Signature-Based Method and Stream Data Mining Technique Performance Evaluation for Security and Intrusion Detection in Advanced Metering Infrastructures (AMI)

Ziaeddin Najafian*, Vahe Aghazarian, Alireza Hedayati
Department of Computer Engineering, Islamic Azad University, Central Tehran Branch, Tehran, Iran.

* Corresponding author. Email: zia.najafian@gmail.com
Manuscript submitted August 10, 2014; accepted March 8, 2015.
doi: 10.17706/ijcee.2015.v7.879

Abstract: Advanced Metering Infrastructure is a system for collecting, measuring and analyzing power energy use which beside the mentioned parameters is responsible to transmit this information between elements of this network. One of the problems of processing in these networks and the most main installation duct is security in the network. Beside the precautionary operations used for achieving security in AMI, today the usage of intrusion detection systems (IDS) is paid attention as a second blocker defense against network security attacks. According to variations of Intrusion Detection techniques in network, many different designs for applying IDS and AMI have been suggested so far. In this paper we aim to evaluate the newest techniques of operation in abnormality-based IDS in Intrusion Detection and security achievement in AMI against signature-based IDS operation with the use of standard criteria in equal situations experimentally. According to the results from this research we can see that the signature-based methods are not useful in IDS systems applied in AMI network. The measurement on anomaly-based IDS which is using data mining techniques showed very hopeful results. However these methods need some improvements in order to achieve their best place.

Key words: Intrusion detection, network IDS, signature, anomaly, advanced metering infrastructure (AMI), stream data mining, performance evaluation, snort.

1. Introduction

Whenever we discuss about transferring information in computer systems, computer networks play a great role. In recent years, in Power science there has been discussed about smart gird (SG) networks installation. According to the importance of energy management and paying attention to environment, today Power Industry is about to encounter a great change in Electronic Resource Management and Energy Management. Power experts try to make smart girds from traditional power distributer networks and traditional management of these networks with the use of this smart gird and take more control on producing and using energy. The term Smart Grid is commonly used to refer to an advanced electrical system in which new and more sustainable models of energy production, distribution and usage will be made possible by incorporating, in the power system, pervasive communication and monitoring capabilities, as well as distributed and autonomous control and management functionalities [1]. The networks as the main most infrastructures of SG empower it to exchange the most advanced information about sensors, metering data and control data of different devices in a two-sided connection between user and producer;

in other words the SG network is a set of computing sources like different sorts of different devices and tools that are connected by different transmission networks. Smart grid applications pose a number of research challenges and opportunities.one of the most important challenge in Smart grid is security and privacy issues in smart metering [1]; Power smart girds are very wide and complex and are made of different subsystems and this huge complexity among these systems causes an increase in security threat; because of being two-sided, Inter-Operable and software oriented nature of smart girds, SG is really poor in front of cyber-attacks.

One of the most important and main elements of a smart gird is the Advanced Metering Infrastructure or AMI. AMI is now one of the most advanced metering systems in the world. This system includes smart metering devices, telecommunication networks and data bases which modernize the power network and have a lot of advances for users and distributor companies and in fact is a connector between user and distributer. The most important operation of AMI is creating a two-sided connection in order to collect, evaluate and analyze data about usage of energy by helping the dynamic power market installation, energy power usage management, self-empowering distribution network and providing a connecter for other systems [2].

With a surface glance, we can conclude that the most basic infrastructure used in AMI is different computer networks used in it. In this paper, we will discuss about providing security in AMI solutions which focus on connectional infrastructures. The Iranian power minister tries to install AMI system in the form of FAHAM method [3] and according to hierarchal architecture provided by OpenMeter and the power distribution network in Iran is going to become automatized, according to sensitivity of interactive information in AMI, if the cyber security is not predicted, these problems might occur because of the greater problems in the whole network national security and even social crises. So the AMI security discussion is one of the most basic and discussable in installing smart girds in a way that a number of experts know security as the bottleneck and the disadvantage of smart girds. So the organizations NIST and FERC think about cyber security as an important task in their framework. The definition of security of network is summarized in protection which includes two general bases. The first basis is prevention which means all the prevention solutions for threats against network and the next one is Detection and Reaction which refers to threat detection and showing reactions against them; so this is really important that except prevention security solutions in networks, these systems such as firewall, detection techniques, decoding etc., some methods for detection and prevention of intrusion in such a complex network will be expected. Attack or intrusion is a set of illegal procedures which may come from inside or outside of a network and it denies security aspects–accuracy, security and accessibility. In this paper, the solution which is used for protecting AMI from Intrusion attacks is using intrusion detection systems. Today IDS is used as an advanced tool in intrusion detection and prevention in computer systems. The Intrusion Detection System is defined to hardware, software or a combination of them which is used for informational computer systems has the responsibility for identifying the efforts for attacking networks and gives necessary alarms. IDS has three responsibilities: collecting information, identifying or analyzing data, reacting and reporting the attack. Generally the main goal in detecting intrusions is detecting illegal use, abuse, and damaging systems and computer networks caused by internal users or external attackers [4].

