Design and Implementation of IPsec VPN IoT Gateway System in National Secret Algorithm

Yan Jiang[1,*], Jing Huang[2], Yunsong Fan[1] and Xiaobin Zhu[3]

[1]*Fujian Expressway Science & Technology Innovation Research Institute Co., Ltd, Fuzhou, Fujian, 350000, China*
[2]*Fujian Expressway Group Co., Ltd, Fuzhou, Fujian, 350000, China*
[3]*Fujian branch of QIANXIN Technology Group Co., Ltd, Fujian, 350000, China*
E-mail: jiangyanjoy@sina.com
[*]*Corresponding Author*

Received 14 December 2023; Accepted 04 February 2024

Abstract

With the development of Internet of Things technology, the security threats faced by the industrial control field are increasing, and strengthening the security protection capabilities of intelligent systems on IoT highways is becoming increasingly important. IPSec VPN tunneling technology can achieve identity authentication and encrypted data transmission, and is an important means to achieve secure data transmission in intelligent systems on Expressway intelligent tunnel system. The commonly used IPSec VPN gateway uses a traditional Linux protocol stack-based approach for data capture, which requires multiple data copies and context switching, resulting in low efficiency of IPSec services. In addition, the commonly used IPSec VPN security gateway is implemented on the basis of the open-source IPSec framework, using internationally recognized algorithms for encryption and decryption, which poses security risks. This article is based on the IPSec

Journal of Cyber Security and Mobility, Vol. 13_4, 677–700.
doi: 10.13052/jcsm2245-1439.1345

protocol, and studies the high-speed network packet capture framework PFRING technology, the fusion technology of national secret algorithm and IPSec protocol. It designs and implements an IPSec VPN IoT security gateway based on national secret algorithm. After experimental verification, the IPSec VPN gateway system constructed in this article has complete functions and better performance than the common open-source IPSec frameworks OpenSwan and strongSwan, and can meet the application requirements of IoT data encryption transmission.

Keywords: IPsec, national secret algorithm, PFRING, security gateway, expressway.

1 Introduction

With the advancement of digital information construction, the Internet of Things (IoT) information technology has experienced significant development. In the field of IoT industrial control, the intelligent systems used for data collection and monitoring in high-speed highway scenarios face an increasing number of security threats. Firstly, the authentication mechanism for connecting terminals in IoT high-speed highway intelligent tunnel systems is not sufficiently robust, and insecure network connections elevate the risk of attacks on the central controller of IoT high-speed highway intelligent tunnel systems [1, 2]. Secondly, during the process of network transmission, critical collected data may be susceptible to hacking and tampering, leading to data leakage. This can disrupt the normal operation of Expressway Data transmission system and potentially result in incalculable economic losses for Expressway Toll System [3]. Thirdly, the real-time requirements of IoT high-speed highway intelligent tunnel systems necessitate high transmission efficiency during information channel transmission. Traditional IoT security gateways, which employ the Linux protocol stack for data forwarding, exhibit low data processing efficiency and fail to ensure the system meets the requirements of high response time delays and throughput rates [4, 5].

Virtual Private Network (VPN) is a technology that utilizes cryptographic techniques to establish temporary secure tunnels in public networks. It is widely used for the secure transmission of data in the Internet of Things (IoT) information networks, assisting enterprises in building dedicated data transmission channels that are physically distributed yet logically unified. Common VPN implementation methods include IPSec technology and SSL

technology [6]. IPSec technology, a set of protocols released by IETF, defines the process of key exchange and encrypted message transmission in an insecure network. It achieves functions such as user authentication, data encryption, and integrity protection. The SSL protocol consists of a protocol suite composed of the record layer protocol and the handshake layer protocol, with functionalities similar to IPSec. The difference lies in that IPSec performs data encryption at the network layer, while SSL encrypts at the transport layer [7, 8]. Therefore, IPSec can be applied not only to communication between hosts and gateways but also to the secure data transmission of IoT devices between subnets, meeting the requirements of applications in high-speed highway intelligent tunnel systems. Currently, VPN gateways based on IPSec VPN technology are mostly implemented using the open-source projects Openswan and strongSwan frameworks [9, 10]. The Openswan framework and strongSwan framework, developed based on the international IPSec standard, do not support the use of domestic cryptographic algorithms for encryption and decryption. Additionally, the encapsulation format of messages during the negotiation process does not comply with the specifications of domestic IPSec VPN technology.

In accordance with the security requirements of the Internet of Things (IoT) expressway intelligent tunnel system business and considering the functional and performance deficiencies in current IPSec VPN gateways, researching an IPSec VPN IoT security gateway based on domestic cryptographic algorithms holds significant importance. The improvement of IPSec VPN gateways over traditional packet capture methods utilizes a high-speed network packet capture framework, enhancing data processing efficiency to meet the real-time requirements of IoT industrial control networks. The IPSec VPN gateway authenticates the connected terminals, reducing the risk of unauthorized connections and potential intrusions. Filtering terminal data according to policies, the IPSec VPN gateway prevents illegal data from entering the tunnel, reducing the risk of attacks on the main network. The IPSec VPN gateway utilizes a domestically developed IPSec service framework based on domestic cryptographic standards, employing highly secure domestic cryptographic algorithms for data encryption, thereby enhancing the security protection of IoT operations. This paper, based on the IPSec protocol, explores the integration of high-speed network packet capture framework PFRING technology, domestic cryptographic algorithms, and IPSec protocol fusion technology. It designs and implements an IPSec VPN IoT security gateway based on domestic cryptographic algorithms.

