



A.T. Zhumabekova¹, G.T. Seitkali^{1,2}, V.I. Karyukin¹

¹Farabi University, Almaty, Kazakhstan

²Energo University, Almaty, Kazakhstan

E-mail: zhumabekova2702@gmail.com

VIRTUAL CYBER TESTING RANGE FOR MODBUS-BASED ICS FOR ANOMALY DETECTION USING MACHINE LEARNING

Abstract. This research shows experiments for anomaly detection with machine learning models in the Modbus Transmission Control Protocol system. It uses a range of testbeds, emulated in Mininet, Supervisory Control and Data Acquisition, and operational technology environments that are connected through virtual network routers and traffic monitoring tools. Normal records were generated with periodic virtual controllers, whereas Denial-of-service (DoS) records were created to present integrity attacks. Scapy technology was used to extract important characteristics of the received traffic, such as protocol types, packet sizes, traffic timing, and packet size variability. The dataset consisted of 500 records, including 280 legitimate data, 100 DoS attacks, and 120 False Data Injection (FDI). It was supplemented with 10% noise to create realistic classification conditions. Classification was performed using logistic regression, support vector machine, and random forest algorithms. The results were evaluated using accuracy, precision, recall, and F1-score metrics. Comparing the results, the logistic regression model showed the best results: accuracy - 0.888, precision - 0.894, recall - 0.888, f1-score 0.885. In summary, the obtained data demonstrated that a fully virtualized cyber-attack detection environment is effective and secure for industrial traffic generation and threat detection testing. It was also demonstrated that it can provide a scalable system.

Keywords: industrial control systems, cyber threats, Modbus TCP, machine learning, anomaly detection, network security.

Introduction.

Industrial systems and SCADA networks play a significant role in reliable cybersecurity protection. This growing number of cyberattacks has put the focus on designing efficient cyber threat detection tools. Nevertheless, security experiments in real industrial systems usually pose safety risks and confidentiality concerns regarding legal restrictions. Different alternatives are provided for isolated and reproducible environments, in which cyber-attacks are simulated. Although some studies have shown the value of cybersecurity experiments, little attention has been given to industrial protocols, such as Modbus TCP. On the other hand, this study focuses on developing a method for generating realistic Modbus



Transmission Control Protocol traffic under normal and malicious scenarios. These scenarios are directed toward designing cyber threat detection approaches using machine learning (ML) models in the Supervisory Control and Data Acquisition communication environment. Through these objectives, the study tries to provide a flexible platform for testing anomaly detection methods. The integration of Industrial Control Systems (ICS) with corporate networks and Internet-based services has increased the exposure of critical infrastructure to cyberattacks. Since experiments on operational systems may disrupt technological processes or damage equipment, cyber ranges and testbeds are widely used to reproduce industrial networks, communication protocols, normal operations, and attack scenarios in controlled environments.

literature review

Genge et al. [1] created a computer model and simulation environment for physical processes. The platform required complex integration of cyber components. In [2], Antonioli and Tippenhauer introduced a lightweight Mininet system, MiniCPS, for programmable controllers and physical processes. This support was particularly useful for industrial control system topologies. Mathur and Tippenhauer [3] have extensively studied the SWaT platform for multi-stage analysis and evaluation of cyber threats and intrusion detection methods. However, the SWaT platform requires specialized hardware and maintenance tools. This problem can be solved with the help of computer simulation. Pospisil et al. [4] have compared physical sensors and automated sensors and described the most important advantages of automated systems and their lower development costs. Dehlaghi-Ghadim et al. [5] have developed a suitable system for industrial scenarios with malicious and legitimate traffic. Although fully simulated environments have been created, Modbus TCP is still an area that needs to be studied. This is because it is widely implemented in SCADA servers and other devices. The experiments in [6], conducted by Goldenberg and Wool, presented an intrusion-detection method that analyzed Modbus TCP communication sequences and identified deviations from normal behavior. The research of Ghosh et al. in [7] used statistical analysis to demonstrate that it is insufficient to utilize only traffic volume for anomaly detection alone, as protocol-related features are also very important. The data generated with Modbus TCP were classified with Support Vector Machine (SVM), K-nearest neighbors, and Random Forest (RF) in the work [8] by Duque Anton et al. The results proved these models to be effective for industrial traffic classification. Then, in the next work [9], SVM and RF were compared on the classification of Modbus and OPC datasets, where RF showed slightly better performance. These results confirmed the efficiency of ML models for anomaly detection. The work [10] generated a wide range of datasets for various threats. The classifiers were also applied to them, and the obtained results were thoroughly analyzed. The research [11] by Dehlaghi-Ghadim et al. simulated network features and various attack scenarios with ICS datasets. The models demonstrated efficiency across various traffic and topology specifications. Generally, the presented research works demonstrated the effectiveness of Modbus



