A Probabilistic Model with the Markov Property for Cyberattack Detection Based on the Analysis of Dynamic Traffic Variations

Nataliia Vyshnevska[1,†], Valerii Kozlovskyi[1,†], Yurii Lysetskyi[1,†], Ihor Makieiev[1,†]

[1] *State University "Kyiv Aviation Institute", 1 Liubomyra Huzara ave., Kyiv, 03058, Ukraine,*

Abstract

In this paper, a probabilistic model for cyberattack detection with a Markov property is proposed. The model integrates a posteriori state estimation with the analysis of a multivariate anomaly indicator derived from network traffic dynamics. It consists of three primary components: the conditional probability of observing the current indicator value, the state transition probability between “normal” and “attack” conditions, and a normalization factor ensuring mathematical consistency and scalable probability estimation. The proposed approach significantly reduces computational complexity by limiting historical dependency to a single previous time step (Markov assumption), while maintaining adaptability to evolving network behaviour. The incorporation of multiscale analysis, Z-normalization, and inertial smoothing enhances the model’s resilience to noise and enables the detection of both instantaneous and gradually unfolding cyberattacks. The feasibility of real-time implementation is demonstrated, making the model suitable for integration into contemporary cyber threat monitoring systems. Experimental validation indicates that the approach achieves a balance between sensitivity to anomalies and computational efficiency, with potential applications in intrusion detection systems (IDS) and security information and event management (SIEM) platforms.

Keywords

cyberattack detection; probabilistic model; Markov process; anomaly indicator; a posteriori probability; network traffic; adaptive threshold; cyber threat; inertia; real-time detection.

1. Introduction

In the context of the rapidly increasing complexity and scale of cyberattacks, the challenge of timely threat detection in information systems becomes critically important. This is particularly relevant for attacks that evolve gradually or exhibit inertia—such as DDoS attacks, low-level slow-rate intrusions, or multi-stage threats that covertly unfold within network traffic. Traditional detection methods based on fixed thresholds or instantaneous signatures often lack sufficient sensitivity to such scenarios or generate an excessive number of false positives. Consequently, there is a growing need for detection models that go beyond analysing the current system state, incorporating prior behaviour, statistical patterns of traffic variation, and temporal probabilistic dependencies among observed events. The use of integrated indicators that aggregate multidimensional information from the network environment allows for the reduction of complex data structures to a unified metric, which can be adaptively estimated over time.

In this paper, we propose a probabilistic model for cyberattack detection based on the analysis of dynamic traffic changes, which incorporates a Markov property between system states and utilizes a posteriori estimation via multiscale traffic analysis. The model consists of three essential components: the conditional probability of the current indicator’s occurrence, the transition probability between

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

* Corresponding author.

† These authors contributed equally

nataliia.vyshnevska@npp.kai.edu.ua (N. Vyshnevska), valerii.kozlovskyi@npp.kai.edu.ua (VKozlovskyi), yurii.lysetskyi@snt.ua (Y. Lysetskyi), 8390988@stud.kai.edu.ua (I. Makieiev)

0000-0002-1358-467X (N. Vyshnevska); 0000-0002-1358-467X (Valerii Kozlovskyi); 0000-0002-5080-1856 (Y. Lysetskyi); 0009-0009-8679-5652 (I. Makieiev)

“attack” and “normal” states, and a normalization factor ensuring appropriate scaling and probabilistic consistency.

Unlike conventional approaches, the proposed model captures the historical context of threats, performs smoothing of the estimation by leveraging the inertia of attacks, and adaptively responds to situational changes in real time. Additionally, the model’s structure reduces computational overhead by limiting the analysis to the current and immediately preceding states, thereby eliminating the need to retain the entire observation history.

1. Research

The goal of this research is the formalization and implementation of a probabilistic method for cyberattack detection that integrates the precision of a posteriori state estimation with high sensitivity to dynamic changes in network traffic.

2. Main part

Mathematical formalization of the model.

To improve the mechanism for detecting cyberattacks, a discrete probabilistic model with a first-order Markov property was used. The model takes into account the current parameters of network traffic and the previous state of the system. This approach describes the inertia of processes inherent in cyberattacks and allows to formalize the temporal dependence between events.

