International Journal of Applied Engineering Research ISSN 0973-4562 Volume 12, Number 14 (2017) pp. 4443-4447
© Research India Publications. http://www.ripublication.com

Impact of Denial of Service (DoS) attack in Smart Distribution Grid Communication Network

Premkumar S [1] and Saminadan V[2]

[1]*Department of Electronics and Communication, Pondicherry Engineering College, Pondicherry, India.*

[1]*Orcid Id: 0000-0002-2864-4209*

[2]*Department of Electronics and Communication, Pondicherry Engineering College, Pondicherry, India.*

[2]*Orcid: 0000-0001-8426-238X*

Abstract

Smart grid is embedded into open communication infrastructures to support vast amounts of data exchange, which makes smart grids vulnerable to cyber-attacks. Smart grid distribution network is a highly complex communication network which shares information about status of the various IEDs (Intelligent Electronic Devices). However, the numerous IEDs being connected through Smart Grid Communication Networks open opportunities for attackers to interfere with communications and trade off utilities resources or take clients private data. Synchrophasors enable synchronized evaluation of phasor data obtained from the PMUs deployed throughout the grid. The Phasor Measurement Units (PMUs) are becoming increasingly widespread instruments in monitoring the performance of power systems due to dynamic loads and higher penetration of Distributed Energy Resources (DER), which changes phase angle values, important for real-time control. PMU devices connected to the communication network are vulnerable to cyber-attacks. In this work, we had analyzed the impact of Denial-of-Service (DoS) attacks when PMU data are transferred over Smart Grid Communication Networks. The Dos attack in smart grid communication network is modeled using a combination of GNS3, openPDC, LOIC (Low Orbit Ion Cannon), Wireshark for the first in the literature.

Keywords: Phasor Measurement Units (PMUs), Denial-of-Service (DoS), Distributed Energy Resources (DER).

INTRODUCTION

In recent years, blackouts around the world stress the importance of real-time situational awareness to improve the grids' stability. Therefore, future smart grid will use advanced two-way communication and intelligent computation technologies to provide better situational awareness to utilities. While these technologies facilitate the aggregation and communication of both system-wide information and local measurement data in selected locations, they introduce new cyber-physical security challenges for smart grids to operate safely and reliably [1].Wide area monitoring systems require installation of PMUs and PDCs (Phasor Data Concentrators) all over the grid for real time monitoring, situational awareness, and continual availability of power to consumers. PMUs and PDCs are networked appliances which use routable protocols. The IEEE C37.118 is the standard established for synchrophasor data transfer which can be used as a guideline for PDC communication. The reporting frequency rates defined by the IEEE C37.118 standard are 10, 25 and 50 Hz for a 50 Hz system and 10, 12, 15, 20, 30 and 60 Hz for a 60 Hz system [2]. The packet travels through routers and switches present in the communication networks adds delay to the packets. The PDC has a latency associated with processing incoming PMU data which is defined in IEEE C37.118 standard.

Securing the power grid and transforming it into smart grid has attracted more attentions from both the academia and industry communities. In [3], the authors discussed about the risk of replacing proprietary network by open communication standards in SCADA systems. A class of false data attacks on state estimation in power SCADA system, bypassing the bad data detection, were firstly presented in [4]. Morris et al [5], analysed DoS attacks such as Internet Control Message Protocol (ICMP) attacks, transport layer attacks in power grid networks with PMUs and PDCs. DoS traffic can also be mitigated using distributed or redundant infrastructure. Felix et al [6] discussed about existing DDOS countermeasures. Countermeasures include filtering routers, disabling IP broadcasts, applying security patches, disabling unused ports, and performing intrusion detection. Shichao et al investigated the effects of Denial-of-Service (DoS) attacks on load frequency control (LFC) of smart grids[7]. In [8], the authors investigated the impact of a cyber-attack on the Automatic

Generation Control (AGC) in a power system network.

Although these works are very promising, they considered only static state estimation in power systems without noticing the impacts of attacks on dynamics of power systems in smart grid communication network. They performed the analysis of the impacts of cyber-attacks on control centers in power system, by using reachability methods. However, they had considered the scenarios in which the control center is attacked by adversaries. In fact, it is harder to attack the control center than to compromise the communication channels in the sensing loop of a power system. Preventing cyber attack is very essential to provide reliable monitoring for proper operation of grid.

