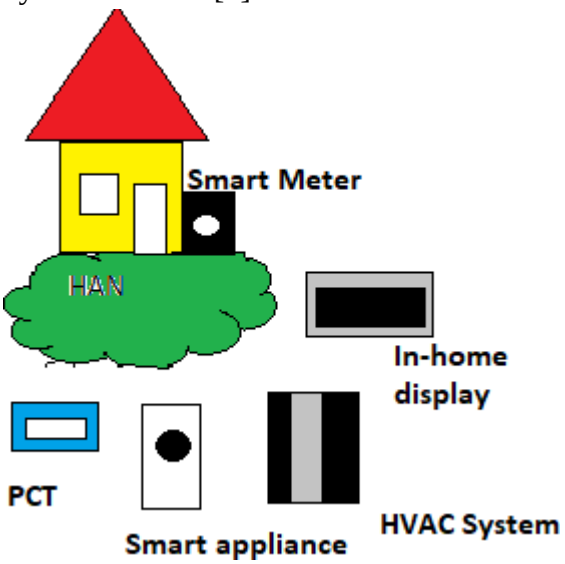

Fig 2.1: Home Area Network (HAN)

2. Building Area Network (BAN): BAN is a network that covers the communication within a building which consists of a number of apartments or homes. Fig. 3 shows the BAN network topology that consists of several numbers of HANs. In order to maintain communication links between BAN and HANs, a device called BAN gateway is installed in the building. The functions of this gateway are to aggregate, monitor and provide information such as power requirement and energy consumption on its HANs, whereby, this information will be sent to the nearest data collector center or NAN gateway[4]. In order to enable the communications between BAN gateway and its HANs, network technologies such as Wi-Fi or WiMAX is a preferably suitable alternative to be used.

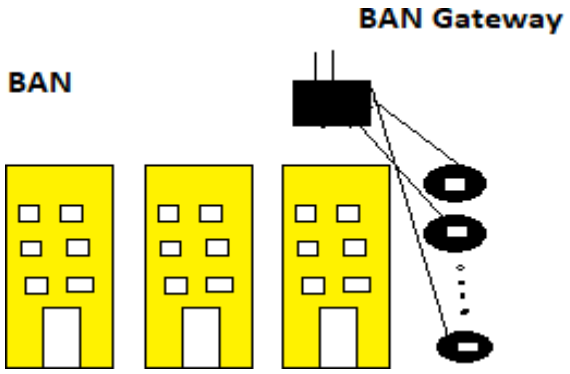

Fig 2.2: Building Area Network (BAN)

3. Neighborhood Area Network (NAN): NAN is a network which provides communication links between utility providers to smart meters that are installed in consumer sites as shown in Fig. 4. Through a NAN collector, the energy consumption of a certain neighborhood can be measured and monitored by the corresponding distribution substation[4]. However, the use of such technologies is still not widely implemented due to several factors such as requiring high investment cost and expensive equipment to be deployed.

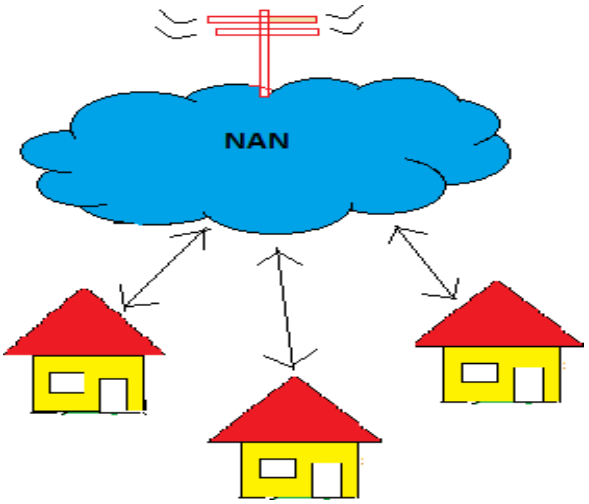

Fig 2.3: Neighborhood Area Network (NAN)

4. Wide Area Network (WAN): WAN is a communication network that covers long-distance data transmission from NAN gateway points to utility's back-office systems or control center. As shown in Fig.2.4, the interface between WAN and NANs consists of base stations, while the interface between NAN and BANs is a BAN gateway which is then connected to smart meters which act as an interface between BAN and HANs. However, in the case of individual residence house, the smart meters act directly as an interface between NAN and HANs. It is indubitable that the introduction of communication technologies in the power grid systems has enabled two-way communication between utility provider and consumer[5]. This two-way communication has allowed more adaptive, efficient and effective ways to manage and utilize the electrical energy. However, with all the provided advantages, the dependency of smart metering networks on Internet-based communication has raised the vulnerabilities, cyber-attacks and privacy violation in smart metering networks.

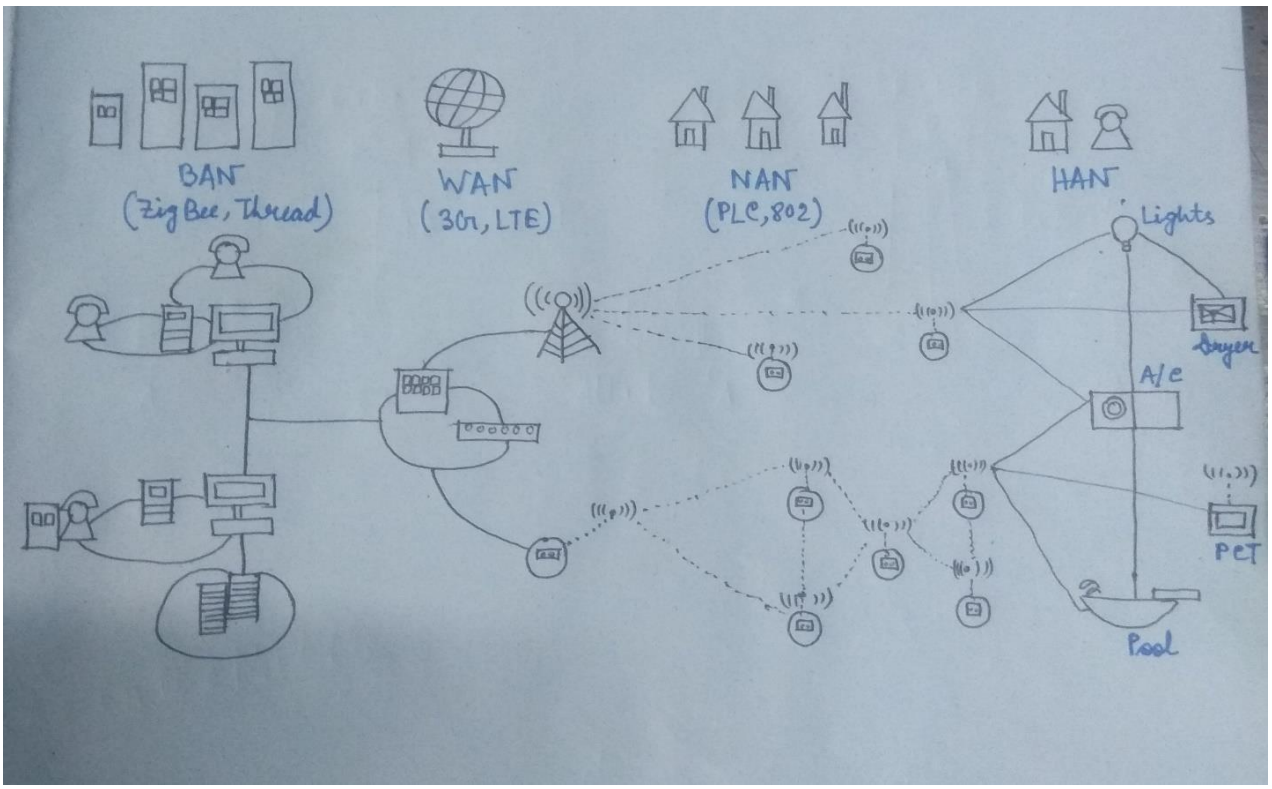

Fig 2.4: Advanced Metering Infrastructure

3. Researches on Smart Grid System & Attacks:

3.1 Vulnerabilities:

Smart grid network introduces enhancements and improved capabilities to the conventional power network making it more complex and vulnerable to different types of attacks. These vulnerabilities might allow attackers to access the network, break the confidentiality and integrity of the transmitted data, and make the service unavailable.

1. Customer security: Smart meters autonomously collect massive amounts of data and transport it to the utility company, consumer, and service providers[8]. This data includes private consumer information that might be used to infer consumer's activities, devices being used, and times when the home is vacant.

2. The lifetime of power systems: Since power systems coexist with the relatively short lived IT systems, it is inevitable that outdated equipments are still in service. This equipment might act as weak security points and might very well be incompatible with the current power system devices.

3. Implicit trust between traditional power devices: Device-to-device communication in control systems is vulnerable to data spoofing where the state of one device affects the actions of another. For instance, a device sending a false state makes other devices behave in an unwanted way.

4. Different Team's backgrounds: In efficient and unorganized communication between teams might cause a lot of bad decisions leading to much vulnerability.

5. Using Internet Protocol (IP) and commercial off-the- shelf hardware and software: Using IP standards in smart grids offer a big advantage as it provides compatibility between the various components. However, devices using IP are inherently vulnerable to many IP-based network attacks such as IP spoofing, Tear Drop, Denial of Service, and others[9].

6. More stakeholders: Having many stakeholders might give raise to a very dangerous kind of attack: insider attacks.

3.2 Attackers and Types of Attacks:

The just mentioned vulnerabilities can be exploited by attackers with different motives and expertise and could cause different levels of damage to the network[8]. Attackers could be script kiddies, elite hackers, terrorists, employees, competitors, or customers. The authors in group attackers into:

1. Non malicious attackers who view the security and operation of the system as a puzzle to be cracked. Those attackers are normally driven by intellectual challenge and curiosity.
2. Consumers driven by vengeance and vindictiveness towards other consumers making them figure out ways to shut down their home's power.
3. Terrorists who view the smart grid as an attractive target as it affects millions of people making the terrorists' cause more visible.
4. Employees disgruntled on the utility/customers or ill-trained employees causing unintentional errors.
5. Competitors attacking each other for the sake of financial gain.

