Research on OPC UA Security

Huang Renjie
College of Computer and Information Science
Southwest University
ChongQing, China
huangrj@swu.edu.cn

Liu Feng, Pan Dongbo
College of Computer and Information Science
Southwest University
ChongQing, China
pandb@swu.edu.cn

***Abstract*—OPC Unified architectures (OPC UA) is a new software interface specification and application framework based on web service for plant automation systems which communicate with each other over the internet. The security issue holds the key to its development for technology feature based on web service. In this paper, the OPC UA security issues are discussed from the two views of network environment security and communication security in OPC UA applications. The network security deployment solution based on distributed firewall was proposed to ensure the host of OPC UA server and client against the different attacks. Sequentially the improved OPC UA security model based on the existing model was presented. A security strategy management module was added into the model, by configuring the module, the security characteristic of OPC UA applications system can adapt to the different security level. At last the information model of the security model is designed. By the above means, the OPC UA communication security and communication efficiency can be balanced better, and it provides the guideline for the development of OPC UA server and the OPC UA applications.**

Keywords-OPC UA; Security Model; Distributed Firewall; Information Model

I. INTRODUCTION

Currently the increasing demands of information integration and device integration call for standard solution for plant automation system. In this situation, OPC Foundation presents OPC unified architectures (OPC UA) based on web service. The OPC UA specification provides a solution for moving information in secure reliable transactions between devices on the plant floor to all kinds of applications in the overall enterprise with web service over the internet [1] [2].

The technology features based on web service and open internet network make the security issue become the key for OPC UA [3] [4]. The OPC UA security model and mapping is presented in the part 2 and part 6 of the series of OPC UA standards. However, it just give the basic model and concepts, it doesn't discuss the network security of OPC UA application, and the existing OPC UA security model can not meet the requirement of configuring the security strategy flexibly for adapting to different application[5] [6].

This paper first introduces an overview of OPC UA and OPC UA security model, then analyses security environment and the security requirement of different systems. Sequentially the secure network environment and communication security in OPC UA system are respectively discussed. At last, the improved security model and the corresponding information model are presented.

II. OPC UA AND OPC UA SECURITY MODEL

A. OPC UA

OPC UA is a platform-independent standard through which various kinds of systems and devices can communicate by sending message between clients and servers over local networks or internet. By standard sets of service and information model, servers can provide access to both real-time and historical data, as well as alarms and Events to notify clients of important changes. OPC UA can be mapped onto a variety of communication protocols and communication data can be encoded in various ways. Figure 1 show the architecture [7] [8].

By defining *AddressSpace* and information model, the device, data, function, event and relation between them in the real world can be mapped into the *node*, such as *object, variable, event, method, reference* and *view* in the *AddressSpace*[9]. OPC UA *AddressSpace* represents these objects to clients by OPC UA service in a standard way. These objects are represented in the *AddressSpace* as *Nodes*. *Reference* is used to describe the relations between *Nodes*. *View* is used for logic group so that *Node* groups can be presented to different client and user. Using object-oriented programming, these objects may be implemented easily.

OPC UA communication stack encodes and decodes OPC UA message, handle the data from the network using different network protocols. OPC UA defines OPC UA Native mapping and XML web service mapping two means to implement OPC UA communication stack. By the mappings, OPC UA communication is independent of the implementation technology.

OPC UA server communicates with OPC UA Client by standard web service supported by OPC UA server. OPC UA defines several sets of standard web services to deal with the communications [10]. These sets of web service are described as following.

SecureChannel service set is used to build secure communication channel and negotiate the secure strategy between server and client. *Session* service set is to build and manage the communication connection between OPC UA applications. The connection is built on secure channel. It provides communication access for other web service.

