Volume 6, Issue 8, August 2016 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Distributed Denial of Service Attack Prevention Technique on Smart Grid

Anoop Jaysawal
M.Tch Student, Department of Computer Science
Bansal Institute of Engineering and Technology,
Lucknow, Uttar Pradesh, India

Mahesh Kumar Singh
Assistant Professor, Department of Computer Science
Bansal Institute of Engineering and Technology,
Lucknow, Uttar Pradesh, India

Abstract*— Smart grid (SG) is considered as next generation power grid is a 2- way connected power system framework which enables simple and sophisticated supervision and maintenance of power systems when compared to the existing power systems. It is depends upon the network protocol and the topology over which it is constructed. Like the conventional connected systems, smart grid is also have number of security threats like Eavesdropping attack, data alteration attack, identity spoofing attack, compromised key attack, replay attack and distributed denial of service (DDOS) attack. In-spite of providing good technology to all the connected systems, there are frequent security breaches like DDOS attack which will extremely influence the availability of smart grid framework. Attacks targeting the availability like DDOS attack are the interruption of access or use of information which may further disrupt the power delivery. This paper discusses the loophole of smart grid system and analyzing and performing DDOS attack on it. We suggest two techniques to protect the framework against DDOS attack that are TTL Value investigation and MAC value examination. Using TTL value with help of Cisco packet tracer, cola soft packet builder and Snort Intrusion detection tool. The uniqueness of the MAC address and IP address are matched with the help of Arpwatch tool and Snort Intrusion detection tool to detect the fake MAC and IP address pair. With these schemes it is possible to pro-actively prevent the DDOS

Keywords*— DDoS attack, Smart Grid, Smart Grid attack, Attack prevention on Smart Grid, Active Attack on smart Grid.

I. INTRODUCTION

1- Smart grid systems

Smart grid is a new method of interconnected system for conveying power from producers to consumers in effective, flexible, efficient, and in more robust manner with high power flow control, self-healing and with high data security by using the digital technology. According to the IEEE standard, Smart Grid is a mixture of power, communications and IT (Information Technology) for well advanced electric power system serving the power load. The word Smart" in Smart Grid is included due to the added benefit of communication and intelligence to the existing power grid which eases the monitoring and maintenance of system. Smart Grid are more efficient transfer of electricity, quicker restoration of power outages, reduced maintenance and operational cost, increased integration of large scale power source and security control. It also helps to make energy efficient process by creating awareness among customers about the power usage.

Some other the benefits of having Smart Grid systems are pointed out here:

- Providing new efficient services to the customers at the ease of a click
- Improving the resilience of the system against the outage
- Strengthening the system against security attacks
- Automation of routine maintenance work
- Efficient routing of power
- Enhancing the efficiency of existing system
- Access to historical data [1]
- Reduction of energy loss.

A brief overview about the components of typical Smart Grid systems. According to IEEE smart grid, the entire smart grid system includes various components.

- Bulk generator
- Transmission
- Distribution
- Customer
- Service Provider
- Operations and Markets

