UDC 004.738.5 DOI: 10.18372/2073-4751.81.20120

Alkema V.V.,
orcid.org/0009-0000-0009-8237,
e-mail: vitalii.alkema@gmail.com,
Huzii M.M., Candidate of Technical Sciences,
orcid.org/0000-0003-4807-8862,
e-mail: nn05@ukr.net

HYBRID MODELS FOR DETECTING SHADOWBURST ANOMALY IN INDUSTRIAL IoT TRAFFIC

State University "Kyiv Aviation Institute"

Introduction

The Industrial Internet of Things (IIoT) represents a convergence of operational technologies (OT) and information technologies (IT), forming intelligent and interconnected cyber-physical systems. These systems are increasingly deployed in sectors such as smart manufacturing, critical infrastructure, and industrial automation, offering benefits such as real-time monitoring, predictive maintenance, and increased operational efficiency. However, the widespread deployment of IIoT devices also significantly expands the attack surface, introducing new vulnerabilities and threats that traditional security architectures are often ill-equipped to handle.

The advent of Industry 4.0 has transformed industrial operations by embedding intelligence into machines, production lines, and cyber-physical systems through the adoption of Industrial Internet of Things (IIoT), real-time analytics, edge-cloud integration, and autonomous control. Smart factories are increasingly reliant on distributed sensor networks, programmable logic controllers (PLCs), and lightweight industrial protocols such as MQTT and OPC-UA. While this interconnectedness enhances operational efficiency, it also creates new and complex cybersecurity vulnerabilities.

A particularly insidious threat in this context is the emergence of latent anomalies that are difficult to detect through traditional monitoring systems. One such class of threat, which we refer to as the ShadowBurst anomaly, exemplifies a stealthy burst of traffic that superficially mimics legitimate IIoT device behavior but represents a deviation from temporal or statistical baselines. These anomalies may be triggered by botnet activation, malware payload delivery, or covert command injection, and typically appear as short, transient spikes embedded within otherwise stable traffic patterns.

In smart manufacturing environments, where deterministic timing and real-time data exchange are crucial, even minor undetected anomalies can propagate into large-scale disruptions, such as production halts, faulty quality control feedback, or unsafe machine states. This makes the detection of anomalies like ShadowBurst mission-critical, especially since they are not detected by traditional signature-based intrusion detection systems (IDS), which rely on known patterns, or basic anomaly detectors that flag only gross deviations. Furthermore, Industry 4.0 environments operate under tight latency constraints, with devices often exchanging millisecond-scale telemetry. ShadowBurst anomalies exploit this precision by injecting high-frequency, low-duration packets that are carefully shaped to evade detection. The anomalies may also be distributed across multiple devices, forming a coordinated low-and-slow attack pattern, further complicating their identification.

As a result, hybrid detection approaches – which combine deep learning, statistical profiling, protocol-specific rules, and edge-level temporal modeling – are increasingly being explored as a defense mechanism. These models aim to learn not only what is happening, but also how and when, enabling

them to capture the timing irregularities and behavioral drift associated with ShadowBurst-type anomalies.

In summary, the complexity of Industry 4.0 ecosystems, combined with the sophistication of ShadowBurst-like anomalies, underscores the need for resilient, adaptive, and context-aware anomaly detection models that can operate in real time across heterogeneous IIoT environments.

One of the most pressing challenges in securing IIoT networks is the detection of anomalous traffic behavior, especially in environments where data volumes are high, device heterogeneity is common, and timing constraints are strict. Unlike conventional enterprise IT networks, IIoT systems often operate under deterministic communication schedules, with devices generating predictable and repetitive traffic patterns [1]. This makes them particularly susceptible to stealthy, well-camouflaged attacks, which can blend into the baseline traffic and evade detection for long periods.

