UDC 004.056: 004.89

Application of Large Language Models for Assessing Parameters and Possible Scenarios of Cyberattacks on Information and Communication Systems

D. Lande[1], O. Novikov[1], L. Alekseichuk[1]

[1] *National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute," Educational and Scientific Physical-Technical Institute*

Abstract. This paper explores the use of large language models (LLMs) to evaluate parameters and identify potential hostile penetration scenarios in corporate networks, considering logical and probabilistic relationships between network nodes. The developed methodology is based on analyzing the network structure, which includes components such as the Firewall, Mail Server, Web Server, administrator and client workstations, application server, and database server. The probabilities of transitions between these nodes during adversarial attacks are determined using a swarm of virtual experts and two sets of prompts aimed at different LLMs. Among the results obtained through the swarm approach are average transition probabilities, which enable modeling the most likely attack paths from both external and internal network origins. Based on logical-probabilistic analysis, penetration scenarios are ranked according to probabilities, execution time, and resource minimization required by attackers. The proposed methodology facilitates rapid response to threats and ensures an adequate level of cybersecurity by focusing on the most probable and dangerous attack scenarios.

Keywords: LLM, corporate network, penetration scenarios, cyberattack, transition probabilities, logical-probabilistic model, swarm of virtual experts, network protection, cybersecurity, attack modeling

Introduction

The issue of ensuring cybersecurity for critical infrastructure in sectors such as information and communication systems, energy, transportation, banking, finance, and others is both important and timely. Cybercriminals are particularly drawn to attacking Industrial Control Systems (ICS) and Supervisory Control and Data Acquisition (SCADA) systems within critical infrastructure objects. The goal of such attacks is to disrupt the operation of control systems, halt key technological processes, or cause operational failures at enterprises. The rise in cyberattack intensity is attributed to outdated cybersecurity systems, the increasing skills of cybercriminals, the significant expansion of the malware market, and other factors.

Scientific research and development play a crucial and effective role in ensuring the cybersecurity of critical infrastructure. One productive research direction involves threat modeling and risk analysis for critical infrastructure objects, a field that has been widely studied by scientists. The tasks of threat modeling, cybersecurity analysis, and other aspects of securing critical infrastructure have been addressed in works [1] - [4] and others.

One approach to addressing threat modeling and risk analysis tasks for critical infrastructure is the logic-probabilistic method, first proposed by British scientist George Boole [5]. A review of work on the development of the logic-probabilistic method is provided in [6], with specific applications and developments of the method discussed in [7–11] and other publications. Formally, the logic-probabilistic method involves creating a model of a dangerous state function using logic algebra operations (Boolean algebra) and then applying probability theory. The resulting model provides a calculation for the probabilistic risk of an undesirable event occurring in an object or a security system due to external influence. In particular, studies [9, 11] examined the cybersecurity of information

and communication systems (ICS) under cyberattack influence.

A crucial question in developing and applying logic-probabilistic models is the accurate determination of their coefficients. In theoretical work on logic-probabilistic modeling, this issue is often left unaddressed, with coefficients suggested by experts in practical examples. Therefore, developing formal methods or procedures for determining the coefficients of such models is relevant.

One promising approach for understanding and predicting potential intrusion scenarios is the use of Large Language Models (LLMs), which have proven their ability to process and analyze large volumes of information, establish logical connections, and estimate event probabilities.

Large language models like ChatGPT, GPT-4, and others are designed to deeply understand language, analyze context, and simulate logical reasoning [12]. Beyond their primary ability to generate text, LLMs can handle complex queries, assess probabilities, and make logical inferences, making them valuable for tasks that require scenario building or identifying potential pathways in complex systems. Using LLMs for cybersecurity, particularly to identify possible hostile penetration scenarios, is a novel approach that helps reduce risks and provides a new tool for analyzing and modeling cyber threats.

A key technique used in this study is employing LLMs to evaluate the likelihood of adversaries transitioning between network components. The network includes components such as firewalls, email and database servers, web servers, as well as administrator and client workstations. Here, the LLM analyzes possible transition paths between nodes. This study proposes two sequences of prompts that allow the model to form a set of the most probable scenarios, considering network structure and logic-probabilistic connections.

