Dynamic Anonymous Access Control Based on Dual-Mode Single-Packet Authentication

Yunfan Wang , Chuan He , Zesheng Xi , Bo Zhang , Tao Zhang *

Posted Date: 7 January 2025

doi: 10.20944/preprints202501.0527.v1

Keywords: Zero trust architecture; Dual-mode single-packet authorization; Software-defined boundaries; Anonymous access; Trust evaluation

Article

Dynamic Anonymous Access Control Based on Dual-Mode Single-Packet Authentication

Yunfan Wang †,‡, Chuan He ‡, Zesheng Xi ‡, Bo Zhang ‡ and Tao Zhang *

State Grid Laboratory of Power Cyber-Security Protection and Monitoring Technology, China Electric Power Research Institute Co., Ltd., Nanjing, China; 230240007@seu.edu.cn; 230240027@seu.edu.cn; 4317045xi@163.com; zhangbo6@epri.sgcc.com.cn

* Correspondence: zhangtao3@epri.sgcc.com.cn

† Current address: School of Cyber Science and Engineering, Southeast University, Nanjing, China.

‡ These authors contributed equally to this work.

Abstract: Anonymous access control is crucial in network security to protect user privacy and support anonymous communication while balancing the need for confidentiality and traceability in specific scenarios. This control mechanism is important for maintaining data security, identity protection and security auditing. Traditional anonymous access control methods currently have two challenges: High performance overhead and Vulnerability to cyber-attacks. To cope with the above challenges, this paper proposes a dynamic anonymous access control method based on dual-mode single-packet authentication. The method utilizes dual-mode single-packet authentication to complete user authentication in the anonymous access phase, dynamically evaluates the user's trust level through the trust evaluation module, and finally decides whether to allow the user to access the network resources. Experimentally verified, the dual-mode single-packet authentication scheme is more advantageous than other schemes regarding communication overhead and computation overhead, and the access efficiency is further improved.

Keywords: zero trust architecture; dual-mode single-packet authorization; software-defined boundaries; anonymous access; trust evaluation

1. Introduction

In the context of the industrial Internet, anonymous access control plays a role in ensuring user identity privacy and security, especially when it comes to sensitive data transmission and access control to prevent leakage or misuse of user information [1].

Existing anonymous access control methods are mainly classified into two categories, one is cryptography-based anonymous access control methods and the other is agent-based anonymous access control methods. Cryptography-based anonymous access control methods refer to the use of cryptographic techniques, such as anonymous credential systems (e.g., anonymous credential signatures) and zero-knowledge proofs, to enable users to gain access to resources without revealing their identity information. Proxy-mediated anonymous access control techniques entail the redirection of client requests via an intermediary proxy server, which in turn transmits the requests to the intended destination server. This process obfuscates the originating client's actual IP address, thereby facilitating anonymous network interaction. Alternatively, a distributed anonymous communication network is used to protect the user's anonymity through multilayer encryption and routing to hide the user's identity information and access activity information.

However, the above approaches face the following two challenges:

1. **High performance overhead:** Anonymous access through encryption requires complex encryption and decryption operations, which require a large number of computing resources, resulting in increased access latency and reduced system efficiency. The forwarding of requests through a proxy server increases network latency and bandwidth consumption, especially in the case of a larger number of users or larger network traffic, the performance overhead is more significant.

 doi:10.20944/preprints202501.0527.v1

2. **Vulnerable to cyber-attacks**: Existing anonymous access control methods make it difficult to identify and block unauthorized access, and attackers can take advantage of the inadequacies of these control mechanisms to access the system under the disguise of a legitimate user [2], thus stealing data or carrying out other malicious operations [3].

This paper proposes a dynamic anonymous access control method based on dual-mode single-packet authentication to address the above challenges. The method utilizes dual-mode single-packet authentication technology to complete user authentication in the anonymous access phase, dynamically assesses the user's trust level through a trust assessment module, and ultimately decides whether to allow the user to access network resources. Among them, dual-mode single-packet authentication is an emerging network authentication technique that combines UDP(User Datagram Protocol)and TCP (Transmission Control Protocol) and completes the initialization of user authentication and the preparation of encrypted communication through a single packet.

