Assessment of Corporate Network Penetration Scenarios Based on Iterative Link Weight Determination Using the MRRW-PageRank Method

Oleksii Novikov[1,†], Dmytro Lande[1,*,†] and Lesia Alekseichuk[1,†]

[1] National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine

Abstract

The article proposes an approach to modeling and ranking scenarios of destructive cyberattacks on corporate information and communication systems, based on the proposed iterative MRRW-PageRank algorithm. Unlike methods that rely on expert assessments or large language models to determine transition probabilities between network nodes, the proposed method utilizes only the structural topology of the network. The algorithm establishes interdependence between node importance (e.g., database servers) and the weights of links leading to them, simulating an adversary's strategy aimed at reaching critical resources via the most probable paths. Using a typical corporate network as a case study, the method's effectiveness is demonstrated in identifying critical intrusion paths and ranking attack scenarios by risk. This approach is particularly relevant during network design phases or initial security audits, when empirical data on vulnerabilities or incidents are unavailable.

Keywords

MRRW-PageRank, cyber risk analysis, penetration scenarios, corporate network, link weights, topological analysis, logical-probabilistic modeling, cybersecurity

1. Introduction

Cyber risk analysis in corporate information and communication systems (ICS) remains one of the most pressing challenges in modern cybersecurity, particularly during network design phases, topological audits, or initial security assessments when empirical data on vulnerabilities, incident history, or access policies are unavailable. Under such conditions, the only accessible source of information is the network structure itself—the topology of interconnections among its components. This creates a need for methods capable of objectively, deterministically, and reproducibly evaluating potential attacker pathways based solely on system architecture.

Among existing approaches to attack scenario modeling, logic-probabilistic models are widely used, formalizing hazardous system states through Boolean functions and probabilities of individual node compromise [1]. However, a key challenge with these models lies in determining their coefficients—specifically, the conditional probabilities of transitions between nodes. Traditionally, these values are elicited from domain experts [2–4], rendering assessments subjective and dependent on the availability of qualified specialists. Recently, large language models (LLMs) have been proposed as a "swarm of virtual experts" to generate such estimates [5]. While this approach demonstrates high flexibility and the ability to capture complex logical dependencies, it remains stochastic, computationally intensive, and does not always guarantee reproducible results.

On the other hand, node centrality analysis methods—particularly PageRank and its variants—have long been employed to identify critical components in networks [6]. However, in most cases, link weights are either assumed equal or assigned based on expert judgment or external data (e.g., CVSS vulnerability scores) [7, 8]. This limits their applicability during early stages of the ICS lifecycle. To address this gap, we propose an iterative algorithm, MRRW-PageRank (Mutually-

[1] SMICS'25: Workshop on Cryptology and Data Security, October 16-18, 2025, Lviv, Ukraine

* Corresponding author.

† These authors contributed equally.

alexnov10@gmail.com (O. Novikov); dwlande@gmail.com (D. Lande); ipt.kpi.ua@gmail.com (L. Alekseichuk)

0000-0001-5988-3352 (O. Novikov); 0000-0003-3945-1178 (D. Lande)

Reinforced Risk-Weighted PageRank) [9], which determines node and link weights in a mutually dependent manner using only network topology. In this approach, a node's importance increases the likelihood of paths leading to it being exploited; simultaneously, each individual path toward a "highly connected" node (i.e., one with many incoming links) receives a lower weight due to reduced uniqueness—effectively reflecting real-world attacker behavior.

This paper introduces a novel approach to penetration scenario assessment that integrates attack modeling (as in [5], [9]) with a newly proposed structural weight estimation method based on MRRW-PageRank. In contrast to prior work, our method is not applied to a simplified 7-node network but to a more realistic topology comprising 12 components: a firewall, router, core switch, web server, database server, Active Directory server, administrator and user workstations, network-attached storage (NAS), a SIEM system, and a Wi-Fi access point. This enables us to demonstrate the method's effectiveness in a more complex, real-world-like environment. The resulting link weights are interpreted as conditional transition probabilities and used to generate and rank attack scenarios according to likelihood, duration, and resource intensity.