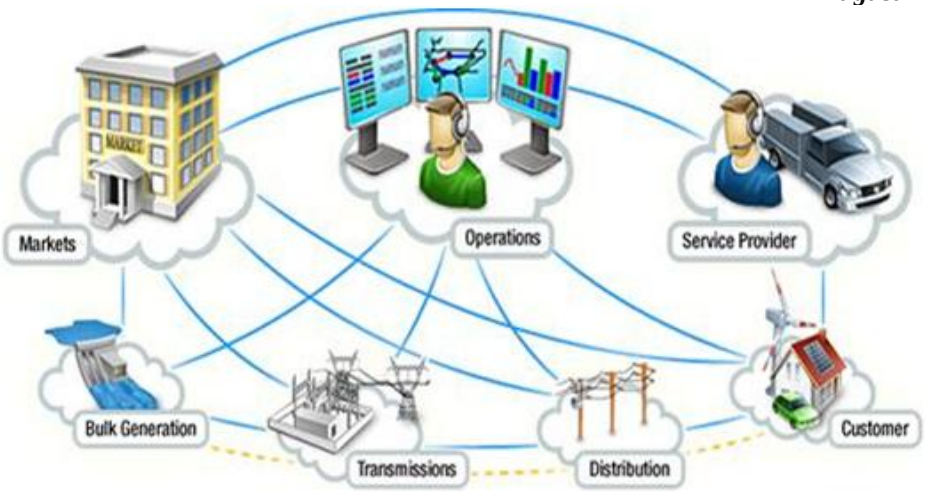

Figure-1: Conceptual smart grid model

II. LITERATURE REVIEW

Smart Grid systems have the goal to enhance performance of the existing power system by providing high availability, enhanced security, authenticated access control, easy maintenance and reduced cost [1]. To ensure the availability of critical real time power system, we must defend the system against all kind of security attacks. Security threats over the Smart Grid systems are applicable to all the industrial systems [3]. Some of such threats are

- Denial of Service attacks [2]
- Eavesdropping [3]
- Man-in-the-middle attack [4]
- Identify Spoofing [4]
- Intrusion attack [4]
- Compromised key attack [2]

III. PROBLEM STATEMENT

In our proposed work we pro-actively scan every incoming packet and mitigate the DDOS attack using the Time To Live (TTL) value [6] and Media access control address (MAC) value analysis. Further we associate multiple routers to produce a Marking on each incoming packet to the victim using Marking based Detection And Filtering (MDADF) mechanism [5].

1- Security objectives

The reliability of a Smart Grid System is depended upon the control and communication systems over which it was developed. Smart Grid needs high powered network connectivity to support new features and better network performance is based upon its protocols which are open to the global community.

2- Security threats in smart grid

Security threats in Smart Grid systems are classified based upon the selfish users and malicious users. Selfish clients are those who are trying to get more network resources than it was allotted to them by tampering standards. Malicious users are the one who have no motto to get advantage for their benefit but still they aim to illegally fetch, update or delete information in the network.

2.1 Eavesdropping

In Eavesdropping attack, the information packets are watched and once the attacker has the right to gain entrance to metering gadget of keen network, he is equipped for sniffing the whole information over the system.

2.2 Data alteration

When the attacker has gained control over the grid, he can change the original data as needed and send back the new version of data to the smart grid systems.

2.3 Identity spoofing attack

In Smart Grid system each metering interface is assigned a unique IP address which is used reveal their identity. Once the attacker gains information about the system by eavesdropping, they can select any IP address from the network by IP spoofing and can send false information.

2.4 Compromised key attack

Compromised key attack is often possible in metering network of smart grid where the system uses identical key for encryption and decryption of the metering data.

2.5 Replay attack

Replay attacks can be launched when an attacker gain access to smart meters and inject control signals to the system. The attacker first needs to record data transmitted from customer to smart meters and analyse them to achieve customer's characteristics of power usage. After analysing, the attacker may inject the data to grid system. Two common purpose of this attack is to steal energy and other is to cause physical damage to the system [7].

IV. ATTACKS OVER THE SMART GRID FRAMEWORK

Smart Grid framework is divided into four components and classified based upon the common attack possible as: power generator, service provider, Smart Grid system and customer. Power generator is responsible for generation and distribution of power to the service provider. Service provider does the monitoring operation over the entire framework for the purpose of billing and routing. Smart Grid system component does the job of load balancing, encrypting and decrypting of user billing data between each customer. Further it takes care of authentication and authorization over the framework. The encrypted data which is received from different customers are decrypted and sent back to the service provider. Different types of attack that are commonly found over the above said smart grid Systems framework is Eavesdropping, Denial of Service attack, Data alteration, Identity Spoofing, Compromised Key attack and Replay attack. Framework depicting the possible attack over different components of Smart Grid network is shown below in the Figure-

