Bio Inspired Cyber Security Architecture for Smart Grid

Muhammad Mostafa Amir Faisal
Dept. of Electronic and Telecommunications Engineering
International Islamic University Chittagong
Kumira, Chittagong, Bangladesh.

Muhammad Ariful Islam Chowdhury
Dept. of Electronic and Telecommunications Engineering
International Islamic University Chittagong
Kumira, Chittagong, Bangladesh.

***Abstract*— Smart grid is an advanced and intelligent form of conventional power grid with high fidelity power-flow control, self-healing, and energy reliability using advance computer and communication technologies. The idea of integrating power systems with complex computer communication has introduced serious cyber security concerns as it requires significant dependence on secured communication infrastructures. Because of the wide nature of smart grid, it is very risky to compromise any component of the grid which may lead to serious damage to the electrical infrastructure, energy theft and unnecessary expenditure. Studying various smart grid security architectures, efficient bio-inspired complete security architecture for smart grid is proposed in this work which can be easily implemented in the smart grid without changing any element of its infrastructure. Bio-inspired cyber security architecture for smart grid is developed with discussion on the core elements of the architecture. The threat detection is tested with simulation using popular KDDDump dataset and real time gas pipe line SCADA data.**

Keywords—Cyber Security; Smart Grid; Cyber Security Architecture; Bio-inspired; KDDDump; SCADA security

I. INTRODUCTION

The real motivation behind the development of this work is that the cyber security of smart grid is a very real issue and the failure to address the cyber security risk within the critical infrastructures may invite serious damage to the national and economic infrastructures. Unlike other infrastructures, compromising smart grid is a high risk and a life threatening issue. Possible threats include terrorism, government-sponsored attacks, energy theft etc. The Stuxnet attack on Iran's Nuclear plant is a great example cyber attack on critical infrastructure [1]. A smart grid consists of many sensors, valves and mechanical instruments which are controlled by PLC (programmable logic controller) / RTU (remote telemetry unit) and these components communicate with simple industrial network protocol like dnp3, Modbus etc [2] and common popular network protocol like Ethernet, 802.11 etc. These systems use common operating systems like windows, linux, mostly early and insecure versions of windows and other common vulnerable routing and switching devices [1]. Security is their last concern because most of the power or engineers are experts on control system, not security. So security experts and control system engineers are working together to solve this burning problem. An attempt has been made to solve the existing problems in this work. This easy to implement cyber security architecture does not demand any alteration in the core infrastructure of current smart grid. The work was inspired from the amazing techniques followed by our body to fight different kinds of bacteria for securing smart grid from intruders, where intruders are analogous to bacteria and infrastructure to body.

II. HACKING THE SMART GRID

A. Approach

There are various approaches to compromise a smart grid. First and the easiest way to hack the smart grid is to compromise the Internet Service Providers and getting into LAN and then compromising based on the vulnerability of the Operating Systems, Routers, and Switches etc. This means that choosing perfect vendor is very important for securing smart grid infrastructure. The main scary thing is that every smart grid user is in local area network of the smart grid which is a great challenge here. When an intruder is in local area network of smart grid, he/they may apply DDOS attack or leverage common device specific and industrial protocol specific vulnerabilities. The intruder can also play with some other attack like MIMT (Man in the middle attack), HMI (Human Machine Interface) propping or they may use blended attacks combining various malwares like "Stuxnet" [3].

B. Attack Vectors

Every component of a SCADA system can be a target for a person with malicious intent. But the main components, compromising which will do serious damage are smart meter, transformer, PLC, HMI, RTU, syncrophasors, recloser, sensors, coolers etc [4].

