Supervised Machine Learning based Routing Detection for Smart Meter Network

Md Raqibull Hasan[1], Yanxiao Zhao[2], Guodong Wang[3], Yu Luo[4], Lina Pu[5], and Rui Wang[6]

[1] Department of Electrical and Computer Engineering
South Dakota School of Mines and Technology, USA.
[2] Department of Electrical and Computer Engineering
Virginia Commonwealth University, USA.
[3] Department of Computer Science
Massachusetts College of Liberal Arts, USA.
[4] Department of Electrical and Computer Engineering
Mississippi State University, USA.
[5] School of Computing Sciences and Computer Engineering
University of Southern Mississippi, USA.
[6] College of Information Engineering and Automation
Civil Aviation University of China, China.
{yzhao7}@vcu.edu

Abstract. It is known that the Ad hoc On-Demand Distance Vector (AODV) routing protocol for smart meter network is vulnerable to denial of service attacks (e.g., black hole attack and selective forwarding attack). In this paper, we introduce supervised machine learning to detect unknown routing attacks under AODV. There are two problems in the existing intrusion detection algorithms. The first problem is that the existing intrusion detection algorithms are mainly applied to a specific and known type of routing attack, which no longer work for unknown attacks. The second one is that constant thresholds are commonly used for detection. To overcome these two problems, we introduce a supervised machine learning based detection approach. To implement supervised machine learning, three steps are involved. First, features and target estimations are selected from malicious AODV behaviors in smart meter network to generate training data sets. Second, we assign a suitable classifier including support vector machine, k-nearest neighbors and decision trees to fit the training and predicted data. Third, we update our training data to maintain a dynamic threshold. Simulations are conducted using Python3.6 to evaluate the accuracy and the time overhead of our proposed supervised machine learning model. The simulation results show that the decision trees algorithm assures 100% accuracy with minimum time overhead to detect routing attacks in AODV.

1 Introduction

Smart grid is perceived as the next generation of power delivery infrastructure, which is fully integrated with emerging communication and information

MOBIMEDIA 2019, June 29-30, Weihai, People's Republic of China

DOI 10.4108/eai.29-6-2019.2283068

technologies, to support bi-directional communications. A major component of smart grid is smart meter networks, which are composed of smart meters and Data Aggregation Points (DAPs) [1] [2]. Smart meters are installed at smart homes or commercial sites, and are responsible for monitoring, reporting, and billing electricity consumption, as well as power demand and renewable power generation information to the utility server [3] [4] [5]. It is reported that nearly 50 million smart meters, about 43 percent of the country, have been installed and are running across USA as of 2014 [6]. This number is expected to continually rise in the near future. DAPs, deployed in neighborhoods, are responsible for relaying information between smart meters and the utility server. Smart meters and the associated DAPs communicate via wireless communications and form smart meter networks. Smart meters are reported vulnerable to security attacks and frequently become attack targets in smart grid. Accordingly, this paper investigates the detection of malicious behaviors on smart meters.

Since most smart meters are not able to directly communicate with their associated DAP due to long distances, they must count on some relay meters for packet transmission to the DAP via multiple hops. Therefore, a smart meter network can be viewed as a mesh network, which requires a routing protocol to find the most efficient path for a packet to the associated DAP. Currently, no specific routing protocol is standardized for smart meter network and Ad hoc On-Demand Distance Vector (AODV) routing protocol is commonly adopted in smart grid. The AODV routing protocol is vulnerable to different forms of routing attacks. Typical routing attack is denial of service including flooding, black hole and selective forwarding attacks. Under attacks, packets are frequently dropped or the data transmission can be delayed, corrupted or even blocked, which significantly damages the network performance. Therefore, routing attack detections under AODV for smart meter network is a critical issue.

There are two problems in the existing work for AODV routing attack detections. The first problem is that the majority work focus on a specific and known routing attack (e.g., black hole or flooding or selective forwarding detection) [9] [10] [11]. It is known that different types of attack exhibit distinct behaviors. The most approaches detect malicious behaviors targeting specific anomalous behavior by adding new control packets or modifying routing protocols [12] [13] [14]. These approaches are not able to detect other types of attack if exist. Furthermore, in real systems, it is very likely that the specific kind of attacks is unknown. The second problem is that a constant threshold is commonly used for detection. If an attacker somehow knows the threshold, it can easily break the intrusion detection system and utilize the routing information to access data packets.