Thus, the objective of this work is to bridge the gap between logic-probabilistic modeling of penetration scenarios and the need for an objective, structure-based method to determine model parameters in situations where empirical data are unavailable.

2. Description of the Corporate Network Model

To demonstrate the effectiveness of the proposed approach to evaluating penetration scenarios, we employ a model topology of a corporate information and communication system (ICS) that reflects the typical architecture of a medium-sized enterprise. This model comprises 12 key components covering the main categories of assets: external interface, switching core, servers of various purposes, administrator and user workstations, as well as auxiliary security and data storage systems.

The network is represented as a directed graph $G = (V, E)$, where the set of vertices V corresponds to the functional components of the ICS, and the set of directed edges $E \subseteq V \times V$ represents possible directed connections (e.g., network access, service invocation, authentication). Each edge $(i, j) \in E$ indicates the possibility of transitioning from resource i to resource j – for instance, via network access, service call, or authentication. This formalization enables the representation of potential attacker movement paths as sequences of transitions between graph nodes.

2.1. Network Composition

The model includes the following nodes (see Tab. 1, Fig. 1).

2.2. Principles of Topology Construction

The connections between nodes are established based on realistic interaction scenarios within a corporate network:

- External traffic flows through FW ⟶ Router ⟶ SwC, reflecting a typical perimeter security architecture.
- The web server (SW) is located in the DMZ, connected to SwC, and has outgoing links to SDB and SAD for data retrieval.
- The Active Directory server (SAD) serves as the central component:
  - it initiates connections to all workstations (WU1, WU2, WA) for authentication and management;
  - it maintains a connection to NAS (to provide storage access);
  - it initiates event transmission to SIEM;

  - it initiates a reverse connection to SwC (e.g., for synchronization or monitoring).
- The administrator workstation (WA) has outgoing links to SDB, SAD, NAS, and SwC, reflecting its elevated privileges.
- User workstations (WU1, WU2) are connected to NAS and SAD, and also connect via WAP.
- The wireless access point (WAP) initiates connections to WU1 and WU2 (as an access point).
- SIEM does not initiate any connections—it only receives events (a passive node).
- SDB has no outgoing links—it serves as an endpoint (the target of an attack).

In total, the graph defines 26 directed connections, representing both legitimate communication paths and potential attack vectors (e.g., using the web server or the administrator workstation as an initial entry point for further movement toward SDB).

Table 1
Abbreviations and Their Purposes

Abbreviation	Full name	Purpose
FW	Firewall	External security interface; entry point from the Internet
Router	Network router	Traffic routing between external and internal network segments
SwC	Switch-Core	Network switching core; central point for internal switching
WU1, WU2	WS-User1, WS-User2	User workstations
WA	WS-Admin	Administrator workstation (with elevated privileges)
SW	Server-Web	Web server accessible from external networks
SDB	Server-DB	Database server (critical resource)
SAD	Server-AD	Active Directory server (central authentication point)
NAS	Network Attached Storage	Network-attached data storage
SIEM	Security Information and Event Management	Security event collection and analysis system
WAP	Wireless Access Point	Wireless access point for mobile devices

In total, the graph defines 26 directed connections, representing both legitimate communication paths and potential attack vectors (e.g., leveraging the web server as an initial entry point for lateral movement toward SAD or SDB).

This topology enables modeling of complex intrusion scenarios, including:

- External attacks via the web interface;
- Insider threats through workstation compromise;
- Vertical privilege escalation via an administrative workstation;
- Lateral movement through the Active Directory server.

This model is realistic and reflects the complexity of modern corporate ICS (Information and Communication Systems). It is also ideally suited for applying the MRRW-PageRank method, as it contains nodes of varying criticality and diverse topological patterns (star, chain, centralized authentication, etc.).