PMU based monitoring and control technology becomes the target of attacks against bulk electric power systems. Threats against PMUs include denial of service attacks, attempts to inject malicious device control commands, attempts to hijack device access credentials and attempts to place a man-in-the-middle between devices. This paper outlines cybersecurity testing performed on PMU and substation PDC.

We consider DoS attacks on the communication channels in the sensing loop (measurements telemetered in remote terminal units (RTUs) are sent to control center) of power systems. We show that adversaries may make power systems unstable by properly designing DoS attack sequences. To launch a DoS attack on the communication channels, the adversaries can jam the communication channels, attack networking protocols, and flood the network traffic etc. If attacked, measurement packets sent from sensors through this channel will be lost. In addition, cyber-security issues may also result in a breach of national security and unpredicted economic losses in the electricity market. The existence of DoS attacks that are able to destabilize power systems is proved by our simulation. Case studies are conducted to evaluate the effects of DoS attacks on the dynamics of a power system.

DENIAL OF SERIVECE ATTACK (DOS)

DoS is an attack on a node or network that reduces accessibility of system resources to its legal users. In a DoS attack, the attackers flood a victim system with unwanted service requests or traffic there by exhausting bandwidth, router processing capacity or network resources. DoS attack leads to unavailability of particular node and slow network performance.

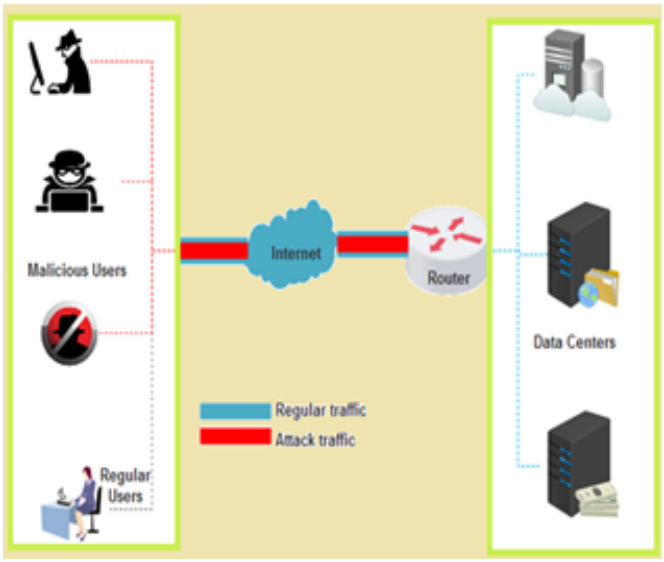

Figure 1: Denial of service (DoS) attack

When an intruder makes the server and resources unavailable to handle legitimate user request and denies valid access of the server, the attack is said to be Denial-of-service attack i.e., when valid user cannot get access to server because of more malicious requests as shown in figure1. Denial of service attacks are of many types. Certain DoS attack completely neglect legitimate users and in others generate unusual packets to confuse the TCP/IP stack of the machine that is trying to reconstruct the packet. We can exemplify this type of attack on a smart grid network infrastructure to halt a substation server from servicing its legal clients. In DoS basically there are three types of attacks – Ping of Death, TCP SYN Flood, and the Distributed DoS. The most common type of DoS attack is an Internet Control Message Protocol (ICMP) Smurf attack. ICMP echo packets are sent by the attacker with the victims IP address. All the hosts accept the ICMP echo packet and reply to the victim computer [9].

The remainder of this paper is organized as follows. In section III the various tools that has been used in the simulation has been discussed. Section IV describes the simulation setup and the existence of DoS attack that make the power system unstable is proved in section V. Finally, conclusion and future work are summarized in section VI.

SIMULATION TOOLS

There are various simulators that are available to provide virtualized networks such as: GNS3 (Graphical Network Simulator 3), NS2 (Network Simulator version2), NS3 (Network Simulator version3), M5 Simulator, OPNET (Optimized Network Engineering Tools), OMNET++ (Optical Micro-Networks Plus), where some of them are widely acknowledged in academia researches and some of them have commercial use. The GNS3 interface is straightforward and

relatively simple to use,. GNS3 (Graphical Network Simulator 3), is an open-source graphical network simulator written in python that allows emulation of complex networks. It is freely available online under the GNU General Public License (GPL License). In the proposed work using GNS3, openPDC, LOIC and Wireshark the impact of DoS attack has been analysed. The main contribution of th work is the modeling and simulation of DoS attack detection in smart grid communication network for the first time in literature to the best of our knowledge.

