International Journal of Advanced Culture Technology Vol.2 No.2 7-10 (2014)
IJACT.2014.2.2.7

IJACT 14-2-2

Enhancing Security Gaps in Smart Grid Communication

Sang-Hyun Lee[1], Heon Jeong[2*], Kyung-Il Moon[3]

[1, 3]*Dept. of Computer Engineering, Honam University, Korea*
{leesang64, kimoon}@honam.ac.kr

[2*]*Fire Service Administration, Chodang University, Korea*
hjeong@cdu.ac.kr

Abstract

In order to develop smart grid communications infrastructure, a high level of interconnectivity and reliability among its nodes is required. Sensors, advanced metering devices, electrical appliances, and monitoring devices, just to mention a few, will be highly interconnected allowing for the seamless flow of data. Reliability and security in this flow of data between nodes is crucial due to the low latency and cyber-attacks resilience requirements of the Smart Grid. In particular, Artificial Intelligence techniques such as Fuzzy Logic, Bayesian Inference, Neural Networks, and other methods can be employed to enhance the security gaps in conventional IDSs. A distributed FPGA-based network with adaptive and cooperative capabilities can be used to study several security and communication aspects of the smart grid infrastructure both from the attackers and defensive point of view. In this paper, the vital issue of security in the smart grid is discussed, along with a possible approach to achieve this by employing FPGA based Radial Basis Function (RBF) network intrusion.

Keywords: *Cost ratio, Device implant attacks, RBF, Smart grid.*

1. Introduction

Artificial intelligence techniques such as fuzzy logic, Bayesian network, neural networks, and other methods can be employed to enhance the security gaps in conventional IDSs. A fuzzy logic approach was used in [3], in which different variables that influence the inference of an attack can be analyzed and later combined for the decision-making process of a security device. Additionally, if each security device serving as an IDS is aware not only of itself, but also of a limited number (depending on local resources and traffic) of surrounding trusted IDS devices, the alerts that these other devices generate can be used to adjust local variables or parameters to better cope with distributed attacks and more accurately detect their presence. Recently, it has been proposed the use of a Trustworthy Cyber Infrastructure for the Power Grid (TCIPG) that focuses on the security of low-level devices and communications, as well as trustworthy operation of the power grid under a variety of conditions including cyber-attacks and emergencies [4]. TCIPG presents a coordinated response and detection at multiple layers of the cyber-infrastructure hierarchy including but not limited to sensor/actuator and substation levels [5]. In this study, we suggest the vital issue of security in the smart grid, along with a possible approach to achieve this by employing FPGA based Radial Basis Function

Manuscript Received: Oct. 15, 2014 / Revised: Nov. 12, 2014 / Accepted: Dec. 5, 2014
Corresponding Author: hjeong@cdu.ac.kr
Tel:+82-61-450-1229,Fax: +82-61-453-4567
Fire Service Administration, Chodang University, Korea

(RBF) network intrusion.

2. Securing the smart grid

When it comes to security, communication is key point, and information should be properly disseminated to all the parties involved, ensuring that everyone has a clear and common understanding of security needs facilitating their implementation and operation. Training and informing users about processes, study of human behavior, and the perception of events related to the processes is as important to the entire security equation, as it is to engineer a secured infrastructure. As a matter of fact, the greatest security threat to any infrastructure is human error, as opposed to the technology securing it. Communications in the smart grid is a key component of the entire infrastructure, and logically we divide it into two sections, the backbone communications (inter domain), which will carry communications among domains such as those shown in Figure 1, and the communications at the local area network (intra domain) limited by perimeters such as a customer's house, or a distribution facility [6]. It would be important to note that due to current limitations, the focus of research on our test bed will be on intra domain communications, without disregard for future considerations of the inter domain aspect.

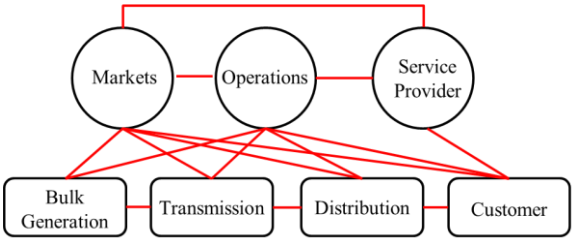

Figure 1. Secure Communication Flow

3. RBF intrusion detection

Artificial intelligence techniques such as fuzzy logic can be employed to enhance the security gaps in conventional IDSs. As shown in Figure 2, a fuzzy logic approach was used in [82], in which different variables that influence the inference of an attack can be analyzed and later combined for the decision-making process of a security device. Additionally, if each security device serving as an IDS is aware not only of itself, but also of a limited number (depending on local resources and traffic) of surrounding trusted IDS devices, the alerts that these other devices generate can be used to adjust local variables or parameters to better cope with distributed attacks and more accurately detect their presence