Let's introduce the main notations and dependencies.

The state of the system at a point in time t is determined by the variable $Y_t \in \{0,1\}$, its value can take two states: the active phase of the attack $Y_t = 1$, indicating the need for prompt/immediate response, and the normal state of the network without signs of anomalies $Y_t = 0$.

The integral indicator of the anomaly is determined by a variable I_t indicating the level of traffic deviation from normal behavior [1-3].

Formally, the binary state of the system can be written as follows:

$$Y_t = \begin{cases} 1 : \textit{The attack takes place at time t} \\ 0 : \textit{No attack occurs at time t} \end{cases} \quad (1)$$

The assessment of the current state of the system takes into account its previous state and makes it possible to analyze the context of events, as well as track the dynamics of traffic changes. The combination of network parameter states provides a comprehensive description of network behavior and reduces the risk of false positives [4-7].

The model for detecting dynamic traffic changes is based on the Bayesian approach using the Markov property. It assumes that the current state of the system is a function of the integral indicator of the anomaly I_t and the state of the system at the previous point in time Y_{t-1}. This approach allows to use the Markov property and take into account the nearest previous state of the system [2, 3, 5, 7, 8].

The probability of the system being in the state of attack at a point in time, t taking into account the current value of the integral index of anomalies and the previous state of the system, is determined by:

$$P(Y_t = 1 | I_t, Y_{t-1}) = \frac{P(I_t | Y_t = 1, Y_{t-1}) \cdot P(Y_t = 1 | Y_{t-1})}{P(I_t | Y_{t-1})} \quad (2)$$

where $P(Y_t = 1 | I_t, Y_{t-1})$ the conditional probability of observation indicates how the current value of the integral indicator I_t corresponds to the standard behavior of the network. Under the normal state, the integral indicator fluctuates near the mean level, and under the condition of the attack, it observes a stable or increasing deviation from the norms.

$$P(Y_t = 1 | I_t, Y_{t-1}) = f(I_t; \theta_{Y_t}) \text{ (3)}$$

where θ_{Y_t} is the threshold parameter that determines the boundary between states; $f(I_t; \theta_{Y_t})$ - a continuous or partial function, the specific form of which depends on the nature of network traffic, namely, small values of the integral indicator correspond to a low probability of an attack, in turn, exceeding the threshold gives a surge in probability growth.

In fact, (2) acts as a mechanism for converting multidimensional traffic characteristics into a single scale of confidence in observation and reduces it to a numerical estimate [0; 1].

$P(Y_t = 1 | Y_{t-1})$ - a priori probability of the system going into an attack state, acts as a filter that allows to be sensitive to successive signs of threats and ignore random fluctuations that are not related to attacks [2-5, 8, 9]. $P(I_t | Y_{t-1})$ - normalization coefficient, which guarantees the correct scaling of the probability within [0, 1]. and provides correct interpretation. It reflects the probability of occurrence of the current value of the integral indicator I_t under conditions, if only known, the previous state of the system Y_{t-1}, regardless of the state of the system (norm-attack) at the present moment of time [2, 3, 5,6].

This approach combines information about past and current observations while maintaining adaptability to changes in traffic.

Due to the previous state of the system, the model displays the inertia of attacks, recognizes continuous or recurring threats, and minimizes false positive responses to single deviations.

Generalization of the three components $P(I_t | Y_t = 1, Y_{t-1})$ in $P(Y_t = 1 | Y_{t-1})$ $P(I_t | Y_{t-1})$ the structure of the Bayesian model with the Markov property allows to reasonably determine the presence of cyberattacks, taking into account both the current signs of the anomaly and the temporal dynamics of events [2, 3, 5, 9].

The proposed model is based on the assumption that the current state of the system Y_t is determined only by the previous state Y_{t-1} and the integral anomaly indicator I_t calculated on the basis of a multiscale analysis of traffic parameters [5, 6, 8]. This reduces computational complexity, because the model analyzes only the last state and the current indicator without the need to store the entire history [4,5,6]. At the same time, the integral indicator I_t aggregates information from all key parameters of network traffic, thereby maintaining high accuracy in detecting attacks [6, 8].

