O‘ZBEKISTON RESPUBLIKASI
RAQAMLI TEXNOLOGIYALAR VAZIRLIGI

MUHAMMAD AL-XORAZMIY NOMIDAGI
TOSHKENT AXBOROT TEXNOLOGIYALARIUNIVERSITETI
SAMARQAND FILIALI

“RAQAMLI TEXNOLOGIYALAR VA SUN’IY INTELLEKT: MUOMMOLAR, YUTUQLAR VA RIVOJLANISH ISTIQBOLLARI”

MAVZUSIDAGI XALQARO
ILMIY-AMALIY ANJUMANI MA’RUZALAR TO‘PLAMI
2025 yil 24-25 oktabr

II TOM

СБОРНИК ДОКЛАДОВ
Международная научно-практической конференции

“ ЦИФРОВЫЕ ТЕХНОЛОГИИ И ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ: ПРОБЛЕМЫ, ДОСТИЖЕНИЯ И ПЕРСПЕКТИВЫ РАЗВИТИЯ”

октябрь 24-25, 2025

O‘ZBEKISTON RESPUBLIKASI
RAQAMLI TEXNOLOGIYALAR VAZIRLIGI

MUHAMMAD AL-XORAZMIY NOMIDAGI TOSHKENT AXBOROT TEXNOLOGIYALARI UNIVERSITETI SAMARQAND FILIALI

“RAQAMLI TEXNOLOGIYALAR VA SUN’IY INTELLEKT: MUOMMOLAR, YUTUQLAR VA RIVOJLANISH ISTIQBOLLARI” MAVZUSIDAGI XALQARO ILMIY-AMALIY ANJUMANI MA’RUZALAR TO‘PLAMI

24-25- oktabr 2025-yil

II TOM

СБОРНИК ДОКЛАДОВ МЕЖДУНАРОДНАЯ НАУЧНО-ПРАКТИЧЕСКОЙ КОНФЕРЕНЦИИ “ЦИФРОВЫЕ ТЕХНОЛОГИИ И ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ: ПРОБЛЕМЫ, ДОСТИЖЕНИЯ И ПЕРСПЕКТИВЫ РАЗВИТИЯ”

24-25- октября 2025 года

SAMARQAND 2025

KONFERENSIYA TASHKILIY QO‘MITASINING
T A R K I B I:

Z. A. Karshiyev	Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti Samarqand filiali direktori
A.R.Axmedjonov	Ilmiy ishlar va innovatsiyalar bo‘yicha direktor o‘rinbosari
O.M.Rajabov	Yoshlar masalalari va ma’naviy-ma’rifiy ishlar bo’yicha direktorning birinchi o’rinbosari
D.K. Yakubjanova	O‘quv ishlari bo‘yicha direktor o‘rinbosari
Sh.Y.Isroilov	Ilmiy tadqiqotlar, innovatsiyalar va ilmiy-pedagogik kadrlarni tayyorlash bo‘limi boshlig‘i
U.X. Narzullayev	Telekommunikatsiya texnologiyalari va kasb ta’limi fakulteti dekani
B.A. Nazarov	Kompyuter injiniringi fakulteti dekani
A.S.Kurbaniyazov	O‘quv-uslubi boshqarma boshlig‘i

DASTURIY QO‘MITA TARKIBI:

R.Sh. Indiaminov	Tabiiy fanlar kafedrasi professori
A.B. Qarshiyev	Dasturiy injiniring kafedrasi professori
M.U.Yaxshiboyev	Tabiiy fanlar kafedrasi mudiri
X.A. Primova	Axborot texnologiyalari kafedrasi professori
N.I. Abdullayeva	Kompyuter tizimlari kafedrasi mudiri
I.M. Boynazarov	Dasturiy injiniring kafedrasi mudiri
I.Sh. Xujayarov	Axborot texnologiyalari kafedrasi mudiri
N.R. Zaynalov	Axborot xavfsizligi kafedrasi mudiri
X.E. Raxmanov	Axborot ta’lim texnologiyalari kafedrasi mudiri
X.B. Mirzokulov	Telekommunikatsiya injiniringgi kafedrasi mudiri
D.F.Toirova	Tillar kafedrasi mudiri
X. Samatov	Ijtimoiy gumanitar fanlar kafedrasi mudiri

