International Journal of Security and Its Applications
Vol. 10, No. 5 (2016) pp.283-296
http://dx.doi.org/10.14257/ijsia.2016.10.5.27

The Research of AMI Intrusion Detection Method using ELM in Smart Grid

Yuancheng Li [1], Chaochao Zhang[2], Liqun Yang [3]

North China Electric Power University, Beijing, China
[1] ycli@ncepu.edu.cn, [2] forclever_zhc@163.com, [3] ylqncepu@163.com

Abstract

Advanced Metering Infrastructure(AMI) is a critical core component in smart grid. Currently, smart grid employs the same computer networks, which is vulnerable to suffer from cyber attacks. Furthermore, applications of traditional intrusion detection methods are restricted due to the limited computing capacity and potential deployment costs of electrical equipments. This paper proposes an ELM-based intrusion detection method for AMI. We first filter and partition the malicious data, and then different types of invasion are effectively extracted. Finally, we can use Extreme Learning Machine(ELM) for detecting different attack types of malicious data. However, traditional machine learning algorithms such as Support Vector Machine(SVM), which results in a longer training time and poor performance, and moreover SVM is not applicable to multi-class problems. In theory, ELM can approximate any target continuous function and classify any disjoint rejoins. As verified by the simulation results, ELM tends to have better scalability and achieve much better generalization performance at much faster learning speed than traditional SVM.

Keywords: *Advanced Metering Infrastructure(AMI);Smart Grid(SG);Extreme Learining Machine(ELM);Intrusion detection;*

1. Introduction

Advanced Metering Infrastructure (AMI) is a two-way communication framework, which is from the client's device with IP address such as smart meters to electric power company. AMI can provide monitoring and responding requests of communication services, but there are some huge potential threats existed in AMI systems. These threats are possible to affect the deployment and development of smart grid. Therefore, it is very important to study methods in detecting intrusion of AMI.

Aiming at the threats faced by AMI, [1] proposed a secure communication protocol method to against intruders, but the inherent protocol flaw still can be used to permeate AMI system. On this account attacker can control a large number of nodes and achieve the intrusion purpose. Faced with such security crisis, few effective progresses have not been made [2-4]. A comprehensive monitoring solution was proposed in reference [5], but this method costs too much and it is not applicable to widespread deployment.

AMI has its own unique requirements compared with the traditional computer networks, and this makes AMI confront with great challenges range from monitoring to intrusion detection. Possible reasons result in this consequence include: 1) The nodes with limited computing capability and physical space, and the sensors can't be deployed at the smart meters [6]. 2) Although researchers suggest that the sensors based on electric meters should be used, the smart grid provides stable suppliers. So it can avoid a large number of additional expenses along with the deployments of smart meters[7-8]. Therefore, most of the proposed methods applied into Intrusion Detection System are lack of realistic feasibility. By the research of the existing methods, [9] adopted the machine learning

ISSN: 1738-9976 IJSIA

method in predicting attack or analyzing the results. Intrusion detection has become an urgent issue, and anomaly-based detection methods have been proposed[10-11]. But there are not feasible and effective methods for detecting intrusion.

Reference [6] used the probability model for detecting intrusion in AMI system, and verified the AMI behaviors in sequential logic by fourth-order Markov chain. What's novel about this method is that data collector can collect data from configuration introduction. Unlike traditional intrusion detection methods, the proposed model doesn't need to be trained as well as large computing capability. Markov and MemiMarkov process were proposed in response to uncertainty in the network link [12], but the model structure relies on the good parameter estimations and these estimations must come from the empirical data, and it is often difficult to obtain. This method adopt fourth-order Markov chain, and 16 smart meters are deployed at each data collector. If there is no correlation with the smart meters, and the behavior is difficult to detect. If an attacker has access to AMI system and obtain the knowledge of AMI, the attacker can circumvent the detection method. [13] proposed a specialized intelligent analyzer for detecting, and this method obtained a high availability. But this analyzer can't set up sound attacking strategy that it doesn't provide functional analysis for smart grid.

The proposed method collects dataset from smart collector and configuration introduction, and uploads the data to remote intelligent processing center, then analyzing and training these data. Compared with other machine learning algorithms, extreme learning machine （ELM） has high precision and fast training speed. ELM is an easy-to-use learning method with effective single hidden layer feedforward neural (SLFNs). It is a simple structure with low computational complexity and there are fewer parameters to adjust. Using ELM to analyze and train data, then we can generate the detection model to detect the potential malicious behaviors. Therefore, this paper proposes using ELM for the intrusion detection in AMI system.