To address this, we introduce and investigate a specific type of anomaly known as the ShadowBurst anomaly. ShadowBurst refers to sudden, short-lived bursts of traffic generated by IIoT devices that mimic normal operational behavior in terms of packet structure and timing but represent a significant deviation from established behavioral baselines. [3] These anomalies can be the result of malicious activity, such as command injection or botnet activation, or benign misconfigurations that go unnoticed due to their transient and subtle nature.

Current detection techniques such as signature-based intrusion detection systems (IDS) and basic statistical models often fail to capture such anomalies. Signature-based systems are limited to known attack patterns, while purely statistical models lack contextual awareness. To overcome these limitations, this study proposes a hybrid detection approach that integrates multiple methodologies, including machine learning (ML), time-series analysis, and behavioral profiling. The hybrid model is designed to combine the strengths of each individual technique to achieve robust and adaptive detection of ShadowBurst anomalies in real-time industrial traffic.

The purpose and objectives of the study

1. formally define the ShadowBurst anomaly in the context of IIoT,
2. evaluate the limitations of existing detection models,
3. assess the effectiveness of the proposed solution using simulation.

The outcomes of this research can contribute to more resilient IIoT security architectures and enable early intervention in the event of hidden network threats.

The growing integration of Industrial Internet of Things (IIoT) systems into critical infrastructure has brought significant advancements in automation but has simultaneously exposed these networks to new cybersecurity threats. One of the pressing challenges is the detection of subtle, fast-evolving anomalies within network traffic. As a result, hybrid models that combine multiple detection paradigms – such as machine learning (ML), statistical methods, and rule-based systems – have gained traction in recent research.

Literature Review

A foundational work by Shahin, Chen, and Hosseinzadeh (2022) introduced a deep hybrid learning model that combines Convolutional Neural Networks (CNN) and Long Short-Term Memory (LSTM) networks to detect cyberattacks targeting IIoT devices. Their model achieved remarkable detection accuracy exceeding 98%, particularly in identifying botnet and spoofing attacks. They emphasize that "hybrid deep learning structures can significantly improve feature abstraction and classification in noisy IIoT data streams" [2].

Similarly, Hao, Yang, and Yang (2021) presented a hybrid statistical-ML model for anomaly detection in industrial cyber–physical systems. Their approach integrates Local Outlier Factor (LOF) and Principal Component Analysis (PCA) with real-time traffic classifiers. Unlike purely ML-driven methods, their framework enhances robustness by incorporating domain-specific statistical features. They demonstrate that combining

"statistical preprocessing with supervised learning yields faster convergence and better outlier sensitivity" [3].

Expanding on distributed architectures, Yang et al. (2023) proposed a cloud-edge coordinated anomaly detection system, where initial traffic filtering is performed at the edge, and advanced pattern recognition is executed in the cloud. This architecture is well-suited for IIoT environments, where latency and resource constraints limit centralized processing. Their experimental results show improved detection latency and accuracy, particularly for transient anomalies that resemble *ShadowBurst*-type behavior [4].

Another relevant contribution by Al-Zaidawi and Çevik (2025) leverages hybrid optimization and Multi-Criteria Decision-Making (MCDM) techniques to fine-tune deep learning models for IIoT network monitoring. Their approach combines metaheuristic optimization with feature-ranking algorithms, which enhances the model's ability to adapt to fluctuating traffic baselines. This is particularly relevant in industrial environments with frequent reconfigurations and device heterogeneity [5].

In the context of Industry 4.0, Srivastav et al. (2025) proposed HYRIDE, a robust hybrid intrusion detection system combining statistical modeling with ensemble machine learning. Tested on the ToN-IoT dataset, their model demonstrates superior resistance to adversarial examples and false positives. The authors argue that hybrid systems provide a "layered defense against both known and unknown threats" [6].

Francis, Souri, and İnanç (2024) focused specifically on the MQTT protocol, a lightweight communication standard widely used in IIoT. They implemented a hybrid detection system incorporating rule-based filtering and anomaly scoring models tailored to MQTT payloads. Their work highlights how protocol-aware hybridization improves specificity and reduces overhead in constrained industrial networks [7].