Amir Faisal *et al*. in [5], claimed that signature-based intrusion detection systems are not relevant for AMI network. The authors of this paper told that lack of accuracy and plentitude of problems in signature-based intrusion detection systems and their costly updating procedure and also the difference between the dynamic nature of AMI network and definition of signature, caused superiority on anomaly-based IDS in comparison with signature-based intrusion detection systems in AMI. Following this claim, the authors of this paper have done some examinations to prove their claim in order to show the operation of anomaly-based IDS, but their problem is that they did not provide a practical comparison between their

solution and signature-based solutions. So here we aim to provide an examination similar to signature-based IDS in order to complete the valuable work of Amir Faisal *et al*. and then examine the accuracy of the claim. Here the OpenMeter standard architecture for AMI network is considered and anomaly-based IDS which are using stream data mining are placed with a special harmony. The authors of this paper tried to Benchmark their architecture on KDD Cup 1999 Dataset and reached some results with the help of MOA tools which are used for stream data mining and with utilizing different sorting algorithms. Considering this situation, we intend to examine what Amir Faisal *et al.* have done, with one of the signature-based IDS called snort, on the same dataset and compare the two results. So moreover to complete their work, we can evaluate the accuracy of the raised claim about superiority of anomaly-based IDS in comparison with Misuse-based IDS. Here our scale or meter for comparison includes FPR (False Positive Rate) and FNR (False Negative Rate).

2. Literature Review

Up to now, there have been several researches on intrusion detection systems for special networks and cyber infrastructures. One of the recent published works on metering IDS operation in physical cyber system stability is [6], [7]. In these papers, the trouble detection issue in infrastructure network has been studied; or in the work of Valenzuela *et al*. [8] the network security issue related to power distributer networks and in general, the SCADA control network has been studied, but unfortunately there have been a few researches on IDS use in AMI. Yet, we can consider works such as research of Bethier *et al.* [9] as a starting point in this issue. In this paper, types of IDS and its possible elements have been discussed. Then Berthier and Sanders in [10] added more information to the existing ones. Grochochi *et al.* in [11] survey the various threats facing AMIs and the common attack techniques used to realize them in order to identify and understand the requirements for a comprehensive intrusion detection solution. The threat analysis leads to an extensive "attack tree" that captures the attackers' key objectives (e.g., energy theft) and the individual attack steps (e.g., eavesdropping on the network) that would be involved in achieving them [11]. With reference to the attack tree, they show the type of information that would be required to effectively detect attacks. They also suggest that the widest coverage in monitoring the attacks can be provided by a hybrid sensing infrastructure that uses both a centralized intrusion detection system and embedded meter sensors [11]; but the first research in which the utilization of types of intrusion detection system techniques was followed seriously is the work of Amir Faisal *et al*. in [5]. Amir Faisal *et al*. claimed that signature-based intrusion detection systems are not relevant for AMI network. The authors of this paper told that lack of accuracy and plentitude of problems in signature-based intrusion detection systems and their costly updating procedure and also the difference between the dynamic nature of AMI network and definition of signature, caused a superiority on anomaly-based IDS in comparison with signature-based intrusion detection systems in AMI. Following this claim, the authors of this paper have done some examinations to prove their claim in order to show the operation of anomaly-based IDS.