III. PROPOSED SECURITY ARCHITECTURE FOR SMART GRID

A thorough study of different types of security architectures available show that most of the smart grid architectures were not built based on security consideration like NISTIR-7628, SGAM by EU M/490 and the SGCG [1]. On the other hand the 3x3 model by MacAfee [1] is a bit complex to implement in a complex structure system like smart grid. The proposed design, on the other hand, can be implement in any reference architecture of smart grid. The smart grid architecture model provided by CEN-CENELEC-ETSI Smart Grid Coordination Group [5] is used and

978-1-5090-6122-8/16/$31.00 ©2016 IEEE

simplified for proposed smart grid security architecture. Simplified security model is shown in Figure – 1.

Like SGAM created by CENELEC, the domains is segmented in five categories. These are generation, transmission, distribution, distributed electrical resources (DER) and customer premises or Advance metering Infrastructure. We divided zones into five segments which are Field zone, Control Zone or Station, operation, enterprise, and market [5].

In this model, each of the elements can communicate with other with proper access. But the control zones should be very restricted to access from any remote zones like HAN (home area network), field zones, and enterprise and market network region. These networks should not be able to directly query or control the other critical infrastructure systems. If any consumer wants to know about any of his/her information which is stored in database management system in enterprise facility, then his/her query should not go through smart meter to AMI to AMI headend to Control Zone to Operation to Enterprise. He/she should generate query via internet to the financial or marketing department then marketing department will generate a safe query to the enterprise network.

The DNA like symbols represent Immune walls at different endpoints. Combining all the Immune walls, a complete Smart Grid Immune System (SGIS) is constructed. If Immune walls are implemented at the end points of any conventional or new smart grid reference architecture and an SGIS is built, it will enhance most of the security features very efficiently.

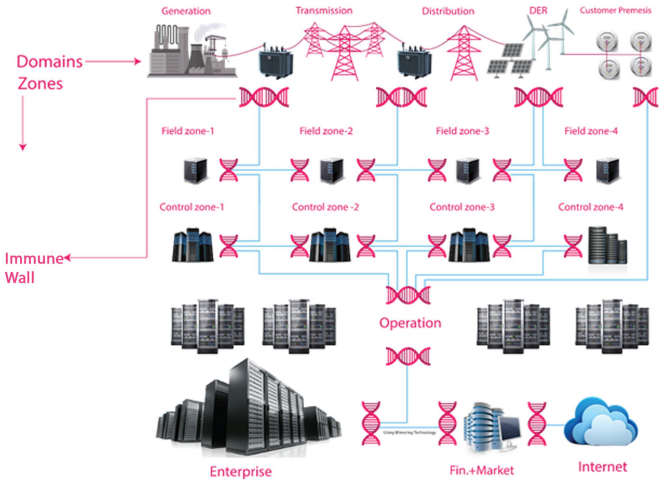

Fig. 1. Security architecture for smart grid. [Stock and images courtesy Freepic.com]

IV. Smart Grid Immune System (SSIS)

Smart grid immune system is the backbone of our architecture. While no one product or technology is certain to stop all attacks, when immune walls are used together in defense-in-depth posture across all areas of the Smart Grid, it is possible to greatly minimize the risk of a successful cyber-attack.

A. *Why Bio-inspired?*

Proposed SGSS is designed being inspired from human Immune System. Historically, immunity meant protection from disease and, more specifically, infectious disease. The cells and molecules responsible for immunity constitute the immune system, and their collective and coordinated response to the introduction of foreign substances is called the immune response [6].

Cardinal Feature of adaptive immune system: All humoral and cell-mediated immune responses to foreign antigens have a number of fundamental properties that reflect the properties of the lymphocytes that mediate these responses[6]. The main features of adaptive immune system are, (1) Specificity, (2) Diversity, (3) Clonal Expansion, (4) Specialization, (5) Contraction and Homeostasis and (6) Nonreactivity to self.

B. *Features of Smart Grid Immune System*

We have designed our smart grid immune system based on these 7 features of adaptive immune system. We have adjusted these features with necessary security requirements for protecting the critical infrastructure from any malicious attempt. The features of the smart grid immune system are describe below:

TABLE I.

