Analysis on the Role of Network Security Protocol Based on Ethernet in Computer Communication Technology

Fu Yu*

Internet of Things Engineering, Beijing University of Posts and Telecommunications University, Beijing 100876, China

*Corresponding Author email: yufu@bupt.edu.cn

Keywords: Ethernet; Network Security Protocol; Computer Communication Technology

Abstract: With the development of computer and communication technology, Ethernet technology is being introduced into substation automation system. However, the CSMA/CD protocol adopted by traditional Ethernet technology is a network communication mode with uncertain delay. And it does not support priority transmission. When the network load is too large, the communication performance will be greatly reduced. To ensure a good Internet environment, it is necessary to ensure that network security protocols are not destroyed, to reduce information leakage and malicious attacks, and to improve the level of network security. Aiming at the current situation of network security, it comprehensively analyzes the causes and common solutions of network security risks, combined with the application of Ethernet-based point-to-point protocol, and found the reasons for the above two attacks in the application of the protocol. The core technology of the existing security protection communication network is in the hands of large foreign companies, and the technology is not open, for the localization of the entire high-speed magnetic levitation technology. It is necessary to conduct research on the security protection communication network. Therefore, it is of great practical value to select the security protection communication network as a research topic.

1. Introduction

With the needs of people and the wider application of network technology, network security has become an influential factor for the further improvement and development of network technology [1]. The network has functions such as information sharing and resource sharing. Although it is convenient for users to communicate, it also has a huge security threat to the network. In the context of the increasing scale of substations, the large increase in the amount of communication data, and the importance of real-time data collection due to the occurrence of many blackouts in recent years, the existing communication network technology has experienced many drawbacks [2]. It has not been able to meet the requirements of rapid collection and transmission of large amounts of data in the substation station in real time, and can not adapt to the rapid development of power system automation, and needs to adopt new communication technologies [3]. Information security and network security are becoming increasingly prominent. The hidden danger of network security is an important reason that threatens network security. Its composition is diverse, and it can be divided into five categories: hardware defects, software defects, protocol vulnerabilities, human errors and virus transmission [4]. In the process of computer network communication, the security protocol encrypts the transmitted data information by means of key distribution and identity authentication, or uses other protection measures to protect the validity and integrity of the data information, so as to ensure the security of data transmission [5]. The operation control system plays a key role in automatic control and safe communication of train operation in the whole maglev transportation system [6].

With people's attention to network security issues, network security protocols have gradually come into people's vision. The main content of the protocol is to achieve a certain goal by involving more than three programs to form a new program [7]. In particular, it is worth mentioning that in order to build a reliable, controllable and economical information transmission network in fast and

  DOI: 10.25236/eeems.2018.012

reliable application scenarios, it is often necessary to closely integrate with the specific application background. Because the requirement of substation integrated automation system for real-time is very different from other fields, the requirement for real-time is very high [8]. The "millennium bug" problem that had been provoked by the rumors was finally solved smoothly by the efforts of global technicians. It did not have much impact on people's work and life, but this problem highlighted the terrible consequences of hardware defects [9]. Because the structure of the hardware has been solidified, once the problem occurs, it is not easy to change, so the severity is often more lethal than the software defect [10]. The partition security computer performs the core functions of the partition control system. Its main task is to protect the trains and access roads in the area to which the partition control system belongs. The access protection includes the traction cutoff function and the switch protection function. The specific tasks of the partition security computer are track protection, train management, safe operation and display, and traction cutoff [11].

Ethernet has the advantages of open technology, fast transmission speed, simple and flexible networking, and easy interoperability of devices. Preliminary applications have been obtained in the two-level communication networks of substation process bus and station-level bus. However, Ethernet uses collision-carrying carrier sense multiple access (CSMA/CD) mechanism for media access control [12]. Information transmission delay has unpredictable randomness, and it has been controversial whether it can meet the real-time requirements of data transmission in substation communication networks. Software can't be 100% flawless and flawless. However, these vulnerabilities and flaws are the preferred targets for attackers [13]. Events of attackers intruding into the network have occurred. Most of these incidents are the bitter consequences of imperfect security measures [14]. Software defects not only refer to network software defects, but also include security-related system defects in operating system and database management system [15]. Most of these defects are due to poor resource control and management, incorrect programming, careless source code auditing, unintentional side effects or some inappropriate binding. When the partition traction cut-off computer receives the cut-off command of the partition safety computer or fails to communicate with the partition safety computer, it is responsible for safely cutting off the traction system [16]. To ensure that the traction or braking current does not enter the railroad cable of the traction system in any operating state.