3. Types of Intrusion Detection Systems

Intrusion detection systems are divided into three main categories in terms of detection and identification: signature-based, anomaly-based and protocol-based. The signature-based techniques are placed in a larger group called misuse-based techniques. By signature we mean a set of regulations according to which an operating attack can be detected in a network. Each signature contains some information which shows the tasks to device and whenever the passing traffic is matched with the signature pattern, an alarm message will be created and the network manager will be acknowledged of an intrusion. One of the most popular signature-based IDS is snort [12]. This system is presented as open-context. It is tried to pay attention to the elements such as practicality, simplicity, and flexibility in snort architecture.

In signature-based method there is no dynamicity and only the defined attacks will be detected, but in anomaly-based or behavior-based intrusion detection method the network behavior will be modeled. If we want to define Anomaly, we can say that it is deviation from norms [13]. It is an eventual anomaly in the system which is abnormally working and operates in a way that we call it a subversive behavior. An anomaly-based IDS draws a schema of usual patterns to itself. Each behavior or event which is very far from this schema is considered as a possible subversion and a threat against the network and usually the event which occurs with a more or less than its normal frequency is considered abnormal [13], [14].

4. Advanced Evaluation of Anomaly-Based Intrusion Detection System in AMI

The work of Amir Faisal *et al.* [5] is considered as the first movement in utilization of anomaly-based IDS in AMI. In general, what has been done in [5] includes using anomaly-based IDS in AMI network architecture and intrusion simulation and rating different intrusion detection algorithms about it. The architecture used for AMI in this paper is the presented architecture by OpenMeter. In the work of Amir Faisal *et al.* for each of defined triple elements of AMI network, an IDS device is designed including respectively M-IDS for advanced metering device, H-IDS for Headend, and DC-IDS for data centralizer. These IDS systems use data mining technique and they are interconnected.

Table 1. Distribution of Connecting Records in the Whole KDD 99 Dataset

Transaction Type	*Number of Training Records*	*Number of Testing Records*
Normal	972781	60593
R2L	1073	11980
U2R	105	4437
DoS	3883370	229853
Probing	41102	4166
Total	4898431	311029

Evaluating the operation of intrusion detection processes needs to use a particular architecture and a special dataset is used in order to meet this goal. The problem that Amir Faisal *et al*. faced in this case and we faced it as well during this work, is lack of real dataset or formal AMI dataset; so in order to this, a sample dataset named Kdd Cup 1999 is used which is specially designed for examining intrusion detection software. This dataset is a copy of the dataset used in evaluating DARPA intrusion detection system program which is created according to the request of DARPA with the help of Lincoln laboratory in MIT University. Kdd 99 includes almost 4GB of dump data in TCP network and training traffic collected from network traffic in 7 weeks. This dataset has exactly 5,209,460 connectional records and its data have 41 features for examining and teaching. There is 24 attacks in these data categorized into 4 main types (see Table 1): Denial of Service (DoS), illegal access from a long distance machine (R2L) such as guessing the password, illegal access to local infra-user's rate (root) such as different kinds of buffer overflow attack, search.

In this research work, one of the new data mining techniques called stream data mining is used. In recent years, stream data have been widely taken into account instead of static data. Daily increase of these data such as marketing data in hypermarkets, mineral resources exploration data such as oil, Bourse and internet attacks, caused an increased activity in this research field of study. In fact, using data mining science for exploring knowledge from big data stream is known as a technique in stream data mining. The main features of stream data include:

- **Volume:** Volume refers to the quantity of data. Stream data are Open Ended; so they can't be saved at a time and a special space. This makes data stream a non-data set so learning according to these data must be additive like.
- **Velocity:** variety refers to the diversity of data types, velocity refers both to how fast data are generated and how fast they must be processed:

1) **Speed:** The high speed of data stream limits the process time for each sample, in other words, before the new sample, the previous sample must be processed already.
2) **Concept drift:** The velocity component of big data stream introduces the idea of concept drift within the learning model. In predictive analytics and machine learning, the concept drift means that the statistical properties of the target variable, which the model is trying to predict, change over time in unforeseen ways. This causes problems because the predictions become less accurate as time passes. We can consider concept drift as a change in class distribution in stream data. For instance, in scopes such as climate forecast regulations and internet attacks, concept draft includes a change in used patterns for climate forecasting or types of internet attack.

The data being exchanged in an AMI network have a high volume, they have been produced and should be processed at a high speed and the concept drift problem lies in them, so we can consider them in big data stream scope.