To tackle the two above-mentioned problems, we propose a new solution that integrates supervised machine leaning and dynamic thresholds. Machine learning has been widely used in a variety of field, but the investigation on routing attack detections is under explored. To fill the gap, our paper introduces machine learning into attack detection that is able to detect several possible types of malicious behaviors by using a specific classifier. Training and updating

are two important features of a machine learning model. These can be achieved by loading new training data or updating training data after a certain time interval. Three test classifiers are evaluated including Support Vector Machine (SVM), k-Nearest Neighbors (KNN) and Decision Tree (DT) algorithm, in terms of detection accuracy and time overhead. In terms of threshold setting, a dynamic threshold is considered in our detection approach. As a result, our approach only generates false positive for a short particular time interval if this occurs.

The main contributions of our papers are summarized as follows.

- The first contribution is to generate possible malicious and normal data based on different kinds of routing attacks in AODV. We consider the malicious behavior as feature or input vectors. Note that, the data sets for input vectors are our training or sample data. Based on each input vector, we assign corresponding target or output vector values.
- The second contribution is to test different classifiers (i.e., SVM, KNN and DT) using training and sample or predicted data. Then, we apply cross-validation method to test those classifier for randomly selected data sets.
- The third contribution is to evaluate those classifiers in terms of detection accuracy and time overhead analysis. The accuracy of any particular classifier represents the percentage of true positive or percentage of fit data. In addition, the time overhead analysis of any classifier notifies whether or not the classifier is applicable for smart meter network under AODV.

The rest of the paper is organized as follows. Section 2 introduces the related works. Section 3 identifies the malicious behaviors from routing attacks in AODV. Section 4 describes the algorithm of supervised machine learning. Section 5 evaluates and analyzes three different classifiers based on simulation results. Section 6 concludes the overall research.

2 Related Works

In this section, we introduce the state-of-the-art of routing attack detection in AODV and smart meter networks.

A comprehensive survey of smart meters and their utilization was described in [15], which focused on key aspects of the metering process, different stakeholders' interests, and the technologies used to satisfy stakeholders' interests. Furthermore, this paper highlighted challenges as well as opportunities due to the advent of big data and the increasing popularity of cloud environments. A behavior-rule based intrusion detection system was proposed in [16] for securing head-ends, DAPs and subscriber energy meters of a modern electrical grid. It demonstrated that a behavior-rule based intrusion detection technique can effectively trade false positives for a high detection probability to cope with sophisticated and hidden attackers to support ultra-safe and secure applications.

A literature survey of machine learning and data mining methods for cyber analytic was described in [17]. It analyzed the complexity of machine learning/data mining algorithms, discussed challenges of using machine learning/data

mining for cyber security, and provided some recommendations on when to use a given method. In [18], the necessity of process automation was interpreted in the Intrusion Detection Systems (IDS) considering critical infrastructures and machine learning techniques in IDS solution. In addition, different levels of automation were studied and it outlined a methodology to endow critical scenarios with preventive automation.

Various supervised machine learning classification techniques were described in [19]. This research provided proper guidelines to the interesting research directions and suggested potential combinations. In [20], the background of Advanced Metering Infrastructure (AMI) and identify major security requirements were discussed. Specifically, an attack tree based threat model was first presented to illustrate the energy-theft behaviors in AMI. In order to provide a deep understanding of security vulnerabilities as well as solutions in AMI, and shed light on future research directions, some open challenges and potential solutions were explored. A new intrusion detection system based on k-nearest neighbor (referred to as k-NN below) classification algorithm in wireless sensor network was proposed in [21]. This system separated abnormal nodes from normal nodes by observing their abnormal behaviors, and analyzed parameter selection and error rate of the intrusion detection system. This paper emphasized on the design and implementation of the detection system which achieved efficient, rapid intrusion detection by improving the wireless AODV routing protocol.

The machine learning techniques for detecting attacks from internet anomalies were studied in [22]. Their proposed machine learning framework consisted of two major components: Genetic Algorithm (GA) for feature selection and Support Vector Machine (SVM) for packet classification. Based on their experimental results, their proposed framework outperformed current real world MDS. A new SVM approach, named Enhanced SVM, was proposed in [23]. It combined two methods in order to provide unsupervised learning and low false alarm capability. It is similar to that of a supervised SVM approach. The experimental results verified that the proposed approach was comparable to real world Network Intrusion Detection Systems (NIDS).