Due to the use of the Markov property, time dependencies are reduced to one step, which corresponds to the inertial nature of many attacks (e.g., in the case of an ongoing cyberattack) [4, 5, 8]. The integral anomaly indicator I_t is calculated based on the deviations of normalized parameters of network traffic from multiscale trends, allowing the level of deviation from the norm to be estimated by a single metric [6,8]. The model also takes into account the previous state of the system Y_{t-1}, and determines if there has already been an attack, then even a moderate deviation of the indicator may indicate its continuation [3, 8, 9].

The use of the Markov property allows to significantly simplify the calculation of the total distribution in the detection model, limiting it only to the current and previous state of the system, without taking into account the full sequence of observations and formalized in the form of:

$$P(Y_t, I_t | Y_{t-1}, I_{t-1}) = P(Y_t | Y_{t-1}) \cdot P(I_t | Y_t, I_{t-1}) \cdot P(Y_{t-1} | I_{t-1}), \text{ (5)}$$

where is $P(Y_t | Y_{t-1})$ the transient probability between the states of the system. It simulates the inertia of attacks and allows the model to distinguish short-term bursts from sequential threats [4, 5, 9]. $P(I_t | Y_t, I_{t-1})$ - conditional probability of observing the current value of the integral indicator, taking into account traffic dynamics [5, 6, 8]. $P(Y_{t-1}|I_{t-1})$ -initial probability, reflects the basic configuration of the system state and anomaly level in the previous step [3,6].

The use of this approach allows: to reduce the amount of processed data on each cycle, thus ensuring high reactivity to real changes in traffic, to recognize sequential or renewed threats due to dynamic updating of dependencies between the current and previous state of the system [5, 8, 9].

This is an important step, because many attacks are periodic or protracted, and an accurate assessment of the probability of an attack at the moment t is possible only if the previous state of the system is taken into account Y_{t-1} and the indicator changes I_t relative to the background of previous observations [3, 8, 10].

In the proposed model, the probability that the system is in a state of attack at a point in time t is determined by a posteriori distribution, which is built on the basis of the total probability of features and the Markov property between the states of the system [2, 3, 5]. The a posteriori probability of detecting an attack is determined by the expression:

$$P(Y_t=1|I_t,I_{t-1})=\frac{P(I_t|I_{t-1},Y_t=1)\cdot P(Y_t=1|Y_{t-1})}{P(I_t|I_{t-1})}, (6)$$

where is $P(I_t|I_{t-1},Y_t=1)$ the conditional probability of observing the anomaly indicator in the event of an attack, taking into account its previous value, which makes it possible to display the dynamics of traffic changes. $P(Y_t=1|Y_{t-1})$ - transient probability reflects the tendency of the system to remain in the state of attack or switch to it from normal mode, $P(I_t|I_{t-1})$ - normalization factor, which acts as a guarantee that the a posteriori probability will be scaled within [0; 1] [2, 3, 4, 5, 6, 8, 9].

The value obtained after the calculation $P(Y_t=1|I_t,I_{t-1})$ allows a decision to be made about the presence of an attack at a point in time t. If this probability exceeds a given adaptive or dynamically calculated threshold, then the system classifies the state of the system as an "attack".

The normalization factor in the model is defined as:

$$P(I_t|I_{t-1})=\sum_{y\in\{0,1\}}P(I_t|I_{t-1},Y_t=y_t)\cdot P(Y_t=y_t|Y_{t-1}),(7)$$

where: $Y_t=0$ - the system is not under attack, $Y_t=1$ - the system is under attack.

This expression provides a posteriori probability normalization and ensures that its value will be in the range $[0;1]$ [2, 3, 5, 9]

This approach allows to focus on the current anomaly indicator and the previous state of the system, which greatly simplifies the computational load and the volume of previous observations. At the same time, the model remains sensitive to the key features of attacks, due to the combination of an integral indicator, preliminary observations, and probabilistic estimation of transitions between states. Thus, it strikes a balance between efficiency and accuracy, providing speed to respond to threats in real time and integrating the model into modern cybersecurity systems [4, 5, 6, 8, 9].

