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, standardized preventing attacks on 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:

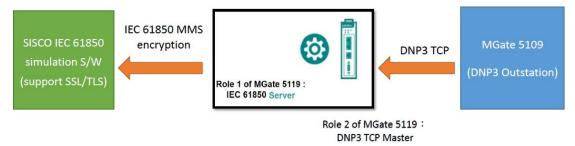
Study the IEC 62351 security standards:
IEC 62351-3(TCP/IP TLS encryption), IEC 62351-4 (MMS encryption), and IEC 62351 5 (DNP3 security authentication).

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.

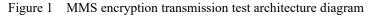
3. Based on the simulation platform test results, provide technical specifications for implementing MMS TLS transport layer encryption and DNP3 security authentication.

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



Key Exchange		Encryption	Hash	Source	Support
Algorithm	Signature	Encryption	114511	Source	Support
TLS_RSA_		WITH_AES_128_CBC_	SHA256	RFC 5246	m
TLS_DH_	RSA_	WITH_AES_128_CBC_	SHA256	RFC 5246	0
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	0
TLS_ECDHE_	RSA_	WITH_AES_128_GCM_	SHA256	RFC 5289	0
TLS_ECDHE_	RSA_	WITH_AES_256_GCM_	SHA384	RFC 5289	0
TLS_ECDHE_	ECDSA_	WITH_AES_128_GCM_	SHA256	RFC 5289	m
TLS_ECDHE_	ECDSA_	WITH_AES_256_GCM_	SHA384	RFC 5289	0