traffic analysis, development of different synthetic datasets, and application of ML models for anomaly detection in industrial systems. As real physical testbeds are expensive to build, most experiments are implemented on virtual systems with the designed technical realization measures. The subsequent experiments focus on developing anomaly attack detection in the Mininet environment using Logistic Regression (LR), SVM, and RF ML models.

Materials and Methods.

The main network architecture is implemented using Mininet. It is a widespread network emulator for creating and evaluating Software-Defined Networking (SDN). Mininet provides the possibility to produce industrial control systems with a flexible testbed. The SDN environment generally presents an operational layer with an IP address range from 192.168.10.1 to 192.168.10.254. At the same time, the Operational Technology (OT) presents logical controllers that work in the range from 192.168.20.1 to 192.168.20.254. A virtual router provides controlled communication between two segments and simulates routing of a real industrial network. In addition, a mirror port captures all transmitted traffic and allows the packets to be checked for security analysis and anomaly detection.

The network traffic presents both normal communications and cyberattack cases within the SCADA environment. Typically, the SCADA server makes these special requests to logic controllers every 1-2 seconds via the Modbus protocol on TCP port 502. This protocol reads process data from industrial equipment, and standard-sized packets represent the network traffic itself.

During the experiments, two cases were analyzed:

1) The first case uses a DoS SYN flood, which sends a very large number of TCP packets in a short period of time (50 packets or more) within 0.001 to 0.01 seconds. This significantly overloads the network and limits the processing of legitimate requests.

2) The second case utilizes a Forged Data Injection (FDI) attack. In this case, a specific script writes extraneous values to PLC registers via Modbus commands. This attack generally generates less traffic than a DoS attack and is therefore more difficult to detect if one analyzes only the packet flood rate. This is precisely the purpose of this type of attack, where the primary intent is not to interrupt data transmission, but to modify it. Similarly, legitimate traffic, DoS, and FDI attacks have their own unique characteristics, which help in their detection in systems.

The types of traffic (SCADA, DoS, and FDI) are identified with the use of several ML models. Among these models are LR, which uses L2 regularization parameters to reduce overfitting; SVM with a radial basis kernel function to capture nonlinear boundaries and class weights; and RF with 200 decision trees and a maximum tree depth of 8.



Results.

To improve the reproducibility of the experimental environment, all components of the cyber range were deployed on a single Ubuntu 22.04 workstation. Mininet was utilized because it allows fast creation of network topologies with low computational resources. All the elements of Mininet were connected with Open vSwitch, providing communication using the Modbus TCP protocol over port 502. The generated network traffic was obtained with tcpdump and preprocessed using the Scapy library. Each flow record consisted of 6 features that characterized protocol behavior, packet sizes, traffic volume, etc.

The first ‘proto’ feature of the dataset indicates the transport protocol: 6 for TCP and 17 for UDP. The ‘length’ feature gives the packet size in bytes. Then, the next ‘ttl’ feature shows the Time-to-Live field of the IP packet itself, and ‘packet_count’ designates the total number of packets. The ‘interarrival’ feature places the time between packet arrivals, and ‘size_var’ characterizes packet dispersion.

During the dataset processing stage, all unnecessary and incorrect records were removed. Hyperparameters were also tuned, based on previous research experience. All these tunings were performed using Scikit-learn. The formed dataset included 500 records: 280 normal, 100 DoS attacks, and 120 FDI attacks. The current distribution shows the dominance of legitimate traffic. In addition, the dataset was extended with 10% of random noise labels to simulate real scenarios. In the conducted experiments, the dataset was split into 75% training and 25% testing data.

The classification results were evaluated with Accuracy, Precision, Recall, and F1-score metrics. These metrics are described by (1)-(4):

$$Accuracy = \frac{TP + TN}{Total_number}, \quad (1)$$

$$Precision = \frac{TP}{TP + FP}, \quad (2)$$

$$Recall = \frac{TP}{TP + FN}, \quad (3)$$

$$F1-score = 2 \times \frac{Precision \times Recall}{Precision + Recall}, \quad (4)$$

The performance of the metrics is shown in Table 1.

