Risk-Oriented Security Management Model for IoT Networks Using a Graph-Autoregressive Approach

Valeriy Lakhno[1,†], Dmytro Kasatkin[1,†], Mykola Tsiutsiura[2,*,†] and Valentyna Makoiedova[2,†]

[1] *National University of Life and Environmental Sciences of Ukraine, Heroiv Oborony 15, 03041, Kyiv, Ukraine*

[2] *State University of Trade and Economics, Kyoto 19, 02156, Kyiv, Ukraine*

Abstract

A new mathematical model of risk-oriented security management in Internet of Things (IoT) networks is proposed. The model combines a graph-autoregressive approach to load forecasting with a decision-making mechanism based on the Conditional Value-at-Risk (CVaR) indicator. The study aims to improve the cyber resilience of IoT networks by integrating spatio-temporal traffic analysis, information security indicators, and economic risk assessment. It is proved that existing methods and models for predicting and detecting anomalies are focused mainly on time series. However, they do not take into account the topological structure of IoT networks and the relationships between nodes, which reduces their effectiveness. The developed graph-autoregressive model simultaneously takes into account the time dependence of traffic and the spatial correlation between network nodes through the Laplacian of the graph. Based on the forecast residuals, the level of anomaly and the probability of an attack are estimated, taking into account behavioral and network security indicators. A risk-oriented decision-making module is proposed that uses CVaR as a criterion for the optimal choice of protective actions. This allowed the defense system to focus on the worst-case scenarios of high-cost attacks, minimizing potential losses. Experimental testing on the data of a smart home-type IoT network confirmed the effectiveness of the proposed model. A comparative analysis with classical approaches (ARIMA, LSTM, Isolation Forest) showed an increase in load prediction accuracy by 15% and an improvement in attack detection quality (F1-score) by 7-10%. The scientific novelty of the work is the synthesis of a graph-autoregressive model with risk-oriented optimization, which takes into account both spatial and temporal changes in the network and economic aspects of security management. The practical significance lies in the possibility of using the model as an analytical module in IoT monitoring and cybersecurity systems for automated selection of countermeasures in real time.

Keywords

Internet of Things (IoT), information security, graph autoregressive model, load forecasting, anomaly detection, risk-oriented management, Conditional Value-at-Risk (CVaR), graph methods

1. Introduction

Over the past decades, the Internet of Things (IoT) technology has become an integral part of many business processes in various fields - from household smart home systems to industrial complexes and critical infrastructure [1]. However, an increase in the number of devices and the complexity of the IoT network topology is accompanied by an increase in the risk of information security (IS) incidents [2]. According to analytical agencies [1], the number of active IoT devices will exceed 25 billion by 2030. And the amount of data generated by IoT devices will grow to several zettabytes per year. That is, the exponential growth in the number of IoT devices is accompanied by a significant complication of the network topology and an increase in inter-node interactions. As a result, this will lead to an increased risk of information incidents.

Information Technology and Implementation (IT&I-2025), November 20-21, 2025, Kyiv, Ukraine

[*] Corresponding author.

[†] These authors contributed equally.

✉ lva964@nubip.edu.ua (V. A. Lakhno); d.kasatkin@nubip.edu.ua (D. Y. Kasatkin); mitsiutsiura@gmail.com (M. I. Tsiutsiura); makoiedova.valentyna@gmail.com (V. O. Makoiedova)

0000-0001-9695-4543 (V. A. Lakhno); 0000-0002-2642-8908 (D. Y. Kasatkin); 0000-0003-4713-7568 (M. I. Tsiutsiura); 0000-0001-7518-894X (V. O. Makoiedova)

Unlike classical IT systems, the IoT environment has a much higher degree of heterogeneity. This makes existing information security methods focused on centralized architectures ineffective. Moreover, the large number of connected IoT network sensors and actuators has created new attack vectors. These include remote control over nodes, data spoofing, distributed denial-of-service (DDoS) attacks, the use of IoT devices in botnets, and more. As a result, IoT networks have become one of the most vulnerable components of modern cyber-physical systems.

It should be noted that most existing anomaly detection and monitoring systems for IoT networks operate in a reactive mode. They only detect deviations after an incident has actually occurred. Such solutions are based mainly on statistical indicators or fixed thresholds. That is, a priori, such solutions reduce their effectiveness in using statistical indicators in the case of targeted low-intensity attacks or changes in device behavior over time. At the same time, the development of machine learning (ML) and time series analysis methods has opened up opportunities for the synthesis of flexible hybrid models capable of predicting the future state of an IoT network and identifying potential threats at the stage of their formation. It should be noted that most of the research in the field of IoT device security is currently focused on time dependencies. These studies do not take into account the spatial structure of the IoT network. Meanwhile, the interconnections between nodes - topological, informational, and behavioral - have a significant impact on the parameters of attacks. For example, compromising a central router or a node with a high degree of centrality will lead to an avalanche of threats to neighboring devices. Therefore, an integrated approach that combines time series analysis, network graph structure, and information security indicators is a relevant topic [3, 4].

The issue of decision-making in cyber defense systems also requires special attention. In most cases, the choice of countermeasures is made without taking into account the expected risks or possible consequences for the quality of service (QoS). This can potentially lead to excessive resource consumption, downtime, or even loss of communication between nodes. In this vein, it is advisable to apply risk-oriented methods. These methods are able to take into account both the probability of an attack and the potential damage in case of its realization. One of these criteria is Conditional Value-at-Risk (CVaR). This indicator will allow to focus the protection strategy on the worst-case scenarios with high losses, increasing the cyber resilience of the system. That is why it is relevant to develop adaptive risk-oriented models that combine predicting the behavior of the IoT system with threat detection and selecting optimal preventive actions to ensure network security.