2. AMI's Structure and Safety Analysis

2.1. AMI System Introduction

Figure 1 shows the structure of the AMI system. There are four major components namely smart meters, intelligent data concentrator, communication networks and data processing centers. Smart meters bi-directionally communicate with data concentrators through a variety of media (ie wired or wireless network) , and intelligent data concentrator bi-directionally communicate with data processing center using the public network. Data concentrator ,connects to LAN and WAN ,mounts on a tower pole, substations and other facilities. It is also a data relay station between smart meters and data processing center. Intelligent data concentrator gather smart meter data to the data center via LAN, and also can send commands and information belong to data processing center to the smart meter and the user .

Data processing center receive data transmitted from the smart data collector via WAN and distribute data to smart meter. Data processing center installed software systems to process the received data and sends the configuration parameters to smart meter and smart data collector. The system converts the data into a database so as to use in other place. Electricity suppliers and consumers can also access the web server provided by data processing center.

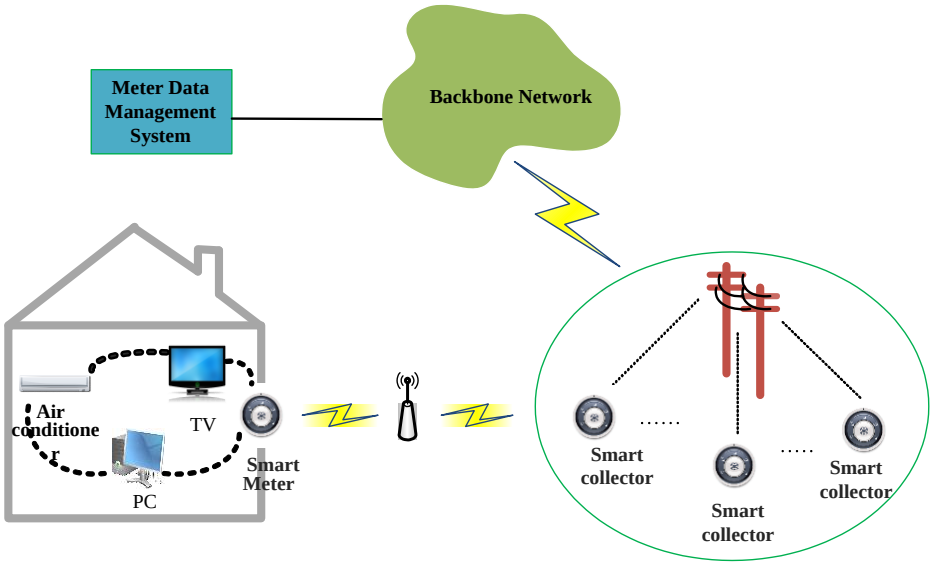

Figure 1. AMI Simulation Architecture Figure

2.2. AMI Communication Network

AMI system uses a fixed two-way communications network, using the communication infrastructure graded. As shown in Figure 1, the entire AMI system has three levels of communication. In [14] the smart grid network architecture is divided into three layer, this paper is basically to take this model. The first part is controllable electrical machine connected to the smart meter constitutes a first-class network ,the network between the smart meter and smart data collectors is the second part, connecting the intelligent data collection network and intelligent data processing center is the third part network .

The first layer of the network and the second network, usually on the speed of communication is not high, so it is the main consideration is the lowest cost to connect to the user. Construction of the network depends communication interfaces provided by smart meters, currently used by more BPL, WiMAX and the PLC. ZigBee is a kind of low-speed short-range wireless network transmission protocol, the bottom is to use IEEE 802.15.4 standards of media access layer and physical layer. The main features of ZigBee are low-speed, low power, low cost ,to support a large number of network nodes ,to support a variety of network topologies, low complexity, fast, reliable and secure[16]. Since 2009, ZigBee uses the IETF IPv6 6 lowpan standard [6] as a new generation of Smart grid-Smart Energy (SEP 2.0) standards, to form a global unified network of integrating with Internet easily to implement end-to-end network communication[17]. This two-tier network where we use ZigBee technology, it has three criteria, namely European standards, North American standards and global standards. Here we use the global standard 2.4GHZ.

The third level network provides communication service between data processing center and intelligent data collector. Intelligent data collection and data processing centers are long-distance transmission, and there is a wide variety of elements, therefore among these components are full of wired and wireless network to improve the availability and reliability. We use wired communication, such as power grid line (PLC), when transferring large amounts of data , and control information transmission is using wireless mode, the paper choose WiMAX communication protocol, mainly because it can provide communication within the range of more than two miles .

Some new vulnerabilities and security issues would be triggered by using the wired and wireless communications technologies for AMI . In order to protect the AMI data transmission confidentiality, integrity and availability, creating a network security strategy

is very imperative. Intrusion Detection System (IDS) provides a technology authenticating network activity, and activities of these networks may be a security policy vulnerabilities. IDS also monitor those activities and network access point, thereby recording and blocking of suspicious behavior and be labeled.