Those attackers can cause a wide variety of attacks, classified into three main categories: Component-wise, protocol-wise, and topology-wise.

- Component-wise attacks target the field components that include Remote Terminal Unit (RTU). RTUs are traditionally used by engineers to remotely configure and troubleshoot the smart grid devices. This remote access feature can be subject to an attack that enables malicious users to take control over the devices and issue faulty states such as shutting down the devices[7].

- Protocol-wise attacks target the communication protocol itself using methods such as reverse engineering and false data injections.

- Topology-wise attacks target the topology of the smart grid by launching a Denial-of-Service (DoS) attack that prevents operators from having a full view of the power system causing inappropriate decision making.

3.3 More attacks:

1. Malware spreading: An attacker can develop malware and spread it to infect smart meters or company servers. Malware can be used to replace or add any function to a device or a system such as sending sensitive information[10].

2. Access through database links: Control systems record their activities in a database on the control system network then mirror the logs into the business network. If the underneath database management systems are not properly configured, a skilled attacker can gain access to the business network database, and then use his skills to exploit the control system network.

3. Compromising communication equipment: An attacker may compromise some of the communication equipment such as multiplexers causing a direct damage or using it as a backdoor to launch future attacks.

4. Injecting false information (Replay Attack): An attacker can send packets to inject false information in the network, such as wrong meter data, false prices, fake emergency event, etc. Fake information can have huge financial impact on the electricity markets.

5. Network Availability: Since smart grid uses IP protocol and TCP/IP stack, it becomes subject to DoS attacks and to the vulnerabilities inherent in the TCP/IP stack. DoS attacks might attempt to delay, block, or corrupt information transmission in order to make smart grid resources unavailable[12][11].

3.4 Some attacks on SMN (smart meter network):

1. False Data Injection Attack (FDI): FDI is a kind of attack that tries to manipulate data integrity by injecting false data into the network with the aim to mislead the control center to make erroneous decision on contingency analysis, power dispatch and billing process. In SMNs, the FDI occurs when attacker successfully intercept and alter the content of the data prior to being sent back to the network.

2. Denial-of-Service Attack (DoS): DoS is a common attack in wired or wireless communications whereby the most well-known DoS in SMNs is jamming attack. A jamming attack basically occurs in wireless networks in which a jammer tries to disrupt the radio frequencies used by the smart meters by transmitting another radio signals to interrupt data

transmission process. In order to mitigate this attack, the authors in have used a game theoretical-based approach called zero-sum stochastic.

3. **Eavesdropping Attack (EVD):** EVD is another common attack in SMNs which can be defined as an act of secretly listening to and recording of data communication over neighboring smart meters. EVD may or may not be dangerous; it depends on the eavesdropper's motivations[11]. However, EVD can invade human's privacy via illegitimate actions such as information theft, identity fraud and profiling human's behavioral patterns. Currently, there exist several schemes focusing on detecting and countering the EVD.

4. **Replay Attack (REP):** REP is an attack attempting to disrupt security by storing or recording unauthorized data and retransmitting the data back at a later time after some modification have been made to the original data. For example, data transmission between smart meters can be captured or intercepted by an attacker and replay the data after performing some modifications. REP can be prevented by using nonce techniques such as timestamp or message sequence number. However, the use of message sequence number requires reliable communication channels whereas, using timestamp would require the exchange of extra messages which may cause communication overhead.

5. **Impersonation Attack (IMP):** IMP or man-in-the-middle attack is an attack where a malicious smart meter snatches the identity of other legit smart meters. IMP may not only happen on meter-to-meter communication but also on meter-to-smart appliances communication which can cause scenarios like demand exceeding supply, billing overcharge or even electricity shutdown to happen.

6. **Repudiation Attack (RPD):** RPD can be referred to as denial of participation in the communication. The role of non-repudiation functions in smart metering networks is mainly to ensure that the consumers or the utilities will not deny that they have been sending and/or receiving their authenticated metering data due to motive like avoiding responsibility. The scheme proposed by uses one time signature generation method in order to protect the smart meter data from repudiation based attacks[9]. The scheme has the ability to counter against non-repudiation attack and at the same time helps to reduce the energy consumption and computational cost. However, the use of one-time signature generation generates another problem called signature flaw. This flaw is related to the use of one key for all authentication process. If this key is compromised, the security of the whole network will be at risk since only one signature is used for the entire communication process.

3.5 Attacks on data:

There are two types of data transmitted by a smart meter; one is the power consumption value of the last slot in the current slot and the other is the smart meter reading in the current slot. Smart meter data which include private information and consumers' electricity activities are collected, recorded and stored in databases. These databases may be shared with, or fall into the hands of criminals, blackmailers, corrupt law enforcer, cyber hackers of wireless communications, power company workers, and other anonymous parties who may perform malicious actions that are detrimental to the occupants of the premises where the smart meter is located. Malicious attackers can affect real-time consumption price in two ways[13]. One is by manipulating the meter readings which can directly affect the quantity of electricity usage. The other way is by manipulating meter readings which will affect the Locational Marginal Prices (LMP) calculation. The hacker can control power consumption, and then eavesdrop on the encrypted value sent by the meter. The most significant attacks that threaten information privacy are intrusion or modification of network communication, illegal access to stored data, man-in-the-middle attacks and malicious software which mainly target smart meter firmware or control systems. Wireless networks are also easily sniffed by attackers and may be vulnerable to Man-in-the-Middle

attacks. Man-in-the-middle attacks can snoop and modify data during transmission, which jeopardize data integrity.

3.6 Some Security Requirements for Smart Metering Networks:

Due to unique properties of SMNs such as two-way communication, it is difficult and challenging task to secure and protect smart meter data from being compromised by the attackers. Although there are many security solutions available for wired and wireless networks, they cannot simply be directly implemented into SMNs. Therefore, it is important to explore the security requirements for this network in order to ensure the security of data communication in SMNs. we highlight and discuss several security requirements for SMNs. As shown in Fig. 3.1, there are six security requirements, namely, data confidentiality, data integrity, data freshness, data availability, non-repudiation and authentication which are of important aspects to be considered in ensuring the security of data communication in SMNs.

In this section, we highlight and discuss several security requirements for SMNs. As shown in Fig. 3.1, there are six security requirements, namely, data confidentiality, data integrity, data freshness, data availability, non-repudiation and authentication which are of important aspects to be considered in ensuring the security of data communication in SMNs.

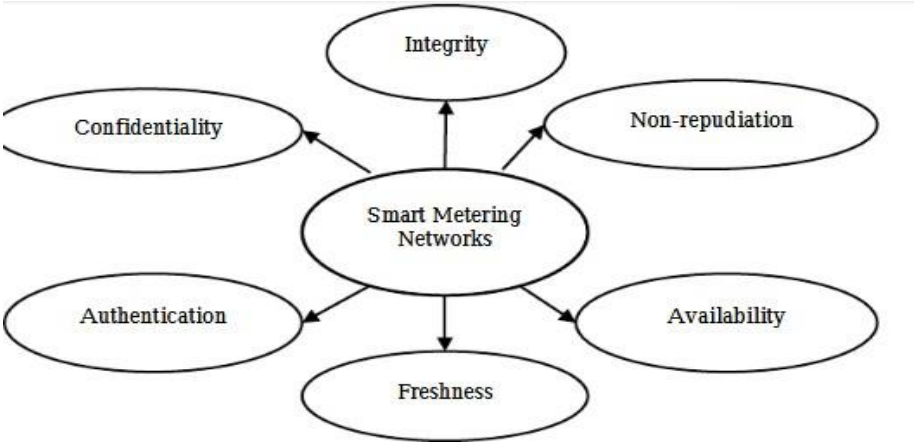

Fig: 3.1. Security requirement for SMNs

1. Data Confidentiality: Data confidentiality needs to be preserved to ensure that the content of data being transmitted will never be exposed to unauthorized parties. In SMNs, data confidentiality is an essential requirement to protect data from attacks like EVD and men-in-the-middle (MIM) and to preserve user's privacy information. In SMNs, data confidentiality can be ensured by using data encryption techniques such as symmetric or asymmetric encryption.

2. Data Integrity: When transferring data over the network, the sender would have wanted to ensure that the receiver gets the data that are of genuine or similar as have been transferred earlier. The purpose of having data integrity in smart metering communication is to ensure that the content of the original data has not been modified or altered either accidentally or maliciously during transmission process. To guarantee data integrity in SMNs, hash functions or Message Authentication Code (MAC) can be added to the encrypted data so that any unauthorized changes to the original data can be detected[10].

3. Data Freshness: Data freshness is another important security requirement to ensure that the transmitted data is fresh and recent. In SMNs, data freshness can be achieved by using nonce techniques which can be represented in the form of a counter, timestamp or message sequence number that is generated randomly using random number generator. To avoid from being altered by an attacker, the nonce will be encrypted with the message before it can be sent to its

destination. The purpose of having such requirement is to protect the data from being manipulated by replay attacker.

4. Data Availability: If confidentiality is associated to privacy, data availability on the other hand is associated to survivability. In SMNs, data availability ensures that the network is alive, and data is accessible even in the presence of DoS attack. A DoS attack could be launched at any layer of SMNs such as jamming attacks which can disrupt physical and Medium Access Control layers functions. At the network layer, an attacker could interrupt or destroy the routing protocol whereas at the application layer, an attacker could disable or deactivate important services such as network broadcast and key management services[12].

5. Non-Repudiation: Non-repudiation is a security requirement to ensure that a sender or receiver cannot deny of having sent or received a message. This requirement is essential especially to detect any existence of an attacker that tries to launch false data injection, flooding and replay attacks. There are many ways to enable this requirement; one of them is by using public key cryptography.

6. Authentication: Authentication is the process of determining or verifying either someone or something is who or what it is claimed to be. Authentication can be divided into entity authentication and data authentication. Entity authentication (EA) or source authentication gives the opportunity to a receiver to verify whether the received data is sent by the right source or not. In this case, an attacker cannot participate or join into any activities in the targeted network because it has no privilege to access the network. Without entity authentication, an attacker could masquerade as a legit smart meter, thus gaining unauthorized access to sensitive data. On the other hand, data authentication (DA) allows a receiver to verify that the received data are of similar ones that have been transmitted[12].

