Available online www.jocpr.com

Journal of Chemical and Pharmaceutical Research, 2014, 6(4):382-387

Research Article

ISSN : 0975-7384
CODEN(USA) : JCPRC5

An identity authentication and key agreement protocol based on industrial ethernet bus

Jun Wang[1,2], Yongxin Li[1] and Jingtao Hu[2]

[1]Dept. of Computer Science & Technology, Shenyang University of Chemical Technology, China
[2]Shenyang Institute of Automation, Chinese Academy of Sciences, Shenyang, China

---

ABSTRACT

For the purpose of preventing illegal device connection and data from being tapped, further improve security and reliability of industrial Ethernet bus network system, the paper puts forward a simple and effective security protocol. This protocol can implement to equipment identity authentication and key agreement for data encryption. The protocol is based on challenge/response mechanism, determine the legitimacy of the equipment by use of dynamic password authentication, and use the key table for key agreement. Finally, the efficiency and security of the protocol is tested and analyzed. The test results show that the protocol can complete mutual authentication and key agreement in a relatively short period of time, at the same time, will bring larger improvement to the industrial network security.

Keywords: Industrial Ethernet security, Security protocol, Identity authentication, Key distribution

---

INTRODUCTION

With the continuous development of Ethernet technology, industrial automation control network make towards to Ethernet technology. Because of some irreplaceable advantages, such as low cost, high communication efficiency, rich in software and hardware resources, strong ability to sustainable development, management and control integration easily achieved, the industrial Ethernet technology has become a strong competitor of field buses [1, 2]. Due to the industrial Ethernet technology will be widely apply the computer network technologies into industrial control systems[3-5], the security threats of industrial control system is becoming more and more serious[6-8]. Therefore the establishment of security mechanism is a very necessary and urgent[9-12].

This paper focuses on the research authentication and key distribution technology to improve the security of industrial Ethernet bus. Through the authentication technology can assure that the control network communication equipment identity is legitimate, prevent illegal equipment malicious connection. The key distribution mechanism is the basis of information encryption, key management scheme can effectively improve the security of keys, prevent data hacking and data tampering in the transmission process.

2. CHALLENGE/RESPONSE MECHANISM

The challenge/response authentication is mainly applied to the client to server authentication. Firstly, the client sends a message to the server for requesting connection. Then server sends the unique challenge value information to the client. Client generates unique dynamic password based on challenge information. Server verify dynamic password to confirm the client's identity. The challenge information includes seed value and N the number of iterations. Each seed values are not the same, so the each dynamic passwords are also not the same. The dynamic password can be used only once, even if the playback of the password is invalid.

Described as follows:
Sender → Receiver: hello;
Receiver → Sender: seed, N;
Sender → Receiver: Key（seed）N;
Receiver will verify the dynamic password.

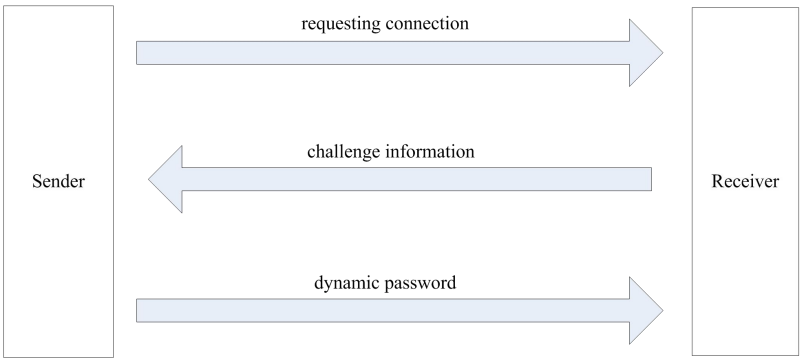

Fig 1. Authentication process of challenge/response

The authentication method of challenge/response is a relatively safe method, but it is suitable for the authentication of server to client, unable to complete the authentication of client to server. In addition, it was designed for the Client/Server mode, but it is not fit for the mode of machine to machine. The industrial Ethernet bus needs a two-way authentication protocol without manual handing for field equipments. And the authentication method of challenge/response can't complete Key distribution. So, this paper designed a new authentication and key distribution protocol.

