The promising method of secure transmission of inelastic data in peer-to-peer networks

Tkachov Vitalii[1]
Chepurna Iryna[1]
Frolov Dmytro[1]

[1]*Kharkiv National University of Radio Electronics, 14 Nauky Ave, Kharkiv UA-61166, Ukraine, iryna.chepurna@nure.ua, vitalii.tkachov@nure.ua, dmytro.frolov@nure.ua*

Abstract. *The report analyses a method for secure transmission of inelastic data in peer-to-peer networks. The method ensures a high level of data protection and integrity. The research also covers the possibilities of optimizing data transmission processes in peer-to-peer systems. The proposed approach reduces transmission delays while guaranteeing the preservation of inelastic data integrity under conditions of large-scale information transfer. This method enhances the efficiency of exchanging large volumes of inelastic data in modern networks.*

Keywords: *Peer-to-peer networks, VPN, latency, inelastic data*

I. OVERVIEW OF THE SUBJECT AREA

Transiting inelastic data, which refers to data that cannot be easily compressed or altered without significant loss of information, in peer-to-peer networks requires adherence to specific conditions related to latency, jitter, and packet loss [1]. These requirements are driven by the nature of inelastic data, which cannot tolerate significant distortions or loss of information.

The decentralised nature of peer-to-peer networks also presents challenges in ensuring data transmission security, as each network node can be a potential source of threats, including unauthorised access to information, errors in routing and updating paths, and DDoS attacks [2]. This research aims to optimise data transmission processes, mitigating risks associated with the decentralised network architecture and enhancing overall information exchange efficiency. The problem statement involves investigating and analysing existing algorithms that can optimise the transmission processes of inelastic data while ensuring its integrity and security within a decentralised environment.

II. THE CRUCIAL RESEARCH PROBLEM

The method addresses the applied task of ensuring the integrity of inelastic data during its secure transmission in a peer-to-peer network. Achieving high speed and minimal latency is essential and critical for transmitting large volumes of inelastic data. One approach to solving these crucial issues is the application of VPN tunnelling at the local network's border node, providing a secure data transmission channel. VPN tunnelling involves encapsulating the data in a private, secure 'tunnel' within the public network, ensuring that the data remains protected and intact during transmission [3]. The subsequent use of the peer-to-peer network serves as a dynamic environment for file exchange with end users, who utilise BitTorrent clients to interact with the source [4]

This method employs a hybrid routing approach that combines static and dynamic processes. Specifically, VPN tunnelling creates a secure channel between the source and recipient, both participants in the peer-to-peer network. Encryption of traffic and transmitted packet contents ensures a high level of protection for the identification data of both parties.

The dynamic approach in the peer-to-peer network helps reduce latency and jitter when transmitting inelastic data by distributing the load across different network nodes. Using metrics such as bandwidth, distance, load, and connection speed allows for selecting the most efficient route for data transmission [5]. This ensures the highest possible transmission speed, minimises latency and jitter, and creates optimal conditions for transmitting inelastic data and massive volumes.

In the proposed method, the algorithm for inelastic data transmission consists of several main stages. In the first stage, a VPN server is configured to ensure secure data transmission and encryption of packet contents, which are subsequently transmitted through the peer-to-peer network. It is important to note that the computational complexity of cryptographic encryption affects the time of encryption and decryption processes, the use of computing resources, and the resistance to attacks in the event of unauthorised access.

In the next stage, the server and end users connect to the peer-to-peer network by installing appropriate software for P2P file sharing. This is due to the decentralised architecture of such networks. The most common clients for file sharing via the BitTorrent protocol are µTorrent, FrostWire, and LimeWire, supported on most modern operating systems. To ensure secure transmission, end users must also install additional software according to the chosen VPN tunnelling protocol:

$$E_{VPN+Peer} = \alpha_1 \cdot \frac{V_{eff}}{B} + \alpha_2 \cdot S_{VPN} - \alpha_3 \cdot L_t - \alpha_4 \cdot R_t \,, (1)$$

where $E_{VPN+Peer}$ – is the overall efficiency of the secure transmission method; V_{eff} – is the effective data transmission speed; B – is the baseline speed without encryption; S_{VPN} – is the VPN security level, determined by the encryption complexity and the chosen VPN protocol; L_t – is the total transmission delay; R_t – is the resources expended on encryption and data transmission; $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ – are the weighting coefficients that define the importance of each parameter.