Additionally, the approach uses the so-called “swarm of virtual experts”—a series of identical queries to the LLM, conducted with different roles and focuses, enabling the model to propose diverse scenarios and take a broad range of potential penetration paths into account. The results from the two prompt chains are averaged to ensure maximum objectivity and accuracy in evaluations. Subsequently, the combined transitions between nodes with probability estimates are passed to the LLM, which then proposes the most likely attack chains, taking into account both external and potential internal threats, including those leveraging social engineering.

Expert evaluation methods can be used to assess transition probabilities in server networks when available data is limited, traffic in the real system cannot be accounted for, historical data is insufficient, or does not fully reflect all possible states and transitions in the network. This is also useful in complex systems with a large number of multi-level connections, where automated methods may be too complex, rare or novel events are considered without sufficient data for modeling, and when dealing with heterogeneous networks where node roles differ. Additionally, experts may better account for specific network characteristics that may be overlooked or misinterpreted by automated models, and when quick decisions are required without time for detailed data analysis, expert knowledge can be decisive. Expert assessment methods include expert surveys [13], the Delphi method [14], the analytic hierarchy process [15], Bayesian networks with expert data, and others.

This work focuses specifically on the expert survey method, which involves gathering assessments of transition probabilities from a group of experts based on their experience and knowledge. A key advantage of LLMs in cybersecurity is their ability to integrate the "swarm of virtual experts" concept, where the model, simulating the work of experts with different approaches [16], can generate a variety of answers to queries from multiple perspectives, including those of human experts. This not only reconciles varied penetration scenarios but also provides a reliable level of substantiation for recommendations, based on several different analytical viewpoints.

Objective of the Work: The objective of this study is to develop a methodology for using Large Language Models (LLMs) to assess parameters and potential scenarios of cyberattacks on an information and communication system. This methodology integrates with well-known logic-probabilistic approaches and is distinguished by a solid mathematical foundation, along with the use of statistically significant and consistent insights

from the most advanced artificial intelligence systems.

Logic-Probabilistic Model of Attack Scenario Success on ICS

Consider an information and communication system (ICS) that is under the influence of cyberattacks.

To describe the logical structure of an information and communication system (ICS), we use a directed graph $G(V,E)$, where $v_i \in V$ is the set of objects/information resources/services of the system, $E=(e_1,...,e_L)$, $e_k=(v_i,v_j)$ denotes the presence or absence of connections between them, represented as $E \subseteq V \times V$.

The description of a corporate network structure allows for detailed consideration of the connections between system elements and the specifics of their interactions. The network architecture is formed based on switching connections and corresponding network configurations that provide certain capabilities and restrictions in data exchange. When building the logical structure of an ICS, it is also necessary to consider possible information flows, which will allow for more accurate modeling of attack scenarios in the future.

In cases where multiple services are hosted on the same physical server and may function as separate objects — either as threat sources or potential targets in attack scenarios — they should be distinguished as separate components. The resulting network structure is represented as a graph, reflecting all possible paths and connections between objects. This graph is presented in the form of an adjacency matrix, also known as an accessibility matrix of objects, which allows the determination of connections between various nodes in the system.

Since the interaction between objects is often directed, meaning that connections can only be initiated from certain objects in one direction, the graph has a directed structure.

Let us consider a logical-probabilistic model of the success of an attack scenario on an ICS as shown in [10]:

$$J(A)=P(G,A,O,P), \qquad (1)$$

where $J(A)$ is the criterion for the probability of a successful attack scenario on the ICS, $G(V,E)$ is the known and fixed network topology, $V=\{v_1,...,v_N\}$ is the set of objects/resources/services in the ICS, $A=\{a_1,...,a_K\} \subset V$ is the set of threat sources, $O=\{o_1,...,o_M\} \subset V$ is the set of critical objects for attacks, and $P=\{P_1,...,P_N\}$ are the probabilities of ICS object capture.

