An Efficient Behavior-based Intrusion Detection System Using OC-ELM for Intelligent Substation in Smart Grid

Yu FU¹*, Jian-wei TIAN², Wan-peng YIN¹ and Yin-qiao XIONG¹,³
¹College of Computer, National University of Defense Technology, Changsha, China
²State Grid Hunan Electric Power Corporation Research Institute, State Grid Corporation of China, Changsha, China
³Department of Electronic Information and Electrical Engineering Changsha University, Changsha, China

*Corresponding author

Keywords: Intelligent substation, OC-ELM, GOOSE, Intrusion detection system.

Abstract. Generic Object Oriented Substation Events (GOOSE), as an essential component of IEC 61850 communication standard, plays an important role in intelligent substation. Any abnormal change of GOOSE field values could cause substation automatic system failures, incorrect switching, or physical damages in the field devices, which will result in probably catastrophic losses. To mitigate the risks caused by vulnerabilities of GOOSE protocol, a behavior-based intrusion detection system is proposed. Different from the existing proposed approaches, considering there is no attack traffic in intelligent substation network so far, one class classifier is used to model the normal behaviors. Compared to the existing approaches, it can usually detect much more complex attacks. To specify the proposed system, when giving a GOOSE message, we first convert it into a feature vector with a specific approach. Considering only normal GOOSE messages are given, One Class classifier with Extreme Learning Machine (OC-ELM) is used to model the information embedded in the normal training set. Extensive experiments demonstrate the efficiency and effectiveness of the proposed intrusion detection system.

Introduction

In recent years, considerable attentions have been paid to security issues in smart grid. As the key node of power grid, intelligent substation is related to every aspect of smart grid. Therefore, the security of IEC 61850, the global standard for communication in substations, is becoming more and more critical. According to different types of services in intelligent substation system, IEC 61850 standard has three kinds of communication protocols, namely, SMV (Sampled Measured Values), GOOSE (Generic Object Oriented Substation Events), MMS (Manufacturing Message Specification). The intelligent substation is logically divided into three levels, substation level, bay level and process level. And the network of an intelligent substation system can be logically divided into two types, namely substation level network and process level network. The substation level network connects the substation level devices and the bay level devices, mainly transports the messages inside the substation level, the messages inside the bay level and messages between the substation level and the bay level. The substation level network messages consist mainly in MMS. Differently, the process level network connects the process level devices and the bay level devices, mainly transports the messages inside the process level, the messages inside the bay level and the messages between the process level and the bay level. The messages of process level network are composed mainly of GOOSE and SMV.

GOOSE is a more important protocol in IEC 61850, embedding select logical and analog data such as circuit breakers status, circuit breaker control, interlocking, general alarms, and power transformers temperature that are transmitted in Ethernet packets[1]. Any abnormal change of GOOSE values could cause automatic failures, incorrect switching, or physical damages in the field devices like power transformers or circuit breakers. GOOSE attacks, once successful, will damage...
IEDs (Intelligent Electronic Devices) of substations, then lead to huge economic losses. It even allows attackers subsequently to control the behavior of substations, causing blackouts and other serious consequences. Therefore, in this paper, we will focus on the security of GOOSE protocol.

In 2007, the same technical committee that develops the IEC 61850 standard released the IEC 62351 standard to provide security to a number of protocols including GOOSE. The objectives of IEC 62351 are authentication of data transfers through digital signatures, prevention of eavesdropping, spoofing, and intrusion detection [1]. It provides security enhancements for all types of messages, such as MMS, GOOSE and SMV. Unfortunately, due to the extremely high end-to-end delay requirement of GOOSE messages, the authentication required by IEC 62351 is difficult to develop in intelligent substation system. Currently, neither the IEC 62351 recommendations nor proprietary manufacturer solutions have been implemented to improve the security of GOOSE message. Meanwhile there is little work about how to implement security for fast GOOSE messages without degrading the actual performance of the IEDs.

In this work, vulnerability in the GOOSE protocol is identified. Some fields such as status number in GOOSE frame provides the opportunities to implement the attacks. The changes in those fields are within the legal range and cannot be detected by simple feature based detection methods. However, they do change the behavior of the GOOSE message and are difficult to detect. Due to the aforementioned challenges, a behavior based intrusion detection system is proposed. The proposed system firstly converts every GOOSE messages into a feature vector with a specific approach. Secondly, considering there is no attack traffic in the substation network so far, no abnormal information can be provided for the classifier. One class classification with extreme learning machine (OC-ELM) is used to predict whether a given GOOSE message is normal or not. Finally, extensive experiments demonstrate the effectiveness and efficiency of the proposed system.

