UDC 004.89

Methodology of a Swarm of Virtual Experts for Evaluating the Weight of Connections in Networks

Dmytro Lande[1], Lesya Alekseichuk[1], Igor Svoboda[1], Leonard Strashnoy[2]

[1] *National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute, " Educational and Scientific Physical-Technical Institute*
[2]*University of California, Los Angeles (UCLA)*

Abstract. This article proposes a new methodology — the Swarm of Virtual Experts (SVE) — for evaluating the weights of connections in complex networks, based on a holistic approach. Traditional methods relying on expert assessments often face issues of subjectivity and limited resources. This paper introduces the methodology of the Swarm of Virtual Experts. The focus is on integrating large language models (LLMs) into the decision-making process, where each model acts as a virtual expert with specific tasks and functions. The core idea is to combine diverse assessments from different LLMs using mathematical tools, including incidence matrices, weighted averages, and aggregation methods. The methodology addresses the issue of fragmented results caused by the probabilistic nature of LLMs and enhances analytical efficiency through role assignment to agents, aggregation mechanisms, and quality evaluation of outcomes. The application of this technique is illustrated with examples, particularly in the field of cybersecurity. Special attention is given to holistic analysis, which provides a comprehensive approach to evaluating the weights of connections between nodes in networks.

Keywords: Swarm of Virtual Experts, large language models, connection weights, incidence networks, cybersecurity, mathematical modeling, aggregation of assessments

---

Introduction

The modern world is characterized by unprecedented complexity in the interconnections that form multi-level networks in various fields such as cybersecurity, risk management, social networks, and others. These connections may represent dependencies between threats and vulnerabilities, elements of corporate systems, or other network components. Traditionally, expert assessments are used for this purpose, but such methods often suffer from subjectivity, limited number of experts, and the complexity of integrating diverse knowledge. Analyzing the weight of connections between nodes in these networks is a key task that allows for identifying hidden dependencies, predicting events, and making strategically important decisions.

At the same time, traditional approaches to network analysis often face challenges, such as limited computational resources, failure to account for the probabilistic nature of modern data, and the inability to adapt to environmental changes.

Against this backdrop, an important task is the development of methods that account for the probabilistic nature of data, utilize modern tools such as large language models (LLM) [1], and are oriented towards achieving clearly defined goals.

A key role in the expert evaluation process today is played by the virtual expert — an image that LLM presents in response to each user query. Each query can be considered as the opinion of a virtual expert, who can evaluate the connections between these network nodes. Virtual experts operate based on knowledge embedded in the model and the texts or documents provided by the user, transforming the LLM into a unique linguistic processor capable of analyzing, classifying, and expanding semantic networks. However, within the scope of the discussed problem, numerical assessments of value are of particular interest.

Modern large language models, such as ChatGPT (GPT-4), Groq (Llama-3), and DeepSeek (o1), facilitate the formation of virtual experts [2] capable of generating evaluations of connections between network nodes. However, individual responses from LLMs may be incomplete or subjective.

A breakthrough in decision-making theory is achieved through the swarm of virtual experts (SVE) [3] — a collection of responses to queries made at different times, on different LLM models, and using diverse approaches to query formulation. The swarm integrates diverse and varied perspectives, adding layers of accuracy and completeness to the semantic network. This swarm generates a set of network parameter evaluations that can be filtered, aggregated, and ranked by a human, enhancing the reliability and comprehensiveness of the knowledge obtained. Each query, and each "expert" in the swarm, represents a fragment of collective knowledge, which, like drops in the ocean, combines to achieve a common goal: constructing a more precise and comprehensive understanding of the studied domain.

The term "swarm" in this context refers to a collective of numerous virtual agents (experts) interacting simultaneously with the AI system (specifically large language models) to obtain the most accurate and balanced evaluations. Each prompt, formulated as a query to an LLM, acts as an individual "virtual expert," contributing to the overall result.

The SVE can be compared to various phenomena and models:

1. Natural Swarms. Just like in ant colonies or flocks of birds, agents in a swarm of virtual experts interact, exchange information, and cooperate to achieve a common goal. Interaction and adaptability are the key characteristics of these systems.
2. Brainstorming. A swarm of experts operates like a group of people during a discussion. Different ideas are evaluated, refined, and aggregated to achieve the best outcome.
3. Genetic Algorithms. The process of SVE resembles evolution in genetic algorithms. Generating a set of solutions, selecting the best ones, mutating (changing the context), and repeating the cycle.