The methodology for constructing such a criterion according to the logical-probabilistic theory of security is as follows:

1. We represent the attack model using a Boolean function (BF) as a conjunction of a sequence of events Z_i, none of which can be removed without violating the corresponding scenario:

$$\varphi_l = \bigwedge_{i \in K_{\varphi_l}} Z_{i,} \qquad (2)$$

where K_{φ_l} represents the sequence of actions by an attacker in the ICS that leads to a dangerous state of a specified system object, which corresponds to the l-th attack scenario.

2. We represent the considered ICS as a function of dangerous states (FDS) — a finite set of attack scenarios (l =1, 2, …, d), and events Z_i (where $i \in K_{\phi_l}$):

$$y(Z_1,...,Z_m)=\bigvee_{i \in K_{\varphi_l}}^{d} \varphi_i = \bigvee_{i \in K_{\varphi_l}}^{d} \left[\bigwedge_{i \in K_{\varphi_l}} Z_{i,} \right]. \qquad (3)$$

3. We express the probability of the ICS transitioning to a dangerous state according to the logical-probabilistic theory as:

$$P\{y(Z_1,...,Z_m)\} = P\left\{ \bigvee_{i \in K_{\varphi_l}}^{d} \left[\bigwedge_{i \in K_{\varphi_l}} Z_{i,} \right] \right\}. \qquad (4)$$

4. We perform direct substitution of the Boolean variables Z_i with their probabilistic values $P\{Z_i=1\}=P_i$ (relation (4)). We then preliminarily transform the FDS (3) into one of its equivalent forms: orthogonal disjunctive normal form, perfect disjunctive normal form, or a non-repetitive function in the conjunction-negation basis.

Based on this methodology, we obtain a logical-probabilistic criterion for the probability of a successful attack scenario on an ICS in the form of (1).

Evaluation of Cyber Attack Parameters on ICS

Considering (1)-(4), we propose using generative artificial intelligence models for

assessing the parameters of the corporate network. The so-called "virtual experts" [17] provide responses to specific queries aimed at analyzing network connections and node characteristics. Based on the answers obtained from the "virtual experts," transition probabilities between nodes are evaluated according to the network structure.

The task is to determine transition probabilities between nodes, where nodes represent different servers in a corporate system, based on expert assessments. These probabilities depend on the type of nodes and the direction of connections, and they are determined using two strategies for querying virtual experts, with subsequent averaging of the results.

The next stage involves forming and examining possible attacker scenarios within the network. Based on the transition probabilities provided by the virtual experts, the most probable chains of potential attacks — both external and internal — are identified. These scenarios are then ranked according to several criteria, including likelihood of implementation, time costs, and minimal resources required by an attacker. These rankings help identify the most critical threats, which are then provided to security personnel for proactive response to potential attacks.

The first strategy, which we'll call the Output algorithm, involves assessing the transition probabilities originating from each network node. This strategy iterates through all nodes and determines transition probabilities along all existing outgoing connections. This approach enables the estimation of the likelihood that an attacker may move from one node to another based on their outgoing connections, providing a comprehensive view of potential movement directions.

The opposite strategy, termed the Input algorithm, focuses on the probabilities of entering each network node. For each node, the probabilities that an attacker could reach it via available incoming connections are assessed. This approach examines the network from the perspective of possible penetration vectors, analyzing the likelihood of reaching a particular node from other connected points.

To evaluate the accuracy and alignment of both approaches in relation to the overall network structure, a measure of mutual proximity between the connection matrices (Output and Input) is computed using the Frobenius norm. It is shown that this proximity measure is smaller compared to that of a random matrix or adjacency matrix, indicating the consistency of both approaches' results.

After calculating all probabilities for each approach, two matrices are generated, and their values are averaged to obtain an overall expert assessment of transition probabilities in the network. The averaged matrix reflects a consolidated picture, representing the agreement between the Output and Input algorithm assessments. It also demonstrates the smallest proximity to the adjacency matrix compared to the corresponding measures for the individual Output and Input matrices, confirming its high accuracy and consistency.

Below, we present the formalization of the approaches used in the Output and Input algorithms for estimating the probabilities of attacker transitions between nodes in the corporate network.