2.3. AMI Security Analysis

AMI is regarded as the most basic realization technology of the smart grid . However, so far, there have been a lot of potential vulnerabilities were found. In the AMI network, smart meters, smart data collector and data processing center, have their own storage space to store large amounts of information. However these information can be easily tampered because of malware implanting. Once these malicious software being embedded, a more serious things ,such as termination of electric meter information transmission, regional power outage etc ,are likely to happen. However the types attacking the each part of the AMI network may also be different.

Wireless network because of its deployment is convenient and low cost, is widely used in smart grid. In the implementation of the smart grid still use a mesh network between the node , which provides an adaptive, multi-path , multi-hop communication and other functions. The mesh network just like multiple communication paths provide redundant communication paths, so that we can compensate for the interruption between nodes and bring communication interruption. ZigBee is a cheap, low-power wireless mesh network protocol, and can be widely deployed and used in a reliable and stable environment. Exposed radio waves of wireless communication technology is very vulnerable to suffer from malicious invasion, such as ZigBee is introduced in [15] suffered a denial of service (DOS) attack, plenty of wireless network attack examples abound, including destroy the integrity of the equipment configuration information, traffic, illegal network operation, tamper with the data, illegal dissemination of customer data, and so on.

Wireless networks are easy detected by attacker, and also vulnerable to attack by man-in-the-middle. Despite some security mechanisms to prevent the illegal use of communication path, but still can't avoid the existence of loopholes. For smart meters, attackers can easily log in to modify its measurement and control command information, this will cause significant error in the power measurement, followed by a serious lack of power supply. Although there are a number of industrial facilities protection rules, but a perfect standard has not yet formed. The main attack types of the first part in AMI network may be the DOS and Probing, namely denial of service attacks and port scan or monitoring; the second part attack type is U2R that unauthorized local super user privileges to access, such as buffer overflow attacks. The third part attack type is R2L, namely remote illegal access to the local host. Experiments of this behind us, in accordance with each part and identify the various categories of attacks targeted experiments, in order to obtain better results.

3. The Proposed Method

3.1. ELM

Extreme Learning Machine(ELM), in 2004, Nanyang Technological University Professor Huang Guangbin proposed, is an easy-to-use and effective single hidden layer feedforward neural network (SLFNs) learning algorithms. The traditional neural network learning algorithm (such as BP algorithm) need to be tuned a large amount of network training parameter, and it's easy to produce the local optimal solution. ELM only need to set up network of single hidden layer nodes, the execution of the algorithm does not need to adjust the network weights of the input and hidden nodes bias, and produce the optimal solution, thus has advantages of fast learning speed and good generalization capability.

ELM is a new type of fast learning algorithm, for a single hidden layer feedforward neural network (SLFNs), ELM can random initialization input weights and bias, and get the output of the corresponding weights. The following detailed introduction of the algorithm.

For a single hidden layer feedforward neural network (SLFNs), assuming that there are N arbitrary sample (X_i, t_i),which

$$X_i = \left[X_{i1}, X_{i2} \ldots, X_{in} \right]^T \in R^n \tag{1}$$

$$t_i = \left[t_{i1}, t_{i2} \ldots, t_{im} \right]^T \in R^m \tag{2}$$

A single hidden layer feedforward neural network with n of hidden layer nodes can be represented as

$$\sum_{i=1}^{N} \beta_i g\left(W_i X_j + b_j \right) = o_j \text{ , j=1, 2, …, N} \tag{3}$$

Which g(x) is the activation function.

$$W_i = \left[w_{i1}, w_{i2}, \ldots, w_{in} \right]^T \tag{4}$$

W_i is the weighted inputs, β_i is the output weights, the i-th hidden layer unit bias is b_i , $W_i \square X_j$ represents W_i and X_j inner product.

A single hidden layer feedforward neural network learning goal is to make the output of the minimum error, can be expressed as

$$\sum_{j=1}^{N} \left\| o_j - t_j \right\| = 0 \tag{5}$$

there are β_i , W_i and b_i to make

$$\sum_{i=1}^{N} \beta_i g\left(W_i X_j + b_j \right) = t_j \text{ , j=1,2, …, N.} \tag{6}$$

It can be expressed as

$$H\beta = T \tag{7}$$

in which H is the output of hidden layer nodes, β is the output weights, T is the desired output.

$$H\left(W_1, \ldots, W_N, b_1, \ldots, b_N, X_1, \ldots, X_N \right) = \begin{pmatrix} g\left(W_1 X_1 + b_1 \right) & \cdots & g\left(W_1 X_1 + b_N \right) \\ \vdots & \cdots & \vdots \\ g\left(W_1 X_N + b_j \right) & \cdots & g\left(W_1 X_N + b_N \right) \end{pmatrix}_{N \times N} \tag{8}$$

$$\beta\left\|H\left(W_i,\hat{b}_i\right)\beta-T\right\|=\min_{W,b,\beta}\left\|H\left(W_i,b_i\right)\beta-T\right\|N \quad , \quad T=\begin{pmatrix}T_1^T\\ \vdots \\ T_N^T\end{pmatrix}_{N\times m} \tag{9}$$