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

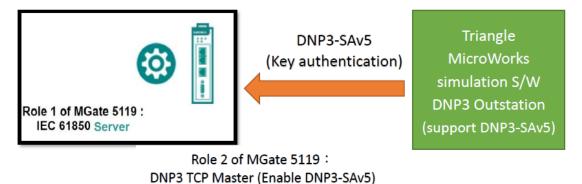
Source: IEC 62351-4

oply a display Rt	<cul-></cul->				
Time	Source	Destination	Protocol	Length Info	
6 5.0549		192.168.127.12	TCP	62 3782 - 51912 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=	1460 W5+2
7 5,8558		192,168,127,253	TCP	54 51912 + 3782 [ACK] Seg=1 Ack=1 Win=1051136 Len=0	
B 5.0552		192.168.127.253	TLSv1.2	154 Client Hello	
9 5.0559		192.168.127.12	TCP	60 3782 + 51912 [ACK] Seq=1 Ack=101 Win=5840 Len=0	
10 5.0903		192.168.127.12 192.168.127.12	TLSV1.2 TCP	1514 Server Hello	an free second of a second list of second
12 5.0904		192.168.127.12	TCP	642 3782 → 51912 [P5H, ACK] Seq=1461 Ack=101 Win=5840 Len=50 54 51912 → 3782 [ACK] Seq=101 Ack=2049 Win=1051136 Len=0	as [ICP segment of a reassembled PD0]
12 5.0904		192.168.127.12	TLSV1.2	843 Certificate, Certificate Request, Server Hello Done	
14 5.1039		192.168.127.253	TCP	2102 51912 + 3782 [PSH, ACK] Seg=101 Ack=2838 Win=1050368 Let	122848 [TCP segment of a reassembled POUL
15 5,1040		192,168,127,253		1312 Certificate, Client Key Exchange, Certificate Verify, C	
16 5,1048		192,168,127,12	TCP	60 3782 - 51912 [ACK] Seq=2838 Ack=1561 Win=8760 Len=0	
17 5.1051		192.168.127.12	TCP	60 3782 + 51912 [ACK] Seg-2838 Ack-2149 Win-11680 Len-0	
18 5.1054	4 192.168.127.253	192.168.127.12	TCP	60 3782 + 51912 [ACK] Seq=2838 Ack=3407 Win=14600 Len=0	Client/Server
19 5.4431	9 192.168.127.253	192.168.127.12	TLSv1.2	145 Change Cipher Spec, Encrypted Handshake Message	
20 5.4438	6 192.168.127.12	192.168.127.253	TLSv1.2	139 Application Data	exchange
21 5.4445		192.168.127.12	TCP	60 3782 + 51912 [ACK] Seq=2929 Ack=3492 Win=14600 Len=0	exenange
22 5,4585	8 192,168,127,253	192.168.127.12	TLSv1.2		
				139 Application Data	cradentials during
23 5.4598	1 192.168.127.12	192.168.127.253	TLSv1.2	1147 Application Data	credentials during
23 5.4598 24 5.4591 bytes on wi col Version ontrol Prot TCP Segnen or Security	1 192.168.127.12 7 192.168.127.12 192.168.127.12 192.168.127.12 192.168.127.12 192.168.127.12 192.168.127.158 197.121.108.127.158 col, Src Port: 3782, Det s (2679 bytes): #10(1374	192.168.127.253 192.168.127.253 captured (6744 bits) 2:20), Dst: MoxaTech_E Dst: 192.168.127.12 Port: 51912, Seq: 284), #11(588), #13(717)]	TLSv1.2 TLSv1.2 on interfac ba:6e:55 (00	1147 Application Data 123 Application Data 20	credentials during a TLS handshake
23 5.4598 24 5.4591 24 5.4591 25 5.4591 26 5.4591 27 6.4592 24 5.4591 24 5.4592 24 5.4592 24 5.4592 24 5.4592 24 5.4598 24 5.45988 24 5.45988 24 5.45988 24 5.45988 24 5.45988 24 5.45988 24 5.45988 24 5.45988 24 5.4598578 24 5.4598578578250557575	1 192.168.127.12 7 192.166.127.12 96.6744 bits), 848 bytes byts:22 009406 e82b73 4, Src: 192.168.127.253, col, Src: Port: 3782, Dat x (2679 bytec): #18(1374 andshake Protocol: Certi ake (22)	192.168.127.253 192.168.127.253 captured (6744 bits) 2:20), Dst: MoxaTech_E Dst: 192.168.127.12 Port: 51912, Seq: 284), #11(588), #13(717)]	TLSv1.2 TLSv1.2 on interfac ba:6e:55 (00	1147 Application Data 123 Application Data 20	0