4. IPV6 and ICMPV6 vulnerabilities and attacks:

Header Structures:

The common way to represent theses header is to draw them as a succession of 32-bit words. The top word is transmitted first and the left most byte of each word is transmitted first.

4.1 IPv4 Header:

IPv4 provides 32-bit address space and has a theoretical upper limit of about 4 billion (4,000,000,000) unique addresses but in practice IPv4 is unlikely to support a sustainable population of no more than about 250 million uniquely addressed nodes. The IPv4 header structure is described below and shown in Figure 4.1.

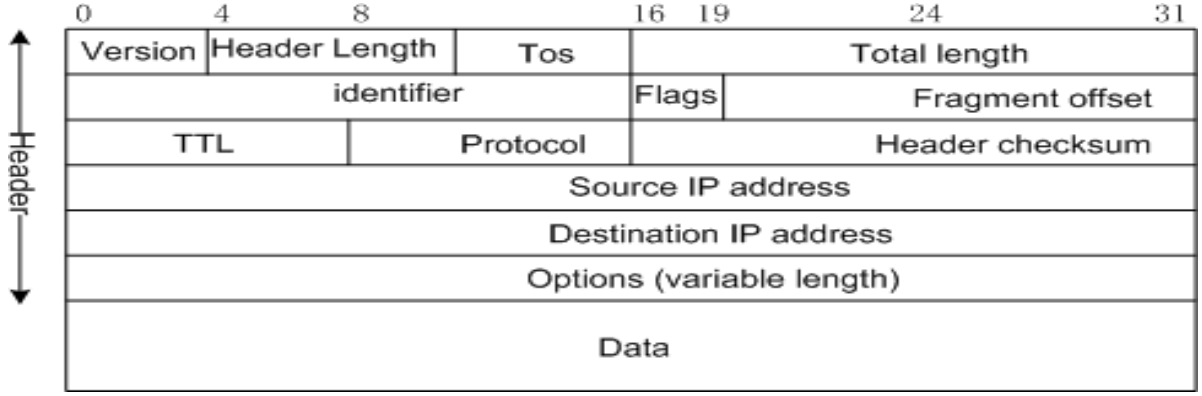

Fig 4.1: IPv4 Header Structure

- **Version**: The Version field specifies the current version which is 4 in this case. The header processing software checks this first and then knows how to process the rest.
- **HLen**: The HLeng specifies the number of 32-bit words in the header. Minimum is 5 where 5×32=160 bits or 20bytes. The maximum is 15 where 15×32=480 bits or 60 bytes.
- **TOS**: Differentiated Services Code Point formerly known as TOS (Type of service) is used to indicate if a packet should receive some sort of special or priority processing.
- **Length**: This is a 16-bit field defining the total length of the datagram (header and data). The minimum is 20bytes and the maximum is 65,535 bytes.
- **Ident**: The Ident is used for identifying fragments of the original datagram.
- **Flags**: The Flags is a 3-bit field used to control and count fragments of the datagram.
- **Offset**: The Offset is a 13-bit field that specifies the offset of a particular fragment relative to the beginning of the original unfragmented datagram. The first fragment has an offset of zero.
- **TTL**: The TTL (Time to Live) reflects historical intention where the time the packet was allowed to exist on the network was considered but it has become more of a hop count than a timer.
- **Protocol**: The Protocol field is a key that identifies to which of the OSI higher-level protocol the IP packet should be passed to. Examples are TCP and UDP.
- **Checksum**: The checksum field is the 16-bit one's complement of the one's complement sum of all 16-bit words in the header.It is used for error checking the header. If an error is detected the packet is discarded and must be resend.
- **SourceAddr**: The SourceAddr (Source Address) is the IPv4 address of the sender. It is included so that the recipient can decide if it wants to receive data from this sender and also to know where to reply to if it wants to reply. Note that during transit a NAT device could change this address.

- **DestinationAddr**: The DestinationAddr (Destination Address) is the IPv4 address indicating the receiver of this packet. Note that during transit a NAT device could change this address.
- **Options** (variable): There may be a number of options at the end of the header but these are not used often.

4.2 IPv6 Header:

Migration to IPv6 support is a gradual process, and mechanisms to gracefully support IPv6 in IPv4 networks have been an important part of the IPv6 development project from the start.IPv6 provides a 128-bit address space and can address 3.4×1038 nodes.
The IPv6 header structure is described below and shown in Figure 4.2.

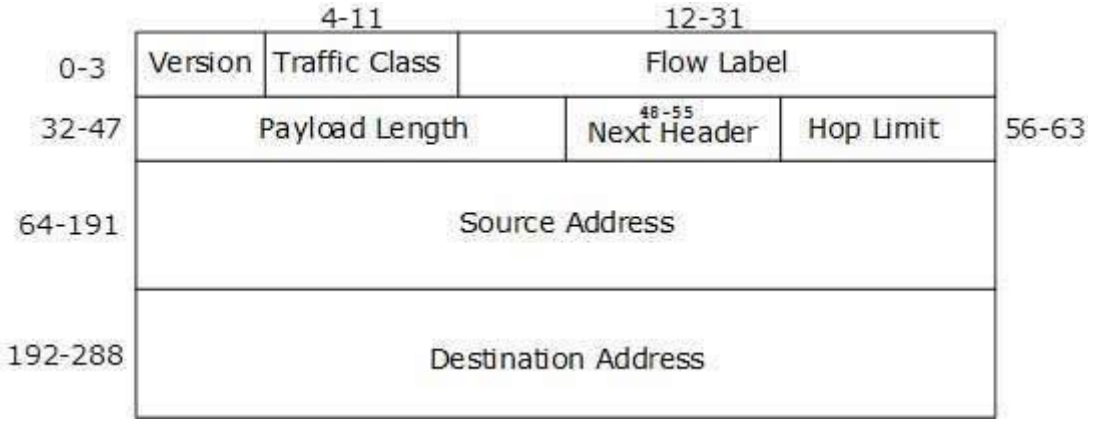

Fig 4.2: IPv6 Header Structure

- **Version**: The Version field is set to 6 for IPv6.
- **TrafficClass**: The TrafficClass field identifies the priority and class of service of this packet.
- **FlowLabel**: The FlowLabel field is for future use in identifying packets that are part of a unique flow, stream, or connection
- **PayloadLen**: The PayLoadLen field defines the length in octets of the packet that follows the IPv6 header.
- **NextHeader**: The NextHeader field identifies the type of header that follows the IPv6 header. This replaces the Options and Protocol field of IPv4.
- **HopLimit**: The HopLimit field is a counter for the number of remaining hops the packet can traverse. This is simply the TTL of IPv4 renamed.
- **SourceAddress**: The IPv6 address of the node that originated this packet.
- **DestinationAddress**: The IPv6 address that this packet is destined for.

4.3 IPV4 VS IPV6:

4.3.1 Similarities between IPv6 and IPv4 vulnerabilities:

IPv6 and IPv4 both fall within the Network Layer of the OSI stack. If for example a network layer application is vulnerable in IPv4, it will also be vulnerable in IPv6.
A list of similar vulnerabilities:

- Attacks against the physical, data link or application layers
- Man-in-the-middle attacks
- Eavesdropping

- Denial of Service (DoS) attacks
- Spoofed packets
- Attacks against routers and other networking devices

4.3.2 Differences between IPv6 and IPv4 vulnerabilities:

The way in which IPv6, as part of the network layer of the OSI stack, interacts with the layers above and below it can also introduce new vulnerabilities.
A list of vulnerabilities where the difference is only slightly:

- LAN-based attacks through the Address Resolution Protocol (ARP) or Neighbor Discovery Protocol (NDP)
- Attacks against Dynamic Host Configuration Protocol (DHCP) or DHCPv6
- Denial of Service (DoS) against routers
- Fragmentation
- Packet amplification attacks

4.3.3 A list of vulnerabilities where the difference is unique to IPv6:

- Reconnaissance(since brute force with the larger address space is more time consuming) and scanning worms
- Attacks against the required component Internet Control Message Protocol for IPv6(ICMPv6)
- Extension Header (EH) attacks
- NDP attacks (Auto configuration) are simple to perform
- Attacks on dual stack implementation migrating from IPv4 to IPv6.
- Mobile IPv6 attacks. Devices that roam are susceptible to much vulnerability.
- IPv6 protocol stack attacks because bugs and shortcomings might exist in the code.

4.4 ICMP Protocol:

4.4.1 ICMPv4:

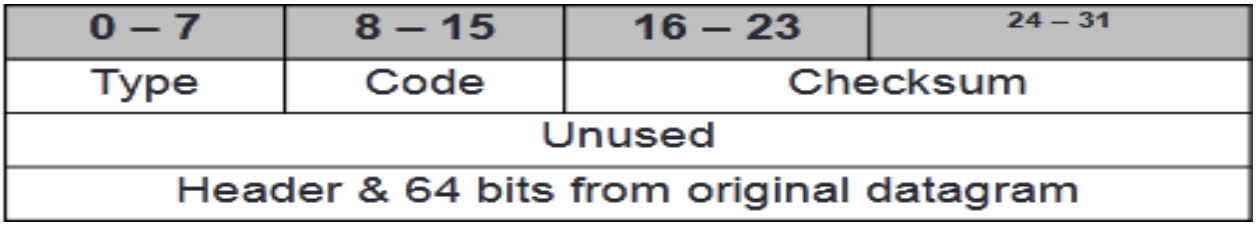

Fig 4.3: ICMPv4 Packet Format

4.4.2 ICMPv6:

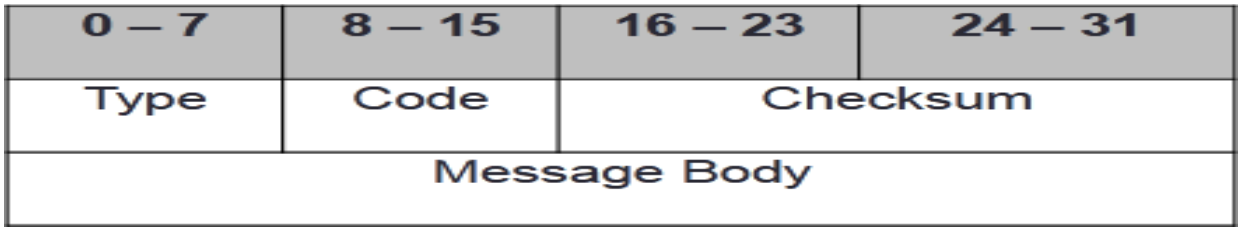

Fig 4.4: ICMPv6 Packet Format

4.4.3 ICMP Attacks:

ICMP Sweep:

Under these attacks, the attackers will send range of 'echo request' continuously and this will force the host to reply the echo requests' continuously. This will keep the host busy replaying to the 'echo requests'. This attack is known as ICMP Sweep attack. This scenario will lead into flooding unnecessary data in the network and degrade the performance of the network. In any typical attack scenario, the attacker will first engage in some reconnaissance and scanning activities in order to

1. Better understand the environment of the target
2. Gather information about the target so as to plan the attack approach
3. Employ the right techniques & tools for the subsequent attack phases

The Figure 4.5 illustrated how these attacks take place in the network.