The primary contributions of this paper are:

1. Reducing communication overhead and computation overhead: the introduction of dual-mode single-packet authentication completes the preparation of authentication and encrypted communication in a single packet, which decreases the packet count and the transmission frequency, and reduces the communication overhead. The SDP gateway pre-calculates the SPA key during the online process. It builds an index table to quickly retrieve the corresponding SPA key, avoiding the need to perform calculations for each authentication, thus reducing the computation overhead. The trust assessment module reasons and calculates through fuzzy logic, which is less computationally intensive and more efficient than traditional rule- or role-based access control methods.
2. Protecting user privacy and resisting a variety of network malicious attacks: the method effectively resists a variety of network attacks such as SPA key theft, knock amplification attacks, identity forgery, and so on, using two-way anonymous access and trust assessment mechanisms. Two-way anonymous access safeguards the confidentiality of users' identity information, rendering it challenging for attackers to uncover their true identities. On the other hand, the trust assessment module further improves system security by analyzing user behavioral data to identify abnormal behaviors, such as frequent access to sensitive resources or the use of abnormal login methods, and taking timely measures to prevent them. In addition, the trust assessment module can dynamically adjust the trust threshold in response to the network environment and attack posture, to cope with evolving attack methods, thereby bolstering the security and stability of the network.
3. In this paper, a dynamic anonymous access control method based on dual-mode single-packet authentication is proposed, and a simulation environment is constructed by the Network Simulator 3 platform, which simulates the interaction of terminal server running SPA, access gateway server, and SDP (Software-defined perimeter) controller, and evaluates the two metrics of communication overhead and computation overhead. The findings from the experiment indicate that this approach demonstrates significant benefits in terms of both communication and computational efficiency, and improves access efficiency.

 doi:10.20944/preprints202501.0527.v1

2. Related Works

At present, many scholars have conducted extensive studies aimed at enhancing the security and anonymity of SDP architecture. C. Decusatis et al. [4] proposed a new network architecture based on steganographic overlay, which uses TCP packet requests to embed authentication tokens, and realizes first-packet authentication and explicit zero-trust architecture. D. idle et al. [5]proposed an experimental test structure to realize autonomous control plane feedback based on the observation, direction, decision, and action framework, which was used to construct a model for the proposed zero-trust cloud data center network. In 2019, the Ministry of Industry and Information Technology listed zero-trust security as one of the key network security technologies in urgent need of breakthroughs in China for the first time. In 2022, Lin Xuan, Wang Hongding, Xu Bao-chen and other scholars proposed a private cloud optimization security solution based on the concept of zero trust, which constructed a virtual boundary through software, and used identity-based access control and complete permission authentication mechanism to provide effective stealth protection. At the same time, Yang Y, Wu Z [6] and other scholars proposed to fully integrate Software Defined Boundary (SDP), Identity and access Management (IAM), and micro Isolation (MSG) in the form of "ZTA platform". In addition, through the innovation of key technologies, the best trusted access control and security isolation are realized. It achieves the security effect of "never trust, always verify" for users' access in the business layer, data layer and terminal layer, and improves the overall security level while reducing the security complexity and operational overhead. Marco Baldi [7] and other scholars proposed the R-SDP (Restricted SDP) protocol to reduce the communication cost and improve security by adjusting the subspace size, thereby enhancing the system's resilience to attacks while also protecting the privacy and ensuring the unaltered transfer of data. In 2023, Shen Q and Shen Y proposed a zero-trust anonymous access scheme [8] under SDP architecture, which used the three-party key agreement to realize the distribution [9] of SPA keys.

3. Methodology

3.1. Overall Architecture

A dynamic anonymous access control method based on dual-mode single-package authentication is composed of two-way anonymous access module, dual-mode single-package authorization module and trust evaluation module. The dual-mode single-package authorization module is deployed in the anonymous access step to solve external attacks and protect the privacy of visitors [10], and the trust evaluation module is deployed in access control. The trust evaluation module is deployed in the anonymous access step, which mainly solves the problem of whether to grant the subject access to the object [11]. It mainly includes four main steps: system establishment, system registration, anonymous access and trust evaluation. Its SDP architecture diagram is shown [12] in Figure 1.