Output Algorithm

The Output Algorithm is based on assessing the probabilities of transitions from nodes to their outgoing connections. Let $P(v_i \to v_j)$ be the probability of transition from node v_i to node v_j, where $E(v_i, v_j) \in E$.

1. For each node $v_i \in V$, we query the LLM to obtain transition probabilities $P(v_i \to v_j)$ for all $v_j \in V$.

2. We form the transition probability matrix P_{out} of size $n \times n$:

$$P_{out} = \begin{bmatrix} P(v_1 \to v_1) & P(v_1 \to v_2) \ldots P(v_1 \to v_n) \\ P(v_2 \to v_1) & P(v_2 \to v_2) \ldots P(v_2 \to v_n) \\ & \cdot \\ & \cdot \\ & \cdot \\ P(v_n \to v_1) & P(v_n \to v_2) \ldots P(v_n \to v_n) \end{bmatrix}. \quad (5)$$

Input Algorithm

The Input Algorithm focuses on assessing the probabilities of transitions to nodes through their incoming connections. Let

$P(v_j \leftarrow v_i)$ be the probability of transition to node iii from node v_j.

1. For each node $v_j \in V$, we query the LLM to obtain transition probabilities $P(v_j \leftarrow v_i)$ from all nodes $v_i \in V$.
2. We form the transition probability matrix P_{in} of size $n \times n$:

$$P_{in} = \begin{bmatrix} P(v_1 \leftarrow v_1) & P(v_2 \leftarrow v_1) \ldots P(v_n \leftarrow v_1) \\ P(v_1 \leftarrow v_2) & P(v_2 \leftarrow v_2) \ldots P(v_n \leftarrow v_2) \\ & \cdot \\ & \cdot \\ & \cdot \\ P(v_1 \leftarrow v_n) & P(v_2 \leftarrow v_n) \ldots P(v_n \leftarrow v_n) \end{bmatrix}. \quad (6)$$

Note that matrices (5) and (6) essentially coincide; the difference in notation is defined only by the different approaches to determining the values of their elements.

Mutual Closeness Measure

To evaluate the mutual closeness of matrices P_{out} and P_{in}, which are obtained by inputting respective prompts into LLM systems, we use the Frobenius norm, which is defined as:

$$\left\| P_{out} - P_{in} \right\|_F = \sqrt{\sum_{i=1}^{n} \sum_{j=1}^{n} \left(P_{out}(i,j) - P_{in}(i,j) \right)^2}. \quad (7)$$

Averaged Probability Matrix

After obtaining probability estimates using both algorithms, we average the values to obtain the overall expert assessment result:

$$P_{avg}\left(v_i \rightarrow v_j\right) = \frac{P_{out}\left(v_i \rightarrow v_j\right) + P_{in}\left(v_j \leftarrow v_i\right)}{2}. \quad (8)$$

The resulting matrix P_{avg} can be used for further analysis of destructive attack scenarios.

Example of Practical Use of the Parameter Evaluation Methodology

Consider the ICS presented in [10] with nodes: Firewall - S1, Mail Server - S2, Web Server - S3, AWP Administrator – S4, AWP Clients - S5, Application Server - S6, DB Server – S7 (Figure 1).

The network nodes are connected by directed links, represented by an adjacency matrix, whose elements can be 0 or 1 (Table 1).

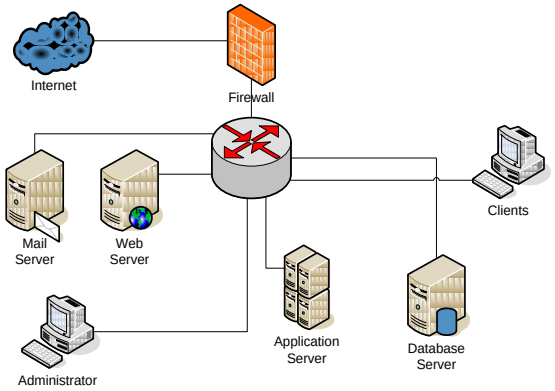

Figure 1 – Physical Structure of ICS

Table 1. Communication Matrix (Links)

	S1	S2	S3	S4	S5	S6	S7
Firewall (S1)	0	1	1	0	0	0	0
Mail Server (S2)	1	0	0	0	0	0	1
Web Server (S3)	1	0	0	0	0	0	1
AWP Administrator (S4)	1	1	1	0	1	1	1
AWP Clients (S5)	0	0	0	0	0	1	0
Application Server (S6)	0	0	0	0	1	0	1
DB Server (S7)	0	0	0	0	0	1	0

When applying the "swarm of virtual experts" methodology, requests are made to generative artificial intelligence services such as ChatGPT (https://chat.openai.com/), Gemini (https://gemini.google.com/), Groq (https://groq.com/), and the Llama-3 model.

