International Journal of Multimedia and Ubiquitous Engineering
Vol.11, No.10 (2016), pp.381-396
http://dx.doi.org/10.14257/ijmue.2016.11.10.36

Research on Dynamic Compliance Analysis Technology of IEC 62351 Standard Based on Finite State Machine Theory

Wang Chen, Ma Yuanyuan, Shao Zhipeng, Huang Xiuli and Fei Jiaxuan

Institute of Information and Communication, State Grid Global Energy Interconnection Research Institute, Nanjing 210003, China
wangchen@geiri.sgcc.com.cn, mayuanyuan@geiri.sgcc.com.cn, shaozhipeng@geiri.sgcc.com.cn, huangxiuli@geiri.sgcc.com.cn, feijiaxuan@geiri.sgcc.com.cn

Abstract

With the development of power industry, communication security has become an important issue affecting the stability of power system. IEC 62351 standard provides security for substation communication system. However, different transmission protocols may lead to different manufacturers to produce different understanding, manufacturing is not compatible with the device. In order to avoid such a situation, the Finite State Machine (FSM) theory is used to model and analyze the transmission protocol of IEC 62351 standard. In this paper, the FSM model is simulated by the StateFlow tool, and it can be considered that the FSM theory is applicable to the analysis of compliance with IEC 62351 standard.

Keywords*: power system, IEC 62351 standard, compliance analysis, Finite State Machine, StateFlow*

1. Introduction

With the rapid development of computer technology, the main equipment of the substation gradually realize intelligent, on the basis of the full realization of digital and new type of substation, the traditional substation is gradually transformed into the intelligent substation [1]. IEC 61850 standard is the international standard of substation communication network and system, but it does not contain security measures, which brings the power system communication transmission protocol security issues [2]. Therefore International Electric Committee aimed at main substation communication protocol and formulated the IEC 62351 security international standard, this standard greatly improves the transmission protocol security, providing a guarantee for the security of substation communication systems and networks. In a manner of speaking, the IEC 62351 standard is the soul of power communication network security.

But because various transmission protocols have many functions and parameters that need to be set, as an international standard, it is impossible to specify the specific implementation methods, such as the technology platform, programming languages, data structures and so on , different product designers and producers may also will make different understandings and interpretations of the same transmission protocol, and there will be some human errors, there will be huge differences in the products with the same transmission protocol which will affect interoperability between products. In order to ensure that the communication software products and equipment can be connected properly, improve interoperability between different products, it is a very necessary measure to carry out transmission protocol security compliance analysis.

Now the main direction of the transmission protocol security compliance analysis includes FSM model, Unified Modeling Language (UML), Markov Chains and so on. The

ISSN: 1975-0080 IJMUE

FSM model is the most widely used, which is suitable for the safety compliance analysis of IEC 62351 standard.

The structure and main contents of this paper are as follows: the second part introduces the background and main content of IEC 62351 standard; the third part introduces the theory of FSM and its components; the fourth part introduces how to use the FSM model to model the IEC 62351 standard; the fifth part focuses on the modeling of TLS protocol using the FSM model; in the sixth part, the security compliance analysis of transmission protocol is carried out by experiment simulation; the seventh part of paper were summarized in this paper.

2. IEC 62351 Standard Introduction

2.1. IEC 62351 Standard Background

Intelligent substation is an important node in the smart grid, its most important feature is “An intelligent device, the two device network, in compliance with the IEC 61850 standard". However, due to the openness and standardization of the transmission protocol, and the current power system communication standards (*i.e*. IEC 61850 standard) itself does not involve security issues. It is urgent to design a new communication transmission protocol with security measures [3].

In 2007 the International Electrotechnical Commission (IEC) aimed at the related communication transmission protocol (DNP 3.0, IEC 61970, IEC 61850, IEC 61850-5, IEC 61850-6 and IEC 61968 Series) and developed new data and communication security standard-IEC 62351 standard. IEC 6235 l is committed to solve the problem of the present situation of the smart grid information security [4].

The key technologies used in the IEC 62351 standard including: data encryption technology, message digest, digital signature, digital certificates and other, these means used to realize the control of access to physical security, make the electric power system run safely and stably [5]. In the IEC62351 standard, authentication and encryption is the core content. Authentication is to ensure the legitimacy and integrity of the information communication; the role of encryption is to ensure the privacy of the information in the communication process, to prevent hackers access to important information.

2.2. The Main Content of the IEC 62351 Standard Adopted in this Paper

Substation Automation System (SAS) has three major functions: control, monitoring and protection, the system is logically divided into 3 layers: substation level, bay level and process level.

The internal communication protocol for substation system includes Transport Layer Security (TLS) protocol, Manufacturing Message Standard (MMS), Generic Object Oriented Substation Event (GOOSE), Sampled Measured Value (SMV) and so on [6].

The TLS protocol security enhancement relates to a transmission layer; MMS protocol security enhancement involves application layer of network four layer structure model, applied to the substation level and the bay level. GOOSE and SMV security enhancement is located above the data link layer.

The network four layer structure corresponding to each communication transmission protocol is shown in Figure 1.