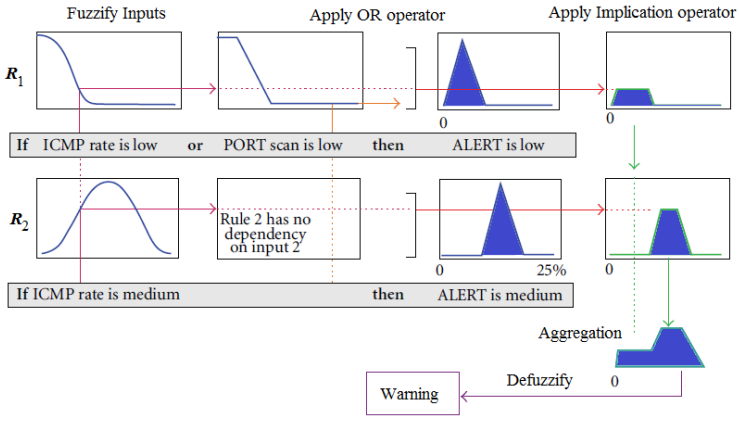

Figure 2. Fuzzy Logic applied to IDS

A RBF neural network for this study consists of three layers, namely the input layer, the hidden layer and the output layer. The input layer takes in the coordinates of the input vector to each unit in the hidden layer. One particular attack is the device implant attack. Let I_r be the ICMP rate, and let P_s be the PORT scan. Then the ratio ($\alpha = I_R/P_s$) directly impacts the frequency of inter-device communication and hence the attack detection rate. Also, let N be the total number of devices operational in the network, and let γ be defined as an estimate on the number of implanted devices within the network. Thus, the input layer takes in the coordinates of the input vector [α, γ]. Each unit in the hidden layer then produces an activation using the radial basis function used in the layer. The general mathematical form of the output units in RBF network is as follows:

$$f(x) = \sum_{i=1}^{h} w_i r_i(x) \tag{1}$$

Here f is the function corresponding to the output unit and is a linear combination of h radial basis functions $r_1, r_2, \ldots, r_h$. In the literature, various algorithms are proposed for training RBF networks, such as gradient descent algorithm and Kalman filtering algorithm [8].

In the RBF networks, each activation function associated with the hidden units is a spherical or symmetrical Gaussian function. Each training sample is given to the network as an input. The learning algorithm places one spherical Gaussian function at each training sample. The general form of the Spherical Gaussian Function network based function approximations is as follows:

$$\hat{f}(v) = \sum_{s_i \in S} w_i \exp\left[-\frac{\|v - s_i\|^2}{2\sigma_i^2}\right] \tag{2}$$

Here v is the input vector, and S is the training samples, and $\|v\text{-}s_i\|$ is the distance between vectors v and s_i. The parameters w_i and σ_i are set by the learning algorithm. We can estimate the value of the density function at s_i as the following below.

$$f(s_i) \approx \frac{(k_1+1)}{S}\left[R(s_i)^m \pi^{m/2} / \Gamma(m/2+1)\right]^{-1} \tag{3}$$

$R(s_i)$ is the maximum distance between s_i and its k_1 nearest training samples, and Γ is the Gaussian approximation function. The value of square bracket is the volume of a hyper sphere with radius $R(s_i)$.

For a training sample s_i, the learning algorithm first conducts a mathematical analysis on a synthesized data set. The challenge is how to figure out the optimal w_i and σ_i values of each Gaussian function. By repeated training the optimal value for σ_i is obtained using the following formula.

$$\sigma_i = \beta\sqrt{\pi}\bar{R}(s_i) / \sqrt[m]{(k_1+1)\Gamma(m/2+1)} \tag{4}$$

Different values of β will give different smoothing effects.

$$w_i = \frac{(k_1+1)\Gamma(m/2+1)}{\lambda^m \pi^{m/2} |S| [\bar{R}(s_i)]^m}, \quad \lambda = \sum_{h=-\infty}^{\infty} \exp\left[-h^2/(2\beta^2)\right] \tag{5}$$

