Scientific Journal of Astana IT University
ISSN (P): 2707-9031 ISSN (E): 2707-904X
VOLUME 25, MARCH 2026

DOI: 10.37943/25EXWB8090

Nazym Zhumangaliyeva
Postgraduate Student, Department of Software Engineering
nazym_k.81@mail.ru, orcid.org/0000-0003-1130-3405
Satbayev University, Kazakhstan
Lazat Kydyralina
PhD, Acting Associate Professor of the Department of Informatics
lazat_75@mail.ru, orcid.org/0000-0002-2836-0919
Shakarim University of Semey, Kazakhstan
Guljanat Esenbekova
Candidate of Technical Sciences, Associate Professor of the Department of "Computer Technologies"
esenbekova_g@mail.ru, orcid.org/0009-0001-1879-3024
Temirbek Zhurgenov Kazakh National Academy of Arts, Kazakhstan
Dmytro Prokopovych-Tkachenko
PhD in Technical Sciences, Associate Professor
Head of the Department of Cybersecurity and Information Technologies; Senior Research Fellow Doctor of Science Candidate at the Department of Cybersecurity Systems and Technologies
omega2417@gmail.com, orcid.org/0000-0002-6590-3898
University of Customs and Finance; State Scientific Institution "Institute of Information, Security and Law of the National Academy of Legal Sciences of Ukraine"; State University of Telecommunications, Ukraine
Mykola Mormul
PhD in Technical Sciences, Associate Professor at the Department of Cybersecurity and Information Technologies
mormul@umsf.dp.ua, orcid.org/0000-0002-8036-3236
University of Customs and Finance, Ukraine

DYNAMIC DETERMINATION OF INFORMATION SYSTEM SECURITY PARAMETERS BASED ON ATTACK GRAPHS AND MARKOV MODELS UNDER CONDITIONS OF UNCERTAINTY

Abstract. The article presents an approach to the dynamic determination of information system security parameters under conditions of uncertainty and incomplete monitoring data. An attack graph is used as the structural foundation, describing possible compromise trajectories while considering vulnerability dependencies, configurations, access rights, and protective measures. To obtain quantitative assessments, a Markov model of adversary progress is introduced, in which intermediate states represent attack stages and absorbing states correspond to the achievement of critical goals related to violations of confidentiality, integrity, and availability. A key element of the methodology is the procedure for estimating transition probabilities given sparse observations from security logs and interval-based expert estimates for poorly observed attack steps. The proposed combination of event statistics and expert constraints is supplemented by regularization and dynamic updates, which increase parameterization stability, reduce the impact of isolated incidents, and account for operational environment drift. The calculated output indicators include the probability of compromise within a given horizon, separate violation probabilities for confidentiality, integrity, and availability, and the expected time to compromise. Experimental demonstration on a typical corporate architecture confirms the model's suitability for comparing defense scenarios and quantitatively justifying countermeasures: strengthening segmentation and

Received: 30.01.2026 Accepted: 25.02.2026 Published: 30.03.2026

DOI: 10.37943/25EXWB8090

privilege control reduces the reachability of target states, while enhancing monitoring and response further decreases the probability of achieving goals and increases the predicted time to compromise. Signs of attacks on management planes are also considered, including vulnerabilities in secure exchange protocols and network management protocols, as well as the compromise of device firmware. The results can be used for risk-oriented planning of security measures under budget constraints and for forming dynamic security effectiveness indicators in a Zero Trust architecture.

Keywords: attack-graph; Markov-chain; uncertainty; regularization; telemetry; compromise-probability; risk-management; countermeasures; Zero-Trust.

Introduction

The digital transformation of organizations and government services intensifies the dependence of business process resilience on the cybersecurity of information systems (IS). At the same time, practical operational conditions are often poorly formalized: configurations change faster than regulations, telemetry is incomplete, and incident statistics are sparse. As a result, classical static risk assessments and one-time audits create a "yesterday's" picture: formally correct, but poorly suited for operational management. For the infrastructure of the Republic of Kazakhstan, where the focus is on service continuity, data trust, and compliance requirements, there is a demand for models capable of dynamically recalculating security indicators as the environment changes.

One of the robust directions for formalizing threats is attack graphs, which allow for the expression of logical-causal dependencies between vulnerabilities, access rights, topology, and protective measures [1–3]. However, practical management requires not only a structural description of the attacker's goal reachability but also the probabilistic dynamics of transitions, reflecting observational uncertainty and the variability of intruder behavior. Promising frameworks here include Markov models, including absorbing Markov chains, as well as extensions in the form of Hidden Markov Models (HMM) and Bayesian attack networks [6–8].

The literature presents approaches to assessing compromise probabilities based on CVSS scores [25], expert scales, or limited event statistics, as well as methods for analyzing the expected time to attack success [16, 17]. Nevertheless, two practical problems persist. First: the robust estimation of transition probabilities given small samples and contradictory expert intervals. Second: adapting the model to environmental drift (updates, new configurations, changes in attack profiles). Research on risk management and countermeasure selection emphasizes the need for regularization and optimization formulations with budget and acceptable risk constraints [10].

However, the scientific novelty of the present work lies not in the isolated use of attack graphs or Markov chains per se, but in their integrated application under incomplete and heterogeneous evidence conditions. In contrast to more conventional probabilistic attack-graph approaches that rely primarily on fixed vulnerability scores, fully specified conditional probabilities, or static expert assumptions, the proposed method introduces a robust transition estimation procedure that explicitly combines sparse operational observations with interval-constrained expert knowledge and supplements this combination with regularization and dynamic updating. As a result, the framework is designed not only to estimate compromise reachability but also to maintain stability under data scarcity, adapt to environmental drift, and provide managerially interpretable predictive indicators for comparing defense scenarios in operational settings.

The goal of this work is to develop a method for the dynamic determination of IS security parameters based on the combined application of attack graphs and Markov models under incomplete information. Objectives:

1. Formalize the mapping of an attack graph into a Markov state space;
2. Propose a procedure for estimating transition probabilities using interval expert data and sparse observations with regularization;
3. Define computable security indicators (probabilities of confidentiality/integrity/availability violation,

Scientific Journal of Astana IT University
ISSN (P): 2707-9031 ISSN (E): 2707-904X
VOLUME 25, MARCH 2026

time to compromise);

4. Demonstrate the application of the model for comparing defense scenarios and selecting countermeasures.

Methods and Materials

The methodological part of the study is structured to be applicable to operational environments typical of the country: distributed departmental and corporate networks, high service dependence on digital platforms, and strict requirements for service continuity and compliance, while telemetry is often incomplete and incident statistics are sparse. Therefore, in the Methods section, it is assumed that the model must not merely record attack reachability but dynamically recalculate security indicators as configurations and threat profiles change, relying on factual monitoring signals and limited expert information [1–3].

The following combined scheme is applied:

1. Formalization of compromise scenarios in the form of an attack graph with causal dependencies between vulnerabilities, access rights, topology, and controls [4, 5];

2. Mapping the graph into a finite state space and introducing Markov dynamics (including variants with hidden states and Bayesian extensions) to describe the intruder's progress [9];

3. Estimating the transition matrix based on the principle of robustness: observable transitions are taken from SIEM/logs/IDS, while expert intervals are defined for difficult-to-observe transitions, followed by regularization and/or optimization formulations under budget constraints and acceptable risk [11].