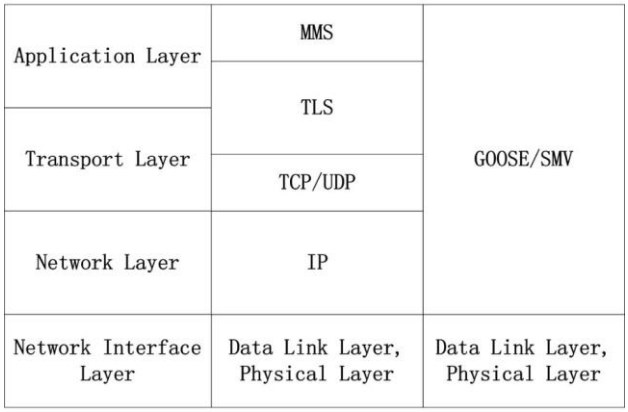

Figure 1. The Network Four Layer Structure Corresponding to Transmission Protocol

IEC 62351 standard has a total of 11 parts. This chapter mainly introduces the IEC 62351 standard cited in this paper:

(1) IEC 62351-3: provide any security standards including TCP/IP, stipulating using TLS protocol instead of reestablishing. TLS protocol is generally used for security interaction on the Internet, including authentication, confidentiality and integrity. IEC 62351-3 also put forward a series of mandatory requirements for the use of TLS to protect the TCP/IP network security solutions, including prohibiting the use of non -encrypted cipher suite; V1.0 TLS that corresponds to more than v3.1 SSL (v3.1 SSL or higher) is allowed.; Message Authentication Code (MAC) should be used; the exchange and confirmation of the certificate shall be two-way, if any party entity does not provide a certificate, the connection shall be terminated; each reference standard should provide a separate TCP/IP port, through this port to exchange the communication flow through the TLS protection, *etc.* [7].

(2) IEC 62351-4: security standard containing the MMS protocol. MMS is an industrial control system communication protocol for bidirectional message communication between programmable devices in computer integrated manufacturing environment. MMS as a real time communication protocol of application layer, the realization of the substation level and bay level communication in the support of computer integrated manufacturing environment. Application layer requires configuring and using the TLS protocol (including authentication, security measures) to protect the security of MMS communication [8].

(3) IEC 62351-6: the security of IEC 61850 peer to peer communication platform. This paper mainly introduces how to provide security mechanism for GOOSE and SMV in the data link layer [9].

3. FSM Theory

The main direction of security compliance analysis of transmission protocol is the formal description and test sequence generation of transmission protocol. Formal description is to avoid the two meaning of transmission protocol description. The main formal description meanings include UML, Markov Chains, FSM model, *etc.*

Using FSM description close to the block diagram of the program, is easier to implement, simultaneously more widely practical value with FSM, for example: FSM can perform precise mathematical calculations, and can be used as a basis for verification of time sequence completeness [10].

The FSM model is the most widely used of the three models, in this paper, we will focus on the FSM.

3.1. FSM Theory Summary

FSM is a mathematical model with discrete inputs and outputs, which is a kind of discrete input and output, which is a kind of finite state calculation process and some language classes [11]. In real life, which can be abstracted as the actual case of the FSM model exist some common characteristics: predictable system will be in a determined state; number of finite state; the presence of input events; input will trigger a series of events, including the implementation of specific functions, resulting in the corresponding output; after the input event is finished, the state is transferred to a relatively stable new state [12].

3.2. Component Elements of FSM

The FSM defined in this paper consists of states, events, transformations, and activities. Each state has a state entry action and a state exit action, each of which has an initial state and a target state associated with the event. When in the initial state, the event occurs and the monitoring condition of the trigger switch is true, the following actions are executed sequentially [13].

(1) The initial state of the exit action;
(2) Switching action;
(3) Entry action of the target state

FSM can be formalized as a one-dimensional array of five elements:

$$M = (Q, \Sigma, T, \sigma, q_0) \tag{1}$$

Among them, Q is the set of finite state, in the determination of arbitrary moment, FSM can only be in a certain state; Σ is for poor event input set, in the determination of arbitrary moment, FSM only receiving a certain input; T is for the conversion of nonempty set; σ is mapping function, $\sigma = Q_i \Sigma \to T, (i = 1,2,3\cdots)$; q_0 is the initial state, $q_0 \in Q$, FSM start receiving input.

Each element in the T can be represented as an array of five elements:

$$T = (SS, TS, IE, Constra\,\text{int}, Action) \tag{2}$$

The SS represents the initial state of the T, the TS represents the target state of T, the IE means that the input event from the Σ (or null), the $Constra\,\text{int}$ indicates the monitoring condition and the input event parameter and so on, the $Action$ indicates the action of the conversion. The main conversion process of FSM is shown in Figure 2.

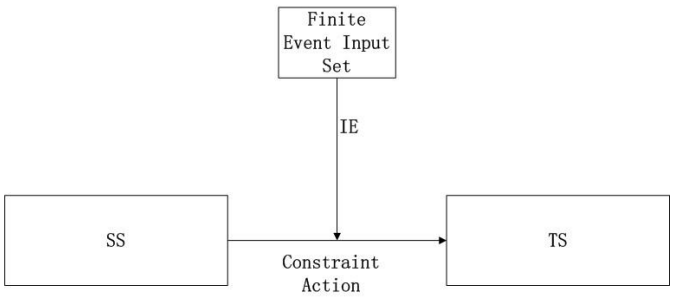

Figure 2. State Transition Process in FSM

4. IEC 62351 Transport Protocol Security Analysis Model

Security compliance analysis of transmission protocol based on FSM refers to: under the given requirements design standards, for a realized system, the FSM model is used to model and analyze the system, to detect whether the system is fully realized and fully meet the given demand design standard [14].