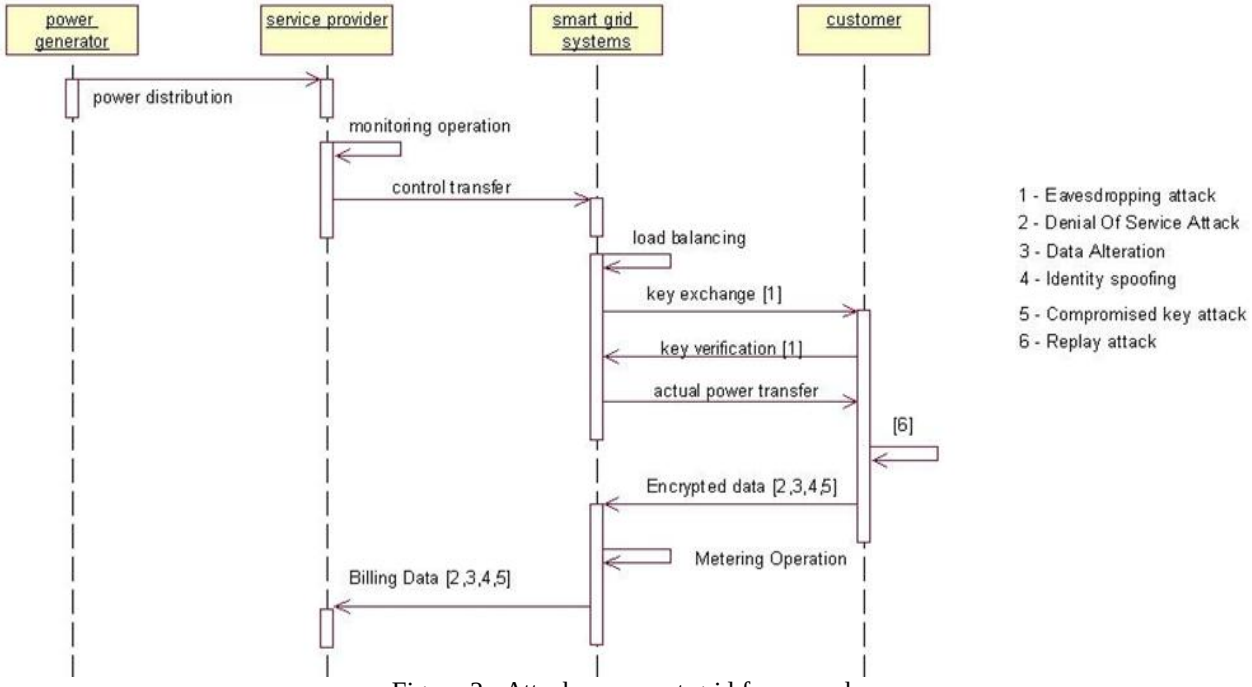

Figure-2 : Attacks on smart grid framework

1- Distributed denial of service attack on Smart Grid

Primary goal of Smart Grid System is availability. Denial of Service attack can severely impact the availability of smart grid system by degrading the communication performance. As the global network increases in size, the attack volume also increases giving birth to the raise of Distributed Denial of Service Attack.

Internet was assembled without much stress about the security and thus painful clients misuse each part of it. The incident which has triggered the interest of many engineers in past few decades is the DDOS attack whose whole purpose is to cut down the availability of services provided over the network to its authentic clients. This is carried out by discovering vulnerabilities in applications, protocols or by depleting the network and computational asset or memory of victimized person. In Distributed Denial of Service, the attacker first takes control of huge number of systems which are traditionally called zombies and then utilize them to send large volume of packets in parallel which are valid most of the time. The attackers in DDOS attack usually modify their identities to hide their presence and make it difficult to differentiate between legitimate and illegitimate traffic packets. This idea of changing the identity with the help of IP address is called as IP Address spoofing.

2- DDOS defence mechanism

DDOS defence mechanism is classified into three categories [5] as given below

- ✓ Preventive Defence Mechanism
- ✓ Source Tracking Mechanism
- ✓ Reactive Solutions Mechanism

2.1- Preventive defence mechanism

Preventive Defence Mechanism points at enhancing the resistance level of frame-work via completing preventive measures even before the victimized person was affected. Proactive server roaming scheme [8] follows preventive

defence mechanism where the system has several number of distributed servers and the area of server changes among them using secure roaming algorithm..

2.2- Source tracking

Source tracking method tries to trace down the source of attacks so that the attacker can be eliminated from the network. The existing solution falls under four groups [5]:

- ✓ Packet Marking
- ✓ Message Trace-back
- ✓ Logging
- ✓ Traffic observation

In Packet marking Scheme, path information of packets are encoded inside each packets as they are travelling through web. This idea is first implemented by Savage et al. [9] called as probabilistic

In Message traceback scheme, routers produces ICMP traceback messages for a percentage of the approaching information and send it with them. We can find the creativity of packets by preparing their TTL refinement.