2. Problem statement

Modern methods of load forecasting in IoT networks are mostly based on time series analysis, which allows to model traffic dynamics and identify periodic patterns in the functioning of individual devices. However, such approaches, despite their technical maturity, have a number of limitations that significantly reduce their effectiveness in cybersecurity tasks for distributed infrastructures. The main drawback is that most models focus exclusively on time dependencies and do not take into account the spatial structure of the IoT network - its topology, the nature of connections between nodes, the intensity of interaction, and the correlation of the behavior of individual devices. As a result, the models ignore the interaction of nodes, which can be crucial when failures or attacks spread across the network.

Another significant limitation of classical approaches is the lack of mechanisms to take into account information security policies and device behavior. In most existing traffic forecasting systems, security factors are not integrated into the analytical core, but are treated as external conditions. This leads to the fact that the breach detection system cannot timely differentiate technical deviations from potentially malicious activity. In particular, even modern machine learning algorithms used in the field of IoT monitoring do not always take into account events detected by Intrusion Detection Systems (IDS) or Security Information and Event Management (SIEM) platforms.

As a result, the analytical system is unable to synthesize a holistic picture of network security and correctly assess the likelihood of cyberattacks.

Another critical aspect is the limitations of existing anomaly detection methods, which mostly rely only on statistical analysis of deviations in traffic or device behavior from the average. While such approaches can identify individual atypical events, they do not provide sufficient contextual depth to detect complex, multi-stage attacks that propagate through interconnected network nodes. As a result, the system responds to incidents mostly after the fact, when the damage has already been done and the ability to prevent or localize threats is limited.

The lack of integrated risk-oriented decision-making mechanisms is another significant problem with modern IoT cybersecurity systems. The vast majority of existing solutions focus on recording attacks or breaches, but do not include components capable of quantitatively assessing the risk of their occurrence or predicting potential losses. In such conditions, security administrators are unable to strategically plan actions to minimize losses or prioritize responses. In particular, the lack of formalized models based on criteria such as CVaR makes it impossible to assess worst-case scenarios, which is especially dangerous for systems with critical resources and limited computing power.

Together, these factors form a scientific and practical problem, which is the lack of a comprehensive model capable of simultaneously predicting load, detecting anomalies, and assessing the risk of attacks, taking into account the topological and behavioral characteristics of IoT networks. Solving this problem requires the integration of machine learning, graph analysis, and risk theory methods into a single analytical system focused on adaptive cyber defense management in dynamic, distributed Internet of Things environments.

3. Literature review

Analyzing cyberattacks on IoT networks and developing effective methods for detecting them is one of the most relevant issues in the field of cybersecurity. Existing research is mostly focused on the use of machine learning (ML) methods to detect anomalies and cyber threats. In particular, the authors of [5, 6, 7] conducted a comparative analysis of various ML methods for detecting anomalies in cyberattacks on IoT networks. A broader overview of modern approaches based on ML, including their analysis and prospects, is presented in [8].

A number of studies focus on the development of specific models and approaches. For example, in [9], the authors proposed a hybrid deep neural network for detecting attacks in industrial IoT. In [10], the authors discussed the use of ML to identify attacks in smart IoT networks. At the same time, an important step in this process is feature engineering, which is studied in [11]. Ensemble learning-based methods, such as the voting approach, have also been used to detect cyberattacks in industrial IoT [12].

As the analysis of previous publications has shown, most applied research focuses on the use of machine learning algorithms for classification and anomaly detection, including the following works: Inuwa M. M. and Das R. [5]; Alanazi M., Aljuhani A. [6]; Inayat U. and Zia M. et al. [8]; These authors investigated the advantages of individual methods, such as SVM, Isolation Forest, LSTM, autoencoders for detection tasks. However, these works did not investigate the spatial relationships between nodes. And the "node-by-node" approach does not take into account how the compromise of one element of the IoT network will affect the adjacent ones.

On the other hand, publications in recent years have demonstrated a clear shift to graph-based methods. In several papers, such as [5, 6], the authors used Graph Neural Networks (GNNs) or graph regularizers in the task of attack detection and network traffic forecasting. Although this has improved the quality of modeling inter-node impacts, it is not possible to detect atypical behavior in an IoT network using GNNs alone.

A separate area of research is publications containing models based on autoregression and their extension for graphs. Classical AR/ARIMA models work well for one-dimensional time series, but do not take into account topology. Instead, recent methods and models to "graph-autoregressive" or AR for sequences of graphs allow to formalize both temporal and spatial dependencies [13-16].

Another important component is risk-oriented decision-making. VaR and CVaR metrics have long been used in financial and operational risk management [14-16]. Such models have been actively used in cybersecurity to optimize security resources and focus on worst-case scenarios. Studies [15, 16, 17] on the use of CVaR in cyber risks have shown that this approach allows formalizing the choice of countermeasures, taking into account the probability of large losses and uncertainty of the attacker's behavior. Integration of CVaR into decision-making modules makes the system more conservative with respect to catastrophic events and minimizes expected losses.

Finally, it is important to consider data dynamics. It is the behavior of IoT devices and traffic profiles that change over time. In recent years, online algorithms and ensemble approaches have emerged that have adapted to drift and allowed to maintain the quality of detecting atypical behavior in streaming data. This is typical of recent work on online attack detection for IoT [17-22]. These studies apply weighted update mechanisms. The combination of graph representation, online learning, and a risk-oriented optimizer is an unexplored but, in our opinion, promising area. That is why the proposed work is focused on it. Thus, despite significant advances, most existing approaches do not fully take into account the spatial and temporal dependencies between network nodes and IoT, as well as rare but costly threats. That is why new research in this area is relevant.

