Journal of Combinatorial Mathematics
and Combinatorial Computing
www.combinatorialpress.com/jcmcc

Study on the Application of SPA-based Single Packet Knocking Technology in Network Security Protection and Resistance Efficacy against DDOS and Web Attacks

Wei Gao[1,✉]

[1] *State Grid Shanxi Electric Power Company, Taiyuan, Shanxi, 030000, China*

ABSTRACT

In response to cybersecurity threats such as security breaches, data leakage, supply chain attacks, and ransomware viruses in digital network environments, more reliable cybersecurity architectures are needed to address these challenges. The article builds a zero-trust firewall applied to network security protection based on zero-trust architecture by integrating SPA single-packet authorisation technology and authentication scheme. Then SPA single packet authorisation technology with SM3 hash algorithm and SM4 algorithm for fully nominal encryption processing is constructed as a network security protection scheme, and the authentication protocol and trust evaluation algorithm are established by using hash and different-or function. In the simulation verification results, the communication volume of SDP client to complete one authentication is 981B, which reduces 27.17% compared to WaverleySDP overhead. The server in the SDP+SPA scenario still retains a certain amount of legitimate data after DDOS attacks and Web attacks, and receives only 53.47% of the traffic of the SDP scenario. The CPU usage of the client deployed with SPA is only 11.47 percentage points higher than that without SPA mechanism. The combination of SPA single-packet knocking technology and zero-trust architecture can achieve network security protection, and can also effectively deal with DDoS and Web attacks, and improve the performance of network security protection.

Keywords: zero-trust architecture, SPA single-packet authorization, hash algorithm, network security protection, DDoS attack

1. Introduction

Cybersecurity is the guarantee of national security, and there can be no national security without cybersecurity. Artificial intelligence is disrupting and changing all areas of human society. This has led to it being called the core technology of the fourth industrial revolution [1-3]. In terms of network security, the double-edged sword effect of AI is particularly obvious; it is irreplaceable in enhancing network security defence capabilities, but at the same time it can be exploited to launch more

✉ Corresponding author.
E-mail address: 1850199706@163.com (W. Gao).
Received 25 March 2024; Revised 05 June 2024; Accepted 30 November 2024; Published Online 15 April 2025.
DOI: 10.61091/jcmcc127a-174

sophisticated and covert attacks that threaten network security. It is of great significance to deeply study and analyse the network security problems and protection in the era of artificial intelligence [4-7].

Since the end of 2022, the generative AI centred on big models has triggered a new round of revolution in the industry, and AI is gradually changing the 'rules of the game' in various industries, including the field of cyber security [8-10]. Targeted attacks, ransomware attacks, zero-day attacks and other increasingly sophisticated and advanced threats pose a serious challenge to enterprise information, assets and operations. From the perspective of enterprises, with the advancement of the digital transformation process, enterprises are facing more cybersecurity challenges [11-14]. The reason for this is that in the process of digital transformation, many enterprises have begun to migrate their assets from the data centre to the cloud, and it may not be just 'a cloud', but a 'multi-cloud' environment. In addition, hybrid office represented by online office is becoming mainstream [15-17]. When employees work in the office, they can build a 'moat' through the firewall. When the mobile office, the attack surface has changed greatly, because many applications are deployed in the cloud, the attacker has more opportunities to launch advanced attacks, the progress of AI technology makes these attacks faster and faster, more and more accurate, which leads to more and more complex network attacks [18-21].

SPA technology is mainly in the network communication layer to protect the back-end services after the firewall, which can be regarded as the access protection of the communication layer, SPA can effectively prevent the risk of untrusted packets. In this paper, based on the zero-trust general architecture and zero-trust protection process, combined with the SPA single-packet authorisation and authentication scheme to establish the zero-trust, the firewall hash algorithm and the whole encryption processing algorithm is applied to the establishment of the security protection SPA scheme. Define the trust value calculated by the trust evaluation algorithm in zero trust, and build a network security authentication protocol combined with SPA single-packet knocking technology to provide support for enhancing network security protection. For the effectiveness of the network security protection scheme designed in this paper, simulation tests are carried out from multiple dimensions, such as communication efficiency, SPA scheme, and security performance.

2. Zero-trust architecture and authentication and authorisation techniques

Identity authentication is the pillar of network security architecture, is the basic step of the zero-trust journey, is a kind of identification of the operation of the user whether the user has the legitimate access and application rights, to ensure that the maintenance of the computer system resources security and other network data resources security absolute core security. Zero Trust is a conceptual approach to effectively protect the security of modern IT network environments by establishing a complete and detailed identity management and access rights system to uniquely confirm identity to create an absolutely secure network. Based on the zero-trust architecture, combined with SPA single-packet authorisation technology, the construction of network security protection strategy aims to enhance the network's ability to prevent security threats.

2.1. Zero Trust Architecture Technology

2.1.1. Zero Trust Generic Architecture. The principle of zero trust considers any area of the network as malicious, any environment as a security threat, intruders at any time, and users, devices, networks, etc. in the system as untrustworthy, and no longer divides protection zones between the intranet and extranet or relates to the location of the entity. According to the idea of zero trust, access requests made by access subjects to access objects (data, services, etc.) should be denied by default [22]. Since identity can uniquely represent a user (person), service (software), device, etc., the zero-trust-based design of the system requires full and thorough identity acquisition of the user, service, device, etc. of

the access subject, authentication of its identity, and judgement of its security status; and then, by acquiring the access subject's actual needs and the attributes of the access object, it grants the access subject the least privilege.

The generic architecture derived from the principle policy of zero trust is shown in Fig. 1. The policy selection is dynamic and continuous, and requires comprehensive judgement based on various types of environments in the system, such as resource data, the importance level of services, and so on. A secure and reliable network environment is also required for policy determination and continuous authentication and authorisation of entities.