To‘plam TATU Samarqand filiali Kengashining 2025-yil 30-sentabrda o‘tkazilgan 2-sonli yig‘ilish qarori bilan chop etishga tavsiya etilgan

© “DOKTOR POLIGRAF” Printing house, 2025
© TATU Samarqand filiali,2025

5-SHO‘BA

MA’LUMOT UZATISH TARMOQLARI VA AXBOROT XAVFSIZLIGI MUAMMOLARI

REAL-TIME IDS FOR ELECTRIC VEHICLE CHARGING NETWORKS WITH ONLINE ML

N. Zaynalov[1], G. Juraev[2], D. Kilichev[3], D. Turimov[4], N. Saydirasulov[4]
[1]Samarkand branch of Tashkent University of Information Technologies named after Muhammad al-Khwarizmi, Uzbekistan
[2]National University of Uzbekistan named after Mirzo Ulugbek, Uzbekistan
[3]Samarkand branch of Tashkent state university of economics, Uzbekistan
[4]Gachon University, Republic of Korea
dusmurod@gachon.ac.kr

Abstarct. *Electric-vehicle (EV) charging networks rely on protocols like ISO 15118 and OCPP, which introduces security risks if traffic is not monitored continuously. We build a real-time intrusion detection system tailored to EV charging that uses online Adaptive Random Forest plus ADWIN to track concept drift. The system operates on streaming network traffic and updates itself on the fly, avoiding expensive retraining. Evaluated on CICEVSE2024, it achieves ~99.1% accuracy (binary) and ~98.4% (multiclass), maintains high precision/recall during drift, and processes events in ~0.0037 s each – suitable for deployment at or near charge points. We outline a clean architecture and discuss how protocol context helps flag abnormal behavior.*

Keywords: *Electric Vehicle Charging Systems, Intrusion Detection, Online Learning, Network Security, Smart Grid.*

Introduction

The global adoption of electric vehicles (EVs) is accelerating rapidly, driven by advances in battery technology, environmental goals, and government incentives. This growth has led to a corresponding expansion of Electric Vehicle Charging Systems (EVCS), which form a critical component of the emerging smart grid ecosystem. EV charging infrastructures rely on intelligent communication among vehicles, charging stations, and cloud-based management systems to ensure efficient energy distribution and billing. Protocols such as the Open Charge Point Protocol (OCPP), Open Charge Point Interface (OCPI), and ISO 15118 facilitate interoperability across manufacturers and service providers. However, these protocols also introduce significant cybersecurity vulnerabilities, as malicious actors may exploit communication channels to disrupt service, manipulate billing data, or gain unauthorized access to user and network resources [1].

Traditional Intrusion Detection Systems (IDSs) are generally trained on static datasets and are therefore unable to adapt to the evolving characteristics of cyberattacks and network behaviors. In the context of EVCS, where data streams are continuous and non-stationary, this limitation becomes critical. Attack patterns can change due to firmware updates, new communication standards, or shifts in user behavior, leading to a phenomenon known as concept drift—where the statistical distribution of data changes over time. Static IDS models degrade quickly under these conditions, resulting in reduced detection accuracy and delayed threat response [2].

To address these challenges, online machine learning techniques have gained attention for their ability to learn incrementally from streaming data without full retraining. Among these, the Adaptive Random Forest (ARF) algorithm, combined with ADaptive WINdowing (ADWIN) drift detection, has demonstrated strong potential for real-time adaptation. ARF maintains an ensemble of decision trees that dynamically evolve as new data arrive, while ADWIN monitors performance metrics to identify and react to drift events automatically. This combination provides a robust mechanism to detect emerging threats in near real-time with minimal computational overhead.