The Paper is granted by Southwest University (XDJK-2009C022)

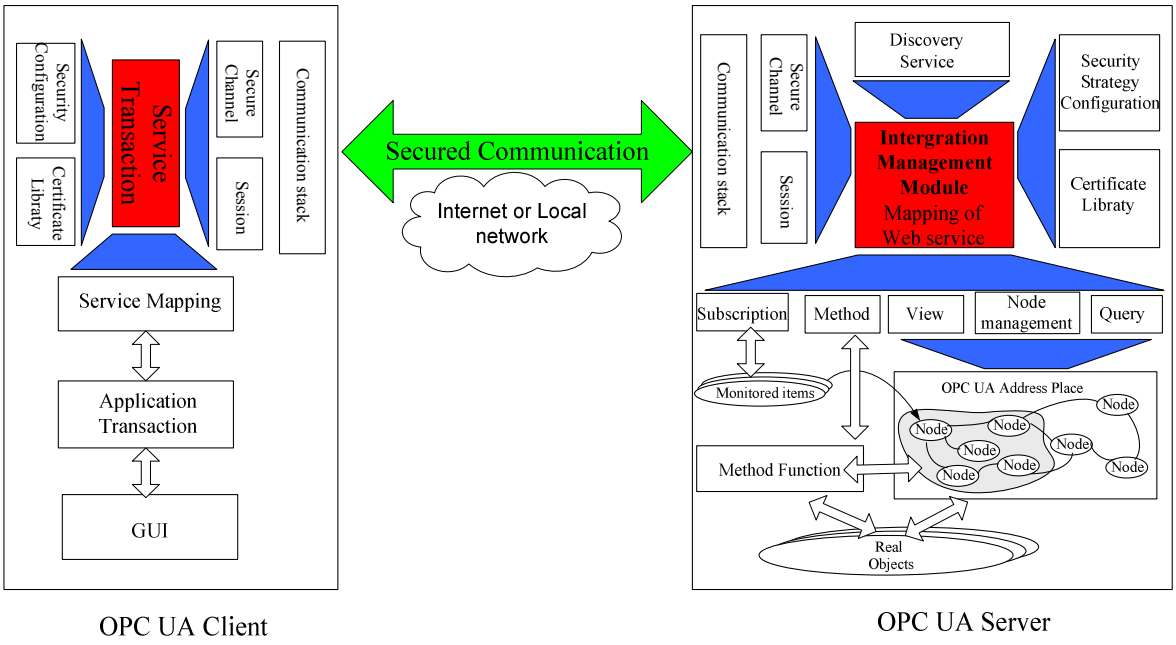

Figure 1. OPC UA Architectures

NodeManagement, *View* and *Attribute* service set are used to operate and manage the *Node* in the address space. Client can get *Node* information from server, and also set attribute or value of variable or object by the service set.

Subscription service set is used to subscribe the cycle data from server by client. By the service set client can get control process data from server periodically. *Method* service set supplies the access to invoke the method which is implemented in objects in server.

B. *OPC UA Security Model*

OPC UA is an interface between components in the operation of an industrial facility at multiple levels: from high-level enterprise management to low-level direct process control of a device. The use of OPC UA for enterprise management involves dealings with customers and suppliers. It may be an attractive target for industrial espionage or sabotage and may also be exposed to all kinds of threats through untargeted malware, such as worms, circulating on public networks. These threats may include *Message Flooding, Message Spoofing, Message Alteration, Message Replay, Malformed Message, Server Profiling, Session Hijacking, Rogue Server, Compromising User Credentials*. All the threats may do harm to OPC UA system [5].

Disruption of communications at the process control end causes at least an economic cost to the enterprise and can have employee and public safety consequences or cause environmental damage. So the security of OPC UA system in industrial automation area is crucial for its applications. In order to secure the OPC UA system, OPC UA communication must meet a set of objectives which include *Authentication, Authorization, Confidentiality, Integrity, Auditability and Availability* [5]. For the objectives, OPC UA defines a security model. Figure 2 shows the model.

In the model, the communication layer provides security functionalities to meet confidentiality, integrity and application authentication as security objectives. OPC UA server and client negotiate about the security functionalities and create the secure channel. This logical channel provides encryption to maintain confidentiality, signatures to maintain integrity and certificates to ensure application authentication for data that comes from the application layer, then passes the secured data to the Transport Layer. The security functions that are managed by the communication layer are provided by the secure channel services.