Process	Details
Packet Filtering – Specificity	Specificity ensures that only the necessary connection will go through to the Immune wall. It will work as the advance packet filtering system.
Classification	Classify all the incoming connections as intrusion or normal connection based on signatures. It will work as a part of supervised learning based classification of intrusions.
Anomaly Detection– Diversity	Classify all the unknown incoming connections as anomaly or normal connections with anomaly detection technique. It will classify the connection based on unsupervised learning.
Synchronized intrusion and malware database– Cloning	Clone i.e update the latest detection signature with all Immune walls so that all immune wall can be ready to classify the new threat type. It will increase the ability to combat repeat attacks by the same intrusions or malware.
Self-healing and Incident response	Heal the effected system or block the exploit connection with predefined policies and the help of the administrator.

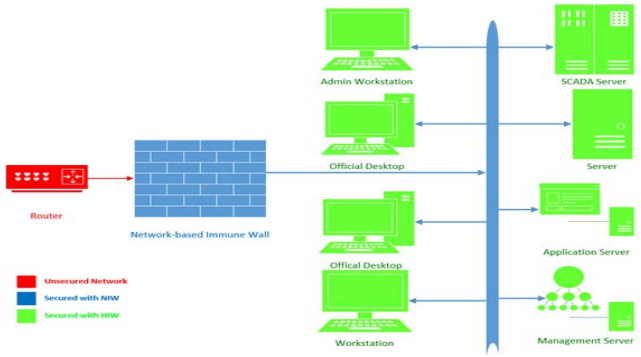

Fig. 2. Simplified structure of SGIS

C. *Structure of immune system*

Smart grid itself is a very distributed and complex system. So, for increasing its security without creating any complexity, a security model is designed which can be implemented at any reference architecture. As shown in Fig. 2, without changing the reference architecture, two security systems are added to it. These are (1) Network-based Immune wall (NIW) i.e. Network-based unified threat management system and (2) Host-based Immune wall (HIW).

V. STRUCTURE OF IMMUNE WALL

A. *Packet Filtering:*

The most important task of the most conventional security mechanism "Firewall" is packet filtering. Firewall is a mechanism used to control and monitor traffic to and from a network for the purpose of protecting devices on the network. It compares the traffic passing through it to a predefined security criteria or policy[7]. Core elements of our packet filter are:

1) *Protocol filter*: The protocol filter should block any other connection using any protocol except SCADA protocol in a SCADA environment. So, the packets with industrial protocol like ModBus, FieldBus, ProfiBus, DNP3 etc. should pass the firewall. This will block majority of other unnecessary protocols like FTP, HTTP etc. where these protocols are not necessary.

2) *Port filter*: By restricting each defined connection to only the specific TCP or UDP port, the other 65,534 TCP/IP stacks are blocked. This port filtering system will block the large window of cyber-attack via malware or any port-specific exploits.

3) *Host filtering*: The major communication in SCADA system occurs by industrial protocols. Most of the contents of the packets are command and control requests from the specific devices like HMI, SCADA server, AMI headend etc. These devices have unique MAC addresses which do not changed until the devices are replaced. As we know that most of the attack are generated from unknown sources. So, this will shield the SCADA equipments from receiving any packet from most of the unknown source.

4) *Basic DDOS filtering*: A firewall can detect basic DDOS based intrusion by analyzing the bandwidth consumption by a single IP. With this rule it can reduce some of the DDOS based attacks.

B. *Classification and Diversity*

Another security measure is still needed after implementing firewall, as a firewall is a dumb device which only follows the defined rules (except modern firewalls [8]). So in this part, an intelligent intrusion prevention system is introduced.

An intelligent intrusion detection system is essential for classifying dynamic attack vector. So in this part, a machine learning technique is implemented to detect most of the predictable and undefined attacks.