23 5.4598 24 5.4591 24 5.4591 24 5.4591 24 5.4591 25 6 6 6 6 6 6 6 6 6 6 6 6 6 6 6 6 6 6 6	1 192.168.127.12 7 192.166.127.12 96.6744 bits), 848 bytes byts:22 009406 e82b73 4, Src: 192.168.127.253, col, Src: Port: 3782, Dat x (2679 bytec): #18(1374 andshake Protocol: Certi ake (22)	192.168.127.253 192.168.127.253 captured (6744 bits) 2:20), Dst: MoxaTech_E Dst: 192.168.127.12 Port: 51912, Seq: 284), #11(588), #13(717)]	TLSv1.2 TLSv1.2 on interfac ba:6e:55 (00	1147 Application Data 123 Application Data 20	0
23 5.4598 24 5.4591 24 5.4591 25 5.4591 26 5.4591 27 5.4592 24 5.5592 24 5.5	1 192.168.127.12 7 192.166.127.12 96.6744 bits), 848 bytes byts:22 009406 e82b73 4, Src: 192.168.127.253, col, Src: Port: 3782, Dat x (2679 bytec): #18(1374 andshake Protocol: Certi ake (22)	192.168.127.253 192.168.127.253 captured (6744 bits) 2:20), Dst: MoxaTech_E Dst: 192.168.127.12 Port: 51912, Seq: 284), #11(588), #13(717)]	TLSv1.2 TLSv1.2 on interfac ba:6e:55 (00	1147 Application Data 123 Application Data 20	0
23 5.4590 24 5.4591 c: MaxaTec col Version antrol Prot Security and Layer: ype: Hands TLS 1.2 (0 674 : Protocol:	1 192.168.127.12 192.168.127.12 (6574 bits), 843 bytes b7ta2:20 (00:00:081b7:a 4, Src: 192.168.127.153, col, Src Pert: 3782, Dbt s (2679 bytes): #10(1374 andshake Protocol: Certisake (22) 300)	192.168.127.253 192.168.127.253 captured (6744 bits) 2:20), Dst: MoxaTech_E Dst: 192.168.127.12 Port: 51912, Seq: 284), #11(588), #13(717)]	TLSv1.2 TLSv1.2 on interfac ba:6e:55 (00	1147 Application Data 123 Application Data 20	0
23 5.4598 24 5.4591 c: MoxaTec ol Version ntrol Prot TCP Segmen Security rd Layer: ype: Hands TLS 1.2 (0 674 Protocol: ake Type: 1	1 192.168.127.12 192.168.127.12 (65744 bits), 843 bytes b712128 (0690688b71) 4, Src: 192.168.127.253, col, Src Port: 3782, Dat s (2679 bytes): #18(1374 andshake Protocol: Certis ske (22) 308) Certificate	192.168.127.253 192.168.127.253 captured (6744 bits) 2:20), Dst: MoxaTech_E Dst: 192.168.127.12 Port: 51912, Seq: 284), #11(588), #13(717)]	TLSv1.2 TLSv1.2 on interfac ba:6e:55 (00	1147 Application Data 123 Application Data 20	0
23 5.4590 24 5.4591 24 5.4591 24 5.4591 24 5.4591 24 5.4591 24 5.4591 24 5.4591 24 5.4591 24 5.4592 24 5.4592 24 5.4592 24 5.4592 24 5.4592 24 5.4590 24 5.4590 24 5.4590 24 5.4590 24 5.4590 24 5.4590 24 5.4590 24 5.4591 24 5.4	1 197.166.127.12 (6744 bit), 843 bytes b/1a2.20 (00:00:00:00 (a, scr: 102.168.127.132 c, scr: 102.168.127.333 cal, scr: 102.168.127.333 cal, scr: 102.168.127.333 cal, scr: 102.168.127.333 and/sket Portcol: Certia det (22) 2003) Certificate certificate certificate certificate certificate certificate certificate certificate certificate	192.168.127.253 192.168.127.253 captured (6744 bits) 2:20), Dst: MoxaTech_E Dst: 192.168.127.12 Port: 51912, Seq: 284), #11(588), #13(717)]	TLSv1.2 TLSv1.2 on interfac ba:6e:55 (00	1147 Application Data 123 Application Data 20	0