3.A NEW CHALLENGE/RESPONSE MUTUAL AUTHENTICATION AND KEY AGREEMENT PROTOCOL BASED ON KEY TABLE

3.1. Key table

The keys are the key to encryption algorithm, the confidentiality of keys is the basic of safeguard information security. In the industrial network communications, the use of symmetric encryption algorithm is more realistic, non symmetric key encryption algorithm can increase too much amount of calculation to the industrial network, and the requirement of industrial network can't accept it. If the symmetric encryption algorithm be used by data encryption, we must consider the problem of how to use keys. If every communications are use the same key, obviously, this is not safe; if each field devices uses a single or a few keys, then face to numerous devices in the bus, will make the keys management become very complex.

If the control network communications use shared N keys and each connection randomly select an encryption key, then not only we can achieve the effect of one-time pad, but also the distribution and management of keys are also become very convenient. In the control network, each device stores a key table, as shown in table 1. There are stored N original keys in the key table. According to the security requirements and the properties of equipments, the value of n can be from a dozen to dozens or more. The mapping values RKS can be at random, this paper is using the hash of mapping values as mapping values.

Table 1: Key table

Keys(KS)		Mapping valures(RKS)
K0	→	Hash(K0)
K 1	→	Hash(K1)
……	……	……
KN	→	Hash(KN)

3.2. The Process of challenge/response mutual authentication and key agerrment

The traditional challenge/response authentication only authenticates the client identity. However, the challenge/response mutual authentication authenticates equipments on both sides of communication to ensure that the communication parties are legal equipments, and to prevent illegal equipments malicious connections. At same time, during the authentication, keys agreement process is ended.

The process of challenge/response mutual authentication and key agreement described as follows, the protocol flow chart shown in figure 2:

1）The sender sends the receiver the requesting information “hello”.
2） The receiver produces a security timestamp C1, and calculates the number of S = C1 mod N. Then receiver sends challenge message including security timestamp C1, the receiver’s device ID RID and the HASH (KS) that maps the value of key KS1.
3）The sender produces a security timestamp C2. Then the C1 and RID come from challenge message is encrypted cipher text with the key KS1 to produce the dynamic password PWS1. The sender sends the response message including the sender’s device ID SID and C2.
4）The receiver calculates the dynamic password PWS2 with the encryption algorithm as the same as process three. If PWS2 compares identically with PWS1 that was from sender, it is successfully verify sender’s identity. Then the receiver calculates the number S2 = C2 mod N, and use the key KS2 to encrypt C2 and SID that comes from sender’s response message as the dynamic password PWR2. The receiver sends PWR1 to the sender.
5）After received PWR1, the sender calculate the PWS2 with the encryption algorithm as the same as process four. If PWR2 compares identically with PWR1 that was from receiver, it is successfully verify receiver’s identity and send the finished message to sender.
6）At last, sender and receiver use the key KS to encrypt, S =（C1+C2）mod N, the process of key agreement and authentication are completed.

