International Journal of Innovations in Engineering and Technology (IJIET)
http://dx.doi.org/10.21172/ijiet.82.046

Review Paper on Different Types of Attack in Grid Computing

Er. Kulveer
Guru Kashi University Talwandi Sabo Bathinda,Punjab

Prof. Dinesh Kumar
Guru Kashi University Talwandi Sabo Bathinda,Punjab

Abstract - As this grid type of network is highly vulnerable to various types of attacks. Major is black hole attack in the grid. This attack will produce the denial of service. Such that node destruction will be taken place. Every data arrives at this node will be dropped in between. In result will drop the performance of the network. To protect the system from this kind of attacks they have uses the centralized IDS(Intrusion Detection Scheme). Which gathers the data about each node and send that to the central collector. So that each node information will be kept at central collector. If any type of node will be found will be stopped from communication in between.

Key Terms: IDS,Smar Grid

I. INTRODUCTION

A smart grid includes a variety of operational and energy measures including smart meters, smart appliances, renewable energy resources, and energy efficiency resources[1]. Smart grids make use of distributed systems to provide its services to its customers. These help in cutting down the cost of providing services in an authentic and systematic manner. Smart grid systems make use of data provided by the customers through a 2-way digital communication.

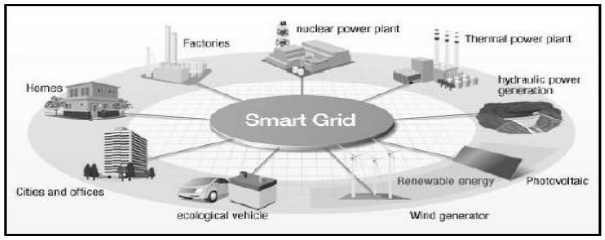

Figure1 smart grid

Figure1 demonstrates the smart grid framework. The power generation is commuted by different sources like wind, solar, nuclear etc. the generated power is then provided to users through different centers. There are five key factors to consider for the efficient operation of the smart grid: communications, smart metering, distributed energy resources, monitoring and controlling [2, 3]. Communication across the power line uses feeder section lines as a medium between consumers and utilities [2]. The distribution of energy resources allows for the moving away from centralized power stations to more widely available options as well the inclusion of alternative energy supplies.

1.1 POSSIBLE THREATS AND THEIR CATEGORIES

With a big number of malicious cyber attacks on the networks, identifying possible vulnerabilities is of great significance. Any attacker can utilize the vulnerabilities discussed in previous section with different intentions and can affect the network security. An attacker can be internal or external to the network.
The authors in [1] have categorized cyber attackers into following categories:
1) Non-malicious attackers; who take the security system as a puzzle and try to decode them with their intellectual concepts.

2) Consumers; mainly the unhappy customers driven by revenge and hatefulness for other consumers or the service provider.
3) Terrorists; who target smart grids and aim to cut down the service or retrieve crucial information.
4) Internal Employees; untrained employees or unhappy employees who have hatefulness for other consumers or the service providers.
5) Rivals; they attack each other for personal benefits or sometimes just to disrupt the resources of counterpart.

Few more categories of attacks are discussed in [1] Including
1) Using Malware: An intruder can use malwares to crash the smart meters or important resources. Malwares can also alter or delete sensitive information.
2) Unauthorized Access: Intruders can access the network through unauthorized access if the database is not using a security mechanism to check the authenticity of the logins. Unauthorized access can exploit the network resources and this is tough to detect if the login is not secure.
3) Replay: An attacker may send false messages or may retransmit same message multiple time to create an unauthorized effect. These false messages have adverse effect. These can engage the receiver unnecessarily or may overload receiver resulting in malfunctioning or slow down of the whole communication.
4) DoS attacks: This type of attack delays the response from servers and since smart grid uses IP, smart grid has the possibility of vulnerabilities inherent in the DoS attacks. Such attacks can also block the transmission of message packets over the network.
5) Traffic analysis: A cyber attack can take a form of simply analyzing the network traffic and the pattern in which data packets are routed. By such attack an attacker can gain crucial information like basic structure of Smart grid, amount of energy usage, price etc.

