M. D. Krentsin; L. M. Kupershtain, Cand. Sc. (Eng.), Associate Professor

HYBRID MULTIFACTOR AUTHENTICATION OF PEER-TO-PEER NETWORK NODES

Method of hybrid multifactor authentication of nodes in the peer-to-peer network is developed. Method includes the authentication both of initial nodes and secondary nodes (connected to the available network). Each node must first perform authentication by the server, as a result of the authentication it obtains the token of access to the server, communication taken (necessary for performing communication with the node), and service token (for the exchange of the service data with other nodes). Further the node must be authenticated by other node. For this purpose predefined identifiers, zero knowledge proof method and network of trust are. Knowing identifier of another user the node can be authenticated after passing verification by zero knowledge proof method in three stages. First it is verified that the node possesses the knowledge of the server address. Further the validity of token is verified by means of verification of the date of issuing a token (in this process, server, which provides date of issue by identifier participates). The last step is verification is if the node can correctly code certain data. For this purpose, pseudo-random sequence of numbers is generated, it must be coded by the server and node. Only server and node know the encryption key (in case of server authentication key is generated for each node). If all verification stages are successful, then the nodes exchange identification data and, thus, become mutually authenticated. By means of the network of trust, if two nodes are not mutually authenticated but are authenticated by the third node, then they can directly exchange identification data without passing the verification process by means of zero knowledge proof. The suggested method is directed to the increase of the security level of peer-to-peer networks. Important aspect is the possibility to cut off potentially harmful nodes before their actual connection to the network.

Key words: *peer-to-peer network, authentication, zero knowledge proof, identifier, network of trust, coding, access token, communication, server.*

Introduction

Nowadays people actively use various programmers and services for communication. In this context data security becomes extremely important task in modern digital world [1]. Usually, communication platforms are generally accessible and are based on the central server, which is the main node of the communication and stores all the data. However, even using various cryptographic algorithms and other methods of protection, central server has a number of drawbacks, especially in cases of corporate communication, as corporate data are confidential and must not fall into the hands of the intruders.

To provide the security of the corporate information peer-to-peer networking technologies are used, they are directed on the provision of the integrity, accessibility and confidentiality [2]. Peer-to-peer (P2P) networks – it is a type of the networks where the participants exchange data without centralized control organ (server). Their popularity grows but at the same time the problem of security becomes more and more important [3]. One of the key issues of confidentiality provision is authentication of the nodes in peer-to-peer (P2P) network. Due to semi-trusted nature of the peer-to-peer networks authentication is critically important for the identification of users and for the secured data exchange. In the decentralized networks the realization of the authentication mechanism is rather complicated due to the lack of the single reliable source of information for user identity confirmation. That is why, the elaboration of the method of nodes identification in P2P networks which provides high security level is a relevant task.

Problem set up

Main problem of peer-to-peer networks is that as a result of their decentralized structure the security is not realized in the same way as in client-server architecture. The security of P2P networks is achieved by means of data coding, nodes authentication, access limitation, system of traffic monitoring, revealing and prevention of harmful activities, etc. [4].

Nodes authentication is the first stage for the provision of the secure communication of peer-to-peer network nodes (Fig. 1) [5].For the interaction of two nodes each of them must pass the authentication procedure. After that they must exchange with the identification data. Only after that the nodes may establish the connection and start data exchange.

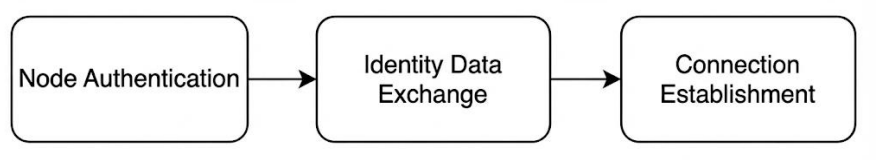

Fig. 1. Steps to be taken before the communication

In peer-to-peer networks there exist three approaches to users authentication:

1. Predetermined identifiers, which are issued in manual mode or can be sent by the third party software [6]. In this case manual mode is rather reliable but difficult to use. Sending by the third party software is rather convenient but less protected as the data may fall into wrong hands.
2. Web of trust is one of the methods to solve the problem of the lack of the trusted central authority [7]. The approach is based on transitivity principle, namely, if node A trusts node B, and node B trusts node C, then node A may trust node C. Correspondingly, nodes A and C may perform communication.
3. Zero knowledge proof, the essence of which is to prove one side to the other side that the statement (as a rule, mathematical) is true, at the same time, any confidential information, except the truth-value of the statement is not disseminated [8]. Computations in zero knowledge proof (ZKP) systems can be carried out by means of creating random numbers as the input data. Concept, being the base of zero knowledge proof, is the verification by the verifier V the fact that node A knows the secret S, but the secret itself is not transferred to the verifier V. That is, the verifier does not know any information about the unknown but can confirm that the node possesses this secret. Verifier asks the node different questions, and if all the answers are correct, it may state that the verification is successful. However, the development of ZKP-protocols is the task, requiring much attention regarding the security and account of the potential attacks [9].

Proceeding from the above-mentioned advantages and disadvantages of each of the approaches it is suggested to use the hybrid multifactor authentication. This is connected with the fact that single factor authentication in peer-to-peer networks is not sufficient. Use of only central server does not provide the sufficient level of autonomy, security and fault tolerance as the centralized system is vulnerable to various attacks, for instance “brute force” method or by means of “masquerade attack”. As a result, the intruder can obtain identification data of the nodes [10]. Use of only predefined identifiers is impossible due to great complexity of network scalability, because under condition of non-use of the unwanted communication channels physical presence of the user is necessary. Belief network is a mechanism, operating only in combination with other methods as the nodes must be preauthenicated by other methods, which, in their turn, will be mutually authenticated according to the principle of belief network.

Thus, the peer-to-peer network node must perform hybrid multifactorial authentication, which includes the use of the central server for the first stage and other node for the second stage.

Results of the research

Let us assume that a participant wishes to connect to the network (become a node of a network), it may be of two types: initial P_n (it becomes the first node of the new network) and secondary P_k (it joins the available network).

Let us consider the authentication process of the initial node P_n.

New participant P_n, who wants to join certain network A, must pass the authentication procedure F by means of the client-server part of the network. This process includes verification and confirmation of the new participant identity. After the successful authentication via the server

$$RA = F(P_n), \quad (1)$$

where RA – is the result of authentication, $F(P_n)$ – is the authentication function; the participant obtains unique identifier Id and the set of keys $K = \{k_1, k_2, k_s\}$, where k_1 – is a symmetric key for coding the service data, and k_2 – is a pair of keys (public and private) that will be used for coding of the identification data, k_s– is the key for coding the data the node exchanges with the server. Additionally, the participant obtains the set of tokens $T = \{t_a, t_c, t_s\}$, envisaged by the security policy. Tokens are of JWT (Json Web Token) format [11]. Each token contains payload, where necessary for the nodes data can be added. Thus payload of tokens is formed (fig. 2 – fig. 4).


```
{
"createdAt": 1713123901470,
"id": "65959cd4-d8f1-4523-895a-2e3137e87425",
"type": "serverAccess"
}
```


Fig. 2. JWT payload of the access token


```
{
"createdAt": 1713124968688,
"id": "65959cd4-d8f1-4523-895a-2e3137e87425",
"type": "communication",
"trustLevelCount": 14
}
```


Рис. 3. JWT payload of the access token


```
{
"createdAt": 1713125070193,
"id": "65959cd4-d8f1-4523-895a-2e3137e87425",
"type": "service"
}
```