Our main contributions can be summarized as follow:

– Currently, there are serious security risks in the process level of intelligent substation. It is mainly from two aspects: the communication protocol has security risks itself and there are no efficient detection approaches to solve those risks. In order to solve these problems, an intrusion detection system is proposed to detect network abnormal behaviors in substation process level network. Focusing on GOOSE protocol in process level of intelligent substation, such intrusion detection system models normal behaviors of GOOSE messages using OC-ELM. With this model, abnormal behavior caused by external attack or invalid operation can be detected efficiently.

– Considering the data collecting from real-world substation does not contains any type of abnormal behaviors, the traditional classifier such as neural networks or support vector machine cannot be simply applied to such intrusion detection system. Additionally, scalability is also an essential issue. To model the normal behaviors and gain a superior performance, one class classifiers are used. In other words, one class classifier can detect much more complex attacks than the existing approaches. Comparing OC-ELM and other types of one class classifiers, extensive experiments demonstrate that OC-ELM can meet these requirements.

The rest of paper are organized as follow. Sections 2 presents the related work about GOOSE attack approaches and the existing intrusion detection systems in intelligent substation. Section 3 simply introduces the content of a GOOSE message and shows how to extract features from a given GOOSE messages. Section 4 gives a brief introduction of OC-ELM to model the normal behaviors. Section 5 presents the experiment results. Section 6 gives out the conclusion of the proposed system.

**Related Work**

Since security properties of GOOSE have so many weaknesses, few researchers have done some work on improving substation safety performance. In [2], Kush et al. describe an exploit of the vulnerability and proposes a number of attack variants. The attacks send the frames containing higher status numbers which prevents legitimate GOOSE frames to the receiving intelligent electronic device (IED). It could cause a hijacking of the communication channel which can be used to implement a denial-of-service (DoS) or manipulate the IED. The authors refer to this attack as a
poisoning of the GOOSE. A number of GOOSE poisoning attacks are evaluated experimentally on a test bed and demonstrated to be successful. In [3], Hong et al. integrate advantages of feature detection and behavior detection, proposes an integrated anomaly detection system based on host and network. Host based anomaly detection analyzes the log information to detect attacks (such as repeated user error passwords, illegal copying of files, etc.). Network based anomaly detection detects attacks by detecting network anomalous behavior. They use WSU network security test bed of substation to simulate attack and validate their algorithms. Test results show that false positive rate (FPR) and false negative rate (FNR) are 0.013% and 0.02% respectively in host based anomaly detection; false positive rate (FPR) and false negative rate (FNR) are 0.013% and 0.016% respectively in network based anomaly detection. In [4], Kwon et al. propose a novel behavior-based IDS for IEC 61850 protocol using both statistical analysis of traditional network features and specification-based metrics. They use real network traffic data captured in an intelligent substation. The network traffic is analyzed by static characteristics and dynamic characteristics to find out abnormal behaviors of network traffic. The result shows that the behavior based IDS can effectively identify all the abnormal data in a given experiment, and has no false positives and high detection rate (99%). These two kinds of methods have high detection rate and low false positive rate but they can only detect known attack types and can’t detect advanced intrusions. In [5], Tsang et al. present a multi-agent IDS architecture that is designed for decentralized intrusion detection in large switched networks. The experiment uses KDDCup99 IDS data set to evaluate training model and four unsupervised feature extraction algorithms (PCA K-means E-M ICA) are applied and evaluated on their effectiveness to improve the clustering results in order to reduce the dimensionality. It can effectively detect known or unknown intrusion and has a higher detection rate, and has a lower FPR in identifying the normal network traffic.