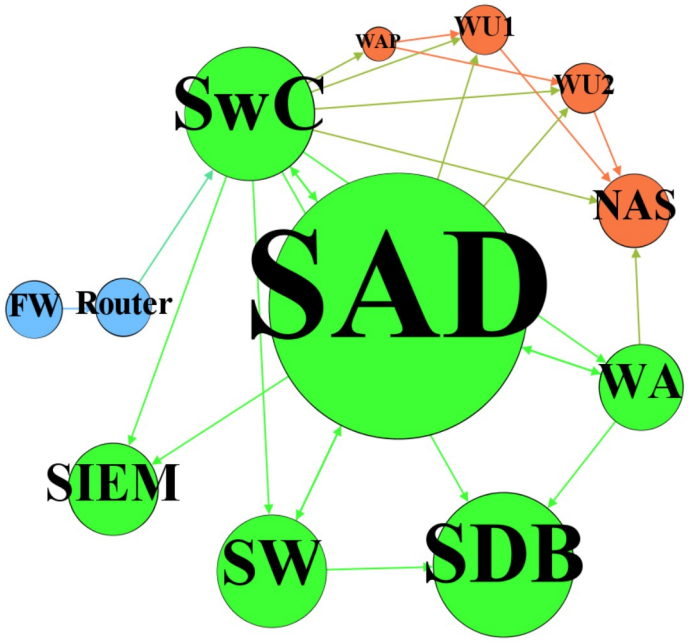

Figure 1. Diagram of nodes and connections in a computer network.

3. Methodology for Scenario Assessment Based on MRRW-PageRank

This section proposes a methodology for evaluating scenarios of destructive actions within a corporate network, based on the application of the iterative MRRW-PageRank algorithm (Mutually-Reinforced Risk-Weighted PageRank). In contrast to approaches that rely on expert judgments or large language models to determine transition probabilities between nodes [1], the proposed method utilizes exclusively the network topology as input data. This makes it particularly suitable for design phases, topological audits, or initial security assessments, where empirical data on vulnerabilities, access policies, or incident history are unavailable.

3.1. MRRW-PageRank Algorithm

The MRRW-PageRank algorithm (Mutually-Reinforced Risk-Weighted PageRank) is built upon the iterative interaction between two network components: the node importance vector and the link-weight matrix. The model is based on the assumption that a node's importance is determined not only by the number of incoming links but also by their quality—specifically, the probability that each of these links will be exploited by an attacker to reach the target node. Conversely, the likelihood of a link being used depends on the importance of the target node and the structural characteristics of its connectivity within the network. This interdependence is modeled as an iterative process converging to a stable weight distribution that reflects potential intrusion risks.

Initialization of node weights

Node weights are initially estimated using the standard PageRank algorithm, one of the most well-known methods for measuring centrality in directed graphs [3]. PageRank models a random walk over the graph, which can conceptually be interpreted as the behavior of an attacker sequentially moving from one resource to another. The initial node importance vector $r^{(0)} \in \mathbb{R}^n$ is computed using the following formula:

$$r^{(0)} = PageRank\left(G, d\right),$$

where $d \in (0,1)$ is the damping factor. This parameter determines the probability that a "random surfer" (in our case, an attacker) will continue navigating along the links rather than jumping to a random node. It prevents the algorithm from getting stuck in absorbing components of the graph and ensures convergence. The vector $r^{(0)}$ is normalized such that the sum of all its components equals one:

$$\left\| r^{(0)} \right\| = \sum_{i=1}^{n} \left| r_i^{(0)} \right| = 1.$$

Iterative update of links weight

At each iteration $k \geq 1$, the link weights are recalculated based on the current approximation of node $r^{(k-1)}$ importance. The weight of link $(i, j) \in E$ is defined as:

$$w_{ij}^{(k)} = \begin{cases} \dfrac{r_j^{(k-1)}}{1 + \alpha \cdot d_j^{in}}, & if \quad (i,j) \in E, \\ 0, & otherwise. \end{cases}$$

where $r_j^{(k-1)}$ is the current importance score of node j from the previous iteration, $d_j^{in} = \sum_{i=1}^{n} A_{ij}$ is the in-degree of node *j*, and α>0 is a normalization parameter controlling the influence of the degree on the weight.