In the IEC 62351 standard, there are two means of communication: one is client / server (C/S) mode, another is subscriber / publisher model. C/S mode can be used for MMS protocol and TLS protocol. It is mainly used to connect the two sides. It is relatively high reliability of the connection process, while providing the end to the end of the information flow control. Subscriber / publisher model is mainly used for GOOSE which services for higher time requirements and SMV services based on the transmission cycle. It provides a one-way information exchange, and is used to send information from multiple sources and information exchange between the publisher and multiple subscribers [15].

4.1. Transmission Protocol Modeling Process

The main objects of observation of security compliance analysis of transmission protocol are Protocol Data Unit (PDU) and the send / receive order of Service Primitive. There are four main types of service primitive: request, indication, response and confirm.

In the FSM service primitives can be used as a finite input event sets Σ, $\Sigma = \{req, ind, rep, con\}$ which req represents request; ind represents indicate; rep represents response; con represents confirmation.

$Q = \{ReqS, IndS, RepS, ConS\}$ in the corresponding C/S mode, $ReqS$ represents the request state; $IndS$ represent the indicate state; $RepS$ represents the response state, $ConS$ indicates the confirm state. As shown in Figure 3.

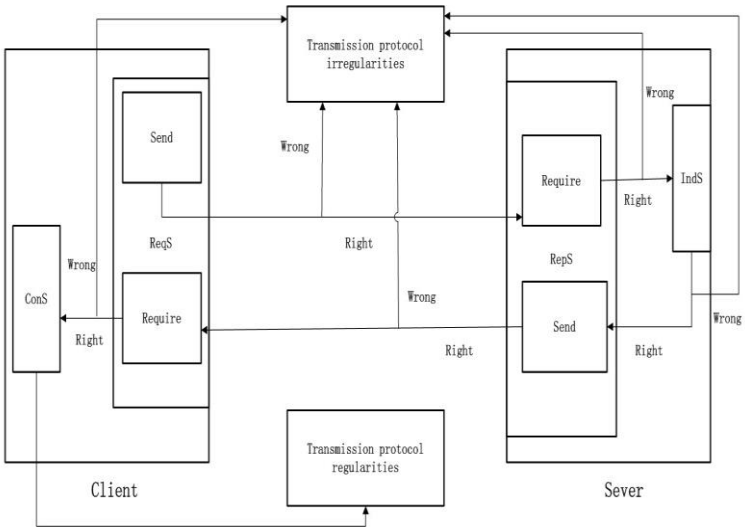

Figure 3. C/S Mode

Publisher finite state set of subscriber / publisher is:

$Q = \{Stop, Retransmission\ Pending, Retransmission\}$, which $Stop$ represents the stop state, $Retransmission\ Pending$ represents the pending retransmission pending state, $Retransmission$ represents retransmission state. As shown in Figure 4.

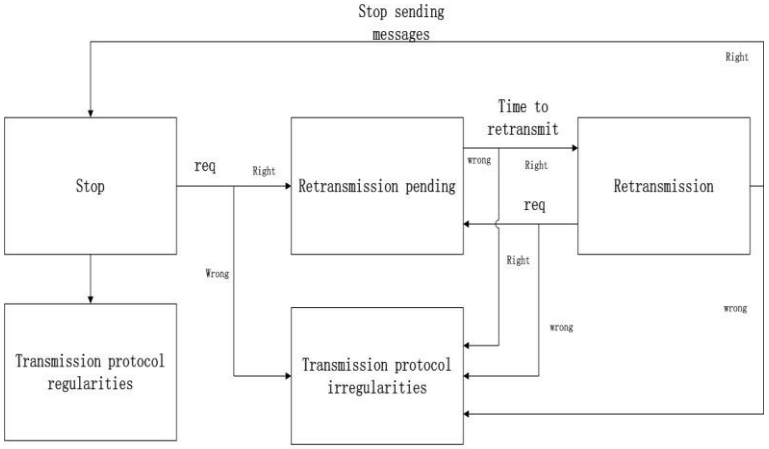

Figure 4. Publisher Mode of Subscriber / Publisher Mode

4.2. The Process of Compliance Analysis of Transmission Protocol

According to the model in the previous section, for communication network in the new interactive process, the process is brought into the model. According to the final state of the implementation of the FSM to judge whether it meets the requirements of the IEC62351 statute provided for safety.

To analyze whether the transmission function satisfies the requirements of the secure transmission protocol, FSM model can be established for an entity that has been implemented in the following 3 processes:

(1) Analysis of the specific content of the transmission protocol and requirements standard;

(2) According to the transmission protocol to establish the state set, event set, mapping function, and further establish the FSM model.

(3) To analyze whether the transmission protocol fully realize and meet the requirements of the design standards.

5. Case Analysis

This chapter studies the application of IEC 62351-3 in the Smart Substation, analyzes how to use TLS Record Layer protocol and TLS Handshake protocol to enhance the security of the communication system for Smart Substation. After that uses the FSM modeling to analyze the compliance of the designed security solutions in actual power communication.

5.1. Main Content of TLS Protocol

The TLS protocol consists of two protocols which belong to different levels: Record protocol and Handshake protocol, these two protocols can provide a connection to the application layer and the TCP/IP layer, this connection is a secure connection through authentication and confidentiality. The top layer of the TLS Record Protocol includes four protocols: TLS Handshake protocol, TLS Change Encryption Standard protocol, TLS Warning protocol and TLS Application Data protocol [16]. Details of the TLS protocol structure as shown in Figure 5.