In the proposed model, transient probabilities form the structural basis of the Markov property and estimates the probability of the system being in the state of attack at the moment of time t, if its state is known at the previous moment of time $t-1$ [4, 9].

These probabilities are described using the matrix of transitions between the states of the system, where the system can be in one of two states: - the $Y_t=1$ system is attacked, $Y_t=0$ - the system is in a normal state.

Formally, the transition matrix has the form:

$$P=\begin{bmatrix}P(Y_t=0|Y_{t-1}=0) & P(Y_t=1|Y_{t-1}=0)\\ P(Y_t=0|Y_{t-1}=1) & P(Y_t=1|Y_{t-1}=1)\end{bmatrix}, (8)$$

where $P(Y_t = 1|Y_{t-1} = 1)$ is the probability of the attack continuing at a point in time t, if it has already occurred at the previous moment, $P(Y_t = 0|Y_{t-1} = 0)$ is the probability that the system remains in a normal state.

Each element of this matrix reflects a scenario of transition between the "attack" and "normal" states. For example, $P(Y_t = 0|Y_{t-1} = 1)$ - the probability of the start of an attack, or $P(Y_t = 1|Y_{t-1} = 0)$ - the probability of ending the attack and returning to a normal state [5, 8, 9].

The values of the transition matrix are taken into account in the a posteriori probability formula $P(Y_t = 1|I_t, I_{t-1})$, where the component $P(Y_t|Y_{t-1})$ is directly taken from the corresponding row and allows the model to take into account attack trends. For example, if the attacks are of a long-term nature, then the value $P(1|1)$ will be high. Also, the values of the matrix are used to form a normalizing factor in the Bayesian calculation [2, 3, 5].

Transient probabilities can be estimated empirically by analyzing the frequency of transitions between "attack" and "normal" states in real or simulated sequences of network events. This approach allows the model to reflect the actual trends in the change in the state of the system, which were observed at previous moments of time [10-12].

In particular, the frequency of transitions from the normal state to the attack state $P(Y_t = 1|Y_{t-1} = 0)$, or vice versa - the completion of the attack $P(Y_t = 0|Y_{t-1} = 1)$ can be statistically calculated and used to construct a matrix of transient probabilities, which plays the role of a probability filter between the current decision and the context.

The use of information from previous observations allows not only to adapt the model to the real profile of attacks in a particular environment, but also to mitigate the impact of single anomalies, namely to avoid false positives, increase resistance to short-term traffic fluctuations, and ensure logical consistency of decisions over time [8, 10, 12].

The next component of the cyberattack detection model is the probability of observations, $P(I_t|Y_t = 1, I_{t-1})$ it allows to simulate the dynamics of changes in network activity over time, taking into account the influence of the previous integral indicator and the current state of the system [5, 6, 8]. Determines how likely the observed value of the integral indicator is I_t at a point in time t, provided that the value of the previous level of the anomaly is known I_{t-1} and the system is in an attack state $Y_t \in \{0,1\}$ [5, 6, 8].

Thanks to this component, the model is able to take into account not only the current deviation, but also the dynamics of anomalies of its increase or fade, which is important for detecting gradually deployed or masked attacks. And also increase the resistance of the model to short-term noise bursts [6, 8, 10,].

The model can implement the probability of observations $P(I_t|Y_t, I_{t-1})$ as parametric or empirical modeling, which allows adapting to different network conditions and attack scenarios [5, 6, 12].

In the structure of the model, the component of conditional probability estimation is of special importance $P(I_t|Y_t = 1, I_{t-1})$, which performs the function of analyzing the correspondence of the current situation in the network to the characteristic state of the attack [5, 6, 8].

Unlike well-known approaches, where conditional probabilities are modeled through distribution densities, this method implements a functional estimation approach that is flexible, easy to implement, and adaptive to the variable behavior of the network environment.

The integral indicator I_t summarizes the multi-scale deviations of traffic parameters from the average values, takes into account the number of threshold exceedances and the strength of the anomaly (for example, according to the Z-assessment) [6, 8]. It also briefly reflects the current state of the network and allows to assess how typical this value is for attacks, taking into account the previous dynamics [5, 8].