Ali and Baheti (2024) explored context-aware hybrid intrusion detection methods that blend packet analysis with temporal features. Their model is particularly effective in detecting coordinated attacks and stealthy traffic manipulation, showing promise in identifying anomalies that may otherwise evade both signature and behavioral models [8].

Further expanding the ensemble landscape, Babbar et al. (2024) introduced a deep-learning–based hybrid model that uses convolutional neural networks and stacked ensemble techniques to protect wireless sensor networks in smart manufacturing environments. Their study utilizes the BoT-IoT dataset and reports significant improvement in anomaly classification precision [9].

Touileb et al. (2024) proposed an LSTM–autoencoder hybrid architecture optimized for IIoT traffic sequences. Their model effectively captures temporal correlations and is capable of detecting subtle deviations in device behavior. The use of reconstruction loss metrics enhances its sensitivity to drift and rare event patterns [10].

Lastly, Sangeetha and Naidu (2024) presented an ensemble-hybrid model that integrates deep learning and traditional classifiers. Their system demonstrates high adaptability across heterogeneous IIoT segments and shows resilience against zero-day anomalies. They advocate for hybridization as a "bridge between interpretability and performance in mission-critical systems" [11].

The growing integration of Industrial Internet of Things (IIoT) systems into critical infrastructure has brought significant advancements in automation, but has simultaneously exposed these networks to new cybersecurity threats. One of the pressing challenges is the detection of subtle, fast-evolving anomalies within network traffic. As a result, hybrid models that combine multiple detection paradigms – such as machine learning (ML), statistical methods, and rule-based systems – have gained traction in recent research.

A foundational work by Shahin, Chen, and Hosseinzadeh (2022) introduced a deep hybrid learning model that combines Convolutional Neural Networks (CNN) and Long Short-Term Memory (LSTM) networks to detect cyberattacks targeting IIoT devices. Their model achieved remarkable detection

accuracy exceeding 98%, particularly in identifying botnet and spoofing attacks. They emphasize that "hybrid deep learning structures can significantly improve feature abstraction and classification in noisy IIoT data streams" [2].

Formal Hybrid Model Architecture

ShadowBurst anomaly refers to a transient, stealthy, and burst-like deviation in network traffic behavior within Industrial IoT (IIoT) environments, characterized by sudden short-lived surges in packet transmission that superficially conform to legitimate operational patterns but violate established statistical or temporal baselines. [2].

Let *T(t)* be the observed traffic volume over time *t* and let *B(t)* be the expected or baseline traffic profile derived from normal device behavior. A ShadowBurst event occurs at time interval $[t_s, t_e]$ if the following conditions are satisfied:

Transient

Burst condition:

$$\exists t_s, t_c \in \mathbb{R},\ t_c - t_s < \Delta_{threshold},\ \text{such that}\ T(t) \gg B(t) \forall t \in [t_s, t_c]. \quad (1)$$

Stealth condition: The traffic structure S(T) during the burst mimics normal patterns:

$$D_{protocol} = \big(T(t)\big) \approx D_{protocol}\big(B(t)\big),\ \forall t \in [t_s, t_c]\ . \quad (2)$$

Deviation from baseline behavior:

The burst causes a significant anomaly score under behavioral or statistical models:

$$A\big(T(t)\big) > \alpha. \quad (3)$$

For some anomaly detection function A and threshold α.

In the context of Industrial IoT traffic monitoring, the anomaly detection function A: $T \rightarrow \mathbb{R}$ maps a segment of observed traffic T(t)to a numerical anomaly score that quantifies the degree of deviation from expected behavior. A traffic segment is flagged as anomalous if its score exceeds a pre-defined threshold α.

In industrial environments operating under the paradigms of Industry 4.0, sensor data is typically time-dependent, noisy, and highly correlated. This makes accurate state estimation and anomaly detection particularly challenging. Kalman Filters (KFs) are widely used for predicting the internal state of linear dynamic systems, offering effective mitigation of measurement noise and latency in sensor streams. However, Kalman filters on their own lack semantic depth and are poorly suited for identifying nonlinear, context-driven anomalies-particularly stealthy, short-lived threats like the ShadowBurst anomaly.