In order to training single hidden layer neural network ,we hope to get W_i , $\hat{b}_i$ and β

$$\beta\left\|H\left(W_i,\hat{b}_i\right)\beta-T\right\|=\min_{W,b,\beta}\left\|H\left(W_i,b_i\right)\beta-T\right\| \tag{10}$$

which i =1,2, …, N , this is equivalent to minimizing the loss function

$$E=\sum_{j=1}^{N}\left(\sum_{i=1}^{N}\beta_i g\left(W_i X_j+b_j\right)-t_j\right)^2 \tag{11}$$

Traditional algorithm based on gradient descent, such as BP algorithm and its variant, can be used to solve this problem, but the basic learning algorithm based on gradient to adjust all the parameters in the process of iteration. In the ELM algorithm, once the input W_i and hidden layer weights bias b_i are randomly determined, the output of hidden layer matrix H is the only sure. Single hidden layer feedforward neural network training can be transformed into solving a linear system $H\beta=T$. And the output weights β can be determined, namely

$$\beta=H^{+}T \tag{12}$$

Where is the matrix H^{+} Moore-Penrose generalized inverse. And β obtained solution may prove the norm is the smallest and uniqueness.

3.2.AMI Intrusion Detection based on ELM

According to the difference attack types for the AMI different level network, as figure 2 shows, for each level network, respectively, we make intrusion detection experiments that attack types is particular.

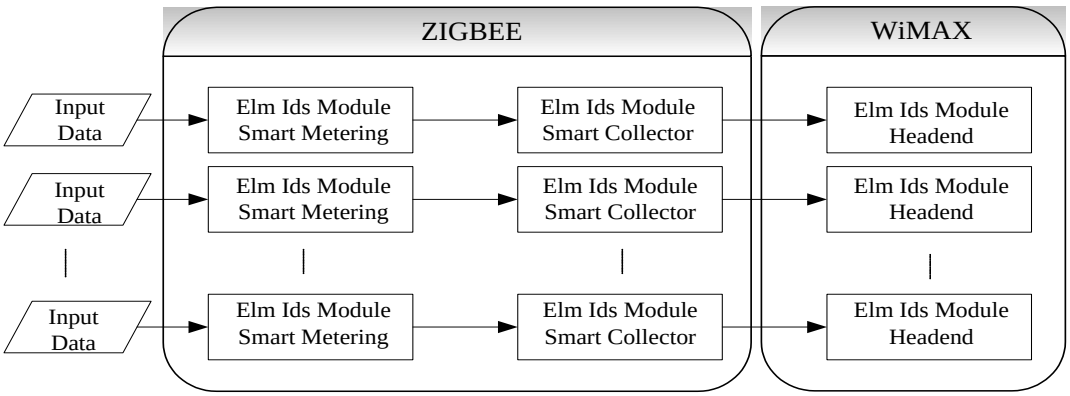

Figure 2. AMI Communication Simulation Diagram

The first level network might suffer from detecting meter data and preventing users from data transmission between consumer smart meter. Except for above attacks, the secondary network mainly suffer from U2R attack, which can modify the data security parameters and control information. In tertiary network, in addition to trapping in the above attack possibly, there are likely to be vulnerable to R2L, this kind of attack change electric meter and control data, even the radio terminal system control commands. A detailed test flow chart shown in Figure 3.

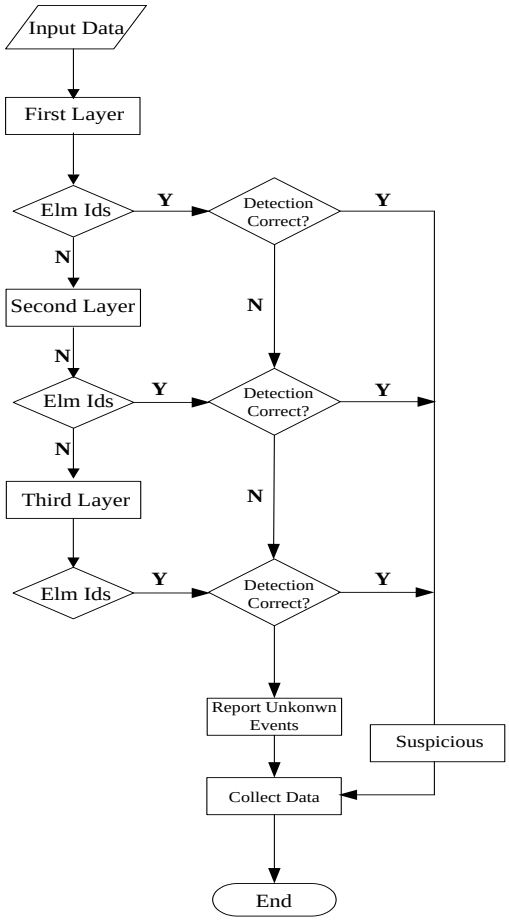

Figure 3. The Flow Chart of AMI Detection based on ELM

4. Analysis of Experiment Results

This section is mainly about the data collection and processing, and then we do simulation experiment aiming at lib-svm and ELM separately and get the simulation data, in the end, according to demonstrating the experiment results graphically, we can obtain the advantage and different of this detection model comparing to other detection algorithms .