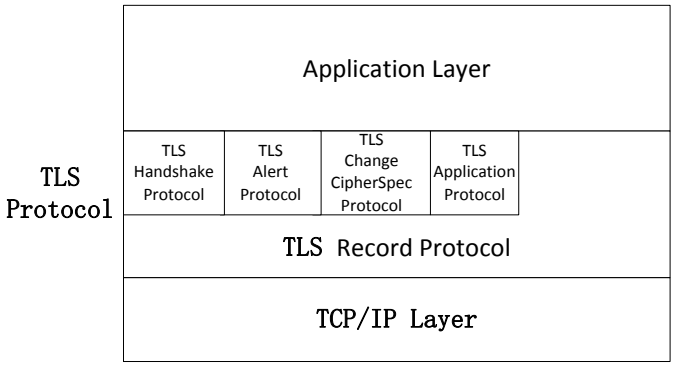

Figure 5. TLS Protocol Architecture

5.1.1. TLS Record Layer Protocol

The TLS Record Layer protocol relies on reliable communication protocol (TCP protocol), which is at the bottom of the TLS protocol, and is used for the transparent encapsulation of various advanced application layer protocol.

If the equipment is the client, its working principle is: First, need to make data that needs to be sent packet, and according to the need to choose whether or not to carry on the data compression processing. Then use the hash function to compute the MAC of the data packet. Finally, encrypt the data and send it. Involves the TLS three service functions: to ensure data integrity; data encryption; the legitimacy of the authentication server and client [17].

If the device is a server, its working principle is: reverser operation to receive messages, including decryption, authenticate MAC value, decompression, reorganization, and transfer the data to the application layer protocol [18].

5.1.2. TLS Handshake Protocol

TLS Handshake protocol is located at the top of the TLS protocol, which is based on the Record Layer protocol, and the handshake protocol can be used to complete the following four major functions [19]:

(1) Consult with the encryption algorithm and compression algorithm between client and server;

(2) Consult with random key for the selected encryption algorithm;

(3) Mutual authentication between client and server;

(4) Negotiation to achieve the Negotiation to achieve the advanced features of session reuse.

In addition, TLS protocol has sub protocols: TLS Change Encryption Standard Protocol, TLS Warning Protocol and TLS Application Data Protocol.

5.2. Transmission Protocol Modeling Process

This paper introduces the process of modeling the TLS transmission protocol using the FSM theory. First, introducing the modeling of the TLS Record Layer protocol by the FSM theory, then introduce the modeling of the TLS Handshake protocol by the FSM theory [20].

5.2.1. Modeling of the TLS Record Layer Protocol by FSM

Modeling of the TLS Record Layer protocol by the FSM theory, it is divided into client state conversion and server state conversion. Client state transitions as shown in Figure 6 below.

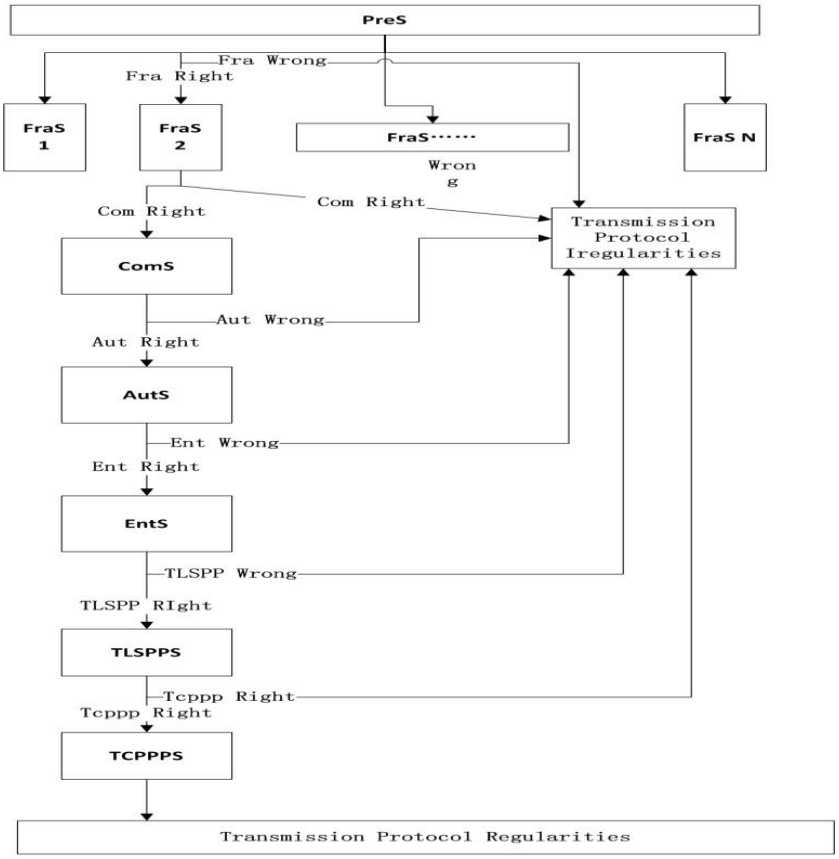

Figure 6. Client State Transition Diagram

Server state transition is the corresponding inverse operation, this paper no longer gives the specific state transition diagram.

