OCSVM model combined with K-means recursive clustering for intrusion detection in SCADA systems

Leandros A. Maglaras, Jianmin Jiang
Department of Computing , University of Surrey, Guildford, UK
{l.maglaras, jianmin.jiang}@surrey.ac.uk

***Abstract*—Intrusion detection in Supervisory Control and Data Acquisition (SCADA) systems is of major importance nowadays. Most of the systems are designed without cyber security in mind, since interconnection with other systems through unsafe channels, is becoming the rule during last years. The de-isolation of SCADA systems make them vulnerable to attacks, disrupting its correct functioning and tampering with its normal operation.**

In this paper we present a intrusion detection module capable of detecting malicious network traffic in a SCADA (Supervisory Control and Data Acquisition) system, based on the combination of One-Class Support Vector Machine (OCSVM) with RBF kernel and recursive k-means clustering. The combination of OCSVM with recursive k-means clustering leads the proposed intrusion detection module to distinguish real alarms from possible attacks regardless of the values of parameters σ and ν, making it ideal for real-time intrusion detection mechanisms for SCADA systems. The OCSVM module developed is trained by network traces off line and detect anomalies in the system real time. The module is part of an IDS (Intrusion Detection System) system developed under CockpitCI project.

I. Introduction- Motivation

Several techniques and algorithms have been reported by researchers for intrusion detection. One big family of intrusion detection algorithms is rule based algorithms. In real applications though, during abnormal situations, the behavior of the system cannot be predicted and does not follow any known pattern or rule. This characteristic makes rule based algorithms incapable of detecting the intrusion.

An intelligent approach based on OCSVM [One-Class Support Vector Machine] principles are proposed for intrusion detection. OCSVM is a natural extension of the support vector algorithm to the case of unlabeled data, especially for detection of outliers. The OCSVM algorithm maps input data into a high dimensional feature space (via a kernel) and iteratively finds the maximal margin hyperplane which best separates the training data from the origin. OCSVM principles have shown great potential in the area of anomaly detection [1], [2]. Several extensions of OCSVM method have been introduced lately [3], [4].

For the OCSVM with an RBF kernel, two parameters σ and ν need to be carefully selected in order to obtain the optimal classification result. A common strategy is to separate the data set into two parts, of which one is considered unknown. The prediction accuracy obtained from the unknown set more precisely reflects the performance on classifying an independent data set. An improved version of this procedure is known as cross-validation. Cross-validation is a model validation technique for assessing how the results of a statistical analysis will generalize to an independent data set. It is mainly used in settings where the goal is prediction, and one wants to estimate how accurately a predictive model will perform in practice.

Unnthorsson et al. [5] proposed a method to select parameters for the OCSVM. In their method, ν was first set to a user-specified allowable fraction of misclassification of the target class (e.g. 1% or 5%), then the appropriate σ value was selected as the value for the classification accuracy curve of training samples first reaches $1-\nu$. The obtained ν and σ combination can then be used in the OCSVM classification.

OCSVM similar to other one-class classifiers suffer from false positive and over fitting. The former is a situation that occurs when the classifier fires an alarm in the absence of real anomaly in the system and happens when parameter σ has too large vale. The latter is the situation when a model begins to memorize training data rather than learning to generalize from trend and it shows up when parameter σ is given relatively small value [6]. In this article we propose the combination of OCSVM method with a recursive k-means clustering, separating the real from false alarms in real time and with no pre-selection of parameters σ and ν.

II. $\mathcal{K}-\mathcal{OCSVM}$

The proposed $\mathcal{K}-\mathcal{OCSVM}$ combines the well known OCSVM classifier with the RBF kernel with a recursive K-means clustering module. Figure 1 illustrates the procedure of intrusion detection of our proposed $\mathcal{K}-\mathcal{OCSVM}$ model.

The OCSVM classifier runs with default parameters and the outcome consists of all possible outliers. These outliers are clustered using the k-means clustering method with 2 clusters, where the initial means of the clusters are the maximum and the minimum negative values returned by the OCSVM module. From the two clusters that are created from the K-means clustering, the one that is closer to the maximum negative value (severe alerts) is used as input in the next call of the K-means clustering. This procedure is repeated until all outcomes are put in the same cluster or the divided set is big enough compared to the initial one, according to the threshold parameter k_{thres}.

K-means clustering method divides the outcomes according to their values and those outcomes with most negative values are kept. That way, after the completion of this recursive procedure only the most severe alerts are communicated from

Research supported by the project "CockpitCI: Cybersecurity on SCADA: risk prediction, analysis and reaction tools for Critical Infrastructures ", funded under European Framework-7 Programme (contract No. 285647)

QSHINE 2014, August 18-20, RHODES, Greece

DOI 10.4108/icst.qshine.2014.256549

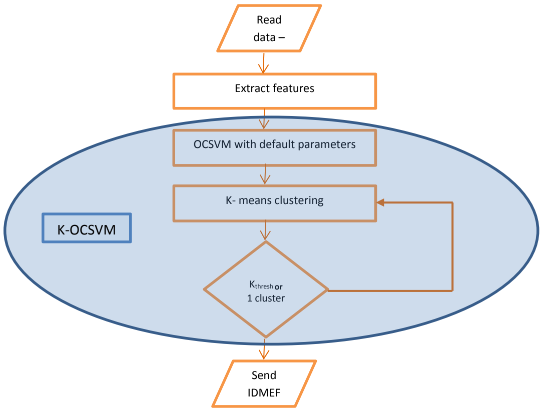

Fig. 1: $\mathcal{K}-\mathcal{OCSVM}$ module

the $\mathcal{K}-\mathcal{OCSVM}$. The division of the data need no previous knowledge about the values of the outcomes which may vary from -0.1 to -160 depending of the assigned values to parameters σ and ν. The method can find the most important/possible outliers for any given values to parameters σ and ν.