 doi:10.20944/preprints202501.0527.v1

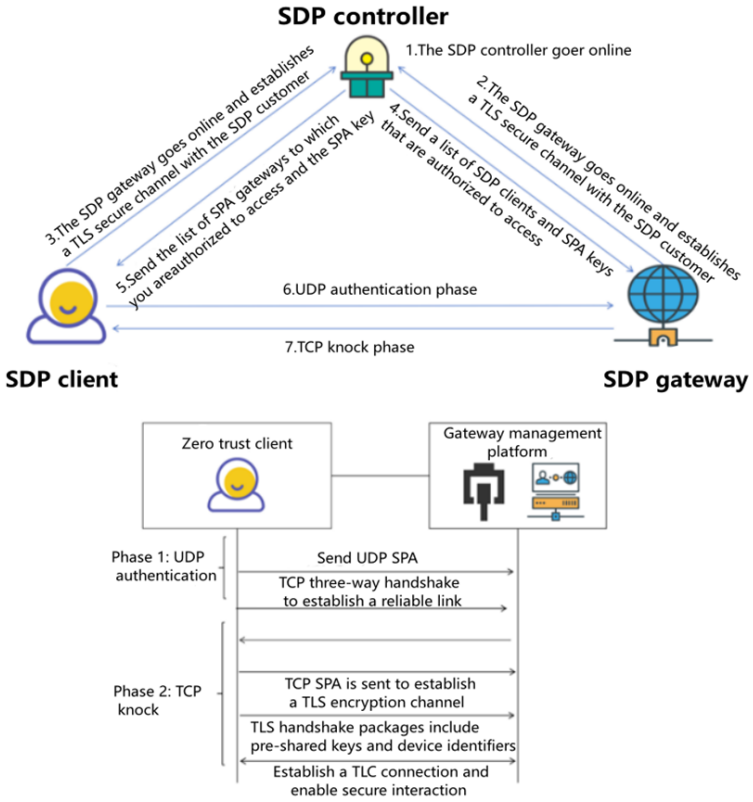

Figure 1. Architecture diagram of dual-mode single-package SDP

3.2. Anonymous Access

The anonymous access phase mainly includes three steps: SDP gateway online, SDP client online, and dual-mode single-package authorization authentication and access.

3.2.1. Launching the SDP Gateway

The SDP gateway performs the following four steps to interact with the SDP controller to go online: First, the private key is randomly selected and the SPA key agreement parameters are calculated. Secondly, the key agreement parameters are sent to the SDP controller, and then the SDP controller queries the list to generate a list of SPA key agreement parameters containing all SDP clients with access rights and sends it to the SDP gateway. Finally, the SPA key was precomputed for all the parameters in the SPA key agreement parameter list, and the index table [13] was established.

3.2.2. SDP Client Is Online

The SDP client performs the following three steps to interact with the SDP controller: first, it randomly selects the private key, calculates the SPA key agreement parameters, and sends the SPA key agreement parameters to the SDP controller. Secondly, the SDP controller generates the SDP gateway information accessible to the SDP client through the SPA key negotiation parameter list and access permission list of the SDP client, and generates the authorized access list. Then the SDP controller generates the linked certificate information and executes the signature algorithm to generate the certificate based on the linked certificate information. Finally, the SDP controller sends the link certificate information, the credentials, and the authorized access list to the SDP client, and the client executes the signing

The name validation algorithm verifies the validity [14] of the credential.

 doi:10.20944/preprints202501.0527.v1

3.2.3. Dual-Mode Single-Packet Authentication Access

Dual-mode single-packet authentication access mainly includes two phases: UDP authentication phase and TCP knocking phase.

The UDP authentication phase is mainly a secure communication process between the client and the SDP controller, which can be divided into four key steps: sending the knock packet, encryption, verification, and how the SDP gateway updates the firewall rules to allow legitimate access based on the verification results. Firstly, the client sends the knock packet to the SDP controller, which contains the user security code, device identification, timestamp, random number and host MAC value. To ascertain the integrity and confidentiality of data transmission, the user security code is encrypted by SM3 hash algorithm, and the device identification is processed [15] by SM4 hash algorithm. Secondly, after receiving the SPA packet transmitted by the network card, the SDP gateway needs to undergo multiple verifications to verify the validity of its data. Finally, when the SPA package is verified, the SDP gateway updates the local firewall rules to open TCP port access rights for legitimate users and device source IP and sets a fixed window time. The purpose of setting the window time is to prevent port amplification from being exposed to potential hacker attacks for a long time. From the perspective of user experience, From the perspective of user experience, the main factors to be considered in the opening window time are network link delay and user authentication time, in order to avoid the TCP knock packet cannot be received due to too short time, thus affecting the user experience [16].