As mentioned above, FSM can be formalized as an array of five elements, $M=(Q,\Sigma,T,\sigma,q_0)$.

Now we can set the array:

$$Q=\{Pres,FraS,ComS,AutS,EntS,TLSPPS,TCPPS\} \tag{3}$$

$Pres$ represents an application layer message ready state. $FraS$ represents the message fragment state, $ComS$ represents the compressed state, $AutS$ represents the authentication state, $EntS$ represents the encrypted state, $TLSPPS$ represents the TLS protocol packaging state, $TCPPS$ represents the TCP packaging state.

$$\Sigma=\{Fra,Com,Aut,Ent,TLSPP,TCPPP\} \tag{4}$$

Fra represents fragment, Com represents compress, Aut represents authenticate, Ent represents encryption, $TLSPP$ represents TLS protocol packaging, $TCPPP$ represents TCP protocol packaging.

$$q_0=\{PreS\} \tag{5}$$

The specific state transition process is [21]:

(1) Fra: After the TLS record layer receives the upper data, it is fragmented into blocks equal to or less than 214 bytes. TLS records support the organization of data from multiple high-level protocols to a fragment.

(2) Com: Compression using a compression algorithm specified in the current state, the compression algorithm must be lossless compression and the length of the compression should not exceed 1024 bytes of the original length. If the decompression function produces more than 214 bytes, then a fatal error is returned;

(3) Aut: In order to protect the data from malicious modification in the process of transmission, increasing MAC in the end of the data fragment. Make the receiver judge the correctness and completeness of the data

(4) Ent: According to the establishment of a secure connection in the process of client and server encryption suite, encrypting the data of the upper layer after compression and add the MAC.

(5) $TLSPP$: Join the TLS record header;

(6) $TCPPP$: Join the TCP header.

5.2.2. Modeling of the TLS Handshake Protocol by FSM

FSM can be formalized as an array of five elements, and now it should be divided into client states and events, server states and events.

5.2.2.1. Client States and Events

Client states

$$Q_1 = \{Null, Creating, Exchange, Commit, Commit2, Open\} \tag{6}$$

Among them, $Null$ represents client starting state; $Creating$ represents the state that the client sends a connection request and waits for the server to respond; $Exchange$ represents starting key negotiation state; $Commit$ represents key negotiation success state; $Commit2$ represents the state that the client notifies server to complete negotiation; $Open$ represents the state that the client receives the server response, completes the negotiation, and the client can transmit application data in the future.

Client events

$$\Sigma_1 = \{C.req, C.cnf, E.res, Commit.req, Commit.cnf\} \tag{7}$$

Among them, $C.req$ represents the event that client generates a connection request ClientHello, and sends it to the server; $C.cnf$ represents the event that the client receives server connection response; $E.res$ represents the event that the client forms client key negotiation message and certificate; $Commit.req$ represents the event that the client sends Change Ciper Spec message, notifies the server to submit the results of the consultation; $Commit.cnf$ represents the event that the client notifies server to complete negotiation; $Open$ represents the event that the client receives the submission of the consultation response of server.

$$q_0 = \{Null\} \tag{8}$$

5.2.2.2. Server States and Events

Sever state

$$Q_1 = \{Null, Creating, Created, Exchange, Opening, Open\} \tag{9}$$

Among them, $Null$ represents the state that the server waits for client connection request; $Creating$ represents the state that the server receives the client connection request message and enters the algorithm choice stage; $Created$ represents the state that the server completes the algorithm selection and enters the key negotiation stage; $Exchange$ represents the state that the server generates its own key agreement and certificate message, and waits for the client key agreement message after sends them to the client; $Opening$ represents the state that the server receives the client's key negotiation message and certificate, calculates the data required for the secure connection, and waits for the confirmation of this agreement; $Open$ represents the state that the server receives the information obtained through the consultation of the algorithm and the key encryption data to obtain the confirmation, the handshake process is completed.

Sever event

$$\Sigma_1 = \{C.ind, C.res, E.ger, E.cnf, Commit.ind\} \tag{10}$$

Among them, $C.ind$ represents the event that server receives ClientHello message from the client; $C.res$ represents the event that the server generates SevrerHello message; $E.ger$ represents the event that the server generates Certificate and Sever Key Exchange message; $E.cnf$ represents the event that the client $E.res$ event is completed; $Commit.ind$ represents the event that the server receives application data on the established connection for the first time.

$$q_0 = \{Null\} \tag{11}$$

5.2.2.3. The Specific Process of TLS Handshake Protocol

The whole handshake protocol can be divided into three stages:

(1) Create: The client sends a connection request to the server, and the server responds to the request.

The client generates a connection request ClientHello message, the main content is to send the relevant parameters of the connection, including version number, encryption algorithm and compression algorithm to client. And to send a connection request to the server, wait for the server to respond. At this point the client state from $Null$ to $Creating$.

The server receives the client request, completes the algorithm choice, generates the SeverHello message. C/S enters the key negotiation stage. At this point the server state transits from $Null$ to $Creating$, and then transits to $Created$.

(2) Exchange: C/S exchange key negotiation information.

Server generates its own key negotiation and certificate message, together with the SeverHello message to send to the client, waits for the client key negotiation. At this time the server state is transited to $Exchange$.