Subsequently, these systems are provided with multiple queries (prompts) to assess the values of system parameters, which are then aggregated by averaging.

Parameter assessment based on the Output algorithm: Sequentially, for all nodes in the network from which connections originate, queries are executed. The results of these queries provide probability estimates for successful transitions between nodes during a cyberattack. Below is an example of these queries, specifically transitions from a node 1 (p12=P(S1→S2), p13=P(S1→S3)):

Prompt: *Suppose there has been a breach into the corporate network through the firewall, and the attackers aim to reach the database server. Quantitatively estimate the conditional probabilities that they have passed from the firewall to the mail server – p12, and to the web server – p13. Provide expert numerical values for the conditional probabilities p12 and p13.*

The queries for transitions between nodes are formed in a similar way:
2 (p21=P(S2→S1), p27=P(S2→S7));
4 (p47=P(S4→S7), p41=P(S4→S1), p42=P(S4→S2), p43=P(S4→S3), p46=P(S4→S6), p45=P(S4→S5));
5 (p31=P(S3→S1), p37=P(S3→S7));
6 (p65=P(S6→S5), p67=P(S6→S7)).

Thus, as a result of executing the prompts from the artificial intelligence systems, the probabilistic parameters were obtained (Table 2):

Table 2. Output Matrix

	S1	S2	S3	S4	S5	S6	S7
Firewall (S1)	0	0.4	0.5	0	0	0	0
Mail Server (S2)	0.28	0	0	0	0	0	0.78
Web Server (S3)	0.27	0	0	0	0	0	0.75
AWP Administrator (S4)	0.55	0.55	0.55	0	0.55	0.225	0.65
AWP Clients (S5)	0	0	0	0	0	1	0
Application Server (S6)	0	0	0	0	0.29	0	0.66
DB Server (S7)	0	0	0	0	0	1	0

Parameter estimation based on the Input algorithms

For all network nodes that include connections, queries are sequentially executed, and the results of these queries are averaged. Let's provide an example of these queries, namely, transitions to node 1 (p21=P(S2→S1), p31=P(S3→S1), p41=P(S4→S1)):

Prompt: *Suppose there has been a breach in the corporate network, and the attackers are attempting to reach the database server. It is known that there is an inquiry to the firewall from an internal segment. Quantitatively assess the conditional probability that the request to the firewall is coming from the mail server (p21), the web server (p31), or the administrator's server (p41). Provide expert numerical values for the conditional probabilities p21, p31, and p41.*

Similarly, requests for transitions to nodes are formed as follows:
2 ((p12=P(S1→S2), p42=P(S4→S2));
3 (p13=P(S1→S3), p43=P(S4→S3));
5 (p45=P(S4→S5), p65=P(S6→S5));
6 ((p46=P(S4→S6), p56=P(S5→S6), p76=P(S7→S6));
7 (p27=P(S2→S7),p37=P(S3→S7), p47=P(S4→S7), p67=P(S6→S7)).

As a result of executing the prompts from the artificial intelligence systems, the parameters of the network have been obtained, corresponding to the Input matrix (Table 3):

Table 3. Input Matrix

	S1	S2	S3	S4	S5	S6	S7
Firewall (S1)	0	0.34	0.3	0	0	0	0
Mail Server (S2)	0.28	0	0	0	0	0	0.25
Web Server (S3)	0.38	0	0	0	0	0	0.3
AWP Administrator (S4)	0.4	0.36	0.35	0	0.44	0.35	0.65
AWP Clients (S5)	0	0	0	0	0	0.4	0
Application Server (S6)	0	0	0	0	0.59	0	0.5
DB Server (S7)	0	0	0	0	0	0.38	0

The evaluation of the proximity measure allows us to see how correlated the obtained matrices are with each other, and how much they differ from a random matrix and a communication matrix.
To perform the calculations, the obtained matrices are normalized (their values will range from 0 to 1) by dividing all elements by the largest value. In this case, the Frobenius norm $\| \cdot \|_F$ is applied.