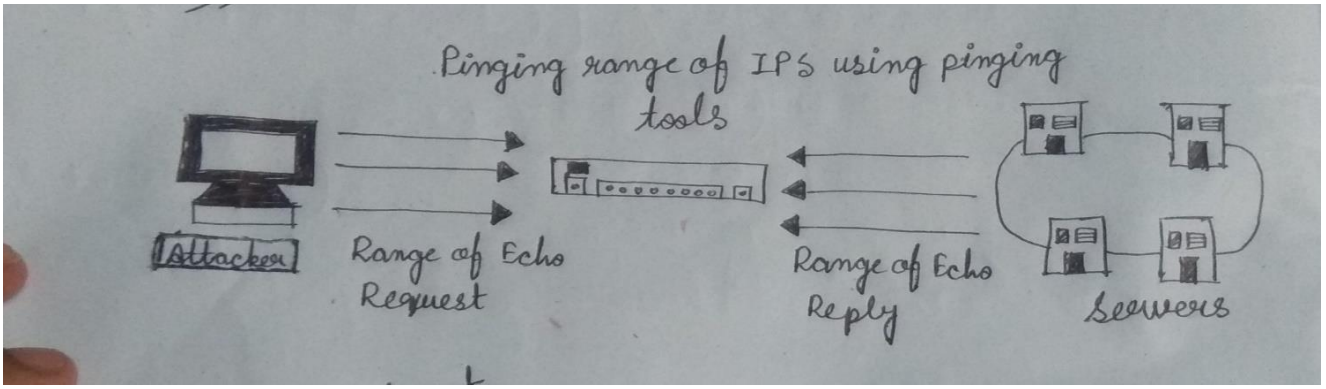

Fig 4.5: ICMP Sweep Attack

ICMPv6 Significant Parameter: Type=128 and Code=0

Inverse Mapping:

Inverse Mapping is a technique used to map internal networks or hosts that are protected by a filtering device. Usually some of those systems are not reachable from the Internet. We use routers, which will give away internal architecture information of a network, even if the question they were asked does not make any sense, for this scanning type. We compile a list of IP's that list what is not there, and use it to conclude where things probably are.

An Inverse Mapping attack is illustrated below:

Step 1. Attacker sends an ICMP reply message to a range of IP addresses presumably behind a filtering device.

Step 2. Upon receiving the series of ICMP reply messages, since the filtering device does not keep state of the list of ICMP requests, it will allow these packets to their destination.

Step 3. If there is an internal router, the router will respond with a ICMP "Host Unreachable" for every host that it cannot reach, thus giving the attacker knowledge of all hosts which are present behind the filtering device.

ICMPv6 Significant Parameter: Type=129 Code =0 without sending Type =120 Code = 0

ICMP Route Redirect:

One of the key functions of ICMP is to facilitate redirect routing in case failing of any one router or in efficient performance of the particular router in the network when ICMP message received from any host.

Attacker would exploit the above mentioned weakness of by redirecting the routing to exploiter's router so that the attackers can again access all the information in the packets. This is the will

allow the Man-In-Middle attacks take place.

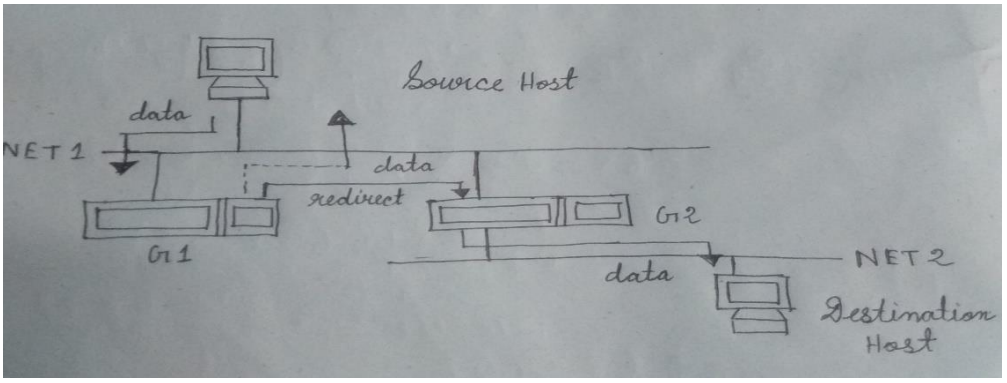

Fig 4.6: ICMP Route Redirect

In Figure 4.6, the attacker will able to intercept the communication between source and destination host via gateway G2 by taking control of the secondary gateway G1 means of sending ICMP route redirect message to the source host. So all traffic bound for destination host has to go through Gateway G1 which leads into Man-In-The-Middle (MITM) attack.

ICMPv6 Significant Parameter Type =5 Type = 137 and Code= 0

ICMP Router Discovery Message Attack:

When a host boots up, it will look out for the default router by issuing a "router solicitation" message. When the attacker listens in to this message, it will spoof a reply to the host. The default route of the host is now will be set to the attacker's IP address in its reply. Now the attacker can initiate attacks such as sniffing, man-in-the-middle attacks for all the traffic outbound traffic via the attacker's machine.

A possible attack scenario is illustrated below:

Step 1. Host boots up and issues a "router solicitation" message to find out the default router on the network.

Step 2. Attacker listens in to the message and spoofs a reply to that host.

Step 3. The default route of the host is now set to the attacker's IP address that the attacker has included in his reply.

Step 4. Now the attacker could employ either sniffing, man-in-the-middle attack for all traffic outbound through the attacker's machine.

Step 5. Denial of service attack is also possible by not forwarding any packets onto the correct subnet.

At the time the denial of service attack is also can be initiated by not forwarding any packets onto the correct subnet as shown by Figure 4.7 as below.

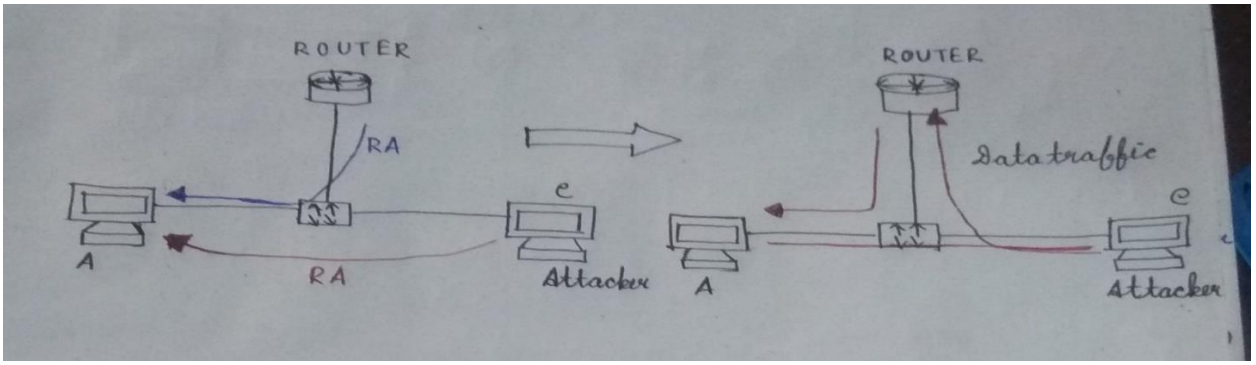

Fig 4.7: ICMP Router Discovery Message Attack

ICMPv6 Significant Parameter Type=9 and 10, Code =0 Type=133 and 134, Code=0

4.4.4 Unique ICMPv6 Attacks:

In IPv6 networks, there are attacks that are only specific to ICMPv6. The following section highlights the attacks that only unique to ICMPv6 only.

Man In The Middle Attack With Spoofed ICMPv6 Neighbor Advertisement:

In IPv4, MITM carried out using ARP Cache Poising and DHCP spoofing. Since in IPv6, ARP is replaced by ICMPv6 neighbor discovery process, so this attacks only unique to IPv6 networks only.
Figure 4.8 shows the process flow of how MITM attack take place in the IPv6 network.