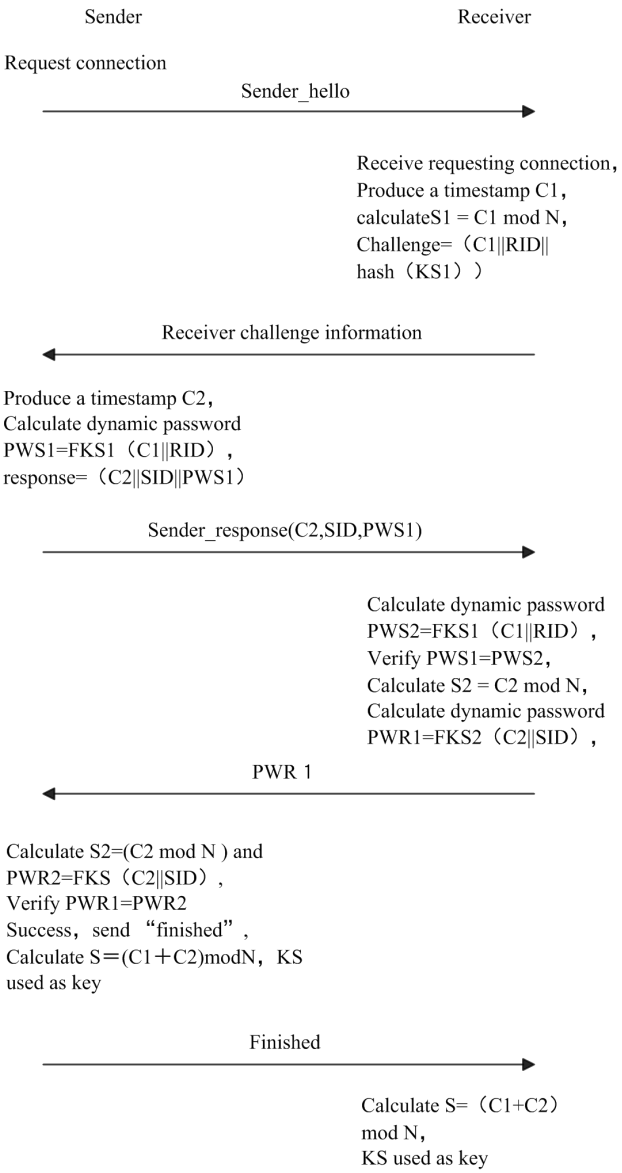

Fig 2. The process of new protocol

4. PERFORMANCE TESTING

The performance of security protocol directly affect bus protocol's real-time, so that the amount of computation overhead must be not too large. The performance overhead during the protocol implementation process is come from the data exchange times and the computation of CPU. This protocol does not appear too complicated public key encryption algorithm, it has only 4 times symmetric encryption algorithm. Computational overhead of the common symmetrical encryption algorithms, such as DES, IDEA, is very small, single chip computers have the ability to complete it. The produce of random number is according to the system time, the amount of calculate is also very few. Table 2 shows that this new protocol compared with other high speed protocols, as a result, the number of data operations are less than the other same type protocols and the difficulty of operations is quite low. During the whole process of new protocol, there are numerical calculation seven times and data exchange three times.

Table 2: New protocol compared with other high speed protocols

Types	Literature[13]	Literature[14]	Literature[15]	This parper
Data exchange	2	3	3	3
Encrypt operations	public-key	public-key		4
Modulus operations	0	3	0	3
Hash operations	2	2	5	0
Exponent poerations	8	4	7	0

By using C, this paper is realized the work flow of new protocol, and then tested the authentication protocol under working condition of TCP protocol. In the process of protocol implementation, this paper uses DES encryption algorithm and 64 bit keys to calculate dynamic password. There are 30 keys in the key table, according to the requirement of security level the number of keys can increase or decrease. The key table needs storage space about 1K~0.5K to store keys and the source code programs needs storage space about 11K~12K. If the storage space of industrial equipments is 2M, then the storage space of security protocol used takes 0.6% of the total space, the impact on industrial equipments storage space is very little. Table 3 and figure 3 shows that the statistics of the time-consuming of authentications ten times and the ratio of authentication time and session time.

Table 3: The time-consuming of authentications ten times

Times	Sender(ms)	Receiver(ms)
1	2.371	2.626
2	4.312	5.992
3	2.048	2.135
4	8.802	5.858
5	7.718	6.172
6	7.133	5.969
7	2.542	2.688
8	3.032	2.052
9	2.864	4.931
10	2.230	1.965
Average values	4.305	4.039