ShadowBurst anomalies are characterized by sudden, transient spikes in traffic or control commands that mimic legitimate device behavior, thereby evading threshold-based or signature-based detection. These anomalies are often embedded within otherwise regular system behavior, making them difficult to isolate in noisy environments.

To address this, we propose a hybrid anomaly detection approach that combines the predictive and smoothing capabilities of Kalman filters with the pattern recognition and generalization strengths of machine learning models – such as Autoencoders, LSTM networks, or Isolation Forests. In this setup, the Kalman filter first estimates the expected behavior of the system, and deviations from this prediction (i.e., residuals) are then analyzed by the machine learning model to detect semantic or structural inconsistencies associated with ShadowBurst events (Fig 1.). This layered methodology enhances both temporal precision and contextual awareness, enabling effective detection of short-duration, protocol-conformant anomalies that traditional methods might overlook.

The diagram illustrates a hybrid anomaly detection architecture designed to identify ShadowBurst anomalies in Industrial IoT (IIoT) traffic. The core of the system is the anomaly detection function A(T), which operates on traffic segments TTT and combines three independent analytical components: a statistical component, a Kalman filter with Isolation Forest, and a behavioral profiling

component. The outputs of these components are linearly combined using weighted coefficients to compute an overall anomaly score.

At the top level, the system receives a traffic segment T, which may consist of packet rates, protocol activity, sensor data, or command sequences over time. This segment is passed to the anomaly detection function:

$$A(T) = \lambda_1 A_{stat}(T) + \lambda_2 A_{hybrid-KF}(T) + \lambda_3 A_{behav}(T). \quad (3)$$

Statistical Component Astat(T): This component evaluates numerical deviations from baseline behavior using standard statistical metrics, such as z-scores. It identifies volume-based anomalies, such as unexpected packet bursts or command frequency shifts, that may indicate a ShadowBurst event.

