International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 04 Issue: 05 | May -2017 www.irjet.net p-ISSN: 2395-0072

An analysis and review against Denial of service attack for smart grid system

Anamika Chourasia [1], Ankit Chourasia[2]

[1] *Assistant Professor, Government polytechnic college, Khurai, MP, India*
[2] *Assistant Professor, SKNSITS, Lonavala, Maharashtra, India*

Abstract - *The global demand for the electrical energy has increased manifold since its invention with the development of modern society. The extensive interconnection between the grids to meet increasing demand & to improve the efficiency has resulted into complex structure of power system and its highly dynamic & unpredictable operation. The dependency on the depleting nonrenewable resources of the energy for generating electricity have raised the concern for security & reliability of supply in future. The existing system suffers from poor power load, security and infrastructure issues. The author provides a survey and analysis on DoS attack and their effects on smart grid system*

***Key Words*: power system, renewable energy, energy efficiency.**

1. INTRODUCTION

In past decades, the improvement of energy networks has not been keeping pace with the modern and social advertisement advancements that definitely increment the request on power supply. For instance, measurements [1] demonstrated that from 1950 to 2008, vitality generation and utilization in the US in- wrinkle roughly two and three times, individually. Smart grid advances bring the chance to improve existing force matrix foundations (i.e., electrical cables, electrical substations, organize control rooms) by enhancing constant appraisal of framework conditions. New computerized gear and gadgets can be deliberately conveyed to complement existing hardware. Utilizing a mix of concentrated IT and conveyed insight inside basic framework control hubs—extending from thermal and sustainable plant controls to network and distribution utility servers to urban communities, business and modern frameworks, and homes—a smart grid can bring phenomenal productivity and stability to the vitality framework. In specific, the general population/business administrations, industry and neighborhoods are the most requesting zones for electricity in the US in 2008.

The smart grid is more than a foundation for more brilliant power era, circulation, and utilization. It will positively affect our current society, with advantages for both individuals and the aggregate populace. A standout amongst the most critical, complex, and astute system we have is the "control framework". This framework comprises of circuits, wires, towers, transformers, sensors, and links interlinked to furnish us with continuous power supply. This framework is predominantly a mechanical framework and has next to no hardware related with it like sensors and correspondence. Be that as it may, as innovation has advanced quickly and all the most recent gadgets require power for their operation, it is essential that we make our present power framework more dependable and effective. The existing power grid is operating under stressed condition with minimal safety margins as the amount of transportation of electrical power is increasing at rapid rate without significant addition in the grid infrastructure. The existing power system is designed to support centralized generation while its operation is limited to one-way flow of energy & information and it hasn't changed much in decades. Growing complexities due to rapid connection of ever increasing loads & its variety has made the system to operate at poor efficiency & vulnerable to frequent failures & blackout.

The connection of nonlinear loads to the grid is deteriorating the quality of power by inducing the harmonics in the supply. Security is no more limited to solution to electricity theft. With advancement in technology being used in interconnection of generation, transmission and distributed system security issues have taken a entirely different form. As these existing systems need to be operated and controlled with communication among them for efficient operation of smart grid, so complex computer network came into existence. With complex network there came network attacks in form of cyber security vulnerabilities. These vulnerabilities can be thrown into the system from public network from across the globe.

1.1 Different levels of decentralization

The electrical power grid in the European Union depends on a major number of heterogeneous members; that are progressively and by each other associated. Each member of the electrical power lattice manufactures and works its piece of the system in its own way; and in the meantime they need to cooperate. So the EU Conceptual Model needs to manage distinctive levels of decentralization (see Figure 1).

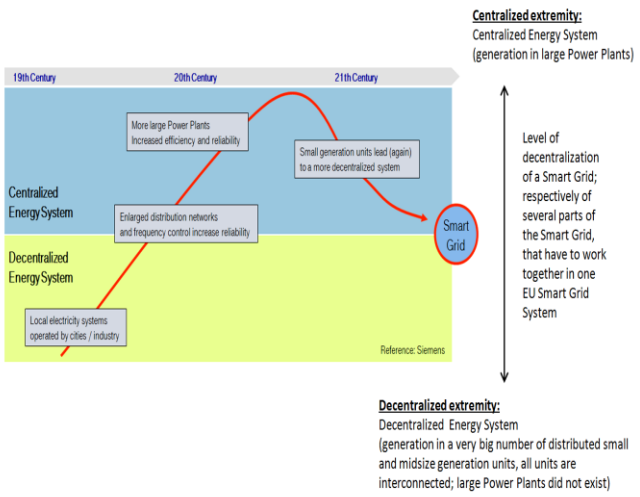

Fig-1: Different levels of decentralization (CENELEC)

Moreover, the vulnerabilities can be transmitted to any section of the system and can simultaneously affect many systems. These threats can send customer off power for uncertain time period depending on the threat spread into the network. The issues are reliable access to useful information, protection from improper information i.e. harmful information, unauthorized modification or destruction of valid information and restriction to accessibility of information to unauthorized individuals. Data management has also to be looked upon and malicious data have to be validated. Figure 2 depicted the reference model of smart grid.