The TCP knocking phase can be divided into five key steps: TCP connection establishment, TLS handshake preparation, SPA token transfer, server-side SPA token authentication, and authentication result processing. First, The client and the SDP gateway establish a connection using the TCP three-way handshake procedure. Second, the client prepares the TLS handshake request and adds the SPA token in the TLS field, so that the data packet carries the dynamic token, and the TLS handshake packet may also contain information such as the user pre-shared key and the device identity. Then the client sends the TLS handshake request containing the SPA token to the SDP gateway [17]. Then, upon receiving the TLS handshake request, the SDP gateway extracts the SPA token from the extended field of the TLS handshake packet and verifies it, which typically includes verifying that the token is valid and valid. Finally, for the authentication result, if the SPA token authentication is successful, the SDP gateway and the client complete the TLS handshake process and establish an encrypted communication channel. If the SPA token authentication fails, the SDP gateway disconnects the TCP connection [18] with the client.

The entire process ensures that before communication can be established from the client to the SDP gateway, the SPA token is first authenticated, and the TLS handshake and data transfer are performed only after successful authentication, thus improving communication security.

3.3. Trust Evaluation

Trust evaluation mainly includes five steps: data processing, specifying fuzzy rules, fuzzy calculation, defuzzification, calculating and comparing comprehensive trust value and trust threshold. The flow chart is shown in [19] Figure 2.

 doi:10.20944/preprints202501.0527.v1

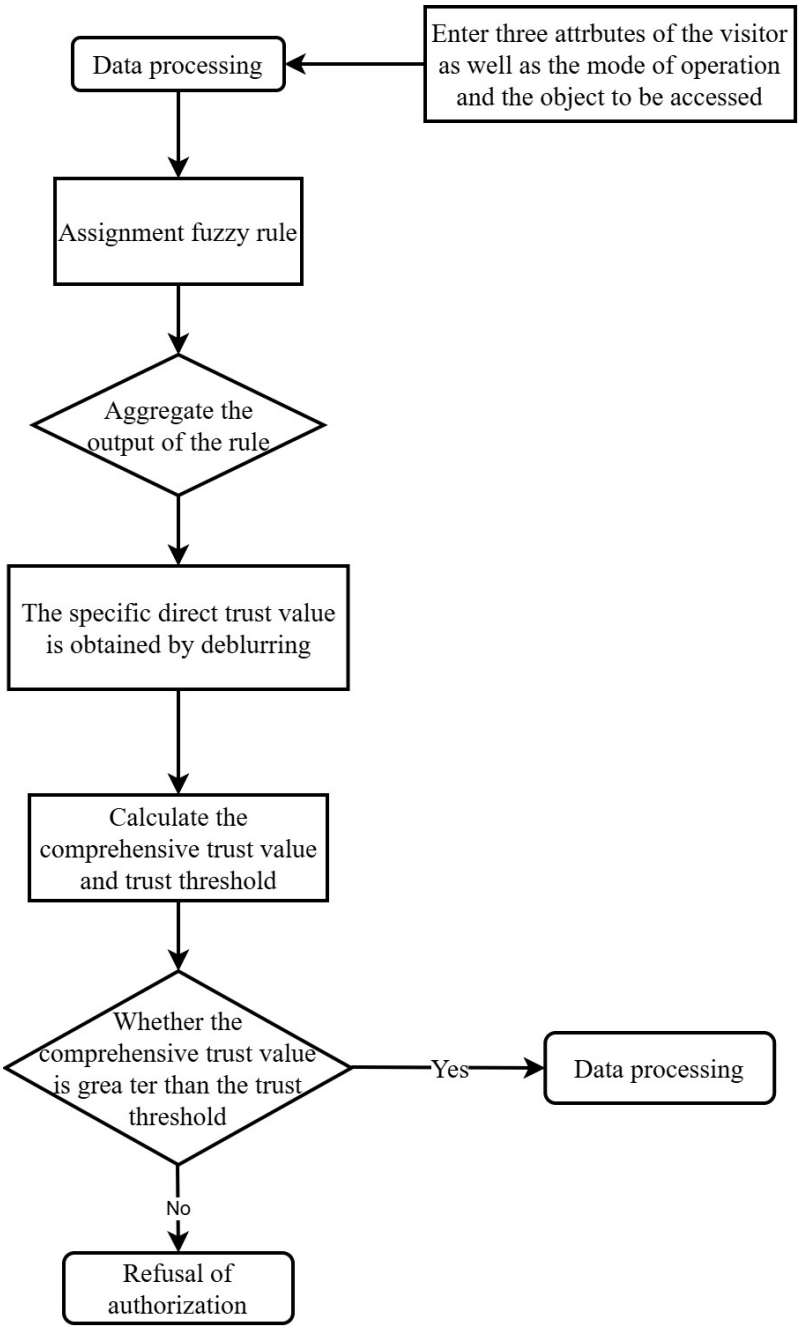

Figure 2. Trust evaluation flow chart

3.3.1. Data Processing

According to the access success rate, the proportion of users' normal behavior and the proportion of trusted requests, these three attribute values are brought into the membership function to calculate the fuzzy set of the three attributes. The membership function is defined as follows:

$$f(x) = \begin{cases} \frac{x-a}{b-a}, a \le x \le b \\ 1, \quad b \le x \le c \\ \frac{d-x}{d-c}, c < x \le d \\ 0, \quad x < a \text{ or } x > d \end{cases} \tag{1}$$

 doi:10.20944/preprints202501.0527.v1

3.3.2. Specify Fuzzy Rules

Having identified the risk and its associated measures, the next logical step is to specify how the risk varies in response to various factors. To this end, a series of fuzzy rules are constructed to explain the relationship between indicators at different levels and risk. These fuzzy rules describe in detail how the access success rate, the proportion of abnormal user behavior, the proportion of trusted requests and the trust degree affect and deduce [20] each other.

3.3.3. Fuzzy Calculation

Input fuzzification, each attribute is converted from a percentage to a membership degree of a fuzzy set according to the fuzzy set and membership function. Fuzzy operation is carried out. After fuzzifying the input data, all the rules that meet the current condition are searched in the rule table made before. For each rule that meets the condition, we will use the operators in fuzzy logic to calculate the membership degree of the confidence under that rule. After the calculation, a membership value representing the credibility is obtained as the output.

The aggregation of rule outputs is performed, which is a process of unifying the fuzzy sets generated by multiple rules into a single fuzzy set. The fuzzy sets derived from each rule (i.e., the membership functions) are aggregated to form a comprehensive fuzzy set. The input of the aggregation process is the membership function calculated by each rule, and the output is a comprehensive fuzzy set of the outcome variable (i.e., confidence degree).

3.3.4. Defuzzification

Determine the final output by calculating the center of gravity of the region bounded by the membership function curve and the abscissa. The combined fuzzy set is used as the input, followed by the computation of the centroid of the region bounded by the membership functions and the abscissa. The formula below describes how to calculate this direct trust value, which is a single, continuous numerical value capable of being directly used in subsequent decisions or system responses.

$$\mathrm{DT} = \frac{\int_0^1 \mathrm{vu}\ (\mathrm{v})\ \mathrm{dv}}{\int_0^1 \mathrm{u}\ (\mathrm{v})\ \mathrm{dv}} \times 100 \tag{2}$$

3.3.5. Calculate and Compare the Comprehensive Trust Value and Trust Threshold

Determine the overall trustworthiness score. The comprehensive trust value is computed by integrating historical dimension data and assigning weights to the immediate trust assessment and that from the previous visit. The formula for calculating the comprehensive trust Value CTi is as shown below:

$$\mathrm{CTi} = \begin{cases} \theta * CT_j + (1-\theta) * DT_i, DT_i \geq CT_j \\ DT_i, DTi < CT_j \end{cases}, \tag{3}$$

$$\theta = e^{-\pi(t_i - t_j)^2} \tag{4}$$

Where, is the time of this request, T_j is the time of the last request; DT_i represents the direct trust level determined by the controller for this particular request, and CT_j is the computed overall trust value at the last request T_j. qIs the Gaussian decay function, and the Gaussian time decay function () is designed to measure the reference valueq [21] of the request.

Next is to calculate the trust threshold. The calculation calculates the trust threshold T_{th} based on the confidentiality and integrity of the target resource and the request type of the visitor. This is from the operation dimension and the object dimension, and the calculation formula is as follows:

$$\mathrm{T_{th}} = \mathrm{MAX}(\mathrm{Op_{con}} * \mathrm{Ob_{con}} * \mathrm{Op_{int}} * \mathrm{Ob_{int}}) \tag{5}$$

 doi:10.20944/preprints202501.0527.v1

Among them, refers to the confidentiality of the customer's access to the target, refers to the completeness of the customer's access to the target. OP represents the impact factor of different operations on resources. The impact factors for different operations are shown in Table 1:

Table 1. Impact factors for different operations

Operation	Confidentiality impact factor	Integrity impact factor
GET	1	0
POST, PUT, DELETE	0	1

Finally, if the calculated aggregate trust value exceeds the trust threshold, the gateway grants access permissions; otherwise, the authorization [18] is denied.

4. Experimental

4.1. Experimental Environment

To evaluate the practical effect of the scheme, this research uses the standard Network communication protocol module built into the Network Simulator 3 platform to build a simulation environment for interaction, simulating terminal server running SPA, accessing gateway server and running SDP controller. The configuration of the specific experimental environment is as follows in Table 2.