4.1 Data Collection and Data Processing

Depending on the different network environment, we divide dataset into the corresponding records. In the first-level network, we mainly detect the intrusion of DDOS and Probing ,which include smurf, ping-sweep, syn flood and ping-of-death and so on. For the second stage network, U2R attack such as guessing password must be focused on.

At the last network, we take R2L attack into consideration expressly, basically, this kind of attack is buffer overflow. Due to large amount of data I wrote linux script for data filtering, which improved the work efficiency. AMI can be as a combination of power system and computer network. So AMI could suffer from all kinds of the computer network vulnerabilities. In other words, intrusion events happened in AMI network can also be found in traditional computer network. Although kddcup99 data is widely used in the computer network to research intrusion detection, but these data characteristics are also accord with aiming to AMI intrusion detection experiments. This is the reason that we decided to use KDDCUP99 data finally.

Mentioned in Figure3 intrusion detection method, in order to detect and prevent intrusion attack, we are deployed in AMI each layer network intrusion detection system (IDS) based on ELM. We use the improved KDDCUP99 data (NSL-KDDCUP) for the attack experiment data.

NSL-KDDCUP is the improved KDDCUP99 dataset, generated by MIT Lincoln lab. KDD99 is widely used for anomaly detection, however it include numerous redundant records. This can make learning algorithms emphasis on redundant data, some records may not be used , and these unused data may be the harmful data, such as U2R and R2L.Therefore,we exploit improved KDDCUP99 dataset(NSL-KDDCUP) for the simulation experiment to increasing the accuracy of the experiment. Table 1 and 2 are the comparison from NSL-KDDCUP and KDDCUP99.

Table 1. Statistics of Redundant Records in the KDD Train Set

	ORIGINAL	IMPROVEMENT	REDUCTION RATE
ATTACKS	3,925,650	262,178	93.32%
NORMAL	972,781	812,814	16.44%
TOTAL	4,898,431	1,074,992	78.05%

Table 2. Statistics of Redundant Records in the KDD Test Set

	ORIGINAL	IMPROVEMENT	REDUCTION RATE
ATTACKS	250,436	29,378	88.26%
NORMAL	60,591	47,911	20.92%
TOTAL	311,027	77,289	75.15%

In AMI's three layers network, we have carried out detection in each layer, and then analyzed the collected experimental data. Experimental data used in this paper is nsl-kddcup, for each layer network we make the appropriate specific intrusion detection, DOS and PROBING attack may commonly occur in the three-tier network, which is the most frequent type of attack. In addition to the former attacks, the second and third layer network may also be subject U2L attacks and R2L attacks, the paper focuses on DOS, PROBING and R2L attacks experiments. In [14], SVM was used for analyzing intrusion detection, this paper also uses lib-svm attack model so that we can compare with the results acquired from this article.

4.2 The Experiment Results Analysis

DOS, PROBING and R2L is the main type of attack, which are the main attack types we used for simulation experiment in this paper, we write linux script to divide the three attack types dataset and do 10 attacks experiments for each attack type.