The research and main achievements of the paper are divided into three aspects:

(1) Addressing the real-time requirements of IoT high-speed highway intelligent tunnel systems, researching high-performance network packet capture technology, combining thread pools, lock-free circular buffers, and the PFRING framework to design and develop a network packet capture module, improving packet processing speed.
(2) Meeting the data reliable transmission requirements in expressway intelligent tunnel systems, researching key negotiation protocols and secure message protocols, designing and developing the IPSec security service module to achieve mutual device authentication and encrypted data transmission, enhancing the ability to prevent illegal intrusions and ensuring the security of data during transmission.
(3) Addressing the specific security requirements of IoT high-speed highway intelligent tunnel systems, researching domestic cryptographic algorithms, designing and developing a cryptographic module based on domestic cryptographic algorithms, further enhancing the security and real-time capabilities of the IPSec VPN gateway.

2 IPsec VPN Technical Study

2.1 Key Exchange Protocol

Key exchange protocol is used for identity authentication and key generation before secure message transmission, which defines the whole process of negotiation interaction and negotiation message format [11]. Key exchange protocol includes two stages of the negotiation process: primary mode and fast mode. The main mode is used to generate the working key, and the fast mode is used to generate the session key. In the primary mode, through the interaction of the first two messages, encryption algorithm and the shared key material are determined. The initiator negotiated with the responder in the quick mode.

Figure 1 shows an overview of the blockchain architecture. In the blockchain architecture, the key exchange protocol generates the session key by exchanging the generated vital parameters [12]. This generation method avoids the risk of exposing the key directly to the network and being obtained by the middleman, leading to vital leakage. The critical negotiation agreement also stipulates the key update method, requiring that the new key must be generated dynamically within the update cycle.

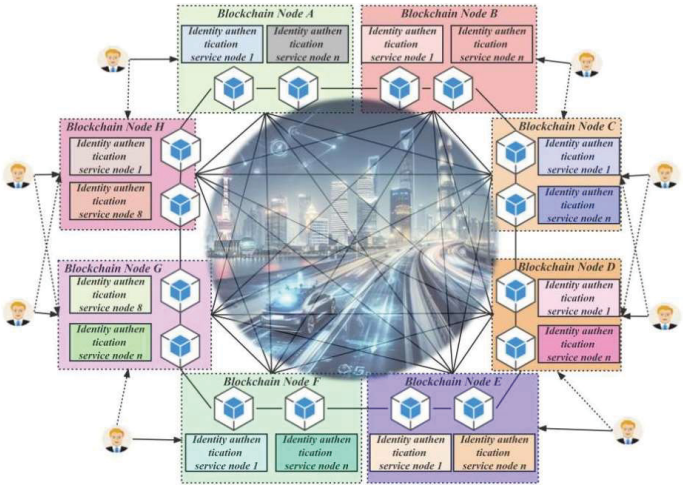

Figure 1 Overview of blockchain architecture for intelligent systems on IoT highways.

2.2 Security Message Protocol

The security message protocol defines the IPsec channel package packaging method, including two security protocols: Identification Head Protocol (AH) package Security Protocol (ESP). The identification head protocol provides integrity verification for the transmitted data and prevents data packets from being stolen and tampered during the transmission. Encapsulation security protocol provides not only integrity verification but also the entire packet encryption service. The encapsulation security protocol uses the IP packets generated by the negotiation process to encrypt and encapsulate the encrypted data into ESP packets, which transmit in the tunnel as ESP packets [13, 14]. The AH protocol lacks a design for data encryption capabilities and can only be used with the ESP protocol. When the AH is used with the ESP, the AH head is placed between the new IP message header and the ESP head. When using the ESP protocol, the ESP header is packaged between the new IP packet header and the original IP packet header. According to the application scenario of this system, the ESP mode is selected in the security message module during the IPsec VPN gateway design.

Using the ESP protocol, the session key generated in the negotiation stage is first used to encrypt the data symmetrically. The encrypted data is then subjected to SM3 summary calculation to obtain the authentication data. Finally, the authentication data is encapsulated at the end of the ESP [15]. I am receiving the ESP data package to the terminal gateway and making

summary calculations to determine whether the data is complete. The verified, approved data packet uses the symmetry algorithm for the decryption operation. The decrypted good message is a complete IP data packet. The ESP protocol guarantees the confidentiality and integrity of the data message during the transmission of the initiator and the responder.

When address conflicts occur, first analyze the total number of address allocation schemes that meet the above conditions. According to the hypothesis, the addresses of all N within each LAN will not conflict, so the number of address allocation schemes in the *i-th* LAN S can be expressed by Equation (1).

$$S_i = C_L^{N_i} \tag{1}$$

According to the multiplication principle, the total number S of all address allocation schemes that meet the assumptions can be represented by Equation (2).

$$S = \prod_{i=1}^{M} (S_i) = \prod_{i=1}^{M} (C_L^{N_i}) \tag{2}$$

Consider again that in all M local area networks, the number of address allocation schemes W without any internal address conflict event can be expressed as Equation (3).

$$W = C_L^{N_i} \prod_{i=1}^{M-1} (C_e^{N_{i+1}}) \tag{3}$$

Equation (4), where W/S indicates the probability of no internal address conflict event under the above assumptions, then P can represent the probability of at least one internal address conflict event.

$$P = 1 - \frac{W}{S} \tag{4}$$

2.3 IPsec VPN Three-layer Key System

The three-layer key of IPSec VPN consists of the device key, working key, and session key. The device key is an asymmetric key pair, which is added and decrypted for the symmetrical critical information during the central mode negotiation or used to check the signature of both parties in the negotiation. Generally obtained directly from the device or in the digital certificate product through the specified function call during the negotiation process. The private key in the equipment key should take high protection measures.

In case of an abnormal situation in the system, emergency measures to destroy the key should be taken to protect the private key from malicious theft.

The working key is a symmetric key obtained through negotiation in the master mode – the initiator and the responded exchange the common critical materials of Nonce, cookie, etc [16, 17]. The Nonce and cookie information saved by both parties are summarized multiple times to obtain the working keys SKYIDa and SKYIDe [18]. The work key ensures the integrity and confidentiality of fast-mode message interaction and is a secure tool for generating a session key.