23 5.4590 24 5.4591 24 5.4591 24 5.4591 24 5.4591 24 5.4591 24 5.4591 24 5.4591 24 5.4591 24 5.4591 25 5.2591 24 5.2591 25 7.2591 25 7.2	1 197.166.127.12 7 192.166.127.12 6 (574 bits), 843 bytes b7122120 (00:00:0105), 843 bytes b7122120 (00:00:0105), 843 bytes b7122120 (00:00:0105), 843 bytes c), 55c Port: 3782, DOI c), 55c Port: 3782, DOI c) (22) c) (23) c) (2)) c) (2)	192.168.127.253 192.168.127.253 captured (6744 bits) 2:20), Dst: MoxaTech_E Dst: 192.168.127.12 Port: 51912, Seq: 284), #11(588), #13(717)]	TLSv1.2 TLSv1.2 on interfac ba:6e:55 (00	1147 Application Data 123 Application Data 20	0
23 5.4590 24 5.4591 24 5.4591 24 5.4591 24 5.4591 24 5.4591 24 5.4591 24 5.4591 24 5.4591 25 5.00 24 5.259 25 7.259 26 7.259 27 7.259 27 7.259 27 7.259 27 7.259 28 7.259 28 7.259 28 7.259 28 7.259 28 7.259 28 7.259 29 7.259 20 7	1 197.166.127.12 (6744 bit), 843 bytes b/12.12 (06006.127.12 (6744 bit), 843 bytes b/12.12 (06006.017.13 cd, src: 102.168.127.33, cd, src: 102.168.127.33, cd, src: 102.168.127.33, andshake Protocol: Certi de (22) 000) Certificate ertificate (11) th: 2867 7 bytes) gth: 1196	122.165.127.253 122.166.127.253 122.166.127.253 122.109.127.253 1220), Dzt: Moxalech, Dzt: 122.168.127.12 Post: 122.168.127.12 Post: 123.168.127.12 Post: 123.168.127.13 Ficate	TLSVI.2 TLSVI.2 on interfactoris (94 199, Ack: 181	1147 application Data 123 Application Data 123 Application Data 129 Application Data 129 Application State 129 Application State 129 Application State 129 Application Data 129 A	a TLS handshake
23 5.4590 24 5.4591 24 5.4591 24 5.4591 24 5.4591 24 5.4591 24 5.4591 24 5.4591 24 5.4591 24 5.4591 25 5.4591 24 7.2591 24 7.2591 24 7.2591 24 7.2591 24 7.2591 24 7.2591 25 7.5	1 197.168.127.12 (6744 bits), 843 bytes b)122/20 (00700-001), 843 bytes b)122/20 (00700-001), 843 bytes b)122/20 (00700-001), 843 bytes b)122/20 (0070-001), 843 bytes b)122/20 (0070-001), 843 bytes b)122/20 (0070-001), 843 bytes s (227) bytes); 810(1374 sc(22)) 2083) Certificate certificate certificate certificate (21) b)128 bytes 2095) Certificate (21) b)128 bytes 2095) Certificate (21) b)128 bytes 2095) Certificate (21) b)128 bytes (21) Certificate (21) b)128 bytes (22) Certificate (21) b)128 bytes (22) Certificate (2	122.165.127.253 122.166.127.253 122.166.127.253 122.109.127.253 1220), Dzt: Moxalech, Dzt: Moxalech, Dzt: Moxalech, Dzt: Moxalech, Dzt: Moxalech, Dzt: Moxalech, 27.12 Port: 5192.68, dzt.27.12 Port: 5192.58, dzt.27.12 Port	TLSVI.2 TLSVI.2 on interfactoris (94 199, Ack: 181	1147 Application Data 123 Application Data 20	a TLS handshake
