Algorithms for proactive security of industrial systems based on machine learning technologies

V. Vasilyev
Dept. of Computer Engineering and Information Security
Ufa State Aviation Technical University
Ufa, Russia
vasilyev@ugatu.ac.ru

A. Vulfin
Dept. of Computer Engineering and Information Security
Ufa State Aviation Technical University
Ufa, Russia
vulfin.alexey@gmail.com

A. Kirillova
Dept. of Computer Engineering and Information Security
Ufa State Aviation Technical University
Ufa, Russia
kirillova.andm@gmail.com

***Abstract*—Approaches to improving the efficiency of network attack detection algorithms in heterogeneous industrial networks based on machine learning technologies are considered. An algorithm for analyzing and processing network traffic has been developed in the task of detecting malicious network activity. The Electra dataset is used to train the proposed machine learning models and heterogeneous neural network models.**

Keywords— network attacks, machine learning, heterogeneous industrial network, dataset.

1. Introduction

At the present stage of digital transformation of the industry [1], there is a trend towards the integration of Industrial Internet of Things (IIoT) devices with traditional data collection and control systems and deep penetration of IIoT into critical infrastructure, which has led to an increase in the likelihood and number of potential cyber attacks on industrial facilities.

To detect multi-step network attacks on industrial systems, it is necessary to analyze a significant amount of incoming, outgoing and local network traffic with the ability to compare it with the information security event stream to detect anomalous activity [2].

Attacks using exploits practically do not change the main characteristics of industrial protocol traffic, which makes it very difficult to select signatures for their detection [3]. The use of machine learning (ML) methods makes it possible to identify the features of anomalous traffic and build an appropriate mechanism for their detection [4, 5].

The aim of the work is to improve the efficiency of algorithms for detecting network attacks in a heterogeneous industrial network based on ML technologies.

2. Algorithm for Detecting Network Attacks in a Heterogeneous Industrial Network

The algorithm for analyzing network traffic parameters in the task of detecting anomalies and malicious network activity based on the use of ML-models is shown in Fig. 1. The main stages of data collection and processing for the construction and use of ML-models are presented.

In order to evaluate the effectiveness of the proposed solution, the Electra dataset [6] was used, generated from the network traffic of a traction electrical substation operating in normal mode and under attack conditions.

To accomplish its task, the electric traction substation consists of 5 PLCs, a SCADA system, a switch and a firewall. All communications between components are implemented by Modbus and S7comm over TCP/IP.

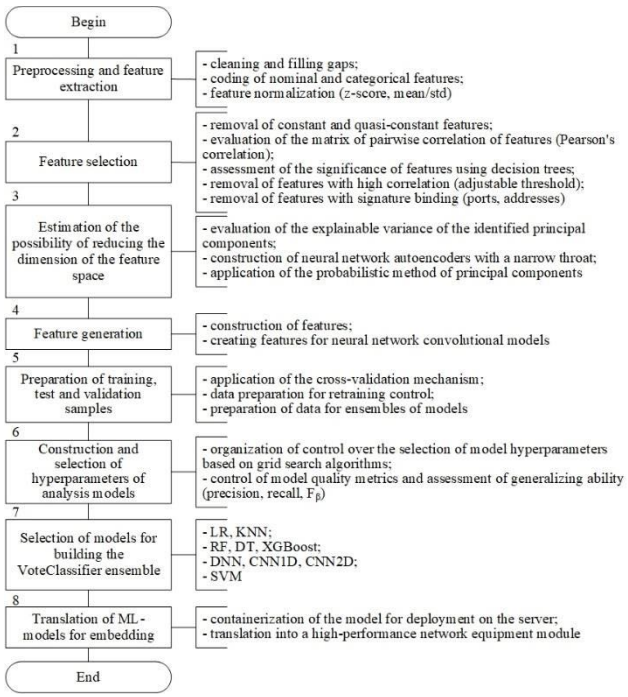

Fig. 1. Generalized network traffic mining algorithm

Electra includes three types of attacks: false data injection, replay, and reconnaissance. Electra is the only dataset available that includes replay attacks. There are two different data sets, one for each Modbus and S7comm communication protocol. The structure of the test bench is shown in Fig. 2.