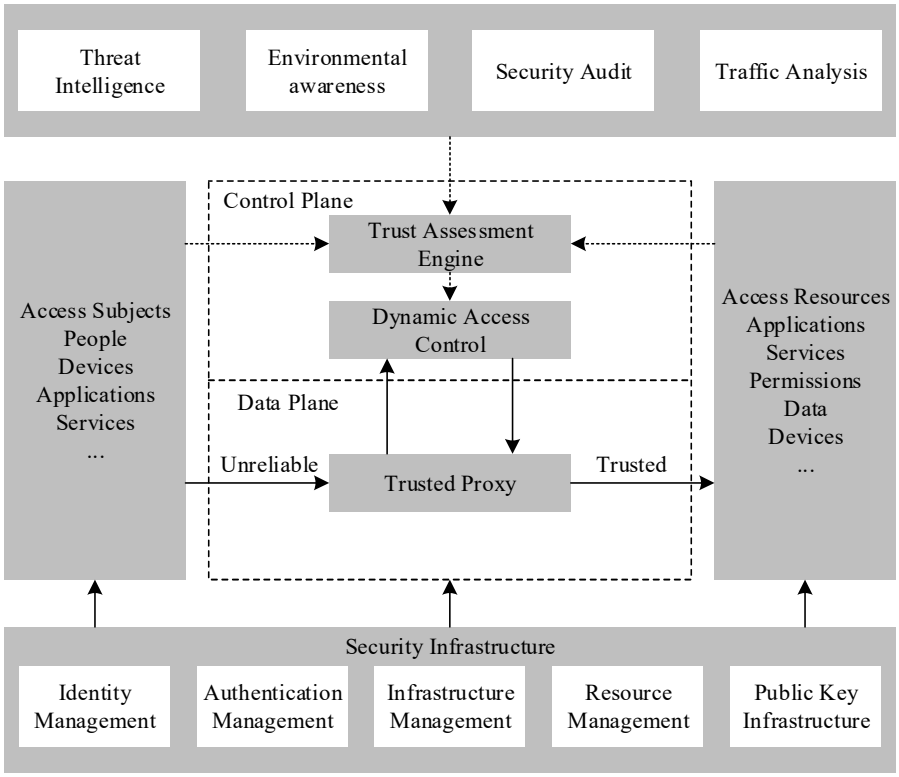


Fig. 1. Zero trust general architecture

When accessing any resource in the system, any accessing entity in the physical and network locations of the mission should be authenticated and authorised. There is also a need to continuously assess the security status of all participating objects in the system, secure channels should be established for each access request in the system, and the policy for granting permissions to accessing entities should dynamically enforce the principle of least privilege.

2.1.2. Zero Trust Protection Process. Defence of network security is based on zero trust mechanism, which forms a zero trust model based on key components of zero trust network and calculates the trust score of visitors. The zero-trust security protection process is shown in Figure 2, and the framework includes the data level for transmitting actual data and the control level for establishing trust. Security policies are implemented through the access control engine for authorisation of access requests, and the dynamic access control engine allows flexible and fine-grained access control for users based on the user trust provided by the trust assessment component.

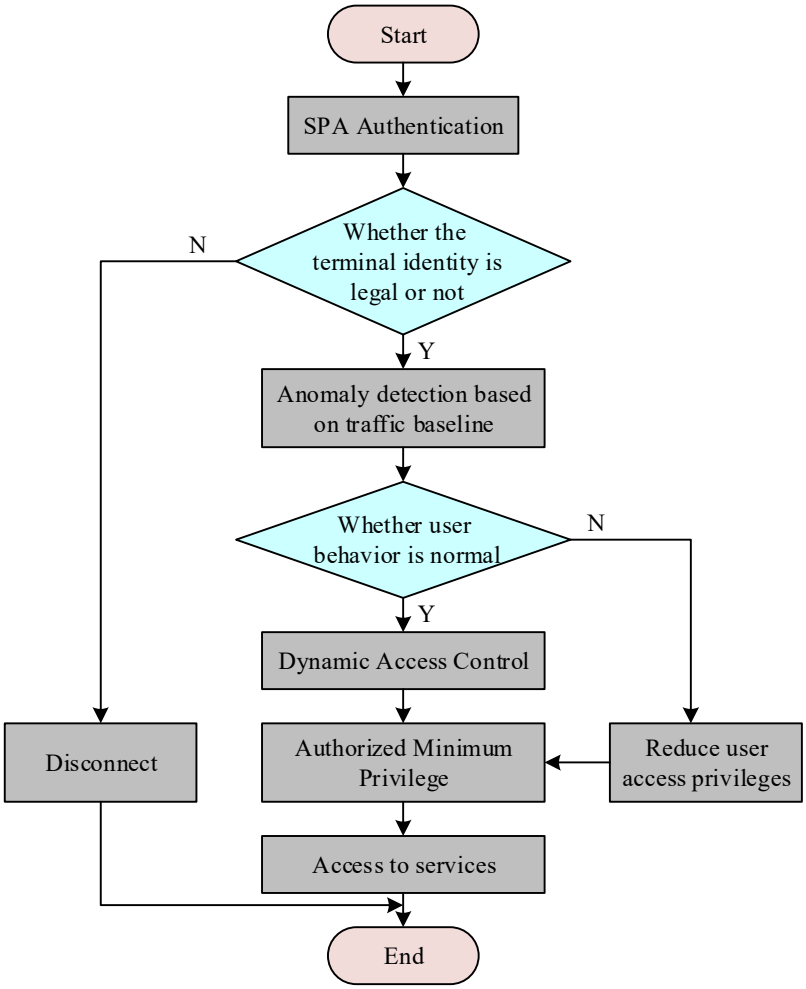


Fig. 2. Zero trust protection process

When a user gains access through the control plane, he or she can interact with the industrial control system through the data plane. The trust evaluation component will continuously evaluate the user access behaviour to ensure that the network traffic is trusted and the user behaviour is trusted. Each event and each operation of the control plane will be recorded, which is used to complete the audit work based on the access flow or access request, and to construct the decision-making, implementation, and anomaly defence disposal of the dynamic access control policy. The specific steps are as follows:

1) User device application authentication. When users access the network system through terminals, they first carry out basic identity authentication through the RADmS server, terminal device authentication server, and system application authentication server.

2) Continuous trust assessment. After the user has passed the identity authentication, the trust assessment component retrieves the user's historical behavioural data information in the trust value database, and the trust assessment component accepts the user behavioural data sent by the trust assessment component. And it sends the calculated user trust value to the dynamic access control engine to determine the user's direct trust level according to the trust metric database.

3) Least privilege access control policy formulation. A user accessing the network system is granted the least privilege required to complete the task, rather than being granted the privileges that the entity wants. If higher access privileges are indeed needed, then the user can and will only be granted those privileges when needed.

2.2. SPA Single Packet Knockout Technology

2.2.1. SPA single package authorization. Single Packet Authorization Authentication (SPA) is a core feature in the zero-trust Software Defined Perimeter (SDP) framework.SPA belongs to a new generation of port knocking technology, which stores authentication messages in packets and transmits them to the server, and dynamically adjusts the opening policy of the firewall ports by setting up a series of rules [23]. The SPA technology can be used in combination with a variety of security technologies to enhance the overall solution's security capabilities.The authentication process of SPA is shown in Figure 3.Typically, SPA packets use the UDP protocol to initiate authentication.