The session key is a symmetric key generated through fast-mode negotiation. KEY [19, 20], the final material of the session key, was generated through the working key and the jointly negotiated parameters. In the secure message phase, the session key for encryption and authentication is obtained from KEY. The system should ensure security of working key and session key. When system has an emergency, the key should be destroyed.

IPSec VPN key system: device key, work key, session key. Asymmetric key pairs, including signature key pairs and encryption key pairs, are used for entity identity authentication, digital signatures, and digital envelopes. Among them, the device key pair used for signature provides identity authentication services based on digital signatures in the first stage of IKE; The device key pair used for encryption provides confidentiality protection for exchanging data in the first stage of IKE. Symmetric key, derived through key negotiation in the first stage of IKE, is used to protect the session key exchange process. Among them, the working key used for encryption provides protective protection for the data exchanged in the second stage of IKE; The working key used for integrity verification provides integrity protection and identity authentication for the data exchanged in the second stage of IKE. Symmetric key, derived through key negotiation in the second stage of IKE, is directly used for encryption and integrity protection of data packets and message MAC. The session key used for encryption provides confidentiality protection for communication data and MAC values; The session key used for integrity verification provides integrity protection for communication data.

3 IPsec VPN Design of IoT Gateway System

3.1 Overall Architecture Design of IoT Security Gateway

Through the analysis of functional and performance requirements, the overall architecture of the power security gateway is designed as shown in Figure 2.

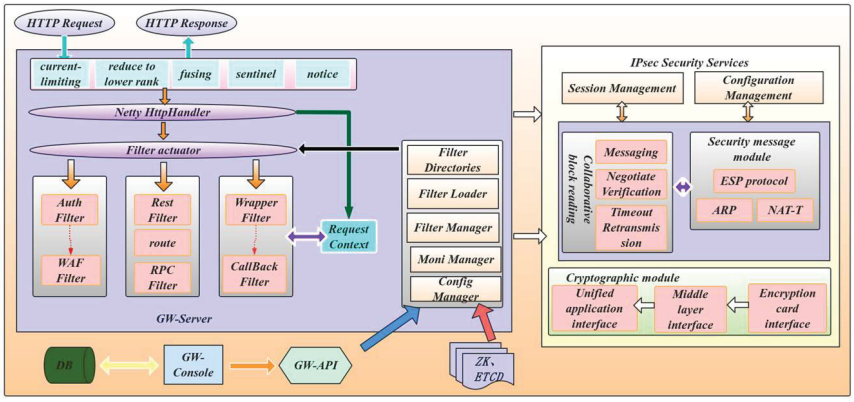

Figure 2 Overall architecture of IoT security gateway.

The gateway system includes five parts: network data package capture module, IPsec security service module, password module, configuration module, and VPN management module. Among them, the network packet capture module is divided into the PFRING receiving module and the PFRING sending module. The IPsec service module is divided into the IKE negotiation module and the safety message module.

After the system is started, the PFRING receiving packet module captures the packet from the network card and sends it to the IPsec security service layer after simple processing. The IPsec security service layer classifies the data packets using the package source, transmission layer protocol, and other information. It processes the encrypted packets according to the negotiation message, security message, and sub-net. The IPsec security service layer uses the national secret algorithm for packet encryption and decryption operation and identity authentication service. Finally, the IPsec security service layer forwards the message required to be forwarded via the PFRING sending module.

The entire hierarchical structure consists of data layer, control layer, application layer, and presentation layer from bottom to top. The data layer is at the bottom level, and the data source of the entire system is clearly the most fundamental level. The control layer is a crucial layer that connects the upper and lower layers, and its main function is the parsing of instructions and the sending and receiving of instructions. The application layer can also be called the business layer, which is closely related to the business logic of the system, and the implementation of some businesses will be realized here. The upper layer is connected to the presentation layer, which can then transmit and

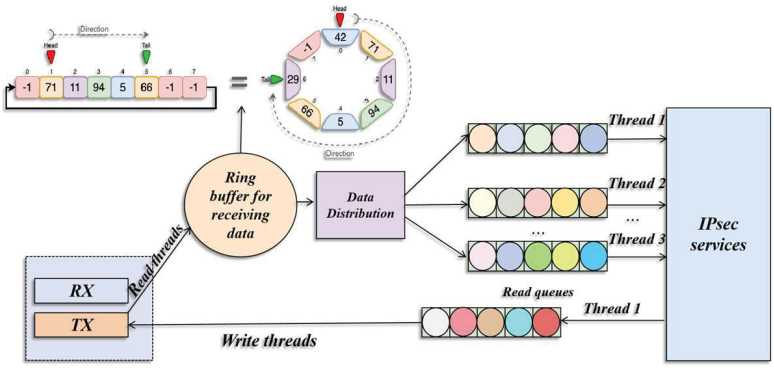

Figure 3 PFRING high-speed capture packet framework.

receive instructions to the device through the control layer. The lower layer is connected to the control layer, which can obtain device related data and submit it to the presentation layer. The presentation layer, also known as the interaction layer, is the starting point for human-computer interaction and data visualization. It is not difficult to see that this level directly interacts with people, so while meeting business needs, it needs to be designed with sufficient humanization.

3.2 Network Data Packet Capture Module Design

The data processing framework designed by the network data packet capture module is based on the PFRING high-speed capture data packet framework, as shown in Figure 3. When receiving data packet, the read thread saves the received data packets in the ring buffer; the data distribution function distributes the data in the ring buffer to the read queue; the working thread preprocesses the data cached by the read queue and then sends the processed data packets to the IPsec service layer. When the gateway forwards data packets, the IPsec service layer saves the data to be forwarded to the write queue through the working thread. The write thread sends the data of the write queue out through the network card.