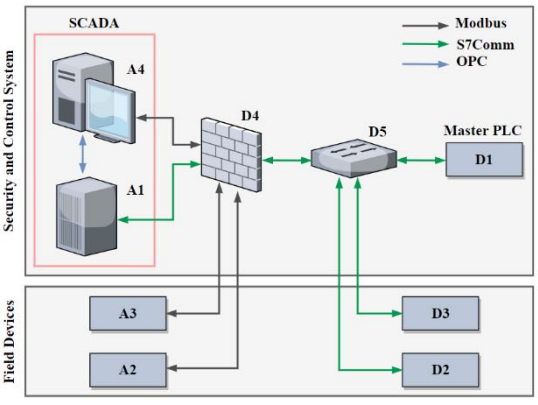

Fig. 2. The structure of the stand for collecting network traffic (A1 (Nanobox) and A4 (HMI) form a SCADA master for Modbus PLC slaves A2 and A3. D1 (PLC) slave for S7Comm A1 slaves and PLCs D2 and D3. D4 – firewall, D5 – switch for connecting devices)

Electra Modbus and Electra S7comm collected network traffic for 12 hours of operation of the stand (Fig. 3), while 94% and 98% of the records correspond to normal operation. The data set contains 387 million records for S7Comm (36.8 GB) and 16 million records for Modbus (1.5 GB). Table 1 shows features of network sessions recorded during traffic collection.

TABLE 1. FEATURES OF NETWORK SESSIONS

Features	Description	Data type
time	Timestamp	string
smac	Source MAC address	string
dmac	Destination MAC address	string
sip	Source IP	string
dip	Destination IP address	string
request	Indicates if the packet is a request (master-to-slave packet)	boolean
fc	Function code	integer
error	Indicates whether there was an error in the read/write operation.	boolean
madd	Memory address to perform a read/write operation	integer
data	Data field	integer
label	Label for attacks and normal patterns	string

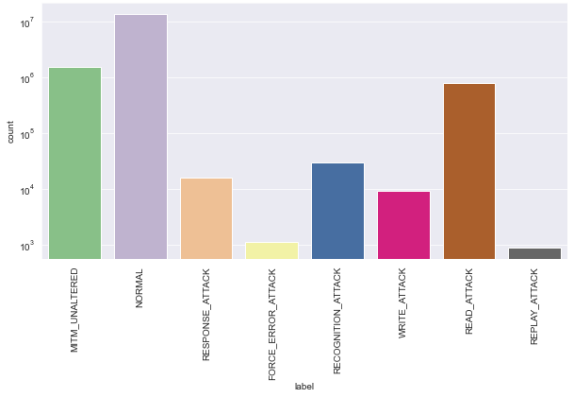

Fig. 3. Distribution of the number of records corresponding to attacks and normal operation

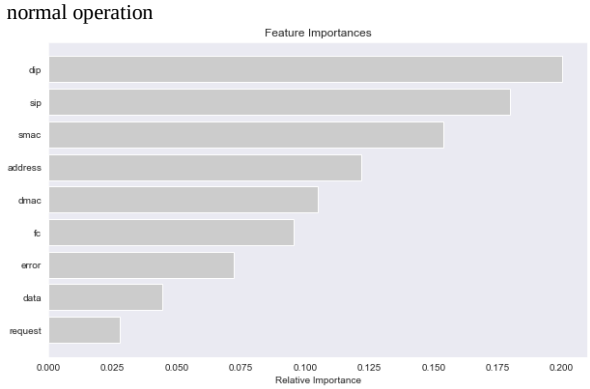

Fig. 4. The histogram of the assessment of the significance of features (y-axis – features), obtained using a classifier based on a committee of decision trees (abscissa – relative units)

3. RESULTS OF THE COMPUTATIONAL EXPERIMENT

Evaluation of the significance of features in the problem of multiclass classification makes it possible to single out those features that are key to assigning a network session to a particular class. Fig. 4 shows a histogram of the feature significance assessment obtained using a classifier based on the random forest classifier.