Methods

The proposed intrusion detection framework is designed to identify cyberattacks in Electric Vehicle Charging Systems (EVCS) using real-time, adaptive learning. It operates as a continuous processing pipeline that collects network traffic, prepares it for analysis, and updates its model incrementally to detect both known and emerging threats. The system focuses on communications

based on ISO 15118 and OCPP protocols, where dynamic message exchanges between vehicles, chargers, and backend servers are common.

The framework was developed and evaluated using the CICEVSE2024 dataset, which contains labeled network traffic from real EV charging sessions, including both benign and multiple attack types. The data were cleaned to remove redundant and incomplete entries, normalized to ensure consistent scaling across features, and encoded into a numerical format suitable for machine learning. This preprocessing ensured that the model could operate efficiently in a streaming environment without retraining from scratch [3].

At the core of the framework lies the Adaptive Random Forest (ARF) algorithm, an ensemble of incremental decision trees capable of updating in real time as new data arrive. Each tree contributes a partial decision, allowing the ensemble to maintain high predictive accuracy while adapting to evolving data distributions. To handle changing attack patterns, the model integrates ADWIN (ADaptive WINdowing), a drift detection method that monitors performance and automatically triggers model updates when significant shifts in data are detected. This mechanism enables the IDS to remain accurate under non-stationary network conditions.

The framework's performance was evaluated through binary (attack vs. normal) and multiclass (specific attack type) classifications. Key metrics included accuracy, precision, recall, and F1-score, along with processing latency per data instance. The system achieved an average accuracy of 99.1% for binary and 98.4% for multiclass detection, while maintaining an inference time of about 0.0037 seconds per instance, confirming its capability for real-time operation. The proposed approach thus provides a practical and scalable solution for safeguarding EV charging infrastructures against evolving cyber threats.

Experimental Results

The proposed real-time intrusion detection framework was evaluated using the CICEVSE2024 dataset, which represents realistic communication traffic in electric vehicle charging systems. The experiments were designed to test the model's detection accuracy, adaptability to changing data patterns, and computational efficiency under streaming conditions. All experiments were conducted using Python-based implementations of the Adaptive Random Forest (ARF) and ADWIN algorithms on a standard workstation with an Intel i7 processor and 16 GB of RAM.

Authors	Year	Dataset	Model	Learning Method	Class	Accuracy	Precision	Recall	F1-Score
Buedi et al. [46]	2024	CICEVSE2024: Network Traffic	Random Forest	offline	15	0.9374	0.9694	0.9374	0.9478
			Support Vector Machine	offline	15	0.9413	0.9151	0.9413	0.9280
Bozömeroğlu et al. [49]	2024	CICEVSE2024: Network Traffic	Decision Tree	offline	13	0.9999	0.9999	0.9999	0.9999
Purohit et al. [50]	2024	CICEVSE2024: Network Traffic	Federated Learning	federated	2	0.9697	-	-	0.9740
Rahman et al. [51]	2025	CICEVSE2024: Host Data	Deep Learning	offline	3	0.9754	0.9757	0.9754	0.9754
Benfarhat et al. [52]	2025	CICEVSE2024: Host Data	Temporal Convolutional Network	offline	2 5 17	1.0 1.0 0.9300	- - -	- - -	- - -
Our Proposed Model	2025	CICEVSE2024: Network Traffic	Adaptive Random Forest	online	2 15	0.9913 0.9840	0.9999 0.9840	0.9914 0.9840	0.9956 0.9831

Table 1: *Performance Comparison of Models*

The dataset was streamed sequentially to the model to simulate real-time network traffic. The data included both normal operational messages and multiple categories of malicious traffic such as denial-of-service, false data injection, and replay attacks. The model was trained incrementally, updating its internal trees as new instances arrived. This approach allowed the system to adapt dynamically without retraining from scratch, maintaining consistent performance even as the underlying data distribution changed [4].