The first and foremost task of an intrusion detection system is to classify attack [9]. Classifying an intrusion based on previous training data is most difficult part to play for an intrusion detection system. To classify intrusions, different renowned learning algorithms are implemented. For learning the classifying ability of the learning algorithms, they are tested with different datasets. This helps to decide the algorithm that is best suited for classification and diversity.

1) *Testing with KDDcup99***:** KDDCUP 99 dataset [10] is used for the first simulation that is carried out by data mining software named WEKA. A training set is chosen to train the classifier and the classifying ability of the classifier is tested by giving some test data. To classify attacks, some popular classifiers are used that are used by commercial intrusion detection. The classifiers were trained with 10% of the training data and 10% testing data. The data was cross checked into 4 folds, all of which give almost similar results.

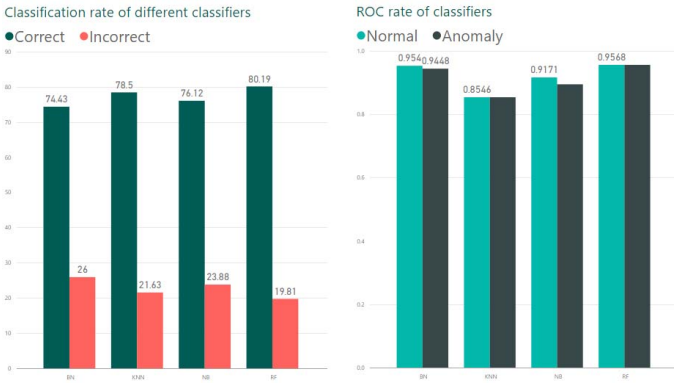

Fig. 3. Classification rate of different algorithms (Bayes Network, K-nearest neighour, Naïve Bays and Random Forest).

So, according to classification rate and ROC curve, Random Forest has high correctly classified instances of 80% with having excellent ROC, KNN correctly classified 78% of the instances with having good ROC. As a result, Random Forest Algorithm is incorporated for classification and KNN for diversity. It has been seen that KNN is best for anomaly detection rather than random forest or bays algorithms.

2) *Testing with SCADA data***:** Real time SCADA dataset created by Dr. Morris and Ian Turnipseed [11] is used for this part of testing. The dataset proposed and created for Ian's research is a second iteration of a previous dataset from a gas pipeline system to fill the void in IDS research for SCADA applications. The first iteration of the dataset was created by Wei Gao [12]. Gao's dataset was found to contain obvious patterns, which caused algorithms to appear to have extremely high detection rates, up to 100%. This data is now classified with elected Random Forest and K-nearest neighbor algorithm by using Weka in the same procedure. The result is highly impressive. Result shown in the Table II below. From this result, it can be said that the method looks promising. If the connections are filtered with Random Forest and then again filtered with KNN, then classification will be highly precise

TABLE II.

Algorithms	Correctly classified instances	Incorrectly classified instances	TP rate	FP rate	AUC
Random Forest	100%	0%	1	0	1
KNN	90%	10%	0.895	0.008	.944

C. *Memory*

Memory is the most important part in smart grid immune system. It consists all kinds of possible attacks and normal connection in a rule based or pcap form so that these can be compared with the incoming packet. Based on the data of the memory, the classifiers will classify a connection.

The memory could be based on sniffed data or rule. It can be created with TCP dump of collection of different types of normal network connections and attacks. Then the classifier will compare the incoming connections with the dataset. Based on classification, the classifier will label the data as normal or anomaly. The rule based database will work the same. The classifier will classify incoming connection by comparing with the rule based data. Then the classifier will classify the data by labeling it as normal or anomaly.

