Research and Implementation of Forward Isolation Device Based on Security Consideration

Chuang PENG*, Shao-qian HU, Li LI, Zhen-yu TANG and Xiao-fei ZHOU
NR Electric Co. Ltd., Nanjing 211102, China
*Corresponding author

Keywords: Deep Packet Inspection (DPI), Two-factor, Encryption, Authentication.

Abstract. This paper presents a forward isolation device based on deep packet inspection and security enhancement to improve the security of power network in the new network security environment and distribution network environment. Based on the principle and vulnerability analysis of the traditional forward isolation device, by using FPGA as the isolated island component, the transmission speed is enhanced and the error bit rate is reduced. Deep packet inspection technology is designed to solve the reverse penetration threat, two-factor authentication technology is adopted to improve the security of HMI management. Moreover, the security of local management is further improved by the encryption and authentication method based on the SM serial algorithm. Therefore, isolation and security are greatly improved compared to traditional forward isolation devices. This scheme has been implemented in several projects and proven effective to improve security of the substation network.

Introduction

With the continuous development of computer network technology and the increasingly complex internal communication network of power systems, more and more cyber attacks intrude LAN of the power system [1,2]. These cyber attacks aimed at directly or indirectly destroying the power system infrastructure. Therefore, security of the power system SCADA network becomes more and more prominent. The forward isolation device is an important component of the power grid defense system. The isolation strength and security are directly related to the operational safety of the power grid.

On the other hand, distribution automation technology and business is an important component of the smart power grid, which has developed rapidly in recent years [3]. According to the relevant regulations, the production control area of the distribution network is required to use the wireless communication network or other external public data network in the vertical connection, it is necessary to design a secure access area. The forward isolation device is the core component of the distribution network security access area, and its network boundary location demands higher requirements on its isolation strength and security.

At present, the mainstream network isolation products mainly include Whale communication's e-GAP series and Spearhead's NETGAP series [4]. e-GAP series network isolation products implement network isolation and real-time data exchange through SCSI interface-based air switch. The main problem is that the system is based on Windows operation, which is detected to have a vulnerability that the preprocessor may be bypassed to obtain source code. NETGAP series network isolation products mainly use hardware-based reflection isolation gatekeepers to achieve isolation and data exchange, but it has also been detected that the content filtering mechanism may be bypassed. In China, many schemes are also proposed. A network isolated communication scheme against covert channels has been proposed in [5], which mainly solves the problem of potential data packet size covert channels and state information covert channels in different network communication protocols. The paper focuses on resisting against covert channel, but the safety of the device was not considered as a whole. In [6], a two-channel switch isolator with buffer is proposed, which adopts independent software switch control and modular design to solve the limitation of the existing product in hardware switch control. USB interface and control chip are used as the isolator. Its transmission speed and
security require to be further improved. In [7], a network isolation scheme using hardware partitioning and IP packet recovery content deep processing technology is proposed, which mainly solves the security isolation between external networks when multiple external networks are accessed. These documents are mainly analyzed from the local safety of the isolation device, and the safety design and solution are not provided as a whole.

Traditional forward isolation devices often require only password-based authentication when a user logs into the human-machine interface (abbreviated as HMI). It can be seen that the security of identity authentication has become a rigid requirement for forward isolation devices.

Traditional forward isolation devices typically use plain text communication when configured/managed locally. This may lead to a risk of eavesdropping or attack on devices configured with network ports. It can be seen that it is very necessary to ensure the confidentiality and reliability of the local management session through encryption and authentication technology.

Based on the analysis of the basic principle and vulnerability of the forward isolation device, this paper presents the design method and implementation of its isolated island security, data transmission security, identity authentication security and local management security. Therefore, isolation and security are greatly improved compared to traditional forward isolation devices.

**Basic Principle of Forward Isolation Device**

**Application Framework**

As shown in Fig. 1, the application system of the forward isolation device consists of LAN client, forward isolation device and WAN server.

![Figure 1. Forward isolation device application system framework.](image)

**Device Implementation Principle**

As shown in Fig. 2, forward isolation device application system framework mainly includes LAN/WAN CPU and isolated island.

![Figure 2. Forward isolation device application system framework.](image)

The inside of the forward isolation device must be implemented by means of “dual CPU + isolated island”. The data processing of LAN and external networks (abbreviated as WAN) is performed by 2 physically independent CPUs. The data interaction between the two CPUs is performed by a separate protocol through the isolated island. The forward isolation device completes the protocol conversion function by the cooperation of these 2 CPUs and the isolated island. The protocol conversion refers to the stripping and reconstruction of the protocol. At the end of the isolation product, the application data in the network-based public protocol is stripped out and packaged as the system-specific protocol, and then it will be passed to the other end of the isolation product. Finally, the proprietary protocol will be stripped and packaged into the required format [8-11].