This formula reflects two key hypotheses regarding attacker behavior: (1) the more important a node *j* is (i.e., the higher r_j), the higher the likelihood that paths leading to it will be exploited; and (2) the greater the in-degree of node j, the lower the weight assigned to each individual incoming link.

Thus, the weight of link w_{ij} is interpreted as the relative attractiveness of this path to an attacker, accounting for both the target's value and its "popularity" within the network topology.

Construction of the transition matrix

Based on the updated link weights, a transition matrix $M^{(k)} \in \mathbb{R}^{n \times n}$ is constructed, defining the probabilities of moving between nodes. Each entry $M_{ij}^{(k)}$ of the matrix is given by the normalized weight of the corresponding link:

$$M_{ij}^{(k)} = \frac{w_{ij}^{(k)}}{\sum_{l=1}^{n} w_{il}^{(k)}}.$$

If node i has no outgoing links (i.e., $\sum_{l=1}^{n} w_{il}^{(k)} = 0$), the standard PageRank damping strategy is applied. This matrix is row-stochastic, allowing it to be interpreted as a transition probability matrix for a Markov chain modeling an attacker's movement through the network.

Node Importance Update

The new node importance vector $r^{(k)}$ is computed using a modified PageRank equation, where uniform weights are replaced by weighted transitions:

$$r^{(k)} = (1-d)\cdot\frac{1}{n} + d \cdot M^{(k)T} r^{(k-1)}.$$

This equation captures two distinct pathways for "visiting" nodes: with probability 1 – *d*, the attacker "jumps" to a random node (modeling unexpected attacks or exploitation of external vectors), and with probability d, the attacker follows weighted links according to the current transition matrix. The process is repeated iteratively until convergence is achieved:

$$\left\| r^{(k)} - r^{(k-1)} \right\|_1 < \varepsilon,$$

where ε is a small constant defining the desired computational precision.

3.2. Interpreting Link Weights as Conditional Probabilities

The core idea is that the link weights obtained upon convergence of the MRRW-PageRank algorithm are interpreted as conditional probabilities of the attacker transitioning from one node to another:

$$P(v_i \longrightarrow v_j) = w_{ij},$$

where w_{ij} is the normalized weight of the link from node v_i to node v_j, obtained after completing the iterative process.

However, to ensure a correct probabilistic interpretation, the weights must be normalized separately for each source node so that the sum of probabilities of all possible transitions from that node equals 1:

$$\tilde{w}_{ij} = \frac{w_{ij}}{\sum_{(i,k)\in E} w_{ik}}.$$

The resulting matrix $\tilde{W} = [\tilde{w}_{ij}]$ is row-stochastic and can be used as the transition matrix in a Markov chain modeling attacker behavior.

3.3. Generation of Penetration Scenarios

A penetration scenario is defined as a directed path in graph $G = (V, E)$ leading from an initial node (threat source) to a target node (critical resource, e.g., a database server SDB). Formally, a scenario s_k is represented as a sequence:

$$s_k = (v_{k1}, v_{k2}, \ldots, v_{km}),$$

where $v_{k1} \in V_{source}$ is the initial node (e.g., FW, WU1, WA), $v_{km} = v_{target}$ is the target node (e.g., SDB), and $(v_{ki}, v_{ki+1}) \in E$ for all $i = 1, \ldots, m-1$.