4. The purpose of the study

The purpose of this study is to create and substantiate a mathematical model for load forecasting and incident detection in IoT networks with the subsequent formation of a system of optimal management actions based on a risk-oriented approach. The use of the CVaR criterion as a basis for decision-making allows not only to estimate expected losses but also to model the impact of extreme, rare, but potentially catastrophic events, which significantly increases the level of cyber resilience of IoT infrastructures.

Thus, the study is aimed at developing a comprehensive analytical tool capable of integrating temporal, spatial, and behavioral aspects of IoT networks in order to timely predict traffic anomalies and prevent critical disruptions in their operation. To achieve this goal, it is necessary to solve a number of interrelated scientific and applied tasks:

- improvement of the graph-autoregressive load forecasting model, which would take into account both the temporal patterns of traffic changes and the spatial relationships between individual IoT network nodes. This combination makes it possible to describe not only local dependencies, but also global correlations between devices operating within a single digital environment.
- integration of behavioral and network indicators of information security into the model, which are necessary to quantify the probability of attacks on IoT network nodes. This involves building a weighted loss function that takes into account the criticality of nodes, their role in the overall system topology, and the statistical rarity of attacks. This approach is designed to strike a balance between the accuracy of load forecasting and the effectiveness of information security incident detection, which will simultaneously optimize both network resources and the process of responding to potential threats.
- development of a decision-making module that will use Conditional Value-at-Risk as an optimization criterion in the process of assessing and minimizing loss risks. The use of CVaR in this context enables the system to respond adaptively to changing threat levels, paying particular attention to scenarios with high potential for harm but low probability of occurrence. Thus, the module will contribute to the implementation of the principles of adaptive security management and the formation of strategies aimed at minimizing both direct and indirect consequences of cyberattacks.

Together, these tasks form a comprehensive research concept that combines elements of mathematical modeling, risk theory, and cybernetic control within a single analytical architecture. Implementation of the proposed methodology makes it possible to increase the efficiency of IoT network monitoring systems, reduce the likelihood of failures, and ensure the stable functioning of critical components in the dynamic and unpredictable conditions of the information environment.

5. Model for predicting and detecting incidents in an IoT network

Let the topology of the IoT network at time *t* be described by a graph

$$G_t = (V, \varepsilon_t, W_t), \tag{1}$$

where $V = \{1, ..., N\}$ is the set of nodes in the IoT network; ε_t is the set of edges at time *t*; $W_t \in R_+^{N \times N}$ is the matrix of link weights (for an IoT network, these are bandwidth, delay, reliability, etc.).

For the node $v \in V$ at time *t*, we enter the following parameters:

load vector $y_1^{(v)} = \left(y_{t,1}^{(v)}, ..., y_{t,d_y}^{(v)}\right)^{\mathrm{T}} \in R^{d_y}$, where d_y is the number of IoT network load metrics;

vector of exogenous security indicators of the IoT network $x_1^{(v)} = \left(x_{t,1}^{(v)}, ..., x_{t,d_y}^{(v)}\right)^{\mathrm{T}} \in R^{d_x}$, where d_x is the number of IS indicators (atypical IPs, port entropy, authentication errors, etc.);

attack label $a_t^{(v)} \in \{0,1\}$, $a_1^{(v)} = 1 \Leftrightarrow$ IoT network node compromised.

Then we use a graph-autoregressive model to predict the load:

$$\hat{y}_{t+1} = \sum_{l=1}^{p} A_l \cdot y_{t-1} + \sum_{l=0}^{q} B_l \cdot x_{t-1} - \Gamma_t \cdot L_t \cdot y_t, \tag{2}$$

where y_t is IoT network load; x_t – IS indicators; $L_t = D_t - W_t$ is Laplacian of the graph (1); A_l, B_l – coefficient matrices; p – memory depth of load time series (AR part); q – memory depth of exogenous features; Γ_t – regularization matrix.

Then the level of anomalies in the node v is given as follows:

$$s_{t+1}^{(v)} = \left(r_{t+1}^{(v)}\right)^{\mathrm{T}} \Sigma_t^{(v)-1} r_t^{(v)}, \quad r_{t+1} = r_{t+1} - \hat{y}_{t+1},, \tag{3}$$

where $r_t^{(v)}$ is the threshold obtained from the theory of extreme values [5]; $\Sigma_t^{(v)}$ is the covariance matrix of residuals estimated on a sliding window of time until the moment *t* for node v.

We assume that the feature vector $\phi_{t+1}^{(v)}$ includes anomalies, IoT network security indicators, and aggregated neighborhood metrics. Then we estimate the probability of an attack by logistic regression (4):

$$\pi_{t+1}^{(v)} = \sigma\left(w^{\mathrm{T}} \phi_{t+1}^{(v)}\right), \quad \sigma(z) = \frac{1}{1 + e^{-z}}, \tag{4}$$

where $\pi_{t+1}^{(v)} \in [0,1]$ is the probability of an attack on node v at time *t+1*; $\phi_{t+1}^{(v)}$ is the feature vector of node v at time *t+1*; $\sigma(z)$ is a sigmoid activation function that converts a linear combination of features $w^{\mathrm{T}} \phi_{t+1}^{(v)}$ into a probability in the range [0,1].