The client receives the server response and key exchange information, completes the key exchange, sends the key exchange information to the server, and the key negotiation is completed. At this point the client state is transited to $Commit$ state.

(3) Commit: C/S exchange of negotiation information, notify the other part of the success of the algorithm and key.

The server receives the client key agreement information. Calculates the data required for a secure connection, and starts to wait for this negotiation to be confirmed. The server is transited to $Opening$ state.

The client generates Cipher Spec Change message, notifies server to submit the results of the negotiation. At this point, the client is transited to $Commit2$ state.

The server receives the negotiation algorithm and the encrypted data, negotiation is confirmed, responds to the results of the negotiation. Server Handshake process is complete. The server is transited to $Open$ state.

Figure 7 shows the status of the client and the server in the TLS Handshake protocol state transition diagram.

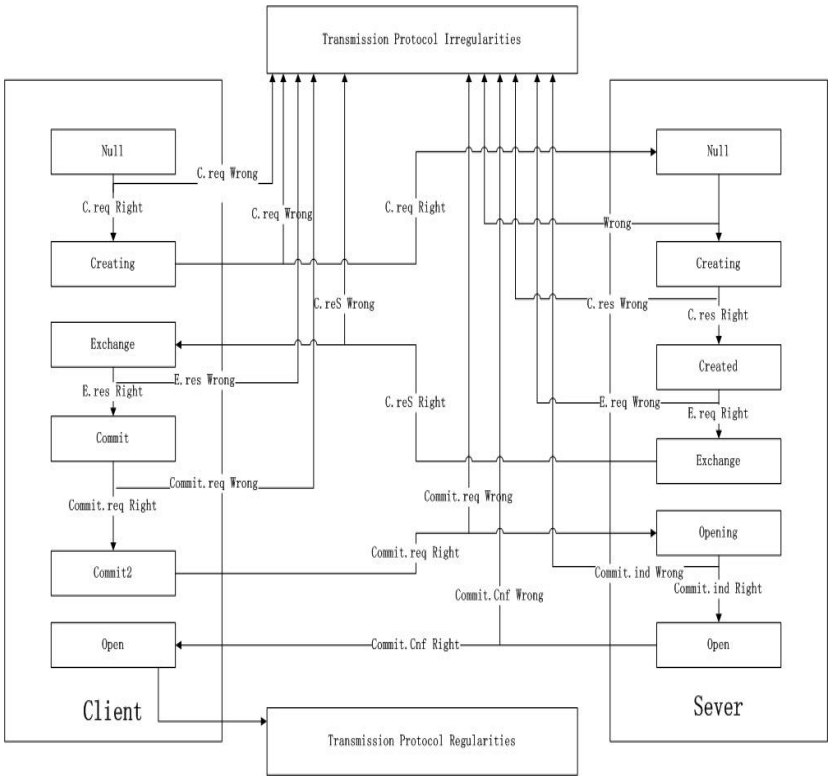

Figure 7. The Status of the Client and the Server in the TLS Handshake Protocol State Transition

6. Experiment and Analysis

This chapter uses the StateFlow tool in Matlab, Stateflow is a graphical tool for FSM. It can be implemented by graphical tools in different states transition. It allows users to draw a FSM model through graphical tools (such as Chart), which can be implemented on the system simulation.

The experiment mainly aimed at the TLS Record Layer protocol which using FSM simulation. Figure 1 represents this event occurs correctly, Figure 0 represents that the event did not happen correctly or complete, a total of seven sets of test sequences, as shown in Table 1.

Table 6-1. Test Sequences

No \	Fra	Com	Aut	Ent	TLSPP	TCPPP	Test sequences
1	X	-	-	-	-	-	(0,0,0,0,0,0)
2	√	X	-	-	-	-	(1,0,0,0,0,0)
3	√	√	X	-	-	-	(1,1,0,0,0,0)

4	√	√	√	X	-	-	(1,1,1,0,0,0)
5	√	√	√	√	X	-	(1,1,1,1,0,0)
6	√	√	√	√	√	X	(1,1,1,1,1,0)
7	√	√	√	√	√	√	(1,1,1,1,1,1)

This experiment selected Ent failed. When Ent fails, that is, the test sequence is (1,1,1,0,0,0). The oscilloscope display is 0, we can get the conclusion that the transmission protocol is irregular, specifically as shown in Figure 8 and Figure 9.