All possible scenarios are generated by exhaustively enumerating all simple paths (i.e., paths without cycles) from each source node to the target node. This can be implemented using depth-first search (DFS) algorithms or specialized attack graph analysis techniques.

3.4. Scenario Probability Assessment

The probability of scenario s_k is computed as the product of the conditional probabilities of transitions between consecutive nodes:

$$P(s_k) = \prod_{i=1}^{m-1} w_{ki,ki+1}.$$

In this formula, instead of the averaged LLM-based estimates used in prior work [1], we employ objective, structurally grounded values derived from MRRW-PageRank.

3.5. Scenario Ranking

After computing the probabilities of all scenarios, they are ranked according to several criteria:

Probability of success $P(s_k)$ – the primary criterion; scenarios with higher probability are considered more realistic.

Duration (path length) $L(s_k) = m - 1$ – shorter paths are more attractive to attackers, as they require less time and effort.

Criticality of intermediate nodes – paths passing through high-ranked nodes (e.g., SAD, WA) may entail elevated risk due to the potential for vertical privilege escalation.

For an integrated ranking, a combined scoring function can be employed:

$$R(s_k) = \alpha \cdot P(s_k) - \beta \cdot L(s_k) - \gamma \cdot C_{avg}(s_k),$$

where $C_{avg}(s_k)$ denotes the average weight of nodes along the path (as a measure of criticality), and $\alpha, \beta, \gamma \geq 0$ are tunable coefficients reflecting the analyst's priorities.

Scenarios are sorted in descending order of the Score $R(s_k)$ value, enabling the identification of the most probable and most dangerous intrusion paths.

3.6. Advantages of the Proposed Approach

The proposed approach offers several significant advantages that enhance its scientific and practical value in the context of cyber-risk analysis.

First, it is deterministic: since the MRRW-PageRank algorithm contains no stochastic components, its results are fully reproducible under identical input conditions, unlike approaches based on large language models, which may produce variable outputs even when given identical prompts.

Second, the method does not rely on expert assessments or external data (e.g., CVSS scores, access logs, or incident history), making it suitable for application during the early stages of designing information and communication systems, when such information is not yet available.

Third, the approach is structurally well-founded: it formalizes the interdependence between the importance of target nodes and the attractiveness of paths leading to them by modeling the strategic behavior of an adversary who seeks to reach critical resources while accounting for the topological "overload" of targets.

Fourth, the resulting edge weights can be directly interpreted as conditional transition probabilities and integrated into existing logic-probabilistic cybersecurity models [7, 10], ensuring compatibility with established formalisms for attack scenario analysis.

Thus, the proposed methodology provides an objective, formalized, and computationally efficient foundation for assessing the likelihood of penetration scenarios, particularly under conditions of limited information about the system's security posture.

4. Simulation Results

To verify the effectiveness of the proposed methodology for assessing penetration scenarios based on MRRW-PageRank, computational simulations were performed using a typical corporate information and communication system comprising 12 components. The simulations were carried out according to the algorithm described in Section 3, employing the link-weight matrix obtained from the convergence of the MRRW-PageRank iterative process.

4.1. Input Data

The database server (SDB) was selected as the target node (i.e., the ultimate objective of an attack) —a critical resource with no outgoing connections and thus representing the logical endpoint of most penetration scenarios. Threat sources were defined as all nodes possessing paths leading to SDB: FW, Router, SwC, WA, SW, SAD, WU1, WU2.

The weight matrix of connections $W = [w_{ij}]$, obtained upon convergence of MRRW-PageRank (15 iterations, precision $\varepsilon = 10^{-6}$), was used to construct the conditional transition probability matrix $\hat{W}$ by normalizing its elements row-wise.