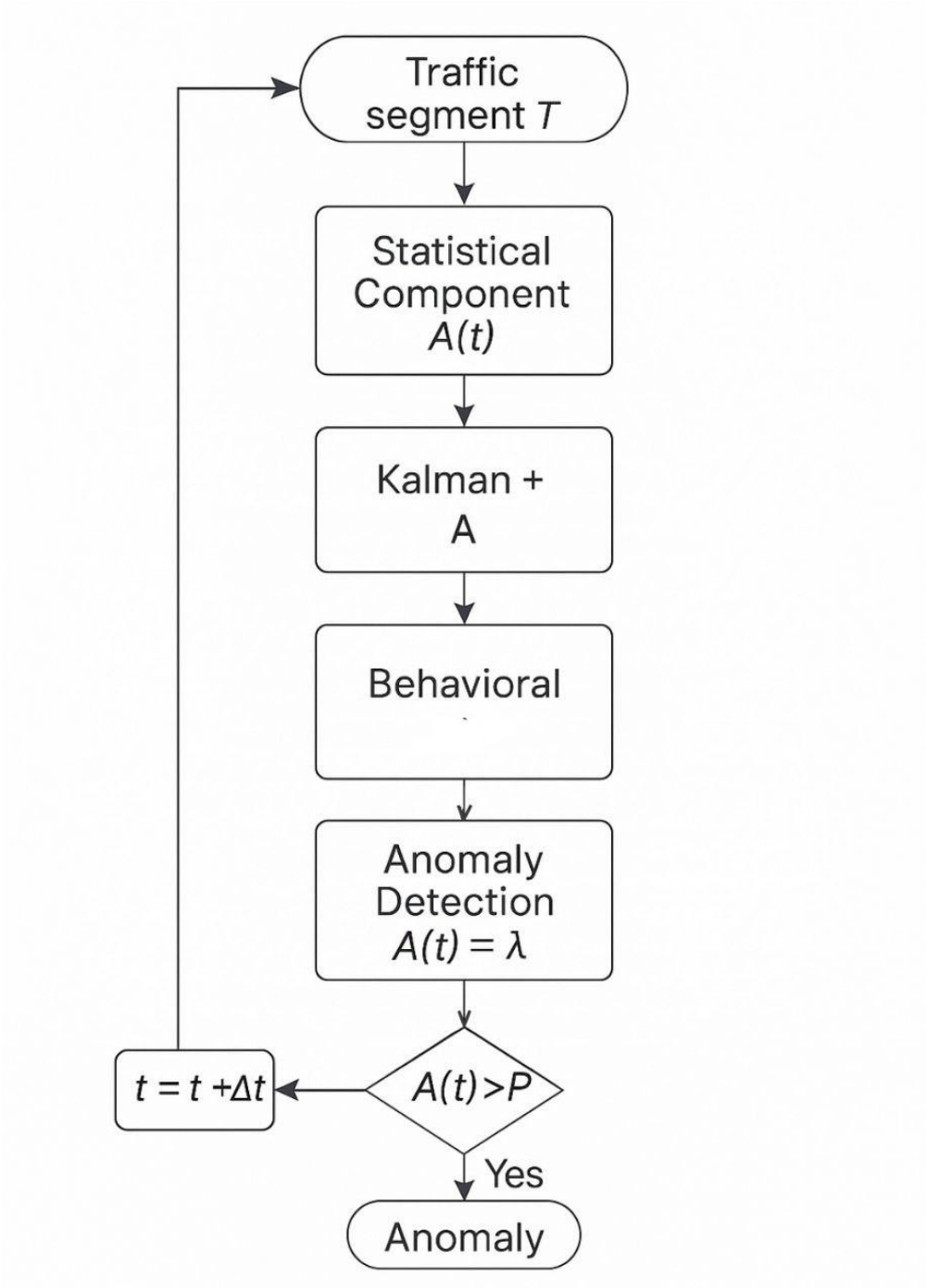

Fig. 1. Hybrid Kalman–Isolation Forest Model

Kalman + Isolation Forest Component A_{hybrid}-*KF(T)*: In this module, a Kalman filter estimates the expected value of an incoming signal $\hat{x}_t = Kalman(z_t)$. The residual $r_t = |z_t - \hat{x}_t|$ captures the deviation between observed and expected behavior. This residual is then analyzed by an Isolation Forest model, which performs nonlinear anomaly detection based on tree-based isolation of outliers. This component is particularly effective at detecting short-lived, stealthy anomalies like ShadowBurst, which may otherwise blend into normal traffic patterns.

Behavioral Component Abehav This component models the temporal and semantic behavior of IIoT devices. It uses divergence measures such as the Kullback–Leibler divergence $D_{KL}(P_t \parallel P_B)$ to compare the current behavior distribution Pt with a historical baseline P_B. It is designed to detect protocol-compliant but suspicious changes, such as irregular command timing or unusual communication intervals.

The outputs of these three subsystems are aggregated through a weighted sum, where the coefficients λ_1, λ_2, λ_3 are tuned based on the sensitivity and reliability of each model in the target environment.

The final step in the flow determines whether the computed anomaly score exceeds a predefined threshold, which would trigger an alert or further investigation. This decision process enables the system to flag subtle, short-duration anomalies that conform to protocol standards yet violate normal system behavior – the hallmark of a ShadowBurst attack.

This hybrid detection framework is particularly suited for Industry 4.0 environments where traffic is time-sensitive, complex, and vulnerable to low-profile attacks that traditional IDS tools fail to capture.