For stream data mining process with data stream mining classifier feature in MOA or massive object analysis Java software is used. This software is produced with the support of Waikato University (the popular data mining software called Weka is produced at the same university). In this software, classifier and arrangement algorithms are used which can solve the Concept-drift problem. In MOA, there are 16 arrangement algorithms the 4 most accurate of which is used in [5]. The procedure in MOA is in a way that after classifying input data, practicality from existing class should be evaluated. Each classifier algorithm needs a trainer in MOA and almost all of the trainers come from Hoeffding Tree (1):

$$\varepsilon = \sqrt{\frac{R^2 \cdot Ln(\frac{1}{\delta})}{2n}} \tag{1}$$

This limit which is known as Chernoff limit states that if α is a random variable with maximum value of R and we have n direct observation of this variable and the average of these observations is $\bar{\alpha}$. The limit states that with the possibility of 1-δ, the real average value is more than $\bar{\alpha}$-ε. The main idea of this method is accessing to the distance between two classification errors instead of accessing only to the number of errors. The improvements of this method are development in the average distance between two errors and improvement in predictions; and it means increase in accuracy and decrease in FNR and FPR in an IDS.

The IDS quality determination criterion is its ability in intrusion detection. A desirable intrusion detection system is one whose degree of error is the least possible. In this case there are three practicality criterions for IDS [13]:

- Accuracy: Accuracy is a metric that measures how correctly an IDS works, measuring the percentage of detection and failure as well as the number of false alarms that the system produces [15].
- FPR: The false positive rate (FPR) is the proportion of normal instances incorrectly classified as anomalous over the total number of normal instances contained in the test data set [15].
- FNR: The false negative rate (FNR) can be defined for the normal class. In other words, the percentage of the samples considered as normal however they are anomalous sample. It means that IDS didn't report a real attack.

In work of Amir Faisal *et al.* [5], after explaining the algorithms and presenting the examination conditions and examining the dataset, the results will be explained for the three mentioned scales (see Table 2):

Table 2. The Results of Examinations [5]

Classifier Algoritm	Accuracy (%)	FPR (%)	FNR (%)
Leveraging Bagging	98.33	0.78	5.15
LimAttClassifier	98.24	0.78	5.26
OzaBagAdwin	98	1.14	5.31
Single Classifier Drift	97.74	1.07	6.79

5. Proposed AMI Architecture Embedding Signature-Based Intrusion Detection Systems

In the last section we evaluated related works, especially work of Amir Faisal *et al*. in [5]. As explained in introduction, in this section we intend to repeat their experiment but in the case of one of popular signature-based IDS systems called snort.

The architecture considered for this, is a schema of AMI OpenMeter architecture. There are two types of meters in open meter architecture. The first type is ordinary meters that transmit data from PLC to DCU and then DCU has the task to transmit them by WAN network to headend, the second type are the meters with the ability to connect to WAN independently (usually by GPRS) and transmit their data to Headend directly which are usually known as point to point Meters. This is clearly shown in Fig. 1. According to the provided architecture in Fig. 1, the considered structure for testing is provided in Fig. 2. In this experiment, providing a same condition as [5], three types of Signature-Based IDS have been standardized. The three main elements of this AMI architecture include Smart Meter, Data Concentrator (DC) and Headend Server, three of which are considered as a computer because in most structures of AMI, a light-weighted Linux is installed on Meter and DC device and Headend is a server computer which has a version of Windows Server or Linux or other operation systems.