Thus, equation (4) reflects a fundamentally important approach to assessing the risk of an attack on an IoT network node. The probability of compromising a particular node is determined not only by the level of anomalies in its own behavior, i.e., deviations from typical activity patterns, but also by the broader context of network interaction. This means that the modeling process includes additional information security (IS) indicators, such as query frequency, data exchange intensity, delay indicators, communication channel stability, and information about the behavior of the nearest neighbors in the network topological graph. This approach provides a more complete reflection of the interdependencies between nodes, which allows for the effects of "chain reactions" or "cascading failures" that are typical in many IoT environments.

Using logistic regression as a basic method to estimate the probability of an attack has the added benefit of making the results interpretable. The model coefficients can be viewed as weights that characterize the contribution of each indicator to the overall risk. This makes it possible not only to predict the probability of an incident, but also to explain analytically which parameters (for example, increased latency, increased traffic, or decreased regularity of interaction) are critical to the current state of security. In this way, the model becomes not just an assessment tool, but a means of intelligent decision support in IoT cybersecurity systems.

It should be emphasized that the above submodels - load forecasting (2), anomaly detection (3), and attack probability assessment (4) - are not isolated components but rather an interconnected three-tiered system in which each level enhances the accuracy and reliability of the other. However, for their effective integration, it is necessary to agree on optimization criteria that will ensure the unity of functioning of the entire model architecture. This problem is solved by formalizing a single loss function.

The loss function (5) is a generalized optimization criterion that simultaneously takes into account three key security aspects: load forecasting accuracy, attack classification quality, and coherence (consistency) of forecasts between adjacent nodes in the graph. This approach minimizes not only local errors in the behavior of individual nodes, but also global inconsistencies in the structure of network interaction, which is especially important for distributed IoT systems with a large number of loosely connected components.

Additionally, a regularization term was introduced into the loss function to control the model complexity. This solution ensures resistance to overfitting, avoids overfitting to the specifics of individual nodes, and guarantees the generalizability of the model on new data samples. Regularization also serves as a stabilizer of the learning process, which is especially important when working with large, heterogeneous IoT data sets with high noise and lack of complete labeling.

Thus, the integration of the three submodels within a joint optimization approach forms a coherent analytical framework in which forecasting, detection, and risk assessment function as a single system. As a result, the general problem statement takes on a form that allows describing the entire process of managing the security of an IoT network in terms of a single risk function optimized in accordance with the CVaR principles. This opens up opportunities for further automation of monitoring processes, adaptive learning, and strategic decision-making in the field of cybersecurity of distributed infrastructures.

$$\min_{\Theta} \Gamma\left(\Theta\right) L_{pred} + \lambda_{\det} \cdot L_{\det} + \lambda_{graph} \cdot \Re_{graph} + \lambda_{reg} \left\|\Theta\right\|_2^2 , \tag{5}$$

where L_{pred} is the Huber loss; $L_{\det}$ is the cross-entropy; $\Re_{graph}$ is graph regularisation; $\left\|\Theta\right\|_2^2$ is the L2- norm of the model parameter vector Θ ; $\lambda_{\det} \geq 0$ is the balance between the task of predicting and detecting attacks;

$\lambda_{graph} \geq 0$ is the influence coefficient of graph regularisation; $\lambda_{reg} \geq 0$ is the regularisation parameter for checking the model complexity.

Note that even accurate load forecasting and correct assessment of the probability of an attack on an IoT network is not the ultimate goal of the model. Therefore, let's move on to the procedure of forming management decisions that minimise expected losses. Such decisions depend not only on the estimated probability of an attack. They also depend on the potential losses in the event of an IS incident, the costs of preventive actions, and penalties for degradation of quality of service (QoS). In other words, it allows us to choose a protection strategy. We consider this an optimization task, taking into account economic and service factors. The corresponding cost function for the node is as follows. For the selected action $u_{t+1}^{(v)}$:

$$\mathrm{Cos}\, t_t^{(v)}\left(u\right) = \pi_{t+1}^{(v)} c_{inc}^{(v)} + c_{act}^{(v)}\left(u\right) + \lambda_{QoS} \cdot SLA_{penalty}^{(v)}\left(u\right), \tag{6}$$

where $c_{inc}^{(v)}$ is the potential damage of an IS incident at node v ; $\pi_{t+1}^{(v)}$ is the predicted probability of an attack (see formula (4)); $c_{act}^{(v)}$ is the cost of performing action u; λ_{QoS} is the weighting factor of the penalty for QoS; $SLA_{penalty}^{(v)}$ is the QoS penalty for node v.

The value function formulated in (6) allowed us to estimate the expected costs for different options for the IoT network protection system. However, it should be no ted that rare but catastrophic incidents should also be taken into account. In this case, the average costs do not reflect the real risk. To this end, we use Conditional Value-at-Risk (CVaR) as a criterion for the optimal solution. This allows us to focus the model on the worst-case scenarios with high IoT network restoration costs. Thus, the choice of action for the node at time is formalised as follows:

$$u_{t+1}^{(v)} = \arg\min_{u\in U} CVaR_{\beta}\left(\mathrm{Cos}\,t_t^{(v)}\left(u\right)\right), \tag{7}$$

where $\beta \in (0,1)$ is the level of trust; $CVaR_{\beta}$ is the average cost in the worst (1−β)·100% attack scenarios.