Table 1 - Performance of classification metrics

Model	Accuracy	Precision	Recall	F1-score
Logistic Regression	0.888	0.894	0.888	0.885
Random Forest	0.880	0.884	0.880	0.877
SVM	0.872	0.881	0.872	0.867

The experimental results showed mostly similar accuracy values of 0.872, 0.880, and 0.888. The LR model had the highest accuracy score of 0.888 among all



three models, while the SVM model showed the lowest accuracy of 0.872. Meanwhile, the RF model showed average performance. Although all three models were effective on average, the LR model also got the best precision and recall values. However, it should be noted that the dataset contained only 500 records, and the obtained results can be characterized as a preliminary assessment of the models' effectiveness, rather than a definitive determination of their dominance.

In addition, the experimental results are also shown as bar charts in Figures 1-4.

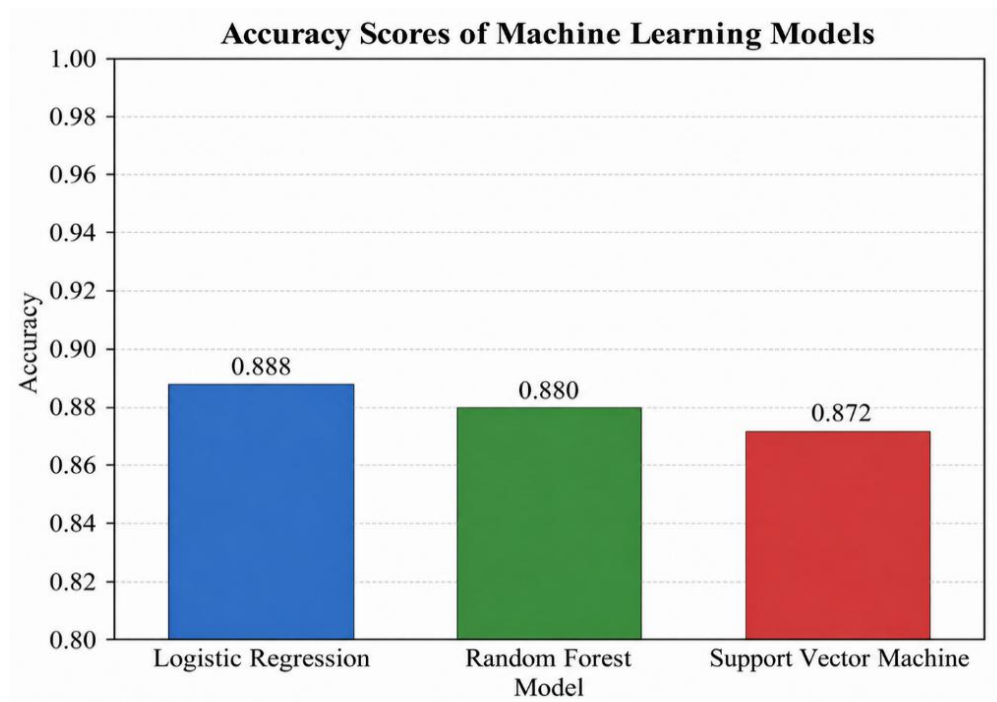


Figure 1 - The Accuracy Bar charts