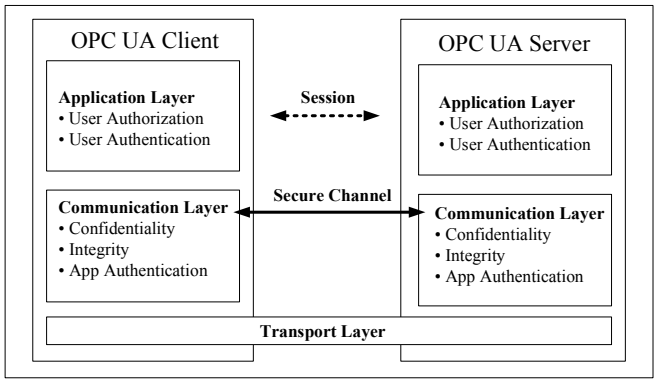

Figure 2. OPC UA Security Model

The routine work of a client application and a server application to transmit plant information, settings, and commands is done in a session in the application layer. The application layer also manages the security functions of user authentication and user authorization. The security functions that are managed by the application layer are provided by the session services. The application can establish a session based on the secured communication, the transferred data in a session pass to the communication layer, communication layer sign and

encrypt the data, then pass it to transfer layer to deliver it to network.

It is possible to achieve the above objectives when OPC UA applications are developed according to the model. Once the OPC UA server has been developed for the special application, user change hard the security functionalities and strategies. It is possible to revise the server, when the security requirement changes. Thus it is hard to implement flexible configuration of security strategy in OPC UA applications.

III. THE ANALYSIS AND CLASSIFICATION OF SECURITY REQUIREMENT IN OPC UA SYSTEM

The network environment together with the security requirement of the transferred data determines the security strategy which should be applied to OPC UA system. For the different plant automation system, the OPC UA system may be built in local network or virtual private dial-network, and it also may be built over the internet. The different application environment confronts different threaten, thus the security strategy for the system should be different. For the different application and transferred data, the requirements to secure the transferred information are different. The different countermeasures are applied to the read-only data and writable data. Even only when person having the corresponding right, he can access the read-only data. Moreover the communication efficiency may be affected when the high-cost encryption algorithms are used in the communication.

According to the network environment, the secure requirement of transferred information and the required communication capacity of the OPC UA application, the five levels of security classification in OPC UA system are represented. Table I shows the information in detail.

TABLE I. OPC UA SECURITY ANALYSIS AND CLASSIFICATION

Class	Conditions			Security measure
	Network	*Information*	*communication efficiency*	
0	L	R	N	N or AA
1	L	R,W	N	AA ,UA and A
2	I	R	H	AA, UA and S
3	VI	SR , W	N	AA,UA, S and A
4	I or VI	SR,SW	L	AA, UA, S, A and E

Note:

- Network: L-Local area network, I-Internet, VI-Virtual Private Dial-Network (VPDN)
- Information: R-Read, W-Write, SR-Sensitive Read, the information to read is sensitive, SW- Sensitive Write, the information to modify is sensitive.
- Communication efficiency: N-Not required, L-Low communication rate is required, H-High communication rate is required.
- Security measure: N-No security measure, AA-Application Authentication, UA- User Authentication. A- Audit, S-Signature, E- encryption.

From the above table, it is obvious that the security requirement is different for the various applications. The above security classifications cover the all applications. It can provide the guideline for the developer and user of OPC UA system. For the actual OPC UA application, the developer can develop the OPC UA server to meet the requirement of security by the mapping technology in the OPA UA. But it is hart to configure the security strategy of OPC UA system according to the existing OPC UA security model, because the security strategy can not be configured in the model.

In order to implement the flexible OPC UA security strategy, in the following sections the security strategy based on distributed firewall will be discussed to deploy the network of OPC UA system for protect the OPC UA server and client from the attacks. And the improved security model will be proposed, so that the flexible security strategy can be configured in the security model for the whole lifetime of the OPC UA system.