For example, for the node SwC (Switch-Core), the sum of outgoing weights equals:

$$\sum w_{SwC,*}=0.0150+0.0150+0.0340+0.0425+0.0210+0.0260+0.0150+0.0240+0.0175=0.210.$$

In this case, the transition probability from SwC to SDB is:

$$\hat{w}_{SwC,SDB} = \frac{0.0210}{0.210} = 0.100.$$

Similarly, all rows of matrix W were normalized, yielding a stochastic transition matrix $\hat{W}$, suitable for modeling attacker behavior as a Markov chain.

4.2. Penetration Scenario Generation

Based on the network graph and the transition matrix $\hat{W}$, all simple paths (without cycles) from the initial nodes to the SDB were generated. In total, 12 unique scenarios were identified; the most probable ones are listed in Table 2.

Table 2
Most Probable Penetration Scenarios to the SDB

No.	Scenario	Node sequence	Probability $P(s_k)$	Length
1	s_1	WA ⟶ SDB	0.339	1
2	s_2	SW ⟶ SDB	0.447	1
3	s_3	SwC ⟶ SDB	0.100	1
4	s_4	SAD ⟶ SwC ⟶ SDB	0.237 × 0.100 =0.0237	2
5	s_5	Router ⟶ SwC ⟶ SDB	1.000·0.100=0.100	2
6	s_6	FW ⟶ Router ⟶ SwC ⟶ SDB	1.000·1.000·0.100=0.100	3
7	s_7	WA ⟶ SAD ⟶ SwC ⟶ SDB	0.419 × 0.237 × 0.100 ≈0.0099	3
8	s_8	WU1 ⟶ NAS ⟶ SwC ⟶ SDB	Impossible (NAS has no outgoing connections)	–

4.3. Scenario Ranking

Scenarios are ranked according to the combined criterion with coefficients $\alpha = 1$, $\beta = 0.1$, $\gamma = 0$ (emphasizing probability and duration):

$$R(s_k) = P(s_k) - 0.1 \cdot L(s_k).$$

The results are presented in Table 3.

Table 3.
Scenario Ranking

Rank	Scenario	$P(s_k)$	$L(s_k)$	$R(s_k)$
1	s_2: SW ⟶ SDB	0.447	1	0.347
2	s_1: WA ⟶ SDB	0.339	1	0.239
3	s_3: SwC ⟶ SDB	0.100	1	0.090
4	s_5: Router ⟶ SwC ⟶ SDB	0.100	2	0.080
5	s_6: FW ⟶ Router ⟶ SwC ⟶ SDB	0.100	3	0.070
6	s_4: SAD ⟶ SwC ⟶ SDB	0.0125	2	-0.1763
7	s_7: WA ⟶ SAD ⟶ SwC ⟶ SDB	0.0099	3	-0.2901

The table shows that the most dangerous scenarios are short paths with high probability, particularly those originating from the web server (SW) and the administrator workstation (WA). This underscores the importance of controlling external interfaces and privileged accounts.

4.4. Results Analysis

Analysis of the obtained results allows for several important conclusions regarding the structure of cyber risks in the examined corporate network.

First, the most dangerous entry points are the web server (SW) and the administrator workstation (WA), as they exhibit the highest probabilities of direct transitions to the database server (SDB)—the primary attack target. Notably, the probability of the scenario SW → SDB (≈ 0.447) even exceeds that of WA → SDB (≈ 0.339), underscoring the critical role of the external attack vector via the web interface. This finding fully aligns with real-world cyberattack statistics, where web applications and privileged accounts consistently rank among the most common initial access points.

Second, although the Active Directory server (SAD) received the highest node weight among all components (0.182), it lacks a direct connection to SDB, and all paths through SAD are indirect and multi-hop (e.g., SAD → SwC → SDB). Due to normalization of outgoing link weights, the transition probability SAD → SwC is only ≈ 0.237, resulting in an overall scenario probability of s_4 ≈ 0.0237—significantly lower than that of direct transitions. This clearly illustrates a key advantage of the proposed method: it does not rely solely on the importance of individual nodes but also accounts for the actual topological accessibility of the target, including the number of alternative paths and their probabilistic weights.