3 Feature Identification from Routing Attacks under AODV

Malicious attack in AODV routing is a serious issue and challenges the routing layer to find a reliable route between a source to a destination. In this section, we introduce two common types of Denial of Service (DoS) attacks including black hole attack and selective forwarding. Their distinct features will be extracted as well.

I. Blackhole attack: Black hole attack is the most severe attack because a malicious meter will trick source meters to send packets to it and then intentionally drops all received packets. Normally, in the default AODV, a source smart meter initiates a fresh RREQ and receives a reply from the destination

(i.e., DAP). During a black hole attack, a malicious meter replies to the source with a tampered high destination sequence number, which claims itself as the shortest path to destination. As a result, the source meter is tricked to send packets to the malicious meter, which will then drop the packets intentionally. It can be seen that unmatched sequence number is an important feature to identify whether or not a blackhole attacker exists throughout the network.

II. Selective forwarding: Unlike black hole attackers, a malicious meter behaves normally and does not tamper the destination sequence number, when the routing information exchanges between a source and destination. However, when the source selects the malicious meter as a relay meter according to a regular routing process, the malicious meter intentionally drops the data packet. The severity of selective forwarding is less than a black hole attack and it is more challenging to detect it. In a wireless environment, relay nodes can trace the packet drop feature within its transmission range. The number of data packet drops is potential information to identify a selective forwarding attack.

To detect possible attacks of the three above-mentioned types, we have extracted three important features including the number of RREQ packets in a certain time interval or RREQ rate, the number of unmatched destination sequence number bearing in numerous RREPs, and the number of data packet drop from one-hop neighbors as input variables for analyzing supervised machine learning classifiers. In addition, time interval is considered as the fourth input feature because smart meters always maintain certain time interval for both scheduling and On-demand operation.

4 Algorithm for Detecting Routing Attack Types

In real systems, it is very likely that when operations become abnormal, we know attacks exist, but we have no clue about the real cause of abnormality or the attack type. Therefore, in this section, we propose to apply machine learning to malicious detection and determine the type of malicious behaviors. Two attack types are assumed present including black hole attack and selective forwarding, as introduced in Section 3,

As illustrated in Fig. 1, assume there are two potential attack types, denoted by y_1 and y_2, in the smart meter network. Let's take black hole attack (y_1) and selective forwarding attack (y_2) as examples. We know each attack exhibits unique features, as summarized in Section 3. To detect black hole attack, unmatched sequence number is an important feature to identify whether or not the black hole attacker exists throughout the network. To identify selective forwarding attack, the number of data packet drops is a potential indicator.

Based on the malicious features of different attack types, we select two important features for detection. These two feature vectors are x_1 and x_2, i.e., x_1 = unmatched sequence number (true or false) and x_2 = number of packet drops (integer values). The decision outputs are as follows: y_1 = black hole attack detection (true or false), depending on inputs x_1; and y_2 = selective forwarding

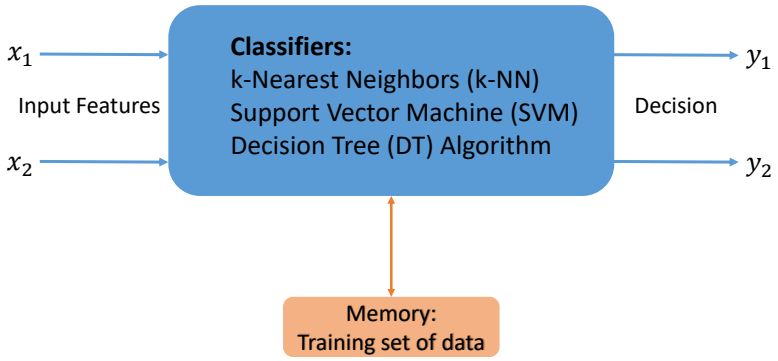

Fig. 1. Intrusion detection module using machine learning algorithm.

attack detection (true or false), which depends on input x_2. Each feature vector contains equal number of data and group of feature vectors make different combination of training set data. For a clear understanding, the mapping of the feature vectors and the classier outputs are summarized as below. Note the feature vectors are x_1 and x_2, and the classifier outputs are y_1 and y_2:
x_1 = Number of unmatched sequence number.
x_2 = Number of data packet drops.
y_1 = Black hole attack detection. Result depends on the input x_1.
y_2 = Selective forwarding attack detection. Result depends on the input x_2.