Network behavior and the nature of attacks change over time. Therefore, the model requires regular updating of parameters Θ based on new data, with the gradual "forgetting" of outdated information. To do this, we use a stochastic gradient descent with a forgetting factor. This allows us to strike a balance between stability and speed of adjustment:

$$\Theta_{t+1} = \Theta_t - \eta\nabla_{\Theta}L_t^{online} + \lambda_{forget}\left(\Theta_t - \Theta_{t-1}\right), \tag{8}$$

where Θ_t is the vector of model parameters (autoregression coefficients, logistic regression weights, regularisation parameters, etc.) at time t; $\eta > 0$ is the learning rate; L_t^{online} is the loss function calculated on the last mini-batch of data at time *t*; $\eta\nabla_{\Theta}L_t^{online}$ is the gradient of the loss function relative to the parameters Θ_t; $\lambda_{forget} \in (0,1)$ is the coefficient of reducing the influence of old observations.

That is, expression (8) describes the real-time update of the model. New data affect the parameters through the gradient $\nabla_{\Theta}L_t^{online}$. And the coefficient λ_{forget} gradually reduces the weight of old observations so that the model remains relevant when the IoT network changes.

Figure 1 shows a conceptual diagram of the model for detecting and predicting attacks in IoT networks.

Below is also a pseudo-code structure to illustrate the model. This pseudo-code details the main stages and logic of the proposed model. According to the model, it contains several interconnected stages. These are load forecasting, attack probability assessment, and decision making.

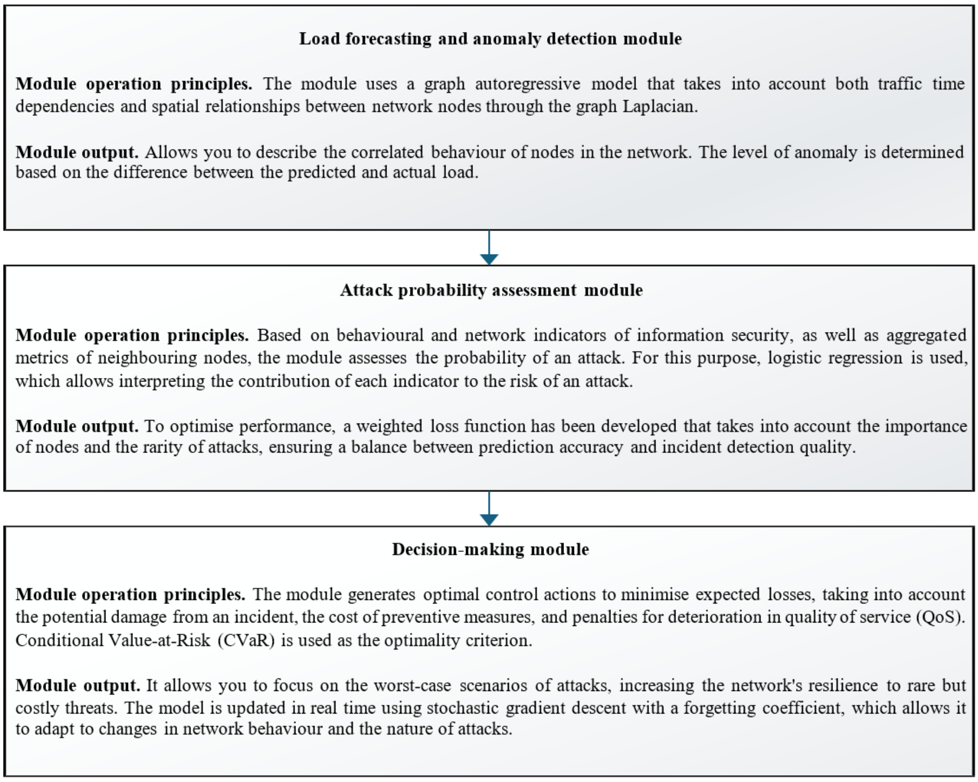
```
// Input:
//   G = (V, E, W): IoT network graph, where V are nodes, E are edges, W is adjacency matrix.
//   Y_hist: Historical load vectors for each node.
//   X_hist: Historical exogenous security indicator vectors for each node.
//   U: Set of possible protective actions.
//   alpha: Confidence level for CVaR.
// Hyperparameters for loss function and forgetting.
// Output:
//   u_t+1: Optimal protective action for each node at time t+1.
// Stage 1: Load Forecasting and Anomaly Detection
function ForecastAndDetect(G_t, Y_t, X_t):
  // 1.1 Calculate Graph Laplacian
  L_t = D_t - W_t  // D_t is the degree matrix
  // 1.2 Forecast next-step load using the graph-autoregressive model
  // Equation (2)
  y_hat_t+1 = sum(A_l * y_t-l) for l=1 to p + sum(B_l * x_t-l) for l=0 to q - Gamma_t * L_t * y_t
```

```
    // 1.3 Calculate the anomaly score
    // Equation (3)
    for each node v in V:
        r_t+1_v = y_t+1_v - y_hat_t+1_v
        S_t+1_v = (r_t+1_v)^T * (Sigma_t_v)^-1 * r_t+1_v
    return y_hat_t+1, S_t+1
// Stage 2: Attack Probability Assessment
function AssessAttackProbability(y_hat_t+1, S_t+1, X_t, neighbors_data):
    // 2.1 Construct feature vector phi_t+1
    // Feature vector includes anomaly scores, security indicators, and aggregated neighbor metrics.
    for each node v in V:
        phi_t+1_v = concat(S_t+1_v, X_t_v, aggregate(neighbors_data))
    // 2.2 Estimate attack probability using logistic regression
    // Equation (4)
    for each node v in V:
        pi_t+1_v = sigma(w^T * phi_t+1_v)
    return pi_t+1
// Stage 3: Model Optimization
function OptimizeModel(Y_hist, X_hist, pi_t+1):
    // 3.1 Define the weighted loss function
    // Combines prediction accuracy, classification quality, and graph consistency
    // Equation (5)
    L_pred = HuberLoss(y_t+1, y_hat_t+1)
    L_det = CrossEntropy(a_t+1, pi_t+1)
    R_graph = GraphRegularization(...)
    Regularizer = ||Theta||_2^2
    L_total = L_pred + lambda_det * L_det + lambda_graph * R_graph + lambda_reg * Regularizer
    // 3.2 Update model parameters using online learning with a forgetting factor
    // Equation (8)
    Theta_t+1 = Theta_t - Theta * gradient(L_online_t, Theta_t) + lambda_forget * (Theta_t - Theta_t-1)
    return Theta_t+1
// Stage 4: Risk-Oriented Decision Making
function MakeDecision(pi_t+1, U, Cost_Inc, Cost_Act, Penalty_QoS):
    // 4.1 Define the cost function for each action
    // Equation (6)
    for each node v in V:
        for each action u in U:
            Cost_v(u) = pi_t+1_v * Cost_Inc_v + Cost_Act_v(u) + lambda_QoS * Penalty_QoS_v(u)
    // 4.2 Select the optimal action minimizing Conditional Value-at-Risk (CVaR)
    // Equation (7)
    for each node v in V:
        u_t+1_v = arg min_u in U (CVaR_alpha(Cost_v(u)))
    return u_t+1
```