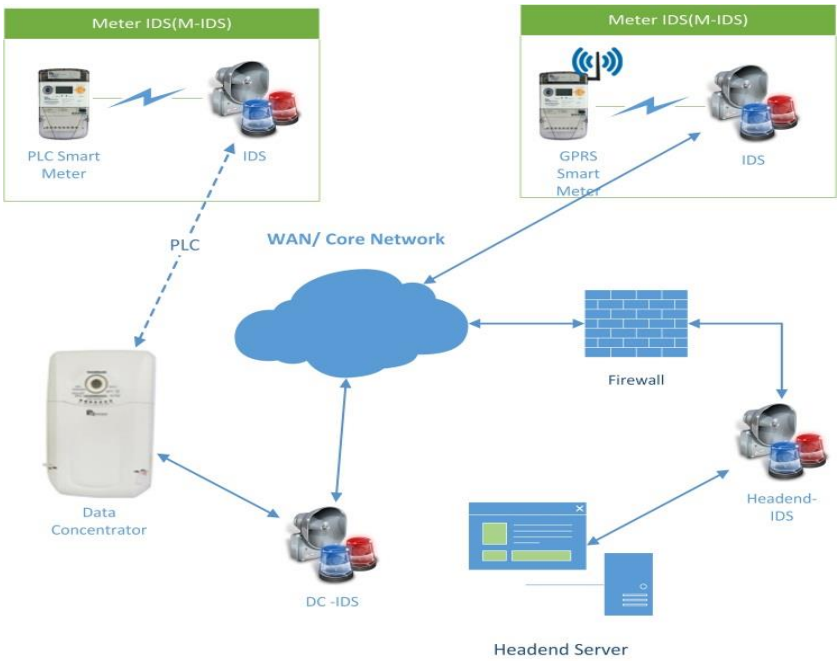

Fig. 1. Architecture of whole IDS in AMI.

6. Experimental Results and Discussions

6.1. Experimental Setup

One of the unique features of snort is its lightweight which besides making it popular, it makes snort installable on almost every operating system. In snort official website, different types of snort versions for all Linux, windows operating systems and even CentOS is provided. So in order to make it easy, a LAN with three computers is provided and in this network which is a model of AMI network, each computer is considered as one of the main elements of AMI triple network Fig. 2.

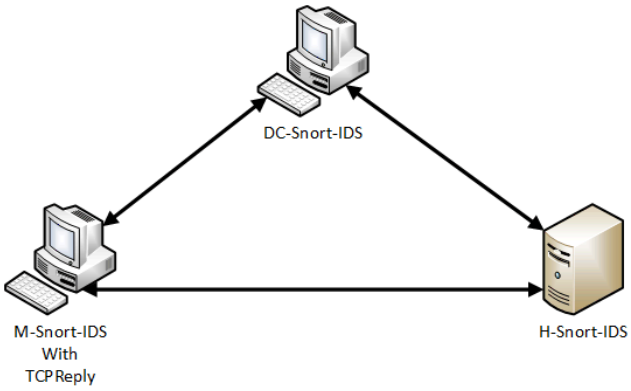

Fig. 2. The considered architecture for examination.

A version of snort 2.9.4.6 is installed on each computer and all of the computers use XP windows and they all have Intel Core i3 processor and the minimum RAM among them is 1GB. So for example, Meter computer with a M-snort installed on it represents and alternates for M-IDS in paper architecture [5]. Note that snort needs WinPcap software to be run, so after installing snort, the last version of WinPcap is also installed. snort can operate in three situations and record its output differently. In this examination, snort operates as a complete intrusion detection system and is programmed in a way that Logs and outputs must be saved in MySQL data base and also the rules used in it are validated and presented by reference website. Due to that, these packages and other information will be saved in MySQL data base, in order to have illegible outputs and analyze the results, we use ACID auxiliary software which is designed for this purpose and snort.

6.2. Dataset Used in Examination

The dataset used in this examination is exactly the same as the dataset used in [5], which is KDD Cup 1999 Full Dataset with the features mentioned in Table 1. However there is a difference here that is, the data records are saved so they don't have the stream feature. In order to solve this problem and simulate data stream in the designed LAN network, a software was needed to simulate data stream. So the 3.4.4 version of TCPReply software was installed on a computer known as Meter. This software simulates online traffic of network packages by injecting its own packages. It means that, this software is able to circulate and placed the information of current packages in Kdd 99 dataset same as when they have been taken out from the main network. So the data stream will be simulated in the considered network like shown in Fig. 1.

6.3. Analyzing the Experiment Results

Here the results will be evaluated and analyzed and presented according to three metrics of accuracy, FPR and FNR to be compared with the previous results the next time. The primary result of this examination is presented in Table 3. The Detection Rate (D.R) is measured with the help of (2) in this table. In (2), x stands for type of attack sample, such as normal, probe and etc.

$$D \cdot R = \frac{DetectedAttack(x)}{TotalNumOfAttack(x)} \quad (2)$$

Table 3. Primary Examination Results with Snort

Transaction Type	Total Number of Records ()	Number of Detected Records	Detection Rate (%)
Normal	1033374	775031	75
R2L	13053	6345	49
U2R	4542	2839	62.5
DoS	4113223	1287438	31.2
Probe	45268	12081	27
Total	5209460	2083734	40

In Table 3, the information about the number of samples detected by snort from KDD 99 full collection is given. The previously defined values cannot be identified from this information, because as mentioned before, an IDS will report an attack wrongly and vice versa. It means that a normal sample will be reported as an attack which is called false positive or an attack sample will be reported as a normal one which is called False Negative. For metering FPR and FNR confusion matrix is used. According to the results, the confusion matrix of this examination for different types of samples in dataset is shown in Table 3. The unit of numbers in the table is sample number. For example, the number gained from the box of Normal row and R2L column means that 4100 samples identified as normal samples were in fact R2L type.