3.3 IPSec Security Service Design

3.3.1 IKE negotiation module

The IKE negotiation module is the basic module of IPsec security service, which provides functions such as primary mode fast mode negotiation, IKE message verification, establishment, and update of SA security alliance,

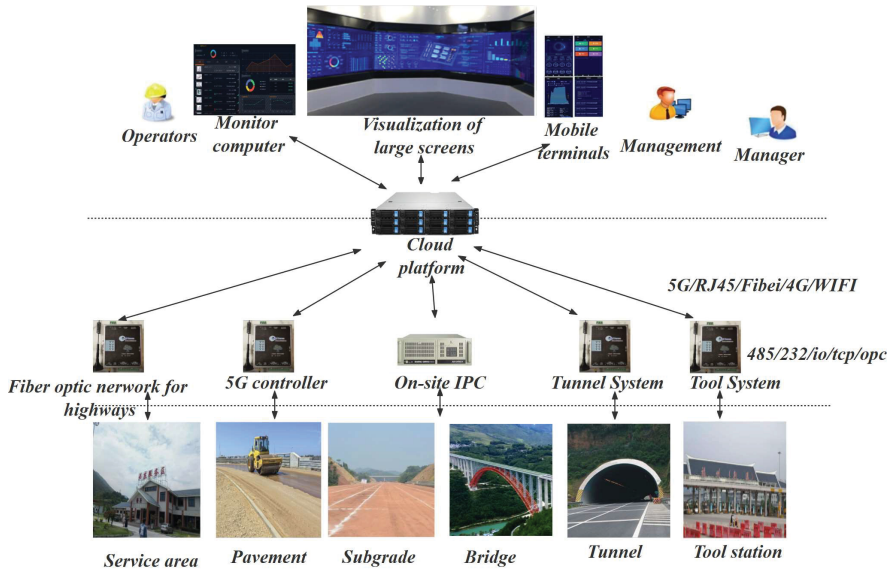

Figure 4 Internet of Things expressway intelligent system.

and of gateway identity authentication and key generation [21, 22]. When the primary mode was negotiated, the two sides exchanged identity information. In the fast mode, the identity is determined by comparing the calculation results with the miscellaneous value obtained by analysis [23]. The whole module is divided into message service, message authentication, identity authentication, key generation, timeout re-transmission, and session management.

Figure 4 shows overall design of the IoT system, in which the message service module classifies all the messages that pass through the IPsec service layer and encapsulates, analyzes, and verifies the primary mode and fast mode messages. Identity authentication function realizes identity authentication of the terminal gateway by combining it with the national secret algorithm. The overtime re-transmission is used to resend the messages that have not been answered, and the session management is used to manage all the session information.

(1) Message service

The message service sub-module is the entrance and exit of the whole IKE negotiation module message and realizes the message type classification by analyzing the message header information. When the gateway acts as the

Table 1 Message processing strategy

Message Type	Operate
Negotiate news	Negotiate verification
Opposite-end security message	Security message analysis
The Intranet requires safely transmitted messages notification message	Security message packaging
The Network is a non-IPsec message	SA update processing bypass

client, start the negotiation function, send the negotiation message, and then monitor the message. The message processing strategy is shown in Table 1.

(2) Message verification

The message verification function analyzes the primary mode and fast mode message format according to the national secret standard specification. At the same time, the response message should be packaged according to the current gateway status. In the central negotiation mode, the encapsulation and resolution of the initiator status and the corresponding message. When the negotiation is in the start state, the SA does not establish a connection, and the timer is not timing.

(3) Identity authentication function

The identity authentication function is used for two-way identity authentication. Standard authentication methods include account and password login technology, login technology using hardware storage media, and digital certificate identity authentication technology. In IPsec, the digital certificate identity authentication technology is used in the negotiation process. During the negotiation, the initiator signs data with private key. After receiver receives the signature message, the recipient reads the public key from the initiator certificate and checks the signature data of the initiator. The identity of the initiator is confirmed by signature verification. Similarly, the initiator also uses this way to verify the recipient's identity.

(4) Key generation

The work key and session key are generated in IKE negotiation. The DH (Diffie et al.) algorithm utilizes shared critical data from both parties to generate the working key. Calculating the working key is shown in (5), and the SKYID value is first calculated.

$$SKYID = PRF(HASH(Nonce\_i|Nonce\_r), cookie\_i|cookie\_r) \quad (5)$$

Then, use SKYID as the key to digest and calculate the cookie to obtain the SKYID_D value, as shown in (6).

$$SKYID\_d = PRF(SKYID, cookie\_i|cookie\_r|0) \tag{6}$$

Similarly, calculate SKYID_e through (7) and (8).

$$SKYID\_a = PRF(SKYID, SKYID\_d|cookie\_i|cookie\_r|1) \tag{7}$$

$$SKYID\_e = PRF(SKYID, SKYID\_a|cookie\_i|cookie\_r|2) \tag{8}$$

The calculated work key protects confidentiality for generating session keys during the fast mode phase. The generation process of the session key follows the following steps. Firstly, encrypt the standard material that generates the session key, encapsulate it in a hash payload, and send it to the other party. The hash data HASH1 and HASH2 are calculated as shown in (9) and (10).

$$HASH1 = PRF(SKYID\_a, MsgID|Nonce\_i|SA[|ID\_i|ID\_r]) \tag{9}$$

$$HASH2 = PRF(SKYID\_a, MsgID|Nonce\_i|SA|Nonce\_r[|ID\_i|ID\_r]) \tag{10}$$

After exchanging materials, the initiator encapsulates HASH3 to verify the previously exchanged data. The calculation method of HASH3 is shown in (11).

$$HASH3 = PRF(SKYID\_a, 0|MsgID|Nonce\_i|Nonce\_r) \tag{11}$$

After data authentication is completed, the method of generating session key KEY is calculated according to the steps shown in Equation (12).

$$KEY = PRF(SKYID\_d, protocol|SPI(Nonce\_i|Nonce\_r) \tag{12}$$

(5) Overtime out re-transmission

When the system sends a negotiation message, start the timer. Set the timeout time when difference between current time and sending time is more significant than the timeout time determines the timeout time. When the system is in the timeout state and receives no reply, reissue the message according to the current negotiation status. The re-transmission of the message is achieved by using the signal quantity. During the message timeout, the system obtains the current state, determines which message needs to be re-posted, and then

obtains the number of the message. If the maximum number of messages the system allows is not reached, the message will be sent again.