Since in (3) the function of conditional plausibility of the observation of the anomaly indicator was introduced, then we will consider its generalization for the case of dynamic modeling, taking into account also the previous level of anomalies I_{t-1}. To do this, use the $P(I_t|Y_t) = f(I_t; \theta)$

$$f(I_t;\theta)=\begin{cases}0, & I_t<\theta_0\\ \dfrac{I_t-\theta_0}{1-\theta_0}, & I_t\geq\theta_0\end{cases}, \quad (9)$$

where $\theta_0 \in [0,5;0,7]$ is a fixed sensitivity threshold that defines the boundary between a slight deviation and a pronounced anomaly [6, 8].

The function $f(I_t)$ has the following properties: the value $f(I_t)=0$ is interpreted as the absence of signs of attack by the current indicator; the value $f(I_t)\to 0$ indicates a high degree of correspondence of observations to the pattern of the attacked state; the interval $I_t \in (\theta_0;1]$ is a linearly scaled "alarm zone" zone.

After converting the integral index I_t to probability using $f(I_t;\theta)$, the model performs inertial smoothing with the estimate obtained on the previous cycle:

$$\hat{P}(Y_t=1)=a\cdot(I_t)+(1-a)\cdot\hat{P}(Y_{t-1}=1) \quad (10)$$

where $\alpha \in (0,1)$ is the coefficient of inertia, which determines the weight of new information in comparison with historical information; $\hat{P}(Y_{t-1}=1)$ - estimation of the probability of an attack, calculated in the previous step [5, 6, 9].

This mechanism allows: to stabilize the behavior of the model in response to short-term bursts, to store an informative memory of recent anomalous states, to take into account the inertia of attacks, which in many cases are not instantaneous [8, 10, 14,15,16].

The effectiveness of the proposed model depends on the dynamics of the network environment. In case of frequent changes in attack types (for example, alternating flood-, low-rate- and application-level attacks), or a high noise level, the model may temporarily lose accuracy, since it does not always have time to adapt to new traffic patterns. This can lead to a delayed reaction or an increase in the number of false positives and false negatives. To increase stability, it is necessary to implement dynamic parameter updates, threshold adaptation and additional mechanisms for classifying anomalies in real time.

Similarly, a high level of noise in network traffic (e.g., short-term spikes, broadcast storms, monitoring queries) may reduce the model's stability, as the conditional observation probability $P(I_t|Y_t=1,I_{t-1})$ in such cases does not reflect a real threat but merely captures statistical deviation. To improve robustness under such scenarios, it is advisable to implement dynamic parameter updates for $f(I_t)$, adaptive thresholding forθ_0, and additional classification or anomaly-type evaluation mechanisms operating in real time.

To assess the effectiveness of the proposed probabilistic, cyberattack detection model, a series of simulation experiments were conducted. These experiments analysed both typical normal traffic and attack models with inertial structure (e.g., DDoS, Low-rate DoS, APT). For each scenario, a traffic parameter set, an integral anomaly indicator, the system state, and the posterior probability of attack presence at a given time step were computed.

A demonstration version of the proposed model under conditions of mixed network load was implemented using a simulated scenario comprising 100 time steps of network traffic (Table 1). The test set included both phases of normal operation and three attack intervals (time steps 20–25, 45–55, and 75–78), along with two noise events (spikes at time steps 10 and 65), aimed at evaluating the model's robustness to fluctuations and false positives.

The integral anomaly indicator I_t varied within the range$[0.1;\ 0.9]$, values within the range: $[0.1;\ 0.9]$ were not registered as anomalies - even if they represented short-term spikes or background noise.

Values in the range $[0,6;\ 0,75]$ were not sufficient for triggering detection on their own, but when accumulated could lead to attack identification.

Values exceeding $[0,75]$ even isolated occurrences - often triggered threat detection.

A return of values below 0.6 was interpreted as the dissipation of the threat. However, if an attack had previously been observed, the posterior probability Y_t could remain elevated due to the inertia mechanism, which retains memory of recent anomalous activity.