2. Peer-to-peer protocol based on Ethernet and its security risks

PPPo E is a point-to-point communication protocol based on ethernet. It can be used for multiple hosts on the same Ethernet to open their PPP sessions to multiple destination hosts through one or more cross-connect (bridge) modems. It is mainly used for broadband remote access technology [17]. From different perspectives, security protocols can be divided into several categories. For example, from the perspective of ISO hierarchical model, security protocols can be divided into two categories: low-level protocol and high-level protocol. From the functional point of view, security protocols can be divided into identity authentication protocols, key authentication protocols, etc. [18]. From the point of view of key, security protocols can be divided into hybrid protocol, multiple protocol, single protocol and public key protocol. Most of the spacer layer equipment needs to collect the voltage and current values under normal and accident conditions from the voltage and current transformers of the process layer, and collect the state information and fault diagnosis information of the equipment [19]. This information includes the position of the circuit breaker and disconnector, the split position of the main transformer, the diagnostic information of the transformer, transformer, arrester and the operation information of the circuit breaker [20]. For the security detection of network security protocols, it is usually proved that the security breach of the network security protocol is more simple and convenient than the security of the network security protocol. At present, the detection of network security protocol security is mainly through the means of attack testing to achieve network security protocol security risks [21]. This method is suitable for long-term failure of one of the networks in the dual network, thus avoiding invalid testing of the faulty network and improving system efficiency, and also for communication to workstations connected only to a single network in

the dual network.

As can be seen from Table 1 and Table 2, WAPI performance is similar to EAP-TLS when precomputation is not considered, but its performance is inferior to EAP-TLS in the presence of precomputation.

Table 1 Protocol performance comparison

Agreement	WAPI*	EAP-TLS (RSN)
Customer certificate	Y	Y
Exchange wheel number	≥2	3(5)
Public Key Encryption/Decryption (MN)	3	3
Exponential Operations (MN)	1	2
Signature (MN)	1	1
Verify Signature and Certificate (MN)	4/2*	2

Table 2 Performance comparison of predicted protocols

Agreement	WAPI*	EAP-TLS (RSN)
Customer certificate	Y	Y
Exchange wheel number	≥2	3(5)
Public Key Encryption/Decryption (MN)	3	1
Exponential Operations (MN)	1	2
Signature (MN)	1	1
Verify Signature and Certificate (MN)	4/2*	2

The attacking host only needs to send fewer SYN connection requests to the port of TCP service provided by the target host, whose source address is disguised and cannot be reached by routing. A successful attack [22] can be implemented by filling the TCP cache queue of the destination host. In practice, attacks are often sustained and high-speed. The establishment of identity authentication protocol mainly refers to the protocol established by one entity and another entity when they communicate information. Key authentication protocol mainly refers to the establishment of corresponding security protocols for multiple entities applying one resource. Authentication key agreement, a user with real-name authentication can establish an information sharing system for secure transmission of resources and data. Between the relevant functional modules within a bay, ie the exchange of data between relay protection and control, monitoring and measurement. This type of information includes measurement data, circuit breaker status, device operating status, and synchronous sampling information. Attack testing is generally divided into attack network security protocol encryption algorithm, attack algorithm and protocol encryption technology, and attack network security protocol itself to discover security vulnerabilities in network security protocols. Improve and optimize network security protocols in a timely manner to improve the security of network security protocols. When the state detection module detects one of the two network channels, the communication uses another network, and the state can only point to the intact network at this time. When the network recovery is detected, the network is restored to the dual network operation.

3. Security of Network Security Protocol

With the development of science and technology and network technology, network security protocols are constantly being improved and supplemented. However, although many protocols have been improved, there are still many loopholes. Network hackers can attack the network system through these vulnerabilities, making the network security protocol invalid. In the model of substation automation communication network, functional modules and communication modules are separated. A single functional module can have multiple communication modules, and functional modules can communicate with each other using point-to-point links established between communication modules. It establishes a reliable connection between the functional modules that need network data communication. Synchronized authentication is widely used in the design of network security protocols. It requires strict synchronization clock between authentication users. It is relatively easy to achieve in good computer network environment. However, when there is a certain delay in the network, it is difficult to achieve synchronous authentication between users. Most network security protocol designers have insufficient understanding of network security itself and have insufficient understanding of relevant knowledge, which has brought many negative effects to the design of network security protocols, which is similar to the design of password encryption. It indicates that the insecure security of network security protocols is much easier than the security of network protocols. The communication module immediately advertises the application layer after receiving the application layer data from the network, and the application layer quickly responds to the notification when the application layer sends data. First check if the sending operation of the communication module is busy. If it is not busy, hand the data to the communication module to send the data, otherwise it will wait for the sending process. The delay curve in each simulation environment is shown in Figure 1-4.