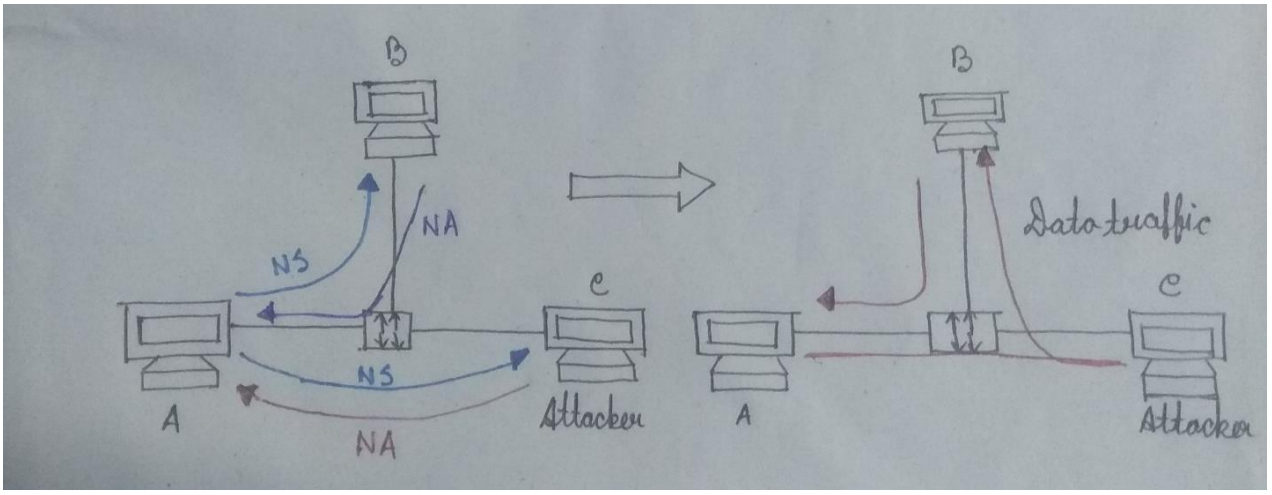

Fig 4.8: MITM with spoofed ICMPv6 NA

In the above attacks both Node A and Node B can perform communication and data transfer normally, but all traffics from Node A to Node B goes through the attacker's node. The attacker also can use this opportunity to intercepting the traffic to steal secret or confidential information, filtering the traffic, hijacking the established TCP connection, etc.
ICMPv6 Significant Parameter Type = 135 and 136, Code =0

Duplicate Address Detection (DAD):

In order to detect whether an IPv6 address already exist in the network under the IPv6 stateless auto configuration, Duplicate Address Detection (DAD) protocol is used to detect the duplication. DAD only applicable for IPv6 networks only. DAD uses ICMPv6 neighbor solicitation by sending to all the nodes multicast addresses. If there are no IPv6 addresses exist on the network, no response will be sent back to the solicitation source host. Under these attacks, since everyone can reply to the ICMPv6 neighbor solicitation, every solicitation sent to detect possible duplication will be replied. Finally no one can join the network. This will scenario will be known as Denial of Service where it prevents new IPv6 host on the network.
ICMPv6 Significant Parameter Type = 135 and 136, Code=0

4.5 Neighbor Discovery Protocol (NDP):

This protocol performs the following functions:

- Address Resolution
- Neighbor Unreachability Detection
- Auto configuration

• Redirect Indication
• Detecting the router and network prefix
• Determining important parameters for packet transmission
• Identifying the next hop

NDP uses five ICMPv6 messages:

• **Router Solicitation (RS) message:** The Router Solicitation message is sent by SM/IPv6 hosts to discover the presence of legitimate DCU/IPv6 routers on the link.

	Bits 0–7	Bits 8–15	Bits 16–23	Bits 24–31
0	Type	Code	ICMP checksum	
32	Reserved			
...	Options			

Fig: 4.9: RS message packet format

• **Router Advertisement (RA) message:** Routers send RA message in response to the RS message.

	Bits 0–7	Bits 8–15	Bits 16–23	Bits 24–31
0	Type	Code	ICMP checksum	
32	Hop limit	M | O | HA | Pref | Proxy |Reserved	Router lifespan	
64	Accessibility time out			
96	Resolution time out			
...	Options			

Fig: 4.10 : RA message packet format

• **Neighbor Solicitation (NS) message:** A Neighbor Solicitation (NS) message is sent by SM to determine the link-layer address of a neighbor, and also to verify whether an address is already present on link or not[14].

	Bits 0–7	Bits 8–15	Bits 16–23	Bits 24–31
0	Type	Code	ICMP Checksum	
32	Reserved			
64	Target address			
96				
128				
160				
...	Options			

Fig: 4.11: NS message packet format

• **Neighbor Advertisement (NA) message**: Hosts send NA message in response to the NS message.

	Bits 0–7	Bits 8–15	Bits 16–23	Bits 24–31
0	Type	Code	ICMP checksum	
32	R | S | O Reserved	Reserved		
64	Destination address			
96				
128				
160				
...	Options			

Fig: 4.12: NA message packet format

• **Router Redirect (RR) message**: The Redirect message is sent by DCU to inform an originating SM of a better DCU address for a specific destination i.e. DCU send it to inform a SM about a better router on its link.

	Bits 0–7	Bits 8–15	Bits 16–23	Bits 24–31
0	Type	Code	ICMP checksum	
32	Reserved			
64	Destination Address (Hop)			
96				
128				
160				
192	Destination address			
224				
256				
288				
...	Options			

Fig: 4.13: RR message packet format

4.6. Smart Meter Communication through NDP:

- Smart meter collects the reading from home appliances. The HAN provides the communication between the Smart Meters in a home and other appliances in that home. DCU collects data from SM's. The NAN connects SMs to the Data Collection Units (DCUs). MDSM collects data from DCU's. WAN provides communication between the DCUs and Meter Data Management System (MDMS). To establish a connection in NAN a SM should find DCU to bind with. Each DCU and SM manages its neighbor cache which stores information about their Neighbor hops and neighbor DCUs.

- Smart Grid System uses NDP protocol to communicate with their neighbors. The Neighbor Discovery (NDP) is the most important part in IPv6; it allows a node to integrate into the local network environment in which IPv6 packets are physically transmitted. Through to this protocol, it becomes possible to interact with the equipment connected to the same support (stations and routers).

- IPv6 uses Network Discovery Protocol (NDP) to find the MAC address. The IPv6 Stateless Address Auto Configuration (SLAAC) of IPv6 is primarily based on the NDP process[15].

5. Proposed Attack Scenarios in AMI:

1. Adversary SM wants to make connection with legitimate DCU by spoofed RS message.

Let there is legitimate SM A, adversary SM B and legitimate DCU C having IP address as IP(A), IP(B) and IP(C) respectively. Let their MAC addresses be MAC(A), MAC(B) and MAC(C) respectively.

- A send RS message to query about MAC address corresponding to IP(C) in its local link.
- Following the genuine RS, B can send spoofed RS (IP(A)-MAC(B)) to query about MAC address corresponding to IP(C) .
- In response legitimate DCU C responds with RA message which contains MAC(C).
- There is a connection establish between IP(A)-MAC(B) with IP(C)-MAC(C) and B update its cache table.

2. Adversary DCU wants to make connection with legitimate SM by spoofed RA message.

Let there is legitimate SM A, adversary DCU B and legitimate DCU C having IP address as IP(A), IP(B) and IP(C) respectively. Let their MAC addresses be MAC(A), MAC(B) and MAC(C) respectively.

- A send RS message to query about MAC address corresponding to IP(C) in its local link.
- In response legitimate DCU C responds with RA message which contains MAC(C).
- Following the genuine RA, B can send spoofed RA (IP(C)-MAC(B)) to IP(A)-MAC(A).
- Neighbor cache of A will update IP (C)-MAC (C) with (falsified) IP (C)-MAC (B).
- There is a connection establish between (IP(A)-MAC(A)) with IP(C)-MAC(B).

3. Adversary SM wants to make connection with legitimate SM by spoofed NS message.

Let legitimate SM A, adversary SM B and legitimate SM C be three smart meters in the same subnet having IP address as IP(A), IP(B) and IP(C) respectively. Let their MAC addresses be MAC(A), MAC(B) and MAC(C) respectively.

- A send NS message to query about MAC address corresponding to IP(C) in its local link.
- Following the genuine NS, B can send spoofed NS (IP(A)-MAC(B)) to query about MAC address corresponding to IP(C) .
- In response legitimate SM C responds with NA message which contains MAC(C).
- There is a connection establish between (IP(A)-MAC(B)) with IP(C)-MAC(C) and B will update its neighbor cache table.

4. Adversary SM wants to make connection with legitimate SM by spoofed NA message.

Let legitimate SM A, adversary SM B and legitimate SM C be three smart meters in the same subnet having IP address as IP(A), IP(B) and IP(C) respectively. Let their MAC addresses be MAC(A), MAC(B) and MAC(C) respectively.

- A send NS message to query about MAC address corresponding to IP(C) in its local link.
- In response legitimate SM C responds with NA message which contains MAC(C).
- Following the genuine NA, B can send spoofed NA (IP(C)-MAC(B)) to IP(A)-MAC(A).
- Neighbor cache of A will update IP (C)-MAC (C) with (falsified) IP (C)-MAC (B).

5. Adversary DCU wants to make connection with legitimate SM/SMs with the help of spoofed RR.

Let there is legitimate SM A, legitimate DCU C, legitimate DCU D and adversary DCU E having IP address as IP(A), IP(C), IP(D) and IP(E) respectively. Let their MAC addresses be MAC(A), MAC(C), MAC(D) and MAC(E) respectively. Let SM A is connected to DCU C.

- D sends RR claiming himself a better router in the network.
- Following the genuine RR, E can send spoofed RR (IP(D)-MAC(E)) to IP(A)-MAC(A).
- Cache of A will update IP (D)-MAC (D) with (falsified) IP (D)-MAC (E).
- A get connected to E.

6. Proposed Mitigation Schemes in AMI:

6.1 Mitigation Technique 1:

1. Mitigation of RS Process:

Adversary SM wants to make connection with legitimate DCU by spoofed RS message.
Let there is legitimate SM A, adversary SM B, legitimate DCU C and legitimate DCU D having IP address as IP(A), IP(B), IP(C) and IP(D) respectively. Let their MAC addresses be MAC(A), MAC(B), MAC(C) and MAC(D) respectively.

- SM A send RS message to query about MAC address corresponding to IP(C) in its local link.
- Following the genuine RS, B can send spoofed RS to DCU C and its neighbor cache.
- DCU C extracts the SM's address by B=A.
- DCU C sends echo request message to its neighbor DCU D.
- DCU D sends echo reply message with the SM's address=A.
- DCU C checks the majority decision of its neighbors.
- Finally, the address did not match and DCU C discards B's RS.
- DCU C responds with a RA message to SM A and get connected with it.