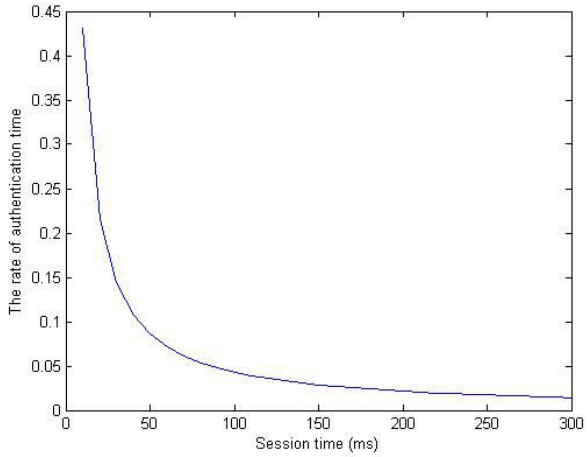

Fig 3. The ratio of authentication time and session time

5. PORTOCOL ANALYSIS OF SECURITY

5.1. Security of encryption key

In the whole process of authentication and key agreement, both sides of communication can reach the goal of hiding keys. The security of symmetric encryption algorithm based on the 128 bit key is very reliable, at present. So attackers are very hard to obtain the encryption keys by cracking the dynamic password. Even if there are one or several keys cracked, the final encryption key KS is produced by calculating the value of S = (C1+C2) mod N and C1, C2 are random number and not related, attackers are also can't obtain the final encryption key. So, through analyzing and cracking the cipher-text to get the key, there is not possible. A large number of field devices are sharing a same key table, which will bring a great convenience to key management. If it is found that equipments were lost, the key table should be immediately updated to prevent security information from leakage.

5.2. The ability of against attacks

By analyzing the new protocol, it can resist the message replay attacks, eavesdropping attacks, illegal connections. During the sessions, the new protocol uses the dynamic password to verify the legitimacy of each others. The protocol encrypts security timestamp and device ID to generate dynamic password, so that the dynamic password has the peculiarity of confidentiality and uniqueness. Therefore, when attackers are trying to tapping the password and replaying to the others, the other devices will not accept the same password again. Table 4 shows the security comparison of the new protocol and other literatures.

Table 4:The security comparison of the new protocol and other literatures

Types	Literature[16]	Literature[17]	Literature[18]	This paper
DoS	True	False	True	False
Replay attack	False	False	True	True
Resist the dictionary attack	False	True	False	True
Illagal connection	True	True	True	True
Eavesdropping	True	True	True	True
Algorithm	Asymmetric	Symmetric	Asymmetric	Symmetric
Temporal synchronization	False	False	False	True

CONCLUSION

Due to the industrial Ethernet equipments on the limited computational capability, this paper is designed a mutual authentication based on dynamic password challenge / response and key agreement protocol. This protocol can complete the identity authentication and key distribution. After the analysis, it shows that the new protocol can effectively resist replay attacks, illegal equipment connections, man in the middle attacks, the execution is high efficiency, and the model is simple and easy to implement on the field equipments.

Acknowledgements

This work was supported by key deployment project of Chinese Academy of Sciences (KGZD-EW-302), Liaoning Provincial Office of Fund (2012219001, Research on perception layer's technologies based on high reliability for Internet of Things in industry) and Liaoning Provincial Office of Education Fund (L2013157, Research on evaluation and reengineering based on reliability for Internet of Things software).

REFERENCES

[1]K. Stouffer et al., *American：National Institute of Standards and Technology*. **2011**, 800(82), 28-45.
[2]RUI Wanzhi et al., *Information and control*. **2012**, 41(1), 83-88.
[3]SONG Yan et al., *Information and control*. **2013**,42(4),521-528.
[4]SUN Ziwen et al., *Information and control*. **2013**, 42(6), 670-676.
[5]Frankel et al., Guide to IPsec VPNs[S], *American: NIST*. **2005**.
[6]Peyravian M. Jeffries C., *Computer Communications*. **2006**,29(5-6), 660-667.
[7]Li Shaofang, *Computer and Modernization*. **2006(**8), 102-104.
[8]WANG Hao et al., *Automation & Instrumenta.* **2011**, 24(7), 24-29.
[9]CHEN Xing et al., *Computer Science*. **2012**,39(10), 188-190.
[10]Li Yumin, *China Instrumentation***.2012**(11), 59-64.
[11] XU Ming et al,, *Computer Engineering and Design*. **2009**, 30(23), 5365-5368.
[12] Zhou Jie et al., *Ship Electronic Engineering.* **2009**, 29(7), 154-157.
[13]WANG Bangju et al., *Geomatics and Information Science of Wuhan University*. **2008**, 33(10) 1073-1075.
[14]Hwang J J et al., *IEICE Transactions on Communications*. **2002**, 85(4),823-825.
[15]YU Sheng. *Computer Engineering and Design*. **2009**, 5337-5339.
[16]XIANG Shun-bo, *Computer Engineering*. **2011**, 37(17), 128-129.

[17]HE Yijun et al., *Computer Applications*. **2007**, l27(7), 1603-1605.
[18]TAN Shi-chong et al., *Journal of University of Electronic Science and Technology of China*. **2008**, 37(1), 17-19.