The calculation results are presented in the table (Table 4). Clearly, the smaller the Frobenius norm, the more similar the corresponding matrices are.

The data in the table indicate a high correlation between the obtained Output and Input matrices, as well as the possibility of using their mean values, which produce results most strongly correlated with the original communication matrix.

Definition and Ranking of Destructive Attack Scenarios

After obtaining the transition probability matrix for the attackers' movements between nodes in the corporate network during successful breaches, the next step is to form

and rank potential destructive attack scenarios. This process involves identifying potential paths that attackers may follow, as well as assessing the likelihood of each scenario's realization. To achieve this, the capabilities of large language models (LLMs) are utilized in combination with the "swarm of virtual experts" method.

Table 4. Matrix difference

Matrix 1	Matrix 2	Matrix difference
Output	Input	0,167
Output	Links	0,248
Intput	Links	0,286
$\frac{Output + Input}{2}$	Links	0,211
Output	Random	0,407
Input	Random	0,520

Definition of Attack Scenarios

Based on the transition probability matrix, which reflects possible intruder movements between nodes, LLM models generate various action scenarios. Each scenario represents a sequence of transitions leading to a specific node or goal within the corporate network. When forming these scenarios, it is essential to consider all possible combinations of transitions, including both external attacks and internal threats, particularly those involving social engineering.

A destructive attack scenario represents a sequence of transitions between network nodes that can be initiated by an attacker. Let S be the set of possible scenarios, where each scenario s_k is a sequence of transitions between nodes.

Let $s_k = \left(v_{k_1}, v_{k_2}, ..., v_{k_m}\right)$, where m is the number of nodes in the scenario, and $v_{k_j} \in V$ represents the nodes of the network.

For each scenario s_k, the probability of realization is calculated as the product of the transition probabilities between adjacent nodes in the given scenario:

$$P(s_k) = \prod_{j=1}^{m-1} P_{avg}\left(v_{k_j} \to v_{k_{j+1}}\right), \quad (9)$$

where $P_{avg}\left(v_{k_j} \to v_{k_{j+1}}\right)$ is the probability of transitioning from node v_{k_j} to node $v_{k_{j+1}}$, determined as the average value from the transition probability matrices.

To implement this process, a prompt is proposed for the above LLM models to help generate destructive attack scenarios.

Prompt: *Generate all possible attack scenarios targeting the DB Server (S7) using the transition probability matrix. Include information on the initial node, the sequence of transitions between nodes, and the final target of the attack. Unspecified elements of the matrix are considered to be zero. We have the following transition probabilities:*
«Firewall (S1); Mail Server (S2): 0.37»
«Firewall (S1); Web Server (S3): 0.4»
«Mail Server (S2); Firewall (S1): 0.28»
«Mail Server (S2); DB Server (S7): 0.57»
«Web Server (S3); Firewall (S1): 0.33»
«Web Server (S3); DB Server (S7): 0.57»
«AWP Administrator (S4); Firewall (S1): 0.48»
«AWP Administrator (S4); Mail Server (S2): 0.46»
«AWP Administrator (S4); Mail Server (S2): 0.45»
«AWP Administrator (S4); AWP Clients (S5): 0.5»
«AWP Administrator (S4); Application Server (S6): 0.28»
«AWP Administrator (S4); DB Server (S7): 0.65»
«AWP Clients (S5); Application Server (S6): 0.7»
«Application Server (S6); AWP Clients (S5): 0.44»
«Application Server (S6); DB Server (S7): 0.58»
«DB Server (S7); AWP Clients (S5): 0.7»

After this, the probabilities of success for cyberattacks corresponding to individual scenario chains are evaluated by multiplying the conditional transition probabilities according to formula (9). As a result, different LLM systems provide identical responses, which are aggregated in Table 6.