2. Mitigation of RA Process:

Adversary DCU wants to make connection with legitimate SM by spoofed RA message.
Let there is legitimate DCU A, adversary DCU B, legitimate SM C and legitimate SM(D) having IP address as IP(A), IP(B), IP(C) and IP(D) respectively. Let their MAC addresses be MAC(A), MAC(B), MAC(C) and MAC(D) respectively.

- SM C sends RS message to query about MAC address corresponding to IP(A) in its local link.
- In response legitimate DCU A responds with RA message which contains MAC(A) .
- Following the genuine RA, B can send spoofed RA with valid prefix.
- SM C extracts the DCU's address = B.
- SM C sends echo request message to its neighbor SM D.
- SM D sends echo reply message with the DCU's address=A.
- SM C checks its own DCU address with its neighbor's DCU address.
- The address did not match and SM C discards RA of adversary DCU B.
- SM C registers SM A as a valid DCU on its link as per the majority decision of its neighborhood data.

3. Mitigation of NS Process:

Adversary SM wants to make connection with legitimate SM by spoofed NS message. Let legitimate SM A, adversary SM B, legitimate SM C and legitimate SM D be four smart meters in the same subnet having IP address as IP (A), IP (B), IP(C) and IP(D) respectively. Let their MAC addresses be MAC (A), MAC (B), MAC(C) and MAC(D) respectively.

- SM A sends NS message to query about MAC address corresponding to IP(C) in its local link.
- Following the genuine NS, SM B can send spoofed NS to SM C and its neighbor cache.
- SM C extracts the neighbor information of B=A.

• SM C sends echo request message to its neighbor SM D.

• SM D sends echo reply message with the SM's address=A.

• SM C checks the majority decision of its neighbors.

• After checking, the address did not match and SM C discards NS of adversary SM B.

• SM C replies with a NA message to SM A and its neighbor cache for getting connected with it.

4. Mitigation of NA Process:

Adversary SM wants to make connection with legitimate SM by spoofed NA message. Let legitimate SM A, adversary SM B, legitimate SM C and legitimate SM D be four smart meters in the same subnet having IP address as IP (A), IP (B), IP(C) and IP (D) respectively. Let their MAC addresses be MAC (A), MAC (B), MAC(C) and MAC (D) respectively.

• A send NS message to query about MAC address corresponding to IP(C) in its local link and its neighbor cache.

• In response, legitimate SM C responds with NA message which contains MAC(C) along with all its neighbors in its neighbor cache.

• A extracts the neighbor information by C=D.

• A unicast a query message to D by asking "Is C your neighbor?"

• D sends a confirmation message by confirming C.

• A builds the neighbor list of C from the confirmation messages received from its neighbor and verifies it with the neighborhood data sent by C itself.

• SM A continues sending queries until it has a majority decision of all the neighbors of C.

• A Sends a new NS message to query about MAC address corresponding to IP(E) in its local link and its neighbor cache.

• Following this genuine NS, Adversary SM B can send a spoofed NA to A and its corresponding neighbor cache.

• A extracts the neighbor information by E=C and waits for the decision of majority.

• A unicast a query message to C, "is E your neighbor?"

• SM C confirms that E is not its neighbor.

• SM A discards the NA message of adversary SM B.

5. Mitigation of RR Process:

Adversary DCU wants to make connection with legitimate SM/SMs with the help of spoofed RR. Let there is legitimate DCU A, adversary DCU B, legitimate SM C, legitimate SM D and legitimate DCU E having IP address as IP(A), IP(B), IP(C), IP(D) and IP(E) respectively. Let their MAC addresses be MAC(A), MAC(B), MAC(C), MAC(D) and MAC(E) respectively. Let SM D is connected to DCU E.

• Legitimate DCU A send RR claiming itself a better router in the network.

• Following the genuine RR, B can send spoofed RR and sends it to the existing SMs in the network(SM C & SM D).

• Legitimate SM C extracts the DCU's address=B.

• SM C sends echo request message to its neighbor SM D.

• SM D sends echo reply message with the DCU's address=A.

• SM C and D send RS messages to DCU A to check whether a new DCU is available or not.

• DCU A respond with RA messages to those SMs(C & D) as there doesn't exist any new

DCU in the network.

- The SMs(C & D) discard B's RR message.

6.2 MITIGATION TECHNIQUE 2:

This section focuses on the proposed Intrusion Detection System (IDS) for detection of RS/RA/NS/NA/RR spoofing attacks.

6.2.1. Assumptions

The proposed model relies on the following assumptions regarding IPv6 LAN.

1. All nodes are IPv6 configured using Stateless address auto configuration (SLAAC) mechanism or have been assigned static IP. The router has a static IPv6 address which sends out various network parameters required by hosts on the network for auto configuration.

2. Genuine non-compromised nodes on the link which are expected to reply a Neighbor Solicitation message (either unicast or multicast) must do so within a specific time interval □□□□.

3. IDS is a trusted machine with a static IP-MAC binding. It has two network interfaces dedicated to their respective purposes; one being responsible to collect network data in the LAN through port mirroring and the other being exclusively used for handling NS/RS or NA/RA probes requests/replies. The proposed system maintains information about the network traffic in data tables described below.

6.2.2. Data tables for the proposed system

Our proposed scheme ensures the genuineness of the IP-MAC pairing by an active verification mechanism. The scheme sends verification messages termed as NS/RS probe requests upon receiving RSs, NSs, RAs and NAs. To assist in the probing and separating the genuine IP-MAC pairs with that of spoofed ones, we maintain some information obtained along with the probe requests, RSs, NSs, RAs and NAs in some data tables. The information and the data tables used are enumerated below. Henceforth in the discussion, we use the following short notations: □□□ - Source IP Address, □□□ – Destination IP Address, □□□□ - Source MAC Address, □□□□ – Destination MAC Address. Fields of any table would be represented by ⟨ □□□□□□□□⟩ ⟨ □□□□⟩ ; e.g., □□□□□□ represents the source IP filed of "Neighbor Solicitation Table. Also,
⟨ □□□□□□□□⟩ □□□ represents the maximum elements in the table at a given time.

1. Router Solicitation Table: (RS□**):**

Purpose: Whenever a router solicitation message is sent, it is recorded in the solicitation table R□□.

Components (Rows): R□□□□ Source IP of the Solicitation message, R□□□□□*s* Source MAC of the Solicitation message, R□□□□□ Destination IP of the Solicitation message and timestamp R□□□□□,

2. Router Advertisement Table: (RA□**):**

Purpose: This table records router advertisement messages sent by nodes in the network. Components: R□□□□□ Source IP of the Advertisement message,*R*□□□□□□ Source MAC of the Advertisement message, R□□□□□ Destination IP of the Advertisement message, R□□□□□□ Destination MAC of the Advertisement message and timestamp R□□□□□.

3. Neighbor Solicitation Table: (□□□):

Purpose: Whenever a neighbor solicitation message is sent, it is recorded in the solicitation table □□□.

Components (Rows): □□□□□□ Source IP of the Solicitation message, □□□□□ Source MAC of the Solicitation message, □□□□□□ Destination IP of the Solicitation message and timestamp

□□□□□□,

4. Neighbor Advertisement table (□□□):

Purpose: This table records neighbor advertisement messages sent by nodes in the network. Components: □□□□□□ Source IP of the Advertisement message,*N*□□□□□□ Source MAC of the Advertisement message, □□□□□□ Destination IP of the Advertisement message, □□□□□□□ Destination MAC of the Advertisement message and timestamp □□□□□□.

5. Router Redirect Table: (□□□):

Purpose: Whenever a router redirect message is sent, it is recorded in the redirect table RR□.
Components (Rows): RR□□□ Source IP of the Solicitation message, RR□□□□*s* Source MAC of the Solicitation message, RR□□□□ Destination IP of the Solicitation message and timestamp RR
.

6. Probe table (□□□):

Purpose: For the verification of an IP-MAC pair, our IDS sends out a Router Solicitation/Neighbor solicitation probe packet and its response (router advertisement/neighbor advertisement) is verified. This process is initiated to inspect suspicious RS, RA, NS, NA, RR messages. The probe table stores the information about the probe packets sent out by IDS. Components: □□□□P IP address for which verification message is being sent, □□□□□□ MAC address for which verification message is being sent.

7. Authenticated bindings table (□□□□):

Purpose: This table records IP-MAC bindings which have been found to be authentic by the verification mechanism of IDS. Components: □□□□□□ and □□□□□□C IP-MAC pair verified to be genuine.

8. Log table (□□□):

Purpose: Whenever a spoofing is detected, the parameters are recorded here along with the timestamp. Components: □□□□□□ Source IP of the Advertisement message, □□□□□ Source MAC of the Advertisement message, □□□□□□ Destination IP of the Advertisement message, □□□□□□□ Destination MAC of the Advertisement message and timestamp □□□□□□.

9. Unsolicited advertisement table (□□□□):

Purpose: This data table stores information about number of neighbor advertisements for which no neighbor solicitation exists sent by a node within a specified time interval □. Also malicious neighbor solicitation messages (those which are not in Log table and Authenticated table) are stored in this table. Components: □□□□□□□ Destination IP of the Advertisement message and timestamp □□□□□□□. Although □□s are sent in response to □□s normally, there are exceptions to it. For example, □□s are unsolicited when sent in order to propagate new information like change in its MAC or IP address or at the time a node joins a network. Such□□s are handled separately and are not included in the Unsolicited Advertisement table.

6.2.3. MITIGATION:

Assumption:

1. IP-MAC pairing of the IDS is already verified.
2. Status flag: Shows the status of the packet sending NS.

1. Mitigation for RS:

1. RS request is added to the Router Solicitation Table (RST).
2. RS packet is searched in Authenticate Binding Table (AUTH).
3. If (match) thren status = GENUINE [IP-MAC pair is already recorded in AUTH table]
4. If (mismatch) then status = SPOOFED and spoofed packet details is recorded in LOG table.
5. If neither of the above cases occurred then the PROBE packet is sent to verify the genuineness of the packet.