ShadowBurst Detection Using Kalman Filter and Isolation Forest Simulation

The simulation and anomaly detection in the presented figure were conducted using Python 3 with core scientific libraries including NumPy, Matplotlib, and scikit-learn. Synthetic Industrial IoT traffic data was generated using NumPy to simulate a low-variance, sinusoidal baseline signal representing normal device behavior. A ShadowBurst anomaly was injected by introducing a short-duration high-frequency spike into the traffic at a specific time interval, simulating a stealthy burst that resembles legitimate traffic patterns. A simple one-dimensional Kalman filter was manually implemented to estimate the expected traffic behavior over time and produce a smoothed prediction signal. The residuals – computed as the absolute difference between observed and predicted values – served as the key input features for anomaly detection. These residuals were passed into an Isolation Forest model from scikit-learn, which assigned anomaly scores and identified outliers corresponding to ShadowBurst events. The complete input to the model included raw traffic observations z_t, Kalman predictions $\hat{x}_t$, residuals r_t, and optional contextual features such as time step indices. This hybrid Kalman–Isolation Forest setup enables effective detection of short, transient anomalies that deviate from temporal norms without violating protocol structures.

Figure 2 illustrates the detection of a ShadowBurst anomaly in synthetic IIoT traffic using a hybrid approach that combines Kalman filtering and Isolation Forest.

The blue line represents the observed traffic signal over time, which simulates normal IIoT behavior with an artificially injected ShadowBurst anomaly between time steps 250 and 260. This anomaly consists of a short, high-frequency burst that mimics legitimate traffic patterns.

The green dashed line shows the predicted signal generated by a Kalman filter, which continuously estimates the expected behavior of the system. The filter effectively smooths out noise and provides a baseline for comparison.

The red crosses indicate data points flagged as anomalies by the Isolation Forest, which operates on the residuals $r_t = |z_t - \hat{x}_t|$ – the absolute difference between the observed and predicted values. These residuals highlight local deviations that escape standard threshold-based detection methods.

This hybrid technique successfully detects the ShadowBurst anomaly despite its transient nature and protocol-compliant structure. The Kalman filter identifies unexpected deviations in system dynamics, while the Isolation Forest captures statistical outliers based on non-linear partitioning of the residual space.

Together, this method demonstrates the effectiveness of combining temporal prediction with machine learning-based anomaly scoring to identify stealthy, short-duration threats that are characteristic of ShadowBurst attacks in Industrial IoT networks.