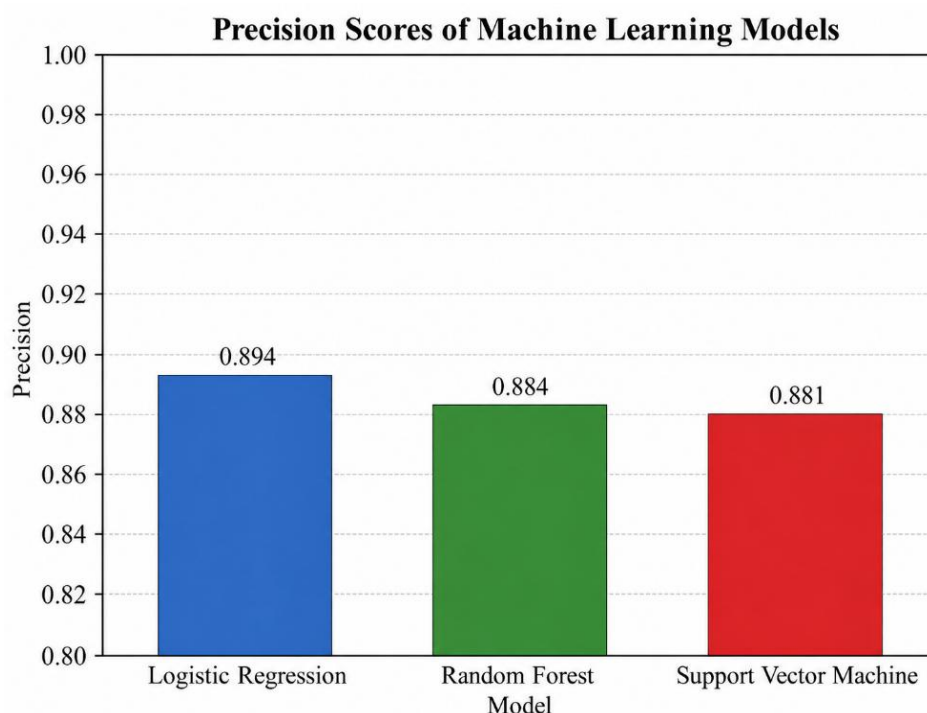


Figure 2 - The Precision Bar charts

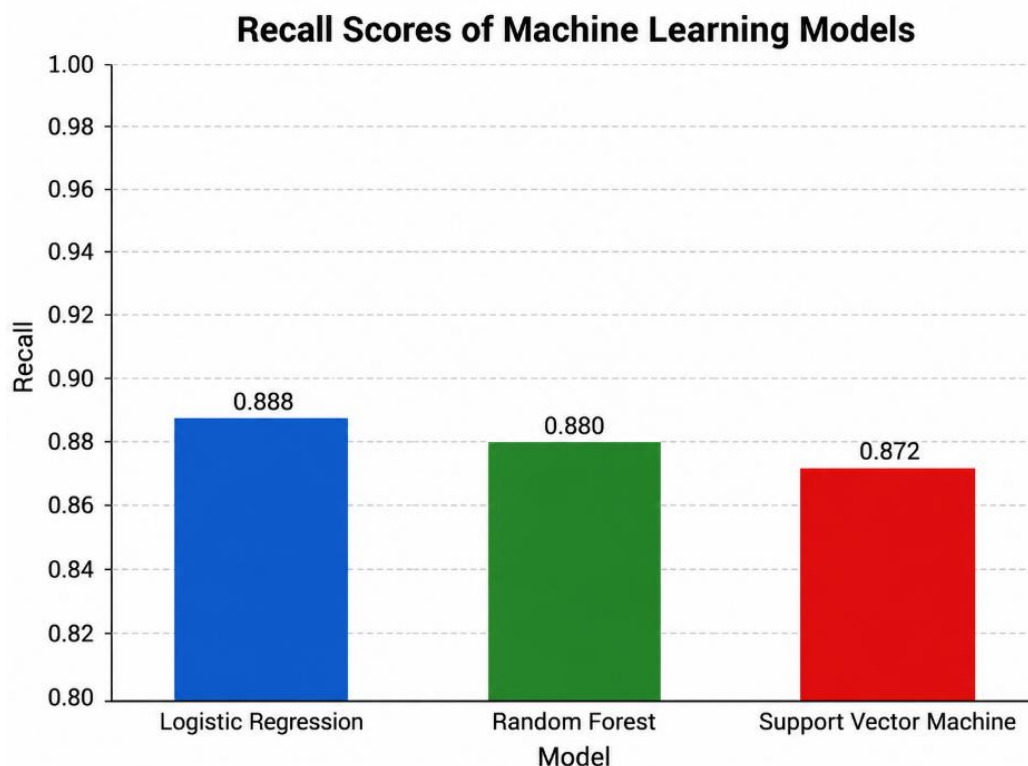


Figure 3 - The Recall Bar charts

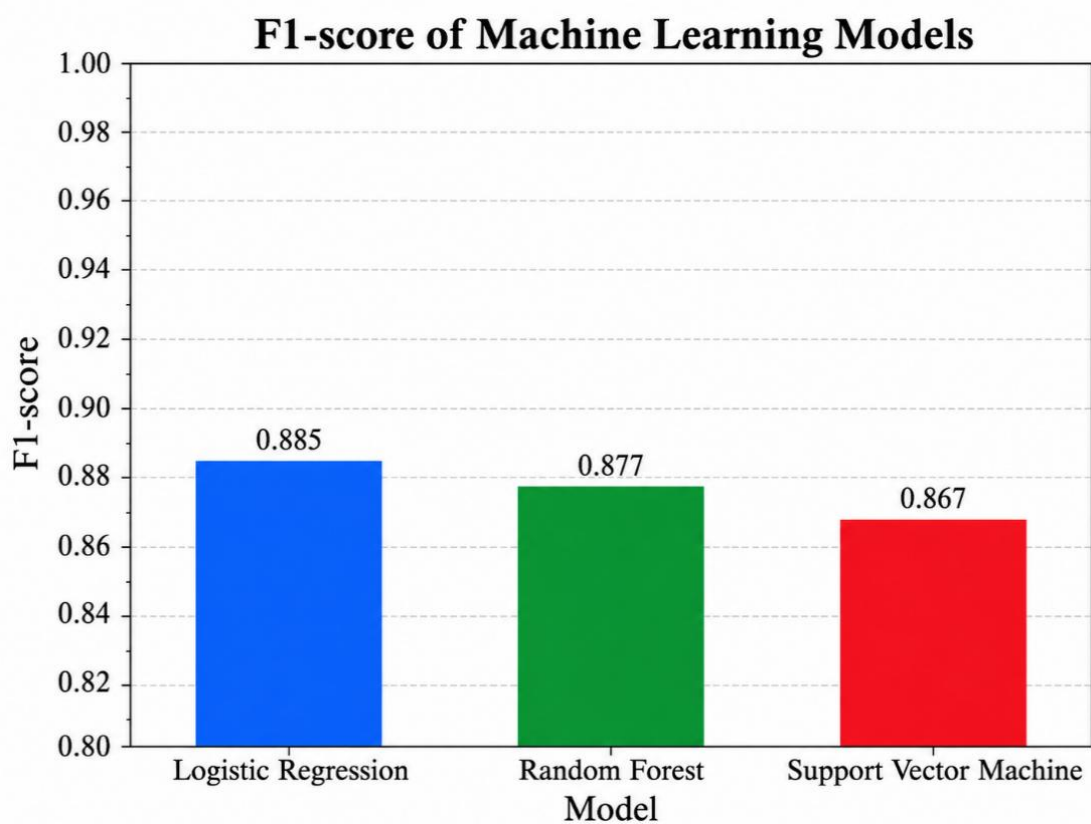


Figure 4 - The F1-score Bar charts



Discussion.

The bar chart analysis demonstrated that all three ML algorithms successfully distinguished normal traffic from malicious traffic with high accuracy scores. Although the classification results between the models did not differ significantly, the LR model got the best results. However, the RF model showed average and balanced results due to its ensemble structure. The SVM scores were lower than the others, as some FDI attacks were classified as normal. Despite these inaccuracies, all models achieved metric values above 0.850, demonstrating their effectiveness.

Conclusion.

The presented work showed the construction of a framework for cyber threat classification. These experiments used Mininet, which generated synthetic traffic. The resulting data was classified by three machine learning models: LR, RF, and SVM. Among these, the LR model achieved the best values for accuracy, precision, recall, and F1-score. Its accuracy score reached 0.888, precision 0.894, recall 0.888, and F1-score 0.885. The RF and SVM models also achieved similar results, demonstrating that this synthetic dataset enables experiments that closely approximate real-world conditions.

It is also necessary to highlight the path of future research. This research should focus on improving the applicability of the proposed framework. One direction is integrating real TCP traffic, which provides data captured from various experimental scenarios. These scenarios could be extended to capture other types of attacks, such as Man-in-the-Middle, SQL injections, Malware, Phishing, XSS, and unauthorized control operations. Many other ML and deep learning models could be applied for anomaly detection mechanisms. Moreover, other types of models can be configured to detect other earlier unseen threats.