One important parameter that affects the performance of $\mathcal{K}-\mathcal{OCSVM}$ is the value of threshold k_{thres}. For given value 2, the final cluster of severe alerts that the method communicates to other parts of the IDS system is limited to 2 to 4 alarms. For bigger value (3 or more) the number of alerts also rises till the method degrades to the initial OCSVM. The optimal value for the given parameter k_{thres} is a matter for future investigation.

III. Performance evaluation

A. Training of OCSVM model

Training of OCSVM module was conducted using a trace file that is sniffed out of a typical wireless network that consists of 10.000 lines each representing a packet send in the network. To train the OCSVM, we adopt the RBF for the kernel equation. This kernel nonlinearly maps samples into a higher dimensional space so it can handle the case when the relation between class labels and attributes is nonlinear.

The training model that is extracted after the training of the OCSVM is used for on line detection of malicious data. Since the model is based on features that are related to network traffic, and since the traffic of the system varies from area to area and from time period to time period, possible generation of multiple models could improve the performance of the module.

B. Testing of OCSVM model

In order to test our model we use another network trace files sniffed from the wireless network. The testing trace file consists of 30.000 lines. We compare the performance of our proposed model against OCSVM classifiers having the same values for parameters σ and ν.

The parameters used for the evaluation of the performance of $\mathcal{K}-\mathcal{OCSVM}$ are listed in Table I.

Parameter	*Range of Values*	*Default value*
σ	0.1 - 0.0001	0.007
ν	0.002 - 0.05	0.01
$Threshold$	2-3	2

TABLE I: Evaluation Parameters

In Table II we show the number of observed anomalies detected from OCSVM and $\mathcal{K}-\mathcal{OCSVM}$ respectively. From this table it is shown how parameters σ, ν affect the performance of OCSVM. Even for a value of ν equal to 0.005, OCSVM produces almost 500 possible attacks, making the method inappropriate for a SCADA system where each false alarm is costly.

Parameter σ	*Parameter* ν	$\mathcal{K}-\mathcal{OCSVM}$	*ocsvm*
0.007	0.002	3	408
0.007	0.01	3	299
0.007	0.005	2	408
0.0001	0.01	3	274
0.1	0.01	2	295

TABLE II: Performance evaluation of $\mathcal{K}-\mathcal{OCSVM}$ and OCSVM for $K_{thers} = 2$.

IV. Conclusions

We have presented a intrusion detection module for SCADA systems that is based in OCSVM classifier and a recursive k-means clustering method. The module is trained off-line by network traces, after the attributes are extracted from the network dataset. The intrusion detection module is part of an IDS system developed under CoCkpitCI.

After the completion of the $\mathcal{K}-\mathcal{OCSVM}$ method only severe alerts are communicated to the system by IDMEF files that contain information about the source, destination, protocol and time of the intrusion. The method is stable and its performance is not influenced by the selection of parameters ν and σ. Further analysis is needed in order to evaluate the performance of the method under different attack scenarios.

References

[1] Y. Wang, J. Wong, and A. Miner, “Anomaly intrusion detection using one class svm,” in *Information Assurance Workshop, 2004. Proceedings from the Fifth Annual IEEE SMC*. IEEE, 2004, pp. 358–364.

[2] L. Maglaras and J. Jiang, “Intrusion detection in scada systems using machine learning techniques,” in *Proceedings of the 2nd SAI conference*. SAI, 2014.

[3] A. Glazer, L. Michael, and S. Markovitch, “q-ocsvm: A q-quantile estimator for high-dimensional distributions,” in *In Proceedings of The 27th Conference on Neural Information Processing Systems (NIPS-2013),Lake Tahoe, Nevada*, 2013.

[4] X. Song, G. Fan, and M. Rao, “Svm-based data editing for enhanced one-class classification of remotely sensed imagery,” *Geoscience and Remote Sensing Letters, IEEE*, vol. 5, no. 2, pp. 189–193, 2008.

[5] T. P. Runarsson and M. T. Jonsson, “Model selection in one-class ν-svms using rbf kernels,” in *Proceedings of 16th International Congress and Exhibition on Condition Monitoring and Diagnostic Engineering Management*, 2003.

[6] X. Li, L. Wang, and E. Sung, “Adaboost with svm-based component classifiers,” *Engineering Applications of Artificial Intelligence*, vol. 21, no. 5, pp. 785–795, 2008.