From the above-mentioned explanation, we have extracted the malicious features and assign big data sets, which are called trained data or sample data, for those features based on different malicious scenarios in smart meter networks. Besides that, we can also determine the output for different combination of those features. Since we have predefined sample data and limited discrete output, in machine learning this kind of system is referred to as supervised for sample data and classification system for limited discrete output. For supervised and classification system, the implementation of machine learning algorithm is easier, applicable and reliable for identifying the detection problems. Algorithms of K-Nearest Neighboring (k-NN), Support Vector Machine (SVM) and Decision Tree (DT) can be employed and will be evaluated. The following will briefly introduce these three machine learning algorithms.

k-Nearest Neighbors(k-NN): This classifier makes the decision or classifies the data set based on the minimum Euclidean Distance from k-neighbor points. For example: if we have $k = 3$, then each time our classifier will first calculate the distance of those three neighbor points from our target point. Among those three distances, the neighbor point with minimum distance is the optimal point for our consideration. Assume, x_i is the input vectors and y_i is the output vectors, then the Euclidean distance, $D_{Euclidean}$ for k neighbors as follows [21]:

$$D_{Euclidean} = \sqrt{\sum_{i=1}^{k}(x_i{}^2 - y_i{}^2)} \quad (1)$$

In our case, all features are of integer data type, therefore, any prediction data containing fraction number is considered as malicious data.

Support Vector Machine (SVM): For training data sets, we need to define a relevant kernel that separates the nonlinear feature or space vector into different linear features or space vectors. After that, it makes a linear decision surface and the classifier takes the decision of any considerable or new point based on the position (above or below) of that point from decision surface. For example: if we have two features like x and y, the feature sets form $x^2 + y^2$ non-linear space in the $x - y$ space. Then, our kernel defines another feature $z = x^2 + y^2$ and now we have x, y and z three different linear features. Therefore, these data sets are linearly separable and makes a linear decision surface. The classifier makes a decision about new points based on the relative distance from the decision surface. However, in smart meter networks, most of the feature vectors are non-linearly separable, so the linearization of the decision surface significant increases false positive.

Decision Tree (DT) Algorithm: Initially, we split our data sets into two trees and then, keep going on as long as we can reach our decision point. This algorithm sometimes makes an over-fitting problem for a complex decision surface where the data sets are very close. Obviously, if the data sets are not linearly separable, decision tree algorithm shows better accuracy. In our case, all data sets are of integer type and we have a long separation among data sets. Therefore, there is no over-fitting problem in our system. In the beginning, we need to define some labels that create a non-linear decision surface. Using that labels, the classifier apply nested if-else condition until it reaches a decision point.

In the following, we will describe the sequential procedure of supervised machine learning algorithm.

Step 1: Assign a set of features to identify different malicious behaviors. Each feature vector contains equal number of data, and group of feature vectors make different combination or training set data.

Step 2: After defining training set of data, we need to implement a classifier on those data sets. In our case, we have implemented three different types of classifier: k-NN, SVM, DT algorithm.

Step 3: After fitting the training set of data, we need to define some out of sample data or new data, which are called testing data in machine learning. We will test our detection module in three ways:

i. By applying the training data and determines the detection accuracy.

ii. By applying cross-validation method which first randomly selects the 20 to 30 percent of training data and then determines the detection accuracy.

iii. By applying out of sample data but known output and determines the detection accuracy.

Step 4: Based on the testing results in terms of data accuracy and time overhead for different classifier, we assign the best classifier for that particular system.

5 Simulation Results

In this section, we have generated maximum possible data sets based on the normal and malicious behaviors of AODV routing. As we described in section 4, unmatched destination sequence number (i.e., inequality between Fake and normal RREPs), and data packet drop are the most common indicators or input features for separating different routing attacks. As mentioned previously, we have considered two routing attacks (i.e., blackhole and selective forwarding). Considering maximum possible malicious routing data, we train and test three different default classifiers (i.e., Support Vector Machine (SVM), k-Nearest Neighbors (k-NN) and Decision Tree(DT) Algorithm) under Scikit-Learn module of Python 3.6. Initially, these classifiers are evaluated based on the detection accuracy or the percentage of true positive decision. Furthermore, the time overhead analysis for each classifier is conducted and the results will suggest which one is most applicable for smart meter networks.