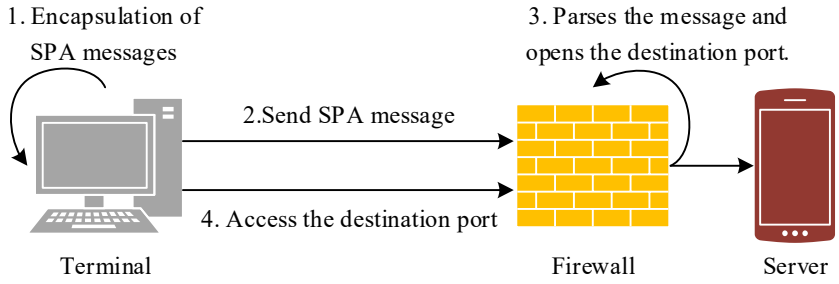


Fig. 3. SPA authentication process

1) SPA client encapsulates SPA messages. The client sends the packet through the shared key and random number, after calculating the SPA key based on the HOTP algorithm defined in RFC4266, and packages it into a UDP data message together with the client ID, random number, timestamp, client IP, and port. Then the HMAC algorithm is used to generate the message digest.
2) The client sends the SPA packet to the server.
3) The server parses the packet and opens the port. When the server receives the SPA packet, it first verifies the message digest to prevent replay attacks. If it is found to be different from the previously received valid message digest, no action is performed. If it is the same, the SPA key is calculated based on the timestamp in the received UDP message, the IP of the client, and the service password stored internally in the server, and compared with the received one, and if it is the same, the service port for the client to apply for access is opened.
4) Client accesses the destination port.

2.2.2. SPA certification programme. When a new device joins the network, the server side will uniformly collect the information of the terminal device, such as user name, IP address, MAC address and operating system, and other basic information, and at the same time negotiate the shared key, and store this information in the server database.
1) Client SPA sending process. When the terminal device wants to access the server, it needs to encapsulate the SPA packet and then send it to the server in the following steps:

Step1 Generate 4-digit 7-bit random numbers and time stamps by using the programme that comes with itself, and generate one-time password STOP by algorithm.

Step2 Collect its own MAC address and OS version number to form the device face field.

Step3 Encapsulate the resource information requested by itself into the message field.

Step4 Use SHA-256 algorithm to hash the first seven fields [Random Number: Username:Timestamp:STOP:IP Address:Device Face:Message] in the packet to get the digest field, which is used for server-side integrity verification.

Step5 At this time all eight fields are ready, encrypt all the fields using field encryption algorithm to get the ciphertext d.

Step6 Encapsulate the ciphertext d as a data part into a UDP datagram and send it to the server.

2) Server SPA authentication process. After the server senses the SPA datagram, it will check the datagram and authenticate the sender in the following steps:

Step1 Parse the UDP packet and remove the first part to get the ciphertext d.

Step2 Decrypt the ciphertext d using the supporting field decryption algorithm to get the plaintext m.

Step3 Perform SHA-256 hash computation on the first seven fields of m to get m. Compare it with the eighth field in m. If they are equal, it passes the integrity verification and continue with the following steps, otherwise discard the packet.

Step4 Compare the timestamp field in m with the current time to check whether it is timeout or not, if it is timeout discard the packet.

Step5 Check whether the user name, IP address, and device face fields correspond to the recorded data in the server database, if not, discard the packet.

Step6 Extract the random number, timestamp and IP address in the packet, generate the one-time password STOP' by the same algorithm, compare it with STOP in m, if it is different then discard the packet.

Step7 Authentication passes.

3. SPA certification programme for cybersecurity protection

With the development of the Internet and the popularity of mobile smart terminals, the security of the network is becoming more and more important. At present, the identity authentication for network security is still based on passwords, and there are many shortcomings in this authentication method. Once the password is obtained by an attacker, he can obtain any information in the network. And since most of the applications in the network nowadays do not do more authentication after unlocking, the attacker is even able to obtain the user data stored in the cloud. Therefore, this paper proposes a security protection scheme under SPA single packet authorisation technique based on zero trust framework to provide support for improving network security protection.

3.1. Security Protection SPA programme

3.1.1. Zero Trust Firewall. Distinct from classic firewalls, the Single Packet Authorisation Zero Trust firewall runs a daemon to accept authentication data sent by clients. By default, the firewall is in the denied access state. After successful verification of the authentication data, the single-packet authorisation firewall temporarily generates appropriate permission rules to allow the client to initiate a connection, and automatically removes the temporary permission rules after a timeout, which is usually set to a short period of time. The firewall daemon should also keep track of established connections and their associated connections and allow them to remain connected until the connection is dismantled.

1) After initialisation of the client, it is necessary to pre-synchronise the relevant encryption and message digest algorithms used for decryption and message digest authentication, the relevant keys, etc. This step can be implemented via a static configuration file without the need to transfer keys across the network. The client constructs the SPA authentication message and sends it to the client. The content of the authentication message that is in the encrypted load can be agreed upon by the server and the client in advance, for example, it can contain the user name, the content of the policy that is temporarily permitted by the firewall, the timeout duration, and so on.

2) After the initialisation of the server side, it is also necessary to pre-synchronise the relevant encryption and message digest algorithms used for decryption and message digest authentication, the relevant keys, etc. This step can be realised through a static configuration file. The server side first sets the firewall to the default no-access state and runs the SPA authentication daemon. The server side receives the SPA message sent by the client, performs message digest verification and decryption, and

also authenticates the decrypted data. Usually single packet authorisation firewalls can be set to target connections that fail authentication without returning any information to the client, which can effectively avoid further information collection by attackers. For clients with successful authentication, the SPA daemon generates a temporary firewall allow access policy and deletes it immediately after a timeout. At this point, the server can be connected by the client normally, the server tracking has been successfully established by the client connection, and keep allowed to the client disconnect.

3.1.2. Security protection programme. Based on the zero-trust framework and combining the zero-trust firewall with SPA single packet authorisation technology, this paper establishes a dual-mode SPA single packet knockdown security protection scheme for network security protection, and its specific architecture is shown in Figure 4. The dual-mode SPA single-packet knock mechanism discards unauthorised packets by default, so that unauthorised clients cannot perceive valid IPs and ports, and protects important digital resources of information system extranets and private networks.