2. Mitigation for RA:

1. Add RAPIPS, RAPMACS, RAPIPD and tau to the Advertisement table (RAT).
2. If ((RAPIPS = RSPIPD for some RSP present in the RST table) and (RAPIPS is found in AUTH table) and (RAPMACS also matched))

Then

Status = GENUINE
3. Otherwise status = SPOOFED and spoofed packet detail is recorded in LOG table.
4. If the advertisement packet entry is not available in any Authenticated table, then a RS probe is sent to verify genuineness.

3. Mitigation for NS:
1. NS request is added to the Neighbor Solicitation Table (NST).
2. NS packet is searched in Authenticate Binding Table (AUTH).
3. If (match) thren status = GENUINE [IP-MAC pair is already recorded in AUTH table]
4. If (mismatch) then status = SPOOFED and spoofed packet details is recorded in LOG table.
5. If neither of the above cases occurred then the PROBE packet is sent to verify the genuineness of the packet.

4. Mitigation for NA:
1. Add NAPIPS, NAPMACS, NAPIPD and tau to the Advertisement table (NAT).
2. If ((NAPIPS = NSPIPD for some NSP present in the NST table) and (NAPIPS is found in AUTH table) and (NAPMACS also matched))
Then
Status = GENUINE
3. Otherwise status = SPOOFED and spoofed packet detail is recorded in LOG table.
4. If the advertisement packet entry is not available in any Authenticated table, then a NS probe is sent to verify genuineness.

5. Mitigation for RR:
1. RR request is added to the Router Redirect Table (RRT).
2. RR packet is searched in Authenticate Binding Table (AUTH).
3. If (match) thren status = GENUINE [IP-MAC pair is already recorded in AUTH table]
4. If (mismatch) then status = SPOOFED and spoofed packet details is recorded in LOG table.
5. If neither of the above cases occurred then the PROBE packet is sent to verify the genuineness of the packet.

7. Simulation:

Simulation tool : Cooja Network simulator

7.1. Trial Network:

Trial Network with rpl-border-router mote and udp-sender mote to understand the simulator.
We used **/contiki/examples/ipv6/rpl-border-router/border-router.c** as a contiki firmware for compiling to create a mote "mote 1". We again used **/home/user/contiki/examples/ipv6/rpl-collect/udp-sender.c** for compiling to create other 24 corresponding motes in the network panel. "Serial Socket (SERVER)" of sky 1 will create a serial port on the Border Router which is accessible via UDP port number 60001 on the local machine[16][17].

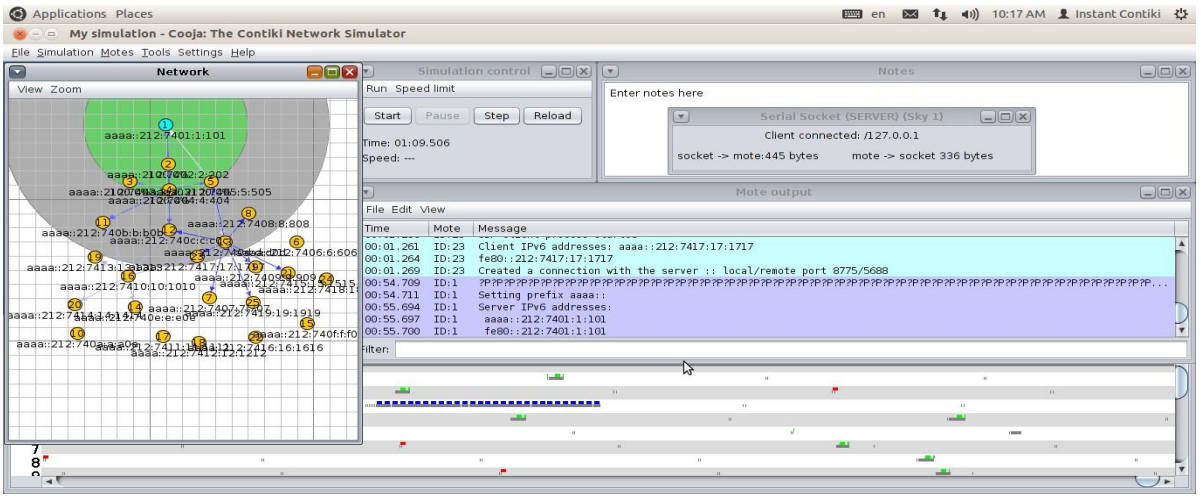

Fig 7.1: Network creation between border-router and udp-sender motes.

A Terminal window is showing the following commands which will establish the bridge to the Border Router. This will return a bridge which has been established and IPv6 addresses assigned with prefix aaaa::/64. The Border Router's IPv6 address of aaaa::212:7401:1:101 can be seen.

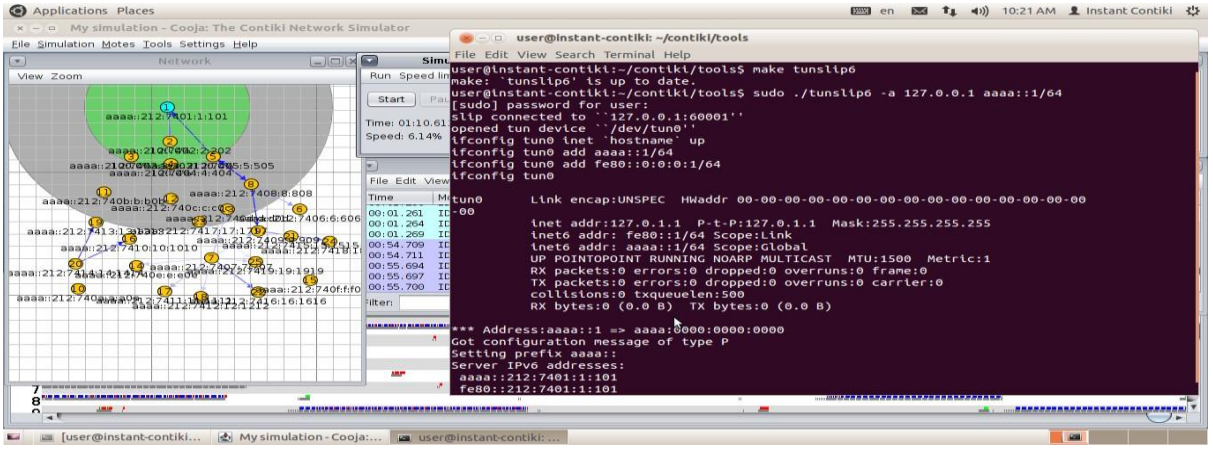

Fig 7.2: Terminal Window output

While the simulation is running, the bridge can be used to Ping motes in the network as follows, although not all are successful due to the volatility of the network:
Finally, tt is also possible to display the Border Router's routing table by opening up a web page and entering the IPv6 address of the Border Router as in the following figure. This shows routes established.

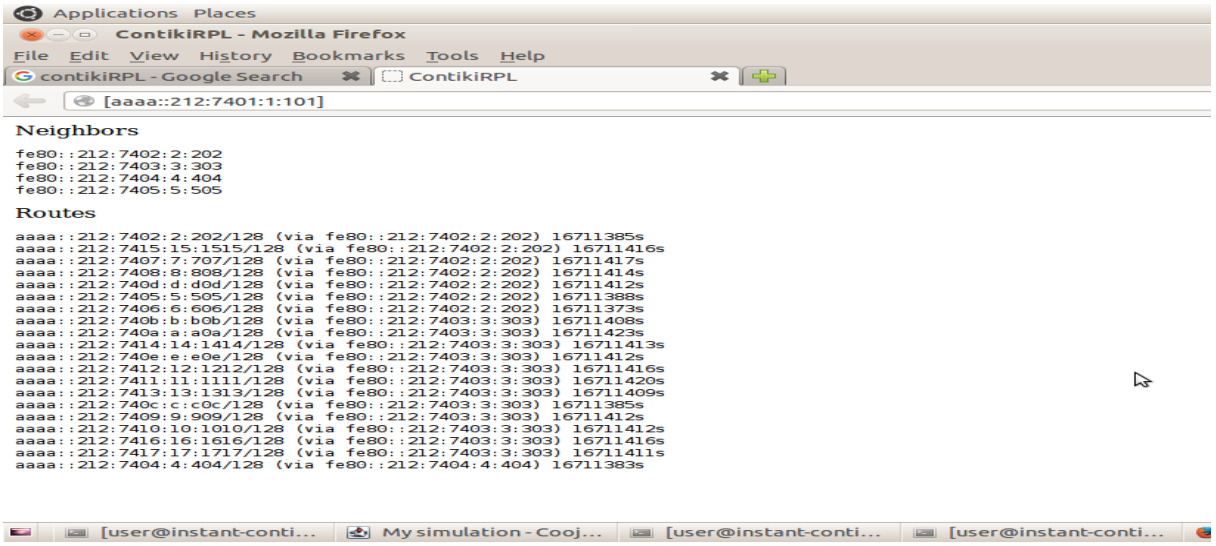

Fig 7.3: Routing Table

7.2 Approach of simulation:

Step 1: Create a NDP network between udp-server mote and udp-client mote and implement proposed attack scenario.
Step 2: Create a NDP network between udp-server mote and udp-client mote and implement proposed mitigation algorithm.
Step 3: Comparative study between step 1 and step 2.

7.2.1 Simulation of Step-1:

We used ~/**contiki-2.7/examples/ipv6/rpl-udp/udp-server.c** as a contiki process to create 2 motes and ~/**contiki-2.7/examples/ipv6/rpl-udp/udp-client.c** to create other 3 motes which got connected, shown in following figure.