23 5.4590 24 5.4591 24 5.4591 24 5.4591 24 5.4591 24 5.4591 24 5.4591 24 5.4591 24 5.4591 24 5.4591 25 5.2591 24 5.2591 25 7.2591 25 7.2	1 197.166.127.12 197.166.127.12 C 197.161.177.12 C 197.161.177.12 C 197.161.177.12 C 197.161.177.12 4. Sec.197.181.177.137 andshake (P21) 2009 C 2079 bytes): #10(1374 amdshake (P21) 2009 C 2079 bytes): #10(1374 C 2079 bytes): #10(1374 C 2079 bytes): #10(1374) 2 bytes): gth: 1196 NEO46220398005020000	122.165.127.253 122.166.127.253 122.166.127.253 122.109.127.253 1220), Dzt: Moxalech, Dzt: Moxalech, Dzt: Moxalech, Dzt: Moxalech, Dzt: Moxalech, Dzt: Moxalech, 27.12 Port: 5192.68, dzt.27.12 Port: 5192.58, dzt.27.12 Port	TLSVI.2 TLSVI.2 on interfactoris (94 199, Ack: 181	1147 application Data 123 Application Data 123 Application Data 129 Application Data 129 Application State 129 Application State 129 Application State 129 Application Data 129 A	a TLS handshake
23 5.4590 24 5.4591 24 5.4591 24 5.4591 24 5.4591 24 5.4591 24 5.4591 24 5.4591 24 5.4591 24 5.2591 25 5.2591 24 5.2591 25 5.5	1 197.166.127.12 197.166.127.12 C 197.161.177.12 C 197.161.177.12 C 197.161.177.12 C 197.161.177.12 4. Sec.197.181.177.137 andshake (P21) 2009 C 2079 bytes): #10(1374 amdshake (P21) 2009 C 2079 bytes): #10(1374 C 2079 bytes): #10(1374 C 2079 bytes): #10(1374) 2 bytes): gth: 1196 NEO46220398005020000	122.165.127.253 122.166.127.253 122.166.127.253 122.109.127.253 1220), Dzt: Moxalech, Dzt: Moxalech, Dzt: Moxalech, Dzt: Moxalech, Dzt: Moxalech, Dzt: Moxalech, 27.12 Port: 5192.68, dzt.27.12 Port: 5192.58, dzt.27.12 Port	TLSVI.2 TLSVI.2 on interfactoris (94 199, Ack: 181	1147 application Data 123 Application Data 123 Application Data 129 Application Data 129 Application State 129 Application State 129 Application State 129 Application Data 129 A	a TLS handshake
23 5.4590 24 5.4591 24 5.4	1 197.166.127.12 4 (2744 bit27, 124 4 (2744 bit27, 124 4 (2744 bit27, 124 4 (2744 bit27, 124 5 (2776 bytes); 2 (2776 byte	102.66.127.753 102.66.127.753 Captured (CF4 B1t5) Captured (CF4 B1t5)	TLSVI.2 TLSVI.2 on interfactoris (94 199, Ack: 181	147 Application Data 123 Application Data 123 Application Data 124 Application Data 125 Application Data 126 Application (Application Data 127 Application Data 128 Application Data 128 Application Data 129 Appli	a TLS handshake
23 5.4590 24 5.4591 24 5.4591 24 5.4591 24 5.4591 24 5.4591 24 5.4591 24 5.4591 24 5.4591 24 5.4591 25 7.4591 24 7.2591 24 7.2591 24 7.2591 24 7.2591 24 7.2591 24 7.2591 24 7.2591 24 7.2591 24 7.2591 25 7.2591 25 7.2591 25 7.2591 26 7.2591 26 7.2591 26 7.2591 26 7.2591 26 7.2591 26 7.2591 26 7.2591 26 7.2591 26 7.2591 27 7.2591 26 7.2591 27 7.2591 27 7.2591 27 7.2591 27 7.2591 27 7.2591 28 7.2591 29 7.2591 20 7.2	1 197.166.127.12 192.166.127.12 (6744 bits), 843 bytes b712/23 (00:00:00:00:00 (4, 5xc: 192.160:127.53), col, 5xc (92.160:127.53), col, 5xc (92.160:127.53), col, 5xc (97.160:127.53), col, 5xc (97.160:12	102.06.127.753 102.06.127.753 102.061.127.04 122.061.127.04 1220).00117.0010001 1220).00117.0010001 1220).00117.001000 101192.001100000000000000000000000000000	TLSVI.2 TLSVI.	147 Application Data 123 Application Data 123 Application Data 124 Application Data 125 Application Data 126 Application (Application Data 127 Application Data 128 Application Data 128 Application Data 129 Appli	a TLS handshake