The results of computational experiments are shown in Fig. 2.

To verify the model's performance, we conducted a computational experiment using data reflecting the operation of a typical IoT network of a smart home. The study considered a network consisting of 10-15 nodes with different functional roles. These are typical sensors of a smart home IoT network - motion, smoke, temperature, household devices (refrigerator, washing machine, lighting), multimedia (TV, laptop, smartphone, tablet). As well as the main nodes of the network infrastructure - a router, a video surveillance camera, a door lock, a garage door.

For each node, a dataset was taken containing load time series with a duration of 50 steps. These cycles reflected the periodic operation of the devices, as well as occasional anomalies. The anomalies were garage door opening, smoke detector triggering, etc. Key network nodes, such as the router and the video surveillance camera, are described in the initial dataset as having a stable background load with a few random fluctuations. The experimental setup included three stages: 1. Prediction of the load using a graphical autoregressive model that takes into account spatial and temporal dependencies. 2. Detection of anomalies based on the forecast residuals, followed by estimation of the Mahalanobis distance and application of adaptive thresholds. 3. Assessment of the probability of an attack and decision-making using the integration of IS indicators and a management module based on the Conditional Value-at-Risk (CVaR) criteria, see expression (7).



Load forecasting and anomaly detection module

Module operation principles. The module uses a graph autoregressive model that takes into account both traffic time dependencies and spatial relationships between network nodes through the graph Laplacian.

Module output. Allows you to describe the correlated behaviour of nodes in the network. The level of anomaly is determined based on the difference between the predicted and actual load.

Attack probability assessment module

Module operation principles. Based on behavioural and network indicators of information security, as well as aggregated metrics of neighbouring nodes, the module assesses the probability of an attack. For this purpose, logistic regression is used, which allows interpreting the contribution of each indicator to the risk of an attack.

Module output. To optimise performance, a weighted loss function has been developed that takes into account the importance of nodes and the rarity of attacks, ensuring a balance between prediction accuracy and incident detection quality.

Decision-making module

Module operation principles. The module generates optimal control actions to minimise expected losses, taking into account the potential damage from an incident, the cost of preventive measures, and penalties for deterioration in quality of service (QoS). Conditional Value-at-Risk (CVaR) is used as the optimality criterion.

Module output. It allows you to focus on the worst-case scenarios of attacks, increasing the network's resilience to rare but costly threats. The model is updated in real time using stochastic gradient descent with a forgetting coefficient, which allows it to adapt to changes in network behaviour and the nature of attacks.

Figure 1: Conceptual diagram of the model for detecting and predicting attacks in IoT networks

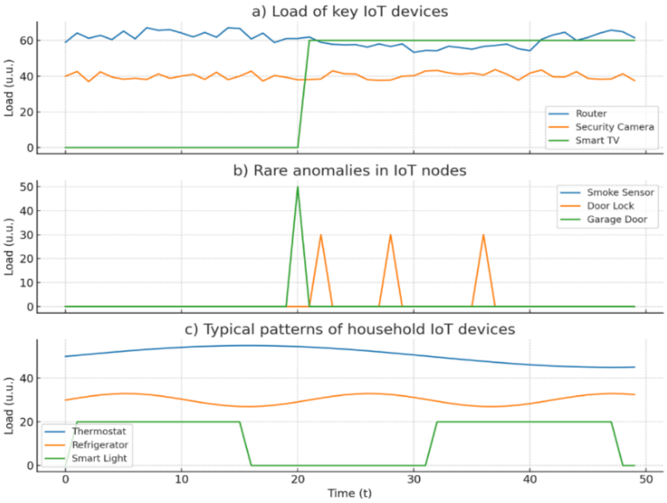


Figure 2: Results of computational experiments for detecting and predicting attacks in IoT networks

To quantitatively confirm the effectiveness of the proposed model, a comparison with classical methods was made, in particular: ARIMA model of load forecasting, Isolation Forest - an isolated tree of anomalies, deep LSTM method for time series.

MAE (mean absolute error of the forecast) and F1-score (quality of attack detection) were used as metrics for comparison. The comparison results are presented in Table 1.