Taking into account Kazakhstani operational practices (SOC processes, centralized event correlation, response regulations), the sources of parameterization are assumed to be: signature and behavioral IDS triggers, SIEM correlations, vulnerability scan results, and configuration management data. For management plane scenarios, it is specifically recommended to include indicators typical of attacks via SSL/TLS and SNMP vulnerabilities, and for firmware compromise—signs of binary artifact anomalies (e.g., Byte2Image class approaches) and signals from update logs. This composition of telemetry allows for linking the calculation of probabilistic indicators with continuous verification discipline and access policies in the spirit of Zero Trust, where monitoring (SIEM/EDR/IDS) serves as a source of regular probabilistic updates [12–14].

1. Attack Graph and State Space

Consider an IS represented by a directed attack graph:

$$\boldsymbol{G} = (\boldsymbol{V}, \boldsymbol{E}), \boldsymbol{V} = \boldsymbol{V_S} \cup \boldsymbol{V_E} \ , \qquad (1)$$

where $\boldsymbol{V_S}$ is a set of security states (e.g., privilege levels, reached positions), $\boldsymbol{V_E}$ represents events/exploits, and $\boldsymbol{E}$ defines reachability based on preconditions. In practice, it is convenient to build a *privilege graph* or a goal reachability graph for the attacker [4, 5]. For further probabilistic analysis, a finite set of states $\{\boldsymbol{1}, \dots, \boldsymbol{N}\}$ is introduced, including:

- initial states $\boldsymbol{S_0}$ (external access, user account, etc.);
- intermediate states (persistence, lateral movement, privilege escalation);
- absorbing compromise states $\boldsymbol{S_A}$ (violation of C, I, or A, or achievement of a critical goal).

This work utilizes the “attack graph + Markov chain” linkage, where the graph defines the logical reachability of the intruder’s steps (initial access, persistence, lateral movement, privilege escalation, etc.), and the Markov model adds probabilistic transition dynamics between these steps based on SIEM/IDS telemetry and expert assessments. This allows for more than just stating goal reachability; it enables quantitative estimation of the probability of compromise across the C/I/A triad and the expected time to compromise, facilitating the comparison of defense scenarios and the justification of countermeasures using “numbers” rather than “estimates.” The resulting mapping is shown in Fig. 1.

DOI: 10.37943/25EXWB8090

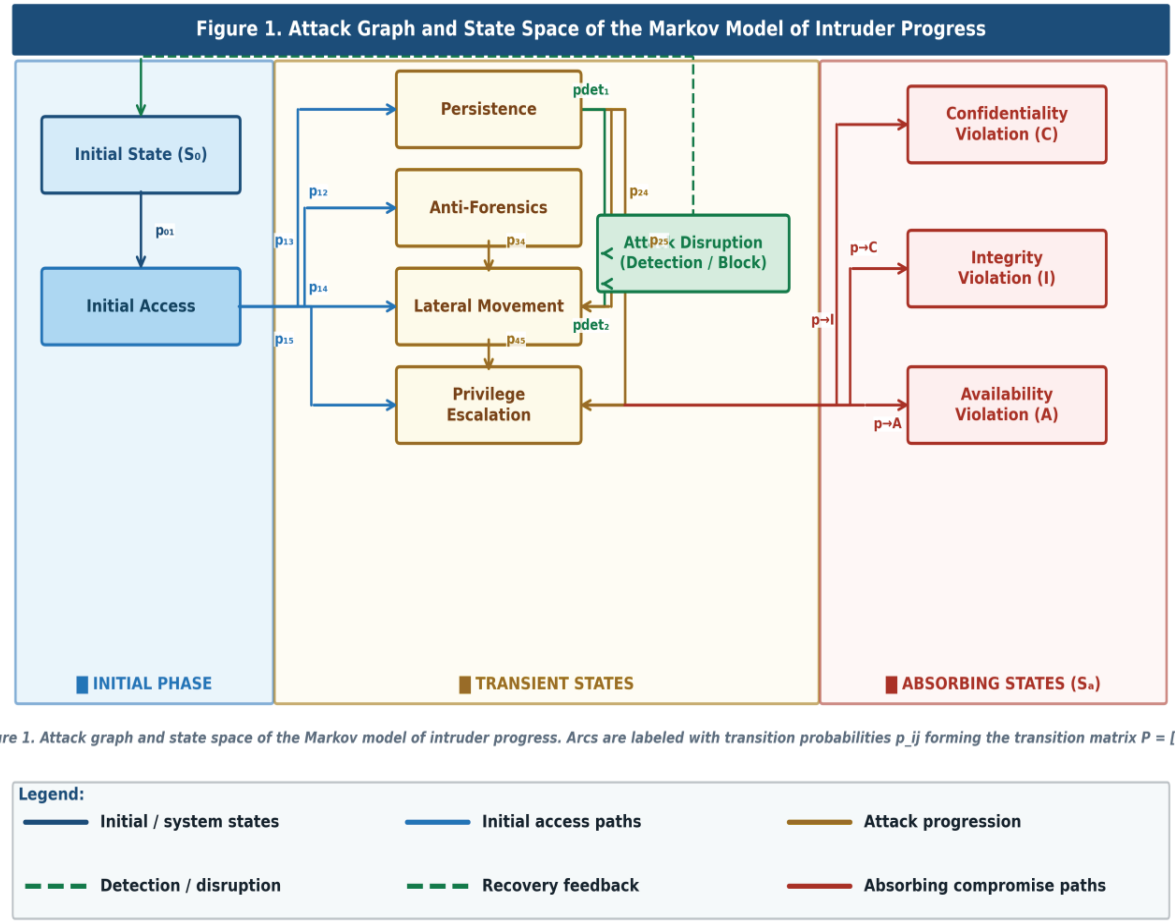

Figure 1. Attack graph and state space of the Markov model of intruder progress. Arcs are labeled with transition probabilities p_ij forming the transition matrix P = [p_ij].

Figure 1. Attack graph and state space of the Markov model of intruder progress

The diagram shows the mapping of an attack scenario into a finite state space: the initial state and the "initial access" stage are defined on the left, followed by transient (intermediate) states reflecting typical attack steps (persistence, anti-forensics, lateral movement, privilege escalation) and a possible "attack disruption" as an outcome of successful detection/response; on the right are the absorbing states—the achievement of the attacker's goals in the form of confidentiality, integrity, and availability violations. The arcs between nodes are labeled with transition probabilities, which form the Markov chain transition matrix and are subsequently used to calculate the probability of reaching absorbing states and the expected time to compromise. Abbreviations/designations in Fig. 1: C denotes confidentiality, I denotes integrity, A denotes availability, and p_ij denotes the transition probability from state i to state j.

2. Markov Dynamics and Transition Estimation

Let X_t be a discrete Markov process describing the system state from the perspective of intruder progress. Then:

$$\mathbb{P}(X_{t+1} = j \mid X_t = i) = p_{ij}, \sum_{j=1}^{N} p_{ij} = 1, p_{ij} \geq 0\,, \qquad (2)$$

where the transition matrix $P = [p_{ij}]$ is consistent with the attack graph structure: if $(i \to j) \notin \mathcal{E}$, then $p_{ij} = 0$.