REFERENCES

1. Genge B., Siaterlis C., Nai Fovino I., Masera M. (2012) A cyber-physical experimentation environment for the security analysis of networked industrial control systems. *Computers & Electrical Engineering*. 2012. - Vol. 38, No.5. P. 1146-1161. DOI: 10.1016/j.compeleceng.2012.06.015.
2. Antonioli D., Tippenhauer N. O. (2015) MiniCPS: A toolkit for security research on CPS networks. *Proceedings of the First ACM Workshop on Cyber-Physical Systems Security and Privacy*. - New York: ACM, 2015. P.91-100. DOI: 10.1145/2808705.2808715.
3. Mathur A. P., Tippenhauer N. O. (2016) SWaT: A water treatment testbed for research and training on ICS security. *2016 International Workshop on Cyber-Physical Systems for Smart Water Networks (CySWater)*. Vienna: IEEE, 2016. P. 31–36. - DOI: 10.1109/CySWater.2016.7469060.



4. Pospisil O., Fujdiak R., Mlynek P., Misurec J. (2021) Application perspective on cybersecurity testbed for industrial control systems. *Sensors*. 2021. Vol. 21, No.23. Art. 8119. DOI: 10.3390/s21238119.
5. Dehlaghi-Ghadim A., Balador A., Helali Moghadam M., Hansson H., Conti M. (2023) ICSSIM: A framework for building industrial control systems security testbeds. *Computers in Industry*. 2023. Vol.148. Art.103906. DOI: 10.1016/j.compind.2023.103906.
6. Goldenberg N., Wool A. (2013) Accurate modeling of Modbus/TCP for intrusion detection in SCADA systems. *International Journal of Critical Infrastructure Protection*. 2013. Vol. 6, No. 2. P. 63-75. DOI: 10.1016/j.ijcip.2013.05.001
7. Ghosh T., Al-Shaer E., Rahman M. (2023) Anomaly detection for Modbus over TCP in control systems using entropy and classification-based analysis. *Journal of Cybersecurity and Privacy*. 2023. Vol.3, No.4. P. 895-913. DOI: 10.3390/jcp3040041.
8. Duque Anton S., Kanoor S., Fraunholz D., Schotten H. D. (2018) Evaluation of machine learning-based anomaly detection algorithms on an industrial Modbus/TCP data set. *Proceedings of the 13th International Conference on Availability, Reliability and Security*. New York: ACM, 2018. Art. 41. P. 1-9. DOI: 10.1145/3230833.3232818.
9. Duque Anton S. D., Sinha S., Schotten H. D. (2019) Anomaly-based intrusion detection in industrial data with SVM and Random Forests. 2019 *International Conference on Software, Telecommunications and Computer Networks (SoftCOM)*. Split: IEEE, 2019. P.1–6. DOI: 10.23919/SOFTCOM.2019.8903672.
10. Gómez Á. L. P., Maimó L. F., Celdrán A. H. et al. (2019) On the generation of anomaly detection datasets in industrial control systems. *IEEE Access*. 2019. Vol. 7. P. 177460-177473. DOI: 10.1109/ACCESS.2019.2958284.
11. Dehlaghi-Ghadim A., Helali Moghadam M., Balador A., Hansson H. (2023) Anomaly detection dataset for industrial control systems. *IEEE Access*. 2023. Vol. 11. P. 107866-107880. DOI: 10.1109/ACCESS.2023.3319379.

Айдана Жұмабекова, PhD, аға оқытушы, Farabi University, Алматы, Қазақстан, zhumabekova2702@gmail.com

Ғазиз Сейтқали, докторант, аға оқытушы, Farabi University, Energo University, Алматы, Қазақстан, g.seitkali@gmail.com

Владислав Карюкин, PhD, доцент м. а., Farabi University, Алматы, Қазақстан, vladislav.karyukin@gmail.com

МАШИНАЛЫҚ ОҚЫТУМЕН АНОМАЛИЯЛАРДЫ АНЫҚТАУҒА АРНАЛҒАН MODBUS НЕГІЗІНДЕГІ ӨНЕРКӘСІПТІК БАСҚАРУ ЖҮЙЕЛЕРІНІҢ ВИРТУАЛДЫ КИБЕРПОЛИГОНЫ



