International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 3 Issue: 3 923 - 926

A New Ranking Approach to Efficiently Detect Anomalies in Cyber Security of Substation

Ruth Rubavathy A. M.E
Department of CSE,
St. Joseph College of Engineering,
Chennai, India.
rutharul18@gmail.com

Mr. M. Navaneetha Krishnan, M.E., (Ph.D.),
Head of the Department
Department of CSE
St .Joseph College of Engineering
Chennai, India
mnksjce@gmail.com

Abstract- Smart Grid advancements present an undetermined level of risk to electric grid reliability. The coupling of the power infrastructure with complex computer networks substantially expand current cyber-attack surface area and will require significant advances in cyber security capabilities. New capabilities for smart grid system and networks, such as broadband and distributed intelligence capabilities can efficiently enhance the efficiency and reliability, but they may also create much new vulnerability if not deployed with the appropriate security controls. Providing security for a large system may seem an unfathomable task, and can leave utilities open to cyber-attacks. The problem is to provide an efficient security mechanism to the power grids. Already many mechanisms are proposed for network and host based cyber security these methods does not provide efficient security mechanism. A new mechanism is proposed based on ranking the network and host based anomalies using Gaussian approximation algorithm. This method will monitor the anomalies occurs in the substation and rank the continuous network level security by implementing additional features such as Traffic Analyzing System, Address Blocks System and Packet Filtering System.

Index Terms—*Anomaly detection, cyber security substations, GOOSE anomaly detection, SMV anomaly detection and Ranking anomaly detection.*

*****

I. INTRODUCTION:

A Smart Grid is an enhanced power grid that transmits, generates, and uses electricity with the support of information and communications technology (ICT) for advanced remote control and automation [1]. A smart grid has the potential benefit power systems and customers, such as improved reliability, efficiency and reduced costs. Automation of the power grid includes substation and distribution automation. The smart substations is a critical issue for the smart grid as it plays an important role in advanced monitoring and control of the power grids. The substation is installed with communication networks and critical devices such as transformers, IEDs, circuit breakers, distribution feeders, and communication systems. A smart substation enhances reliability and efficiency of operation, monitoring, control and protection [2]. Therefore, an effective measure to address this issue is to detect, mitigate and prevent malicious activities at the substations. Anomaly refers to the task of finding abnormal behaviors in data networks; it is a concept widely adopted in computer networks [8]. The term Intrusion Detection System (IDS) is also used for cyber security in a substation. It monitors user access logs, system event logs, file access logs and to see if there is any anomaly in the host system.

This model uses statistics for anomaly detection and an intrusion detection expert system (IDES). Typical approaches to intrusion detection are either network or host-based methods. A network-based IDS (NIDS) collects packets from a communication network and analyze network activities. A host-based ID monitors a host system and generates alarms when anomalies and malicious activities are observed. However, both network- and host-based intrusion detection methods have their own weaknesses. The network-based anomaly detection is focused on multicast messages in a substation network it also detects in a real-time environment, anomalies that detect the undesirable behaviors. The main contribution of this paper is a new method for 1) an power grid creation, e.g., IEDs, firewall, and user-interface 2) a network-based anomaly detection algorithm that can be used the test results demonstrate that proposed anomaly detection algorithms are effective for the detection of simulated attacks. These attacks are ranked by a Gaussian approximation algorithm and secure the power station. In the remaining of this paper, Section II describes cyber security vulnerabilities in a network substation. Section III includes algorithms for host and network-based anomaly detection schemes, the network-based substation multicast messages are analyzed for anomaly detection. Section IV provides the results of ranking anomaly detection system and the simultaneous intrusion detection at many substations. The conclusions and recommendations for future work are given in Section V.

II. CYBER SECURITY VULNERABILITY OF A SUBSTATION

A Power Substation may consist of various types of equipment such as Global Positioning System (GPS) network devices, user-interface, Server, firewall, IEDs, and remote access points. In host and network based anomaly detection GOOSE and SMV are introduced. GOOSE is used to send tripping signals from IEDs. Sampled Measured Voltage and current values (SMV) are sent from a Merging Unit (MU) to an IED. Many devices are accessed by GPS. MMS is used for reporting, monitoring, and controlling between the user-interface and IEDs. The vulnerabilities of the substation network and mitigation of cyber-attacks are critical subjects for anomaly detection. The remote accesses to a substation network from corporate offices or locations external to the substation is not uncommon for control and maintenance purposes. Virtual Private Network (VPN) and wireless are available mechanisms between remote access