The openPDC is an application that can be used to transfer messages between the openPDC service and a client machine. Using openPDC real-time data are generated and transmitted through the smart grid grid communication network designed using GNS3. The openPDC is a complete set of applications for processing streaming time-series data in real-time. The name stands for "open source phasor data concentrator" and was originally designed for the concentration and management of real-time streaming synchrophasors. There are number of standard phasor protocols inbuilt in openPDC which can be used to send and receive data from devices, supported by IEEE C37.118 protocol. The LOIC tool is used to attack the target source in this simulation[10]. LOIC performs a DoS attack (or when used by multiple individuals, a DDoS attack) on a target site by flooding the server with TCP or UDP packets with the intention of disrupting the service of a particular host. The smart distribution grid communication network with DoS attacks is modeled using GNS3, VMware and open PDC [11], [12].

SCENARIO FORMATION

Figure 2 shows the smart distribution grid communication network diagram which we considered. In this network we have chosen Host 3 (192.16.10.50) as source and Host 4 (192.16.10.54) as destination which are connected to Router R3 and R9. The routers R3 and R9 come under the Customer Edge networks.

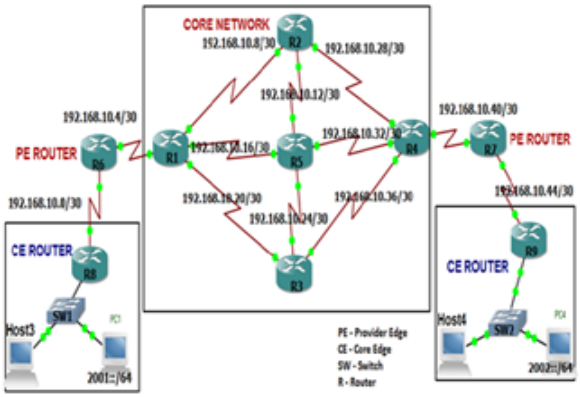

Figure 2: Proposed Smart Grid Communication Network Using GNS3

Here, Host 3 is connected to the local PC and the Host 4 is connected to virtual machine which is created by VMWare. All other routers are coming under ISP Router. After creating the network, addresses were assigned. Here we choose logical addressing scheme which is IP addressing.

Here, we use both IPv4 and IPv6 addressing. which is sub netted by using VLSM to reduce the minimum wastage of IP's. The core network of the proposed architecture uses IPv4 and from customer edge to the end nodes we use IPv6 since more number of nodes can be added with IPv6 addressing. IPV6 packet will not travel through IPV4 channels.

If we want to make communication between IPv and IPv6 a tunnel between IPV4 and IPV6 has to be created. Here we use IPV6 to IPV4 tunnel in both R3 and R9. Figure 3 shows how to integrate our PC to GNS3 network. Similarly Host 4 present in the virtual machine will be connected to the GNS3 network using VMnet interface.

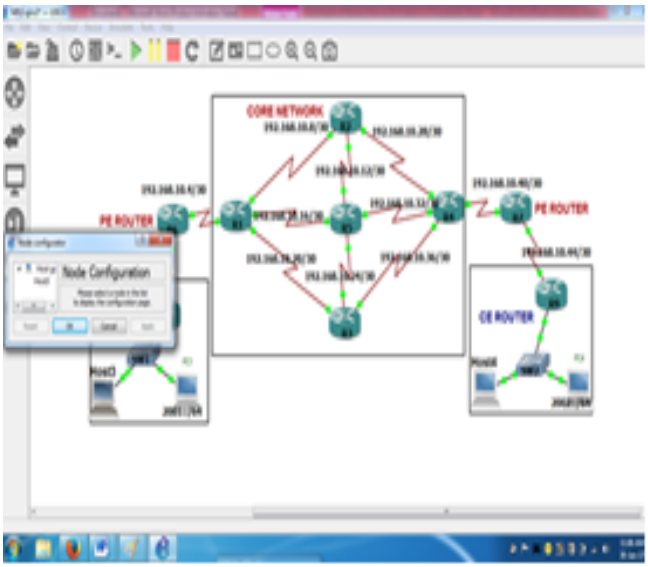

Figure 3: Integrating PC to GNS3 network

This link creates communication between GNS3 network and Virtual PC which is created by VMWare. Figure 4 shows the communication between the source node to destination node through GNS3 network. To check the communication between the desired nodes we use ping command, which works based on ICMP protocol. Based on echo request and echo reply between the source and destination we can find the communication status.