Рис. 4. JWT payload of the access token

By means of the first t_a the nodes have the possibility to perform the request to the server for obtaining certain service information. By means of the second token t_c the nodes will be able to send data to other nodes (and they in their turn have to validate them prior to answer the request). By means of the third toke t_s nodes can perform service data exchange. While granting token access t_a, the server registers the date and time of its granting, this is coded in the token itself. These data are an important element for determination of the temporal context and can be used for further control of the access and performing nodes verification in the network. Thus, the result of the authentication function RA may be presented in the following way:

$$RA = \{Id, K, T\}. \quad (2)$$

Authentication process of the secondary node will be considered:

1. The first stage is analogous both for a new participant and for the node, which joins the available network. In both cases the participant must pass the authentication procedure by means of client-server part of the network to provide security and determine identifiers and keys for further interaction in the network.

2. After the successful confirmation by the server, the participant $b_j \in B$can be authenticated, knowing the identification data of the other node $b_i \in B$, or having only the identifier, be authenticated after passing the verification by the node b_j. Verification occurs by the method of zero knowledge proof, i.e., certain function is carried out

$$ZNPR = ZNPF(b_j), \quad (3)$$

where $ZNPR$ – is the result of verification, $ZNPF$ – is verification function. The subject of verification is access token t_a of the node b_j. Data exchange in the format question-answer takes place, namely (fig. 5):

a. Node b_i sends the request Q_1 to the participant b_j, to obtain the address of the server Res_1.

b. Participant b_j sends the response Res_1.

$$Res_1 = Ans(Q_1), \quad (4)$$

where Ans– is the function of response delivery.

c. Node b_i compares it with what it knows, namely $Addr$. If the values are equal

$$CHK_1 = (Res_1 \Leftrightarrow Addr), \quad (5)$$

where CHK_1– is the result of verification, then the verifier (node b_i) passes to another question. In other case the process is interrupted and participant b_j is added into the black list of the network, as it can be malicious.

d. Node b_i sends the request Q_2 to the participant b_j, what the date and time of the token dt_{t_a} issue is. At the same time node b_i sends the request Q_2' on the server in order to obtain the information regarding the date and time of token dt'_{t_a} issue on certain identifier $dt^s_{t_a}$ (in this case neither node nor server know the token).

$$dt_{t_a} = Ans(Q_2), \quad (6)$$

$$dt'_{t_a} = Ans(Q_2'). \quad (7)$$

e. In case if the response of the participant b_j and server are the same

$$CHK_2 = (dt_{t_a} \Leftrightarrow dt'_{t_a}), \quad (8)$$

where CHK_2 – is the result of verification, then the verifier passes to the next question. If not – the process stops and the participant b_j is added to the black list of the network.

f. Node a_i generates pseudo-random sequence of numbers NS and sends the request Q_3 to the participant b_j to code it with its key from the access token. Response Res_3 is expected. The same request is sent to the server and the encoded value from the server Res_3' is expected:

$$Res_3 = Ans(Q_3), \quad (9)$$

$$Res_3' = Ans(Q_3') \quad (10)$$

g. In case if the response of the server is the same as of the participant b_j, then the verification stage is successfully completed. Otherwise – the participant b_j is added to the black list of the network, as it can be malefactor. Verification function is presented in the following way:

$$CHK_3 = (Res_3 = Res_3'), \quad (11)$$

where CHK_3 – is the result of the verification.

$$ZNPR = \{CHK_1, CHK_2, CHK_3\}. \quad (12)$$

Thus, all $CHK_i \in CHK$, where CHK – is a set of the results of the verification of the participant by the verifier, must have the value of «truth», it means the successful verification. After successful verification by the node a_i, the participant b_j becomes the authenticated node of the network. Node b_i sends all the necessary data to node b_j for further communication.

