Research on the Security Enhancement of MMS and DNP3 Communication Protocols

ICT Research Lab: Lin, Cheng-Hung; Huang, Wei-Heng

1. Research Background

With the deployment of advanced information and communication technologies (ICT) in power systems, traditional power grids are gradually transforming into smart grids. The interoperable IEC 61850 power system communication standard has many advantages. However, the widespread application of ICT may also make the power grid vulnerable to cyber-attacks as the grid becomes digitized. Recent power grid attack incidents, such as the Ukraine power grid blackout and the Stuxnet virus attack, are examples of such attacks. Therefore, preventing attacks on standardized communications in smart grids is an important security issue that must be considered during developing smart grids. Given this, the International Electrotechnical Commission (IEC) has published the IEC 62351 power system security standard, which provides security guidelines for protecting power systems.

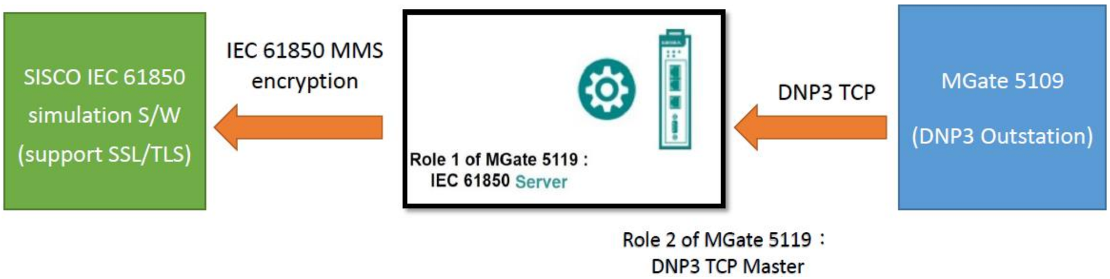
2. Research Content

In this research, we have established an MMS TLS transport layer encryption mechanism and a DNP3 application layer security authentication test platform in the laboratory to verify their effectiveness in enhancing security and resistance against replay attacks and man-in-the-middle attacks. The main research content and objectives are as follows:

1. Study the IEC 62351 security standards: IEC 62351-3(TCP/IP TLS encryption), IEC 62351-4 (MMS encryption), and IEC 62351-5 (DNP3 security authentication).
2. Based on IEC 62351-4 and -5, establish an experimental MMS Client/Server architecture with a TLS encryption transmission mechanism and a DNP3 Master/Outstation security authentication mechanism simulation platform.
3. Based on the simulation platform test results, provide technical specifications for implementing MMS TLS transport layer encryption and DNP3 security authentication.

3. Research Results

This research uses the test certificates provided by SISCO AX-S4 61850 simulation software. The certificates are configured in the test environment that simulates IEC 61850 Client/Server MMS packet transmission encryption established, as shown in Figure 1. After the Client/Server successfully verifies their respective certificates, they can establish a TLS connection. The MGate 5119 gateway converts DNP3 TCP packets into MMS packet format, implements IEC 61850 MMS encryption using the cipher suite recommended by IEC 62351-4 in Table 1, and verifies secure message exchange in the IEC 61850 Client/Server simulation environment. Since the packet is encapsulated with the TLS encryption algorithm, the Wireshark can neither parse the packet message nor display its content, so the message is protected during transmission (Figure 2).



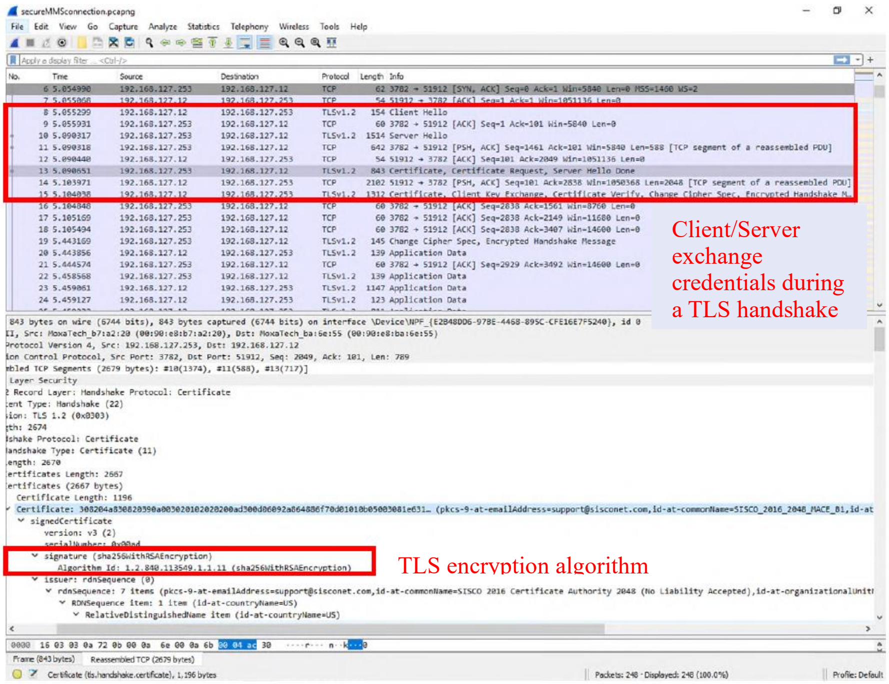
Source: This project

Figure 1 MMS encryption transmission test architecture diagram

Table 1 IEC 62351-4 cipher suites specification for native mode

Key Exchange		Encryption	Hash	Source	Support
Algorithm	Signature				
TLS_RSA_		WITH_AES_128_CBC_	SHA256	RFC 5246	m
TLS_DH_	RSA_	WITH_AES_128_CBC_	SHA256	RFC 5246	o
TLS_DH_	RSA_	WITH_AES_128_GCM_	SHA256	RFC 5288	m
TLS_DHE_	RSA_	WITH_AES_128_GCM_	SHA256	RFC 5288	m
TLS_DH_	RSA_	WITH_AES_256_GCM_	SHA384	RFC 5288	o
TLS_ECDHE_	RSA_	WITH_AES_128_GCM_	SHA256	RFC 5289	o
TLS_ECDHE_	RSA_	WITH_AES_256_GCM_	SHA384	RFC 5289	o
TLS_ECDHE_	ECDSA_	WITH_AES_128_GCM_	SHA256	RFC 5289	m
TLS_ECDHE_	ECDSA_	WITH_AES_256_GCM_	SHA384	RFC 5289	o