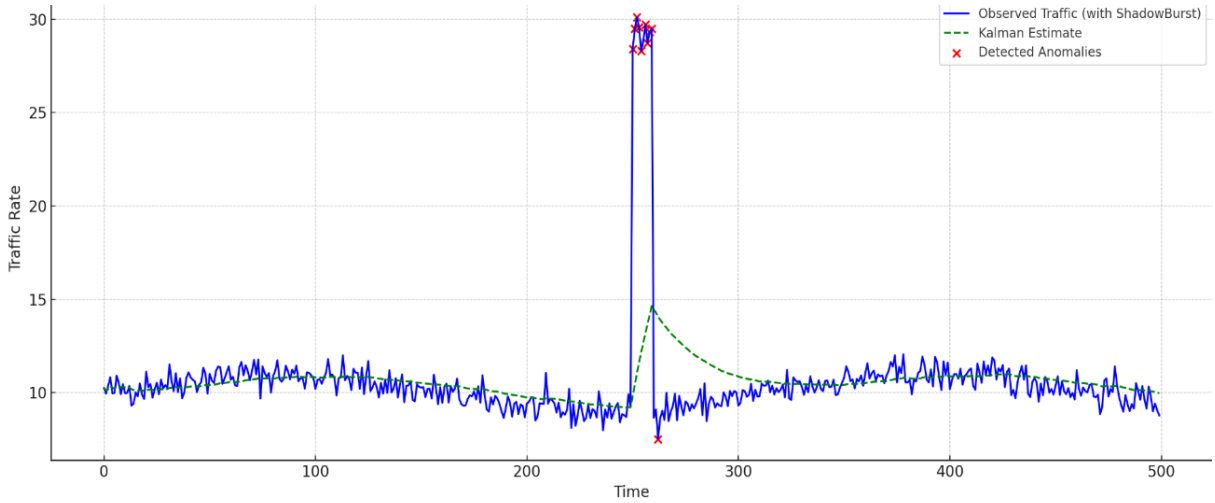

Fig. 2. ShadowBurst Detection using Kalman Filter + Isolation Forest

Conclusions

This study introduces ShadowBurst as a new class of short-duration, stealthy anomalies that pose a significant risk to Industrial IoT infrastructures. These anomalies, due to their timing precision and protocol compliance, often go undetected by conventional IDS or statistical outlier models. To address this challenge, a hybrid detection function was designed, combining Kalman filtering for predictive state modeling and residual analysis with Isolation Forest for pattern-based anomaly scoring. The results of simulation experiments indicate that this hybrid architecture is capable of accurately detecting ShadowBurst anomalies, even in noisy or high-frequency IIoT traffic streams. The modular design of the detection function also allows for contextual enrichment through statistical and behavioral components, enabling dynamic adaptation to different industrial settings. This work lays the foundation for developing real-time, scalable, and intelligent threat detection solutions that align with the demands of Industry 4.0 environments. Future work may extend this approach to include deep learning-based behavior modeling and evaluation against real-world IIoT datasets.

References

1. Santiago C. J. S., Abbas H., Thangamani P. An automated workflow for condition monitoring of centrifugal compressors using a combined data-driven and physics-based approach. SPE Annual Technical Conference and Exhibition : proceedings, New Orleans, LA, USA, September 2024 / 2024. P. 414–415. URL: https://onepetro.org/SPEATCE/proceedings-abstract/24ATCE/24ATCE/563693.

2. Shahin M., Chen F. F., Hosseinzadeh A. A deep hybrid learning model for detection of cyber attacks in industrial IoT devices. *The International Journal of Advanced Manufacturing Technology*. 2022. Vol. 121. P. 1597–1614. DOI: 10.1007/s00170-022-10329-6.

3. Hao W., Yang T., Yang Q. Hybrid statistical–machine learning for real-time anomaly detection in industrial cyber–physical systems. *IEEE Transactions on Automation Science and Engineering*. 2021. Vol. 18, no. 3. P. 1234–1247. DOI: 10.1109/TASE.2021.3066927.

4. Yang T., Hao W., Wang W. Cloud-edge coordinated traffic anomaly detection for industrial cyber-physical systems. *Expert Systems with Applications*. 2023. Vol. 213. 119193. DOI: 10.1016/j.eswa.2022.119193.

5. Al-Zaidawi M.Q.J., Çevik M. Advanced deep learning models for improved IoT network monitoring using hybrid optimization and MCDM techniques. *Symmetry*. 2025. Vol. 17, no. 3. 388. DOI: 10.3390/sym17030388.

6. Srivastav S. et al. HYRIDE: Hybrid and robust intrusion detection approach for enhancing cybersecurity in Industry 4.0. *Internet of Things*. 2025. Vol. 22. 100840. DOI: 10.1016/j.iot.2024.100840.

7. Francis G. T., Souri A., İnanç N. A hybrid intrusion detection approach based on message queuing telemetry transport (MQTT) protocol in industrial internet of things. *Transactions on Emerging Telecommunications Technologies*. 2024. Vol. 35, iss. 9. 15 p. DOI: 10.1002/ett.5030.

8. Ali R. M., Baheti M. R. Enhancing IoT security: a study on hybrid intrusion detection methods. *2024 IEEE 3rd World Conference on Applied Intelligence and Computing (AIC)* : proceedings, Gwalior, India, 27–28 July 2024 / IEEE. 2024. P. 1373–1380. DOI: 10.1109/AIC61668.2024.10731133.

9. Babbar H., Rani S., Boulila W. Fortifying the connection: cybersecurity tactics for WSN-driven smart manufacturing in the era of Industry 5.0. *IEEE Open Journal of the Computer Society*. 2024. Vol. 5. P. 112–125. DOI: 10.1109/OJCS.2024.10599217.