Values of I_t were transformed into the probability function $f(I_t)$, which linearly scales deviations when $I_t > 0,6$, when (9)

$$f(I_t) = \frac{I_t - 0,6}{1 - 0,6} = \frac{I_t - 0,6}{0,4},$$

each threshold exceedance $\theta_0 = 0,6$ corresponds to a partial probability of anomaly, estimated at scale $[0;1]$

Table 1
Scenario of 100 Time Steps of Network Traffic

Step	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**
I_t	0.474	0.537	0.505	0.476	0.464	0.464	0.553	0.453	0.553	0.910	0.483	0.548	0.452	0.549	0.532	0.465	0.465	0.466	0.523	0.760
$f(I_t)$	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.775	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.400
Y_t	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.543	0.163	0.049	0.015	0.005	0.002	0.001	0.000	0.000	0.000	0.280
State	Norm	Norm	Norm	Norm	Norm	Norm	Norm	Norm	Norm	Norm	Norm	Norm	Norm	Norm	Norm	Norm	Norm	Norm	Norm	Norm
Step	**21**	**22**	**23**	**24**	**25**	**26**	**27**	**28**	**29**	**30**	**31**	**32**	**33**	**34**	**35**	**36**	**37**	**38**	**39**	**40**
I_t	0.792	0.824	0.856	0.888	0.920	0.538	0.470	0.468	0.532	0.541	0.532	0.464	0.464	0.464	0.464	0.543	0.453	0.470	0.457	0.534
$f(I_t)$	0.480	0.560	0.640	0.720	0.800	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000
Y_t	0.346	0.417	0.489	0.562	0.633	0.443	0.310	0.217	0.152	0.106	0.074	0.052	0.036	0.025	0.017	0.012	0.008	0.006	0.004	0.003
State	Norm	Norm	Norm	Norm	Norm	Norm	Norm	Norm	Norm	Norm	Norm	Norm	Norm	Norm	Norm	Norm	Norm	Norm	Norm	Norm
Step	**41**	**42**	**43**	**44**	**45**	**46**	**47**	**48**	**49**	**50**	**51**	**52**	**53**	**54**	**55**	**56**	**57**	**58**	**59**	**60**
I_t	0.467	0.537	0.465	0.535	0.744	0.779	0.813	0.847	0.882	0.916	0.950	0.984	1.000	0.891	0.758	0.534	0.464	0.537	0.468	0.468
$f(I_t)$	0.000	0.000	0.000	0.000	0.360	0.438	0.519	0.599	0.682	0.762	0.842	0.922	1.000	0.727	0.395	0.000	0.000	0.000	0.000	0.000
Y_t	0.002	0.002	0.001	0.001	0.253	0.341	0.429	0.516	0.603	0.687	0.770	0.851	0.931	0.893	0.797	0.558	0.391	0.274	0.192	0.134
State	Norm	Norm	Norm	Norm	Norm	Norm	Norm	Norm	Norm	Norm	Norm	Norm	Norm	Norm	Attack	Norm	Norm	Norm	Norm	Norm
Step	**61**	**62**	**63**	**64**	**65**	**66**	**67**	**68**	**69**	**70**	**71**	**72**	**73**	**74**	**75**	**76**	**77**	**78**	**79**	**80**
I_t	0.468	0.465	0.539	0.466	0.801	0.462	0.466	0.465	0.535	0.463	0.462	0.536	0.462	0.537	0.759	0.802	0.845	0.887	0.538	0.469
$f(I_t)$	0.000	0.000	0.000	0.000	0.502	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.397	0.504	0.594	0.717	0.000	0.000
Y_t	0.094	0.066	0.046	0.032	0.267	0.187	0.131	0.092	0.064	0.045	0.031	0.022	0.015	0.011	0.287	0.376	0.463	0.548	0.384	0.269
State	Norm	Norm	Norm	Norm	Norm	Norm	Norm	Norm	Norm	Norm	Norm	Norm	Norm	Norm	Norm	Norm	Norm	Norm	Norm	Norm
Step	**81**	**82**	**83**	**84**	**85**	**86**	**87**	**88**	**89**	**90**	**91**	**92**	**93**	**94**	**95**	**96**	**97**	**98**	**99**	**100**
I_t	0.466	0.536	0.465	0.465	0.462	0.464	0.462	0.464	0.465	0.537	0.463	0.462	0.539	0.466	0.465	0.463	0.538	0.464	0.462	0.538
$f(I_t)$	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000
Y_t	0.188	0.132	0.092	0.064	0.045	0.032	0.022	0.015	0.011	0.008	0.006	0.005	0.004	0.003	0.002	0.002	0.001	0.001	0.001	0.001
State	Norm	Norm	Norm	Norm	Norm	Norm	Norm	Norm	Norm	Norm	Norm	Norm	Norm	Norm	Norm	Norm	Norm	Norm	Norm	Norm