When the data message is received, obtain the source IP and destination IP of the data message. Calculate the key from the acquired IP message. Look up the session from the session table based on the critical value, and if the session does not exist, decide whether to insert the session into the session table based on the configuration file information. If the session exists in the session table, process the data message according to the VPN status and then update the session status. Remove the SA corresponding session from the session table when the tunnel is closed, or the SA is timed out.

(6) Session management

The information of the security Alliance SA is stored in the session table, and realizing the management of the session is to realize the management of the SA. If you use an array storage session, you need to traverse the array each time. In order to improve query efficiency, the IPSec VPN gateway system uses the hash two-way link to store the data. It establishes the local address and receiver address as the critical value.

3.3.2 Safety message module

This module implements the ESP protocol in the IPsec protocol cluster, and the encryption algorithm adopts the national secret algorithm. After the critical negotiation process, the security message module can provide the encrypted transmission of data packets in the sub-network and the resolution and forwarding of ESP messages from the terminal gateway.

(1) Packaging and parsing

When the gateway receives the data packet to be forwarded from the Intranet, first find the security alliance SA to determine whether the tunnel is established. Then, the IP message is encapsulated in the ESP format and forwarded to the other gateway. When encapsulating, package the network layer message in the ESP load. When the gateway receives the ESP message from the terminal gateway, first find the security alliance SA to determine whether the tunnel is valid. If the SA is not present, the received message is discarded. If the SA is valid, the received packets are parsed in the standard format, and then the decrypted message is forwarded to the end in the subnetwork again.

(2) Data integrity protection and data source verification

Data integrity protection and data source validation were implemented using the SM3 algorithm. SM3 certification scope includes ESP head, original

IP message, and ESP tail. When encapsulating the message, the calculated MAC value is enclosed in the tail of the data packet. When analyzing, the receiver will make the same miscellaneous calculation of the obtained data to judge whether data is tampered with during transmission process. Verify the successful message, and then use the symmetrical key decryption to obtain the original IP data packet. They are comparing the source IP information in the original packet with the matching sub-net segment in the configuration file to determine whether it comes from a trusted connection.

(3) The NAT crossing function

If NAT equipment exists in the communication link, NAT crossing is required. When the gateway is started, determine whether the gateway is calculated by reading the information of the configuration file to open the NAT crossing function, and then package the NAT-D load and send the NAT-D load package the initiator cookie, the source cookie, the source port, and the source IP>. After receiving the receiving party, make the same calculation and determine whether the IP conversion occurs in the link by comparing whether the two hash values are the same. If the IP switches, NAT-T equipment is in the link.

(4) Anti-replay attack

The security message module provides packet forwarding within the subnetwork; if there is no implementation of packet resistance replay attack when the hackers in the tunnel intercept the ESP package, the gateway sends many the same message, the gateway will spend much time to deal with these invalid messages, IPsec processing efficiency will be reduced, even unable to handle the standard IPsec request [24, 25]. When the message is received, you should first judge whether the message is a replay and if it is discarded.

(5) Fragmentation and recombination

The transmission of data packets in the link is limited by the MTU (maximum transmission unit). When the IP data packets are repackaged when the packaged IP message is larger than the MTU, shard processing is required [26, 27]. When the fragmentation data belonging to the same source IP message reaches the opposite end gateway, the IP needs to be reorganized. The logo, logo, and offset fields in the IP header are used to serve the fragment reorganization.

3.4 Password Module Design

The password module involved in the system has the following contents: (1) the acquisition of the signature certificate and the encryption certificate information in the central mode negotiation. (2) In messages 3 and 4, the two parties encapsulate the common key material and encrypt it symmetrically with the vital key. The key uses the SM2 algorithm to encrypt the public key in the paired-end encryption certificate. At the end of the packet, both parties are digitally signed using the SM2 algorithm. (3) After the first four steps of message interaction, the two parties of the communication respectively use the miscellaneous collection algorithm to calculate the working key. Messages 5 and 6 use the SM3 algorithm to verify entity identity. (4) In the fast mode negotiation, the data is encrypted by SM4 first, and the encrypted data is calculated by hash value by SM3 miscellaneous algorithm, which is used for the integrity test of messages and entity identification. SM1, SM2, SM3 and SM4 were used in the negotiation process. The timing and effect of the algorithm calls are shown in Table 2.

Everyday national secret hardware products include chips, intelligent IC cards, password machines, passwords, encryption hard disks, etc. These products can provide essential password operation, data encryption and decryption, identity authentication, and password anti-counterfeiting verification functions [28, 29]. The use of hardware encryption and decryption has the following two features:

The hardware device saves the algorithm, key, and other information with the hardware, which cannot be displayed in plain text. Each encryption algorithm can only be obtained by calling the hardware interface to prevent data leakage and tampering. In addition, the hardware encryption device generally has an anti-interference, anti-loss system, further ensuring data

Table 2 Password algorithm calling scenarios

Algorithm	Scene	Effect
SM2	Holotype	Provide the role of encryption, decryption, signature verification, used to identify the identity of the terminal gateway and guarantee the message non repudiation
SM3	Main mode, fast mode	Summary calculation to ensure the integrity of data in network transmission
SM4/SM1	Main mode, fast mode, security message module	Provide the encryption and decryption function of the data packets

security. The user connects the hardware encryption device to the computer and makes a function call according to the operation manual [30].

This scheme uses a PCIE card as a hardware password to connect to the computer. PCIE card built-in digital certificate, with the function of password operation, to achieve multiple encryption and decryption algorithms. At the same time, the hardware structure of the PCIE cards can provide high-intensity guarantees for the safe operation of the cryptographic algorithms. There are many PCIE cards on the market; according to the number of channels, the physical specifications are divided into five modules. In order to reduce the dependence between the modules, when a new PCIE card is added, the change in the original system can be reduced.