Table 6. Scenarios, Probabilities, and Probabilistic Risks

Path	Success Probability	Risk
S1 → S2 → S7	0.21	Medium
S1 → S3 → S7	0.23	Medium
S2 → S7	0.57	High
S3 → S7	0.57	High
S4 → S7	0.65	Critica
S4 → S2 → S7	0.26	Medium
S4 → S5 → S6 → S7	0.20	Medium
S4 → S6 → S7	0.16	Low
S5 → S6 → S7	0.41	High

Ranking of Attack Scenarios

After generating attack scenarios, they can be ranked according to several criteria to identify the most probable and dangerous

attack options. Ranking can be carried out based on parameters such as:

1. Probability of success, where scenarios with higher probabilities of transitions between nodes are ranked higher.
2. Execution time, where scenarios that can be executed faster should be prioritized as they may lead to more urgent threats.
3. Minimal costs – scenarios that require fewer resources from attackers should also be highly rated, as they may be more attractive for attack.

The ranking process can also involve a swarm of virtual experts, who, based on different models and criteria, evaluate and provide their conclusions regarding each scenario. This can be achieved by querying various LLM systems, with an example prompt provided below.

***Prompt**: Evaluate all generated attack scenarios based on three criteria: probability of success, execution time, and minimal costs. Formulate a ranking of scenarios based on these parameters.*

Aggregated values obtained from large language models are shown in Table 7.

Table 7. Scenarios rated according to the specified features

Number	Path	Time	Costs	Score
1	S1 → S2 → S7	2	Low	2.07
2	S1 → S3 → S7	2	Low	2.11
3	S2 → S7	1	Very low	2.86
4	S3 → S7	1	Very low	2.86
5	S4 → S7	1	Very low	3.0
6	S4 → S2 → S7	2	Low	2.18
7	S4 → S5 → S6 → S7	3	Medium	1.77
8	S4 → S6 → S7	2	Low	1.86
9	S5 → S6 → S7	2	Low	2.27

For a final conclusion based on the data from Table 7, a query can be directed to LLM systems as follow:

***Prompt**: Based on the rated scenarios, provide conclusions on the most critical threats to the corporate network. What recommendations can be made to improve security?*

Based on the data in Table 7 regarding ICS, virtual experts would provide an answer approximately like this:

"The scenarios with S4, S2, and S3 to S7 show that the DB Server is vulnerable to attacks, where an attacker can infiltrate through bypass nodes such as the Mail Server, Web Server, and AWP Administrator. The most critical scenario is S4 → S7, with a high probability of success (65%), highlighting the need to protect against internal and external threats through the AWP Administrator. Scenarios including S2 → S7 and S3 → S7 also have high potential due to low costs and short execution times. AWP Administrator (S4) is one of the most vulnerable starting nodes, as it provides direct access to several critical nodes, including the DB Server. This node is vulnerable both to attacks via other systems and to direct access to the DB Server."

Once the scenario formulation and ranking phase is complete, the results are passed to network security specialists for final decision-making. This allows for measures to be taken to prevent potential attacks, thereby improving the overall security level of the corporate information system.

Conclusions

This article presents a methodology for assessing the probabilities of attacker transitions between nodes in information and communication systems (ICS) and for identifying and ranking potential cyberattack scenarios, illustrated with a practical example. The primary focus of this work is the development of a systematic approach applicable to various networks, regardless of their specific characteristics or architectures.

The use of large language models (LLMs) in risk assessment allows for the generation of well-reasoned results, facilitating the creation of detailed attack scenarios. Integrating LLMs into threat assessment processes opens up new opportunities for automating the detection of network vulnerabilities.

The proposed methodology also enables the ranking of attack scenarios based on criteria such as probability of success, execution time, and resource minimization, allowing organizations to prioritize the most dangerous threats and respond to them promptly, thereby enhancing overall security.

This methodology not only contributes to improved ICS security but can also be adapted

for use in various contexts, making it a versatile tool in the field of cybersecurity. The results of this work include not only theoretical advancements but also practical recommendations that can be implemented in real corporate networks to enhance their security and resilience against cyber threats.