The critical components of this task are the overall data transmission delay and system resources. These parameters are determined by various factors that affect the data transmission speed and can be described as follows:

1. The total delay L_t is defined as the sum of delays due to encryption, data transmission through the VPN and peer-to-peer network, as well as delays related to node load and jitter:

$$L_t = \frac{1}{\mu_{VPN}} + \frac{\lambda_{peer}}{\mu_{peer}\left(\mu_{peer} - \lambda_{peer}\right)} + J + L_{sh} + L_l, \quad (2)$$

where μ_{VPN} - is the average request processing speed in the VPN; λ_{peer} - is the request rate in the peer-to-peer network; μ_{peer} - is the request processing speed in the peer-to-peer network; L_{sh} - is the delays due to encryption; L_l - is the delays due to node load; J - is jitter.

In this case, jitter can be calculated as the standard deviation of the packet delay times in the peer-to-peer network, which can be expressed through the average delay of each packet:

$$J = \sqrt{\frac{1}{n}\sum_{i=1}^{n}\left(L_i - \overline{L}\right)^2}, \quad (3)$$

where L_i - is the delay for each packet; $\overline{L}$ - is the average transmission delay for all packets; n - is the number of packets transmitted.

2. The efficiency E of computational resource utilisation is determined by the volume of data transmitted and the resources expended on encryption and transmission:

$$E = \frac{D_{peer}}{R_{sh,VPN} + R_{trans,\,peer}}, \quad (4)$$

where D_{peer} - is the volume of inelastic data transmitted through the peer-to-peer network; $R_{sh,VPN}$ - are the resources expended on encryption in the VPN; $R_{trans,\,peer}$ - are the resources expended on transmission through the peer-to-peer network.

This approach allows for a comprehensive assessment of the effectiveness of the secure transmission method for inelastic data in a peer-to-peer network, considering the complexity of cryptographic algorithms, queuing models, the resource intensity of encryption and data transmission, and transmission delay. The application of these models provides a more accurate quantitative evaluation of the relationship between security level, transmission speed, and resource utilisation efficiency, which is crucial for optimising transmission methods using VPN in a peer-to-peer network.

III. CONCLUSIONS

The secure transmission of inelastic data in peer-to-peer networks involves VPN tunnelling at border nodes for further data transmission through the peer-to-peer network. The model of this network, based on the M/M/1 queuing system, demonstrates that this approach reduces transmission delays by leveraging the more significant number of nodes typical of peer-to-peer networks while maintaining high data integrity and protection. Traffic encryption and the concealment of source and recipient identification data further enhance security against unauthorised access. Distributed hash tables (DHT) used in peer-to-peer networks also support efficient file sharing with high data transmission speeds. Hybrid routing approaches contribute to increased network fault tolerance and reduced delays, jitter, and packet loss, critical factors in ensuring the effective transmission of inelastic data.

REFERENCES

[1] Tkachov V. Architecture of overlay network with nested vpn tunneling / M. Hunko, V. Tkachov, M. Bondarenko // "Сучасні напрями розвитку інформаційно комунікаційних технологій та засобів управління" : матеріали Дев'ятої міжнар. наук.-техн. конф., 9-10 квітня 2020 р. – Харків, 2020. – С. 36.

[2] Аналіз проблем безпеки піринговых мереж / Л.М. Куперштейн, М. Д. Кренцін, А. В. Дудатьєв, В. А. Каплун // Інформаційні технології та комп'ютерна інженерія. – 2022. – № 2. – С. 5-13.

[3] Verkhovskyi, I., & Tkachov, V. (2023). Metody pobudovy virtually tunnel extranet-system [Methods of building virtual tunnels for extranet systems]. Scientific Review, 4(89), 22. https://doi.org/10.26886/2311-4517.4(89)2023.2.

[4] Кренцін М. Д. Аналіз протоколів піринговых мереж [Електронний ресурс] / М. Д. Кренцін, Л. М. Куперштейн // Матеріали LI науково-технічної конференції підрозділів ВНТУ, Вінниця, 31 травня 2022 р. – 2022.

[5] Moltafet, M., Leinonen, M., & Codreanu, M. (2020). Average Age of Information for a Multi-Source M/M/1 Queueing Model With Packet Management. In 2020 IEEE International Symposium on Information Theory (ISIT), Los Angeles, CA, USA. https://doi.org/10.1109/isit44484.2020.9174099.