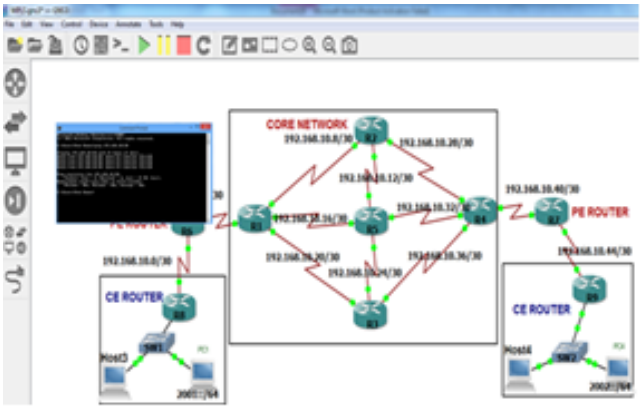

Figure 4: Ping status between Host3 and Host 4

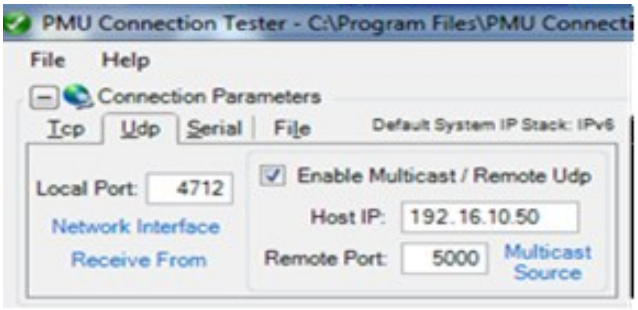

Figure 5: Connection parameters

Using open PDC the PMU data generated from Host 3 is sent through the network to Host 4. The Connection Parameters screen section as shown in figure 5 displays the details concerning the connection between the PMU Connection Tester and the tested device. The details differ depending upon the communication protocol selected.

Local Port: The port number through which the PMU Connection Tester is receiving data from the tested device.

Enable Multicast / Remote Udp: If the tested device listens on UDP, select this check box which makes the following screen elements available.

Host IP: The internet address of the device being tested.

SIMULATION ANALYSIS

Our main concern and purpose of this simulation is to show the impact of DoS attack in the proposed smart grid distribution network. The data packets sent from Host 3 to Host 4 can be captured using wireshark. Figure 6 shows wireshark starts capturing the packets from the selected interfaces of customer edge router.

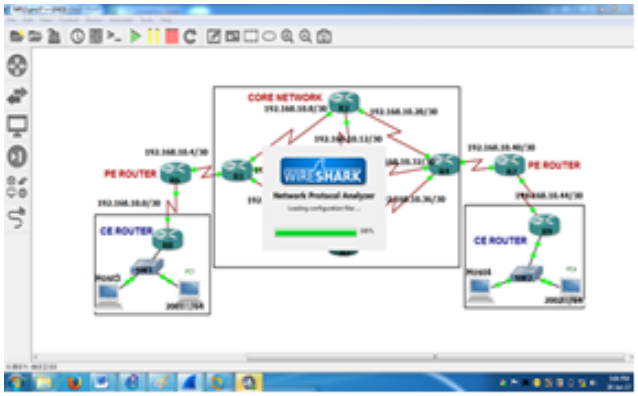

Figure 6: Wireshark capturing data packets sent from Host 3 to Host 4

Figure 7 shows the captured PMU data which is sent by Host 3 before DoS attack.