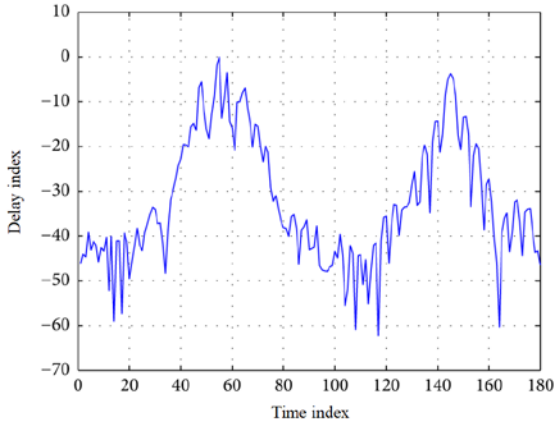

Figure 1 10 M shared Ethernet link delay

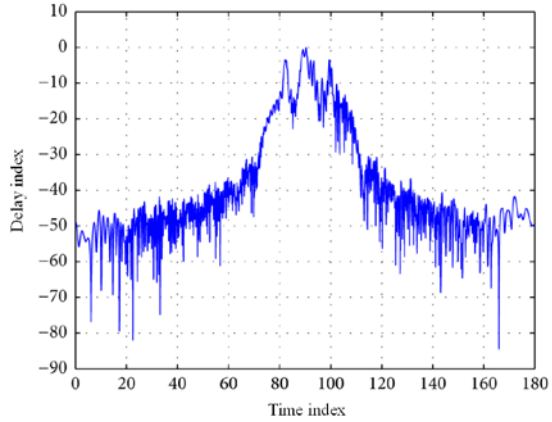

Figure 2 100 M shared Ethernet link delay

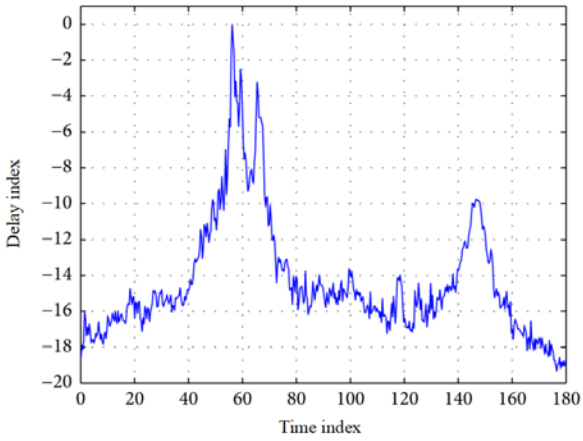

Figure 3 Delay of 10 M Shared Ethernet Link Influenced by CBR Data

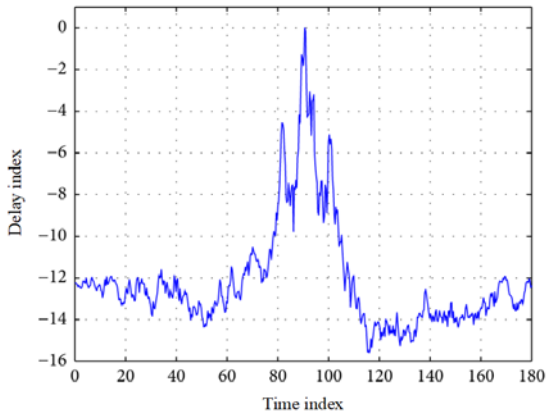

Figure 4 Delay of 100 M Shared Ethernet Link Influenced by CBR Data

The periodic data stream A can be expressed as:

$$A^T G = \sum_i A_i^T G_i \tag{1}$$

If the message cannot be submitted to the target task before the prescribed time limit, the performance of the system will be degraded and the catastrophic consequences will be serious. Therefore, periodic data flow often has the following time constraints:

$$G^m = \left[G_1^T, G_2^T, ..., G_k^T \right]^T \tag{2}$$

If it is recorded as the average arrival rate of the message, k is the number of arrivals of the message, then the probability that a message arrives within the time interval n obeys the Poisson distribution with the parameter. For any d, there are:

$$2k \le n, k \le a, 2k-1 \le d \le n-r \tag{3}$$

Assuming a single data source M state duration is, its distribution function is:

$$\left(\alpha_{MMSR}, \beta_{MMSR}\right) = \left(\frac{M}{k}, \frac{M}{k\left(d-k+1\right)} \right) \tag{4}$$