In Logging scheme, data about packets are logged at routers. The route to the attacker could be perceived by the router exchanging data with each other.

In Traffic-observation Scheme, attack way is dictated by watching the rate of progress of movement on victimized person. Throughout attack stage, assaulter sends tremendous number of packets to the victimized person. Via completing the connection test constantly, the attacker might be discovered.

V. PREVENTION METHODOLOGY

General flow structure

We use twp methods to detect and prevent DDOS attack the methods are TTL Value analysis and MAC value analysis. If the packets which are found positive in any of the methods then it have to be reject to enter the victim system. Here MAC value analysis works only when the attack packets are originated within the network. Similarly TTL value analysis works only when the packets are originated outside the network since packets which are originated within the network has no change in TTL Value.

1- TTL value analysis

In Internet, every IP packet goes across not more than 30 routers before reaching its destination. But some IP packets have abnormal TTL values which are decreased by more than 30 hops. We assume that IP packets with strange TTL values in IP headers as malicious packets and hence it is discarded. These packets are likely to be generated by special tools. Every computer x the TTL value when it sends the packet based upon the operating system and the protocol which sends the packet. It is possible to estimate the total number of routers between source and destination using the TTL values. TTL Values of popular operating system were given below in the Table 1.

Table -1: TTL values of different operating systems

Operating system	Protocol	TTL Value
Linux kernel 2.2.14	ICMP	255
Windows Server 2008	ICMP, TCP, UDP	128
Windows 7	ICMP, TCP, UDP	128
Windows XP	ICMP, TCP, UDP	128
Free BSD 5	ICMP	64
MACOS 10.5.6	ICMP, TCP, UDP	64
Solaris 2.8	TCP	64
Sun OS 5.7	ICMP ,TCP	255

Tools used to implement TTL value analysis are,

- ➢ Cisco packet tracer, for simulating real time network depicting the smart grid
- ➢ Cola soft packet builder, to create a packet with fake TTL value
- ➢ Snort, an IDS tool to detect and isolate the packets with fake TTL value which falls in the range of abnormal TTL value

TTL values of normal and abnormal IP packets based upon the average hop count is given below:

Normal TTL value: if 30< ttl <= 64 : 98 < ttl <= 128 : 225 < ttl <= 255

Abnormal TTL value: if 1< ttl <= 30 : 64 < ttl <= 98 : 128 < ttl <= 2

Cisco Packet tracer is used to simulate a network topology consisting of six clients connected to two servers via three routers and two switch. Each node ping's the node present in other network to test the decremented TTL value. Below Figure-3 shows the Network created using Cisco packet tracer to analyse the TTL values.