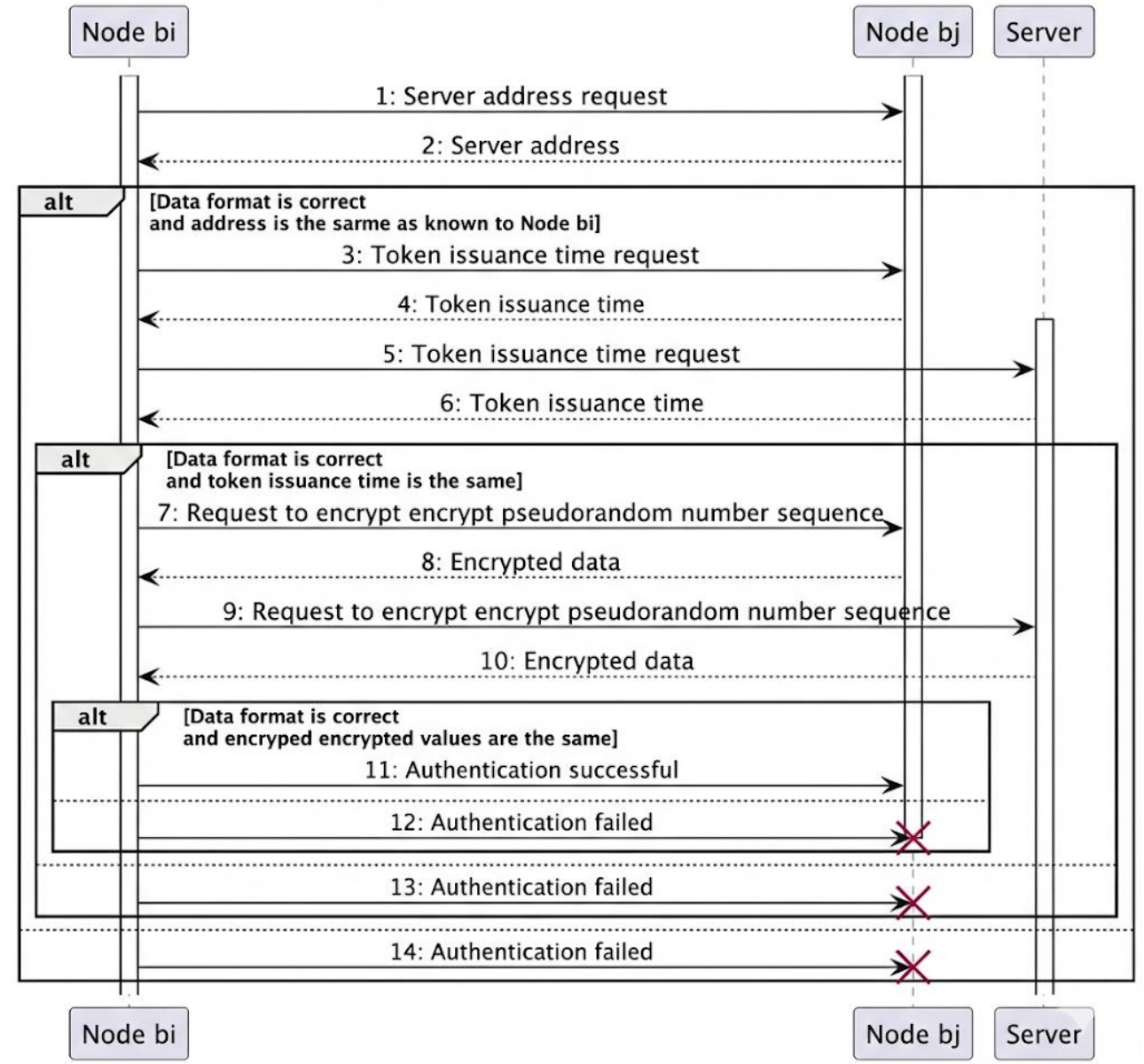

Fig. 5. UML-diagram of the node verification process

On the base of the method of the network of trust, node b_j can perform the data exchange with other nodes of the network. That is, if node b_i verified node b_j and it is the part of the network and node b_i performs communication with certain node b_k, then according to the principles of the network of trust, node b_j will be able to establish the connection with the node b_k without passing the verification. Formally, $(b_i \Rightarrow b_j), (b_i \Rightarrow b_k) \Rightarrow (b_j \Rightarrow b_k), i \neq j \neq k$. Thus, according to the principle of the network of trust, node b_j has the right to obtain identifications of the node b_k and have the possibility to perform the communication with it.