Table 4. Confusion Matrix in Examination with Snort

		Normal	**R2L**	**DoS**	**Probe**	**U2R**	**Total**
Number and Type of Detected attacks	Normal	702111	4100	62914	3851	45	775031
	R2L	1014	5112	52	120	47	6345
	DoS	67039	4901	1215402	96	0	1287438
	Probe	2737	235	0	998	11	12081
	U2R	1726	473	0	0	640	2839
	Total						2083734

With the use of confusion matrix, (see Table 4), the triple considered values can be metered. Accuracy is a metric that measures how correctly an IDS works, measuring the percentage of detection and failure as well as the number of false alarms that the system produces. If a system has 80% accuracy, it means that it correctly classifies 80 instances out of 100 to their actual classes.

Note that the accuracy used in this paper is for comparing with other similar works that is general accuracy. For calculating general accuracy, sum of total number of correct detected samples of all types must be divided into sum of total detected samples. In confusion matrix the value of accuracy is equal to sum of values in core diameter into total detected samples that is equal to 92.34%.

For calculating FPR and FNR we have, if consider sum value of orange boxes in Table 4 as α (False Positive), the value of yellow box as ψ (True Positive), sum value of green boxes as β (False Negative) and sum value of white boxes as λ (True Negative), according to (3) and (4), value of FPR is equal to 5.6 and value of FNR is equal to 9.17.

$$FPR = \frac{\alpha}{\alpha + \lambda} \tag{3}$$

$$FNR = \frac{\beta}{\beta + \psi} \tag{4}$$

6.4. Discussion and Evaluation on Results

Now the results from anomaly-based Intrusion Detection System by Amir Faisal *et al*. in [5] and results from snort examination which is a signature-based intrusion detection system is comparable in Table 5.

Table 5. Comparison between Anomaly-Based IDS Results and Signature-Based Snort in AMI Network

Intrusion Detection Method	Algorithms and Tools	Accuracy (%)	FPR (%)	FNR (%)
Anomaly based (MOA Algorithms)	Leveraging Bagging(LB)	98.33	0.78	5.15
	LimAttClassifier (LAC)	98.24	0.78	5.26
	OzaBagAdwin (OBA)	98	1.14	5.31
	Single Classifier Drift (SCD)	97.74	1.07	6.79
Signature based	Snort IDS	92.34	5.6	9.17

In the first look it seems that snort is the loser for several rounds in this difficult competition! So the stated claim in [5] can be accepted. Signature-based IDS is not suitable in sensitive networks such as AMI; because this low accuracy and high rate of error means that the network is always vulnerable to attack and losing its information. As shown in Fig. 3, the accuracy of snort is almost 92.5% which seems to mean a good accuracy percentage, but it operated much lower than the poorest anomaly-based algorithm in the Single Classifier Drift examination. It means that almost 80 out of 1000 evaluated samples is not detected correctly and if we consider even 30 of them as a dangerous attack, the security of a sensitive network such as AMI will be endangered. In terms of FRR, the difference between signature-based IDS and anomaly-based IDS is almost high Fig. 4.

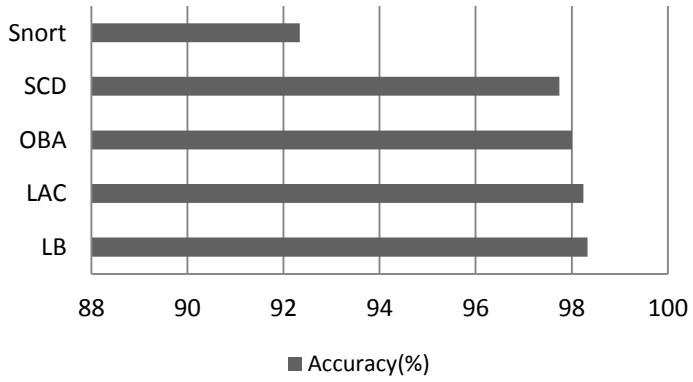

Fig. 3. Comparing accuracy level chart.