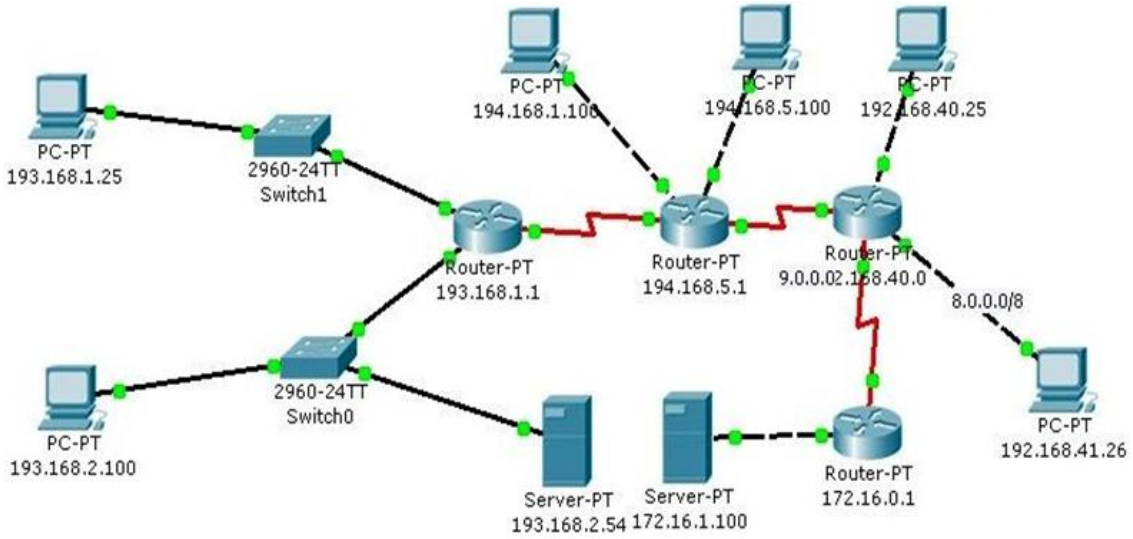

Figure-3: Network used for TTL value analysis

2- MAC value analysis

Many IP addresses attached to the same MAC would mean that many IP's coming through the same interface and hence those packets can be rejected with the help of table maintaining the list of source with its IP Address and MAC address. In most of the modern attacks, single attacker creates random source flooding attack and hence it is easy to distinguish the source with fake MAC address. Hping3 tool is used to create Random source flooding attack which creates thousands of Packets in few minutes. It produces a real time DDOS attack with same MAC address. But MAC address does not appear in the IP packet once it crosses the network on which originates. Hence MAC value analysis is useful only when the fake IP packet rises within the network. ARPwatch tool is used to analyze the list of newly added IP and MAC pairs in the ARP table. ARPwatch tool produces an alert when there is a new entry of new IP address and MAC value pairs into the ARP table which can be verified with the help of Wireshark tool also. Figure 4 shows the result of arpwatch tool depicting the occurrence of changed MAC and IP pair.

Tools used: Hping, ARPWatch, Snort, Wireshark

- Hping tool is used to create an random source flooding attack . **hping** is a free packet generator and analyzer for the TCP/IP protocol distributed by Salvatore Sanfilippo (also known as Antirez). It is one of tools for security auditing and testing of firewalls and networks, and was used to exploit the idle scan scanning technique (also invented by the hping author), and now implemented in the Nmap Security Scanner..
- **Arpwatch** is an open source computer software program that helps you to monitor **Ethernet** traffic activity (like **Changing IP** and **MAC Addresses**) on your network and maintains a database of ethernet/ip address pairings. It produces a log of noticed pairing of IP and MAC addresses information along with a timestamps, so you can carefully watch when the pairing activity appeared on the network. It also has the option to send reports via email to an network administrator when a pairing added or changed.
- This tool is specially useful for **Network administrators** to keep a watch on **ARP activity** to detect **ARP spoofing** or unexpected **IP/MAC** addresses modifications.
- Ethernet traffic activity like Changing IP and MAC address address is maintained in the database and dropped using Snort tool
- Wireshark is used to cross verify the presence of fake IP and MAC entry.Wireshark is software that "understands" the structure (encapsulation) of different networking protocols. It can parse and display the fields, along with their meanings as specified by different networking protocols. Wireshark uses pcap to capture packets, so it can only capture packets on the types of networks that pcap supports. Some features are as follows:
- Data can be captured "from the wire" from a live network connection or read from a file of already-captured packets.
- Live data can be read from a number of types of network, including Ethernet, IEEE 802.11, PPP, and loopback.
- VoIP calls in the captured traffic can be detected. If encoded in a compatible encoding, the media flow can even be played.
- Raw USB traffic can be captured.
- Wireless connections can also be filtered as long as they transverse the monitored Ethernet.
- Various settings, timers, and filters can be set that ensure only triggered traffic appear.

Arpwatch Added new station with Mac address Entry.

```
Apr 15 12:45:17 tecmint arpwatch: new station 172.16.16.64 d0:67:e5:c:9:67
Apr 15 12:45:19 tecmint arpwatch: new station 172.16.25.86 0:d0:b7:23:72:45
Apr 15 12:45:19 tecmint arpwatch: new station 172.16.25.86 0:d0:b7:23:72:45
Apr 15 12:45:19 tecmint arpwatch: new station 172.16.25.86 0:d0:b7:23:72:45
Apr 15 12:45:19 tecmint arpwatch: new station 172.16.25.86 0:d0:b7:23:72:45
```