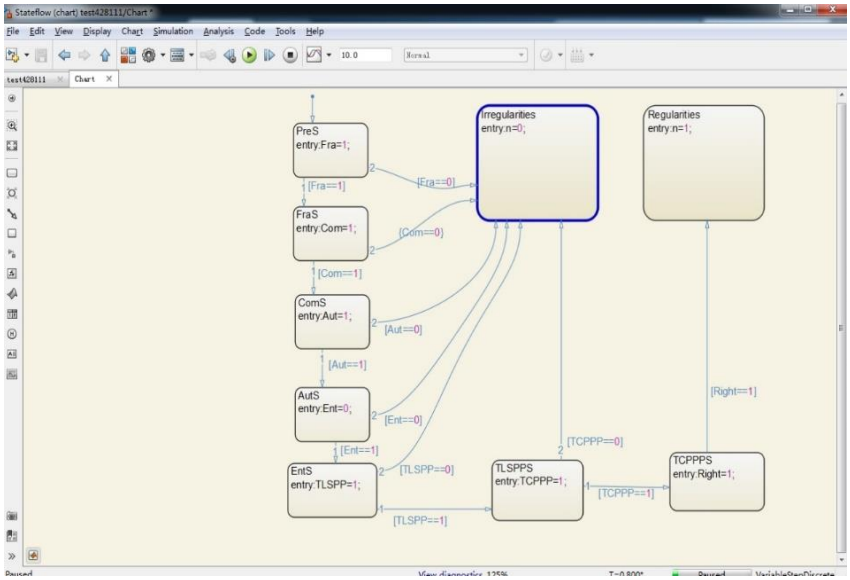

Figure 8. StateFlow Diagram of Irregular Transmission Protocol

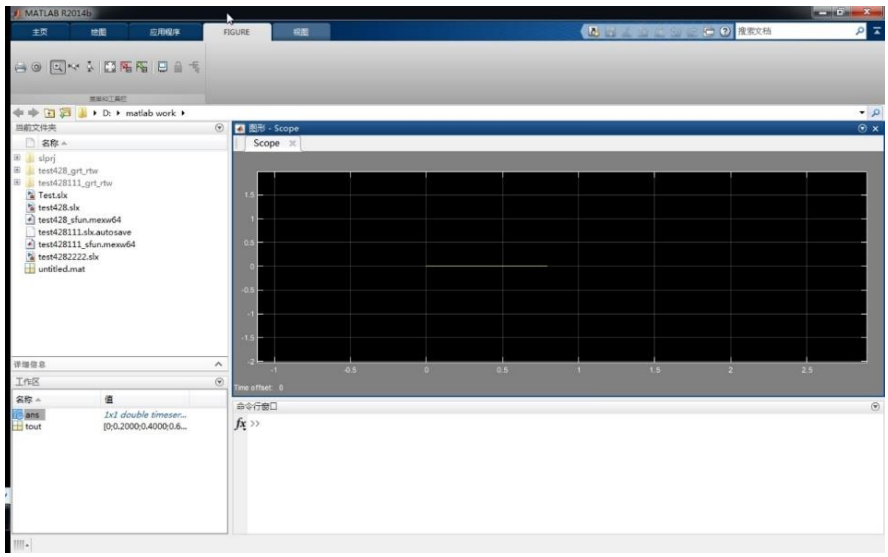

Figure 9. Scope Diagram of Irregular Transmission Protocol

When the transmission protocol is successfully implemented, that is, the test sequence is (1,1,1,1,1,1). The oscilloscope display is 1, we can get the conclusion that the transmission protocol is regular, specifically as shown in Figure 10 and Figure 11.