Table 2
Interpretation of Detection System Modelling Results

Value I_t	**Result** $f(I_t)$	**Description**
0.60	0.000	Normal situation
0.68	0.20	Minor anomaly
0.72	0.30	Initial alert zone
0.83	0.575	Probable attack
0.95	0.875	Severe threat
1.00	1.000	Maximum attack probability

Subsequently, the values are smoothed to Y_t using the formula:

$$Y_t = \alpha \cdot f(I_t) + (1-\alpha) \cdot Y_{t-1},$$

where $\alpha = 0,7$ is the inertia coefficient, preserving the context of changes from previous time steps. If moderate anomalous values are detected over several cycles, this approach accumulates probabilities.

Table 3
Interpretation of Model Results for Different Situations

Event type	I_t	$f(I_t)$	Y_t	**System response**
Normal activity	0,30 - 0,55	0,00	$< 0,2$	No alert triggered
Short-term spike (10th step)	$\approx 0,90$	0,75	$\approx 0,5$ $(\downarrow \text{ low value})$	No alert triggered (suppressed)
Attach phase (20–25)	0,76 - 0,95	0,40 - 0,875	$\uparrow$ *up to* $0,9$	Attack detected
Attach phase (45–55)	0,80 - 0,98	0,50 - 0,95	$\uparrow$ *up to* $0,95$	Attack detected
Attach phase (75–78)	0,83 - 0,92	0,575 - 0,8	$\uparrow$ *up to* $0,85$	Attack detected
False positive (65th step)	$\approx 0,72$	0,30	$\approx 0,76$	False positive

The “attack” state is confirmed when $Y_t \geq \theta = 0,75$.

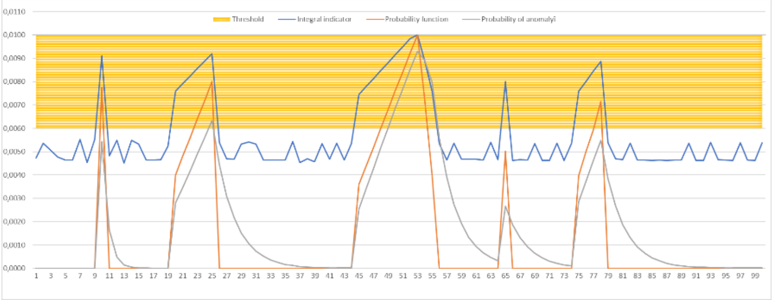

Figure 1: Dynamics of the integrated anomaly indicator I_t, the conditional likelihood $f(I_t)$ and the a posteriori probability of attack Y_t under simulated mixed network load conditions

According to the modelling results, all three attack phases were successfully detected — the indicator Y_t exceeded the threshold during phases 20–25, 45–55, 75–78.

Short-term noise spikes (e.g. $I_t = 0,68$ at 10th step) did not trigger false positives — inertia-based smoothing kept Y_t below the detection threshold. A single false positive was recorded at 65th step, resulting from the combined impact of a short-term noise fluctuation and a low inertia coefficient.

3. Conclusions

A probabilistic model with a Markov property has been developed and substantiated. It consists of multiscale traffic analysis, an integrated anomaly indicator, and Markovian logic for state transitions. The a posteriori probability, as the main diagnostic indicator, allows the model to respond not only to current deviations but also to account for the temporal development of events.

One of the key advantages of this model is its ability to operate in real-time environments with limited data volume, due to the use of local memory and inertia-based estimation.