The above output displays new workstation. If any changes are made, you will get following output.

```
Apr 15 12:45:17 tecmint arpwatch: changed station 172.16.16.64 0:f0:b8:26:82:56 (d0:67:e5:c:9:67)
Apr 15 12:45:19 tecmint arpwatch: changed station 172.16.25.86 0:f0:b8:26:82:56 (0:d0:b7:23:72:45
Apr 15 12:45:19 tecmint arpwatch: changed station 172.16.25.86 0:f0:b8:26:82:56 (0:d0:b7:23:72:45
Apr 15 12:45:19 tecmint arpwatch: changed station 172.16.25.86 0:f0:b8:26:82:56 (0:d0:b7:23:72:45
Apr 15 12:45:19 tecmint arpwatch: changed station 172.16.25.86 0:f0:b8:26:82:56 (0:d0:b7:23:72:45
```

Here is an example of an email report, when a **IP** changing his **MAC** address.

```
        hostname: centos
      ip address: 172.16.16.25
       interface: eth0
ethernet address: 00:24:1d:76:e4:1d
 ethernet vendor: GIGA-BYTE TECHNOLOGY CO.,LTD.
       timestamp: Monday, April 15, 2012 15:32:29
```

Here is an example of an email report, when a **IP** changing his **MAC** address.

```
            hostname: centos
          ip address: 172.16.16.25
           interface: eth0
    ethernet address: 00:56:1d:36:e6:fd
     ethernet vendor: GIGA-BYTE TECHNOLOGY CO.,LTD.
old ethernet address: 00:24:1d:76:e4:1d
           timestamp: Monday, April 15, 2012 15:43:45
  previous timestamp: Monday, April 15, 2012 15:32:29
               delta: 9 minutes
```

In above, it records, **Hostname**, **IP address**, **MAC address**, **Vendor name** and **timestamps**. For more information, see the arpwatch man page by hitting '**man arpwatch**' on the terminal.

Figure-4: MAC value analysis

VI. RESULT AND CONCLUSION

From the above analysis it is clear that we can determine and prevent the attacks by Using TTL value with help of Cisco packet tracer, cola soft packet builder and Snort Intrusion detection tool. The uniqueness of the MAC address and IP address are matched with the help of Arpwatch tool and Snort Intrusion detection tool to detect the fake MAC and IP address pair. With these schemes it is possible to pro-actively prevent the DDOS.

REFERENCES

[1] Gianni Fenu, Marco Nitti, and Pier Luigi Pau. A complex network approach for a regional power grid analysis. In Digital Information Processing and Communications (ICDIPC), 2012 Second International Conference on, pages 45{50. IEEE, 2012.

[2] Mini S Thomas, Ikbal Ali, and Nitin Gupta. A secure way of exchanging the secret keys in advanced metering infrastructure. In Power System Technology (POWERCON), 2012 IEEE International Conference on, pages 1{7. IEEE, 2012.

[3] Jingcheng Gao, Yang Xiao, Jing Liu, Wei Liang, and CL Chen. A survey of communication/networking in smart grids. Future Generation Computer Systems, 28(2):391{404, 2012.

[4] T. Littler S. Sezer Eul Gyul Im Z.Q. Yao B Pranggono H F Wang Y. Yang, K. McLaughlin. Man-in-the-middle test bed investigating cyber-security vulnerabilities in smart grid in scada systems, sustainable power generation and supply, 2012.

[5] Yao Chen, Shantanu Das, Pulak Dhar, Abdulmotaleb El-Saddik, and Amiya Nayak. Detecting and preventing ip-spoofed distributed dos attacks. IJ Net-work Security, 7(1):69{80, 2008.

[6] Ryo Yamada and Shegeki Goto. Using abnormal TTL values to detect malicious ip packets. Proceedings of the Asia-Pacific Advanced Network, 34:27{34, 2013.

[7] Jong-Ho Lee Thien-Toan Tran, Oh-Soon Shini. Detection of replay attacks in smart grid systems. CHECK IN INTERNET, 34:27{34, 2013

[8] R. Melhem D.Mosse S.M. Khattab, C. Sangpachatanaruk and T. Znati. Proactive server roaming for mitigating denial-of-service attacks. pages 500{ 504. Elsevier, 2003.

[9] Stefan Savage, David Wetherall, Anna Karlin, and Tom Anderson. Practical network support for ip traceback. ACM SIGCOMM Computer Communication Review, 30(4):29.