The main purpose of this article is to develop and substantiate the methodology of a swarm of virtual experts for evaluating the weights of connections in networks, aimed at achieving specific goals. The goal-oriented approach involves defining the primary objectives of the analysis, formulating intermediate goals, and developing tools to achieve them.

A distinctive feature of using a swarm of virtual experts is that this process is supervised by a human who coordinates queries to the system, formulates prompts, and integrates the responses received from various agents. This allows for maintaining a certain level of control over the process, avoiding systemic errors that may arise due to the lack of oversight, and addressing a number of tasks, such as improving the accuracy and completeness of the analysis, automating the processing of large volumes of data, and harmonizing disparate results.

The principle of operation of the swarm of virtual experts is that each virtual expert receives a query (prompt) in the form of specific instructions containing information about threats, vulnerabilities, or other system parameters. Once several experts provide their evaluations, these evaluations are aggregated. Aggregation can be performed using weighted averages or more complex methods, such as probabilistic fusion techniques. Although each expert operates autonomously, the human role in this process involves supervising the formulation of queries, correcting responses, and evaluating the consistency of the obtained results. Humans can adjust the prompts or introduce additional clarifications as needed.

The use of a swarm of virtual experts for evaluating the weights of connections in networks has several advantages, such as considering a multiplicity of viewpoints, ensuring the accuracy of evaluations, offering flexibility and adaptability, and reducing the impact of the human factor. Automating the process of assessing threats and vulnerabilities reduces the likelihood of errors associated with the human factor. At the same time, the human role remains crucial for ensuring the correctness of the results.

Methodology

The main principles of the swarm of virtual experts

A swarm of virtual agents is a hierarchical structure where each agent essentially represents a query to a large language model, performing tasks according to a defined role. The main principles of swarm construction are goal orientation, collaboration, and the ability to assume different roles. Accordingly, each agent is assigned a clearly defined goal, agents interact with each other to achieve the overall objective, and agents perform different functions that complement one another.

Large language models, such as GPT, are capable of generating different responses to the same queries depending on the session and the roles of the agents. The responses depend on the model's probabilistic factors, such as sampling from a probability distribution. Assigning different tasks to each model, such as analyst, critic, or moderator, influences the context in which the response is formed.

This probabilistic nature creates conditions for collective work, where a set of agents with diverse characteristics complements one another.

The scheme of the swarm of virtual experts

Figure 1 shows a diagram illustrating the interaction between agents, roles, the client, and the LLM within the swarm of virtual experts. The following processes are implemented:

1. The client sends the input query q_k to the swarm of agents.
2. Each agent receives the query and generates a response based on its role.
3. The agents exchange their responses through interaction.
4. The client coordinates and aggregates the responses from different LLMs.
5. The result aligns with the objectives.

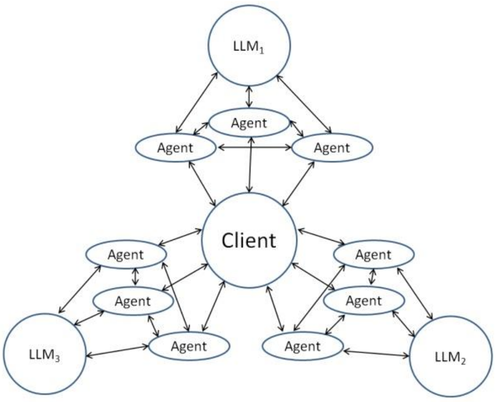

Figure 1. The diagram of the swarm of virtual experts

Additionally, the swarm is also formed thanks to the connection between agents and the client (human) who coordinates the process. The main aspects of the connection are the exchange of information between agents, the common client context, and the aggregation of results by the human. One agent can consider the response of another in order to refine its own result. The agents work towards a common goal set by the client, but they perform different roles. The results of each agent are analyzed and merged at the client level to form a single decision.