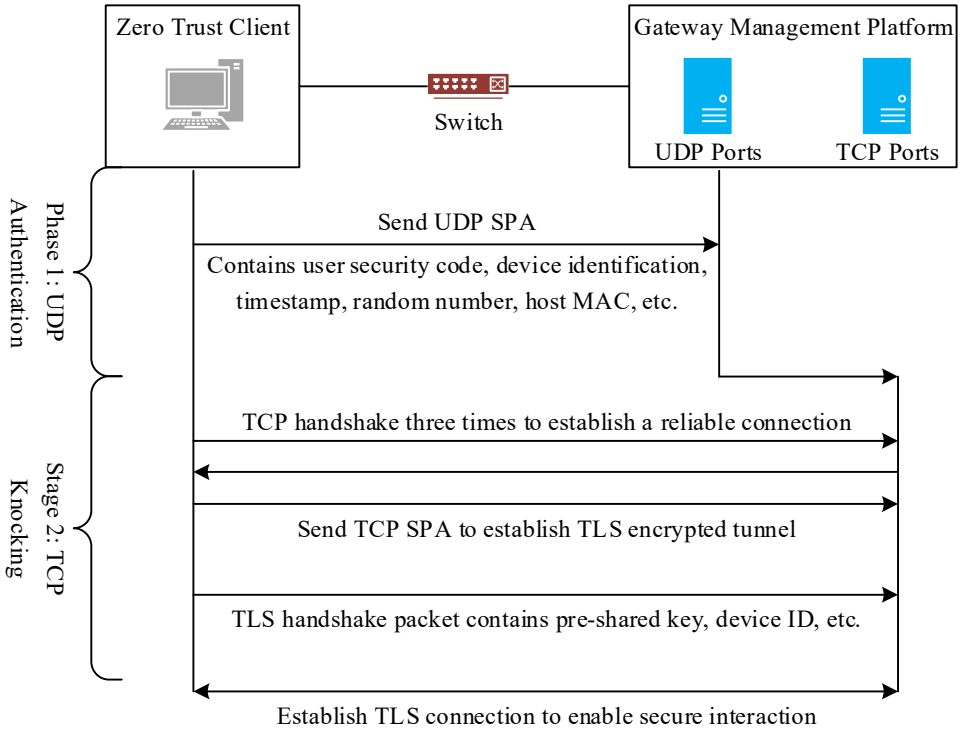


Fig. 4. Dual mode SPA scheme authorization sequence diagram

The network security protection scheme under the dual-mode SPA single packet knocking mechanism can be divided into two phases, UDP authentication and TC knocking. The details are as follows:

1) UDP authentication phase. The client under zero-trust architecture sends knock packets to the SDP controller. The knock packet mainly contains user security code, device identification (MAC address, computer name), timestamp, random number and host MAC value. To ensure transmission security, the user security code is encrypted using the SM3 hash algorithm, and the device identification is processed using the SM4 algorithm for full-name encryption.The SM4 algorithm contains the steps of round function, round key expansion, and round iteration to provide high-strength data protection.

Device Identifier Plaintext Input (L_0, L_1, L_2, L_3) A total of 32 rounds of 128 bits of data, the round key is represented as:

$$R_i (i = 0, 1, \ldots, 31) \tag{1}$$

Derived using the SM4 algorithm encryption:

$$L_{i+4} = L_i \oplus T(L_{i+1} \oplus L_{i+2} \oplus L_{i+3} \oplus R_i) \quad (2)$$

Where $\oplus$ is the different-or operation and T is the non-linear transformation of the encryption algorithm.

The device identification code is encrypted by SM4 and the output ciphertext is:

$$(M_0, M_1, M_2, M_3) = (L_{31}, L_{30}, L_{29}, L_{28}) \quad (3)$$

So as to guarantee the security of the knocking process of the terminal equipment.

2) TCP knocking phase. Under the zero-trust security architecture, the SDP gateway will dynamically update the local firewall rules according to the UDP knock request and temporarily open the TCP port for the client to use.

In order to complete SPA knock authentication, the client needs to communicate using TCP knocking. The client establishes a connection with the SDP gateway using the TCP three times handshake and makes the packet carry a dynamic token by adding the SPA token to the TLS field. After receiving the TLS handshake request, the server authenticates the SPA token, and if the authentication is successful, the TLS handshake is established successfully, otherwise the connection is disconnected. The TLS handshake packet sent by the client contains information such as the user's pre-shared key and device identification. The server verifies the SPA packet information in the extended field of the TLS handshake packet; if the verification is successful, the TLS handshake is established successfully. At this point, the trust link between the client and the SDP gateway is formally established, and secure data interaction can take place.

3.2. Authentication Protocol Construction

3.2.1. Authentication protocols. This paper combines Internet application scenarios, introduces the zero-trust security concept into the design of identity authentication protocol, and proposes an identity authentication protocol (hereinafter referred to as the protocol) based on zero-trust security control points. By analysing actual network security incidents, it is found that attacks or abnormal behaviours of internal users usually occur when users log in off-site, and malicious users make use of internal user accounts to tamper with system information and modify users' personal data through off-site logins, which usually contain two kinds of login device abnormalities and login address abnormalities. Therefore, this protocol adds these two factors as strict security control conditions into the design of the protocol, so that they participate in the key negotiation and calculation process of the entire protocol. Maximum restriction on user access conditions from the protocol level makes the whole network more secure from the authentication protocol stage, which in turn improves the security of the whole network [24].

At the same time, due to the particularity of the Internet, its requirements for data security are also higher, the security protocol for the wireless body area network should meet the hierarchical protection of data, and the operation authority should also be graded, and the access to different data and devices should meet the corresponding security level requirements, so this agreement is designed to minimize authorized access to protected resources (such as data, computing resources and applications) by adding a user-device matching authentication table. Even if an attacker attacks from within the system, the threat to the rest of the network is greatly reduced.

In addition, in order to meet the requirements of the Internet information transmission low latency, the various stages of this protocol are completed only by the hash and the heterodyne function computation, in order to ensure the security of the premise of the completion of the entire protocol of the lightweight design, but also saves a certain amount of network computing resources. Finally, this protocol also meets the three-factor authentication and other characteristics, with the ability to resist most network attacks.