4 Results and Discussion

When testing system performance, the IPSec VPN gateway performance is reflected by deploying the IPsec open-source project as an experimental control. Openswan and strongSwan are common IPsec framework. First, the source code is improved by registering the national secret algorithm in the algorithm library of Openswan and strongSwan, and then the Openswan system and strongSwan system based on the national secret algorithm are installed on host A and host B in the 5.1 environment, to keep the same hardware environment of the three schemes during the test.

(1) Round-trip delay

Run the IPsec VPN systems implemented in the three schemes, the test terminal 1 in the server sub-network and the test terminal 2 in the Ping client sub-net. Change the ICMP packet size to record the size of the round-trip delay when the packets are sent as 32 bytes, 64 bytes, 128 bytes, 256 bytes, and 512 bytes.

Figure 5 shows comparison of the round-trip delay. After the test of the round-trip delay of the IPSec VPN system realized by three schemes, it is found that the round-trip delay of the IPSec VPN system designed in this paper is the lowest, which shows that the whole process of data packet encryption packaging and decryption is less than the VPN system realized by open-source framework.

(2) TCP throughput

This paper tests the size of the VPN system TCP throughput implemented by three systems. First, the three types of IPsec VPN systems were run

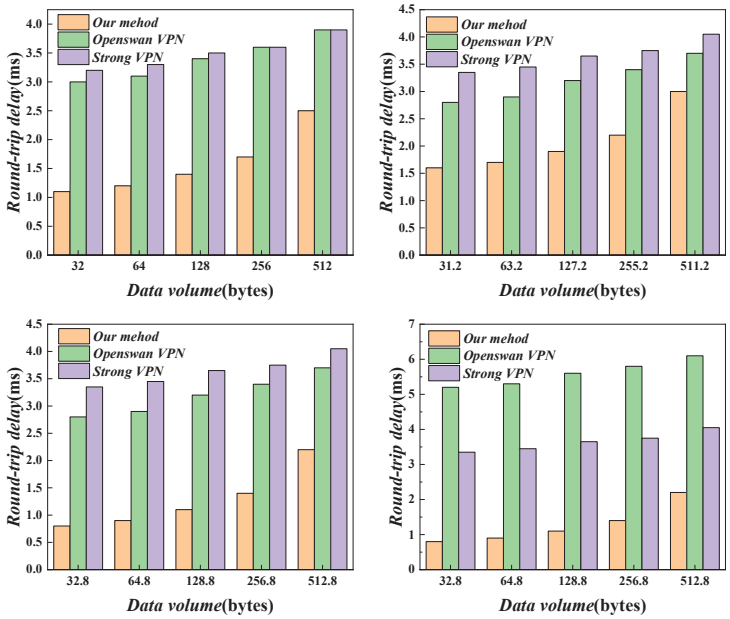

Figure 5 Comparison of round-trip time delay.

respectively. Then, test terminal 1 in the server sub-network opens the iperf server mode, and test terminal 2 in the client sub-network opens the client connection. Finally, under the same network bandwidth, make the client send different sizes of packets for testing, recording the size of TCP throughput.

Figure 6 shows comparison of TCP throughput. Comparative test shows that the designed IPSec VPN system has the highest TCP throughput and high transmission efficiency under the same conditions.

(3) UDP throughput

Finally, this paper tests the size of the UDP throughput of VPN systems implemented by three schemes using the network performance test tool perf. First, the three types of IPsec VPN systems were run respectively. Then, test terminal 1 in the server subnetwork opens the iperf server mode, and test terminal 2 in the client subnetwork opens the client connection. Finally, the magnitude of the UDP throughput at different network bandwidths is recorded by changing the bandwidth limit value.

Figure 7 shows comparison of UDP throughput. The comparative test shows that the IPsec VPN system UDP designed in this paper has a high

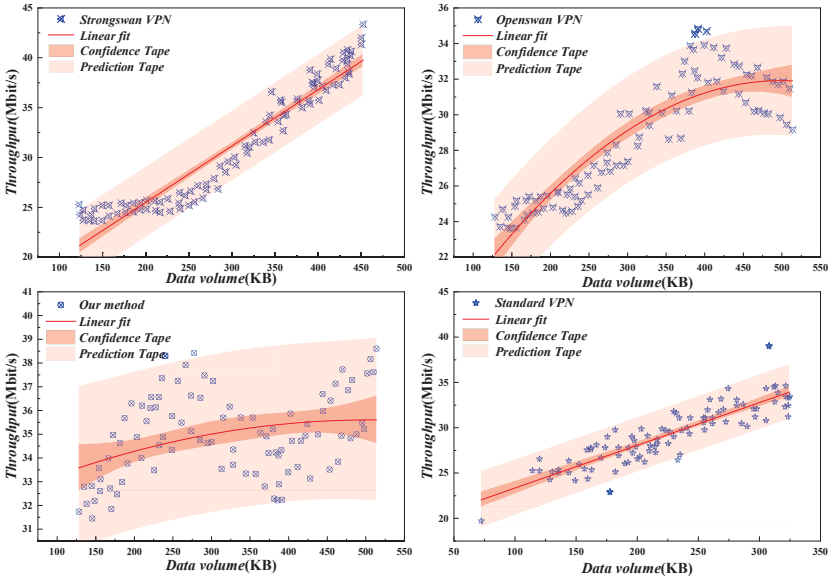

Figure 6 Comparison of TCP throughput.