Mathematically, this can be formalized as a set of interconnected agents: $A=\{a_1,a_2,\ldots,a_n\}$, where a_i — is the agent, and each of its responses r_{ik} is a function not only of the query q_k, but also of the results of other agents $R_{-i,k}$:

$$r_{ik} = f\left(a_i, q_k, R_{-i,k}\right).$$

Assigning roles to agents

A key element of the SVE is the assignment of roles to agents, each of which corresponds to a specific function in the system. The main roles may include, for example:

- **Analyzer (r_{an})**,who formulates the main alternatives and analyzes possible scenarios.
- **Optimizer (r_{opt})**, who determines the best solutions.
- **Critic (r_{opt})**, who checks the consistency and reliability of the data.
- **Moderator (r_{mod})**, who aggregates and summarizes the results.

The multi-role approach enables multi-channel data analysis, providing a deeper understanding of the query.

Assigning roles not only allows the functions to be distributed among agents but also adapts the swarm to the specific needs of a given study.

Using different LLMs

One of the advantages of SVE is the ability to use multiple LLMs, which creates additional diversity in responses. As a result, the outputs of one model can be adjusted based on the results of another, ensuring coverage of a broader range of possible answers.

The client acts as the central link, synchronizing identical queries between different LLMs and aggregating their results.їхні результати:

$$R_k = \bigcup_{m=1}^{M} R_{m,k},$$

where M is the number of models, and $R_{m,k}$ is the model's m response to the query k.

Formulating queries and receiving responses

Each query to the swarm (q_k) has a clear structure that takes into account the set goal. Based on the query, the agents generate a set of responses:

$$R_{i,k} = \left\{ r_{i,k}^{1}, r_{i,k}^{2}, \ldots, r_{i,k}^{p_{i,k}} \right\},$$

where $p_{i,k}$ is the number of response variants provided by agent a_i.

Aggregation of results

The responses obtained from all agents are processed through an aggregation function f_{agg}, which takes into account the quality of the response (based on a metric), the weight of the agent according to its role, and the consensus among the agents.

Focus on the goal

The main task of SVE is to achieve a specific goal. Each agent acts with a goal-oriented approach, which includes forming sub-goals for individual roles, determining intermediate results, and aligning all results with the global objective.

The goal serves as the key reference point that sets the direction of work for all agents in the swarm.

Mathematical model of a swarm of virtual experts

The assessment of the weight of connections

To evaluate the weight of connections in a network, the following function is used:

$$w_{ij} = \sum_{k} \delta_{ij,k} \cdot eval(R_k),$$

where:

- $\delta_{ij,k}$ is an indicator that accounts for the presence of the connection e_{ij} in the responses.
- $eval(R_k)$ is the function for evaluating the quality of the responses.

Aggregation of results

To reconcile the results, the agents' responses are aggregated using: $\hat{w}_{ij} = f_{agg}(R_k)$, where f_{agg} is the aggregation function that considers the weights of the agents and the quality ratings of their responses.

To efficiently aggregate responses from different LLMs within the "swarm of virtual experts" concept, a weighted average method can be organized by considering the number of tokens in each LLM. This parameter can be used to assign higher weight to those models. Additionally, the relevance of the responses to test queries, previous test results, or expert evaluations can be considered. Newer releases of LLMs should have more up-to-date knowledge, consider current technologies and methods, and feature improved architecture.

After determining the weight values for each model (e.g., $w_1, w_2, \ldots, w_n$), where w_i is the weight of the corresponding LLM), the average response can be calculated considering the contribution of each model. If each model gives a weight score for the connection as a_i, then the weighted average response A is computed as:

$$A = \frac{\sum_{i=1}^{n} w_i \cdot a_i}{\sum_{i=1}^{n} w_i}.$$

Thus, responses from models with higher weights will have a greater impact on the final result, increasing accuracy and reducing errors.

Quality assessment of the results

The swarm of virtual experts generates numerical assessments based on the specified factors. In the node incidence table, each cell reflects the weight of the connection between nodes. Using the "average" method, the swarm's assessments for each table cell can be aggregated. The average assessment for each pair of connections between nodes is determined as the mean value of all virtual experts' assessments:

$$\hat{m}_{ij} = \frac{1}{K}\sum_{k=1}^{K} m_{ij}^{k}.$$

This average score provides a general understanding of the weight of the connection between nodes based on the swarm's evaluations.