Third, the external path FW → Router → SwC → SDB has a probability of 0.100, which adequately reflects the realistic external threat without overstating it as dominant compared to internal attack vectors. This confirms the model's balance: it does not inflate the risk of external attacks when they require traversing multiple layers of defense.

Finally, all hypothetical scenarios involving traversal through the Network Attached Storage (NAS) or the SIEM system proved topologically infeasible, as these nodes possess no outgoing connections. This validates the correctness of the model construction and demonstrates its ability to automatically filter out unrealistic intrusion paths, thereby enhancing the reliability of the analysis.

Thus, the proposed approach not only identifies critical assets but also ranks realistic attack vectors based on the structural properties of the network, making it especially valuable during network design and initial security audit phases.

4.5. Comparison with the LLM-Based Approach

In contrast to approaches where transition probabilities were determined through expert judgment and incorporated subjective assessments (e.g., P(WA→SDB) = 0.65), the proposed method differs fundamentally:

- Transition probabilities are determined objectively based solely on network topology, without relying on expert opinions or external data;
- Results are deterministic and fully reproducible: under identical input conditions, the algorithm always yields the same outcome, unlike large language models (LLMs), which may produce varying estimates even for identical prompts;
- The method does not require vulnerability data, CVSS scores, or incident history, making it particularly suitable for network design phases or initial security audits when such information is not yet available.

It is important to emphasize that within the MRRW-PageRank framework, the probability P(WA→SDB) is computed by normalizing the weights of all outgoing links from WA, yielding

P(WA→SDB) ≈ 0.339 – a value grounded in the actual network structure rather than subjective assumptions. Thus, the proposed method not only eliminates subjectivity but also provides a structurally justified, transparent, and computationally efficient alternative to LLM-based approaches during early-stage cyber risk assessment.

5. Conclusions

This work proposes a novel approach to evaluating intrusion scenarios in corporate information and communication systems by integrating the problem of logic-probabilistic modeling of cyberattacks with a structural risk assessment method based on an iterative MRRW-PageRank algorithm. Unlike prior studies that relied on expert judgments or large language models to estimate transition probabilities between network nodes, the proposed method utilizes solely the network topology as its input data source. This makes it particularly suitable for design phases, topological audits, or preliminary security assessments, where empirical data on vulnerabilities, access policies, or incident history are unavailable.

Application of the method to a realistic 12-node network—including a firewall, router, core switch, servers of various purposes, administrator and user workstations, network-attached storage, a SIEM system, and a Wi-Fi access point—demonstrated its ability not only to identify critical assets (notably the Active Directory server and the database server) but also to rank intrusion scenarios according to their likelihood, duration, and structural attractiveness of the paths involved. The results revealed that the most probable attack vectors are direct transitions from the administrative workstation to the database server and external paths via the web server—findings fully consistent with known real-world cyberattack practices.

The scientific novelty of this work lies in the first formalization of intrusion scenario evaluation through the lens of interdependent weight updates for nodes and links: the importance of a target node increases the likelihood of paths leading to it, yet each individual path to a “highly connected” node (i.e., one with many incoming links) receives a lower weight due to reduced uniqueness. This approach effectively models the strategy of a real-world adversary who seeks to reach the most valuable resources but selects not just any path, but rather the one offering maximum effectiveness with minimal effort. This fundamentally distinguishes the proposed method from classical PageRank or other centrality metrics, which do not treat links as carriers of risk.

Furthermore, this study is the first to demonstrate that link weights derived via MRRW-PageRank can be directly interpreted as conditional transition probabilities within a Markov chain modeling attacker behavior and subsequently employed within a logic-probabilistic framework to compute full attack scenario probabilities.