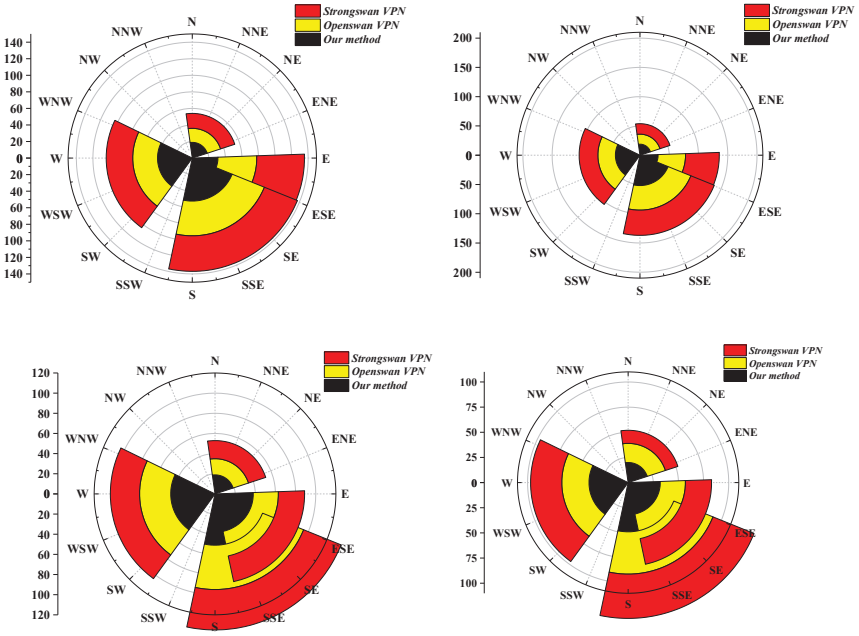

Figure 7 UDP throughput comparison.

throughput and can maximize the network bandwidth. Furthermore, the gateway system has undergone joint testing with FUJIAN EXPRESSWAY GROUP CO.LTD. FUZHOU BRANCH and has entered the pilot application phase. The system has been deployed on-site by Fujian Expressway Science & Technology Innovation Research Institute Co., Ltd., and from April 2023 to the present, it has been running stably. The system is capable of encrypting data during transmission, effectively addressing security issues in the data transfer process within the high-speed highway intelligent tunnel system.

5 Conclusion

The security of data in the Internet of Things (IoT) high-speed highway intelligent tunnel system is crucial for the stable operation of IoT companies' businesses. In order to enhance the reliability of data transmission in the high-speed highway intelligent tunnel system, this paper is based on the IPSec protocol, high-speed network packet capture technology, and cryptographic techniques, and designs and implements an IPSec VPN IoT security gateway based on domestic cryptographic algorithms. The research and achievements of this paper are summarized in the following aspects:

(1) Research on the security threats faced by the current high-speed highway intelligent tunnel system and the IPSec security protocol. The study also explores IPSec VPN product-related standards and specifications, proposing an independent research project on developing an IPSec VPN IoT security gateway based on domestic cryptographic algorithms without relying on open-source frameworks such as Openswan and strongSwan. Through the exploration of key technologies in IoT security gateways, a foundational technical system for designing and implementing IoT security gateways has been developed.

(2) Research on the PFRING high-speed network packet capture technology and the design and implementation of a network packet capture module. The module's data processing efficiency is improved through thread pool technology, lock-free circular buffer technology, and thread binding technology. The module's packet sending function is realized through Ethernet frame format and ARP protocol. The implementation of the network packet capture module addresses the low efficiency issue in common IPSec VPN gateway packet capture, meeting the real-time requirements of high-speed highway intelligent tunnel systems.

(3) Research on IPSec-related protocols and the design and implementation of the IPSec security service layer. The implementation includes the

realization of the IKE protocol's main and quick mode negotiation processes for mutual device authentication and secure session key generation. The ESP protocol is implemented for the secure transmission of messages within the tunnel. The use of a hash table improves session lookup speed, thereby enhancing system service speed. The implementation of the VPN management system fulfills the visualization management requirements of IPSec VPN power security gateways. The implementation of the IPSec security service layer addresses issues commonly found in IPSec VPN gateways based on open-source frameworks, such as low security and poor autonomy, meeting the security and reliability requirements of high-speed highway intelligent tunnel systems.

(4) Research on IPSec product testing methods and testing the functionality and performance of the implemented IPSec VPN security gateway. Comparative performance testing is conducted by deploying the Openswan and strongSwan source codes, concluding that the performance of this proposed gateway surpasses that of common open-source frameworks.

Funding

This work was supported by the"Key Science and Technology Projects of the Transportation Industry of the Ministry of Transport in 2022, NO, 2022-ZD6-074"

References

[1] Xi, W., Suo, S., Cai, T., Jian, G., Yao, H., and Fan, L. (2019). A Design and Implementation Method of IPSec Security Chip for Power Distribution Network System Based on National Cryptographic Algorithms. 2019 IEEE 3rd Information Technology, Networking, Electronic and Automation Control Conference (ITNEC). IEEE.

[2] Sun, M., Yang, S., Wang, D., Gu, J., and Cai, H. (2022). Design and implementation of control system for submersible agv. Academic Journal of Computing & Information Science.

[3] Bhattacharya, P., and Rao, S. (2021). User and IoT (internet of things) apparatus tracking in a log management system. US10938926B2.

[4] Bhavani, N. G., Kumar, R., Panigrahi, B. S., Balasubramanian, K., Arunsundar, B., and Abdul-Samad, Z., et al. (2022). Design and implementation of iot integrated monitoring and control system of renewable energy in smart grid for sustainable computing network. Sustainable computing: Informatics and systems.

[5] Dzogovic, B., Mahmood, T., Santos, B., Feng, B., Do, V. T., and Jacot, N., et al. (2021). Advanced 5g network slicing isolation using enhanced vpn+ for healthcare verticals. Springer, Cham.

[6] Gheisariy, M., Wang, G., Khanz, W. Z., and Christian Fernández-Campusano. (2019). A context-aware privacy-preserving method for iot-based smart city using software defined networking. Computers & Security, 87.