23 S.4598 24 S.4591 24 S.4591 24 S.4591 24 S.4591 24 S.4591 24 S.4591 24 S.4591 24 S.4591 24 S.4591 25 S.4591 24 S.2592 25 S.2	1 197.168.127.12 7 197.168.127.12 7 197.168.127.12 7 197.168.127.12 7 197.168.127.12 7 197.108.127.135 7 197.03 8 197.127.21 (199.168.127.235) 8 (287 bytes) = \$10(1)74 8 and habe Protocol: Certi 9200) Certificate ertificate ertificate 10: 2367 7 hytes) 10: 1367 7 hytes) 10: 1367 10: 1287 7 hytes) 10: 1287 7 hytes) 10: 1287 10: 128	102.46.127.35 102.46.127.45 102.46.127.45 102.46.127.45 102.46.127.45 102.46.127.45 104.102.46.127.15 104.102.46.127.15 104.102.46.127.15 104.102.46.127.15 104.102.46.127.15 104.102.46.127.45 104.102.45 104.102.	TLSVI.2 TLSVI.2 on interfarance	187 Application Data 123 Application Data 124 Application Data 124 Application Data 125 Application Data 125 Application Data 128 TLS encryption algorithm	a TLS handshake
23 S.4500 24 S.4501 24 S.4501 25 S.4	1 197.168.127.12 197.168.127.12 (6744 bits), 843 bytes byts2120 (001001081710 col, 574 bits), 843 bytes (1974 bits), 843 bytes (1970 bytes), 810 bits (1970 bits), 810 bits), 81	102.46.127.35 102.46.127.25 102.46.127.25 102.46.127.25 102.46.127.45 102.46.127.45 102.46.127.45 102.4	TLSVI.2 TLSVI.2 on interfarance	147 Application Data 123 Application Data 123 Application Data 124 Application Data 125 Application Data 126 Application (Application Data 127 Application Data 128 Application Data 128 Application Data 129 Appli	a TLS handshake
23 S.4500 24 S.4501 24 S.4501 25 S.4501 26 S.4501 27 S.4501 26 S.4	1 197.166.127.12 197.166.127.12 197.166.127.12 197.166.127.12 197.166.127.12 197.167.127.127 197.167.127.157 4. Seci 192.166.127.235 4. Seci 192.166.127.235 198.127.235 2020 2	102.66.127.53 102.66.127.53 102.66.127.53 102.66.127.53 102.66.127.64 102.66.127.13 102.66.127.13 1041 102.66.127.13 1041 102.16.127.13 1041 102.157.13 1041 102.157.137.13 1041 102.157.137.137 1041 102.157.137.137 1041 102.157.137.137 1041 1041 1041 1041 1041 1041 1041 1041	TLSV1.2 TLSV1.2 Son Arteria Sar6255 (% S9, Ack: 182 Sa6f7ad0101 Scruption)	187 Application Data 123 Application Data 124 Application Data 124 Application Data 125 Application Data 125 Application Data 128 TLS encryption algorithm	a TLS handshake
22 5.4590 24 5.4591 24 5.4591 25 5.4591 26 5.4591 27 5.5591 27 5.55911 27 5.55911000000000000000000000000000000000	1 197.168.127.12 197.168.127.12 (6744 bits), 843 bytes byts2120 (001001081710 col, 574 bits), 843 bytes (1974 bits), 843 bytes (1970 bytes), 810 bits (1970 bits), 810 bits), 81	102.66.127.53 102.66.127.53 102.66.127.53 102.66.127.53 102.66.127.64 102.66.127.13 102.66.127.13 1041 102.66.127.13 1041 102.16.127.13 1041 102.157.13 1041 102.157.137.13 1041 102.157.137.137 1041 102.157.137.137 1041 102.157.137.137 1041 1041 1041 1041 1041 1041 1041 1041	TLSV1.2 TLSV1.2 Son Arteria Sar6255 (% S9, Ack: 182 Sa6f7ad0101 Scruption)	187 Application Data 123 Application Data 124 Application Data 124 Application Data 125 Application Data 125 Application Data 128 TLS encryption algorithm	a TLS handshake