1.2 NIST Smart Meter Framework

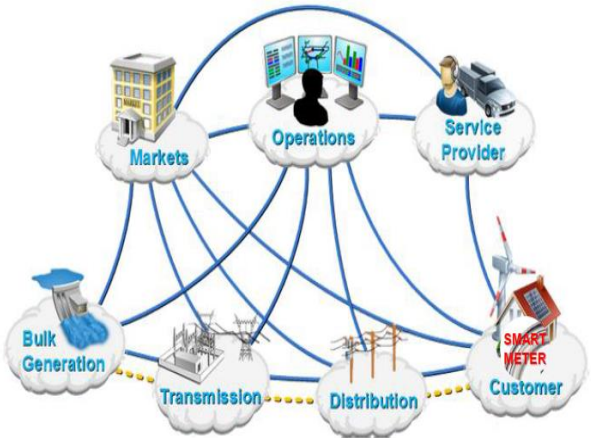

Fig-2: Smart grid reference architecture (NIST Smart Meter Framework 1.0 Sept 2009)

As indicated by NIST's theoretical model [3], the Smart Matrix comprises of seven consistent areas: Bulk Generation, Transmission, Distribution, Customer, Markets, Service Supplier and Operations. The initial four elements the two-way power and data streams. The last three feature data gathering and power administration in the smart Grid. Accordingly, comparing with legacy power control frameworks, the smart Grid will use both wired and wireless network innovations to give a progressive worldview of extensive scale, exceptionally conveyed, and various leveled communication frameworks for vitality conveyance and administration later on. To guarantee secure and dependable operation, such a confounded data framework requires a comprehensive security treatment [8] in light of the particular components in the Smart Grid.

2. FEATURES OF SMART GRID COMMUNICATION NETWORKS

It is apparent that the Smart Grid correspondence network is like the Internet regarding the many-sided quality what's more, various leveled structure. The following are the features of the smart grid:

1. Traffic model: In power systems, notwithstanding, a lot of movement streams are intermittent [8,9] with the end goal of reliable screening, for example, crude information testing in power substations also, intermittent meter perusing in home-zone systems [4].
2. Communication model: The end-to-end guideline is the basis of the Internet with the end goal that it can bolster peer-to-peer correspondence between any hub match in the world.
3. Protocol stack: The Internet is built upon the IP protocol and is moving forward to IPv6. It has been widely expected that the Smart Grid will use IPv6 [3] as the major network-layer protocol.
4. Timing requirement. Over the Internet, most IP traffic is best-effort traffic while the delay-sensitive traffic has delay requirements of 100–150 ms in order to support voice-over-IP and multimedia services [7].

3. SMART GRID SECURITY REQUIREMENTS

The main objective of security is to provide secure and valid communication over the network. The cyber security working gathering in the NIST Smart grid interoperability board has recently released a comprehensive rule for Smart Grid digital security [10] based on the CIA triad (see fig3).

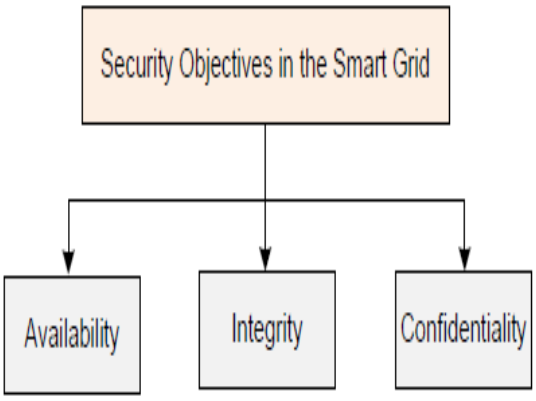

Fig-3: CIA triad

- Availability: Ensuring timely and reliable access to and use of information is of the most importance in the Smart Grid.
- Confidentiality: Preserving authorized restrictions on information access and disclosure is mainly to protect personal privacy and proprietary information.
- Integrity: Guarding against improper information modification or destruction is to ensure information non-repudiation and authenticity.

The NIST report [10] moreover prescribes particular security necessities for the Smart Framework, including both digital security and physical security. In particular, the digital security part indicates security issues and prerequisites identified with Smart Grid data what's more, system frameworks; and the physical security part indicates necessities relating to physical gear what's more, condition security and in addition representative and staff security strategies. The table1 provides the comparison of smart grid with internet.