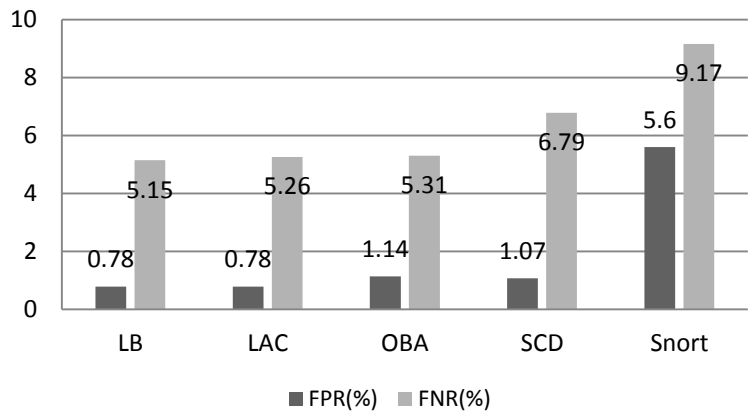

Fig. 4. FPR and FNR comparison among the anomaly based classifiers and custom snort.

FPR criterion can indicate IDS operation accuracy and does not necessarily indicate security danger for system and only increases the number of nonsense alarms. But for FNR, the case is more serious because here, the more dangerous samples will be considered in terms of normal IDS and enters the network Fig. 4. As shown in Fig. 4. FNR is higher than FPR. One reason could be Dataset anomalies and other reason could be caused due to the learning process in anomaly based intrusion detection algorithms. Again in this case, signature-based IDS with less difference than other cases, failed from anomaly-based IDS which is using stream data mining system.

7. Conclusion

In this paper, the relative advantage of anomaly-based intrusion detection Systems which use stream data mining system in comparison with signature-based intrusion detection systems such as snort, for being used in advanced metering infrastructures in distribution network has been proved. We tried to make a just and equal comparison about them with designing a just and equal competition. In this paper we tried to cover the problems of previous works in proving the advantage of operating anomaly-based IDS in comparison with signature-based IDS by using previous works in IDS design in order to use in AMI network and make an equal situation for practical examination of signature-based IDS. So it can be concluded that using anomaly-based IDS in AMI, despite having some problems, is more trustable, dynamic, and fast in comparison with signature-based IDS. However anomaly-based IDS which uses stream data mining technique, already needs improvement in time and speed because in a complex, wide, and high tech network such as AMI, the least security problem may cause irrecoverable damages. This research work can be used by scholars and the people who want to step in this field and make an improvement in the security of new networks such as AMI.

8. Future Works

- One of the problems of smart gird research is lack of AMI Dataset for examinations and simulations which seems normal according to novelty of AMI. So one of future works can be creating from an AMI dataset.
- According to the high practicality of Stream data mining in Intrusion Detection Systems, it is nice to install and design an open-context project in the field of intrusion detection system design which is using stream data mining technique exactly the same as snort open-context project.
- Designing AMI intrusion detection system as one of its main modules.
- According to development of AMI networks, more researches will be done in AMI security with the use

of Intrusion Detection Systems. So creating a Test bed will be suitable for this purpose. However this needs some infrastructures which will be operated with the help of Industry.

- If using IDS in AMI become a fashion in future and these two systems integrate, IDS must be equipped with AMI risk management and error tolerance features as a vital module.

Acknowledgment

This research was sponsored by PaudRaad Industrial Group and Advanced Metering Infrastructure R&D unit of Paya Energy Company.

References

[1] Conti, M. (January 2014). Present status and future challenges. *Computer Communications*, *37*, 1-4.

[2] Arian, M., Soleimani, V., Abasgholi, B., Modaghegh, H., & Gilani, N. S. (March 2011). Advanced metering infrastructure system architecture. *Proceedings of 2011 Asia-Pacific Power and Energy Engineering Conference* (pp. 1, 6, 25-28).