Conclusions

Method of nodes authentication in P2P network is elaborated, it is the hybrid multifactorial process. The given method combines three basic authentication methods: predefined identifiers, zero knowledge proof and network of trust. Additionally, server is needed for performing the first stage of authentication prior the authentication by another node will be carried out. Also the server is used for several steps of verification by ZKP method. The elaborated method can be used for improving the security of P2P networks.

An important aspect is the possibility of cutting the potentially harmful nodes prior to their actual connection to the network. Process of cutting is realized at several stages, this provides high reliability and efficiency in the process of authentication.

REFERENCES

1. Kupershtain L. M. Analysis of peer-to-peer networks development trends / L. M. Kupershtain, M. D. Krentsin // Bulletin of Khmelnytskyi National University. – 2021. – №4. – P. 25 – 29. (Ukr).
2. A privacy data leak age prevention method in P2P networks [Electronic resource] / Cheol-JooChae // Peer-to-Peer Networking and Applications. – 2015. – T. 9, № 3. – P. 508–519. – Access mode: https://doi.org/10.1007/s12083-015-0371-x.
3. Analysis of security problems of peer-to-peer networks / L. M. Kupershtain, M. D. Krentsin, A. V. Dudatiev [et al.] // Information technologies and computer engineering. – 2022. – №2. – P. 5 – 14. (Ukr).
4. Qureshi H. P2P Networking [Electronic resource] / Haseeb Qureshi // NAKAMOTO. – Access mode : https://nakamoto.com/p2p-networking.
5. Yik L. Z. A Systematic Literature Review on Solutions of Mutation Testing Problems [Electronic resource] / Loh Zheung Yik, Wan Mohd Nasirbin Wan Kadir, Norainibinti Ibrahim // 2023 IEEE 8th International Conference On Software Engineering and Computer Systems (ICSECS), Penang, Malaysia, 25–27 August . 2023 p. – Access mode: https://doi.org/10.1109/icsecs58457.2023.10256324.
6. Identifier | Encyclopedia of Computer Science [Electronic resource] // DL Books. – Access mode : https://dl.acm.org/doi/abs/10.5555/1074100.1074468.
7. Anonymous and Distributed Authentication for Peer-to-Peer Networks [Electronic resource] / PasanTennakoon // Journal of Computer Science. – 2023. –T. 19, № 1. – P. 1–10. – Access mode: https://doi.org/10.3844/jcssp.2023.1.10.
8. A Resilient Group Session Key Authentication Methodology for Secured Peer to Peer Networks using Zero Knowledge Protocol [Electronic resource]. – Access mode: https://doi.org/10.1016/j.ijleo.2022.170345.
9. Establishing Trustusing Zero Knowledge Succinct Proof in Peer-to-peer Data Transfer [Electronic resource] / Sai Kiran Deversetti // Proceedings of 36th International Conference on Computer Applications in Industry and Engineering. – Access mode: https://doi.org/10.29007/jqw8.
10. Magnusson A. 11 Common Authentication Vulnerabilities You Need to Know | Strong DM [Electronic resource] / Andrew Magnusson // Strong DM: Your Partnerin Zero Trust Privileged Access. – Access mode: https://www.strongdm.com/blog/authentication-vulnerabilities.
11. JWT.IO [Electronic resource] // JSON Web Tokens - jwt.io. – Access mode: https://jwt.io/.

Editorial office received the paper 23.06.2024.
The paper was reviewed 27.06.2024.

Krentsin Mykhailo – Post Graduate with the Department of Information Security, e-mail: mishatron98@gmail.com.
Vinnytsia National Technical University

Kupershtain Leonid – Cand. Sc. (Eng.), Associate Professor with the Department of Information Security.
Vinnytsia National Agrarian University.