Advanced Engineering Forum *Online: 2012-09-26*
ISSN: 2234-991X, Vols. 6-7, pp 481-484
doi:10.4028/www.scientific.net/AEF.6-7.481

A Protocol with Security Mechanism for Electrical RTU

Wang Huiran[1,a], and Ma Ruifang[2,b]

[1]College of Computer Science, Xi'an Polytechnic University, Xi'an, Shaanxi, P. R. China

[2]Software Engineering School, Xi'an Jiaotong University, Xi'an, Shaanxi, P. R. China

[a]hrwang127@sohu.com, [b]rfma@263.net

Keywords: electricity, remote terminal units, security mechanism, encryption, authentication

Abstract. We dissected disadvantages of the existing transmission protocols and improved its performance of dada communication security. We have proposed a security communication protocol, called as RTUSec, for remote terminal units. RTUSec adds a security layer to the existing three layer model, so that the data security is improved. After analyzing advantage and disadvantage of the present algorithms of cryptography and authentication for data communication, we have designed a security mechanism with DES and HMAC to deal with security problems like spoofing during the communication between RTUs and controlling centers.

Introduction

The electric power plays a critical role in the national economy. Electrical power grid consists of power stations, substations, transmission/distribution lines, consumers and so on. Electrical remote terminal units (abbreviated to RTU) are installed in power stations or substations to test voltage, energy consumption and other parameters of power grid, and to transmit these parameters to the controlling centers. Protocols used widely during communication between the controlling centers and RTUs include IEC870-5-101, DNP3, MODBUS, and CDT. These protocols have no security mechanism. Previously the security threats did not take consideration as the power grids are small in scale. It becomes serious nowadays with increase of the scale of the power grid. Collapses of Power grids in Europe and America reflect the importance of security of power grid.

Depending on the above analyses, security mechanism of power grid is studied in this paper.

Architecture for Remote Monitoring Systems

The physical structure of remote monitoring systems of power grid is depicted in Fig. 1. In a monitoring system, there are two kinds of stations. One kind of stations is referred to as control

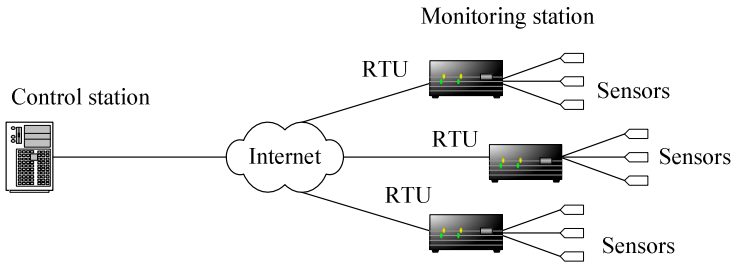

Fig. 1 Architecture of remote monitoring systems for power supply

stations. The other kind is termed as monitoring stations. Master Terminal Unit (MTU) is installed in control stations. Various types of Remote Terminal Units (RTU) are installed in monitoring stations. The performance of power grid is to be monitored by means of RTUs. Varieties of measuring instruments are connected to RTUs. Parameters of the performance of power grid are measured and transmitted to control station, where the measured data is stored, analyzed, and processed. Parameters generally monitored are electric voltage, electric current, and electric power.

Security threats faced by RTUs

Security threats faced by RTUs during communication are divided in two kinds, i.e. natural and man-made ones. Natural threats include environmental interferences, aging equipment, and a variety of natural disasters. Man-made threats are further classified into accidental threats such as fault operations, bugs of programming and intentional attacks. According to ways of attack, attacks are divided into active and passive ones.

A passive attack means that hackers do not interact with any of the communication parties involved, attempting to break the system solely based upon observed data (i.e. the ciphertext). This can also include known plaintext attacks where both the plaintext and its corresponding cipher text are known. As most classical ciphers are vulnerable to this form of attack, most ciphers are designed to prevent this type of attack. Types of passive attacks are traffic analysis and release of message contents. In traffic analysis, the eavesdropper analyzes the traffic, guess the contents of communication. Incoming and outgoing traffic of network is analyzed but not changed. Passive attacks are very difficult to detect since they do not make alteration of the data. It can be prevented by encryption of the communication data.

An active attack requires hackers to be able to transmit data to one or both of the communication parties, or block the data stream in one or both directions. Hackers can stop all or parts of the data sent by the communicating parties. By means of active attack, intruders may insert his own data into the data stream, playback data from another connection, playback data that had previously been sent in the same and opposite direction on the same connection, delete data. Man-in-the-middle attack is another type of an active attack. This is one of the most serious forms of attack since many companies' operations critically depend on data.

We realize from the discussion above that threats faced by RTUs during communication with controlling centers include eavesdropping, identity counterfeiting and information tampering. Eavesdropping is the use of an electronic transmitting or recording device to monitor conversations without the consent of the parties involved. Information tampering is a type of attack in which certain information in the frame entered by a user is changed without that user's authorization. By means of identity counterfeiting, hackers transmit data to the other RTU taking advantage of a legal identity.

For the sake of security of communication between RTUs and controlling centers, a solution of security mechanism is proposed in this paper to deal with the problems mentioned above.

Architecture of Security Mechanism

There are two security mechanism frequently used, i.e. encryption and authentication in the information security filed.

Cryptographic techniques allow a sending RTU to disguise data so that a hacker can gain no information from the intercepted data. The receiving RTU, of course, must be able to restore the original data from the disguised data.