points and the substation Local Area Network (LAN). The access points are potential sources which are connected with cyber vulnerabilities. When remote access points have been expediently by an intruder to access critical information, so the Substation Configuration Description (SCD), can be launched. This paper assumes that the remote access point is the main intrusion point to the substations. The intruders may be able to access the substation network after the firewall is compromised. It may capture, modify, and retransfer GOOSE packets and operate circuit breakers in a substation. The attacker may also send fabricated GOOSE to other substations. The consequence of a fabricated sample message attack can generate high current values to a control center and it may lead to an undesirable operation. After malicious anomalies are detected in a substation network using the proposed integrated anomaly detection system, an intruder can be interrupt by collaboration between the IDS and firewall. This can be improved by dynamic rejection rules or interrupt connecting open ports. The proposed IADS uses anomaly and specification-based detection algorithms. Therefore, the unknown or intelligent attacks that are not defined in the algorithm. Inside attack: if a USB is already infected by an attacker. Outside attack: Remote access points may be used for maintenance, control and operate. Once an intruder accepts the remote access, the attack may be able to pass the firewall and has a profit access to the substation network. Both inside intrusion and outside intrusion can be host-based or network-based attacks.

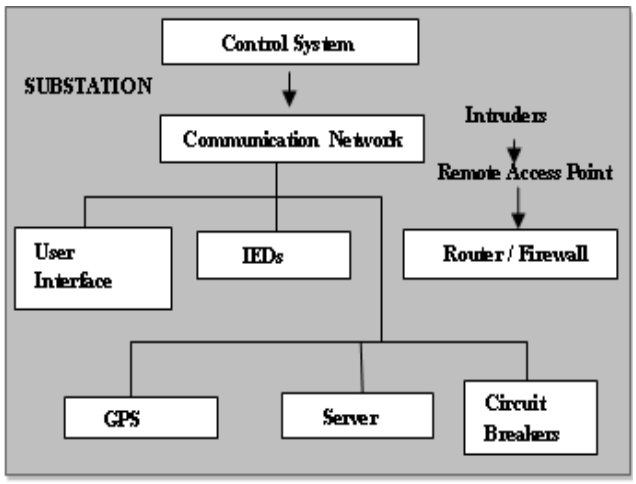

Fig: 1 Intruders points in a substation automation system.

III. ANOMALY DETECTION

Anomaly detection refers to finding patterns that indicate abnormal or undesirable behaviors. It is a method for detection of cyber security intrusions that requires data analysis and correlation of events. Anomaly detection is performed based on logs of intruders' footprints.

A. Host based Anomaly Detection

The main assumption of the temporal anomaly detection for host-based anomaly detection is that the engineering software and hardware are able to generate system logs. For occurrence, if an intruder makes a wrong password attempt to IED, the action will generate a wrong password attempt flag. Similar method is done by the intruder when tries to copy or change a file in the user-interface, it gives as an unauthorized file change flag. The generalized method has set of substation logs and messages and extends the capability to scenarios involving multiple substations. Host-based anomaly detection is used for temporal anomaly and can be determined between event logs from different time periods. Data logs at substation networks are used for the host-based anomaly detection algorithm. After applying to the logs, a data convertor module will change all temporal logs to binary values. If wrong attempt occurs then the value is changed from 0 to 1.

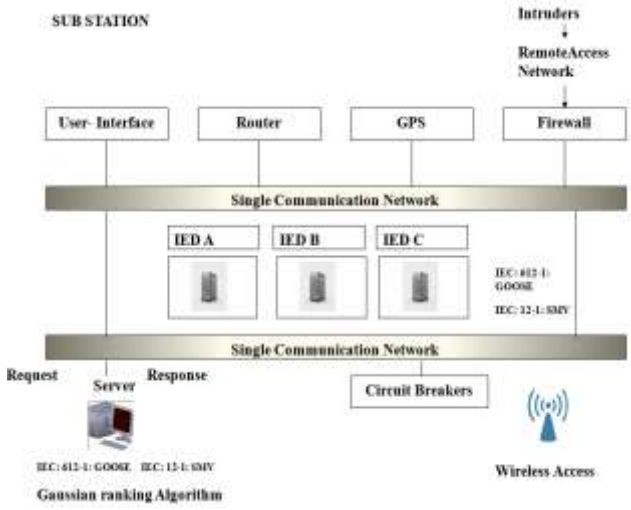

Fig: 2 Architecture Diagram

B. Network based Anomaly Detection

The proposed method also provides a network-based anomaly detection algorithm for multicast messages in the substation automation network. The multicast messages are based on GOOSE and SMV messages. GOOSE is used to send tripping signals from IEDs. Sampled Measured Voltage and current values (SMV) are sent from a Merging Unit (MU) to an IED. A GOOSE message format will contain Threshold violation, Sequence and state number violation, Time and date violation. An SMV message format will contain threshold violation, Count Violation and data violation. Any detected anomaly in threshold violation, sequence and state number violation, GOOSE time violation, and GOOSE data violation will change GOOSE network-based anomaly indicator from false to true.