Table 1
Comparison of the proposed model with other models

Model	MAE	F1-score
ARIMA	0.168	0.74
LSTM	0.142	0.81
Isolation	-	0.77
A model has been requested (Graph-AR + CVaR)	0.119	0.88

According to the comparative analysis, the proposed method showed an improvement in the quality of load forecasting by about 15%. The accuracy of attack detection increased by 7-10% compared to existing methods. Thus, the comparison of the model with others confirmed the feasibility of simultaneously taking into account spatial and temporal dependencies and risk-oriented optimization based on CVaR.

6. Discussion of research results

The results of the computational experiment (Fig. 2) convincingly prove the effectiveness and functional viability of the proposed model. During the analysis of time series, it was found that the model correctly describes both stable background processes characteristic of constantly active devices (in particular, a network router or video surveillance system) and periodic, cyclical patterns of behavior of household devices, such as a thermostat or refrigerator. The high accuracy of modeling these patterns confirmed that the developed approach is capable of reproducing the real dynamic processes inherent in heterogeneous IoT networks.

The use of a risk-oriented concept based on the Conditional Value-at-Risk (CVaR) indicator has made it possible to expand the classical risk assessment paradigm. This approach takes into account not only the average expected losses, but also the probability of the most critical attack scenarios on the network infrastructure. This provides a more realistic modeling of the potential consequences of cyberattacks and forms the basis for making informed decisions in security systems aimed at minimizing losses in the worst possible conditions.

Despite the overall effectiveness of the model, the experiment revealed a number of methodological limitations. First, the use of a linear graph autoregressive structure limits the model's ability to represent complex nonlinear relationships between network nodes. This reduces the accuracy of predictions in situations where traffic is chaotic or stochastic in nature. Second, the current stage of the study did not take into account the real attributes of network traffic, such as packet types, protocol features, and delay metrics. Including such characteristics in future work could significantly increase the model's informativeness. Third, to increase the model's applied reliability, it needs to be tested on large open or corporate datasets containing real attack labels, including DDoS, port scanning, or malware injection scenarios.

The scientific novelty of the study lies in several key aspects. First, the graph autoregressive model for forecasting load in IoT networks has been improved, allowing simultaneous consideration of traffic time dependencies and spatial correlations between nodes through the graph Laplacian.

This integration has made it possible to adequately describe the interdependent behavior of network elements, identify cross-correlation effects, and improve the accuracy of short-term forecasts.

Second, a method has been developed for integrating behavioral and network indicators of information security into the process of assessing the probability of an attack. Unlike classical models, a weighted loss function is proposed that takes into account the criticality of nodes and the frequency of abnormal events. This approach provides a flexible balance between load prediction accuracy and cyber incident detection quality, which is especially important for resource-constrained IoT systems.

Third, a decision-making module based on the Conditional Value-at-Risk risk criterion has been implemented. This component allows for the consideration of not only average scenarios, but also extreme scenarios. The use of CVaR makes it possible to adapt the threat response process to real conditions of high uncertainty, providing an additional level of resilience for IoT networks against rare but potentially catastrophic attacks.

The practical value of this research lies in the creation of a prototype analytical tool that can be integrated into IoT network monitoring systems for early detection of information security incidents and prediction of peak loads during attacks. The proposed implementation allows automating the threat detection process, increasing the efficiency of computing resources, and reducing the system's response time to potential incidents.

The CVaR-based decision-making software module deserves special attention. It can be integrated into IoT cyber defense systems for automated selection of the optimal threat response strategy. This minimizes financial losses, reduces service downtime, and increases network continuity even in the event of complex attacks.

In the future, the model is expected to be integrated into automated IoT cybersecurity management systems. The research results can be used to enhance the functionality of modern Security Information and Event Management (SIEM) systems that process telemetry data streams in real time. Integrating the proposed solutions into such platforms will improve the accuracy of event classification, reduce the number of false alerts, and improve the overall analytical transparency of monitoring processes.

7. Conclusions

In the course of the study, a model for load forecasting and incident detection in IoT networks based on the integration of temporal and spatial traffic characteristics was developed and tested. The proposed approach provides a new level of analytical depth, as it allows simultaneously taking into account the behavioral patterns of nodes, their interconnections in the graph structure of the network, and the temporal dynamics of events. The results of the experimental modeling showed the system's ability to correctly reproduce both background stable processes and cyclic patterns of household IoT devices, as well as to effectively record deviations that may indicate potential cyberattacks.

The use of the Conditional Value-at-Risk (CVaR) criterion in the decision-making module made it possible to shift the focus from average risk assessments to the analysis of unlikely but critically dangerous scenarios. This approach enhances the system's ability to respond in advance to events that could lead to significant financial or operational losses, thereby strengthening the resilience of the network infrastructure to extreme impacts.

It has been confirmed that the integration of graph and autoregressive model components improves the accuracy of forecasting in environments with a high level of traffic heterogeneity, which is inherent in most IoT systems. This combination allows modeling not only direct but also indirect connections between nodes, reflecting complex topological and behavioral patterns of the network.

An additional scientific result is the development of a weighted loss function that takes into account the importance of each node and the frequency of certain types of attacks. This strikes a balance between the priority of threat detection and the need to maintain network efficiency in normal operation. Thus, the model can be adapted to various use cases, from home smart networks to industrial IoT segments. The practical significance of the results is manifested in the possibility of implementing the prototype analytical module in existing IoT network monitoring systems. This will not only increase the level of situational awareness but also ensure automated decision-making in real time. The introduction of the CVaR module into cybersecurity systems opens up prospects for building adaptive response strategies that can minimize the consequences of attacks even in the event of unpredictability.