Cryptographic techniques may be further categorized into two types, i.e. Secret Key Cryptography and Public Key Cryptography. With secret key cryptography, a single key is used for both encryption and decryption. The sender uses the key to encrypt the plaintext and sends the cipher text to the receiver. The receiver applies the same key to decrypt the message and recover the plaintext. Because a single key is used for both parties, secret key cryptography is also called symmetric encryption.

Generic Public Key Cryptography employs two keys that are mathematically related although knowledge of one key does not allow someone to easily determine the other key. One key is used to encrypt the plaintext and the other key is used to decrypt the cipher text. The important point here is that it does not matter which key is applied first, but that both keys are required for the process to work. Because a pair of keys is required, this approach is also called asymmetric cryptography. One of the keys is called the public key and may be advertised as widely as the owner wants. The other key is called the private key and is never revealed to another party.

During communication in power grid, A RTU has to confirm where a message come from and whether this message is altered on the path. It can be achieved by HMAC. HMAC stands for Hash-based Message Authentication Code. It involves a cryptographic hash function in combination with a secret key and may be used to simultaneously verify both the data integrity and the authenticity of a message. Authentication is the act of confirming the truth of an attribute of a message received by a RTU. Data integrity means that both the sender and receiver want to insure that the content of a message is not altered, either maliciously or by accident, in transmission.

Since RTUs works in industry areas and have limited resources, we use HMAC for data integrity and the authenticity, use DES (Data Encryption Standard) for encryption. DES takes shorter time during calculation.

Design of Security Protocol

In order to meet the demand of plants, we proposed a proprietary security protocol, i.e. RTUSec, which comes from Remote Terminal Units Security. RTUSec is based on IEC60870-5-102, whose disadvantage is to transmit messages in plain codes without consideration of security threads. We improve three layer model of the protocol IEC60870-5-102 by adding security layer including DES cryptography and HMAC authentication.

The frame format is shown in fig. 2. It contains 13 fields. These fileds are used for functions as

0x98
Frame length
Version
0x98
Control
1st byte of addr
2nd byte of addr
LPDU
Padding
Padding length
HMAC
Checksum
0x16

Fig. 2 RTUSec frame format

following:

(1) 0x98：Beginning of frame.

(2) Frame length: byte count from control field to checksum field.

(3) Version：Version of the security mechanism used by this RTU.

(4) Control: consists of multiple flags. Function flag defines the function of the frame. A value of 12 indicates that an authentication error occurs. This may be resulted from alteration of the frame or an illegal sender. Value 13 of function flag indicates that the sender and the receiver use different version of security mechanism, and the two version is not compatible with each other.

(5) LPDU: abbreviated from Link Protocol Data Unit and used to encapsulate ASDU (the application service data unit). It is the payload data of the frame. LPDU take the form of the cipher codes.

(6) HMAC: digest of HMAC used for the purpose of authentication.

(7) Checksum: Arithmetic sum of the bytes from beginning of control field to end the HNAC field.

(8) 0x16: sign of the frame end

Rules for the security mechanism to transmit data are illustrated in fig. 3.

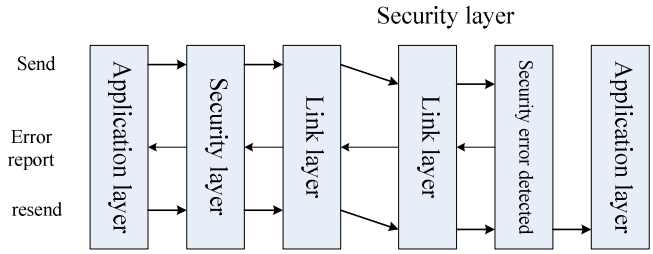

Fig. 3 Security mechanism

(1) New transmission can not start until the end of previous transmission

(2) Sending side make security fames by encryption and authentication processes.

(3) Initialize the sending process.

(4) Receiving side start the security process after obtaining a frame.

(5) Check the security version. Response with message “version error” if version is incompatible with sending side.

(6) Decryption and restore the original frame.

(7) Start authentication processes. Response with message “authentication error” if any error is detected.

(8) The original frame is passed onto the application layer.

Conclusion

Based on analyses of the disadvantages of the previous transmission protocols frequently used in the power grid, we propose a new protocol, called RTUSec, to improve security of those protocols. We have defined the frame format and the communication mechanism. And we have applied RTUSec to a type of RTU, i.e. HT2000 miniRTU which has been put into production.

Acknowledgement

This research is sponsored by Program of Shaanxi Education Bureau No.07JC03.

References

[1] Yang Tao. Review of Application of Electrical Automation [J]. Science & Technology Information, 2010, (23):886. (In Chinese)

[2] Zhang Jian. Automation of Monitoring and Dispatch of Power Grids [M]. Beijing: China Electricity Publishing House, 2007: 3-9. (In Chinese)

[3] Smid M E, Branstad D K. Data Encryption Standard: past and future [J]. Proceedings of the IEEE, 1988, 76(5):550-559.

[4] Tian Xiaoxia, ZhaoGang. Application of Encryption IDEA to Intelligent Sensors [A]. The Fourth Proceedings of China Conference on Surveying , 2006. (In Chinese)

[5] Jianmin Jiang. Pipeline algorithms of RSA data encryption and data compression [J]. Communication Technology Proceedings，1996.

[6] Chang Ya-Fen，Shiao Wei-Cheng. A Comparative Study of Elgamal Based Digital Signature Algorithms [J]. Intelligent Systems Design and Applications，2008.

[7] IEC. IEC 60870-5-102 Companion standard for the transmission of integrated totals in electric power systems.