Аңдатпа. Ұсынылған жұмыста аномалияларды анықтау мақсатында машиналық оқыту алгоритмдерін Modbus TCP (Transmission Control Protocol) жүйесіне қолдану арқылы тәжірибелер жасалынған. Трафикті бақылау құралы және виртуалды желілік маршрутизатор көмегімен қосылған Mininet пен SCADA (Supervisory Control and Data Acquisition) технологияларында эмуляцияланған бірқатар тәжірибе алаңдары қолданылған. Тұтас деректерге шабуыл жасау үшін қызмет көрсетуден бас тарту (DoS) шабуылдары және виртуалды контроллерлер көмегімен легитімді жазбалар құрылды. Scapy технологиясын алынған трафиктің хаттама түрлерін, пакет өлшемдерін, тарфик уақытын, пакет өлшемінің өзгергіштігін сипаттайтын сияқты маңызды ерекшеліктерді алуға пайдаланылды. Деректер жиынтығы 500 деректен тұрды, оның ішінде 280 легитімді деректер, 100 қызмет көрсетуден бас тарту шабуылдары, 120 жалған деректерді енгізу шабуылы (FDI) болды. Шынайы классификациялау шарттарын жасау үшін 10 пайыз шуммен толықтырылды. Классификациялау логистикалық регрессия, тірек векторлық машина, кездейсоқ орман алгоритмдерін қолдана отырып жүргізілді. Accuracy, precision, recall және f1-score көрсеткіштерінің көмегімен нәтижелер бағаланды. Нәтижелерді салыстыра келе логистикалық регрессия моделі ең жоғарғы нәтижеге қол жеткізген: accuracy – 0.888, precision – 0.894, recall – 0.888, f1-score 0.885. Нәтижелерді қорытындылай келе, алынған деректер толық виртуалдандырылған кибер шабуылдарды анықтау ортасы өнеркәсіптік трафикті генерациялау және қауіпті анықтау тестілеулерін жүргізу үшін тиімді, қауіпсіз екені анықталды. Сонымен қатар масштабталатын жүйені қамтамасыз ете алатыны да көрсетілді.

Түйінді сөздер: машиналық оқыту, өнеркәсіптік басқару жүйелері, кибер шабуылдар, Modbus TCP, аномалияларды анықтау, желілік қауіпсіздік.

Айдана Жұмабекова, PhD, старший преподаватель, Farabi University, Алматы, Казахстан, zhumabekova2702@gmail.com

Ғазиз Сейтқали, докторант, старший преподаватель, Farabi University, Energo University, Алматы, Казахстан, g.seitkali@gmail.com

Владислав Карюкин, PhD, и.о. доцента, Farabi University, Алматы, Казахстан, vladislav.karyukin@gmail.com

ВИРТУАЛЬНЫЙ КИБЕРПОЛИГОН ДЛЯ ПРОМЫШЛЕННЫХ СИСТЕМ УПРАВЛЕНИЯ НА БАЗЕ MODBUS ДЛЯ ОБНАРУЖЕНИЯ АНОМАЛИЙ С ИСПОЛЬЗОВАНИЕМ МАШИННОГО ОБУЧЕНИЯ

Аннотация. В представленной работе были проведены эксперименты с использованием алгоритмов машинного обучения в системе Modbus TCP (Transmission Control Protocol) для обнаружения аномалий. Использовался ряд эмуляций в технологиях Mininet и SCADA (Supervisory Control and Data



Acquisition), подключенных с помощью инструмента мониторинга трафика и виртуального сетевого маршрутизатора. Для атаки на все данные были созданы атаки типа отказ в обслуживании (DoS) и легитимные записи с использованием виртуальных контроллеров. Технология Scapy использовалась для извлечения важных характеристик полученного трафика, таких как типы протоколов, размеры пакетов, время трафика и вариативность размера пакетов. Набор данных состоял из 500 записей, включая 280 легитимных данных, 100 DoS-атак и 120 атак с внедрением ложных данных (FDI). Он был дополнен 10% шумом для создания реалистичных условий классификации. Классификация проводилась с использованием алгоритмов логистической регрессии, машины опорных векторов и случайного леса. Результаты оценивались с помощью показателей accuracy, precision, recall и f1-score. Сравнивая результаты, модель логистической регрессии показала наилучшие результаты: accuracy – 0.888, precision – 0.894, recall – 0.888, f1-score 0.885. Подводя итоги, полученные данные показали, что полностью виртуализированная среда обнаружения кибератак эффективна и безопасна для генерации промышленного трафика и тестирования обнаружения угроз. Также было показано, что она может обеспечить масштабируемую систему.

Ключевые слова: машинное обучение, системы промышленного управления, кибератаки, Modbus TCP, обнаружение аномалий, сетевая безопасность.

Received: August 06, 2026

Peer-reviewed: August 12, 2026

Accepted: August 28, 2026