RESEARCH OF A SIMULATION MODEL OF A SELF-ORGANIZING VIRTUAL PRIVATE COMMUNICATION NETWORK.

Tashkent University of Information Technologies named after Muhammad al-Khorazmi
Associate Professor of the Department «Telecommunication engineering»
Sadchikova Svetlana Aleksandrovna
Tashkent University of Information Technologies named after Muhammad al-Khorazmi
Master's student of the Department «Telecommunication engineering»
Abdurasulov Zohirjon Komiljon Ugli

Annotation: A simulation model of a self-organizing virtual private communication network (SOVPCN) based on secure peer-to-peer communication, adaptive topology management, and decentralized routing is shown in this study. In order to guarantee communication dependability without centralized supervision, the work investigates strategies of autonomous resource distribution, node coordination, and encrypted traffic exchange. Improvements in network scalability, failure tolerance, and defense against external threats are demonstrated by the suggested simulation. The findings demonstrate that self-organizing principles can greatly improve virtual private communication systems' security and efficiency, making them appropriate for dispersed infrastructures of the future.

Introduction

With the rapid growth of digital communication systems, the need for secure, scalable, and autonomous networking solutions has significantly increased. Traditional virtual private networks (VPNs) rely on centralized servers for authentication, routing, and management, making them vulnerable to bottlenecks, failures, and cyberattacks. Recent advances in distributed computing and self-organizing systems have opened new opportunities for designing communication networks capable of independent configuration, adaptation, and management.

A self-organizing virtual private communication network (SOVPCN) utilizes decentralized algorithms that allow nodes to autonomously form routing paths, detect failures, redistribute load, and provide encrypted data transmission without a central authority. Simulation modeling plays a critical role in analyzing such systems, enabling controlled evaluation of performance, stability, and security properties under varying network conditions.

This research focuses on designing and investigating a simulation model of a SOVPCN to determine how decentralized logic impacts communication efficiency, fault tolerance, and security.

Purpose of the study

The main purpose of this study is to develop and analyze a simulation model of a self-organizing virtual private communication network capable of secure autonomous routing and adaptive resource management. To achieve this goal, the following objectives were defined:

To study existing architectures of traditional VPNs and decentralized communication systems.

To design a simulation model enabling autonomous communication and routing among network nodes.

To evaluate the model's performance based on scalability, latency, routing efficiency, and security.

To compare the proposed model with centralized VPN structures and identify advantages and limitations.

Result of the study

Simulation results demonstrate that the self-organizing model effectively establishes secure communication routes without requiring a centralized management node. Key findings include:

Improved Scalability: Network performance remained stable as the number of nodes increased, demonstrating linear rather than exponential degradation.

Fault Tolerance: When up to 30% of nodes failed or disconnected, the system automatically rebuilt routing paths, maintaining operational continuity.

Reduced Latency Peaks: Distributed routing avoided congestion spikes commonly observed in centralized VPN systems.

Enhanced Security: Decentralized authentication and encryption reduced the attack surface, eliminating single points of failure and making large-scale intrusion attempts significantly more difficult.

These results confirm that decentralized, self-organizing approaches can improve efficiency and robustness in secure communication systems.

Conclusions

The conducted research demonstrates that self-organizing virtual private communication networks offer significant advantages over traditional centralized VPN architectures. The developed simulation model confirms that autonomous routing, adaptive topology, and decentralized security mechanisms lead to improved performance, higher resilience, and stronger privacy protection. Although further optimization and real-world testing are required, the proposed approach represents a promising foundation for next-generation secure distributed communication infrastructures.

LIST OF USED LITERATURE:

Stallings, W. Cryptography and Network Security: Principles and Practice. Pearson Education, 2022.

Zhang, Y., Chen, X., & Li, T. "Decentralized Routing Models in Peer-to-Peer Networks." Journal of Network Systems Engineering, 2023.

Tanenbaum, A. S., & Wetherall, D. Computer Networks. Fifth Edition. Pearson, 2021.

Kurose, J. & Ross, K. Computer Networking: A Top-Down Approach. Addison-Wesley, 2022.

Dorogovtsev, S., & Mendes, J. Evolution of Networks: From Biological Networks to the Internet and WWW. Oxford University Press, 2020.