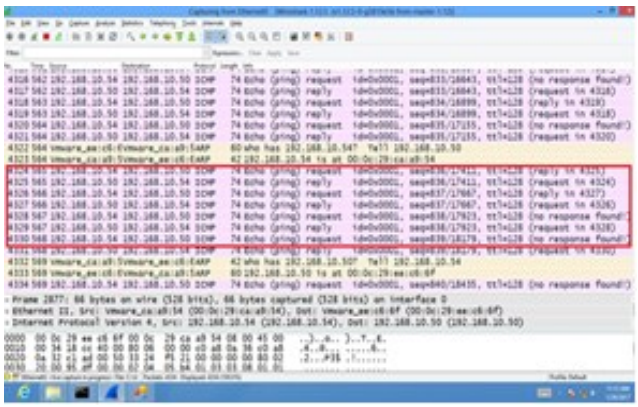

Figure 7: Data packets sent from Host 3

By specifying the target IP in the LOIC tool the packets start flooding and start attacking the destination as shown in figure 8.

Figure 8: Attacked target IP address

From figure 9 we can observe the flow of TCP packets and its replies through the network. Here we can notice the PMU data(which is marked in black and the flooded data marked

with red are) transmitted from the source are arriving at the destination with huge latencies due to the flooding of data. Continuous flow of same packets to the destination leads to unavailability of services. Since the PDC has a very low latency associated with processing incoming PMU data the unavailability of services at Host 9 leads to instability in the power grid.

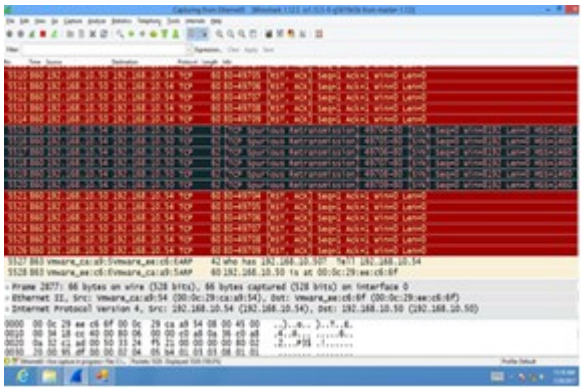

Figure 9: PMU data in black and Flooded data in red

CONCLUSION

In this work, we considered the proposed system architecture of WAMS in smart gird. The impact of DoS attack in a WAMS communication network has been studied by the co-simulation of GNS3, PMU connection tester, Wire shark and LOIC tools. The simulation result clearly shows the vulnerability of DoS attack in power system monitoring. In our future work we focus on how to mitigate and prevent DoS attack by applying mechanisms such as intrusion detection and prevention systems by considering large number of nodes.

REFERENCES

[1] W.Wang and Z.Lu, "Cyber security in the Smart Grid: Survey and challenges," Computer Networks, vol.57, no.5, pp.1344-1371, April 2013.

[2] IEEE Standard for Synchrophasors for Power Systems, in IEEE Std C37.118-2005 (Revision of IEEE Std 1344-1995), 2006.

[3] E.Byres and J.Lowe (2004, October). "The myths and facts behind cyber security risks for industrial control systems," In Proceedings of the VDE Kongress (Vol. 116, pp. 213-218).

[4] Y.Liu, P. Ning, and M. K. Reiter "False data injection attacks against state estimation in electric power grids," ACM Transactions on Information and System Security (TISSEC) vol.14, no.1,p.13, 2011.

[5] S.Pan, T.H. Morris, U. Adhikari, and V. Madani, (2013, January). "Causal event graphs cyber-physical system intrusion detection system," In Proceedings of the Eighth Annual Cyber Security and Information Intelligence Research Workshop (p. 40). ACM.

[6] F. Lau, S.H. Rubin, M.H. Smith, L. Trajković, "Distributed denial of service attacks, in: Systems, Man, and Cybernetics," 2000 IEEE International Conference on, 2000, pp.

[7] S.Liu, X.P. Liu andA. El. Saddik, " Denial-of-Service (DoS) attacks on load frequency control in smart grids. In Innovative Smart Grid Technologies (ISGT)," 2013 February IEEE pp. 1-6. IEEE.

[8] P.M .Esfahani, M. Vrakopoulou, K.Margellos, J.Lygeros and G.Andersson, "Cyber attack in a two-area power system: Impact identification using reachability," In American Control Conference (ACC), 2010, pp. 962-967. IEEE, 2010.

[9] S.T.Zargar, J. Joshi, J and D. Tipper, "A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks, IEEE communications surveys & tutorials,vol. 15, no. 4,pp. 2046-2069.

[10] http://www.loic.org.nz/howtouseloic.htm

[11] https://docs.gns3.com

[12] https://openpdc.codeplex.com