Table 2. Experimental environment parameter table

Categories	Name	Description
Hardware	Operating system	Centos7_X64
	CPU	Intel(R) Core(TM) i5-10500
	Running memory	16GB
Software	Programming languages	C++
	Development platform	Visual Studio 2020; Network Simulator 3

4.2. Experimental Evaluation Metrics

In order to evaluate the experimental results, this paper assesses the expenses associated with communication and computation.

The main communication overhead of the proposed scheme mainly comes from the Software-Defined Perimeter controller distributing SPA key agreement parameters to the Software-Defined Perimeter client and the Software-Defined Perimeter gateway, and the Software-Defined Perimeter client authenticating with the Software-Defined Perimeter gateway in a single packet. The specific calculation formula is shown in Eq. (6) :

$$\mathcal{L}_{\text{Cert}} + \mathcal{L}_{\text{SPA}} + 2\mathcal{L}_{\text{Para}} + 2\mathcal{L}_{\text{DC}} + 2\mathcal{L}_{\text{G}} + 2\mathcal{L}_{\text{H}} \tag{6}$$

Where L_{SPA} represents the length of SPA data packet, L_H represents the output length of hash algorithm, L_{Cert} represents the length of TL digital certificate, L_{KEY} represents the length of SPA key, L_{Para} represents the length of SPA key agreement parameters, L_{DC} represents the length of specified signature credential, L_G represents the length of the number of additive group members, L_{ID} represents the length of identity identification.

The computational overhead of the proposed scheme mainly comes from the calculation of SPA key and the generation and verification of specified signature credential. The calculation formula is shown in (7) - (9) :

$$3\mathrm{T}_{\text{bp}} + \mathrm{T}_{\text{enc}} + 2\mathrm{T}_{\text{dec}} + \mathrm{T}_{\text{h}} \tag{7}$$

$$2T_{bp} + 2T_{enc} + T_{dec} + 8T_{ed} + 2T_h \tag{8}$$

 doi:10.20944/preprints202501.0527.v1

$$3T_{bp} + 2T_{enc} + 2T_{dec} + 8T_{ed} + 2T_h \quad (9)$$

Where T_{bp} stands for bilinear mapping, T_{enc} stands for asymmetric encryption algorithm, T_{dec} stands for asymmetric decryption algorithm, T_s stands for signature algorithm, T_v stands for signature verification algorithm, T_{ed} stands for symmetric encryption and decryption algorithm, T_h stands for hash algorithm. Eq. (7) denotes the additional computational cost necessary for SDP controller authentication, Eq. (8) denotes the additional computational cost necessary for SDP gateway authentication, and Eq. (9) represents the computational overhead required for SDP client authentication.

4.3. Experimental Results

4.3.1. Analysis of Communication Overhead Results

Firstly, Network Simulator 3 is used to evaluate the communication overhead of SDP client, SDP controller and SDP gateway authentication after a complete authentication process. Under the same experimental conditions, the proposed scheme is compared with the UDP-based SDP scheme, and the experimental results are as follows:

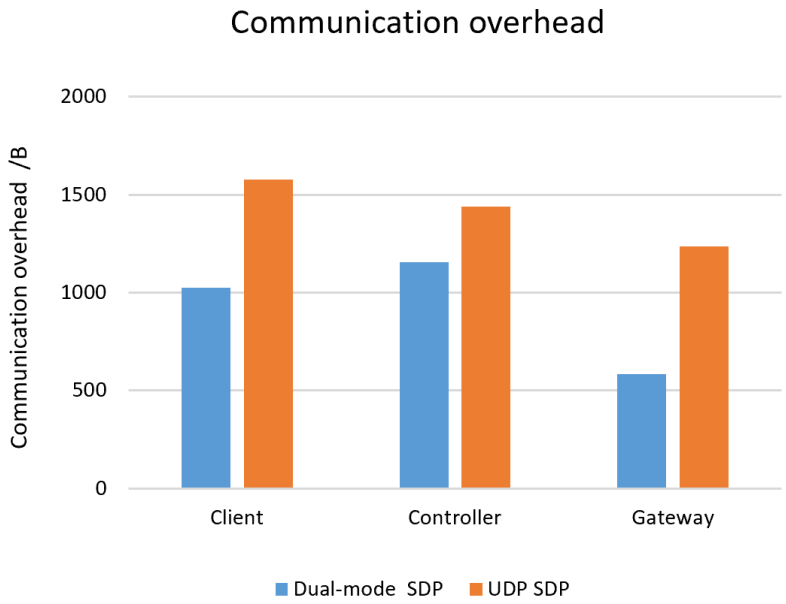

Figure 3. Communication overhead

The traditional UDP SDP scheme requires one-to-one correspondence between authentication information and knock information during authentication. If the IP address in the SPA knock packet is in the SNAT environment, the returned information cannot be associated with the real access terminal, which will generate additional communication overhead. In this scheme, UDP and TCP are combined, and the SPA knock packet sent contains more abundant information, which can accurately establish a connection for each TCP and complete the knock action, and greatly improve the accuracy of access authentication. The outcomes of the experiments indicate that the communication overhead of the proposed scheme to perform a complete dual-mode single-packet access authentication is 2764B, and the communication overhead of the UDP-based SDP scheme to perform a complete single-mode single-packet access authentication is 4362B. Compared with the UDP-based SDP scheme, the communication overhead required by the proposed scheme is reduced by 37%.

4.3.2. Analysis of Time Cost Results

To assess the effectiveness of our approach, we use the average authentication delay from the initiation of authentication request to the completion of anonymous authentication as the performance

 doi:10.20944/preprints202501.0527.v1

index, and build a simulation environment based on Network Simulator 3. The environment is initialized with different numbers of clients and gateways, and the fundamental settings for the experimental parameters are presented in the Table 3

Table 3. Experimental parameters

Simulation parameters	Parameter values
Number of SDP clients	50; 100; 150; 200; 250; 500
Number of SDP gateways	5; 10; 15; 20; 25; 50

This experiment assumes that the SDP gateway and SDP client have been online, and simulates the behavior of dual-mode single-packet access authentication. The number of SDP clients is set to 50, 100, 150, 200, 250, 500, and the corresponding number of SOP gateways is 5, 10, 15, 20, 25, 50, respectively. In order to make the experiment closer to the real environment, the access frequency was randomly accessed according to the preset number. The network data transmission data is set to 4Mbps. The average authentication latency comparison is shown in the Figure 4.

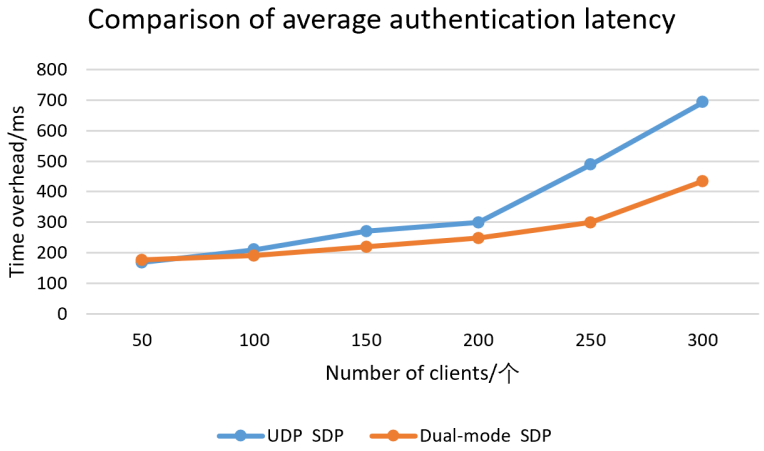

Figure 4. Average Authentication Latency Comparison

The figure illustrates that as the quantity of SDP clients rises , the access frequency increases, and the SDP gateway sends requests to the controller frequently. The method adopted by the SDP gateway in this scheme has stronger precomputation ability, so the time overhead is effectively reduced. The findings from the experiment indicate that the time overhead of the proposed scheme is gradually better than that of other single-mode single-packet authentication schemes when the number of clients increases. In the case of 500 SDP clients and 50 SDP gateways, the time overhead of the proposed scheme is 783ms, while the time overhead of the UDP-based SDP scheme is 1324ms. Compared with the UDP-based SDP scheme, the time overhead of the proposed scheme is reduced by 41%.

5. Conclusions

Zero-trust security protection applications have defects, network risks are diverse, and user identity authentication and privacy protection are urgent. In this case, the proposed dynamic anonymous access control method based on dual-mode single-packet authentication performs well, can withstanding numerous types of attacks attacks, and the security exceeds the existing software-defined boundary (SDN) schemes. Compared with other single-packet authentication schemes, the proposed scheme offers greater benefits in communication overhead and computational overhead, and the access efficiency is further improved.