A key advantage of the proposed approach is its determinism and reproducibility: unlike LLM-based methods, results do not depend on random sampling, model version, or prompt formulation, thereby ensuring reliability and transparency of the analysis. At the same time, the method does not aim to fully replace LLM-based approaches; rather, it complements them by providing an objective, structurally grounded foundation for further refinement. For instance, MRRW weights can serve as initial values in Bayesian networks or as contextual input for LLM queries, thereby enhancing accuracy and reducing response variability.

A limitation of the method is its disregard for actual vulnerabilities, security configurations, or behavioral anomalies—yet precisely this characteristic renders it a universal tool for early stages of a system’s lifecycle. Future work will focus on integrating MRRW-PageRank with dynamic data (e.g., CVSS scores, access logs) to develop a hybrid model that combines structural soundness with adaptability to the real-time security state. Thus, the proposed approach not only fills a gap in existing cyber-risk analysis methodologies but also opens new avenues for building evolutionary, self-tuning cyber defense systems.

Declaration on Generative AI

During the preparation of this work, the authors used ChatGPT and Qwen to: translate certain text fragments into English, perform grammar and spelling checks, and paraphrase or reword content. After using these tools, the authors carefully reviewed and edited the content as needed and take full responsibility for the publication's content.

References

[1] L. Alekseichuk, O. Novikov, A. Rodionov, D. Yakobchuk. Cyber Security Logical and Probabilistic Model of a Critical Infrastructure Facility in the Electric Energy Industry . Theoretical And Applied Cybersecurity - Vol.5 No. 1, 2023, c. 61-66. DOI: 10.20535/tacs.2664-29132023.1.287365L

[2] Muhammet Aydin, Emre Akyuz, Osman Turan, Ozcan Arslan. *Validation of risk analysis for ship collision in narrow waters by using fuzzy Bayesian networks approach.* Ocean Engineering. Volume 231, 1 July 2021, 108973. DOI: 10.1016/j.oceaneng.2021.108973

[3] Cameron J. Williams, Kevin J. Wilson, Nina Wilson. A Comparison of Prior Elicitation Aggregation Using the Classical Method and SHELF, *Journal of the Royal Statistical Society Series A: Statistics in Society*, Volume 184, Issue 3, July 2021, Pages 920–940, https://doi.org/10.1111/rssa.12691

[4] Dooyoul Lee, Kybeom Kwon. *Dynamic Bayesian network model for comprehensive risk analysis of fatigue-critical structural details.* Reliability Engineering & System Safety, Volume 229, 2023, 108834, DOI: 10.1016/j.ress.2022.108834.

[5] Lande D., Novikov O., Alekseichuk L. Application of Large Language Models for Assessing Parameters and Possible Scenarios of Cyberattacks on Information and Communication Systems // Theoretical and Applied Cyber Security. Vol. 6 No. 1 (2024). DOI: 10.20535/tacs.2664-29132024.1.315242

[6] Gleich D.F., 2015. PageRank beyond the web. *Siam REVIEW*, 57(3), pp. 321-363. DOI: 10.1137/140976649.

[7] Al-Eiadeh, M.R. and Abdallah, M., 2024, June. AARA-PR: Asset-Aware PageRank-Based Security Resource Allocation Method for Attack Graphs. *In 2024 4th Interdisciplinary Conference on Electrics and Computer* (INTCEC) (pp. 1-6). IEEE. DOI: 10.1109/INTCEC61833.2024.10603228.

[8] Wan, P., Yang, W.L., Luo, J.W. and Ma, X.F., 2025. Importance Analysis of Causative Nodes for Accident Chains of Railway Locomotive Operation Based on STPA-PageRank Method. *Promet-Traffic&Transportation*, 37(1), pp.137-150. DOI: 10.7307/ptt.v37i1.659.

[9] Aydin, M., Sezer, S.I., Akyuz, E. and Gardoni, P., 2025. Improved Z-number based Bayesian network modelling to predict cyber-attack risk for maritime autonomous surface ship (MASS). *Applied Soft Computing*, *180*, p.113416.