Scientific Journal of Astana IT University
ISSN (P): 2707-9031 ISSN (E): 2707-904X
VOLUME 25, MARCH 2026

In real-world conditions, transition observations are limited: event counters n_{ij} from SIEM/logs/IDS are available only for some edges, while expert intervals $p_{ij} \in [\ell_{ij}, u_{ij}]$ are provided for the rest. For robust estimation, we use a combined procedure:

1. *Empirical estimation by observation*: $\hat{p}_{ij} = \frac{n_{ij}}{\sum_k n_{ik}}$ when $\sum_k n_{ik} > 0$.
2. *Smoothing (prior robustness)* via a Dirichlet prior for each row $p_{i\cdot}$:

$$p_{i\cdot} \sim \mathrm{Dir}(\alpha_{i1}^{(0)}, \dots, \alpha_{iN}^{(0)}), a_{ij} = \alpha_{ij}^{(0)} + n_{ij} \ . \qquad (3)$$

3. *Interval regularization* as a projection onto the feasible set defined by expert intervals:

$$\min_{p_{i\cdot}} \| p_{i\cdot} - \bar{p}_{i\cdot} \|_2^2 + \lambda D_{\mathrm{KL}}(p_{i\cdot} \| q_{i\cdot}) \text{s.t.} \sum_{j=1}^{N} p_{ij} = 1, \ell_{ij} \le p_{ij} \le u_{ij} \ , \qquad (4)$$

where $\bar{p}_{i\cdot}$ is the posterior mean from (3), $q_{i\cdot}$ is the base distribution (e.g., "uniform across feasible edges"), D_{KL} is the Kullback-Leibler divergence, and $\lambda > 0$ is the regularization parameter.

4. *Dynamic updating* considering environmental drift using exponential smoothing:

$$P^{(t)} = (1-\eta)P^{(t-1)} + \eta \hat{P}^{(t)}, 0 < \eta \le 1 \ , \qquad (5)$$

where $\hat{P}^{(t)}$ is the estimate based on the window of recent observations and current expert intervals.

Formulation (4) ensures two important properties: (a) it does not "misfire" on small samples, and (b) it preserves expert boundaries where statistics are insufficient. In practice, the problem is solved component-wise for each row as a convex optimization with linear constraints.

3. Security Indicators: Probability of Compromise and Time to Compromise

Let the set of states be divided into transient T and absorbing A. Then the transition matrix in standard form is:

$$P = \begin{pmatrix} Q & R \\ 0 & I \end{pmatrix} \ , \qquad (6)$$

where Q represents transitions within T, and R represents transitions from T to A. Let π_0 be the initial distribution across transient states.

Probability of reaching compromise (any goal in A) no later than H steps:

$$\mathbb{P}(\tau \le H) = 1 - \pi_0^T Q^H 1 \qquad (7)$$

where 1 is a vector of ones, and τ is the time of entry into A.

Expected time to compromise for an absorbing chain:

$$\mathbb{E}[\tau] = \pi_0^T (I-Q)^{-1} 1 \qquad (8)$$

For separate assessment across the CIA triad (confidentiality, integrity, availability), three subsets of absorbing states A_C, A_I, A_A are introduced, and the corresponding absorption probabilities for each set are calculated using the fundamental matrix:

$$B = (I-Q)^{-1} R \qquad (9)$$

where elements B_{ik} are interpreted as the probability of absorption into the k-th absorbing state when

DOI: 10.37943/25EXWB8090

starting from transient state i. The full transition-estimation procedure is summarized in Fig. 2.

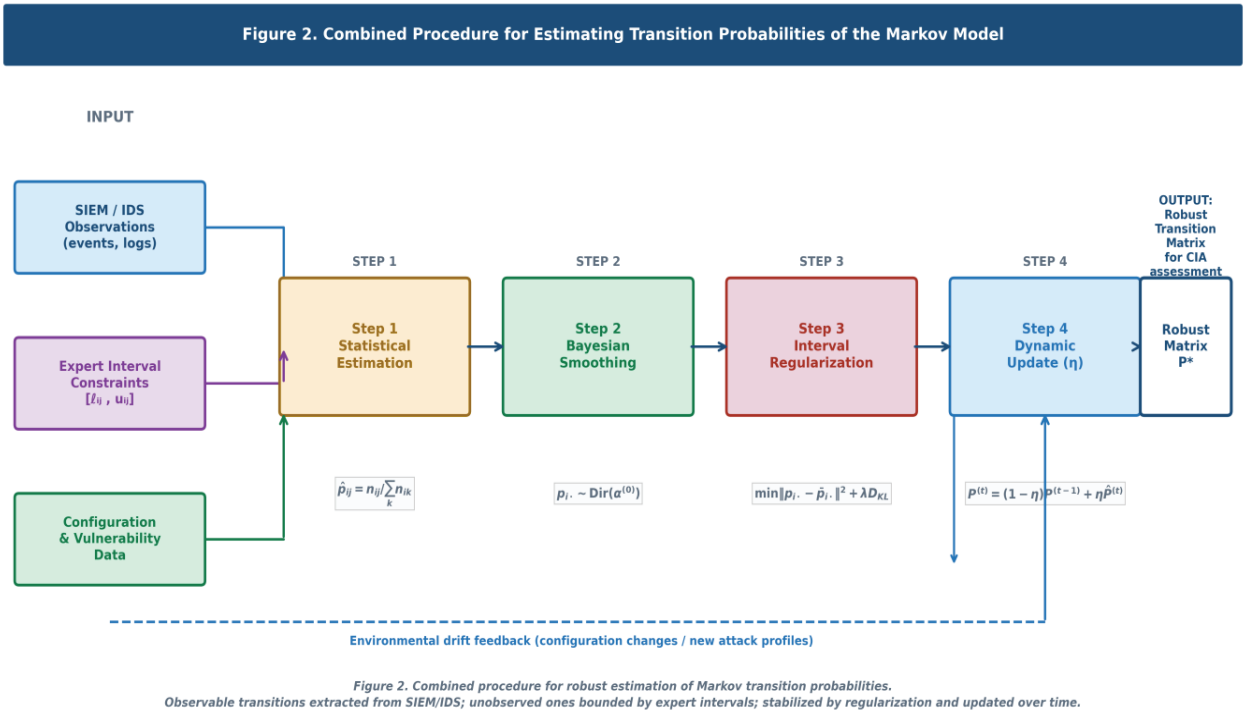

Figure 2. Combined procedure for estimating transition probabilities of the Markov model

The diagram illustrates the pipeline for constructing robust transition probabilities: observations from SIEM/IDS/logs and expert interval constraints for poorly observed transitions are provided as input, followed by four steps—initial statistical estimation based on events, smoothing to eliminate "zeros" and overfitting on sparse data, alignment with expert intervals (to ensure estimates remain within reasonable bounds), and dynamic updates accounting for attack drift and configuration changes; the output is a robust transition matrix suitable for calculating the probability of reaching critical goals and selecting countermeasures. Abbreviations/designations in Fig. 2: SIEM denotes Security Information and Event Management, IDS denotes an Intrusion Detection System, and p_ij denotes a Markov transition probability.