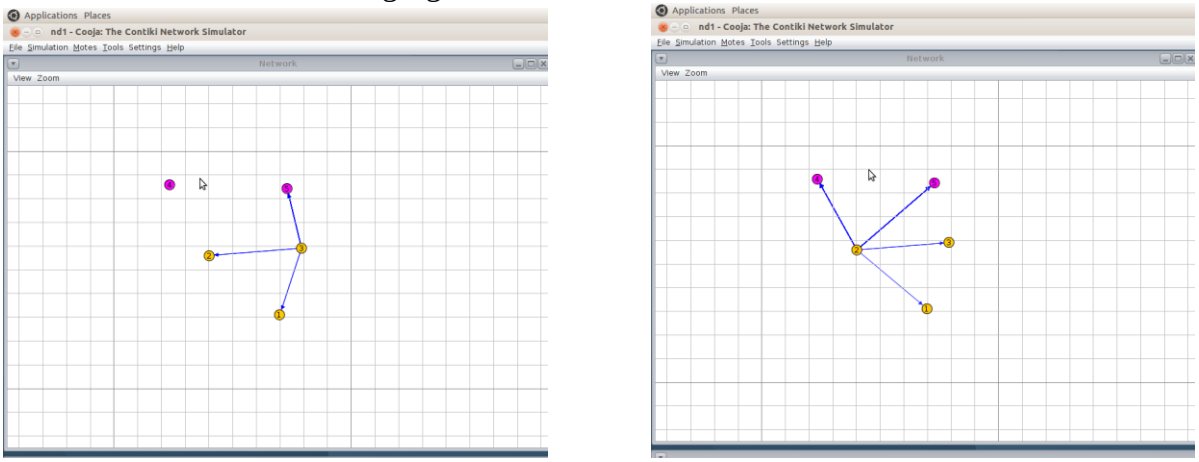

Fig 7.4: Radio traffic between motes.

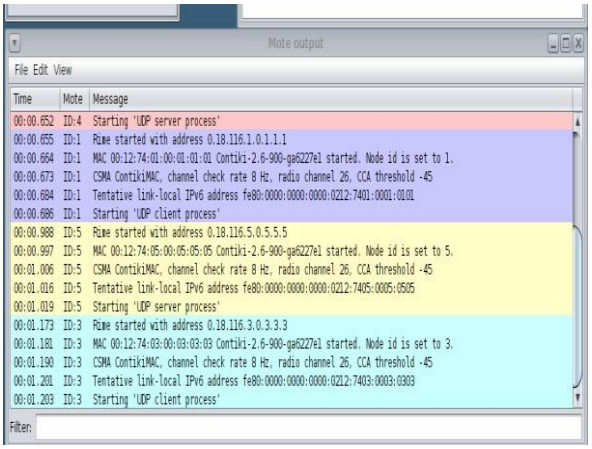

Fig 7.5: Mote Output

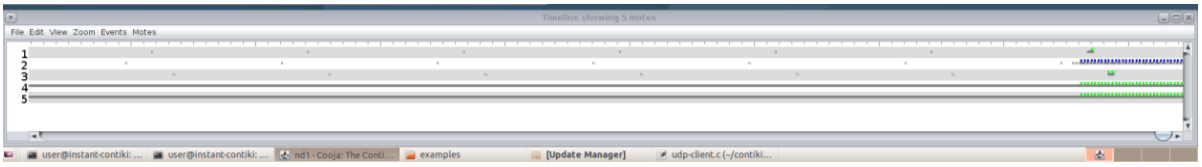

Fig 7.6: Timeline Output

8. Inference:

As IPv6 is compatible with Advance Meter Infrastructure, in the paper the problem of using ICMPv6 in NDP are discussed. We performed identification of possible effects and their respective mitigation of attacks. An attacker can perform attacks in the network by establishing connection with genuine DCU or Smart meter by spoofing message transmission. We can mitigate these type of spoofing attack by implementing proposed mitigation discussed in the paper. In the simulation phase we created a connection between server and client. client can connect with server via communicating by falsified ND messages in network environment and vice versa. The flow of messages between server and client motes is as packet format. Every packet has a unique IP address. Every corresponding neighbor has to keep track of the records of every mote. To identify if a mote claiming itself legitimate is actually legitimate or not by incorporating additional echo message and the echo reply by the neighbor motes. Hence, the mitigation can be performed to get rid of such spoofed attack.

9. Conclusion:

The transformations of power grid systems have brought significant benefits to not only utility providers but also to consumers and environment. The introductions of smart meter, wireless technologies and bidirectional communication to the power grid system have urged the need for a reliable communication for data exchange in smart metering networks. In this paper, we present the fundamental discussion of SMNs communication architecture which consist of several topologies including HAN, BAN, NAN and WAN. We have also investigated several types of attacks that occurred in SMNs as well as their security requirements. Integrating IPv6 in Smart Grid because IPv6 is compatible with the size of Smart Grid network. The large address space, auto configuration of addresses helps Smart grid to construct a large network with a unique address specified for each and every device, efficient routing, and end-to-end security. In this paper, the problems of using ICMPv6 in NDP and the possible effects of these problems on Smart Grid are considered. Five messages of NDP: Router Solicitation, Router Advertisement, Neighbor Solicitation, Neighbor Advertisement, Route Redirect are discussed with respect to Smart Grid environment. We proposed some attack scenarios based on those five NDP messages. As per the attack scenarios, respective mitigation schemes are proposed.

Reference:

SL No.	PAPER/ARTICLE
1.	C. W. Potter, A. Archambault, and K. Westrick, "Building a Smarter Smart Grid Through Better Renewable Energy Information," Proceeding of the IEEE/PES Power Systems Conference and Exposition
2.	V. K. Sood, D. Fischer, J. M. Eklund, and T. Brown, "Developing a Communication Infrastructure for The Smart Grid," Proceeding of the IEEE Electrical Power & Energy Conference (EPEC),
3.	M. M. Fouda, Z. M. Fadlullah, and N. Kato, "Assessing Attack Threat Against ZigBee-based Home Area Network for Smart Grid Communications," Proceeding of the International Conference on Computer Engineering and Systems (ICCES),
4.	H. Yi, L. Husheng, K. A. Campbell, and H. Zhu, "Defending False Data Injection Attack on Smart Grid Network Using Adaptive CUSUM Test," Proceeding of the 45th Annual Conference on Information Sciences and Systems (CISS)
5.	V. Namboodiri, V. Aravinthan, S. N. Mohapatra, B. Karimi, and W. Jewell, "Toward a Secure Wireless-Based Home Area Network for Metering in Smart Grids," IEEE Systems Journal
6.	L. Husheng, L. Lifeng, and R. C. Qiu, "A Denial-of-Service Jamming Game for Remote State Monitoring in Smart Grid," Proceeding of the 45th Annual Conference on Information Sciences and Systems (CISS)
7.	V. Aravinthan, V. Namboodiri, S. Sunku, and W. Jewell, "Wireless AMI Application and Security for Controlled Home Area Networks," Proceeding of the IEEE Power and Energy Society General Meeting
8.	J. Choi, I. Shin, J. Seo, and C. Lee, "An Efficient Message Authentication for Non-repudiation of the Smart Metering Service," Proceeding of the First ACIS/JNU International Conference on Computers, Networks, Systems and Industrial Engineering (CNSI)
9.	H. Alzaid, E. Foo, and J. G. Nieto, "Secure Data Aggregation in Wireless Sensor Network: A Survey," Proceeding of the Sixth Australasian Conference on Information Security (AISC '08)
10	W. Mesbah, "Securing Smart Electricity Meters Against Customer Attacks," in IEEE Transactions on Smart Grid, vol. 9, no. 1, pp. 101 110, Jan. 2018, doi: 10.1109/TSG.2016.2545524.
11	S. Tan, W. Song, M. Stewart, J. Yang and L. Tong, "Online Data Integrity Attacks Against Real-Time Electrical Market in Smart Grid," in IEEE Transactions on Smart Grid, vol. 9, no. 1, pp. 313-322, Jan. 2018, doi: 10.1109/TSG.2016.2550801.
12	A. F. Taha, J. Qi, J. Wang and J. H. Panchal, "Risk Mitigation for Dynamic State Estimation Against Cyber Attacks and Unknown Inputs," in IEEE Transactions on Smart Grid, vol. 9, no. 2, pp. 886-899, March 2018, doi: 10.1109/TSG.2016.2570546.

13 Y. Tan, Y. Li, Y. Cao and M. Shahidehpour, "Cyber-Attack on Overloading Multiple Lines: A Bilevel Mixed-Integer Linear Programming Model," in IEEE Transactions on Smart Grid, vol. 9, no. 2, pp. 1534-1536, March 2018, doi: 10.1109/TSG.2017.2726338.

14 M. R. Mengis and A. Tajer, "Data Injection Attacks on Electricity Markets by Limited Adversaries: Worst-Case Robustness," in IEEE Transactions on Smart Grid, vol. 9, no. 6, pp. 5710-5720, Nov. 2018, doi: 10.1109/TSG.2017.2695120.

15 R. Moghaddass and J. Wang, "A Hierarchical Framework for Smart Grid Anomaly Detection Using Large-Scale Smart Meter Data," in IEEE Transactions on Smart Grid, vol. 9, no. 6, pp. 5820-5830, Nov. 2018, doi: 10.1109/TSG.2017.2697440.

16 Thomson, Craig & Romdhani, Imed & Al-Dubai, Ahmed & Qasem, Mamoun & Ghaleb, Baraq & Wadhaj, Isam. (2016). Cooja Simulator Manual. 10.13140/RG.2.1.4274.8408.

17 Kurniawan, A. (2018). Practical Contiki-NG: Programming for Wireless Sensor Networks.

Links to Articles

1. https://www.tarlogic.com/en/blog/smart-meters-threats-and-attacks-to-prime-meters

2. https://blog.trendmicro.com/trendlabs-security-intelligence/smart-meter-attack-scenarios/

3. https://smartgridawareness.org/2017/06/28/smart-meter-cyber-attacks-clear-and-present-danger/

4. https://www.elsevier.com/about/press-releases/research-and-journals/smart-electrical-grids-more-vulnerable-to-cyber-attacks

5. https://www.ionos.com/digitalguide/server/know-how/what-is-neighborhood-discovery- protocolndp/

6. https://ukdiss.com/examples/secure-neighbor-discovery-protocol.php

7. https://www.researchgate.net/publication/250928837_Detection_of_neighbor_discovery_protocol_based_attacks_in_IPv6_network

8. https://www.hindawi.com/journals/scn/2018/1816462/

9. https://anrg.usc.edu/contiki/index.php/Build_your_own_application_in_Contiki

10. https://anrg.usc.edu/contiki/index.php/RPL_objective_function_modification_and_simulation_in_cooja