Cyber security requirements for the Smart Grid are as follows:

1. Secure and efficient communication protocols
2. Identification
3. Attack detection and resilience operations
4. Authentication and access control

In communication networks, security attacks can be classified into two types: selfish misbehaving users and malicious users. Selfish misbehaving users are those attempting to obtain more network resources than legitimate users by violating communication protocols [11]. Accordingly, both selfish and malicious users pose challenging security problems to communication networks.

In the Smart Grid, malicious behavior is a more concerned issue than selfish behavior, as millions of electronic processing devices are utilized for observing what's more, control purposes as opposed to giving information administrations for example, record downloading and sharing [9].

Table -1: Comparison of security requirements between smart grid and internet [10]

Security Functions	**Smart Grid Communication Network**	**The Internet**
Authentication and access control	Strictly enforced for all communication flows throughout the system	Mostly free end-to-end flows without access control
Attack detection and countermeasures	Essential and widely-deployed everywhere	Mainly for critical routers and servers
Security for network protocols	From MAC-layer to application-layer security	From network-layer to application layer security
Every node	Basic cryptographic functions	No specification

The author considers malicious attacks are of three types based on the Smart Grid security objectives, i.e., availability, integrity and confidentiality. Attacks targeting availability, also called denial-of service (DoS) attacks, attempt to delay, block or corrupt the communication in the Smart Grid. Attacks targeting integrity aim at deliberately and illegally modifying or disrupting data exchange in the Smart Grid. Attacks targeting confidentiality intend to acquire unauthorized information from network resources in the Smart Grid.

4. DENIAL-OF-SERVICE ATTACKS

Denial of service attack (DoS) attacks servers, networks or systems with activity keeping in mind the end goal to overpower the casualty assets and make it troublesome or inconceivable for authentic clients to utilize them. While an assault that crashes a server can frequently be managed effectively by basically rebooting the network, flooding attacks can be more hard to recover from[15,18]. The DoS attack can occur in all the layers of network model. The table2 provides information about layers and the type of attack on the same.

Table-2: DoS attack on power system [1]

S. No.	Communication layer	Attack
1	Application layer	
2	Transport/ Network layer	Traffic flooding
3	MAC layer	ARP spoofing
4	Physical layer	Jamming in substations

Three scenarios are mentioning here for finding out the Dos attack problems for smart grid, they are:

DoS attack, As IEC 61850 depends on Ethernet and TCP/IP [21], IEDs in a substation can move toward becoming targets of DoS attack, for example, movement flooding and TCP SYN attack. Be that as it may, neighborhood DoS attack propelled by traded off IEDs are restricted in scale and may not lead to huge effects on the correspondence execution, since there are set number (tens) of IEDs in a power substation [13,14]. In this manner, the risk of vast scale DoS attack that overpower a substation system is chiefly from the outside of a substation.

In such manner, the substation PC (the system door of the substation) turns into the essential target of TCP/IP DoS attack. At the end of the day, substation doors must authorize solid get to control and sifting arrangements for approaching correspondence streams. In other words, substation gateways must enforce strong access control and filtering policies [19] for incoming communication flows. Furthermore, when wireless technologies are adopted in a substation, jamming attacks may become a primary security threat. Therefore, anti-jamming technologies need to be used to protect wireless communication in substations.

1. The second situation, alluded to as is about observing, control and security, which are not restricted in neighborhood. In this procedure, electronic gadget status and readings in neighborhood can likewise be conveyed to the SCADA community for incorporated administration [21]. A traditional server and-customers correspondence display in a multi-bounce and various leveled organize, which is like the Internet and sensor systems. As the SCADA focus fills in as the sink hub to which information bundles are conveyed, it turns into an essential focus of dispersed DoS (DDoS) assaults that can be propelled from different neighborhood. In like manner, the SCADA focus can use existing DDoS assault safeguard methodologies to countermeasure potential DDoS assaults.

2. Information gathering and total in Case 3 is additionally powerless against DDoS assaults. Moreover, the SCADA focus may not be the essential focus for this situation; aggressors can target neighborhood and dispatch generally little scale DoS assaults to postpone or square information conveyance from those frameworks. Since state estimation can be performed as it were at the point when all information is adequately gathered from neighborhood frameworks [17,20], such little scale DoS assaults can come about in fractional inaccessibility of information tests for state estimation.

5. CONCLUSIONS

Cyber security in the Smart Grid is another zone of research that has pulled in quickly developing consideration in the government, industry and the scholarly world. In this paper, the author provided a complete review of DoS attacks in the smart Grid. Components of the Smart Grid correspondence arrange, for example, heterogeneous devices and system engineering, network devices, delay constraints, adaptability, what's more, expanded abilities of installed devices, make it in fact illogical to consistently send solid security approaches everywhere throughout the Smart Grid. The Smart Grid requires fine-grained security arrangements outlined particularly for distinct network applications, making cyber security for the Smart Grid an exceptionally productive and testing research zone in future.