Requirements for the isolated island for the forward isolation device are:
1) Provide a unique reliable physical channel;
2) Implemented by a proprietary protocol;
3) No network protocol stack;
4) Only one side is connected at any one time.

Information transmission process is shown in Fig. 3.

When LAN data requires to be sent to WAN, the LAN client immediately initiates a data connection to the isolated device. The isolation device strips all the protocols and writes the pure raw data into the high-speed data transmission channel. Data interaction with LAN can not be performed through the isolated island. Once the data is completely written into the one-way secure channel of the security isolation device, LAN side of the isolation device immediately disconnects the connection with LAN, pushing the data in the one-way security channel to the WAN side, and then WAN side receives the data and then initiates WAN data connection. When the response data of WAN requires to be transmitted to LAN, the data transmission needs to be performed through the dedicated secure channel of the isolation device, and the transmission principle is the same as above.

Traditional Forward Isolation Device Vulnerability Analysis

Isolated Island Security

Conventional forward isolation devices usually use high-speed FIFO chips as transmission channels. They are ease to use, transmission rate can meet the requirements, and product development cycle is short. But it is impossible to verify the data or suppress the interference generated by the hardware, which may cause errors in the transmitted data.

Data Transmission Security

As shown in Fig. 4, multi-condition message filtering requires to be supported by the forward isolation device. Filtering for the quintuple, MAC address, usage time and keyword is implemented by comparing actual packets with configuration rules. Filtering of the connection direction means that only the connection initiated from LAN is allowed for the TCP connection, and the TCP connection initiated from WAN requires to be blocked. UDP messages can only be sent from LAN to WAN. UDP messages from WAN to LAN will be blocked.
Reverse single-bit refers to the TCP packet sent from WAN to LAN. The application data is only allowed to carry 1 bit of data. Since the basic unit of the Ethernet transmission content is a byte, only the 0x00 or 0xFF application layer data transmission is allowed in the reverse direction. Reverse single-bit transmission is often used for acknowledgment or heartbeat response of application layer data.

LAN device can transmit data to WAN through the forward isolation device. WAN only responds to data through the single-bit mode of the TCP application layer. From the mechanism of layer-by-layer filtering and the limitation of reverse single-bit filtering, the possibility or data amount of transmitted from WAN to LAN is limited strictly. However, by analyzing the TCP protocol format and the possibility of IP and TCP packet header traversal reversely, the isolation mode can carry out reverse data transmission by carrying application data in IP or TCP packet header.

In a reverse TCP packet, up to 80 bytes of content can be carried from the IP and TCP headers through the forward isolation device. If there is a corresponding illegal program on LAN to analyze and process the content, isolation of the forward isolation device is greatly reduced, which may cause threat to reverse data security.

Design & Implementation Based On Deep Packet Detection & Security Enhancement

FPGA-based Bidirectional FIFO

In this scheme, FPGA is used to implement two-way FIFO, and FPGA itself is independent to LAN and WAN CPUs. The use of FPGA to design the isolated island not only ensures that the isolated island provides a unique and reliable physical channel for LAN and WAN CPU, but also ensures the real-time and high rate performance of the channel, the accuracy of data transmission and the flexibility of the interface.

The isolated island hardware mainly consists of one-way IO, data decoding module, 64kb FIFO buffer and protocol encoding module, as shown in Fig. 5.

In hardware application, the unidirectionality of the transmission IO is ensured. By increasing the bus width and other methods, the transmission efficiency of the FIFO is greatly improved. Moreover, data verification function is added in FIFO, data integrity verification is performed automatically, and the intermediate isolation island hardware interference error will be filtered. Therefore, stable and reliable data transmission is realized, and the requirements of the isolation island are met. Result of the test indicates that the isolated island of the FPGA can achieve a transmission rate of 700Mbps.

Data Transmission Based on Deep Packet Detection

Aiming at the reverse penetration threat of the traditional forward isolation device proposed in Section “Data Transmission Security”, this paper proposes a deep packet detection algorithm, which is different from the depth detection algorithm [12][13] for message content by hardware or software. This paper mainly checks the IP header and TCP header in the reverse TCP packet. The basis for the verification is derived from the specific application scenarios of forward isolation and the specific definitions of related options in RFC793, RFC1323 and RFC2018. The specific method is introduced as below.
For the IP header: If any of the following option types exist in the header of the IP packet, the detection fails, including security and processing restrictions, record path, timestamp, loose source route selection, and strict source route selection. These options are mainly used in the military field, record routing, and sender-specified routing scenarios. For forward isolation devices, their security requirements should not support the function of record routing, while hosts for LAN/WAN communication usually do not go through the router, when it requires to pass through the router, the source station routing function can not be adopted because the routing path can not be obtained.