IV. THE SECURITY DEPLOYMENT SOLUTION BASED ON THE DISTRIBUTED FIREWALL

OPC UA system is the classic distributed applications. The OPC server and client can locate in the any place in the enterprise over the internet. It may confront with various threats. Some of these threats such as the worms and compromising user credentials can not be resisted by the secured communication. In order to provide secure and reliable running surrounding for OPC UA application, the strategies of multiple layer of protection must be implemented. The distributed firewall technology can provide the boundary protect and intrusion detection. And it can protect the server and client from the threats in the local network. Thus it is feasible to deploy the OPC UA system based on distributed firewall for the secured applications environment. Figure 3 shows the OPC UA system based on distributed firmware.

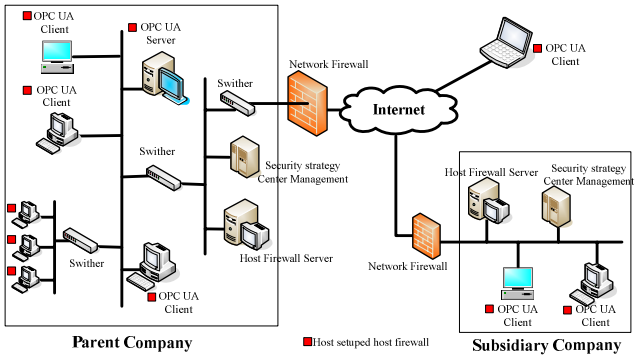

Figure 3. OPC UA system based on distributed firewall

Distributed firmware architecture is consists of network firmware, host firmware and center strategy server [11]. In OPC UA system, the network firmware is used to protect the OPC UA application from the threats coming from the public internet, host firmware is used to protect OPC UA client and server from the inner attack in the enterprise network, host firm

ware set up in the computer on which OPC UA client and server run. The center strategy server is used to configure the strategy between host firmware and network firmware. By configuring the network firmware, the computer in the specific network area such as sub-enterprise can access the UA OPC Server. In this way, it may resist the threat from network region in the outside sub-enterprise. By configuring the host firmware, OPC UA client and server can determine which computer in local network can access it on what ports. Furthermore the logs of network firmware and host firmware can be managed together by configuring security strategy.

The security deployment based on distributed firewall only discusses the secured application environment from the view of network. But it is not far enough to ensure the application safe. The protections in components of the system also are important. It may include hardened configuration of the operation systems, security patch management, anti-virus programs. These protects are necessary for OPC UA system.

V. THE IMPROVED OPC UA SECURITY MODEL BASED ON THE SECURITY STRATEGY LIBRARY

The secured application environment only is the base for the OPC UA applications. It can not resolve the security issues in the OPC UA system radically. The measures such as authorization, authentication, signature and encryption in the inner OPC UA server must be implemented to secure the communication. But it may not be the best solution to apply all the measures to the various OPC UA applications. For the user, it is the best solution that they can configure the OPC UA security strategy according to the requirement. In order to implement the flexible configuration of security strategy, an improved security model is presented on the basis of the existing the OPC UA security model in this section. Figure 4 shows the model in detail.

In the model, the OPC UA communication stack is the key part. It provides the basic interface for the above OPC UA web service. The above OPC UA web service implementation module can access the functions in the communication stack by calling the API to create and manage the communication connection. It consists of soap stack layer, secure channel layer, security strategy management module and the session layer. All together take charge of the secured communication. The web services management module manage the services which be registered by the OPC UA server. By the module, the OPC UA client can discover the services in the OPC UA server and get the information about security strategy. The security strategy management module manage the security strategy, user can configure the security measures in it. The secure channel layer is used to create and manage the secure channel based on the measure such as signature or encryption in the security strategy management module. In the layer, the message can be signed or encrypted according to the configuration in the security strategy management module. The session layer is used to create and manage the session. The soap stack is used to deal with the soap messages.