Assuming that a message is transmitted from the sending node to the receiving node, through a network intermediate node and a communication link, there are:

$$RSRP_{n_i,n} + (\lambda_j - \lambda_R) = RSRP_{n_i,m} \tag{5}$$

Thus, the total delay R experienced by the message transmission can be expressed as:

$$R_{n_i}^C = \log_2(1+\frac{p_{mac,n_i}\left\|\boldsymbol{h}_{mac,n_i}^T \boldsymbol{W}_{mac,n_i}\right\|_2^2}{\sigma^2}) \quad (6)$$

With the enhancement of computing power of mobile nodes and the speed of public key algorithms, public key technologies are more and more widely applied to wireless environments. From the aspect of computational complexity, there is no big difference in the computational complexity between EAP-EWAP and EAP-TLS. The former has two public key encryption/decryption times, the exponential operation is three times, and the pre-computation is reduced. For the first 1 and 1 time. The performance comparison between the protocol and EAP-TLS and WAPI is shown in Table 3. If the precomputation is considered, the performance comparison between the protocol and EAP-TLS and WAPI is shown in Table 4.

Table 3 Protocol performance comparison

Agreement	WAPI*	EAP-TLS (RSN)	EAP-EWAP
Customer certificate	Y	Y	N
Exchange wheel number	≥2	3(5)	3
Public Key Encryption/Decryption (MN)	2	3	2
Exponential Operations (MN)	0	1	3
Signature (MN)	1	1	1
Verify Signature and Certificate (MN)	4/3#	2	4/3#

Table 4 Performance comparison of predicted protocols

Agreement	WAPI*	EAP-TLS (RSN)	EAP-EWAP
Customer certificate	Y	Y	N
Exchange wheel number	≥2	3(5)	3
Public Key Encryption/Decryption (MN)	2	1	1
Exponential Operations (MN)	0	2	1
Signature (MN)	1	1	1
Verify Signature and Certificate (MN)	4/3#	1	4/3#

In the design of network security protocols, it is necessary to consider and predict the difficulties and attacks that the protocol will face, as well as the design cost and application value of the protocol itself. The information of interaction between PSCAD and IED equipment includes synchronization information number, relay protection equipment serial number, three-phase voltage and current, and main protection starting signal. Backup protection start signal, main protection trip signal, backup protection trip signal, protection of the number and status of circuit breakers controlled, main protection block signal, backup protection block signal. After system recovery and security vulnerability repair, the impact of intrusion events on intruded systems and related systems should

also be analyzed. If the intrusion event may cause the system files to be illegally modified, the system-wide reinstallation and configuration should be performed as soon as possible after the emergency elimination and recovery to prevent hidden dangers. Adopt a design that is resistant to conventional attacks. The network security protocol must have the ability to defend against network attacks such as common plaintext attacks, hybrid attacks, and expired information attacks, preventing network hitters from obtaining key information from response messages. For the method of asynchronous authentication in the network security protocol, it is also necessary to design a verification number. This verification number can solve the problem that the network environment is poorly authenticated, and the authentication security factor can be improved. To defend against denial of service attacks, defense only makes sense when you know the defense target. Since it is impossible to protect all systems from denial of service, the decision to use limited resources is extra careful when constructing protection.

4. Conclusion

Because of the network system itself and other reasons, some vulnerabilities and shortcomings inevitably exist in the design process of network security protocols, which requires designers to pay attention to observation and summary of experience in design. The current network security protocols are supplemented and improved to further improve the security level of network security protocols. In this paper, the transmission rule of message in substation automation system based on Ethernet is analyzed, and the composition and characteristics of message transmission delay are studied. On this basis, many factors affecting the real-time performance of substation automation system based on Ethernet are obtained. The application of network security protocol in computer communication technology can not only ensure the integrity and security of data information, but also improve the security of computer network communication, which is conducive to the processing of computer data information. The application scope of computer network security protocols is more and more extensive, and the research on network security factors is gradually increasing, which improves the data transmission speed and security of computer networks. Based on the quantitative analysis and analysis of the results, it is concluded that the information processing capability of the end nodes is a very important factor affecting the real-time information, and the link layer delay is relatively stable. The impact of information delay is often the time it takes for the information to be processed at the end node, and this time is several times the link delay in the event of a fault. Switched Ethernet is a good choice when choosing a network structure, but you need to properly configure the switch's buffer to meet network requirements.