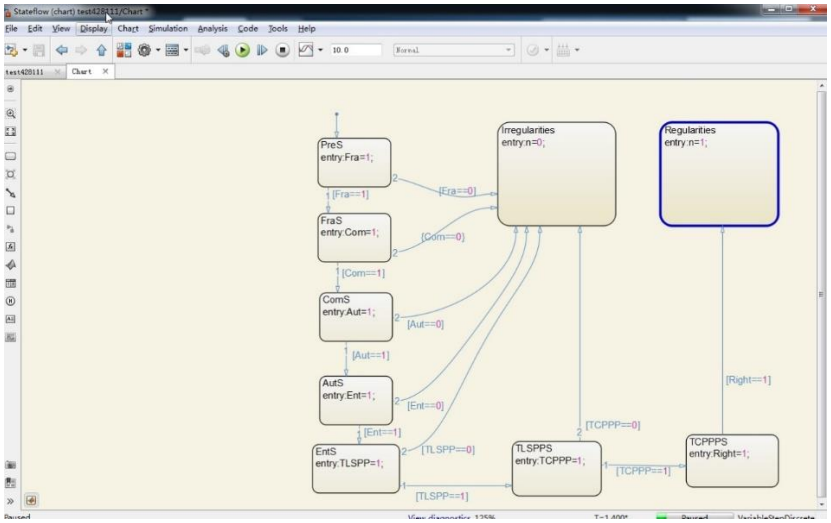

Figure 10. StateFlow Diagram of Regular Transmission Protocol

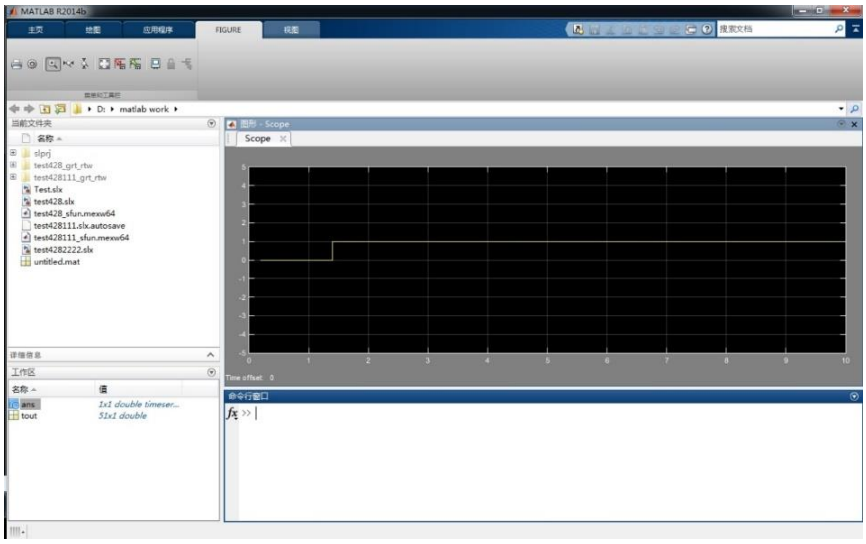

Figure 11. Scope Diagram of Regular Transmission Protocol

7. Conclusion

According to the requirements of the actual power system transmission protocol security compliance analysis, this paper firstly introduces the establishment background of IEC 62351 standard, and several communication protocols in substation system are introduced briefly: TLS, MMS, GOOSE, SMV, as well as the contents of the IEC 62351 standard referenced in this article. Secondly, the theory of FSM and its components are introduced. And then introduces the FSM theory of compliance analysis, and using FSM to model IEC62351 standard, making experimental simulation. Finally, the experiment uses the StateFlow tool to simulate the TLS Record Layer protocol, and verifies the compliance of the transmission protocol with different test sequences. It is considered that FSM is an effective theory for the safety analysis of IEC 62351 transmission protocol. In the actual power system in the future, FSM theory can be used to realize the programming language, and the use of Smart Substation security system, to further ensure the communication security of Smart Substation.

References

[1] U. C. Netto, D. de C. Grillo, I. D. Lonel, E. L. Pellini and D. V. Coury, "Journal Electric Power Systems Research", vol. 130, **(2016)**.
[2] L. Anderson and C. Brunner, "Substation automation based on IEC 61850 with new process-close technology", Proceedings of IEEE PowerTech Conference, Bologna Italy, **(2003)**.
[3] T. Chu, "Journal of VLSI Signal Processing", **(1994)**, pp. 1-2.
[4] D. Bin and L. Bing, "Design of Security state machines of Access control for control object based on IEC 61850", Proceedings of IEEE PES General Meeting. Montreal, Quebec, Canada, **(2006)**.
[5] C. M. R. Mohammad, R. H. Rossebø and J. E. Y., "Challenges when securing manufacturing message service in legacy industrial control systems", Proceedings of IEEE Emerging Technology and Factory Automation (ETFA), Barcelona, Spain, **(2014)**.
[6] D. Bin, C. Guoqi and L. Yuanyuan, "Journal Nanosci", Nanotechnol, vol. 19, **(2009)**.
[7] L. L. Xin, M. P. Qing and W. J. Fang, "Journal Electric Power Systems Research", vol. 2, **(2006)**.
[8] G. Rong-liang.J. Shanghai Electric Power, 6**(2006)**
[9] F. Yongjun, "Journal Mathematical modeling of engineering problems", vol. 3, no. 1, **(2016)**.
[10] Q. W. Mei, G. D. Wei, Z. C. Yan, X. Y. Xia and W. Gan, "Journal Mathematical modeling of engineering problems", vol. 2, no. 3, **(2015)**.
[11] W. Youlong and H. Guifen, "Journal China Standardization", no. 8, **(2012)**, pp. 112-113.
[12] P. P. Parikh, T. S. Sidhu, and A. Shami, "Journal Industrial Informatics", **(2012)**.
[13] D. Mian, S. gang, H. Qiang and X. Wei, "Journal Review of Computer Engineering Studies", vol. 1, no. 2, **(2015)**.
[14] S. T., S. Johannessen and C. Brunner, "Journal IEEE Control System Magazine", vol. 22, no. 3, **(2002)**, pp. 43-51.
[15] D. Westermann and M. Kratz, "Journal IEEE Transaction on Industrial Electronics", vol. 4, **(2010)**.
[16] M. S. Thomas and I. Reliable, "Journal IEEE Transactions on Power Delivery", vol. 10, **(2010)**.
[17] Z. Jing, L. Xianbo, L. ke, Y. Xiaoming, W. Chanjin and Lsicai, "The application of identity based cryptography in information security of Substation", Automation of Electric Power System, Nanjing Jiangsu, **(2011)**.
[18] F. M. Cleveland, "IEC 62351-7: communications and information management technologies -network and system management in power system operations", Proceedings of IEEE/PES Transmission and Distribution Conference and Exposition, Chicago, IL, **(2008)**.
[19] Z. Jing, W. Jingchan, and S. Chao, "Journal Zhejiang Electric Power", **(2013)**.
[20] Z. Wei and C. Feiyun, "Journal Communications Technology", vol. 46, no. 12, **(2013)**, pp. 74-76.
[21] K. Choi, X. Chen, S. Li, M. Kim, K. Chae and J. C. Na, "Journal Engies", vol. 5, no. 10, **(2012)**, pp. 4091-4109.

Authors

Wang Chen, was born in 1982 and now he is an engineer working in Institute of Information and Communication, Global Energy Interconnection Research Institute. His current research interest is power information security.

Ma Yuanyuan, was born in 1978 and now she is a senior engineer working in Institute of Information and Communication, Global Energy Interconnection Research Institute. Her current research interest is power grid network information security.

Shao Zhipeng, was born in 1984 and now he is an engineer working in Institute of Information and Communication, Global Energy Interconnection Research Institute. His current research interest is Information security technology and its application in electric power system.

Huang Xiuli, was born in 1979 and now she is an engineer working in Institute of Information and Communication, Global Energy Interconnection Research Institute. Her current research interest is power information security.

Fei Jiaxuan, was born in 1984 and now he is an engineer working in Institute of Information and Communication, Global Energy Interconnection Research Institute. His current research interest is power grid engineering control safety.