Since assessments for each pair of nodes are generated by different virtual experts, it is important to assess the accuracy of the average scores. An accuracy criterion can be introduced for each connection, allowing us to determine how precise the average scores are.

To do this, we introduce an accuracy function that determines the difference between the average score and the actual score given by human experts (real experts):

$$\delta_{ij} = \left|\hat{m}_{ij} - \hat{m}_{ij}^{true}\right|,$$

where $\hat{m}_{ij}^{true}$ — the score received from real experts.

To evaluate the effectiveness of the swarm of virtual experts, criteria such as the mean squared error (MSE) can be used, which allows comparing the average scores with real data:

$$MSE = \frac{1}{N}\sum_{i=1}^{N}\sum_{j=1}^{M}\left(\hat{m}_{ij} - \hat{m}_{ij}^{true}\right)^{2},$$

where N and M — the number of threats and vulnerabilities, respectively.

Examples of applying the methodology

Analysis of relationships between threats and vulnerabilities

In modern research in the field of risk assessment for critical infrastructure objects, a methodological approach to evaluating the relationship between threats and vulnerabilities is crucial [4-5]. Traditionally, methods based on expert evaluations are used for these purposes; however, such approaches often face issues of subjectivity, a limited number of experts, and difficulties in integrating diverse knowledge.

The paper [6] presents information on the application of the swarm of virtual experts methodology to assess the relationship between threats and vulnerabilities of critical infrastructure objects, using large language models and their mathematical modeling to improve the accuracy and reliability of risk assessments in the field of cybersecurity.

To obtain assessments from virtual experts, implemented using ChatGPT (https://chatgpt.com/), Groq (https://groq.com/, Llama-3 model), DeepSeek (https://www.deepseek.com/), the following prompt was used:

We have: for a certain critical infrastructure object, the following list of elements that characterize vulnerabilities is formed: b_1 – vulnerability of input drivers for incoming information; b_2 – vulnerability of drivers for information processing tools; and so on.

The list of identified threats from cyberattacks on this object is provided below: u_1 – threat of loading malicious (virus) software using features of an alternative operating system with elevated privileges; u_2 – threat of unauthorized copying of information; and so on.

Create an incidence matrix, where rows represent (u) and columns represent (b).

The incidence matrix obtained in the example appears consistent and logical, but to ensure its correctness, each connection was verified for compliance with specific technical scenarios and conditions of the object. In the example presented in the paper, the human expert confirmed the logical coherence of the obtained assessments, taking into account several verification criteria, namely the logical consistency of the connections, the completeness of the matrix, redundancy of connections, and alignment with real security practices.

The estimation of transition probabilities between nodes in the corporate network

In the article [7], the application of the swarm of virtual experts methodology is discussed for forecasting the potential paths of an attack spread within a network. Parameters are assessed, and evaluations of possible scenarios of hostile penetration into corporate networks are determined, taking into account the logical-probabilistic connections between network nodes. The methodology presented in the work is based on the analysis of the network structure, which includes components such as Firewall, Mail Server, Web Server, administrator and client workstations, application server, and database server. The probabilities of possible transitions between these nodes during attacks by intruders are determined, evaluated using the swarm of virtual experts and two sequences of prompts targeting different LLMs. Among the results obtained from using the swarm, averaged transition probabilities are calculated, which allow modeling the most likely attack paths from both external and internal sources. Based on the logical-probabilistic analysis, penetration scenarios are ranked according to probabilities, execution time, and minimization of resources required by attackers.

The information corporate network is considered with the following nodes: Firewall - S1, Mail Server - S2, Web Server - S3, AWP Administrator – S4, AWP Clients - S5, Application Server - S6, DB Server – S7 (Fig. 2).