References

[1] Bruce N, Kang Y J, Kim H R, et al. A Security Protocol based-on Mutual Authentication Application toward Wireless Sensor Network. Lecture Notes in Electrical Engineering, 2015, 339: 27-34.

[2] Bugliesi M, Calzavara S, M?Dersheim S, et al. Security protocol specification and verification with AnBx . Journal of Information Security and Applications, 2016, 30: 46-63.

[3] Gupta S, Dhurandher S K, Woungang I, et al. [IEEE 2013 IEEE 9th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob) - Lyon, France (2013.10.7-2013.10.9)] 2013 IEEE 9th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob) - Trust-based Security Protocol against blackhole attacks in opportunistic networks . 2013: 724-729.

[4] Elfgee E B, Arara A. Technical Requirements of New Framework for GPRS Security Protocol Mobile Banking Application. Procedia Computer Science, 2014, 37: 451-456.

[5] Avalle M, Pironti A, Sisto R. Formal verification of security protocol implementations: a survey .

Formal Aspects of Computing, 2014, 26 (1): 99-123.

[6] Lv X, Mu Y, Li H. Non-Interactive Key Establishment for Bundle Security Protocol of Space DTNs. . IEEE Transactions on Information Forensics & Security, 2013, 9 (1): 5-13.

[7] Bagheri N, Safkhani M, Perislopez P, et al. Comments on "Security Improvement of an RFID Security Protocol of ISO/IEC WD 29167-6" . IEEE Communications Letters, 2013, 17 (4): 805-807.

[8] Safkhani M, Bagheri N, Mahani A. On the security of RFID anti-counting security protocol (ACSP) . Journal of Computational and Applied Mathematics, 2014, 259: 512-521.

[9] Lee J W, Lee Y H, Syrotiuk V R. The performance of a watchdog protocol for wireless network security. International Journal of Wireless & Mobile Computing, 2015, 2 (1): 28-36 (9).

[10] Quan Q, Yan-Long J, Rui Z. RFID Security Protocol Based on Synchronous Update of Random Number. Computer Engineering, 2013, 39 (8): 9-14.

[11] Jang C S, Lee D G, Han J W, et al. Hybrid security protocol for wireless body area networks . Wireless Communications & Mobile Computing, 2015, 11 (2): 277-288.

[12] Zhang X, Ye F, Fan S, et al. An adaptive security protocol for a wireless sensor-based monitoring network in smart grid transmission lines. Security & Communication Networks, 2016, 9 (1): 60-71.

[13] Liu B J, Wang J X. Research on the Network Security Protocols Based on the Strand Spaces Theory. Applied Mechanics and Materials, 2013, 457-458: 1134-1138.

[14] Jurcut A, Coffey T, Dojen R. A Novel Security Protocol Attack Detection Logic with Unique Fault Discovery Capability for Freshness Attacks and Interleaving Session Attacks. IEEE Transactions on Dependable and Secure Computing, 2017: 1-1.

[15] Gao L, Zhang L, Ma M. Low Cost RFID Security Protocol Based on Rabin Symmetric Encryption Algorithm. Wireless Personal Communications, 2017, 96 (1): 683-696.

[16] Zhang B, Wan G G. SRCE: Security Protocol in RFID Back-End System Based on Certificate and ECDH. Applied Mechanics and Materials, 2014, 577: 970-973.

[17] Jianfeng L. RFID Security Protocol Based on Reader and Double ID Verification. Computer & Modernization, 2013, 1 (8): 179-183.

[18] Niu Y, Wu L J, Liu Y, et al. A 10 Gbps in-line network security processor based on configurable hetero-multi-cores. Journal of Zhejiang University: Science C (Computers and Electronics), 2013, 14 (8): 642-651.

[19] Dener M, Bay O F. TeenySec: a new data link layer security protocol for WSNs. Security and Communication Networks, 2016, 9 (18): 5882-5891.

[20] Chaudary A, Salah K. Modelling and analysis of rule-based network security middle boxes. Information Security Iet, 2015, 9 (6): 305-312.

[21] Yang, Ru. Study on ARP Protocol and Network Security in Digital Manufacturing. Applied Mechanics and Materials, 2014, 484-485: 191-195.

[22] Honda M, Huici F, Raiciu C, et al. Rekindling network protocol innovation with user-level stacks . ACM SIGCOMM Computer Communication Review, 2014, 44 (2): 52-58.