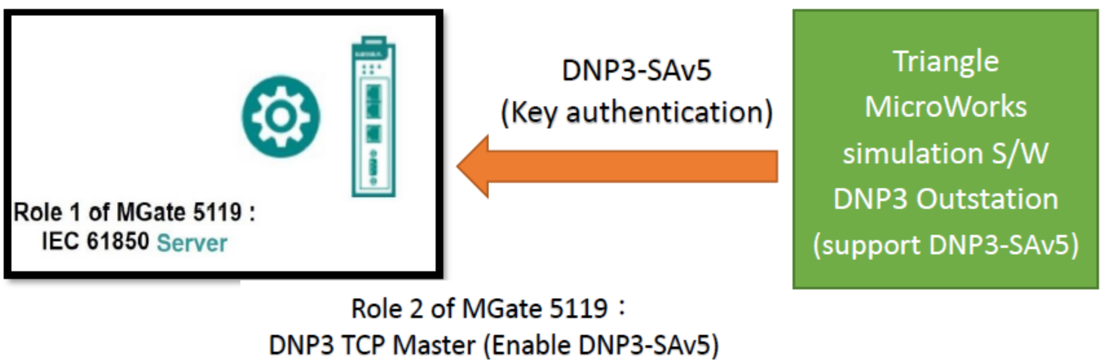
Source: IEC 62351-4



Source: This project

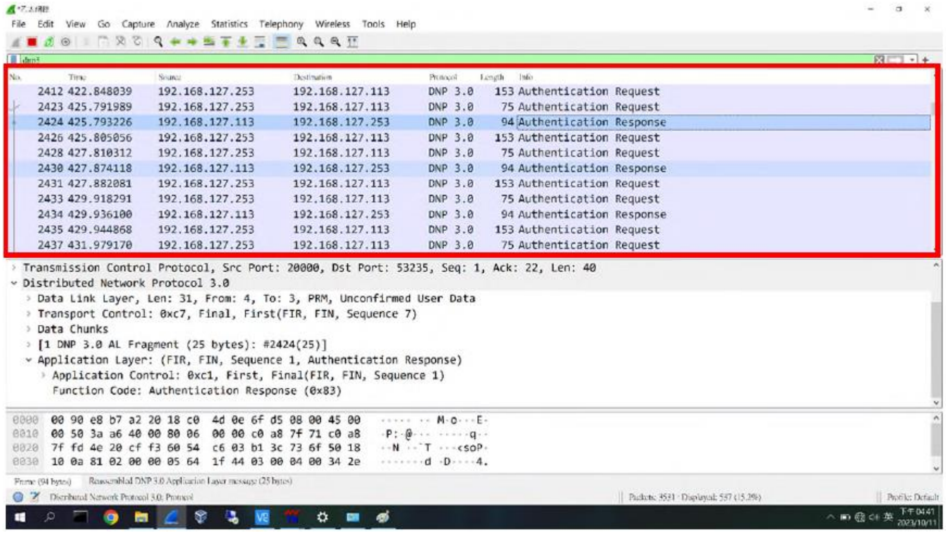
Figure 2　Client/Server exchange credentials during a TLS handshake

The DNP3 security certification test uses the DNP3-SAv5 security certification version based on the IEC 62351-5 security standard, using Triangle Microworks DNP3 Slave simulation software and the MGate 5119 gateway that plays the role of DNP3 Master for key certification (Figure 3). After the DNP3 Master/Slave security authentication connection setting is completed, the Wireshark intercepts the DNP3 communication packets and finds that the Client (Master) 192.168.127.253 sends an authentication request to the Server (Slave), and 192.168.127.113 responds with an authentication response, indicating that the security authentication connection is completed (Figure 4). After successfully passing the security authentication, the DNP3 message exchange is performed to confirm that the message is sent by an authorized person who has passed the identity authentication.



Source: This project

Figure 3　DNP3-SAv5 security certification test architecture diagram



Source: This project

Figure 4　DNP3 Master/Slave complete security authentication request and response

Table 2 compares TLS encryption security functions and DNP3 security authentication. TLS encryption focuses on protecting the confidentiality and integrity of transport layer communications through encryption and two-way identity authentication, while DNP3 security authentication provides security requirements such as a device-level authentication mechanism, data integrity, and message replay protection based on shared keys at the application layer. The research results can be applied to protect IEC 61850 MMS and DNP3 message transmission between smart substations and control centers to enhance the network communication security of the system.

Table 2　Comparison of security features for TLS and DNP3-SA

Protocol security features	TLS	DNP3-SA
Communication session authentication	Yes	No
Spoof protection (device authentication)	Yes	Yes
Eavesdropping protection (confidentiality)	Yes	No
Tamper protection (integrity)	Yes	Yes
OSI hierarchy	Transport layer	Application layer
Message replay protection	Yes	Yes
Effective message retention and flood protection	No	Yes
Out-of-order message protection	No	Yes
Support symmetric keys	No	Yes
Support asymmetric keys	Yes	Yes (SAv5 only)

Source: This project