For the TCP header, the following requirements must be satisfied:

1) The option type can only be limited to these 7 types as shown in Fig. 6:

   ![](image)

   Figure 6. TCP header optional content allowed to be transmitted.

   Where:
   ① Option table end;
   ② No operation;
   ③ Maximum segment length;
   ④ Window expansion factor;
   ⑤ Timestamp;
   ⑥ Selection confirmation including support for SACK option;
   ⑦ Selection confirmation including specific SACK information option.

2) These option types can only appear in the message containing the TCP flag SYN:
   Option type 3 (“Maximum segment length”),
   Option type 4 (“Window expansion factor”),
   Option type 6 (“Selection confirmation including support for SACK option”).

3) Option type 7 (“Selection confirmation including specific SACK information option”) can meet this criterion: the right edge value of each block of the confirmation number is greater than the left edge value, and all the confirmation numbers are within the sliding window of the opposite side.

For Requirement “1)”:
Option type 1 (“Option table end”) and Option type 2 (“No operation”) are the basic TCP header options;
Option type 3 (“Maximum segment length”) is used to indicate the maximum packet length that can be received when establishing a connection;
Option type 4 (“Window expansion factor”) and Option type 5 (“Timestamp”) are used to process the long fat pipeline;
Option type 6 (“Selection confirmation including support for SACK option”) and Option type 7 (“Selection confirmation including specific SACK information option”) are used for connections that support SACK.

These options have already covered the TCP header option in the forward isolation device application scenario.
Requirement “2)” and “3)” are derived from the RFC standard requirements for these header options. They are focused here to avoid malicious attackers trying to penetrated forward isolation device reversely by simply constructing a message that conforms to Requirement “1)”. If all the above 3 requirements are met, the test passes. Otherwise, the test fails.

Two-factor Based Identity

In this scheme, a combination of identity authentication based on password \cite{14} and UKEY-based identity authentication is proposed. The UKEY-based identity authentication mechanism will be introduced here. UKEY is a USB device that integrates smart card and card reader. It supports hot plug in/out and plug and play. UKEY’s own hardware determines that it can only be accessed through a dedicated interface, thus effectively protecting stored certificate in it \cite{15}.

Process of generating a user UKEY is introduced as below:

1) Insert UKEY into the USB port of the forward isolation device.
2) Initialize the PIN code of UKEY, encrypt it by SM4 algorithm and save it locally.
3) UKEY built-in encryption and decryption chip is used to generate SM2-based digital certificate. The private key is stored in the secure storage area of UKEY and can not be read, but the private key can be used for encryption or signature. The digital certificate is stored locally by the SM4 algorithm.

Local Management Based on SM serial Algorithm Encryption and Authentication

SM serial algorithm is a set of Chinese national standard cryptographic functions. In this scheme, the SM2-based public key \cite{16-17} encryption to allocate the SM4 symmetric key to achieve the confidentiality and authentication of the communication between the local management configuration tool and the device. Communication process is listed in Fig. 7.

![Figure 7. Key distribution with security and authentication.](image)

In the figure above, the client represents the debugging software, and the server represents the forward isolation device. PKc and PKs represent the public key of the client and server respectively, and the corresponding private keys are represented as SKc and SKs. E represents SM2 encryption.

Specific communication process is introduced as below:

1) Two sides of the communication will exchange public keys.
2) Client encrypts a random number N1 by using the public key PKs of the server, and then sends it to the server. N1 is used to uniquely identify the service.
3) After the server obtains N1, it generates a new random number N2, and encrypts N1 and N2 with the public key PKc of the client, and then sends it to the client. Because only the server can decrypt and obtain N1, the N1 sent by the server can make the client believe that the other side is indeed the server.
4) After obtaining N1 and N2, the client encrypts N2 with the public key PKs of the server, and then sends it to the server, so that the server can believe that the other side is indeed the server.
5) The client selects a symmetric encryption key Ks, and then sends the EPKs[EKs[Ks]] to the server. The server-side public key is used to ensure that only the client can interpret the encryption result. The client's private key is used to ensure that the encryption result can only be sent by the client.
6) After the server obtains Ks by decryption, both sides of the communication will use the Ks as the symmetric encryption key to perform confidential communication based on SM4 encryption.