The proposed model demonstrates high accuracy in threat detection, flexibility to changes in network conditions, and robustness against false positives. Results of the demonstration simulation confirm its capability to identify both explicit attacks and gradual or stealthy attack phases.

A promising direction for model enhancement involves the integration of mechanisms for dynamic parameter updating in real time, including the adaptation of threshold values, inertia coefficients, and state transition probabilities based on changing input traffic statistics.

In future research, the model can be adapted to real-time incident response systems, integrated into cybersecurity architectures for critical infrastructure, and expanded toward multiclass classification of attack types

Declaration on Generative AI

The authors have not employed any Generative AI tools.

References

[1] Shannon C. E. A mathematical theory of communication // Bell System Technical Journal. – 1948. – Vol. 27(3). – P. 379–423.

[2] Jensen F. V., Nielsen T. D. Bayesian networks and decision graphs. – New York: Springer, 2007. – 447 p.

[3] Pearl J. Probabilistic reasoning in intelligent systems: networks of plausible inference. – San Francisco : Morgan Kaufmann, 1988. – 552 p.

[4] Rabiner L. R. A tutorial on hidden Markov models and selected applications in speech recognition // Proceedings of the IEEE. – 1989. – Vol. 77(2). – P. 257–286. https://doi.org/10.1109/5.18626.

[5] Ghahramani Z. An introduction to hidden Markov models and Bayesian networks // Int. J. of Pattern Recognition and Artificial Intelligence. – 2001. – Vol. 15(1). – P. 9–42.

[6] Bishop C. M. Pattern recognition and machine learning. – New York: Springer, 2006. – 738 p.

[7] Xiong A. Theory of Markov Chain Monte Carlo and its several applications // Science and Technology of Engineering, Chemistry and Environmental Protection. – 2024. – Vol. 1. – DOI: 10.61173/5snnx446.

[8] Enli M. B., Genovese A., Agostinello D., Piuri V. Robust DDoS attack detection with adaptive transfer learning // Computers & Security. – 2024. – Vol. 144. – 103962. https://doi.org/10.1016/j.cose.2024.103962.

[9] Lux T. Bayesian estimation of agent-based models using adaptive Markov Chain Monte Carlo // Computational Economics. – 2022. – Vol. 59. – P. 453–476. https://doi.org/10.1007/s10614-021-10155-0.

[10] Chandola V., Banerjee A., Kumar V. Anomaly detection: a survey // ACM Computing Surveys. – 2009. – Vol. 41(3). – Article 15. https://doi.org/10.1145/1541880.1541882.

[11] Kozhukhovskyi A. D. Bayesian network-based methodology for predicting insider threats // Information Security. – 2023. – № 3. – DOI: 10.31673/2409-7292.2023.030404.

[12] Khraisat A., Gondal I., Vamplew P., Kamruzzaman J. Survey of intrusion detection systems: techniques, datasets and challenges // Cybersecurity. – 2019. – Vol. 2. – https://doi.org/10.1186/s42400-019-0038-7.

[13] Lakhno, V., Boiko, Y., Mishchenko, A., Kozlovskyi, V., Pupchenko, O. (2017). Development of the intelligent decision-making support system to manage cyber protection at the object of informatization. Eastern-European Journal of Enterprise Technologies, 9(86), 53–61.

[14] Tolubko, V., Kozelkov, S., Zybin, S., Kozlovskyi, V., Boiko, Y. (2019). Criteria for evaluating the effectiveness of the decision support system. *Advances in* Intelligent Systems and Computing, 754, 320–330.

[15] Yudin, O., Boiko, Y., Frolov, O. (2015). Organization of decision support systems for crisis management. In: Proc. of the 2nd International Scientific-Practical Conference "Problems of *Infocommunications Science and Technology" (PIC S&T)*, October 2015, 115–117.

[16] Barannik, V., Yudin, O., Boiko, Y., Ziubina, R., Vyshnevska, N. (2019). Video Data Compression Methods in the Decision Support Systems. In: *Communications in Computer and Information Science*, vol. 1007, Springer, 531–548. DOI: 10.1007/978-3-319-91008-6_30.