6. REFERENCES

[1] Wenye Wang, Zhuo Lu,"Cyber Security in the Smart Grid: Survey and Challenges", Department of Electrical and Computer Engineering, North Carolina State University, Raleigh NC 27606, US, Elsevier.M. Young, The Technical Writer's Handbook. Mill Valley, CA: University Science, 1989.

[2] G. Lu, D. De, W.-Z. Song, SmartGridLab: A laboratory-base smart grid testbed, in: Proc. of IEEE Conference on Smart Grid Communications, 2010.

[3] A. Huang, M. Crow, G. Heydt, J. Zheng, S. Dale, The future renewable electric energy delivery and management (freedm)

[4] Office of the National Coordinator for Smart Grid Interoperability, NIST framework and roadmap for smart grid interop-erability standards, release 1.0, NIST Special Publication 1108 (2010) 1–145.

[5] V. C. Gungor, F. C. Lambert, A survey on communication networks for electric system automation, Computer Networks (2006) 877–897.

[6] T.-I. Choi, K. Y. Lee, D. R. Lee, J. K. Ahn, Communication system for distribution automation using cdma, IEEE Trans.

[7] T.-I. Choi, K. Y. Lee, D. R. Lee, J. K. Ahn, Communication system for distribution automation using cdma, IEEE Trans.

Power Delivery 23 (2008) 650–656.

[8] S. Mohagheghi, J. Stoupis, Z. Wang, Communication proto cols and networks for power systems - current status and future trends, in: Proc. of Power Systems Conference and Exposition (PES '09), 2009.

[9] P. M. Kanabar, M. G. Kanabar, W. El-Khattam, T. S. Sidhu, A. Shami, Evaluation of communication technologies for IEC61850 based distribution automation system with distributed energy resources, in: Proc. of the IEEE Power and Energy Society General Meeting (PES '09), 2009.

[10] M. J. Karam, F. A. Tobagi, Analysis of the delay and jitter of voice traffic over the Internet, in: Proc. of IEEE INFOCOM '01, 2001.

[11] The Smart Grid Interoperability Panel - Cyber Security Working Group, Guidelines for smart grid cyber security, NISTIR 7628 (2010) 1–597.

[12] IEC Standard, IEC 61850: Communication networks and systems in substations.

[13] M. E. Crovella, A. Bestavros, Self-similarity in world wide web traffic: Evidence and possible causes, IEEE/ACM Trans. Networking 5 (6) (1997) 835 – 846.

[14] T. S. Sidhu, Y. Yin, Modelling and simulation for performance evaluation of IEC61850-based substation communication systems, IEEE Trans. Power Delivery 22 (3) (2007) 1482–1489.

[15] D. Jin, D. M.Nicol, G. Yan, An event buffer flooding attack in dnp3 controlled scada systems, in: Proceedings of the 2011 Winter Simulation Conference, 2011.

[16] U. Premaratne, J. Samarabandu, T. Sidhu, R. Beresh, J.-C. Tan, An intrusion detection system for IEC61850 automated substations, IEEE Trans. Power Delivery 25 (2010) 2376–2383.

[17] Z. Lu,W.Wang, C.Wang, From jammer to gambler: Modeling and detection of jamming attacks against time-critical traffic, in: Proc. of IEEE INFOCOM 2011, 2011.

[18] Y. Liu, P. Ning, M. Reiter, False data injection attacks against state estimation in electric power grids, in: Proc. of ACM Computer and Communication Security (CCS), 2009.

[19] C. L. Schuba, I. V. Krsul, M. G. Kuhn, E. H. Spafford, A. Sundaram, D. Zamboni, Analysis of a denial of service attack on tcp, in: Proc. of IEEE Symposium on Security and Privacy (S&P 1997), 1997.

[20] A. Yaar, A. Perrig, D. Song, Pi: A path identification mechanism to defend against DDoS attacks, in: Proc. of IEEE Symposium on Security and Privacy (S&P 2003), 2003.

[21] J. Mirkovic, P. Reiher, A taxonomy of DDoS attack and DDoS defense mechanisms, SIGCOMM Comput. Commun. Rev. 34 (2) (2004) 39–53.

[22] S. Ranjan, R. Swaminathan, M. Uysal, A. Nucci, E. Knightly, Ddos-shield: Ddos-resilient scheduling to counter application layer attacks, ACM/IEEE Trans. Networking 17 (1) (2009) 40–53.