II. COMPARATIVE STUDY OF VARIOUS PAPERS ON ATTACKS

Author name	**What they have Done**	**Constraints**
Nadia Boumkheld	Smart grid is the new electrical grid that will change forever the way we use energy, thanks to the deployment of sensing and communication technologies. It allows consumers to become more aware and in control of their energy consumption. However, the pervasive communication infrastructure deployed inside the smart grid makes it a target to different types of attacks, which is why security is an essential element in building a robust grid.	In this article we develop an Intrusion Detection System (IDS) that uses data mining techniques for the detection of a Denial of service (DOS) attack in a smart grid, the so called blackhole attack.
Jun Yan, Yufei Tang	Smart Grid security has motivated numerous researches from multiple disciplines. Among the recently discovered security challenges, the	

	False Data Injection (FDI) has drawn great attention from power and energy, computer, and communication research community, because of its potential to manipulate measurements in state estimation (SE) without being identified by conventional bad data detection (BDD) methods.	
Goran Kišan	Using Intelligent Control Systems for Dynamic Management of Smart Grid Network in energy distribution systems will reduce cost, reach manageability, provide safety of energy supply chain to end customer and provide new innovative energy service delivery.	Network management architecture covers a wide area, including security, performance, fault tolerancy and networking configuration. There are two way approach to effective network management by using in-band and out-of-band monitoring.
Shivani Agrawal	The proposed scheme aims to enhance the reliability of text based passwords for advanced users by adapting a combination of text and graphical passwords. In this way a more secure way will be provided to users for granting access to an authenticated system.	The proposed idea could be highly beneficial for ATM machines where access method is via a dummy password.
Abdulghani Suwan	Grid computing systems are complex and dynamic systems and therefore require appropriate automated management, which would enable stable and reliable operation of the whole grid environment. The research community has addressed this requirement with a number of monitoring frameworks, which serve to collect data at various levels to support decision taking	

	and management activities within grids.	
Suman Avdhesh Yadav	The conventional power grid is now maturing to smart grid that incorporates a heterogeneous amalgam of operating measures like smart appliances, meters, renewable energy resources.	Smart grid merges the conventional electrical power grid with ICT. Electric convenience can now realize three sets of amendments: framework upgrade, digital inclusion; the ethos of smart grid; and business process transformation, that make capital out of investments in smart technology.

III. CONCLUSION

There is a major difference between securing an IT network and securing a smart grid. IT networks focus on securing data repositories and network using well defined protocols; whereas when we talk about securing energy grids, the control is in hand of service providers. The protocols used in smart grids are defined by the vendors. Also, the Quality of Service (QoS) metrics are different for IT networks and Smart grids. Smart grids maintain the availability in presence of individual component failures and updates; whereas IT networks need to reboot the complete system. This variation raises a requirement to establish new solutions to security of Smart Grids.

REFERENCES

[1] Nadia Boumkheld , Mounir Ghogho, and Mohammed El Koutbi," Intrusion Detection system for the Detection of Blackhole Attacks in a Smart Grid" 978-1-5090-3488-8/16
[2] Jun Yan, Yufei Tang, Bo Tang, Haibo He, and Yan (Lindsay) Sun," Power Grid Resilience Against False Data Injection Attacks",vol. 5 issue 11 2016.
[3] Goran Kišan, Silvi Kolarić, Marin Šagovac, Zoran Baus," Using Intelligent Control Systems for Dynamic Management of Smart Grid Network", 978-1-5090-3720-9/16.
[4] Shivani Agrawal, Adil Zafar Ansari, M. Sarosh Umar," Multimedia Graphical Grid Based Text Password Authentication For Advanced Users", 978-1-4673-8975-4/16
[5] Abdulghani Suwan, Francois Siewe and Nasser Abwnawar," Towards Monitoring Security Policies in Grid Computing: A Survey", SAI Computing Conference 2016 July 13-15, 2016.
[6] 1Suman Avdhesh Yadav, 2Shipra Ravi Kumar, 3Smita Sharma, 4Akanksha Singh," A Review of Possibilities and Solutions of Cyber Attacks in Smart Grids", 978-1-5090-2084-3/16.
[7] Bari, A. 2014. "Challenges in the Smart Grid Applications: An Overview." International Journal of Distributed Server Networks 2014 (1): 1-11.
[8] Ericsson, G. 2010. "Cyber Security and Power System Communication—Essential Parts of a Smart Grid Infrastructure." IEEE Transactions on Power Delivery 25 (3): 1501-7.
[9] Knapp, E. D., and Samani, R. 2013. Applied Cyber Security and the Smart Grid: Implementing Security Controls into the Modern Power Infrastructure. New York: Elsevier Inc.
[10] McLaughlin, S. 2009. "Energy Theft in the Advanced Metering Infrastructure." IEEE Journal on Selected Issues in Communications 6027 (15): 176-87.
[11] Molazem, F. 2012. "Security and Privacy of Smart Meters: A Survey." In Overview of Computer Security, British Columbia: University of British Columbia.
[12] Cleveland, F. 2008. "Cyber Security Issues for Advanced Metering Infrastructure." In Proceedings of the Power and Energy Society General Meeting—Conversion and Delivery of Electrical Energy in the 21st Century, 1-5.
[13] Mohhammad Zahran, "Smart Grid Technology, Vision Management and Control" WSEAS TRANSACTIONS on SYSTEMS, Volume 12, Issue 1, January 2013.