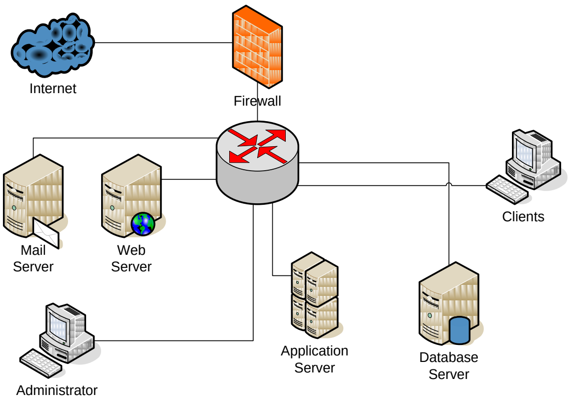

Figure 2. Physical Structure of the Corporate Network

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

Table 1. Communication Matrix

	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, queries are made to generative artificial intelligence services such as ChatGPT, Gemini, and Groq (Llama-3 model). Sequentially, for all network nodes that have outgoing connections, queries are executed, and the results provide the probability estimates of successful transitions between nodes during a cyberattack.

For example, the following queries concern transitions from node 1 (p12 = P(S1→S2), p13 = P(S1→S3)):

Prompt: *Suppose an intrusion occurred into the corporate network via a firewall, and the attackers aim to reach the database server. Quantitatively assess the conditional probability that they successfully moved from the firewall to the mail server—p12, and to the web server—p13. Provide expert numerical values for the conditional probabilities p12, p13.*

Similarly, queries are formed for transitions from nodes 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)), and 6 (p65 = P(S6→S5), p67 = P(S6→S7)).

After obtaining the results from executing the prompts and aggregating the results, a table of conditional transition probabilities is formed.

Having obtained the matrix of conditional probabilities for attackers' transitions between nodes of the corporate network in the case of successful intrusions, the next step is to form and rank the possible scenarios of destructive attacks. This process involves identifying potential paths that attackers may take, as well as assessing the probability of each scenario's realization.

Application in the Analytic Hierarchy Process

The Analytic Hierarchy Process (AHP) is a decision-making method developed by Thomas Saaty [8-9] that is used to select the optimal option among several alternatives based on multiple criteria. This method formalizes complex decision-making processes using a hierarchical structure. AHP is often applied to select the best supplier, investment project, or to assess risks across various industries.

Traditionally, AHP is implemented with the involvement of human experts. However, when using virtual experts, the generative capabilities of LLM systems can be utilized to define their roles. In this case, it is proposed to create role-based "experts" that evaluate various aspects of cybersecurity in the context of a specific decision. For example, this can be achieved using the following prompt [10]:

Prompt:
"Provide 5 expert roles from whose perspective cybersecurity issues can be considered."

Below is a sample response provided by the ChatGPT system:

- **Cybersecurity Analyst:** Assesses threats and vulnerabilities, helping to identify system weaknesses.
- **Ethical Hacker:** Identifies vulnerabilities in systems to improve their security.
- **Network Security Engineer:** Specializes in protecting networks by implementing firewalls and other security tools.
- **Compliance Officer:** Ensures adherence to legislative requirements and security standards.
- **CISO (Chief Information Security Officer):** Responsible for the overall cybersecurity strategy within an organization.

Criteria represent a separate level in the hierarchy being constructed. The procedure for determining the key criteria for ensuring cybersecurity can be implemented using the virtual expert methodology, taking into account various responses and identifying the most frequently occurring ones (the final list of criteria, of course, can be confirmed by a human expert).

Once the roles of the experts have been defined, specific queries can be directed to each of them to determine the criteria important for ensuring cybersecurity. This can be repeated multiple times, obtaining diverse responses from virtual experts. Below is an example of a prompt and a response generated by an LLM

Prompt:
"Identify the 5 main cybersecurity criteria from the perspective of a Cybersecurity Analyst."

ChatGPT response:

- **Threat Detection**: Network traffic monitoring and detection of malicious attacks.
- **Vulnerability Assessment**: Assessment of systems for vulnerabilities.
- **Incident Response**: Development and implementation of incident response plans.
- **Security Monitoring**: Continuous security monitoring and analysis.
- **Security Policy Compliance**: Verification of compliance with policies and security standards.

As a result, we obtain a list of criteria from all virtual experts, which allows for the creation of a hierarchical structure for further analysis.

By summarizing the responses obtained from all the aforementioned virtual experts, the criteria are derived:

Access control;

Incident response;

Security awareness;

Security policies;

Threat modeling;

Vulnerability assessment;

Encryption.