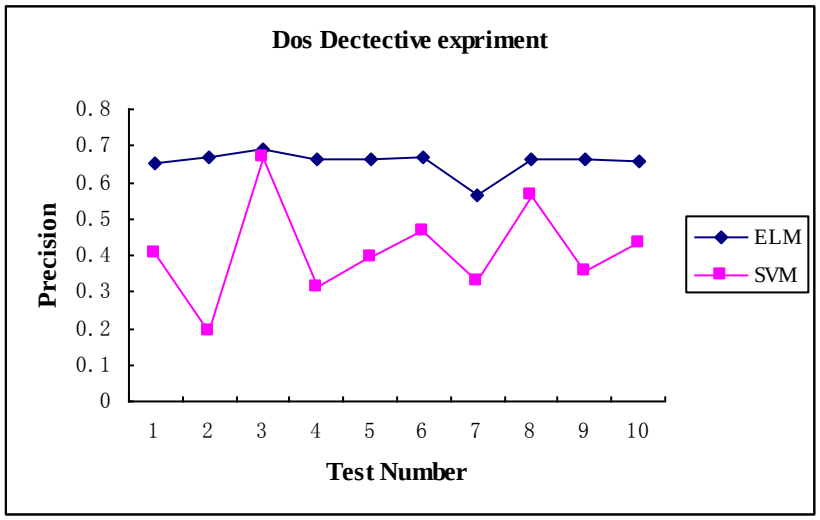

Figure 4. The Contrast Trend Chart of Dos Attack Detection Accuracy

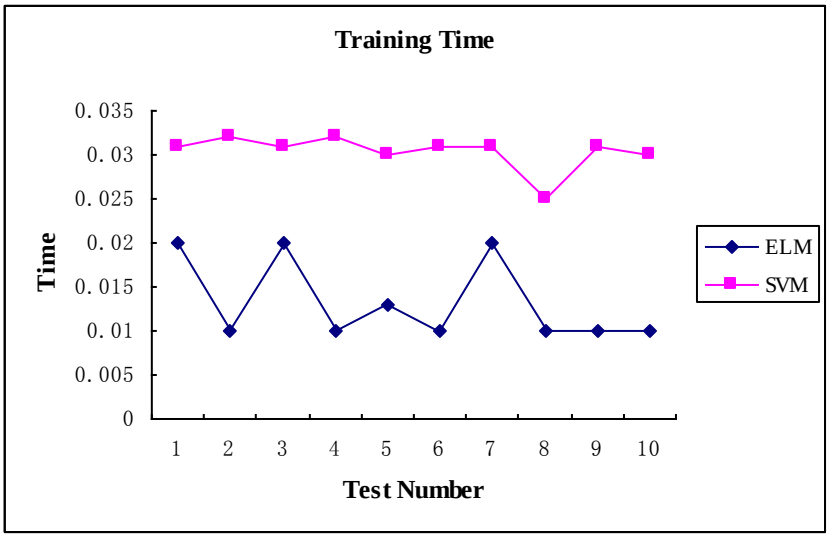

Figure 5. The Training Time Comparison Chart of Dos Attack tType

Figures 4 and 5's data were resulting from the test of DOS attacks, the attack types may occur in the three layer network. According to the level of the TCP/IP protocol, DDOS attacks can be divided into attack based on ARP, IP, ICMP, UDP, TCP and application layer. In Figure 4, distinctly, the precision and stability in the intrusion detection based on ELM(blue curve) is obvious higher than the SVM(red curve). In figure 5, the training time under the ELM detection model is much faster than the SVM. And, furthermore, the test time, another parameter we don't have given in the graphics, is also superior than SVM compared with ELM.