The results show that the proposed method achieves high accuracy and robustness across both binary and multiclass detection tasks. For binary classification, distinguishing between benign and malicious events, the model reached an average accuracy of 99.1%, with a precision of 99.9%, recall of 99.1%, and an F1-score of 99.6%. For multiclass classification, which identifies specific attack types, the system achieved an overall accuracy of 98.4% and an average F1-score of 98.3%. These outcomes confirm that the model can correctly identify a wide range of attacks with minimal false positives or missed detections (Table 1).

In addition to accuracy, computational performance was evaluated to ensure the framework's suitability for real-time deployment. The average processing time per instance was approximately 0.0037 seconds, demonstrating that the model can handle continuous, high-volume data streams without introducing significant latency. The integration of ADWIN further improved adaptability, allowing the system to recover rapidly from concept drift events while sustaining accuracy levels above 98% throughout all drift scenarios [1].

Conclusions

This study presented a real-time intrusion detection framework designed to enhance the cybersecurity of Electric Vehicle Charging Systems (EVCS) using online adaptive machine learning. The proposed approach combines the Adaptive Random Forest (ARF) algorithm with the ADWIN drift detection method to enable continuous learning and automatic adaptation to evolving attack patterns. By processing network traffic in a streaming fashion, the framework eliminates the need for complete retraining, reducing computational overhead and improving responsiveness to concept drift in dynamic charging environments.

References

1. Makhmudov, F.; Kilichev, D.; Giyosov, U.; Akhmedov, F. Online Machine Learning for Intrusion Detection in Electric Vehicle Charging Systems. *Mathematics* 2025, *13*, 712. https://doi.org/10.3390/math13050712

2. Kilichev, D.; Turimov, D.; Kim, W. Next–Generation Intrusion Detection for IoT EVCS: Integrating CNN, LSTM, and GRU Models. *Mathematics* 2024, *12*, 571. https://doi.org/10.3390/math12040571

3. Kilichev, D.; Kim, W. Hyperparameter Optimization for 1D-CNN-Based Network Intrusion Detection Using GA and PSO. *Mathematics* 2023, *11*, 3724. https://doi.org/10.3390/math11173724

4. A. Abdusalomov, D. Kilichev, R. Nasimov, I. Rakhmatullayev and Y. Im Cho, "Optimizing Smart Home Intrusion Detection With Harmony-Enhanced Extra Trees," in IEEE Access, vol. 12, pp. 117761-117786, 2024, doi: 10.1109/ACCESS.2024.3422999

6-SHO‘BA. RAQAMLI MODELLASHTIRISH VA HISOBLASH USULLARI

“RAQAMLI TEXNOLOGIYALAR VA SUN’IY INTELLEKT: MUOMMOLAR, YUTUQLAR VA RIVOJLANISH ISTIQBOLLARI” MAVZUSIDAGI XALQARO ILMIY-AMALIY ANJUMANI

MA’RUZALAR TO‘PLAMI

24-25 oktabr 2025-yil

II TOM

“DOKTOR POLIGRAF” MChJ. nashriyot - matbaa ijodiy bo`limi,

Samarqand - 2022.

Tasdiqnona № 12364 (17.03.2015)

Chop etishga ruxsat etildi: 15.10.2025 y.

© **“DOKTOR POLIGRAF” MChJ.** nashriyot - matbaa ijodiy bo`limi, Samarqand.

22.10.2025 yilda chop etildi.

Qog‘oz bichimi A5, 60x84 1/8, Ofset qog‘ozi.

“Times New Roman” garniturasi.

Nashr bosma tabog‘i 48,75

Buyurtma № 005/23A. Adadi 25 nusxa

“DOKTOR POLIGRAF” MChJ.

Nashriyot - matbaa bo‘limida chop etildi.

Tasdiqnona № 12364 (17.03.2015)

Manzil: Samarqand vil. Samarqand sh. Buyuk Ipak Yo`li.