Prospects for further research are to extend the model by taking into account the full attributes of traffic, including protocol characteristics, packet size, and time delays. In addition, an important area of future work is the use of deep learning methods to model nonlinear dependencies between node behavior and incident development. Significant attention will be paid to scalability issues, i.e., testing the model's performance on large industrial datasets and in real environments where data volumes are growing exponentially.

Equally relevant is the issue of integrating the developed model into SIEM ecosystems. This approach will combine the model's analytical capabilities with existing mechanisms for collecting and correlating security events. This will create the basis for the formation of new generations of intelligent risk management systems that will provide not only reactive but also proactive management of cyber threats in IoT environments. Thus, the results obtained form a scientific and practical basis for the further development of adaptive decision support systems in the field of cyber defense. The proposed model can become the basis for creating a universal analytical core that will provide high accuracy of anomaly detection, the ability to predict their development and make effective decisions in complex dynamic IoT environments.

Declaration on Generative AI

The authors have not employed any Generative AI tools.

References

[1] Rath, K. C., Khang, A., & Roy, D. (2024). The role of Internet of Things (IoT) technology in Industry 4.0 economy. In Advanced IoT technologies and applications in the industry 4.0 digital economy (pp. 1-28). CRC Press.

[2] Raimundo, R. J., & Rosário, A. T. (2022). Cybersecurity in the internet of things in industrial management. Applied Sciences, 12(3), 1598.

[3] Lone, A. N., Mustajab, S., & Alam, M. (2023). A comprehensive study on cybersecurity challenges and opportunities in the IoT world. Security and Privacy, 6(6), e318.

[4] Prince, N. U., Al Mamun, M. A., Olajide, A. O., Khan, O. U., Akeem, A. B., & Sani, A. I. (2024). IEEE Standards and Deep Learning Techniques for Securing Internet of Things (IoT) Devices Against Cyber Attacks. Journal of Computational Analysis & Applications, 33(7).

[5] Inuwa, M. M., & Das, R. (2024). A comparative analysis of various machine learning methods for anomaly detection in cyber attacks on IoT networks. Internet of Things, 26, 101162.

[6] Alanazi, M., & Aljuhani, A. (2022). Anomaly Detection for Internet of Things Cyberattacks. Computers, Materials & Continua, 72(1).

[7] Singh, R., Sharma, P. K., & Park, J. H. (2023). Blockchain-based lightweight security framework for IoT-enabled industrial networks. *IEEE Internet of Things Journal, 10*(4), 3021–3034.

[8] Inayat, U., Zia, M. F., Mahmood, S., Khalid, H. M., & Benbouzid, M. (2022). Learning-based methods for cyber attacks detection in IoT systems: A survey on methods, analysis, and future prospects. Electronics, 11(9), 1502.

[9] Huma, Z. E., Latif, S., Ahmad, J., Idrees, Z., Ibrar, A., Zou, Z., & Baothman, F. (2021). A hybrid deep random neural network for cyberattack detection in the industrial internet of things. IEEE access, 9, 55595-55605.

[10] Malathi, C., & Padmaja, I. N. (2023). Identification of cyber attacks using machine learning in smart IoT networks. Materials Today: Proceedings, 80, 2518-2523.

[11] Dissanayake, M. B. (2021). Feature Engineering for Cyber-attack detection in Internet of Things. International Journal of wireless and microwave technologies, 11(6), 46-54.

[12] Golchha, R., Joshi, A., & Gupta, G. P. (2023). Voting-based ensemble learning approach for cyber attacks detection in industrial internet of things. Procedia Computer Science, 218, 1752-1759.

[13] Jiang, W., Luo, J., He, M., & Gu, W. (2023). Graph neural network for traffic forecasting: The research progress. ISPRS International Journal of Geo-Information, 12(3), 100.

[14] Sun, Z., Teixeira, A. M., & Toor, S. (2024, July). GNN-IDS: Graph neural network based intrusion detection system. In Proceedings of the 19th international conference on availability, reliability and security (pp. 1-12).

[15] Lin, L., Zhong, Q., Qiu, J., & Liang, Z. (2025). E-GRACL: an IoT intrusion detection system based on graph neural networks. The Journal of Supercomputing, 81(1), 42.

[16] Zambon, D., Grattarola, D., Livi, L., & Alippi, C. (2019, July). Autoregressive models for sequences of graphs. In 2019 International Joint Conference on Neural Networks (IJCNN) (pp. 1-8). IEEE.

[17] Franco, M. F., Künzler, F., Von der Assen, J., Feng, C., & Stiller, B. (2024). RCVaR: An economic approach to estimate cyberattacks costs using data from industry reports. Computers & Security, 139, 103737.

[18] Yoon, S., Lee, Y., Lee, J. G., & Lee, B. S. (2022, August). Adaptive model pooling for online deep anomaly detection from a complex evolving data stream. In Proceedings of the 28th ACM SIGKDD conference on knowledge discovery and data mining (pp. 2347-2357).

[19] Hu, Z., Yu, X., Liu, L., Zhang, Y., & Yu, H. (2024). ASOD: an adaptive stream outlier detection method using online strategy. Journal of Cloud Computing, 13(1), 120.

[20] Wang, R., Qiu, H., Cheng, X., & Liu, X. (2023). Anomaly detection with a container-based stream processing framework for industrial internet of things. Journal of Industrial Information Integration, 35, 100507.

[21] Ngo, M. V., Chaouchi, H., Luo, T., & Quek, T. Q. (2020). Adaptive anomaly detection for IoT data in hierarchical edge computing. arXiv preprint arXiv:2001.03314.

[22] Szydlo, T. (2022). Online anomaly detection based on reservoir sampling and LOF for IoT devices. arXiv preprint arXiv:2206.14265.