References

[1] Dinesh Kumar Saini. *Cyber Defense: Mathematical Modeling and Simulation.* International Journal of Applied Physics and Mathematics, Vol. 2, Iss. 5, September 2012, p. 312-315.
DOI: 10.7763/IJAPM.2012.V2.121.

[2] Juan Fernando Balarezo, Song Wang, Karina Gomez Chavez, Akram Al-Hourani, Sithamparanathan Kandeepan. *A survey on DoS/DDoS attacks mathematical modelling for traditional, SDN and virtual networks.* Engineering Science and Technology, an International Journal, Vol. 31, July 2022, 15 p.
DOI: 10.1016/j.jestch.2021.09.011

[3] Saeed Ahmadian, Xiao Tang, Heidar A. Malki, Zhu Han. *Modelling Cyber Attacks on Electricity Market Using Mathematical Programming With Equilibrium Constraints*. IEEE Access, vol. 7, 2019. DOI:10.1109/ACCESS.2019.2899293

[4] Rajaa Vikhram Yohanandhan, Rajvikram Madurai Elavarasan, Premkumar Manoharan, Lucian Mihet-Popa. *Cyber-Physical Power System (CPPS): A Review on Modeling, Simulation, and Analysis With Cyber Security Applications*. IEEE Access, vol. 8, 2020. DOI:10.1109/ACCESS.2020.3016826

[5] Boole George. An investigation of the laws of thought, on which founded the mathematical theories of logic and probabilities. London, 1854. 343p.
https://www.gutenberg.org/ebooks/15114

[6] Lorenz Demey, Barteld Kooi. Logic and Probability, First published Thu Mar 7, 2013; substantive revision Thu Aug 17, 2023. Stanford Encyclopedia of Philosophy.
https://plato.stanford.edu/entries/logic-probability/

[7] Balan A.O. *An enhanced approach to network reliability using Boolean algebra*. An honors thesis presented to the departments of computer science and mathematics of Lafayette College on May 16 2003. Pp. 1-43.
https://www.semanticscholar.org/paper/An-Enhanced-Approach-To-Network-Reliability-Using-Balan/e35fcaa892503d42e2c4139f676b5cb31ec2234a

[8] Anrig B., Beichelt F. *Disjoint sum forms in reliability theory* // ORiON. 2001. Vol. 16. No. 1. Pp. 75–86.
DOI:10.5784/16-1-413

[9] 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

[10] L. Alekseichuk, O. Novikov, A. Rodionov, D. Yakobchuk. *The Best Scenario of Cyber Attack Selecting on the Information and Communication System Based on the Logical and Probabilistic Method*. Theoretical And Applied Cybersecurity - Vol.5 No. 2, 2023, c. 81-88.
DOI:10.20535/tacs.2664-29132023.2.288973.

[11] Ланде Д.В., Новіков О.М., Алексейчук Л.Б. *Визначення коефіцієнтів логіко-ймовірнісних моделей кібербезпеки з використанням віртуальних експертів*. Theoretical and Applied Cybersecurity. Матеріали другої всеукраїнської науково-практичної конференції (TACS-2024). - Київ: Інжиніринг, 2024. - С. 11-20.ISBN 978-966-2344-98-1.
http://is.ipt.kpi.ua/is/TACS-2024/

[12] Dmytro Lande, Leonard Strashnoy. *GPT Semantic Networking: A Dream of the Semantic Web - The Time is Now*. - Kyiv: Engineering, 2023. - 168 p. ISBN 978-966-2344-94-3.

[13] 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

[14] 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,
DOI:10.1111/rssa.12691

[15] 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.

[16] Strashnoy Leonard, Lande Dmytro. Implementation of the concept of a "swarm of virtual experts" in the formation of semantic networks in the field of cybersecurity based on large language models (October 03, 2024). SSRN Preprint.
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4978924.

[17] Dmytro Lande, Leonard Strashnoy. Swarm of Virtual Experts in the Implementation of Semantic Networking. ResearchGate Preprint, 2024.
DOI:10.13140/RG.2.2.16686.11845