5.1 Accuracy Evaluation of Different Classifiers

We first evaluate the detection accuracy for the three different classifiers (i.e., k-NN, SVM and DT) to detect different attacks. Since different classifiers use different parameters, x-axis is set as the corresponding parameter for each classifier (i.e., k nearest neighbors for k-NN, C for SVM and minimum number of split for DT). We test the detection accuracy of these three classifiers under two attack types (i.e., black hole and selective forwarding attacks) and the result is shown in Fig. 2. From the figure, we can conclude that the detection accuracy of DT algorithm is not affected by parameters and always shows 100% accuracy. The detection accuracy of SVM classifier is poor when C is small, but it can achieve satisfied accuracy by increasing the number of C. By contrast, the k-NN classifier did not exhibit comparable detection accuracy with the other two classifiers. It shows a high rate of false positive with the increase of value k. In other words, under a high value of k, the accuracy goes down because of the over-fitting problem.

5.2 Time Overhead Comparison of Different Classifiers

Second, we evaluate the time overhead of three classifiers. Results in Fig. 3 show the time overhead under two attack types (i.e., black hole and selective forwarding attacks). This figure suggests that DT requires less time overhead and k-NN is next to it. By contrast, the maximum time overhead of SVM (around 28s in Fig. 3) is almost 1000 times higher than SVM. By analyzing detection

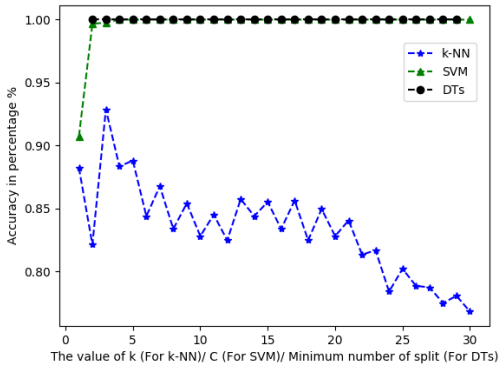

Fig. 2. Accuracy evaluation of different classifiers considering blackhole and selective forwarding routing attacks.

accuracy and time overhead, it is noticed that SVM and k-NN show a trade off, more or less, between accuracy and time overhead. However, DT algorithm still maintains minimum overhead (less than 25ms as shown in Fig. 3). As a summary, the DT algorithm outperforms k-NN and SVM in terms of detection accuracy and time overhead, which is most applicable to AODV routing attack detection in smart meter networks.

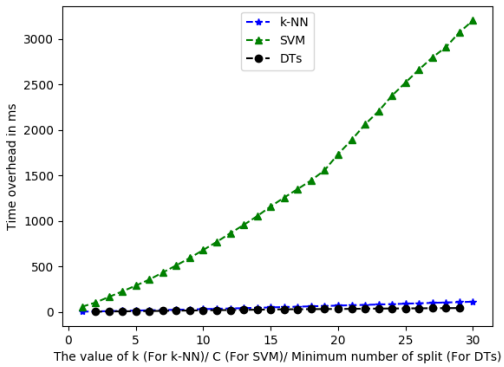

Fig. 3. Time overhead analysis of different classifiers considering blackhole and selective forwarding routing attacks.

6 Conclusion

This paper implements supervised machine learning algorithm for different routing attacks detection under AODV routing in smart meter network. To analyze and evaluate our proposed machine learning approach, we utilized three existing classifiers (i.e., SVM, k-NN, DT algorithm) under Scikit-Learn module in Python3.6. Two important performance metrics including detection accuracy and time overhead are examined. The simulation results reveal that the DT algorithm obtains the maximum accuracy (100%) with the minimum time overhead (less than 25ms). Conversely, SVM and k-NN show a trade off, more or less, between detection accuracy and time overhead. In conclusion, the DT algorithm exhibits the maximum fitness on our training data sets and shows the minimum delay to execute detection module which is embedded with each smart meter. More attack detections including flooding attacks will be investigated as future work.