A. *Soap Stack*

The soap stack is the underlying part in the OPC UA comm-unication stack. It encodes and decodes the messages. And it sends the soap message to OPC client communication stack and receives them from the OPC UA client communication stack according to TCP/UDP or Https protocols. In the soap message encoding/decoding part, both OPC UA Binary and XML two encoding means are implemented for soap message transactions. The developer can configure the encoding means in the soap stack management module. Both the TCP/UDP and HTTP protocols are implemented in the layer. In the development process, the communication protocols can be configured by the developers in the soap stack management module. In this way, the OPC UA developers can freely select the technologies to develop the OPC UA server.

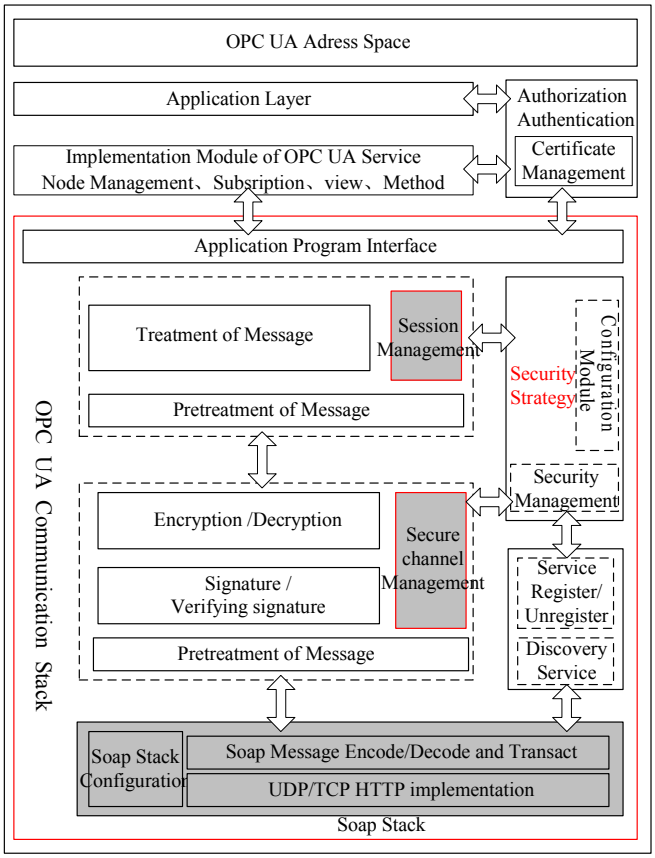

Figure 4. The Security model based on Security Strategy Library

B. *Security Channel*

The secure channel layer is the key part to implement the secured communication. It is used to build the secured communication and sign the message and encode/decode the message. When it receives the messages from the soap stack which are send by client, firstly the pretreatment of message module decode the messages, and judge the type of the message. If the message is the request service to build the secure channel, the secure channel management module will deal with the message, it store the client security information into security management module, and configure the secure channel with the security measures such as the signature, application authentication and encryption algorithms from the security management module. Then it creates the secure

channel and response the message to client. If the messages from the soap stack are the other messages which are based on the connected secured channel, the signature module will validate the signature, if it is valid, it will be passed to encryption/decryption module, the module decrypt the message and pass it to the session layer.

When the different mapping technologies are adopted to implement the OPC UA communication stack, the signature and encryption algorithms are different. When XML web service mapping is adopted, the XML signature and XML encryption are used to sign and encrypt the message. When the OPC UA binary mapping is adopted, the signature algorithms such as HMAC-SHA1, RSA-SHA1 and the encryption algorithms such as AES128-CBC are used to sign and encrypt the message. All the means are implemented in the layer, so that the developer can select it according to the mapping technology which they select.

In the layer, the secure channel management module is core part. It creates and manages the secure channel, and interacts with the security management module. User can configure the security strategy such as the signature and encryption algorithms or select no signature and encryption according to the actual OPC UA application. When the messages come from the client, the pretreatment module of the message judge what signature and encryption algorithms the secure channel based on, and send it to the corresponding module to validate and decrypt the message. If no signature and encryption are adopted, the message will be send to the session layer.