10. Touileb L. et al. A hybrid LSTM-autoencoder based approach for network anomaly detection system in IoT environments. *2024 IEEE International Mediterranean Conference on Communications and Networking (MeditCom)* : proceedings, Madrid, Spain, 08–11 July 2024 / IEEE. 2024. P. 125–130. DOI: 10.1109/MeditCom61057.2024.10621202.

11. Sangeetha V., Naidu R. C. A., Bhat A. Integrating deep learning with ensemble approach for anomaly detection in network traffic. *2024 4th International Conference on Mobile Networks and Wireless Communications (ICMNWC)* : proceedings, Tumkuru, India, 04–05 December 2024 / IEEE. 2024. P. 1–5. DOI: 10.1109/ICMNWC63764.2024.10872226.

Alkema V.V., Huzii M.M.

HYBRID MODELS FOR DETECTING SHADOWBURST ANOMALY IN INDUSTRIAL IoT TRAFFIC

The increasing deployment of Industrial Internet of Things (IIoT) systems within Industry 4.0 environments has introduced new cyber-physical vulnerabilities, particularly in the form of stealthy and short-lived anomalies that evade traditional detection mechanisms. This paper introduces and formalizes a novel anomaly type, referred to as ShadowBurst, which consists of protocol-conformant, high-frequency microbursts embedded in otherwise stable traffic streams. We propose a hybrid detection architecture that integrates Kalman filtering for temporal state estimation with machine learning techniques, specifically Isolation Forest, for residual-based outlier detection. The detection function is further enhanced by incorporating statistical scoring and behavioral profiling to improve anomaly visibility. Simulation results confirm that this hybrid Kalman–ML approach enables effective identification of ShadowBurst anomalies in time-sensitive IIoT traffic, addressing gaps left by signature-based and purely statistical models. The proposed model demonstrates high responsiveness to low-duration, protocol-mimicking threats and supports real-time deployment in smart manufacturing environments.

Keywords*: Industrial IoT (IIoT); trafic anomaly; anomaly detection; Kalman filter; Isolation Forest; hybrid models; Industry 4.0; time-series analysis; smart manufacturing.*

Алькема В.В., Гузій М.М.

ГІБРИДНІ МОДЕЛІ ДЛЯ ВИЯВЛЕННЯ АНОМАЛІЙ ТІНЬОВОГО СПЛЕСКУ В ТРАФІКУ ПРОМИСЛОВОГО IoT

Зростаюче розгортання систем промислового Інтернету речей (IIoT) у середовищах Індустрії 4.0 принесло нові кіберфізичні вразливості, зокрема у вигляді прихованих та короткочасних аномалій, які уникають традиційних механізмів виявлення. У цій статті представлено та формалізовано новий тип аномалії, який називається ShadowBurst, що складається з протокольно-сумісних високочастотних мікросплесків, вбудованих у стабільні потоки трафіку. Ми пропонуємо гібридну архітектуру виявлення, яка інтегрує фільтрацію Калмана для оцінки часового стану з методами машинного навчання, зокрема з лісом ізоляції, для виявлення викидів на основі залишків. Функція виявлення додатково покращується шляхом включення статистичного скорингу та поведінкового профілювання для покращення видимості аномалій. Результати моделювання підтверджують, що цей гібридний підхід Калмана-МО дозволяє ефективно ідентифікувати аномалії ShadowBurst у чутливому до часу трафіку IIoT, усуваючи прогалини, залишені моделями на основі сигнатур та суто статистичними моделями. Запропонована модель демонструє високу чутливість до короткотривалих загроз, що імітують протоколи, та підтримує розгортання в режимі реального часу в інтелектуальних виробничих середовищах.

***Ключові слова**: промисловий Інтернет речей (IIoT); аномалія трафіку; виявлення аномалій; фільтр Калмана; ізоляційний ліс; гібридні моделі; Індустрія 4.0; аналіз часових рядів; інтелектуальне виробництво.*