4. Simulation

The simulator for testing the effectiveness of our proposed RBF based scheme was implemented in MATLAB. The simulations were carried out for varying values of α and γ, and its effect was analyzed, and compared with the results by fuzzy reasoning [1]. The total number of devices, N, was varied to study its effect on the detection rate and it was found that for N = 10, 20 and 30 the results are almost identical and therefore we only present results for N=30. Figure 3 denotes the density function for the frequency of communication between the SGI devices for pattern exchange and reconstruction. Figure 2 denotes the density function for attack detection rate. It can be inferred from the figures that an increase in the number of

implanted devices results in a higher cost of communication as the frequency of communication is increased between the devices. However, increasing values of γ also result in better attack detection rate and thus higher attack detection rates. Figure 4 is the overall detection rate by using the suggested RBF network. It has much smaller MSE (0.0001) relative to that of fuzzy logic. It can be observed for lower values of γ, it is preferable to use a higher value of α. This implies that higher total cost needs to be detected to achieve a reasonably higher detection rate. For networks with larger number of implant devices higher values of overall function are achieved with relatively lower cost ratios. It can be inferred from the figure that as the intensity of rogue devices in the network is increased the frequency of communication among devices increases and thus does the communication cost.

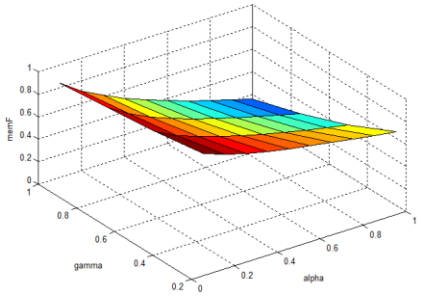

Figure 3. density for frequency of communication

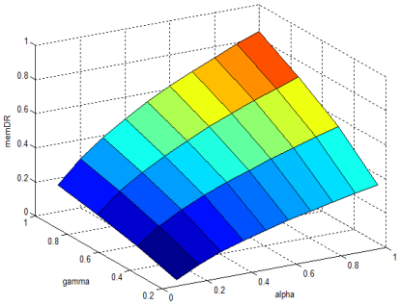

Figure 4. density for attack detection rate

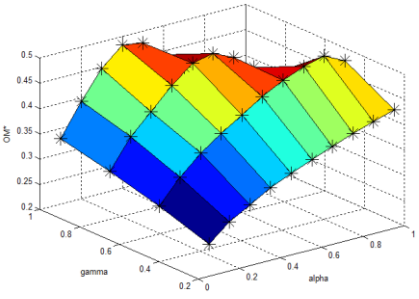

Figure 5. Overall detection rate surface

5. Conclusion

Security for the smart grid is still in the incipient stages, and is the topic of significant research focus. This article addresses the impending problem of securing the smart grid, in addition to the possibility of applying FPGA based neural network intrusion detection for the smart grid. However, it is also vulnerable to malicious attacks of varying types that can severely obstruct its widespread acceptance. In this work we proposed a noble approach based on RBF network, in which the input layer takes in the coordinates of the cost ratio and the estimate on the number of implanted devices, and the output layer is corresponding to overall detection rate. From experimental results obtained it can be concluded that the good value for α lies between 0.4 and 0.6, and the good value for α lies above 0.5 for all combinations of parameter values tested.

References

[1] A. Saif, A. B. Zubair, Fuzzy-based optimization for effective detection of smart grid cyber-attacks, Interna tional Journal of Smart Grid and Clean Energy, vol.1, no.1, Sept., 2012.
[2] D. Simon, Training radial basis neural networks with the extended Kalman filter, Neurocomputing, 48, 455-475, 2002.
[3] Z. Koldovsky and P. Tichavsky. Blind instantaneous noisy mixture separation with best interference-plus-noise rejection. *InPro ceedings of the 7th international conference on Independent component analysis and signal separation*, pp. 730-737(2007).
[4] L. Husheng, M. Rukun, L. Lifeng, and R. Qiu. Compressed Meter Reading for Delay-Sensitive and Secure Load Report in Smart Grid. In Smart Grid Communications, 2010. SmartGridComm 2010. First IEEE International Conference on, (2010).
[5] D. Donoho, Compressed sensing, Information Theory, *IEEE Transactions on*. 52(4), 1289-1306, (2006).
[6] R. C. Qiu. Cognitive Radio and Smart Grid. *Invited presentation at IEEE Chapter* (2010). URL http://iweb.tntech.edu/rqiu.