[3] Monenco Iran Consulting Engineers. (2007). Specification of general, economical, functional, technical and communicational requirements for the advanced metering infrastructure (AMI). Farasamaneh Hooshmande Andazegiri va Modiriateenergy (FAHAM), Iran Energy Efficiency Organization, Electricity and Power Ministry, Islamic Republic of Iran. form http://www.iransg.com/saba_content/media/image/2011/06/2203_orig.pdf

[4] Sample, C., & Schaffer, K. (Jan.-Feb 2013). An overview of anomaly detection. *IT Professional*, *15(1)*, 8, 11.

[5] Faisal, M. A., Aung, Z., Williams, J. R., & Sanchez, A. (2012). Securing advanced metering infrastructure using intrusion detection system with data stream mining. *Proceedings of Pacific Asia Workshop of Intelligence and Security Informatics* (pp. 96-111). Kuala Lumpur, Malaysia.

[6] Tartakovsky, A. G., Polunchenko, A. S., & Sokolov, G. (Feb. 2013). Efficient computer network anomaly detection by change point detection methods. *IEEE Journal of Selected Topics in Signal Processing*, *7(1)*, 4, 11.

[7] Mitchell, R., & Chen, I. (March 2013). Effect of intrusion detection and response on reliability of cyber physical systems. *IEEE Transactions on Reliability*, *62(1)*, 199-210.

[8] Valenzuela, J., Wang, J., & Bissinger, N. (May 2013). Real-time intrusion detection in power system operations. *IEEE Transactions on Power Systems*, *28(2)*, 1052, 1062.

[9] Berthier, R., & Sanders, W. H. (12-14 Dec., 2011). Specification-based intrusion detection for advanced metering infrastructures. *Proceedings of 2011 IEEE 17th Pacific Rim International Symposium on Dependable Computing*, 184-193.

[10] Berthier, R., Sanders, W. H., & Khurana, H. (4-6 Oct., 2010). Intrusion detection for advanced metering infrastructures: Requirements and architectural directions. *Proceedings of 2010 First IEEE International Conference on Smart Grid Communications* (pp. 350-355).

[11] Grochocki, D., Huh, J. H., Berthier, R., Bobba, R., Sanders, W. H., Cardenas, A. A., & Jetcheva, J. G. (5-8 Nov., 2012). AMI threats, intrusion detection requirements and deployment recommendations. *Proceedings of 2012 IEEE Third International Conference on Smart Grid Communications* (pp. 395-400).

[12] Padmashani, R., Sathyadevan, S., & Dath, D. (27-29 Nov., 2012). BSnort IPS Better Snort Intrusion Detection / Prevention System. *Proceedings of 12th International Conference on Intelligent Systems Design and Applications* (pp. 46-51).

[13] Scarfone, K., & Mell, P. (Feb. 2007). NIST guide to intrusion detection and prevention systems (idps). National Institute of Standards and Technology, Special Publication 800-94.

[14] Jyothsna, V., Prasad, V. V. R., & Prasad, K. M. (August 2011). A review of anomaly based intrusion detection systems. *International Journal of Computer Applications*, *28(7)*.

[15] Fiore, U., Palmieri, F., Castiglione, A., & de Santis, A. (December 2013). Network anomaly detection with the restricted Boltzmann machine. *Neurocomputing*, *122(25)*, 13-23.

Ziaeddin Najafian received the BS degree in information technology engineering from University of Kurdistan, Islamic republic of Iran, in 2011. Currently, he is working toward his MS degree in software engineering, Islamic Azad university, Central Tehran branch, Iran. His research interests include network security, intrusion detection, support vector machines, swarm intelligence, firewall, power systems security, smart grid security and AMI Security.

Vahe Aghazarian received the MSc and Ph.D. degrees in computer engineering from Azad University, Sciences and Research Branch, Tehran, IRAN, in 2002, and 2007. He obtained the top student awards in MSc and Ph.D. courses. He is currently an assistant professor in the Department of Computer Science, Azad University, Central Branch, Tehran, Iran. In 2008, Dr. Vahe Aghazarian won the top researcher award in Azad University, Central Tehran Branch. His current research interests are in the areas of communication and networking, Internet QoS, microprocessors, and information technology.

Alireza Hedayati received his Ph.D. degree in computer hardware engineering from Azad University of Tehran Science and Research Branch in 2011. He is currently a faculty member of Computer Hardware in Azad University of Tehran Central Branch. His research interests include network security, optical networks, next generation network, network management and QoS.