GOOSE Anomaly Detection

In multicast messaging GOOSE message will be transmitted from client to server. Initially this message is set to 0. A time stamp will be fixed and the message will be transmitted. If the message is not received in time then anomaly will be detected in time stamp itself. It will be fixed with threshold value, data, and time and sequence number. If any violation occurs in these parameters then the

 ISSN: 2321-8169
923 - 926

indicator will be changed from 0 to 1 and indicates anomaly occurred. In Network based Anomaly Detected GOOSE messages plays the role which provide high speed and consistently good in quality mechanism of transferring event data over entire substation networks this message also implements the signatures of each message and groups all the violation and vulnerability in the message and which is detected by Intelligent Electronic Device.

SMV Anomaly Detection

The threshold value of SMV message is assumed based on the sampling values. It is also initially set to 0. The anomaly detection system will first check the MAC address of the message and then check the transmission time and change in name of identification and dataset if any changes occur then the indicator changes from 0 to 1 and ensure anomaly occurred. SMV messages are used for learning algorithm that analyze data and recognize patterns, used for regression analysis method which gets the sample value from IED.

IV. RANKING ANOMALIES DETECTION

This method includes the ranking of frequently occurring anomalies. The Gaussian algorithm will be implemented in the GOOSE and SMV Messages. This function will assign weightage value and when anomaly occur the weight value increases. This process will be done for every incoming message. Finally this algorithm ranks the most frequently occurring anomaly and indicates the system to prevent from the anomaly and protect more security to the grid.

Gaussian Approximation Detection

For this method, the data is assumed to follow the Gaussian probability distribution. Therefore, the detectors detect anomalies based on the Gaussian method where each sample is compared to thresholds which are based on the mean and standard deviation of its underlying distribution. To compute the probability assigned to each observation Mk (t) by a Gaussian distribution we need to quantize Mk (t). To do so, we partition the data range into a set of buckets fb1; b2: g be the width, and Q be the function that maps the data range to the set fb1; b2::: g. Let ~ P (bi) denote the probability of a sample falling into bucket bi, i.e., if X is a standard Gaussian random variable, then the probability that Q(X) = bi is given by ~ P (bi). The Gaussian assumption allows us to compute ~ P (bi) using the cumulative distribution function of the standard Gaussian distribution.

Then the ranking algorithm is described below.

1) Compute the Z-score of Mk (t) based on the sample mean _k of Mk and the sample standard deviation _k of Mk. The Z-score is defined as

$$z_{k(t)} = \frac{M_{k(t)} - \mu_k}{\sigma_k}$$

2) The local detector approximates the probability of the observed window as

$$P_k(Z_k(t-W+1), Z_k(t-W+2), \ldots, Z_k(t)) = \prod_{j=t-w+1}^{t} P(Q(Z_k(j))$$

where we assume that the measurements are statistically independent. Observe that if the number of buckets is very large, since they are of equal width, this probability reduces to

$$P_k(Z_k(t-W+1), Z_k(t-w+2), \ldots Z_k \approx c.\exp\left(-\frac{1}{2}\sum_{j=t-W+1}^{t} Z^2/_j\right)$$

where c is a constant, and can be ignored for ranking purposes. This follows from the fact that the probability distribution function approximates ~ P(-) well as the number of buckets grows.

4) The local detector transmits the node computed probability to the central node

5) At time t, the central node gets the probability of the corresponding window to t(W+1) to t from all the local detectors and ranks them according to their probabilities Pk, the least probable receiving the highest ranking.

V. RESULT

The result of host and network based is done by client server model by deployment of control system, server, IEDs. The user main page is created with required details and is connected with server after registration. When registration is wrong it is reported to the server and the threshold value from 0 changes to 1 if unauthorized user access it. It is been implemented via voltage in electrical current system. Hosted based anomalies are temporal so we switch on to network based detection by GOOSE and SMV anomaly detection. Finally we introduce a ranking anomalies detection method to rank all the unauthorized anomalies and provide additional security mechanism for network and host based methods.