For each criterion, alternatives are formulated that can be proposed to achieve it. For example, for the "**ACCESS CONTROL**" criterion, we can send a query to the ChatGPT system:

Prompt:
"Name 2 primary alternative solutions for addressing cybersecurity ACCESS CONTROL criteria."

ChatGPT response:

Role-Based Access Control (RBAC): A model that provides access based on user roles.
Attribute-Based Access Control (ABAC): A

model that considers various attributes of users and resources for flexible access management.

This process is repeated for each criterion, allowing for the creation of a complete list of alternatives for all aspects of cybersecurity.

Based on the obtained alternatives and criteria (Fig. 3), the pairwise comparison method can be applied to determine priorities. Virtual experts can be involved to assess the importance of each criterion and alternative, in order to determine their weight coefficients by creating a pairwise comparison matrix.

For example, if it is necessary to evaluate the priority of alternatives based on the "**ACCESS CONTROL**" criterion, the ChatGPT system can help generate the relevant comparisons, which are then used to calculate the weights for each alternative.

The final step of the AHP procedure is to check the consistency of the obtained answers and evaluations, which allows determining whether optimal solutions have been achieved. After that, the hierarchical structure for decision-making in the field of cybersecurity can be completed, taking into account all criteria and alternatives.

To determine the weight coefficients of the alternatives (or criteria, if comparing criteria), it is sufficient to find the eigenvectors of the matrix A. The values of the eigenvector corresponding to the maximum eigenvalue will serve as the weight coefficients of the criteria (the weight coefficient—an element of the eigenvector corresponds to the number of the criterion). However, this approach is valid only if the pairwise comparison matrix is consistent. We will verify the consistency of the matrices obtained based on these methodological principles.

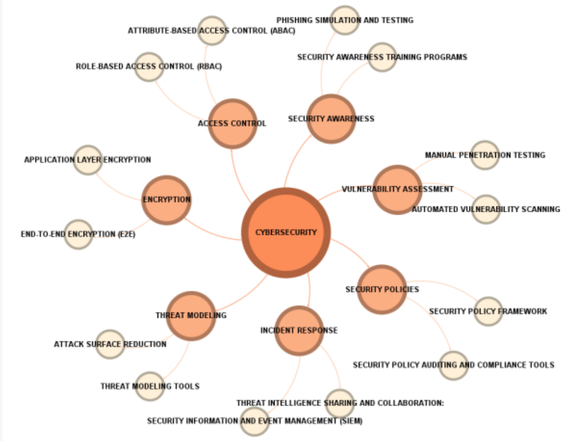
PHISHING SIMULATION AND TESTING
ATTRIBUTE-BASED ACCESS CONTROL (ABAC)
ROLE-BASED ACCESS CONTROL (RBAC)
SECURITY AWARENESS TRAINING PROGRAMS
ACCESS CONTROL
SECURITY AWARENESS
APPLICATION LAYER ENCRYPTION
MANUAL PENETRATION TESTING
ENCRYPTION
VULNERABILITY ASSESSMENT
AUTOMATED VULNERABILITY SCANNING
END-TO-END ENCRYPTION (E2E)
CYBERSECURITY
SECURITY POLICIES
SECURITY POLICY FRAMEWORK
THREAT MODELING
INCIDENT RESPONSE
ATTACK SURFACE REDUCTION
SECURITY POLICY AUDITING AND COMPLIANCE TOOLS
THREAT MODELING TOOLS
THREAT INTELLIGENCE SHARING AND COLLABORATION:
SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM)

Figure 3. Criteria and alternatives for the cybersecurity assurance problem

To ensure the consistency of the comparison matrix, the consistency coefficient μ\muμ is calculated. It is computed using the following formula:

$$\mu = \frac{|\lambda_{\max} - n|}{n - 1},$$

where $\lambda_{\max}$ is determined as follows: from the values of the comparison matrix and the eigenvector values, a matrix E is constructed, each element of which is $e_{ij} = a_{ij}\frac{w_i}{w_j}$, where w_i, w_j are the elements of the eigenvector. Next, the sum of the elements of the matrix E is computed for each row, and the maximum value $\lambda_{\max}$.