[7] Raut, S. D., Awasarmol, V. V., Ghule, B. G., Shaikh, S. F., Gore, S. K., and Sharma, R. P., et al. (2018). Corrigendum: γ-irradiation induced zinc ferrites and their enhanced room-temperature ammonia gas sensing properties (2018 mater. res. express 5 035702). Materials Research Express, 5(4), 049501 (1pp).

[8] Qiji, Q. U., and Lin, Z. (2018). Design and implementation of embedded multi-gateway system based on 6lowpan. Journal of Computer Applications.

[9] Swarup Kumar, J. N. V. R., and Suresh, D. (2021). Design and implementation of an adaptable trickle algorithm for amelioration of rpl usage in internet of things networks. Journal of Computational and Theoretical Nanoscience.

[10] Park, S., Park, S., Park, L., Park, S., Lee, S., and Lee, T., et al. (2018). Design and implementation of a smart iot based building and town disaster management system in smart city infrastructure. Applied Sciences, 8(11).

[11] Rahmani, A., Dibaj, M., Akrami, M., and Su, M. A. (2024). Enhancing Heat Storage Cooling Systems via the Implementation of Honeycomb-Inspired Design: Investigating Efficiency and Performance.

[12] Zhao, F., Zhu, W., Jiang, J., and Shan, Z. (2021). Design and implementation of intelligent meter reading system in smart power grid. Journal of Physics: Conference Series.

[13] Hussien, A. G., Sumit, K., Simrandeep, S., Jeng-Shyang, P., and Hashim, F. A. (2024). An enhanced dynamic differential annealed algorithm for global optimization and feature selection. Journal of Computational Design and Engineering (1), 1.

[14] Dominguezdager, B., Gomezdonoso, F., Roigvila, R., and Cazorla, M. (2024). Holograms for seamless integration of remote students in the classroom.
[15] Kwak, B. O., and Chung, T. S. (2018). Design and Implementation of Trust Domain Gateway System. 2018 International Conference on Information and Communication Technology Convergence (ICTC).
[16] Tariq, H., Abdaoui, A., Touati, F., Al-Hitmi, M. A. E., and Mnaouer, A. B. (2020). Design and Implementation of Cadastral Geo-spatial IoT Network Gateway Analyzer for Urban Scale Infrastructure Health Monitoring. 2020 10th Annual Computing and Communication Workshop and Conference (CCWC).
[17] Hadi, M. H., Issa, A. H., and Sabri, A. (2022). Modified salp swarm optimization algorithm (mssoa) based implementation of intelligent fault detection and isolation system for smart wireless sensor network.
[18] Rao, R. Y., Koola, J. J., Mehta, N. D., and Haque, A. M. (2019). Design and Implementation of Adaptive Control Algorithm for IoT Based Domestic Irrigation System. 2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT). IEEE.
[19] Sun, C., Zheng, F., Zhou, G., and Guo, K. (2020). Design and Implementation of Cloud-based Single-channel LoRa IIoT Gateway Using Raspberry Pi. 2020 39th Chinese Control Conference (CCC).
[20] Bhoir, R., Thakur, R., Tambe, P., Borase, R., and Pawar, S. (2020). Design and Implementation of Smart Compost System Using IOT. 2020 IEEE International Conference for Innovation in Technology (INOCON). IEEE.
[21] Tongkaw, S., and Tongkaw, A. (2018). Multi-Vlan Design Over IPSec VPN for Campus Network. ICWise 2018 IEEE Conference on Wireless Sensors. IEEE.
[22] Owada, Y., Sato, G., Temma, K., Kuri, T., and Nagano, T. (2019). An Implementation of Layer 2 Overlay Mesh Network and Edge Computing Platform for IoT. 2019 Twelfth International Conference on Mobile Computing and Ubiquitous Network (ICMU).
[23] Subratie, K., Aditya, S., and Figueiredo, R. J. (2023). Edgevpn: self-organizing layer-2 virtual edge networks. Future generations computer systems: FGCS.
[24] Stokes, J., and Barker, C. (2022). Think mass transit is ready for cybersecurity breaches? time to think again. Mass Transit (8), 47.

[25] Mochalski, K. (2022). Visibility and cybersecurity in energy companies from control room to the substation. vgbe energy journal.
[26] Barton, R. E., Henry, J., Yen, C. T., and Akhter, A. S. (2021). Automatic on-boarding agent for IOT edge routers in connected vehicles. US11064030B2.
[27] Maharaja, R., Iyer, P., and Ye, Z. (2020). A hybrid fog-cloud approach for securing the internet of things. Cluster Computing, 23(4).
[28] Shamsi, J. (2020). Security, privacy and trust in the iot environment. Computing reviews(12), 61.
[29] Dong, S., Li, Z., Tang, D., Chen, J., Sun, M., and Zhang, K. (2019). Your smart home can't keep a secret: towards automated fingerprinting of iot traffic with neural networks.
[30] Sartori, D., Zou, D., Pei, L., and Yu, W. (2023). Near-optimal 3d trajectory design in presence of obstacles: a convolutional neural network approach. Robotics and Autonomous Systems, 167.

Biographies

Yan Jiang graduated from Harbin University of Science and Technology with a master's degree in Electronic and Communication Engineering. I am currently employed at Fujian Provincial Highway Technology Innovation Research Institute Co., Ltd., familiar with the operation of Fujian's highway network, safety, and business. My research focuses on smart travel and safety assurance on highways.

Jing Huang is employed at Fujian Expressway Group Co., Ltd., serving as a supervisor in the Operations Management Department, engaged in daily service management and research work of transportation electromechanical engineering.

Yunsong Fan graduated from Peking University with a doctoral degree, currently employed at Fujian Expressway Science & Technology Innovation Research Institute Co., Ltd. as Deputy General Manager, with a research focus on expressway electromechanical informatization.

Xiaobin Zhu is currently the technical director of the Fujian branch of QiAnXin Technology Group Co., Ltd. He has more than ten years of work experience in the field of network security, and has previously worked for international network security companies such as Symantec, TrendMicro, and Veritas.