References

1. Yanxiao Zhao, Suraj Singh, Guodong Wang, and Yu Luo: Performance evaluation of black hole attack under AODV in smart metering network. International Conference on Communications and Networking in China, 159-168 (2016).
2. Guodong Wang, Yanxiao Zhao, Jun Huang and Winter, Robb M: On the data aggregation point placement in smart meter networks. IEEE International Conference on Computer Communication and Networks (ICCCN), pp. 1–6, 2017.
3. Amjad Anvari-Moghaddam, Hassan Monsef, and Ashkan Rahimi-Kian: Optimal smart home energy management considering energy saving and a comfortable lifestyle. IEEE Transactions on Smart Grid, 6 (1), 324-332 (2015).
4. Bingnan Jiang and Yunsi Fei: Smart home in smart microgrid: A cost-effective energy ecosystem with intelligent hierarchical agents. IEEE Transactions on Smart Grid, 6 (1), 313 (2015).
5. Mingfu Li and HungJu Lin: Design and implementation of smart home control systems based on wireless sensor networks and power line communications. IEEE Transactions on Industrial Electronics, 62 (7), 4430-4442 (2015).
6. Adam Cooper: Utility-scale smart meter deployments: Building block of the evolving power grid. Inst. for Electron Innovation, Washington, DC. IEI Rep (2014).
7. Himanshu Khurana, Mark Hadley, Ning Lu, and Deborah A. Frincke: Smart-grid security issues. IEEE Security & Privacy, 8(1), 2010.
8. Ye Yan, Yi Qian, Hamid Sharif, and David Tipper: A survey on cyber security for smart grid communications. IEEE Communications Surveys & Tutorials (2012).
9. Hasan, Md Raqibull and Zhao, Yanxiao and Wang, Guodong and Luo, Yu and Winter, Robb M: Enhanced AODV: Detection and Avoidance of Black Hole Attack in Smart Meter Network. Computer Communication and Networks (ICCCN), 2017 26th International Conference on, 1–6 (2017).
10. Choubey, Rajnish and Sahu, Sandeep and Dubey, Rajshree S and Dubey, Sanjeev: Flooding Attack Prevention Algorithm in AODV Protocol for Mobile Ad-hoc Network. International Journal of Science and Advanced Technology, 1 (6), (2011).

11. Tumrongwittayapak, Chanatip and Varakulsiripunth, Ruttikorn: Detecting sinkhole attack and selective forwarding attack in wireless sensor networks. Information, Communications and Signal Processing, 2009. ICICS 2009. 7th International Conference on, 1–5 (2009).
12. McLaughlin, Stephen and Podkuiko, Dmitry and McDaniel, Patrick: Energy theft in the advanced metering infrastructure. International Workshop on Critical Information Infrastructures Security, 176–187 (2009).
13. Sikora, W and Carpenter, M and Wright, J: Smart grid and AMI security concerns. InGuardians and Industrial Defender, 2009.
14. Goodspeed, Travis and Highfill, Darren R and Singletary, Bradley A: Low-level design vulnerabilities in wireless control systems hardware. Proceedings of the SCADA Security Scientific Symposium, 3–1 (2009).
15. Alahakoon, Damminda and Yu, Xinghuo: Smart electricity meter data intelligence for future energy systems: A survey. IEEE Transactions on Industrial Informatics, 12 (1), 425–436 (2016).
16. Mitchell, Robert and Chen, Ray: Behavior-rule based intrusion detection systems for safety critical smart grid applications. IEEE Transactions on Smart Grid, 4 (3), 1254–1263 (2013).
17. Buczak, Anna L and Guven, Erhan: A survey of data mining and machine learning methods for cyber security intrusion detection. IEEE Communications Surveys & Tutorials, 18 (2), 1153–1176 (2016).
18. Cazorla, Lorena and Alcaraz, Cristina and Lopez, Javier: Towards automatic critical infrastructure protection through machine learning. International Workshop on Critical Information Infrastructures Security, 197–203 (2013).
19. Kotsiantis, Sotiris B and Zaharakis, I and Pintelas, P: Supervised machine learning: A review of classification techniques. Emerging artificial intelligence applications in computer engineering, 160, 3–24 (2007).
20. Jiang, Rong and Lu, Rongxing and Wang, Ye and Luo, Jun and Shen, Changxiang and Shen, Xuemin Sherman: Energy-theft detection issues for advanced metering infrastructure in smart grid. Tsinghua Science and Technology, 19 (2), 105–120 (2014).
21. Li, Wenchao and Yi, Ping and Wu, Yue and Pan, Li and Li, Jianhua: A new intrusion detection system based on KNN classification algorithm in wireless sensor network. Journal of Electrical and Computer Engineering, 2014 (2014).
22. Shon, Taeshik and Kim, Yongdae and Lee, Cheolwon and Moon, Jongsub: A machine learning framework for network anomaly detection using SVM and GA. Information Assurance Workshop, 2005. IAW'05. Proceedings from the Sixth Annual IEEE SMC, 176–183 (2005).
23. Shon, Taeshik and Moon, Jongsub: A hybrid machine learning approach to network anomaly detection. Information Sciences, 177 (18), 3799–3821 (2007).