3.2.2. Trust assessment algorithms. Define the trust value V calculated by the trust evaluation algorithm in Zero Trust as a number between 0 and 1, i.e., $V \in [0,1]$. Remember that the user's historical trust value is V_P, the user's latest trust value is V_N, and the trust value based on the authentication method and the result of the authentication is V_C, and if the authentication fails, the value of V_C is 0. Based on the level of security of each authentication method, the trust value of each authentication method will be evaluated by an expert V_C. The algorithm flow is as follows:

$$W = [1 - V_P, V_P] \tag{4}$$

$$M = [V_P, V_c]^T \tag{5}$$

$$V_N = W \times M \tag{6}$$

In this scheme, the trust level is divided into four levels, i.e., full trust, high level trust, low level trust and no trust at all, with value domains of (0,7,1.00], (0,5,0.7], (0,2,0.5], and (0,0,0.2], respectively.

Let the user history trust value be V_P:

$$-V_P^2 + V_P(1 + V_C) \tag{7}$$

For a more intuitive view, the above equation is reduced to:

$$-x^2 + x(1 + c) \tag{8}$$

Then its derivative is:

$$-2x + 1 + c \tag{9}$$

From equation (8), it can be seen that equation (9) obtains the maximum value $(1+c)^2/4$ at $x = (1+c)/2$. In this scheme, the definition domain of setting V_P, V_C is [0,1], so the maximum value that can be obtained by equations (7) and (8) is 1, and the minimum value is 0. The result still falls into the closed interval [0,1]. Therefore, the trust evaluation algorithm designed in this scheme satisfies the requirement in zero trust, which is called closed set property. Its monotonicity is proved as follows:

Let the definition domain of x in Eq. (8) be $[0,c]$, where $c \in [0,1]$. Then there are:

$$0 \le x \le c \le \frac{(1+c)}{2} \tag{10}$$

From Eq. (9), it can be seen that the value computed in Eq. (8) is monotonically increasing at $x \in [0,c]$ and achieves its maximum value at $x = c$, c. The above process, apart from proving the monotonicity of the function, also yields a very nice property, which is that we can constrain the final value of the trust value by bounding the range of V_C. That is, when $V_C \ge V_P$, the value obtained by this trust evaluation algorithm will not exceed V_C.

4. Example of SPA certification for network security protection

In order to solve the security risks such as blurred network boundaries and easy failure of the access mechanism when accessing resources through network security, a zero-trust platform is built as a bridge to network resources. Based on the zero-trust framework, the SPA single-packet knock mechanism is taken as the core, and the dynamic authorisation mechanism with identity, environment, behaviour, software and hardware as the evaluation factors is established, which realises the terminal access to network resources under minimum authorisation, micro-isolation, dynamic authorisation and continuous monitoring. Therefore, this paper is based on the zero-trust architecture, through the single-packet authorisation knock verification mechanism, with a view to solving the network security problems brought about by the technology.

4.1. Communication efficiency and SPA testing

4.1.1. Protocol communication efficiency. The main communication overhead of this paper's scheme mainly comes from the SDP controller distributing the SPA key negotiation parameters to the SDP client and the SDP gateway as well as the single packet authorisation authentication between the SDP client and the SDP gateway. The hash algorithm and the symmetric encryption algorithm used in this paper are SM3 and SM4, and their output lengths are 64B and 32B, respectively.The communication overheads required for a client to complete a single authentication are obtained by choosing the improved SDP architecture and the Waverley SDP as the comparative schemes, as shown in Table 1. Compared with WaverleySDP, the improved SDP architecture provides security enhancements to the original SDP architecture, but the communication overhead is still significantly higher than the scheme in this paper due to the lack of a relatively efficient SPA key distribution scheme. Unlike WaverleySDP, where both parties need to establish a TLS secure channel with the SDP controller to obtain the SPA key every time the SDP client accesses the SDP gateway, this paper's scheme completes the distribution of the SPA key negotiation parameters in one go at the time when the SDP client or the SDP gateway goes online, thus effectively reducing the communication overhead.The amount of communication required for the SDP client to complete authentication is 981B, compared to the amount of communication required for the SDP client to complete authentication. Is 981B, which reduces the overhead by 27.17% compared to WaverleySDP.

Table 1. Communication overhead for authentication

Scheme	Communication overhead	Traffic volume
Improved SDP	2LCert+LSPA+2LKEY+LID	1503B
WaverleySDP	2LCert +LSPA+4LH+2LKEY+2LID	1347B
This article	LCert+LSPA+2LPara+2LDC+2LG+2LH	981B

In this paper, the communication overhead required by each participant to perform a complete authentication process for this paper's scheme, the improved SDP architecture scheme, and WaverleySDP is tested in a simulation environment based on the Network Simulator platform.The interaction between SDP clients, SDP controllers, and SDP gateway nodes is performed using the built-in standard network communication protocol modules built into the Network Simulator platform to simulate the real network environment and improve the accuracy of the experimental data. Figure 5 shows the communication overhead comparison results of different authentication protocols.

The experimental results confirm that this paper's scheme reduces the number of times of establishing TLS secure channel, which can significantly optimise the communication overhead of SDP client and SDP gateway, and the communication overheads of its participants are 1019 B and 598 B. In addition, this paper's scheme optimises the distribution process of SPA key, which can reduce the communication overhead of the SDP controller by a small margin. Overall, compared to WaverleySDP, the communication overhead required by this paper's scheme to perform a complete authentication process is reduced by 33.67%. This indicates that the authentication protocol designed in this paper can effectively reduce the authentication communication overhead of network security and improve the authentication communication efficiency.