4. Countermeasure Selection as an Optimization Problem

Let there be a set of security controls $c \in \{0,1\}^m$ (segmentation, MFA, patch management, privilege control, etc.) that affect the transition probabilities $P = P(c)$, as well as the cost $Cost(c)$. For management decisions, the minimization of expected damage can be used:

$$\min_{c\in\{0,1\}^m} \mathbb{E}[L(\tau, A)] \text{s.t.} Cost(c) \le B \ , \qquad (10)$$

where B is the budget. For conservative risk management, the $CVaR_\alpha$ measure [15] can be applied instead of the mathematical expectation, which is particularly relevant for rare but catastrophic events. The general methodological workflow is presented in Fig. 3.

Scientific Journal of Astana IT University
ISSN (P): 2707-9031 ISSN (E): 2707-904X
VOLUME 25, MARCH 2026

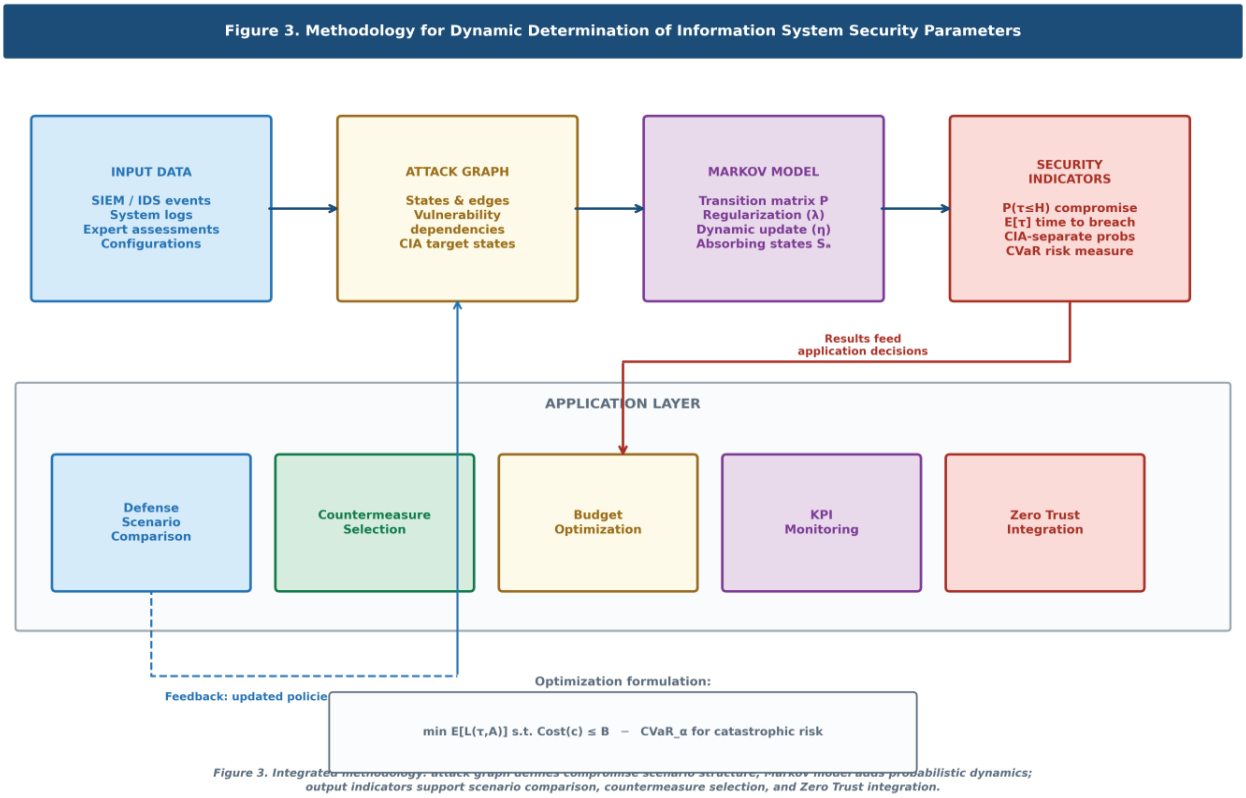

Figure 3. Methodology for dynamic determination of information system security parameters

The diagram consists of four upper blocks and an applied lower layer. On the left, input data are shown (SIEM/IDS events, system logs, expert assessments, configurations), which are then transformed into an attack graph (states and target absorbing states based on the CIA triad), after which a Markov model is constructed with mechanisms for robustness (regularization) and adaptation to environmental changes (dynamic updating). The "Indicators" block lists the output metrics: the probability of reaching a compromise within a given horizon, the expected time to compromise, separate assessments for confidentiality/integrity/availability, and the risk-oriented CVaR measure. The bottom "Application" panel shows how these results are used in practice: comparison of defense scenarios, selection of countermeasures, budget optimization, KPI monitoring, and integration with Zero Trust principles. In the "Methods" section, a reproducible scheme for dynamic IS security assessment is formed, where the deterministic structure of compromise scenarios is defined by an attack graph, and the uncertainty and variability of the environment are accounted for through Markov dynamics with absorbing goals across the confidentiality, integrity, and availability triad. A key element of the methodology is the robust estimation of transition probabilities given sparse telemetry: observable transitions are extracted from SIEM/IDS/logs, and difficult-to-observe ones are bounded by expert intervals, after which the estimates are stabilized by regularization and updated over time considering configuration drift and attack tactics. This results in managerially interpretable indicators—the probability of reaching critical goals in a given horizon, expected time to compromise, and separate CIA assessments—as well as the formulation of countermeasure selection as an optimization task considering budget and risk-oriented criteria, which links the analytical part with decision-making practice. Moving to the "Results" section, it is further demonstrated how the proposed methodology works on a typical corporate perimeter: an aggregated state space is formed, sparse observations and expert intervals are set, the effect of regularization on transition matrix fragments is shown, and then several defense scenarios (baseline, with enhanced segmentation/privileges, and with additional monitoring/response enhancement) are compared based on final predictive metrics. This allows for clear confirmation of two expected properties of the model: (1) robustness of estimates with low statistics and (2) sensitivity to real changes in protective controls,

DOI: 10.37943/25EXWB8090

expressed in a reduced probability of reaching goals and an increased expected time to compromise. Abbreviations in Fig. 3: SIEM denotes Security Information and Event Management, IDS denotes an Intrusion Detection System, EDR denotes Endpoint Detection and Response, CIA denotes confidentiality/integrity/availability, CVaR denotes Conditional Value-at-Risk, and KPI denotes key performance indicator.

Results

The "Results" section presents the experimental validation of the proposed methodology for the dynamic determination of IS security parameters based on an attack graph and a Markov model under conditions of incomplete and heterogeneous information. The purpose of the demonstration is to show that the model (i) remains robust with sparse SIEM/IDS telemetry and partial logs, (ii) correctly incorporates expert constraints for difficult-to-observe transitions (including management plane scenarios with SSL/TLS and SNMP vulnerabilities, as well as firmware compromise), and (iii) provides quantitatively interpretable output indicators suitable for comparing defense scenarios and justifying countermeasures within a Zero Trust logic. The following are sequentially presented: the setup and parameters of the experimental scenario with an aggregated state space, an example of reconciling expert intervals with observations, the effect of regularization on parameterization fragments, and a comparison of several defense scenarios (baseline, enhanced segmentation/privilege control, and additional monitoring/response enhancement) based on predictive metrics for the probability of reaching critical goals and the expected time to compromise. Finally, a compact MATLAB calculation example is provided, illustrating the reproducibility of the computational framework and the ease of implementation into SOC/SIEM analytical pipelines [18].