C. The Session

The session layer also is the key part in the model. It receives the message from the secure channel, and passes the message to the according application. When it receives the message, it judges that the message is the request to build the session or the generic messages. If the message is the message requesting to create the session, the session management module will get the security information from it, and deal with the information together with the security strategy management module. Then it creates the session and store the ID of the secure channel and the ID of the session. And it stores the information of client into the session management module. If the message is the other service built on the foregone session, it will pass it to the implement module of OPC UA services, the module deal with it and get data from OPC UA address space via the application business, at last response the result to the client.

D. Security strategy Management Module

The Security strategy management module is the module to manage and configure the security strategy. By the configuration interface, user can configure what signature, application authentication and encryption algorithms be adopted in the secure channel. After configuration, the module manages and maintains the strategy. OPC UA client can get the security strategy by the *Discovery* and *GetSecurityPolicies* services. With the information about the security strategy, the OPC UA client requests to create the secure channel with the OPC UA server. The server creates the secure channel according to the information. In the process, the server saves the security information about the client in the module for uniform management. The certificate of the client will be passed to the certificate management module, so that the applications layer can implement authorization and authentication. In the module, the flexible security mechanism is implemented by configuring its security strategies.

E. User authorization, user authentication and application layer

The user authorization and user authentication are in the level the application layer lying in. Both of them implement the application layer security. The module manages the authorization and authentication mechanism, and it also manages the certificates. By configure the authorization and authentication strategies, the application can select the different authorization means such as no authorization, userID, Pass word and etc. The application layer access the address space, process transaction and map the data into the implementation module of OPC UA services. And it implements the different authorization and authentication means, user can specify the authorization and authentication means by configuring the user authorization and user authentication module.

In a word, the model of OPC UA server is the generic model. For different mapping technologies, the encoding methods and security technologies such signature and encryption adopted are different. But the security architecture and OPC UA server model is similar. Thus by the mapping technology such as the XML web service mapping and the UA native mapping, the model can use for the development of OPC UA server and the OPC UA application [12] [13].

VI. THE INFORMATION MODEL OF SECURITY MODEL

For the feature based on web service of the OPC UA, we select the visual studio development tool and .net framework of Microsoft as the development platform. Windows Communication foundation (WCF) is applied to the design. It is easier to deal with web service and the exchange of soap message.

According to the above model, the generic information model of the OPC UA communication stack is designed by the OOD method in the platform. Figure 5 shows the information model.

In the model, the *StandardStack* is the base class of communication stack. It has the dependency on the *StackConfiguration* class. In the *StackConfiguration* class, the *StandardStack* may be configured. The *StandardStack* class is the complex of the *StackInternalData*, and the *StackInternalData* class has the *IDataInternal* interface, it can provide access to the *StackInternalData* class for the other class or component. The *StackInternalData* is complex of the *ResourceManager*, *SessionManager, ChannelManager* and *SoapConnectionManager* classes. The Session class, *SecureChannel* and *SoapConnection* class have the dependency relation. The *SecureChannel* class is complex of the Channel class and *SecureObject* class, the *SecureObject* and the *SecureObjectConfiguration* has the dependency relation. The *SecureObjectConfiguration* can configure the secure object. The secure object is complex of Signature class and Encryption

class. The actual signature and encryption algorithms are implemented in the Signature and Encryption classes. All the SecureChannel objects are managed by *ChannelManager* instance. All the *SoapConnection* objects are managed by *SoapConnectionManager* instance. The *SoapConnection* objects are complex of TCP/UDP and HTTP class. Both is deal with underlying physical connection. And the communication protocol of *SoapConnection* can be configured by the *SoapConnectionConfiguration.*