Fig I: User Main Page

Fig II: Login of Server

The user and the login server is illustrated and it is been used by first server. It has three sever but the users choose the first server for process details. The rest of the servers are idle until the user communicate with their IP address.

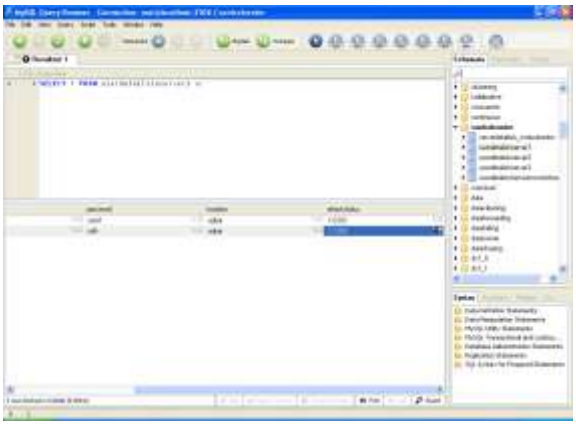

Fig III: Changing of value 0 to 1

VI. CONCLUSION

Rank based anomaly detection in the substation using Gaussian approximation algorithm is proposed in this work. First the host based anomaly is detected in the server using matrix based violation indicator with time and the network based anomaly is detected using GOOSE and SMV message. Finally Gaussian approximation algorithm is implemented in these messages to detect anomalies and rank the most frequent anomalies. This ranking method indicates the security system to concentrate more on the ranked anomalies and if the system focuses on these anomalies the substation will be more secured. The future improvement of this project includes providing additional security mechanism for network and host based methods.

REFERENCE

[1] S. Sridhar, A. Hahn, and M. Govindarasu, "Cyber-physical system security for the electric power grid," *Proc. IEEE*, vol. 100, no. 1, pp. 210–224,Jan.2012.

[2] A. Hahn and M. Govindarasu, "Cyber-attack exposure evaluation framework for the smart grid," *IEEE Trans. Smart Grid*, vol. 2, no. 4,pp. 835–843,Jun. 2011.

[3] M. Kezunovic, "Smart fault location for smart grids," *IEEE Trans.Smart Grid*, vol. 2, no. 1, pp. 11–22 , Mar. 2011.

[4] F.Li,W.Qiao, H. Sun,H. Wan, J. Wang,Y.Xia, Z.Xu, and P. Zhang, "Smart transmission grid: Vision and framework," *IEEE Trans. SmartGrid*, vol. 1, no. 2, pp. 168–177, Sep. 2010.

[5] A.R. Metke and R. L. Ekl, "Security technology for smart grid networks,"*IEEE Trans.Smart Grid*, vol. 1, no. 1, pp. 99–107, Jun. 2010.

[6] C.-W. Ten, J. Hong, and C.-C. Liu, "Anomaly detection for cybersecurity of the substations," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp.865–873, Dec. 2011.

[7] C.-W. Ten, C.-C. Liu, and G. Manimaran, "Vulnerability assessment of cybersecurity for SCADA systems," *IEEE Trans. Power Syst.*, vol.23, no. 4, pp. 1836–1846, Nov. 2008.

[8] J.-W.Wang and L.-L. Rong, "Cascade-based attack vulnerability on the US power grid," *Safety Sci.*, vol. 47, no. 10, pp. 1332–1336, Dec.2009

[9] D.E.Denning, "An intrusion detection model," in *Proc. 7th IEEE Symp. Security Privacy*, May 1986, pp. 119–131.

[10] *NIST Framework and Roadmap for Smart Grid Interoperability Standards*, NIST 1108R2, National Institute for Standards and Technology, Feb.2012

Biography

First Author

Ms. RUTH RUBAVATHY A, received the B.Tech from Anna University, Chennai in 2013 and pursuit for M.E (Computer Science Engg) From St. Joseph college of Engineering, Chennai, India. She is now attending the M.E course in CSE and her research interest include Computer Networks, with specialized in Security and programming languages (JAVA, J2EE) and Web Development, DBMS.

Second Author

Mr. M.NAVANEETHA KRISHNAN, M.E., (Ph.D.), received the M.E in Mepco Sclenk Engineering College and pursuit his Ph.D in M.S University. He is specialized in Cyber Security and programming languages.