The above key distribution process has confidentiality and authentication, which can prevent passive attacks and active attacks.
Application

Application of this scheme is listed in Fig. 8.

It is a 220kV substation, in which the security area 2 comprehensive application server needs to send online monitoring data to the control center. The online monitoring data will be first converted into a file, and then sent to the security area 3 data gateway through the forward isolation device, and finally sent to the control center side by the security area 3 data gateway.

In this substation, the forward isolation device realizes the transmission of file data from security area 2 to security area 3 by configuring the transparent mode. The transmission mode adopts a user-defined one-way TCP/IP protocol. The main transmission process is: firstly, the client transfers the file name and the file size, and then transfers the file content. Finally, the server replies 0x00 to indicate file transmission failure, and replies 0xFF to indicate file transmission success.

![Forward isolation device applied in substation](Figure 8)

Device failure/alarm contact is connected to the common bay control unit (abbreviated as BCU), and the device clock is synchronized by IRIG-B method. Test result indicates that the throughput of the device 1024-byte UDP packet is 173.972 Mbps, the forwarding delay is 2 ms, and the full-load data packet loss rate is 0, and stable long-time onsite operation is confirmed.

Test results of device safety are shown in Table 1.

<table>
<thead>
<tr>
<th>Item</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>DoS attack (80Mbps) test</td>
<td>OK</td>
</tr>
<tr>
<td>FUZZER test</td>
<td>OK</td>
</tr>
<tr>
<td>Stack Scrambler test</td>
<td>OK</td>
</tr>
<tr>
<td>Reverse penetration test</td>
<td>Illegal messages are prohibited</td>
</tr>
</tbody>
</table>

DoS attack includes the SYN/ICMP/UDP Flood attack; FUZZER test performs protocol fuzzing tests for common-used network protocols; Stack Scrambler test is mainly designed to verify the system protocol stack robustness after the packet is deformed in the IP layer, the TCP layer or the UDP layer.

Above 3 types of tests were performed by using IXIA PerfectStorm ONE, while the reverse penetration test mainly tests whether the packet can be sent from WAN to LAN by carrying illegal field information in the IP or TCP header.

Compared with the traditional forward isolation device, this device further improves the transmission rate and reliability through the isolation island built by FPGA, and further improves security of data transmission and one-way isolation by using the deep packet detection technology. Security of HMI management is further improved by two-factor identity authentication. Moreover, the security of local management is further improved by the encryption and authentication method based on the SM serial algorithm.
Detailed comparison is shown in Table 2. The “Isolated island data verification” can only rely on the application program to verify because the FIFO chip itself can not provide data verification. But the FPGA-based isolated island can realize data verification in various ways.

For security of reverse penetration, the traditional forward isolation device can only test the reverse single-bit of the application layer, but can not prevent the illegal content penetration of the IP or TCP header.

For identity authentication, traditional forward isolation device only supports password mode login, but does not support two-factor identity authentication.

For local management, the traditional forward isolation device uses serial port configuration or plaintext network port communication, and does not support communication methods based on encryption and authentication.

By usage of the above technologies, the boundary protection between the security area 2 and security area 3 of the substation is improved greatly.

<table>
<thead>
<tr>
<th>Item</th>
<th>Traditional forward isolation device</th>
<th>Forward isolation device in this scheme</th>
</tr>
</thead>
<tbody>
<tr>
<td>Isolated island data verification</td>
<td>Low</td>
<td>High</td>
</tr>
<tr>
<td>Reverse penetration security</td>
<td>Middle</td>
<td>High</td>
</tr>
<tr>
<td>Identity security</td>
<td>Low</td>
<td>High</td>
</tr>
<tr>
<td>Local management security</td>
<td>Low</td>
<td>High</td>
</tr>
</tbody>
</table>

**Conclusion**

This paper proposes design and implementation of forward isolation device based on deep packet detection and security enhancement. The deep packet detection technology can effectively avoid the reverse data transmission because protocol stripping in only performed in the network layer in the network isolation device (especially the one-way network isolation device). Therefore, the isolation between LAN and WAN is improved greatly, and the overall security of the system is enhanced.

By application of isolated island data verification, identity security and local management security, the security of device operation and maintenance is greatly improved. This paper mainly analyzes and designs the security for the application layer of the forward isolation device. Security of the operating system layer of the device requires further research and enhancement in the future.

The method proposed in this paper can also be applied to the traditional network isolation device, and it is applicable to the two-way transmission and processing of the message. This scheme has been implemented in several projects and proven effective to improve security of the substation network.

**References**