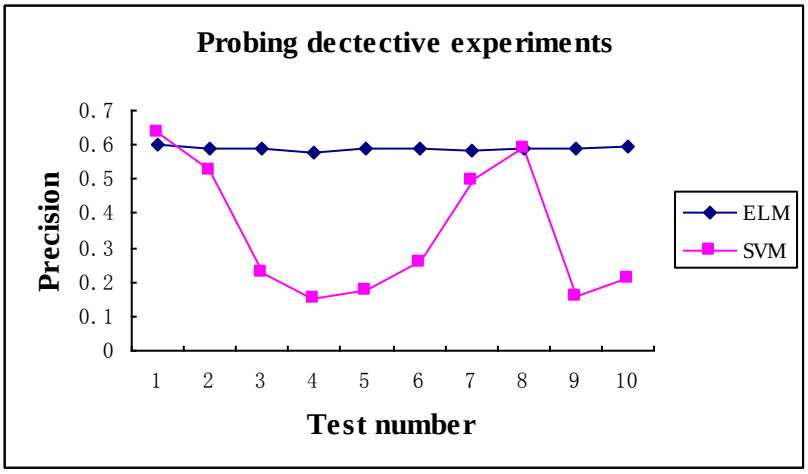

Figure 6. The Contrast Trend Chart of Probing Attack Detection Accuracy

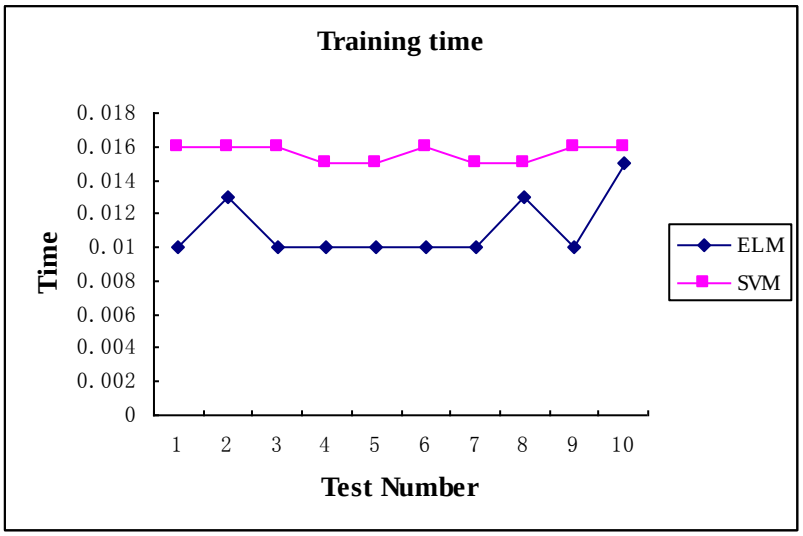

Figure 7. The Training Time Comparison Chart of Probing Attack Type

Figures 6 and 7 are the intrusion detection experimental results of PROBING attack type, probing is the port attack, which generally attack vulnerabilities by scanning port. Attackers can get the system weaknesses from this attack types. That is to say, the port scanning send messages to each port, just send a message at a time. Attackers can get the port state from received response type and find weaknesses. What can be seen from the test data is much higher than SVM compared with ELM, stability is also very good, accuracy is basically maintained at around 60%, while SVM is not very stable, Although sometimes there will be higher than ELM situation, but on the whole ELM is better than SVM and the training time is much less than the SVM, As to handling large amounts of data each day for AMI system, time is particularly important.

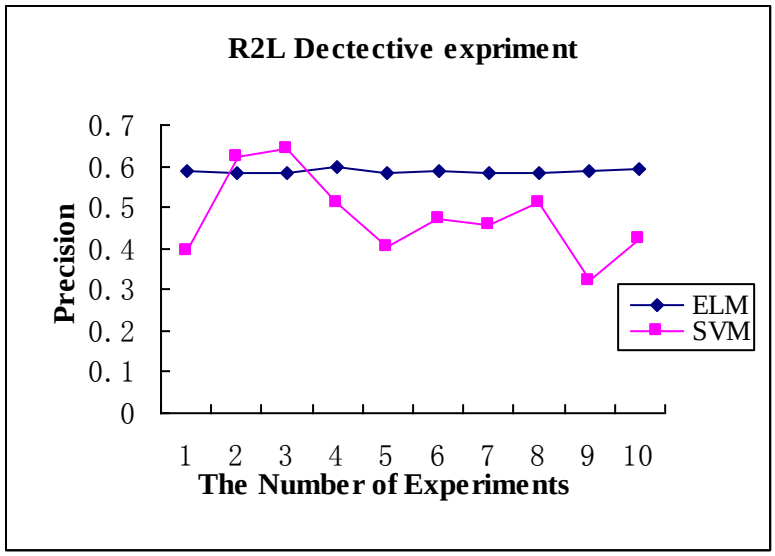

Figure 8. The Contrast Trend chart of R2L Attack Detection Accuracy

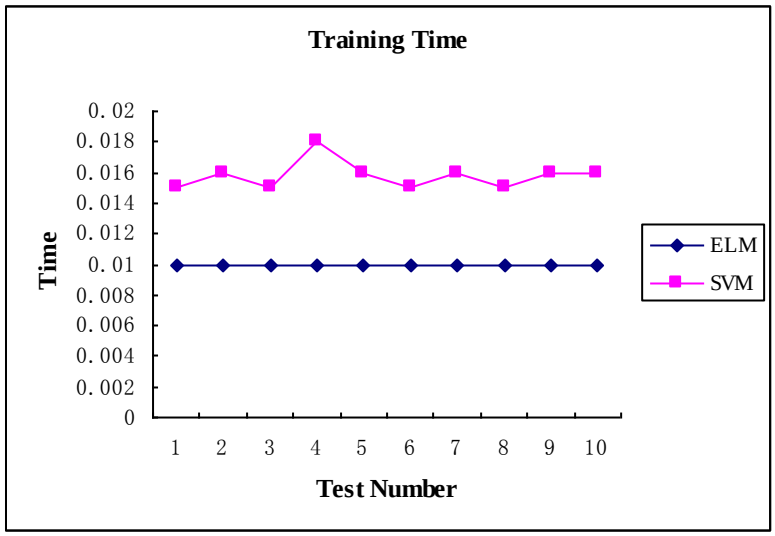

Figure 9. The Training Time Comparison Chart of R2L Attack Type

Figure 8 and 9 are intrusion detection research about R2L attack type, R2L is a remote user attacks, generally, caused by remote control vulnerability without the user's password security. Attackers can remotely log on the computer, and then use the computer account and weak passwords to access and operate the computer, such as long-range attacks against 3389 port. The experiment conclusion is same as before, Intrusion detection systems based on ELM, whether in testing and in training time accuracy, are better than SVM. Precision means detecting the error rate, clearly we can get that ELM-based intrusion detection systems is much higher than SVM from all the figures.

5. Conclusion

AMI system is a combination of electric power network and the traditional communication network, The outstanding characteristic of this paper is the intrusion

detection based on ELM. The research content ranges from AMI system's weakness and vulnerability to network security Analyzing and then put forward the research methods against network attack. Firstly, this paper introduce the operation mechanism aimed at the Electric power AMI system. Secondly，we set out to describe the intrusion detection method based on the extreme learning machine. The innovative point of this detection method is firstly putting forward the intrusion detection method based an ELM, which is used to determine the effectiveness of the attack. On account of the particularity of the AMI system network, the determination of AMI attack is very challenging. The system has the advantages of relatively higher on time and accuracy. The system can be easily applied to the AMI system based on other communication protocol, and has good extensibility.