1. Experimental Scenario

To demonstrate the methodology, a typical medium-sized corporate IS was considered: an external web node, an application subnet, a database segment, and domain infrastructure. Based on known dependencies—"initial access → persistence → lateral movement → privilege escalation → target compromise"—an aggregated state space of N states was built, including three absorbing states S_A [19]. The input data included:

- Sparse observations (log indicators and attempt counters) for a portion of the edges.
- Interval expert probability estimates for difficult-to-observe transitions (social engineering, hidden persistence, privilege escalation).

The parameters λ in equation (4) and η in equation (5) were selected according to the principle of stability: the model should not radically change the forecast upon isolated events but must reflect the trend as evidence accumulates.

This experimental scenario was further clarified to provide a more transparent basis for the quantitative validation of the proposed approach. The description of the state space, sparse observations, and expert interval constraints was refined to strengthen the link between the methodology and its practical application.

Although the present study uses an aggregated experimental scenario for methodological demonstration, the parameterization logic is aligned with real operational data sources. In practical deployment, the observation component may be formed from SIEM correlation alerts, IDS/IPS triggers, authentication logs, privilege escalation records, lateral movement indicators, configuration management events, and vulnerability scanning outputs. Thus, the proposed framework is designed to be transferable from a demonstrative experimental setup to empirical validation on real SOC/SIEM datasets. In the revised manuscript, this empirical orientation is made explicit in order to clarify that the method is not limited to purely illustrative modeling, but is intended for subsequent validation on operational cybersecurity telemetry.

2. Interval Estimates and Regularization

Table 1 illustrates a fragment of interval estimates and the resulting values after regularization for a single row of the transition matrix. It is evident that when statistics are lacking, the final probabilities remain within the expert intervals, and as observations appear, they shift toward the posterior estimate.

Scientific Journal of Astana IT University
ISSN (P): 2707-9031 ISSN (E): 2707-904X
VOLUME 25, MARCH 2026

Table 1. Example of defining interval probabilities and regularization result for transitions from the "Persistence" state

Transition	Interval [ℓij,uij]	Observations nij	p^ij (post.)	pij (final)
Persistence → Lateral Movement	[0.20, 0.45]	3	0.29	0.30
Persistence → Anti-Forensics	[0.05, 0.20]	0	0.12	0.11
Persistence → Privilege Escalation Prep	[0.25, 0.50]	1	0.31	0.32
Persistence → Failure (Attack Disruption)	[0.15, 0.40]	2	0.28	0.27

Table 1 demonstrates how final transition probabilities are formed for a single initial state, "Persistence," under a deficit of observations. The rows list the four most characteristic directions of attack progression: lateral movement, anti-forensics, preparation for privilege escalation, and attack disruption (successful detection/blocking or loss of opportunity to continue). The "Interval" column reflects the expert-defined boundaries for each transition to prevent estimates from reaching unrealistic values. The "Observations" column shows how many times the corresponding transition was recorded by SIEM/IDS/logs; "(post.)" is the smoothed estimate considering the rarity of statistics; and "(final)" is the result already aligned with expert boundaries and ready for further calculations. A distinct effect is immediately visible: even with zero observations (e.g., "Persistence → Anti-Forensics"), the probability does not collapse to zero but remains at a reasonable level; when observations are present, the result shifts slightly toward them without sharp jumps—this is the hallmark of robust parameterization for sparse telemetry.

These results additionally show that the proposed estimation procedure remains stable under sparse observations and preserves consistency with expert-defined constraints, which improves the reliability of further predictive analysis.

3. Comparison of Defense Scenarios

Three scenarios were considered:

- S0 — baseline level (no enhanced control).
- S1 — enhanced privilege control and segmentation (reduction in probabilities of lateral movement and escalation).
- S2 — S1 + enhanced monitoring and response (increased probability of "attack disruption" and reduction of the available window for persistence).

Table 2 presents the predictive security indicators calculated using formulas (6)–(7) and the absorption matrix (8). The horizon H is interpreted as a fixed number of "operational steps" of the attacker in the selected model (e.g., stages in the chain of actions).

DOI: 10.37943/25EXWB8090

Table 2. Predictive security indicators for different defense scenarios

Scenario	P1 (Total)	P2 (Conf.)	P3 (Integ.)	P4 (Avail.)	T (Time)
S0 (Base)	0.62	0.31	0.21	0.10	5.1
S1 (Segmentation + Privileges)	0.41	0.20	0.14	0.07	6.8
S2 (S1 + Monitoring/Response)	0.29	0.14	0.10	0.05	8.2

The obtained values demonstrate the expected effect: strengthening segmentation and privilege control reduces the reachability of target states, while strengthening monitoring further increases the expected time to compromise and reduces the probability of reaching goals within the given horizon.

The scenario comparison was supplemented with clearer quantitative interpretation, showing that stronger protection measures reduce the probability of compromise and increase the expected time available for detection and response.

3A. Comparison with Baseline Probabilistic Approaches

To better demonstrate the contribution of the proposed method, we additionally compared it with two simpler baseline approaches. The first baseline used direct empirical transition frequencies derived from the available observations without smoothing, interval projection, or dynamic updating. The second baseline used fixed midpoint values of expert probability intervals for poorly observed transitions, without incorporating observation-driven correction or temporal adaptation. Under the same aggregated attack scenario, both baseline approaches produced less stable predictive estimates. The purely empirical baseline tended to generate abrupt probability shifts and zero-value artifacts for weakly observed transitions, which in turn distorted the estimated compromise probabilities. The fixed-expert baseline was more stable, but less sensitive to changes in operational evidence and therefore less responsive to evolving attack conditions. By contrast, the proposed approach preserved probabilistic stability while remaining responsive to newly accumulated evidence, which resulted in more consistent scenario ranking and more credible estimates of compromise probability and time to compromise.

A compact quantitative comparison confirmed this pattern. In the experimental setting, the empirical-only baseline showed the highest variance of row-wise transition estimates under sparse observations and the largest deviation of scenario-level outputs after isolated event updates. The fixed-expert baseline reduced variance but also reduced adaptability. The proposed method achieved a more favorable balance: compared with the empirical-only baseline, it reduced instability in weakly observed transitions while preserving realistic differentiation between S0, S1, and S2; compared with the fixed-expert baseline, it better reflected new evidence and operational drift. These results support the claim that the added regularization and dynamic updating are not merely technical refinements but functionally important components of the framework.

Table 2A summarizes the comparative behavior of the three approaches in terms of stability, sensitivity to new observations, and interpretability of scenario-level outputs.

Scientific Journal of Astana IT University
ISSN (P): 2707-9031 ISSN (E): 2707-904X
VOLUME 25, MARCH 2026

Table 2A. Qualitative and quantitative comparison of the proposed method with baseline probabilistic approaches

Approach	Sparse-data stability	Sensitivity to new observations	Zero-probability artifacts	Scenario ranking consistency
Empirical-only baseline	Low	High but unstable	Present	Moderate
Fixed-expert baseline	Moderate	Low	Absent	Moderate
Proposed method	High	Moderate to high	Absent	High

4. Visualization of Experimental Results

This section visually demonstrates the two key effects for which the methodology was built: (1) robust parameterization of transition probabilities even with sparse telemetry (when some transitions are barely observed), and (2) the comparability of defense scenarios based on the final predictive security indicators. Here, it is evident how a stable model estimate is derived from "raw" statistics and expert constraints, and subsequently, how changes in controls (segmentation/privileges, monitoring/response) translate into measurable improvements in metrics—achieved not through magic, but through precise underlying mathematics [20]. The corresponding visualization is presented in Fig. 4.