1) *Structure of Netwrok based Immune Wall*: Network based immune wall is the most vital point of smart grid immune system. Each endpoint of smart grid should be secured with NIW (Network-based Immune Wall). It will protect the infrastructure from primary attacks. The flow chart of network based immune wall is shown in Fig. 4. If a NIW is implemented, then all incoming connections should go through this. At first, connection will go through the packet filter region "Specificity" and will be filtered through if it doesn't meet the requirements the filters want to block. Then the filtered connection will again be classified by the random forest algorithm comparing with the database at the second phase "Classification". Then if it classified with anomaly then the system will block the connection and report at the log. If the connection is classified as normal connection, then it has to go through the second phase "Diversity". In this phase filtered data from random forest, will again be filtered and classified through the K-nearest neighbor algorithm. If it is classified as anomaly, system will block the connection and report the log, if not then system will pass the connection and report the log at SIEM (security information and event management).

2) *Structure of host based immune wall*: Host based immune wall is another important part of the smart grid immune system. The network based immune wall can protect the system from DDOS type attack. NIW can also protect the network infrastructure from various types of large attacks. But, a network based immune wall cannot protect the host from malware because the packages coming and going through this network are encrypted as the packets will only decrypt at the host system. NIW can protect the network from major attacks. But it cannot protect the hosts from specific

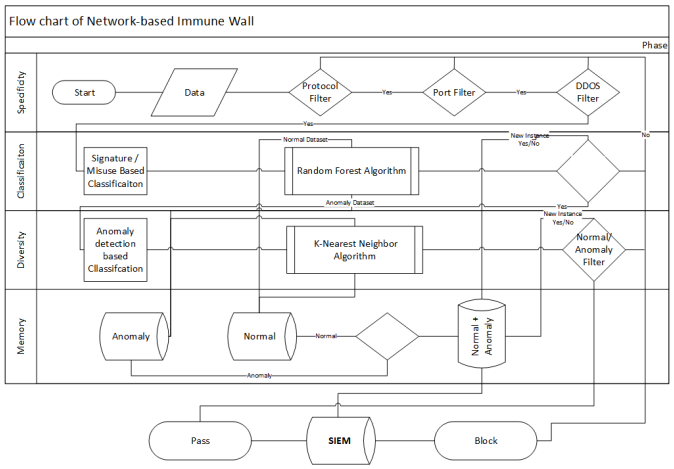

Fig. 4. Flow chart of NIW

attacks, where the use of host-based immune wall comes. Fig. 5 shows the flow chart of the entire host based immune wall. From the figure we can say that a host based immune wall is almost same as the network based immune wall. But there are few changes. It is most probable that a DDOS attack will occur at the endpoint end. If NIW detects the DDOS attack, then host can be safe. But the major threat of host network is device specific attack. That is why a MAC filtering system is added. Most of the threats that occur in SCADA system are device specific, i.e. the target is specifically for a HMI, RTU or for sensors created from the SCADA servers. If the SCADA servers and HMI are protected with HIW and specific MAC addresses are listed in the HIW that are usually communicate for command and control, then the command created from unknown MAC addresses will be declined. A NIW cannot inspect the packet elements because of the encryption but a HIW can inspect the packet because it lies in the host system. So an antivirus is included in the HIW so that it can protect the host from any kinds of malware like military grade malware, SCADA malware etc.