Funding: This study was supported by the National Key Research and Development Program of China (Project No. 2022YFB3104300).

 doi:10.20944/preprints202501.0527.v1

References

1. You, H., Ko, D., Kim, D., et al. Dynamic access control method for SDP-based network environments. *EURASIP J. Wirel. Commun. Netw.* **2023**, *2023*, 94.
2. Li, Z., Wang, P., Wang, Z., et al. Flowgananomaly: Flow-based anomaly network intrusion detection with adversarial learning. *Chin. J. Electron.* **2024**, *33*, 58–71.
3. Xu, M., Chen, B., Tan, Z., et al. AHAC: Advanced Network-Hiding Access Control Framework. *Appl. Sci.* **2024**, *14*, 5593.
4. DeCusatis C., Liengtiraphan P., Sager A., et al. Implementing zero trust cloud networks with transport access control and first packet authentication. In Proceedings of the IEEE International Conference on Smart Cloud (SmartCloud), New York, USA; Pagination: 5-10.
5. Eidle D., Ni S. Y., DeCusatis C., et al. Autonomic security for zero trust networks. In Proceedings of the IEEE 8th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference (UEMCON), New York, USA; Pagination: 288-293.
6. Yang, Y., Wu, Z., Yang, Y., et al. A survey of information extraction based on deep learning. *Appl. Sci.* **2022**, *12*, 9691.
7. Baldi, M., Battaglioni, M., Chiaraluce, F., et al. A new path to code-based signatures via identification schemes with restricted errors. *arXiv preprint arXiv:2008.06403* **2020**.
8. Shen, Q., Shen, Y. Endpoint security reinforcement via integrated zero-trust systems: A collaborative approach. *Comput. Secur.* **2024**, *136*, 103537.
9. Huang W., Xie X., Wang Z., Feng J., Han G., Zhang W., ZT-Access: A combining zero trust access control with attribute-based encryption scheme against compromised devices in power IoT environments, *Ad Hoc Netw.* **2023**, *145*, 103161, ISSN 1570-8705.
10. Li Z, Zhang Z, Fu M, et al. A novel network flow feature scaling method based on cloud-edge collaboration. In Proceedings of the IEEE 22nd International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), Location of Conference, Country, 2023; Pagination: 1947-1953.
11. Wang Z X, Li Z Y, Fu M Y, et al. Network traffic classification based on federated semi-supervised learning. *J. Syst. Archit.* **2024**, *149*, 103091.
12. Syed N F, Shah S W, Shaghaghi A, et al. Zero trust architecture (zta): A comprehensive survey. *IEEE Access* **2022**, *10*, 57143–57179.
13. Wang F, Li G, Wang Y, et al. Privacy-aware traffic flow prediction based on multi-party sensor data with zero trust in smart city. *ACM Trans. Internet Technol.* **2023**, *23*, 1–9.
14. Major W, Buchanan W J, Ahmad J. An authentication protocol based on chaos and zero knowledge proof. *Nonlinear Dyn.* **2020**, *99*, 3065–3087.
15. Xu M, Guo J, Yuan H, et al. Zero-Trust Security Authentication Based on SPA and Endogenous Security Architecture. *Electronics* **2023**, *12*, 782.
16. Mahmood K, Arshad J, Chaudhry S A, et al. An enhanced anonymous identity-based key agreement protocol for smart grid advanced metering infrastructure. *Int. J. Commun. Syst.* **2019**, *32*, e4137.
17. Tang F, Ma C, Cheng K. Privacy-preserving authentication scheme based on zero trust architecture. *Dig. Commun. Netw.* **2024**, *10*, 1211–1220.
18. Zhiyu Chen, Longchuan Yan, Zitong Lü, Yanling Zhang, Yonghe Guo, Wenjing Liu, Jiaxing Xuan. Research on Zero-trust Security Protection Technology of Power IoT based on Blockchain. *J. Phys.: Conf. Ser.* **2021**, *1769*, 012039.
19. Chen B, Qiao S, Zhao J, et al. A security awareness and protection system for 5G smart healthcare based on zero-trust architecture. *IEEE Internet Things J.* **2020**, *8*(13), 10248–10263.
20. Tang Fei, Pang Junjie, Cheng Kefei, et al. Multiauthority traceable ring signature scheme for smart grid based on blockchain. *Wirel. Commun. Mob. Comput.* **2021**, *1*, 1–9.
21. Wang Min, Zhang Yuexin, Ma Jinhua, et al. A universal designated multi verifiers content extraction signature scheme. *Int. J. Comput. Sci. Eng.* **2020**, *21*, 49–59.