Feature Extraction

By analyzing captured GOOSE message, we are able to classify it into specific fields. Except for some fields similar to fields in other Ethernet frame such as preamble and start field, the GOOSE frame has its own characteristics. In the Ethernet header of the GOOSE message, there are 6 octets represent the source MAC address and 6 octets represent the destination MAC address. After that, 2 octets 88-B8 is the Ether-type of a GOOSE message. In the GOOSE header of a GOOSE message, there four fields, they are APPID, Length, Reserve1 and Reserve2. The APPID fields indicates the application ID of message. The length indicates the total number (less than 8) of bytes in the frame. The Reserved1 and Reserved2 fields are reserved for future standardized applications and default to 0. After that is the Protocol Data Unit (PDU), which can be defined by eleven fields. These field are GocbRef, TimeAllowedtolive, DatSet, GoID, T, StNum, SqNum, Test, ConfRev, NdsCom and NumDatSetEntries. The field GocbRef is GOOSE control block reference. The field TimeAllowedtolive is the time that the receiver has to wait for the next message. The field DatSet is object reference of control block. The field GoID is GOOSE message identification. The field T is time to StNum increase. The field StNum is status number, a counter that increments each time a GOOSE message has been sent with any change in the values of the Data Set. The field SqNum is sequence number, containing an incremental counter for each time a GOOSE message has been sent [6]. The field Test indicates if the message is a test or not. The field ConfRev is configuration revision. The field NdsCom indicates if reconfigured occur or not. The field NumDatSetEntries is used to specify the number of members.

Not all fields of GOOSE message can selected as feature of IDS. We finally selected 10 features based on the relation between the fields and the correlation between the field and the network behavior, as shown in Table 1.
### Table 1. Description of Selected Features.

<table>
<thead>
<tr>
<th>Fields</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Src</td>
<td>Source MAC address</td>
</tr>
<tr>
<td>Dst</td>
<td>Destination MAC address</td>
</tr>
<tr>
<td>Length</td>
<td>Total number of bytes in the frame</td>
</tr>
<tr>
<td>GocbRef</td>
<td>GOOSE control block reference</td>
</tr>
<tr>
<td>DatSet</td>
<td>Object reference of control block</td>
</tr>
<tr>
<td>GoID</td>
<td>GOOSE message identification</td>
</tr>
<tr>
<td>T</td>
<td>Time to StNum increase</td>
</tr>
<tr>
<td>StNum</td>
<td>Status number</td>
</tr>
<tr>
<td>SqNum</td>
<td>Sequence number</td>
</tr>
<tr>
<td>NumDatSetEntries</td>
<td>Specify the number of members</td>
</tr>
</tbody>
</table>

### Intrusion Detection

In real-world intrusion detection systems, the learning algorithms have to handle a large number of goose messages from the intelligent substations and achieve quickly to meet the strong demand of real-time detection. Take a small-scale substation as an example, hundreds of gigabytes (GB) data (containing millions of goose messages) are generated every day. Unfortunately, many existing learning algorithms always have less scalabilities and unsurprisingly results in a poor performance. Besides, to our best knowledge, there is no attack traffic on the substation until now. In other words, no abnormal data information can be used for learning algorithms. Due to the aforementioned challenges, One Classification with Extreme Learning Machine (OC-ELM) [7], a single hidden layer neural networks with a high learning speed for one class classification, is used for the proposed intrusion detection systems. For the sake of simplicity, a quick and simple introduction to OC-ELM is given.

Extreme Learning Machine (ELM) [8] is one of the most popular neural networks. Different from the existing neural networks, ELM randomly generates the weights between input layers and hidden layers. Additionally, ELM trains these weights by solving a least square optimization problem instead of operating error back-propagation. Because of the aforementioned advantages, ELM can usually achieve a high learning speed and get a good generalization ability.

In details, given a training set $X_{\text{train}}$ containing $n$ data points with $d$ dimensions and $L$ hidden nodes,

$$
\beta = H^T \left( \frac{1}{C} + HH^T \right)^{-1} T
$$

where $C$ and $T$ are the regularization coefficient and target output. The prediction of a input data point $x$ is given by:

$$
f(x) = h(x)\beta = h(x)H^T \left( \frac{1}{C} + HH^T \right)^{-1} T
$$

where $h(x)$ is the random mapping of $x$. Kernel functions can also be used to determine the prediction of $x$:

$$
f(x) = K^T_{\text{test}} \left( \frac{1}{C} + K^T_{\text{train}} \right)^{-1} T
$$

where both $K^T_{\text{train}}$ and $K^T_{\text{test}}$ are kernel matrices.