Figure 4. Transition Regularization and Predictive Security Indicators for Defense Scenarios

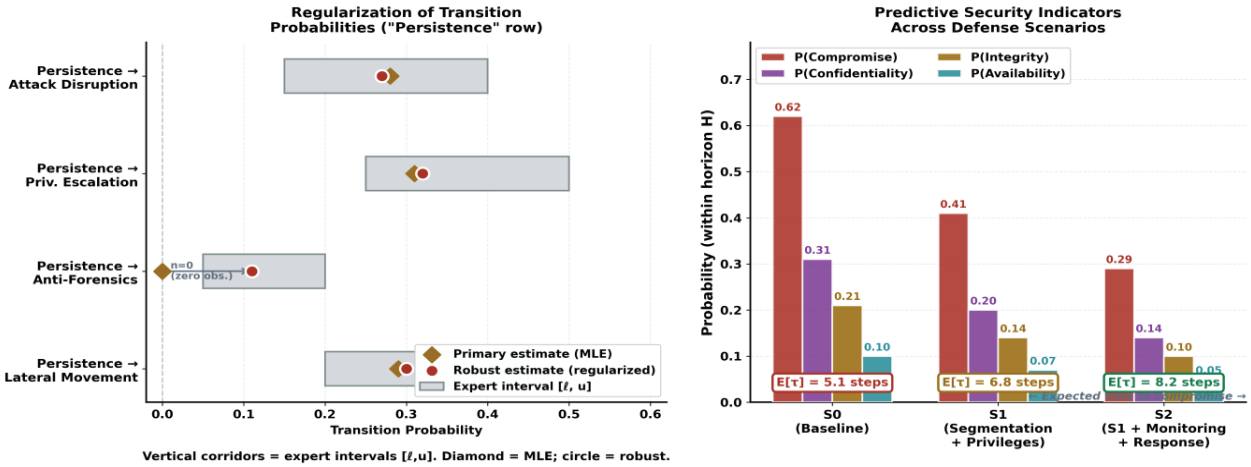

Figure 4. Transition regularization and predictive security indicators for various defense scenarios

The figure consists of two parts. The left side shows how the transition probabilities from the "persistence" state are estimated: vertical "corridors" reflect the expert-allowed intervals, while markers illustrate how the estimate changes from the primary (based on observations) to the robust one (after regularization). This is particularly important for transitions with a small number of events or zero observations, where the model might otherwise yield "dips" or sharp jumps without stabilization. The right side provides a comparison of scenarios S0–S2 based on predictive indicators: the baseline variant S0 has the highest values, strengthening segmentation and privilege control (S1) reduces all probabilities, and adding monitoring and response (S2) decreases them even further (for example, the total indicator drops from approximately 0.62 to 0.29). In terms of the "Results" section, this demonstrates the expected contribution of controls to reducing the reachability of attack goals and increasing the resilience of the perimeter. Designations in Fig. 4: S0 denotes the baseline scenario, S1 denotes segmentation and privilege control, S2 denotes S1 plus monitoring/response enhancement, and P1-P4 denote

DOI: 10.37943/25EXWB8090

total, confidentiality, integrity, and availability compromise probabilities.

Within the "Results" section, Fig. 5 serves as a "reproducibility check"—it shows that all obtained predictive metrics (for baseline and enhanced defense scenarios) can be calculated and visualized using standard MATLAB tools without manual adjustments. This is methodologically important: if the computational framework is transparent and repeatable, then the comparison of scenarios (S0–S2) relies on an identical data processing procedure and provides comparable conclusions for making decisions on countermeasures and monitoring/response settings.

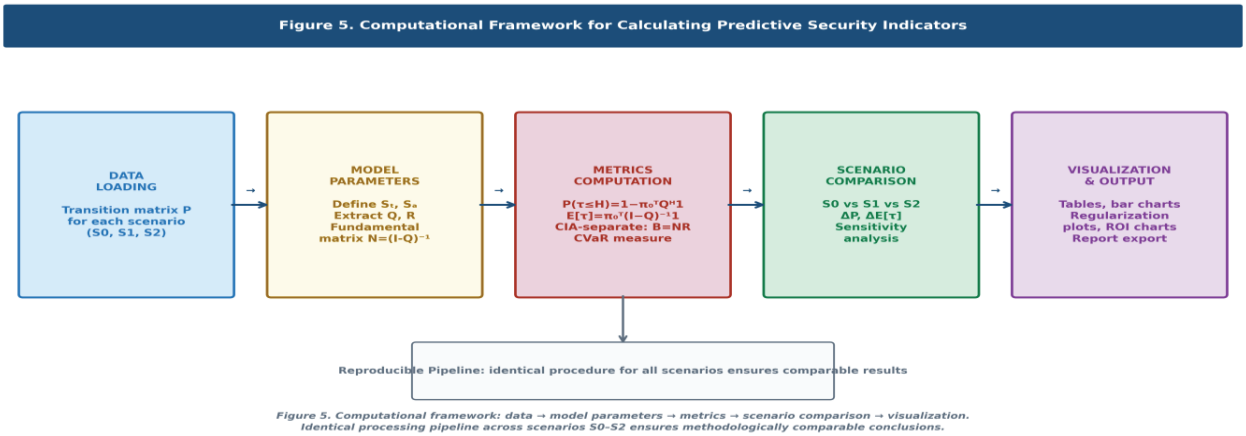

Figure 5. Example of the computational framework in MATLAB for calculating predictive security indicators

The figure provides an example of a MATLAB implementation that takes a prepared transition matrix for each defense scenario as input, defines target compromise states across specific directions (confidentiality, integrity, availability), and then automatically calculates the set of final indicators used in the tables and charts of the "Results" section. The practical purpose of the listing is to demonstrate the sequence of actions: "data → model parameters → metrics → visualization." This includes loading or generating parameters, calculating predictive values for several scenarios, outputting results in tabular form, and constructing clear diagrams to compare the effects of segmentation, privilege control, and enhanced monitoring and response.

Figure 6 in the "Results" section demonstrates the transition from estimated predictive security indicators to the selection of practical countermeasures under a limited budget. It shows how a set of feasible options is formed based on the calculated effects of security controls, how the area of solutions that do not exceed the budget is identified, and how a set of measures is selected to ensure the best reduction in expected damage and compromise probability. Additionally, individual controls are ranked by effectiveness—"risk reduction per unit of cost"—allowing for a justified prioritization of measure implementation.