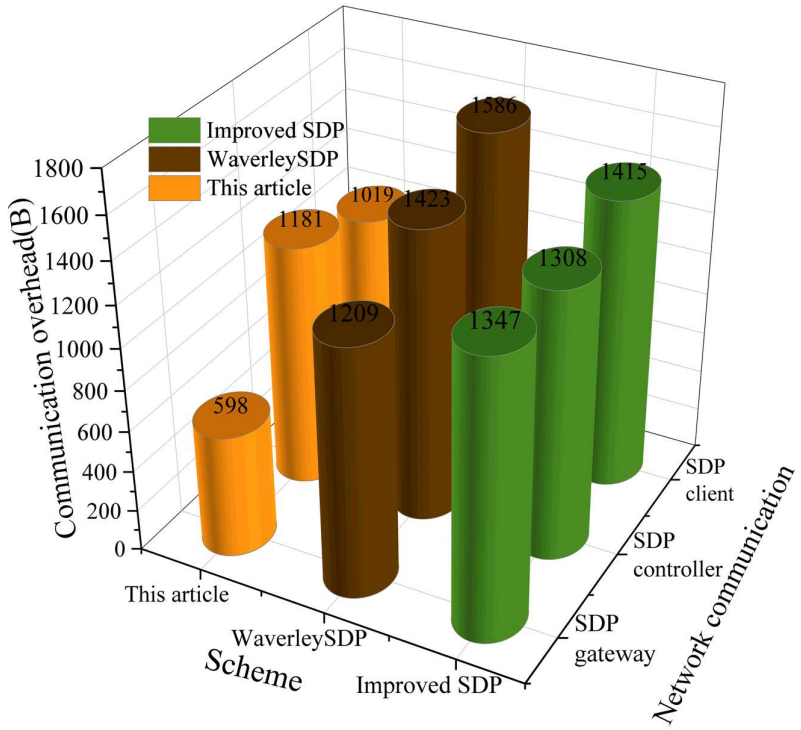


Fig. 5. Comparison of Communication Overhead

4.1.2. Comparison of SPA tests. In order to verify the performance of the SPA scheme, a test environment is set up to simulate the terminal server and access gateway server for simulation verification. The server operating system is Centos7_X64, and the configuration is Intel(R) Xeon CPU E3-1230 @2.40 GHz.The simulated terminal server runs SPA and IH client programs, and the access gateway server runs SDP controller and AH server programs. Both the client and server are written in Linux C language. The experiment simulates the time consumed by the access gateway to complete single-packet authorisation and secure access under different numbers of terminals, and compares this paper's SPA protocol with FWKNOP and OPENSPA protocols, and Figure 6 shows the comparison results.

With the increase of the number of terminals, the SPA protocol of this paper is significantly better than OPENSPA protocol and FWKNOP protocol. When the number of terminals is 10000, the running time of FWKNOP protocol and OPENSPA protocol is 1.33 times and 2.29 times than that of SPA protocol in this paper, respectively. Therefore, the SPA protocol in this paper is more suitable for single-packet authorisation of a large number of terminals on the Internet. In addition, through the analysis of packet capture, it can be seen that OPENSPA protocol consumes 2447B to complete a request and response, and FWKNOP protocol consumes 1376B to complete a request and response, but the configuration of FWKNOP protocol is more complicated, and it needs to generate the access key of the device in advance.OPENSPA and FWKNOP protocols use standard RSA and SHA algorithms, which consume more computational resources, and the convenience and security aspects are more difficult to achieve. Consumption is large, and there are shortcomings in convenience and security. The SPA protocol in this paper adopts SM3 and SM4 algorithms to achieve encryption and signature, and only 1019B is needed to complete a single packet authorisation, which effectively reduces the size of communication packets under the premise of guaranteeing security, and greatly reduces the communication and computation pressure of IoT terminals.

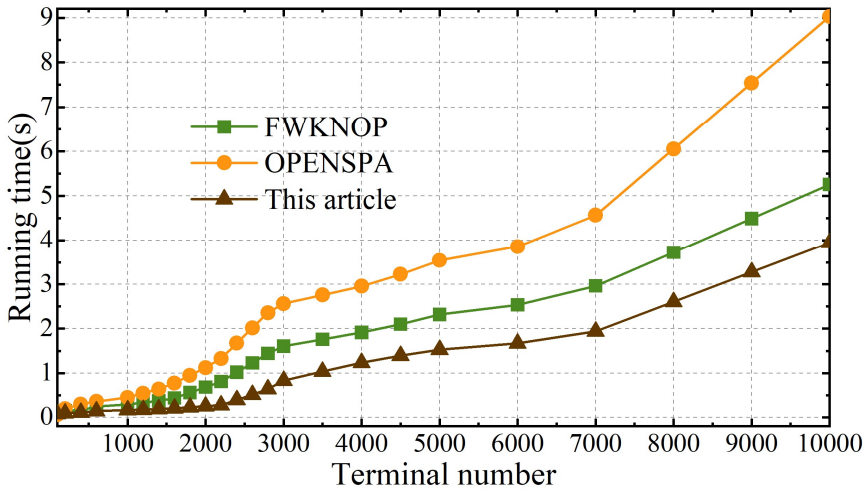


Fig. 6. SPA test comparison results

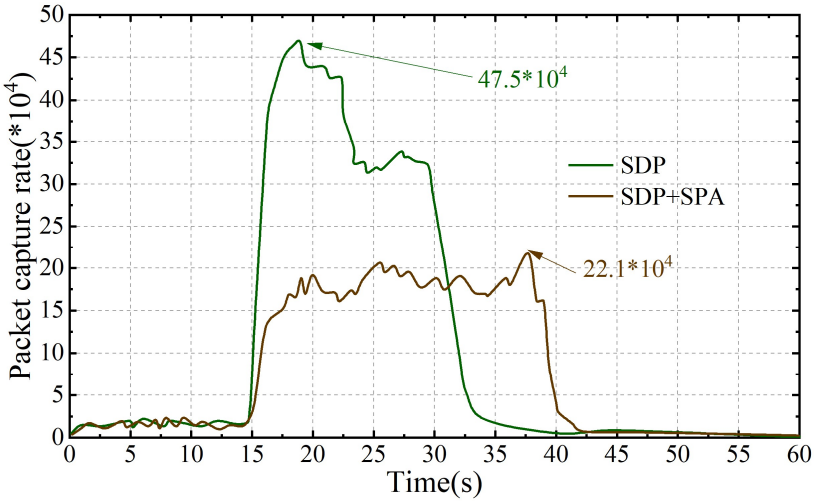
4.2. Safety analysis and performance analysis

4.2.1. Security performance testing. In order to test the network security protection performance of SPA single packet knocking scheme with zero trust architecture, two attacks are simulated in this experiment, DDoS attack and Web port scanning attack. The DDoS attack is chosen because it poses a threat to data and service availability in modern networks, while the Web port scanning attack poses a threat to data privacy. These two attacks represent two of the threats and problems faced by networks that introduce zero-trust architectures. Therefore, by testing these two attacks, the effectiveness of the security protection SPA scheme designed in this paper in enhancing network security can be effectively verified.