When applying extreme learning machine to one class classification problem, OC-ELM directly maps all the hidden layer outputs to one target output value. Considering the outputs of OC-ELM of a given training set $y = [y_1, ..., y_n]$, the mapping error of training sample $x_i$ to the target value $y_i$ is $|d_i - y_i|$. A threshold $d_T$ is chosen to exclude a small fraction (p) of farthest training points ($d_i > d_T$), which can prevent the outliers in training set from degrading data description performance of OC-ELM. According to [7], Gaussian kernel is used to improve the best performance of OC-ELM.
Experiment

In this section, we conduct several experiments to demonstrate the efficiency and effectiveness of our proposed method in the real-world dataset.

Dataset. The dataset comes from a substation under construction in Hunan province, China. More than 300000 of GOOSE messages are collected from the real world substation. We randomly select 35000 samples due to the limited memory in our experiment environment.

Evaluation Metrics. In classification problems, “positive” and “negative” refer to the classifier’s prediction. “True” and “false” refer to whether that prediction corresponds to the external judgement. Here are some definitions as the following table shows.

<table>
<thead>
<tr>
<th>Observation</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Prediction</strong></td>
<td><strong>Observation</strong></td>
</tr>
<tr>
<td>TP(true positive)</td>
<td>FP(false positive)</td>
</tr>
<tr>
<td>Correct result</td>
<td>Unexpected result</td>
</tr>
<tr>
<td>FN(false negative)</td>
<td>TN(true negative)</td>
</tr>
<tr>
<td>Missing result</td>
<td>Correct absence of result</td>
</tr>
</tbody>
</table>

Table 2. Basic Definitions in Classification Problems Observation.

False negative is used to evaluate the effectiveness and other comparative methods. The less value of false negative means the better accuracy.

Comparative Algorithms. Considering that the there is still no attack traffic to real world substation, a simple comparison between one class classification with extreme learning machine and other state-of-art methods under the proposed feature extraction method is conducted. Here is a simple introduction of these state-of-art methods.

GaussianDD[8]: A simple Gaussian target distribution, without any robustifying. The target class is modeled as a Gaussian distribution. To avoid numerical instabilities the density estimate is avoided, and just the Mahalanobis distance is used.

KNNDD[9]: A k-nearest neighbor data description. It can be derived from a local density estimation by the nearest neighbor classifier. The method avoids the explicit density estimation and only uses distances to the first nearest neighbor.

PCA[10]: Principal Component Analysis is used for data distributed in a linear subspace. The PCA tries to find the orthonormal subspace which captures the variance in the data as best as possible.

OCELM[7]: One class classification with Extreme Learning Machine. A detailed introduction has been given in the previous section.

For fair comparison, all the test code is implemented by both DDTOOLS[11] and oc-elm toolbox[12] with Matlab under Intel i7 6700, 16GB memory and NVIDIA Geforce 1070. 10-fold cross validation is used to show the runtime and the classification accuracy.

Result Analysis. Each test is conducted for 20 times with 35000 GOOSE messages. Runtime and False Negative on the real-world data set are reported in table 3.
Compared to other methods, focusing on the accuracy, OC-ELM outperforms all of the comparative methods. The main reason is that OC-ELM, as a kind of neural network, has a better performance to fit the data than other methods. In other words, OC-ELM can be regarded as a charming method to be applied into an intrusion detection system in a substation.

Table 3. Performance of OC-ELM and other state-of-art methods with 35000 GOOSE messages.

<table>
<thead>
<tr>
<th>Model</th>
<th>Runtime</th>
<th>Error rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>GaussianDD</td>
<td>0.49sec</td>
<td>9.99%</td>
</tr>
<tr>
<td>KNND</td>
<td>2134.97sec</td>
<td>9.95%</td>
</tr>
<tr>
<td>PCA</td>
<td>0.95sec</td>
<td>10.00%</td>
</tr>
<tr>
<td>OCELM</td>
<td>741.34sec</td>
<td>8.71%</td>
</tr>
</tbody>
</table>

Conclusion

In this paper, especially aiming at developing a reliable behavior-based intrusion detection system in real-world substation, a proper feature extraction method is proposed to transform every GOOSE messages into a feature vector. By comparing some existing state-of-art methods (OC-ELM and other state-of-art methods), extensive experiments demonstrate that OC-ELM outperforms other state-of-art methods in the classification accuracy. Combining a proper feature extraction method and OC-ELM, the proposed intrusion detection system can meet the requirements of an intrusion detection system of a real-world substation.

Acknowledgement

This work is supported by National Natural Science Foundation of China (NO. 61572514).
This work is supported by Science and Technology Planning Project of Changsha (NO. ZD1601042)

References