An ensemble of classifiers has been implemented, which includes a committee of decision trees (RF), a classifier based on the gradient boosting algorithm on an ensemble of decision trees (XGBClassifier), and an ExtraTreesClassifier. Committee parameters: voting type – “soft” (voting and weighting model predictions for each class); model weights are distributed as {2, 1, 3}.The accuracy metric for the ensemble for the test sample is 0.975, the estimate of the F1- score is 0.964. The assessment of prec recall, F1-score and the number of examples (support) by attack classes in the test sample are shown in Table 2.

Таблица II. EVALUATION OF THE QUALITY OF MULTICLASS CLASSIFICATION FOR A TEST SAMPLE OF AN ENSEMBLE OF CLASSIFIERS

attack classes	precision	recall	F1-score	support
FORCE_ERROR_ATTACK	1.00	1.00	1.00	1043
MITM_UNALTERE	1.00	1.00	1.00	3488
NORMAL	1.00	1.00	1.00	7354
READ_ATTACK	0.84	1.00	0.91	3486
RECOGNITION_ATTACK	1.00	1.00	1.00	3528
REPLAY_ATTACK	1.00	0.03	0.06	686
RESPONSE_ATTACK	1.00	1.00	1.00	3546
WRITE_ATTACK	1.00	1.00	1.00	3469

4. CONCLUSION

Algorithms for intelligent analysis of scattering parameters in the tasks of detecting malicious activity have been developed. An ensemble of classifiers is built based on traditional ML-models. The estimate of the F1- score when working with test samples reaches 96.4%.

ACKNOWLEDGMENT

The reported study was funded by RFBR according to the research project No. 20-38-90078.

REFERENCES

Fig. 1. Threat landscape for industrial automation systems. 2019 year. Kaspersky ICS CERT [Electronic source]. – Available: https://ics-cert.kaspersky.ru/reports/2020/04/24/threat-landscape-for-industrial-automation-systems-2019-report-at-a-glance/ (31.01.2022).

[8] Ten, C.W. Cybersecurity for critical infrastructures: Attack and defense modeling / C.W. Ten, G. Manimaran, C.C. Liu // IEEE Transactions on Systems, Man, and Cybernetics-Part A: Systems and Humans. – 2010. – Vol. 40(4). – P. 853-865.

[9] Cecil, A.A Summary of Network Traffic Monitoring and Analysis Techniques [Electronic source]. – Available: https://www.cse.wustl.edu/~jain/cse567-06/ftp/net_monitoring/ index.html (31.01.2022).

[10] Ten, C.W. Anomaly detection for cybersecurity of the substations / C.W. Ten, J. Hong, C.C. Liu // IEEE Transactions on Smart Grid. – 2011. – Vol. 2(4). – P. 865-873.

[11] Vulfin, A.M. Network traffic analysis based on machine learning methods / A.M. Vulfin, V.I. Vasilyev, V.E. Gvozdev, K.V. Mironov, O.E. Churkin // Journal of Physics: Conference Series. IOP Publishing. – 2021. – Vol. 2001(1). – P. 012017.

[12] Gomez, A.L.P. On the generation of anomaly detection datasets in industrial control systems / A.L.P. Gomez, L.F. Maimo, A.H. Celdran, F.J.G. Clemente, C.C. Sarmiento., C.J.D.C. Masa, R.M. Nistal // IEEE Access. – 2019. – Vol. 7. – P. 177460-177473.