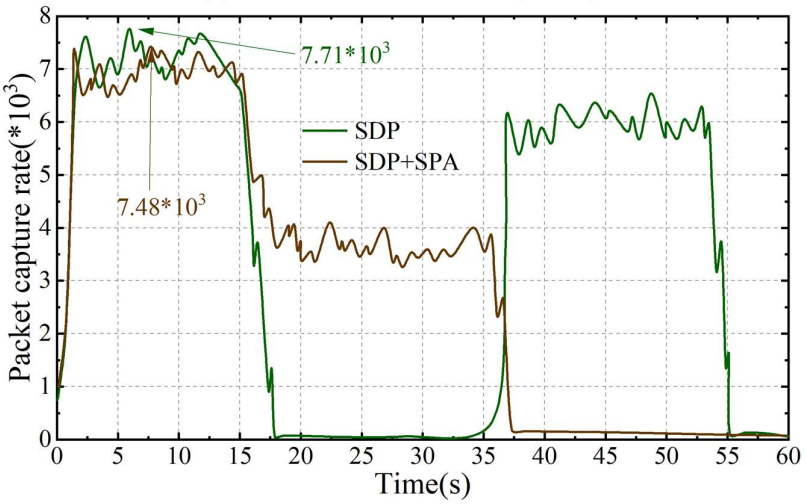
The DDoS attack test is conducted using Hping3 to view the changes in network throughput of the two schemes, SDP+SPA and SDP, before and after being subjected to a DDoS attack and a web attack, respectively, by transmitting 300MB of raw data traffic and DDoS traffic between a legitimate client (SDP IH) and a web service using a netcat application. The traffic at the public interface of the gateway and at the service side is captured in the experiment and analyzed in detail. Fig. 7 shows the experimental results of the security protection scheme, where Fig. 7(a)~(b) shows the traffic information at the gateway and the server side, respectively.

In the traffic information at the public interface of the gateway, the traffic in 0-15 seconds is the authorized packets of legitimate clients, and in the 15th second DDoS attack is carried out by injecting a large amount of SYN flood traffic, and the gateway (SDP AH) immediately captures a large amount of traffic, which are mainly attacking SYN packets in the scenario where only the SDP component is enabled, and in the scenario where the SDP+SPA component, the received traffic is only 53.47% of the traffic with the SDP scheme. This is because the SDP AH module in the SDP+SPA scenario adopts a “drop-all” policy, which discards all attack traffic, does not respond to the requests of attack traffic, and only authorized SDP IHs can communicate. Only authorized SDP IHs can communicate. That is, TCP packets with SPA packets are received and sent, while the SDP-only scenario has not only attack SYN request packets, but also ACK packets in response to the request packets. At the 30th second, the DDoS attack ends, but the traffic does not return to normal immediately, this is because a lot of packets have been accumulated at the gateway interface and at the server side, so the traffic captured in the two scenarios will gradually return to normal. In addition, the traffic information on the server side reflects the packets received on the server side. In 0-15 seconds, the traffic of the two schemes is stable between 6.5*103~8.0*103 packets/sec. After the DDOS attack and Web attack, the server in the SDP+SPA scheme still retains a certain amount of legitimate data due to the filtering of the SDP AH. However, the client in the SDP scheme is flooded by the attack traffic due to the lack of security

interception, resulting in the server's traffic dropping to zero. Only after the DDoS attack and Web attack stopped in the 30th second, the traffic in the SDP scheme gradually returned to normal. In summary, the use of SDP+SPA single packet knocking mechanism component in the network can effectively protect against DDoS attacks and Web attacks, effectively ensuring the network security performance.



(a) Traffic information in the gateway



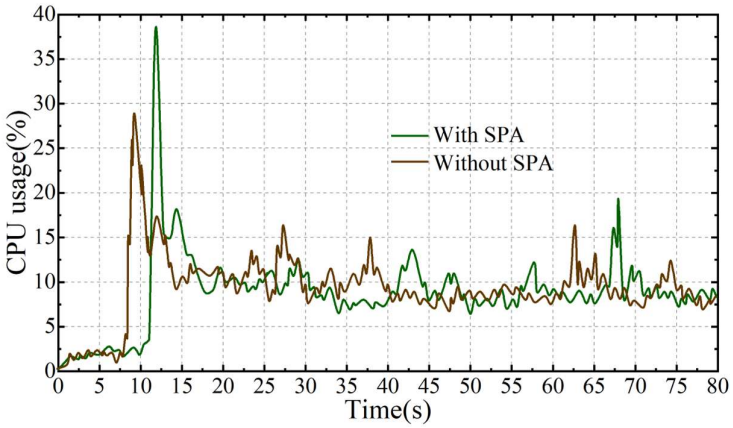
(b) Service traffic information

Fig. 7. Results of the safety protection scheme

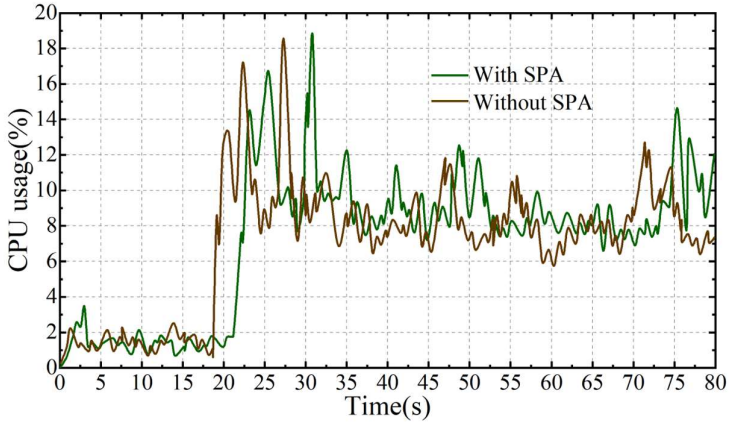
4.2.2. Programme performance analysis. The single packet authorisation mechanism adds an extra step of SPA authentication to the normal network communication, an extra SPA packet generated by the client is bound to have an impact on the energy consumption of the device, and since the authentication of the SPA is performed by the well-resourced controllers, it does not generate additional computational needs for the server. In addition the SPA authentication process increases the communication delay. In order to compare the energy consumption and communication latency with and without SPA authentication, a comparison of the client and server CPU utilisation in both cases was carried out. Fig. 8 shows the experimental results of the authentication process, where Fig. 8(a)~(b) shows the CPU utilisation of the client and server side respectively.

The client starts a programme to record the average CPU load once per second during the communication period, and the client in both cases communicates with the server at the same time at 10s. The CPU usage in 15s can reach up to 38.42% due to the extra SPA packet sent by the client deployed with SPA, which is 11.47 percentage points higher than the CPU usage without SPA mechanism. And due to the small size of SPA packets, the energy consumption is not significantly

higher. And from the change of CPU usage of the server, it can be seen that SPA has no effect on the energy consumption of the server. This also verifies that the SPA mechanism has a small impact on the CPU usage, and considering its security performance, the impact of the SPA mechanism on the CPU usage can be effectively ignored. In addition, the network communication with the SPA module running has a delay of about 0.85s, which comes from the authentication of the client by the controller. The authentication process occurs only once before data transmission, and this one-time delay has no significant impact on the overall communication. Overall, in the process of network security protection, the combination of SPA single-packet knocking mechanism under the zero-trust framework can achieve network security communication and improve the efficiency of network security information transmission.