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 connection authentication 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

dent						
o, Tirac	Sound	Destination	Protocol	Eength Info		
2412 422.848039	192.168.127.253	192.168.127.113	DNP 3.0	153 Authentication	Request	
2423 425.791989	192.168.127.253	192.168.127.113	DNP 3.0	75 Authentication	Request	
2424 425.793226	192.168.127.113	192.168.127.253	DNP 3.0	94 Authentication		
2426 425.805056	192.168.127.253	192.168.127.113	DNP 3.0	153 Authentication	Request	
2428 427.810312	192.168.127.253	192.168.127.113	DNP 3.0	75 Authentication	Request	
2430 427.874118	192.168.127.113	192.168.127.253	DNP 3.0	94 Authentication	Response	
2431 427.882081	192.168.127.253	192.168.127.113	DNP 3.0	153 Authentication	Request	
2433 429.918291	192.168.127.253	192,168,127,113	DNP 3.0	75 Authentication	Request	
2434 429.936100	192.168.127.113	192.158.127.253	DNP 3.0	94 Authentication	Response	
2435 429.944868	192.168.127.253	192.168.127.113	DNP 3.0	153 Authentication	Request	
2437 431.979170 Transmission Contr Distributed Networ > Data Link Layer,	192.168.127.253 ol Protocol, Src Port k Protocol 3.0 Len: 31, From: 4, To	192.168.127.113 1: 20000, Dst Port: 53 0: 3, PRM, Unconfirmed	DNP 3.0 8235, Seq: 1 d User Data	75 Authentication		
2437 431.979170 Transmission Contr Distributed Networ > Data Link Layer, > Transport Contro > Data Chunks > [1 DNP 3.0 AL Fr > Application Layer > Application Layer	192.168.127.253 ol Protocol, Src Port k Protocol 3.0 , Len: 31, From: 4, To bl: 0xc7, Final, First ragment (25 bytes): # er: (FIR, FIN, Sequent ontrol: 0xc1, First,	192.168.127.113 t: 20000, Dst Port: 53 o: 3, PRM, Unconfirmed t(FIR, FIN, Sequence 7 2424(25)] ce 1, Authentication F Final(FIR, FIN, Sequen	DNP 3.0 3235, Seq: 1 d User Data 7) Response)	75 Authentication		
2437 431.979170 Transmission Contr Distributed Networ > Data Link Layer, > Transport Control Data Chunks > [1 DNP 3.0 AL F, Application Layer > Application Co Function Code 000 00 90 e8 D7 az 00 00 50 as a6 44	192.168.127.253 ol Protocol, Src Port & Protocol 3.0 Len: 31, From: 4, Tc bi: 0xc7, Final, First right, Fin, Sequen control: 0xc1, First, : Authentication Resp 2 20 18 c0 4d 0e 6f 9 06 80 60 00 00 c	192.168.127.113 :: 20000, Dst Port: 53 o: 3, PRM, Unconfirmed ((TIR, FIN, Sequence 1 2424(25)] ce 1, Authentication R Final(FIR, FIN, Sequenonse (0×83) d5 08 00 45 00 87 77 1.0 a 8 P:-{	DNP 3.0 3235, Seq: 1 d User Data 7) Response) nce 1) 	75 Authentication , Ack: 22, Len: 40		
2437 431.979170 Transmission Contr Distributed Networ Data Link Layer, Transport Contro Data Chunks 1 10MP 3.0 AL Fr Application Layer Application Code 000 00 90 00 57 3: 10 00 50 3a a6 44 000 7 fd 42 80 c: 10 00 81 80 20	192.168.127.253 101 Protocol, Src Port k Protocol 3.0 Len: 31, From: 4, Tr li: 0xc7, Final, First vagment (25 bytes): #2 r: (FIR, FIN, Sequene ontrol: 0xc1, First, : Authentication Resp 2 20 18 c0 4d 0e 6f 0	192.168.127.113 :: 20000, Dst Port: 53 o: 3, PEN, Unconfirmer t(FIR, FIN, Sequence 7 2424(25)] ce 1, Authentication F Final(FIR, FIN, Sequenous onse (483) d: 68 00 45 00 a8 7f 71 c0 a8 P: 4 3c 73 6f 96 18 M	DNP 3.0 3235, Seq: 1 d User Data 7) Response) nce 1)	75 Authentication , Ack: 22, Len: 40		

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 device-level as а

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.

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)	

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

Source: This project