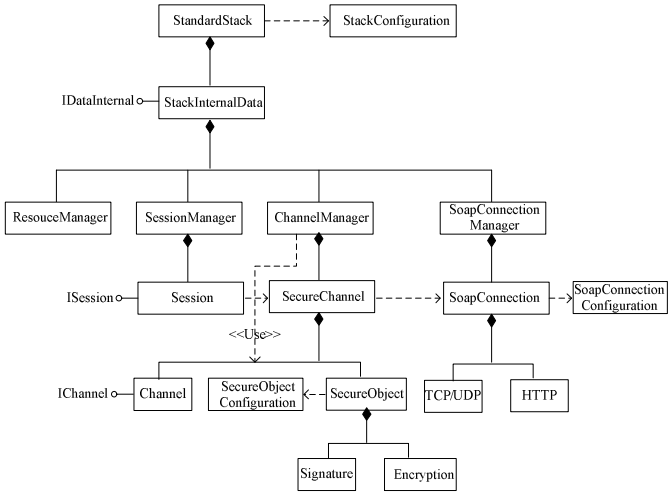

Figure 5. The information model of security model

VII. INCLUSIONS AND FULTURE WORKS

In the Paper, OPC UA system secure issues are discussed from the views of OPC UA application environment and OPC UA communication security. In order to ensure OPC UA application system against all kind of attacks from network, the security deployment solution based on distributed firewall of OPC UA applications was proposed. By defining the security strategy in the security strategy server of distributed firmware, OPC UA server and client will be protected from threat from local network and internet. The security strategy of their host can customized for distinguishing themselves from the other hosts in the enterprise. In this way, the flexible and secure network and application environment can be customized to accommodate the different OPC UA system applications.

For the OPC UA communication security, on the basis of analyzing the network environment and the security requirement of transferred data synthetically, the OPC UA communication security requirements are classified into five classes, and the safeguard for each class are discussed in detail. Aiming at the disadvantage of the existing security model in the OPC UA standards, then a security strategy management module is added into the exciting model. By the means, developer and user can configure the module to accommodate the above five levels of security requirement of the OPC UA applications. At last, the information model of the new security model was discussed.

In conclusion, by the means we have proposed, the OPC UA application environment security and communication security may be ensured. In this way, the OPC UA communication efficiency and security can be balanced better. It can provide technology guide for OPC UA application and the development of OPC UA server. But the solutions are still are rude, they has not been validated in the actual development and applications. Moreover design of security strategy in the security strategy server of distributed firewall also was discussed in detail.

In future works, further research will be dedicated to the validation of the security model and design of security strategy. Moreover the efficient OPC UA signature and encryption also will be discussed.

ACKNOWLEDGMENT

This work was supported by a grant form Southwest University in China (No.XDJK-2009C022).

REFERENCES

[1] [1] Vu Van Tan, Dae-Seung Yoo, and Myeong-Jae Yi, “A Framework towards OPC Web Service for Process Monitoring and Control”, International Conference on Advanced Language Processing and Web Information Technology, 2008, P.562-568.

[2] [2] Miriam Schleipen, “OPC UA supporting the automated engineering of production monitoring and control systems”, Emerging Technologies and Factory Automation, 2008, P.640-647.

[3] [3] Huang, Renjie Liu, Feng,” Research on OPC UA based on Electronic Device Description”, Industrial Electronics and Applications. 2008. ICIEA 2008. P.2162-2166.

[4] [4] Annerose Braune, Stefan Hennig, Sebastian Hegler,”Evaluation of OPC UA Secure Communication in Web Browser Applications”, IEEE INDIN 2008, P.1660-1665

[5] [5] IEC 62541-2: OPC Unified Architecture Specification-part 2: Security Model. 2007

[6] [6] IEC 62541-6: OPC Unified Architecture Specification-part 6: Mapping. 2007

[7] [7] Tom Hannelius,” Roadmap to adopting OPC UA”,IEEE INDIN 2008,756-761.

[8] [8] IEC 62541-1: OPC Unified Architecture Specification-part 1: Overview and Concepts. 2007

[9] [9] IEC 62541-3: OPC Unified Architecture Specification-part 3: Address Space Model. 2007

[10] [10] IEC 62541-4: OPC Unified Architecture Specification-part 4: Services. 2007

[11] [11] Wang Qinghong, Study of Distributed Firewall Based Security system, Computer Security, 2009.6, P.54-56.

[12] [12] IEC 62541-5: OPC Unified Architecture Specification-part 5: Information Model. 2007

[13] [13] IEC 62541-7: OPC Unified Architecture Specification-part 7: Profiles. 2007.