(a) CPU usage at the client



(b) CPU usage at the service

Fig. 8. Experimental results of the certification process

5. Conclusion

The article combines the zero-trust framework and SPA single-packet authorisation technique to establish a single-packet knocking mechanism for security protection SPA, and constructs an authentication protocol to enhance network security protection.The communication volume for SDP clients to complete one authentication is 981B, which reduces the overhead by 27.17% compared to WaverleySDP. When the number of terminals is 10000, the FWKNOP and OPENSPA protocols run 1.33 times and 2.29 times longer than the SPA protocol in this paper, respectively. The traffic of SDP+SPA and SDP scheme is stable between 6.5*103~8.0*103 per second in 0-15 seconds, and after the DDOS attack and Web attack, the server in the SDP+SPA scheme still retains a certain amount of legitimate data due to the filtering of SDP AH. The CPU usage of the client deployed with SPA can reach up to 38.42%, which is 11.47 percentage points higher than the CPU usage without SPA mechanism. Although the introduction of SPA single packet knocking mechanism increases the client CPU usage by

a certain amount, it is negligible compared to its security protection performance and communication efficiency. Overall, SPA single packet knocking technology can effectively improve the network security protection effect, and can also effectively ensure the safe transmission of network data after facing DDoS and Web attacks.

References

[1] Pawar, M. V., & Anuradha, J. (2015). Network security and types of attacks in network. Procedia Computer Science, 48, 503-506.

[2] Hua, T., & Li, L. (2019). Computer network security technology based on artificial intelligence. Journal of Intelligent & Fuzzy Systems, 37(5), 6021-6028.

[3] Liang, X., & Xiao, Y. (2012). Game theory for network security. IEEE Communications Surveys & Tutorials, 15(1), 472-486.

[4] Kumar, S. N. (2015). Review on network security and cryptography. International Transaction of Electrical and Computer Engineers System, 3(1), 1-11.

[5] Ciampa, M. (2015). CompTIA security+ guide to network security fundamentals. Cengage Learning.

[6] Xie, L., Hang, F., Guo, W., Lv, Y., Ou, W., & Shibly, F. H. A. (2021). Network security defence system based on artificial intelligence and big data technology. International journal of high performance systems architecture, 10(3-4), 140-151.

[7] Bian, L. (2023). Design of computer network security defense system based on artificial intelligence and neural network. Wireless Personal Communications, 1-20.

[8] Moustafa, N. (2021). A new distributed architecture for evaluating AI-based security systems at the edge: Network TON_IoT datasets. Sustainable Cities and Society, 72, 102994.

[9] Latif, S. A., Wen, F. B. X., Iwendi, C., Li-Li, F. W., Mohsin, S. M., Han, Z., & Band, S. S. (2022). AI-empowered, blockchain and SDN integrated security architecture for IoT network of cyber physical systems. Computer Communications, 181, 274-283.

[10] Li, J. H. (2018). Cyber security meets artificial intelligence: a survey. Frontiers of Information Technology & Electronic Engineering, 19(12), 1462-1474.

[11] Chen, Y., Gao, X., & Wu, X. (2021, March). Application of ai technology in defense of big data network security. In Journal of Physics: Conference Series (Vol. 1802, No. 3, p. 032105). IOP Publishing.

[12] Shafique, R., Rustam, F., Choi, G. S., & Jurcut, A. D. (2024, April). Enhancing in-vehicle network security against ai-generated cyberattacks using machine learning. In 2024 IEEE Wireless Communications and Networking Conference (WCNC) (pp. 1-6). IEEE.

[13] Hou, J., & Jia, X. (2021, November). Research on enterprise network security system. In 2021 2nd International Conference on Computer Science and Management Technology (ICCSMT) (pp. 216-219). IEEE.

[14] Lyu, M., Gharakheili, H. H., & Sivaraman, V. (2024). A survey on enterprise network security: Asset behavioral monitoring and distributed attack detection. IEEE Access.

[15] Shin, B. (2021). A practical introduction to enterprise network and security management. Auerbach Publications.

[16] Li, W., & Zhu, H. (2021, June). Research on Comprehensive Enterprise Network Security. In 2021 IEEE 11th International Conference on Electronics Information and Emergency Communication (ICEIEC) 2021

IEEE 11th International Conference on Electronics Information and Emergency Communication (ICEIEC) (pp. 1-6). IEEE.

[17] Zhao, L., He, Q., Guo, L., & Sarpong, D. (2023). Organizational digital literacy and enterprise digital transformation: Evidence from Chinese listed companies. IEEE Transactions on Engineering Management.

[18] Ou, X., & Singhal, A. (2011). Quantitative security risk assessment of enterprise networks. Springer New York.

[19] Arefin, M. T., Uddin, M. R., Evan, N. A., & Alam, M. R. (2021). Enterprise network: Security enhancement and policy management using next-generation firewall (NGFW). In Computer Networks, Big Data and IoT: Proceedings of ICCBI 2020 (pp. 753-769). Springer Singapore.

[20] Yusuf, S. E., Ge, M., Hong, J. B., Kim, H. K., Kim, P., & Kim, D. S. (2016, December). Security modelling and analysis of dynamic enterprise networks. In 2016 IEEE International Conference on Computer and Information Technology (CIT) (pp. 249-256). IEEE.

[21] Regenold, J., Wang, K., Smith, G., Liu, Q., & Chen, L. (2017, December). Enhancing enterprise security through cost-effective and highly customizable network monitoring. In 10th EAI International Conference on Mobile Multimedia Communications (pp. 133-142).

[22] P. SumanPrakash,K. Seshadri Ramana,Renzon Daniel CosmePecho,M. Janardhan,Meryelem Tania Churampi Arellano,J. Mahalakshmi... & K. Samunnisa. (2024). Learning-driven Continuous Diagnostics and Mitigation program for secure edge management through Zero-Trust Architecture. Computer Communications94-107.

[23] Antonio Paya,Vicente García & Alberto Gómez. (2024). Securesdp: a novel software-defined perimeter implementation for enhanced network security and scalability. International Journal of Information Security(4),2793-2808.

[24] Dongbo Zhong,Qi Xi,Faiz Ul Islam,Zhiyong Cui & Yufei Xie. (2024). An efficient key tag missing identification protocol for multiple regions in the Industrial Internet of Things. Physical Communication102409-102409.