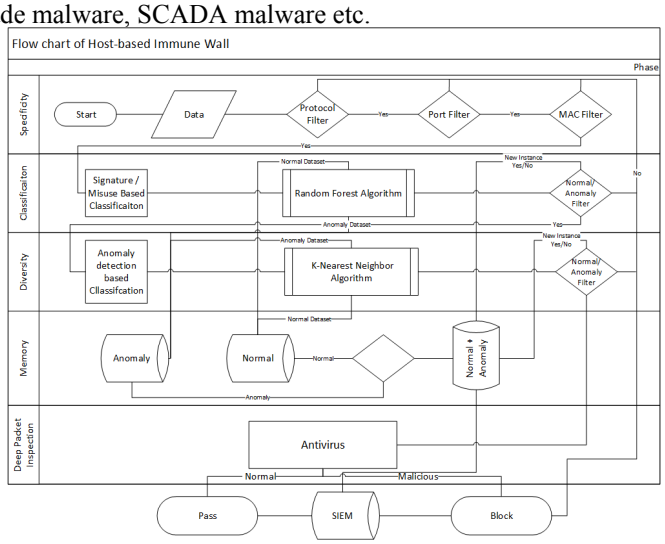

Fig. 5. Flow chart of HIW

VI. Conclusion

In this research, a bio inspired security architecture for smart grid is proposed. The security system in explained in detail and it is shown that every element of the security architecture is crucial. The classification accuracy of the proposed system is also tested. The results show that the system is capable of detecting, with high accuracy, all SCADA intrusions, including injections, replays, and man-in-the-middle attacks. Moreover, the results show that the period of the learning phase plays an important role in improving the detection accuracy of the detection system. However, the detection accuracy of the system is still high even for a one-day learning period because it is basically designed to scale for SCADA systems applications. The advantages of the proposed method can be summarized as follows: (1) detects SCADA–specific attacks; (2) performs real-time detection; (3) shows high detection accuracy even with short learning periods; (4) low false positive (FP) rates; (5) packet filtering rules are added which can filter a huge amount of undesired data; (6) total security solution needed for a smart grid is covered; (7) It is a plug and play method. Just by implementing the NIW in the endpoint and installing the HIW in the host system, highest security can be ensured..

Acknowledgment

First of all, we would like to convey our gratitude to the Almighty Allah (SWT), for giving us the right direction while attempting the task. The real spirit of achieving a goal is through the way of excellence and austere discipline.

We acknowledge with due respect the constant support and patience of our family members for completing this research.

References

[1] Knapp, Eric D, and Raj Samani. Applied Cyber Security And The Smart Grid. Waltman, MA: Syngress, 2013. Print.

[2] Knapp, Eric. Industrial Network Security. Waltham, MA: Syngress, 2011. Print.

[3] Flick, Tony, and Justin Morehouse. Securing the Smart Grid: Next Generation Power Grid Security. Amsterdam: Syngress, 2011. Print.

[4] Knapp, Eric D., and Raj Samani. "Hacking the Smart Grid." Applied Cyber Security and the Smart Grid (2013): 57-86. Web.

[5] CEN, CENELEC, ETSI, SGCG report on reference architecture for the smart grid external version V2.0. SGSC Reference Architecture Working Group (RAWG); August, 2011.

[6] Abbas, Abul K., Andrew H. Lichtman, and Shiv Pillai. *Cellular and Molecular Immunology*. Philadelphia, PA: Saunders Elsevier, 2011. Print.

[7] Medhi, Deepankar, and Karthikeyan Ramasamy. "IP Packet Filtering and Classification." *Network Routing* (2007): 534-81. Web

[8] Turcanik, Michal. "Packet Filtering by Artificial Neural Network." *International Conference on Military Technologies (ICMT) 2015* (2015): n. pag. Web.

[9] R. Bace and P. Mell, "Intrusion detection systems, NIST Technical Report 800-31," National Institute of Standards and Technology (NIST), 2001.

[10] http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html

[11] Morris, Thornton, Turnipseed. "Industrial Control System Simulation and Data Logging for Intrusion Detection System Research". Mississippi State University Starkville, MS, USA. Web.

[12] Morris, Thomas, and Wei Gao. "Industrial Control System Traffic Data Sets for Intrusion Detection Research." *IFIP Advances in Information and Communication Technology Critical Infrastructure Protection VIII* (2014): 65-78. Web.

[13] N. S. A., "Defense in depth: A practical strategy for achieving information assurance in today's highly networked environments." Available at http://www.nsa.gov/ia/_files/support/defenseindepth.pdf.

[14] T. Bass and R. Robichaux, "Defense-in-depth revisited: Qualitative risk analysis methodology for complex network-centric operations," in Military Communications Conference, 2001. MILCOM 2001. Communications for Network-Centric Operations: Creating the Information Force. IEEE, vol. 1, pp. 64–70, 2001.