If the matrix of alternatives is fully consistent, then $\lambda_{\max} = n$, otherwise $\lambda_{\max} > n$. There is a table of reference consistency indices, which contains the values of reference indices for different values of $n - \mu_T(n)$. If $\mu / \mu_T(n) < 0.1$, is less than or equal to the corresponding reference value, the matrix of alternatives is considered consistent.

The matrices are considered consistent according to the criterion described above.

Conclusions

The swarm of virtual experts methodology is an approach that combines the capabilities of large language models, probabilistic analysis, and principles of collaborative work. Its primary scientific achievements include expanding the capabilities of LLMs, specifically through the use of multiple probabilistic responses from one or several LLMs to obtain more comprehensive and multifaceted information, introducing roles to model real interactions among experts, creating a mechanism for agent interactions that simulates knowledge transfer within real expert groups, and developing mathematical models for evaluating the quality and aggregation of responses, that take into account agent weights and the level of consensus.

This approach opens new horizons for leveraging LLMs to address complex analytical tasks such as evaluating the weights of connections in networks, forecasting, and decision-making.

In the context of SVE, the human expert performs two key functions: swarm coordination and aggregation/synthesis. The expert evaluates agents' responses, synthesizes the best among them, and formulates the final decision. Humans are the central element of the swarm, setting goals, formulating queries, and evaluating the results obtained.

The human role is indispensable in task formulation, result refinement, and validation. This highlights the necessity of harmonizing artificial intelligence with human expertise.

The SVE methodology has significant potential in various fields such as social sciences, ecology, and cybersecurity, where it can be applied to analyze relationships between threats, vulnerabilities, and network objects, assess risks, and develop protection strategies.

The methodology of the swarm of virtual experts facilitates the creation of adaptive and highly efficient decision-support systems. By leveraging LLMs and integrating principles of collective work, SVE significantly enhances the quality of complex network system analysis. In the modern context of rapid data growth and increasing task complexity, this methodology represents a significant advancement in the development of intelligent technologies.

References

[1] 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, DOI: 10.5281/zenodo.14278893

[2] Ilani A., & Dolev S. (2023, June). Common Public Knowledge for Enhancing Machine Learning Data Sets. In Proceedings of the 5th workshop on Advanced tools, programming languages, and PLatforms for Implementing and Evaluating algorithms for Distributed systems (pp. 1-10). DOI: 10.1145/3584684.3597263

[3] Lande Dmitry; Strashnoy Leonard. 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. SSRN Preprint (Oct 17, 2024). - 15 p. DOI: http://dx.doi.org/10.2139/ssrn.4978924

[4] Aslan Ömer, Semih Serkant Aktuğ, Merve Ozkan-Okay, Abdullah Asim Yilmaz, and Erdal Akin. "A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions." Electronics 12, no. 6 (2023): 1333. DOI: 10.3390/electronics12061333

[5] Ghelani Diptiben, Tan Kian Hua, and Surendra Kumar Reddy Koduru. "Cyber security threats, vulnerabilities, and security solutions models in banking." Authorea Preprints (2022). DOI: 10.22541/au.166385206.63311335/v1

[6] D.V. Lande, V.I. Polutsyganova, S.A. Smirnov. Methodology of the Virtual Experts' Swarm for Assessing the Interconnection of Threats and Vulnerabilities of Critical Infrastructure Objects //Artificial Intelligence and Security, Proceedings of the Scientific-Practical Conference, November 19-21, 2024, Kyiv: G.E. Pukhov IMEE NAS of Ukraine, IIR NAS of Ukraine, 2024. - P. 4-7.

[7] 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

[8] Saaty Thomas; Alexander Joyce (1989). Conflict Resolution: The Analytic Hierarchy Process. New York, New York: Praeger. 252 p.

[9] T.L. Saaty, L.G. Vargas. Decision Making with the Analytic Network Process. Economic, Political, Social and Technological Applications with Benefits, Opportunities, Costs and Risks. International Series in Operations Research & Management Science. Springer New York, NY. ISBN 978-1-4419-4154-1. 2006. 278 p.

[10] Lande Dmitry, Strashnoy Leonard. Hierarchical Formation of Causal Networks Based on ChatGPT. SSRN Preprint (May 8, 2023). - 13 p. DOI: https://dx.doi.org/10.2139/ssrn.4440629