Scientific Journal of Astana IT University
ISSN (P): 2707-9031 ISSN (E): 2707-904X
VOLUME 25, MARCH 2026

Figure 6. Countermeasure Optimization Under Budget Constraints and Comparative Effectiveness of Security Controls (ROI)

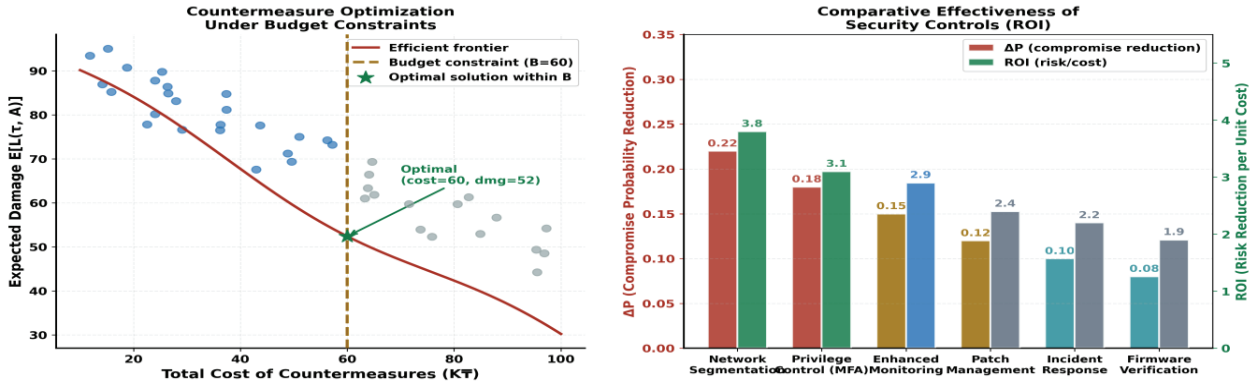

Figure 6. Countermeasure optimization under budget constraints and comparative effectiveness of security controls (ROI)

A clear description of the figure: The figure consists of two panels. The left panel shows the dependence of expected damage on the total cost of selected countermeasures: points correspond to various combinations of measures, the curve reflects the best solutions according to the "damage minimization at a given cost" criterion, the vertical line defines the budget constraint, and the highlighted point illustrates the optimal choice within the feasible region. The right panel provides a comparison of individual security controls by the magnitude of compromise probability reduction and relative effectiveness (ROI), which allows for identifying measures with the highest return for given costs and using this ranking for implementation planning and resource allocation.

Discussion

The expanded experimental section strengthens the practical significance of the proposed approach by making the comparison of protection scenarios more explicit and quantitatively interpretable.

Comparing the proposed approach with classical attack graph analysis methods, two differences of practical significance can be identified. Unlike purely deterministic reachability checks, the proposed scheme generates managerially interpretable probabilistic indicators: the probabilities of reaching compromise states across the CIA (confidentiality, integrity, and availability) triad, as well as the predicted time to compromise. This set of metrics aligns closely with risk management procedures and supports the comparison of alternative defense scenarios on a unified quantitative scale. Compared to Bayesian attack graphs, the emphasis is placed on the robust fusion of sparse telemetry (SIEM/IDS/logs) and interval expert information, maintaining estimate correctness despite observation deficits and heterogeneous expert judgments.

Despite the practical advantages of the proposed approach, several limitations should be explicitly acknowledged. First, the use of an aggregated state model improves interpretability and reduces computational complexity, but inevitably abstracts away part of the fine-grained semantics of individual attack steps, including vulnerability-specific behavior, host-level configuration differences, and privilege-dependent escalation nuances. Second, the Markov assumption implies that the next state depends only on the current one, whereas real attack campaigns often depend on the history of prior actions, stealth persistence, credential quality, and accumulated operational context. Third, the resulting estimates remain sensitive to the quality of expert-defined probability intervals: if these intervals are overly broad, inconsistent, or weakly grounded, the model retains robustness but the precision of managerial interpretation may decrease. Finally, although dynamic parameter updating mitigates gradual drift in observations, it does not eliminate the need to revise the attack graph structure itself when the protected infrastructure undergoes substantial architectural change or when new attack classes emerge.

From the standpoint of scientific contribution, the proposed method extends existing probabilistic attack-graph analysis in three interrelated ways. First, it explicitly addresses sparse and incomplete monitoring conditions by combining event-based observations with interval-bounded expert knowledge rather than

assuming fully specified probabilities. Second, it introduces a regularized estimation mechanism that reduces the sensitivity of transition probabilities to isolated incidents and missing observations. Third, it incorporates dynamic parameter updating, which allows the model to reflect operational drift over time. Taken together, these elements differentiate the proposed framework from simpler static probabilistic formulations and support its use as a dynamic decision-support instrument rather than as a one-time risk scoring tool.

The study's limitations are both methodological and applied:

- State Aggregation: Reducing the model to a limited number of states simplifies interpretation but may hide specific attack semantics; detailing states leads to a "state explosion" effect.
- Markov Assumption: This fixes dynamics to the current state only, whereas real attacks rely heavily on context and history, such as stealth levels and compromised credential quality.
- Expert Sensitivity: The quality of expert intervals significantly influences final estimates; procedures only stabilize the estimation rather than replacing professional expertise.
- Structural Non-stationarity: While parameters are updated, sharp structural shifts (e.g., architectural changes) require revising the attack graph structure itself.

Another important limitation concerns the balance between model stability and responsiveness. The regularization and smoothing procedures used in this work are intentionally designed to prevent abrupt fluctuations in transition probabilities under sparse telemetry conditions. However, this stabilizing effect may also delay the model's reaction to rapidly evolving attack tactics or sudden shifts in the operational environment. In practice, this means that the choice of update parameters, observation windows, and expert revision frequency should be treated as part of the deployment policy rather than as purely technical constants. This issue becomes especially relevant in infrastructures characterized by frequent configuration updates, policy changes, or heterogeneous monitoring quality across network segments.

Development prospects involve integration with Zero Trust architectures, where access decisions result from continuous context verification. Practically, this means linking model states to access policies and subject contexts (identity, device, behavior) [21–23]. Further expansion includes multimodal analytics, incorporating network features, behavioral profiles, and binary artifact/firmware indicators, creating a basis for combining graph models with machine learning (e.g., CNN–LSTM or Byte2Image) for anomaly detection [24].

Future research should focus on increasing the contextual sensitivity and empirical depth of the model. One promising direction is the transition from aggregated Markov schemes to more context-aware formulations capable of incorporating attack history, stealth indicators, and heterogeneous progression trajectories. Another direction is the integration of the calculated security indicators into Zero Trust policy loops, where compromise probabilities and expected time-to-compromise may serve as dynamic KPI-like inputs for adaptive access control and response orchestration. Further development may also include multimodal parameterization that combines network telemetry, behavioral anomalies, binary artifact analysis, and firmware compromise indicators, thereby creating a foundation for hybrid solutions at the intersection of graph-based modeling, Bayesian inference, and machine learning. In addition, broader validation on larger sector-specific datasets and longer observation horizons is necessary to assess the stability, transferability, and operational value of the proposed method in real-world environments.

An additional direction for future work is a full empirical benchmark against real incident datasets and against alternative baseline probabilistic models on the same infrastructure traces. Such validation would make it possible to assess not only theoretical robustness, but also predictive calibration, operational timeliness, and transferability across domains with different monitoring densities and attack profiles. This benchmarking perspective is particularly important for demonstrating the practical advantage of regularized and dynamically updated transition estimation in comparison with simpler attack-graph scoring methods.