References

[1] S Mclaughlin, D Podkuiko, S Miadzvezhanka S, et al. "Multi-Vendor Penetration Testing In The Advanced Metering Infrastructure[C]". Computer Security Applications Conference. (**2010)**: pp. 107-116.

[2] F. M. Cleveland. "Cyber security issues for advanced metering infrastructure (AMI)." In IEEE Power and Energy Society General Meeting - Conversion and Delivery of Electrical Energy in the 21st Century (**2008**)

[3] Idaho National Laboratory (INL). NSTB assessments summary report: Common industrial control system cyb- er security weaknesses, May **(2010).**

[4] S MCLAUGHLIN,., D PODKUIKO,., S MIADZVEZHANKA, ., A DELOZIER, ., AND P. MCDANIEL,. "Mul- tivendor penetration testing in the advanced metering infrastructure." In Proceedings of the 26th Annual Computer Security Applications Conference, (ACSAC) **(2010).**

[5] R. Berthier, ., and W Sanders,. "Specification-basedintrusion detection for advanced metering infrastructures." In IEEE 17th Pacific Rim International Symposium on Dependable Computing (PRDC) **(2011).**

[6] M.Q. Ali, E. Al-Shaer, M.Q. Ali. "Probabilistic model checking for AMI intrusion detection[C]" Smart Grid Communications (SmartGridComm), 2013 IEEE International Conference on. IEEE, (**2013**): pp.468 - 473.

[7] ,M. A. FAISAL, Z. AUNG, J WILLIAMS., AND, A SANCHEZ. "Securing advanced metering infrastructure using intrusion detection system withdata stream mining." In Proceedings of Pacific Asia Workshop on Intelligence and Security Informatics (PAISI) (**2012**).

[8] Y. ZHANG, L. WANG, W. SUN, R GREEN., AND, M. ALAM "Distributed intrusion detection system in a multi-layer network architecture of smart grids." IEEE Transactions on Smart Grid **(2011).**

[9] M Jun, Coll. of Inf. Sci. & Eng., J Zuo Univ., J Zuo, China ; "Feng Shuqian Research of intrusion detection system based on machine learning Computer Engineering and Technology(I-CCET)", (**2010**) 2 nd International Conference on Vol. 7.

[10] F. M Cleveland. "Cyber security issues for advanced metering infrastructure (AMI)." In IEEE Power and Energy Society General Meeting - Conversion and Delivery of Electrical Energy in the 21st Century (**2008**).

[11] S Mclaughlin, D Podkuiko, S Miadzvezhanka, et al. "Multi-Vendor Penetration Testing In The Advanced Metering Infrastructure[C]//" Computer Security Applications Conference. (**2010**): pp. 107-116.

[12] M Q Ali, E Al-Shaer. "Configuration-based IDS for advanced metering infrastructure[C]". Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security. ACM, (**2013**): pp. 451-462.

[13] M A Rahman, P Bera, E Al-Shaer. "Smart Analyzer: A noninvasive security threat analyzer for AMI smart grid[C]" INFOCOM, 2012 Proceedings IEEE. IEEE, (**2012**): pp. 2255 - 2263.

[14] Y Zhang; L Wang; W.Sun; Green, R.C.; Alam, M. "Distributed Intrusion Detection System in a Multi-LayerNetwork Architecture of Smart Grids Smart Grid", IEEE Transactions on (**2011**).

[15] W Somkaew, S Thepphaeng, C Pirak. "Data security implementation over ZigBee networks for AMI systems[C]" Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI-CON), 2014 11th International Conference on. IEEE, (**2014**): pp. 1–5.

[16] Q Zhang; S Pirak, Y; Z Cui "Application and analysis of ZigBee technology for Smart Grid Computer and Information Application (ICCIA)," 2010 International Conference on (**2010**).

[17] Y Yun, Q Yi, S Hamid. "A secure and reliable in-network collaborative communication scheme for advanced metering infrastructure in smart grid[C]" Wireless Communications and Networking Conference (WCNC), 2011 IEEE. IEEE, (**2011**): pp. 909 - 914.

Authors

Yuancheng li, received the Ph.D. degree from University of Science and Technology of China, Hefei, China, in 2003. From 2004 to 2005, he was a postdoctoral research fellow in the Digital Media Lab, Beihang University, Beijing, China. Since 2005, he has been with the North China Electric Power University, where he is a professor and the Dean of the Institute of Smart Grid and Information Security. From 2009 to 2010, he was a postdoctoral research fellow in the Cyber Security Lab, college of information science and technology of Pennsylvania State University, Pennsylvania, USA.His current research interests include Smart Grid operation and control, information security in Smart Grid.