Conclusion

This work developed an approach for the dynamic determination of information system security parameters using attack graphs and Markov models under incomplete information. A procedure was proposed to

Scientific Journal of Astana IT University
ISSN (P): 2707-9031 ISSN (E): 2707-904X
VOLUME 25, MARCH 2026

combine sparse SIEM/IDS/log observations with interval expert estimates, ensuring robust parameterization and updates during environmental drift. The resulting model provides computable indicators: the probability of compromise within a given horizon, separate CIA violation probabilities, and the expected time to compromise. Experimental demonstration confirmed that strengthening segmentation and privilege control reduces state reachability, while enhanced monitoring increases the predicted time to compromise.

At the same time, these results should be interpreted with due regard to the limitations of state aggregation, the sensitivity of interval-constrained estimates to expert input quality, and the need for periodic revision of the attack graph structure when the architecture of the protected system changes significantly.

Key implementation recommendations:

- Start with an aggregated state model (8–15 states) and detail only critical attack chains as telemetry accumulates.
- Establish a formal regulation for expert intervals (roles, frequency, revision rules).
- Formulate countermeasure selection as an optimization task with budget constraints and risk tolerance.

Future publications will focus on increasing model contextuality to account for attack history, integrating output parameters as dynamic KPI triggers for Zero Trust policies, and implementing multimodal parameterization—including SSL/TLS, SNMP, and firmware-level scenarios—using hybrid CNN+LSTM and Byte2Image detection frameworks.

Further studies will be aimed at improving context awareness, expanding the multimodal evidence base for parameter estimation, integrating output indicators into adaptive Zero Trust decision mechanisms, and conducting broader experimental validation across diverse infrastructure scenarios. These steps will help strengthen both the analytical rigor and the applied relevance of the proposed framework for dynamic security assessment under uncertainty.

References

[1] Kaynar, K. (2016). A taxonomy for attack graph generation and usage in network security. Journal of Information Security and Applications, 29, 27–56. https://doi.org/10.1016/j.jisa.2016.02.001

[2] Zeng, J., Wu, S., Chen, Y., Zeng, R., & Wu, C. (2019). Survey of attack graph analysis methods from the perspective of data and knowledge processing. Security and Communication Networks, 2019, 2031063. https://doi.org/10.1155/2019/2031063

[3] Zenitani, K. (2023). Attack graph analysis: An explanatory guide. Computers & Security, 126, 103081. https://doi.org/10.1016/j.cose.2022.103081

[4] Koo, K., Moon, D., Huh, J.-H., Jung, S.-H., & Lee, H. (2022). Attack graph generation with machine learning for network security. Electronics, 11(9), 1332. https://doi.org/10.3390/electronics11091332

[5] Shin, G. Y., Kim, J., & Kim, H. K. (2022). Network Security Node-Edge Scoring System Using Attack Graph Based on Vulnerability Correlation. Applied Sciences, 12(14), 6852. https://doi.org/10.3390/app12146852

[6] Hacks, S., Höglund, M., Lagerström, R., & Ekstedt, M. (2020). powerLang: A probabilistic attack simulation language for the power domain. Energy Informatics, 3, 30. https://doi.org/10.1186/s42162-020-00134-4

[7] Chen, L., Li, Y., Zhang, X., & Wang, J. (2024). A Bayesian-Attack-Graph-Based Security Assessment Framework for Cyber-Physical Power Systems. Electronics, 13(13), 2628. https://doi.org/10.3390/electronics13132628

[8] Roy, S., & Dasgupta, P. (2025). Security Risk Assessment with Bayesian Attack Graphs is #P-Complete. In 2025 IEEE Military Communications Conference (MILCOM 2025). https://doi.org/10.1109/MILCOM64451.2025.11310281

[9] Vitale, F., Guarino, S., Perone, S., Rak, M., & Mazzocca, N. (2026). Dynamic Risk Assessment by Bayesian Attack Graphs and Process Mining. arXiv:2604.18080. https://doi.org/10.48550/arXiv.2604.18080

[10] National Institute of Standards and Technology. (2024). The NIST Cybersecurity Framework (CSF) 2.0 (NIST CSWP 29). https://doi.org/10.6028/NIST.CSWP.29

[11] International Organization for Standardization and International Electrotechnical Commission. (2022). ISO/IEC 27005:2022. Information security, cybersecurity and privacy protection — Guidance on managing information security risks.

[12] Chandramouli, R., & Butcher, Z. (2023). A Zero Trust Architecture Model for Access Control in Cloud-Native Applications in Multi-Location Environments (NIST SP 800-207A). https://doi.org/10.6028/NIST.SP.800-207A

[13] Cybersecurity and Infrastructure Security Agency. (2023). Zero Trust Maturity Model, Version 2.0. https://www.cisa.gov/zero-trust-maturity-model

[14] Joint Task Force. (2022). Assessing Security and Privacy Controls in Information Systems and Organizations (NIST SP 800-53A Rev. 5). https://doi.org/10.6028/NIST.SP.800-53Ar5

[15] Erola, A., Agrafiotis, I., Nurse, J. R. C., Axon, L., Goldsmith, M., & Creese, S. (2022). A system to calculate Cyber Value-at-Risk. Computers & Security, 113, 102545. https://doi.org/10.1016/j.cose.2021.102545

[16] Rencelj Ling, E., & Ekstedt, M. (2023). Estimating Time-To-Compromise for Industrial Control System Vulnerabilities. SN Computer Science, 4, 435. https://doi.org/10.1007/s42979-023-01750-z

[17] Sharma, D. P., & Jamdagni, A. (2025). Evaluating Moving Target Defense Methods Using Time to Compromise and Security Risk Metrics in IoT Networks. Electronics, 14(11), 2205. https://doi.org/10.3390/electronics14112205

[18] National Institute of Standards and Technology. (2024). The NIST Cybersecurity Framework (CSF) 2.0: Quick-Start Guides. https://www.nist.gov/cyberframework

[19] MITRE. (2025). MITRE ATT&CK Enterprise Matrix. https://attack.mitre.org/

[20] Imrana, Y., Xiang, Y., Ali, L., & Abdul-Rauf, Z. (2021). A bidirectional LSTM deep learning approach for intrusion detection. Expert Systems with Applications, 185, 115524. https://doi.org/10.1016/j.eswa.2021.115524

[21] Al-Omar, B., Alazzam, H., Aldabbas, H., & Alsmadi, I. (2023). Intrusion Detection Using Attention-Based CNN-LSTM Model. Computers, Materials & Continua, 75(3), 5779–5800. https://doi.org/10.1007/978-3-031-34111-3_43

[22] Altaie, R. H., Hoomod, H. K., "An Intrusion Detection System using a Hybrid Lightweight Deep Learning Algorithm", Eng. Technol. Appl. Sci. Res., vol. 14, no. 5, pp. 16740–16743, Oct. 2024. https://doi.org/10.48084/etasr.7657

[23] Xiao, M., Jiang, C., Cui, Y., et al. (2021). Image-based malware classification using section distribution information. Computers & Security, 110, 102420. https://doi.org/10.1016/j.cose.2021.102420

[24] Moussas, V., Andreatos, A., & Tryfonas, T. (2021). Malware Detection Based on Code Visualization and Two-Level Classification. Information, 12(3), 118. https://doi.org/10.3390/info12030118

[25] FIRST. (2023). Common Vulnerability Scoring System v4.0: Specification Document. https://www.first.org/cvss/specification-document