A hybrid encryption algorithm in the application of equipment information management based on Internet of things

Peng Xu[1] Min Li[2] Yu-Jie He[3]

Abstract. This paper established the system structure of Internet of things (IOT) and analyzed the security threats in practical application of IOT equipment management system. Meanwhile, proposed a hybrid encryption algorithm based on DES encryption algorithm and DSA digital signature, which can realize the electronic tags encryption in IOT equipment management system to ensure the security of equipment information.

Keywords: Internet of things (IOT) • security threats • DES • DSA

1 Introduction

The management of the weapons and equipment is an important part of daily management. Military weapons and equipment have utilized in large quantities, frequently in and out of storage, security management task being heavy in use and supervision, thereby increasing the level of information management of the weapons and equipment being imminent with the emergence of the Internet of things(IOT) technology which provide a means for weaponry visualization techniques and achieve identification and tracking of the weapons and equipment in management and transport, achieve dynamic information about the equipment accurately, comprehensively and timely, and finally achieve efficient management of the weapons and equipment.

Equipment management technology based on the IOT has promoted the process of information construction, and the application of the IOT realized real-time monitoring, improved the predictability of status of weaponry predictability, made it easy on the accident predict in advance, improved efficiency of the maintenance and management and prolonged the working safety life of weapons and equipment, ensure the whole process of equipment manageable and controllable. The IOT provide a great convenience to weapons and equipment management, and also faced with many potential threats and security challenges, of which the most prominent is the data processing and retrieval of massive information and privacy protection and copyright protection of digital products and other safety issues.

[1]Peng Xu(✉)
Xi'an Research Inst. of Hi-Tech ,710025 ,Shaanxi Province, P. R. C.
e-mail: 727604092@qq.com
[2]Min Li
Xi'an Research Inst. of Hi-Tech ,710025 ,Shaanxi Province, P. R. C
[3]Yu-Jie He
Xi'an Research Inst. of Hi-Tech ,710025 ,Shaanxi Province, P. R. C
This work was supported by the National Natural Science Foundation of China under Grant No. 61102170

2 The System structure of IOT applications

IOT (The Internet of things) is an important part of the new information technology and is considered as the expansion of Internet applications. IOT[1] refers to through a variety of information sensing devices such as sensors, radio frequency identification (RFID) technology, Global Positioning System, infrared sensors, laser scanners, gas sensors and other various devices and techniques, acquire real-timely any the sound, light, heat, chemical, biological, location, and other desired information of any objects or processes need to be monitored, accessed, interactive, and form a huge network with the Internet. Its purpose is to achieve a connection between things and people, things and things, all objects and the Internet to facilitate the management, identification and control. The IOT was built based on the Internet and EPC system of radio frequency technology. Now international research on the structure of the IOT is mainly divided into two categories: the EPC system in Europe and America and the UID system in Japan.

EPC system is composed of the MIT Auto ID Center in 1999 in research and development of RFID technology with the United States Uniform Code Council (UCC) support, proposed the Electronic Product Code (EPC) concept, which is a new technology based on RFID technology, followed by creating RFID standards, and with the combination with network technology to form EPC system. EPC system is a comprehensive, advanced and complex system. It consists of three parts: EPC coding system, RFID systems and information network system, and the EPC architecture includes six aspects: EPC tags, EPC coding, reader, EPC middleware, Object Naming Service (ONS) and EPC Information Services (EPCIS). EPC system encodes the items on the global unified and stores the code n the EPC tags in the form of digital information and the reader read the label of EPC code through the wireless air interface, and finally transmitted by the EPC middleware to the information control center through the Internet, where the corresponding data processing is done. EPC structure is shown as Figure 1:

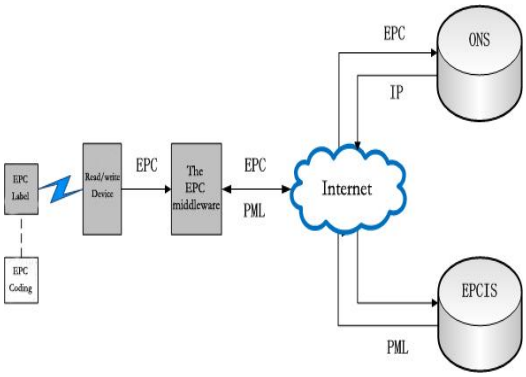


Figure 1 EPC system structure

3 Security threats of IOT equipment management system

Things is a system which is an extension and expansion of the client to any goods and goods, tracking and monitoring the object, and achieves information exchange and communication, it is widely used in logistics, transportation, industrial, medical, agriculture, health, military and many other fields. The IOT management

and applications systems can get equipment EPC information through interface between capture software (such as Savant), and to find the equipment PML information server through the ONS, thus obtaining equipment details, in order to achieve various applications. The application must meet the require that is automatic, real-time identification of objects, locate, track, monitor and trigger the corresponding event, make the equipment "intelligent equipment" equipped with dynamic information and make information flow and logistics equipment fully synchronized.

The IOT is very vulnerable to attack in Information transmission in the application of equipment management, because every piece of equipment must be perceived in real time, and the IOT machine / sensor nodes deployed in unattended most scenes, unattended and is a dynamic operation. To ensure information security and prevent information being stolen and eavesdropping in a wireless environment, will be the major issues need to be addressed in construction of equipment management.

Outside attacks to the IOT is mainly from three aspects: security threats on the perception layer, the transport layer (network layer) and the application layer. Security threats on perception layer mainly relate to RFID, WSN nodes and terminal of the IOT. Security threats on transport layer and network layer are mainly relate to transport security such as wireless sensor networks, the Internet and private networks, and transport in heterogeneous network security issues. IOT application layer security mainly involves intelligent terminal security, data confidentiality, integrity, availability, security, and application system itself [2, 3]. In this paper, the method for RFID security secrets is studied systematically; attacks on RFID systems are information tracking and eavesdropping, channel interference, the node camouflage, crack and tampering attacks, interference and denial of service attacks, inactivated tag attacks.

The fundamental safety objective of the IOT is to achieve confidentiality, integrity, Accountability, availability in the process of data or information transmission, storage and used of[4]. Implementation of information management of the equipment must first make information be written in the label, so that the tag information about the equipment can easily be leaked in the perception process. For example, reader which can cover a range of antennas can read out the RFID tags information, so that others can grasp equipment trends; greatly reduce the system's safety factor. In order to improve the security of management of the equipment, we use a DES digital signature algorithm and authentication technology in information processing, mainly from aspects of the data integrity, verifiable, tamper to protect confidential information between communications equipment, identified the source and accuracy of message, in order to ensure that the information in the secure transmission.

4 DES encryption algorithm and DSA digital signature

4.1 DES encryption algorithm

DES is an encryption algorithm in symmetric cryptosystem, plain text are grouped according to the 64-bit data, then encryption and decryption. The key length is 64 bits which contains 8-bit parity bits, so the actual key length is 56 bits. DES algorithm uses multiple combinations of alternative algorithms and exchange algorithm, and makes the plaintext strength compiled into a high cipher text.

4.2 DSA Digital Signature

A digital signature is to sign the information in electronic form instead of writing the signature or seal through a string generated by public key encryption technology, to identify the signer's identity and recognition on the information contained in data. Such a digitally signed data or transform allows the recipient of the data unit to confirm the source and the integrity of the data unit to protect the integrity of the data, and prevent malicious forgery and tampering. It is a sign messages method used in electronic form, because the "digital signature" technology is relatively mature, strong operability t has been widely used in the field of e-commerce and e-government, through the use of electronic signatures ensure the confidentiality, integrity and non-repudiation of the information in the transmission.

Complete digital signature algorithm consists of two parts: the message digest algorithm and the encryption and decryption algorithms, the Secure Hash Algorithm SHA-1 is the most commonly used in digest algorithm. This algorithm can achieve data integrity and authentication very good, and has good resistance to aggressive. Digital Signature Algorithm using public key cryptosystem DSA, DSA verify data integrity and data sender's identity for recipients with the use of public key.

5 Improved encryption algorithm based on DES and DSA

In the IOT equipment management system, RFID readers are scattered arrangement in a given weaponry, and the reader directly connected to the equipment management information system of the weapons and the electronic tag is moving, as long as the reader with an antenna can cover a range can read out electronic tag information, the reader scan the data information on the label to input weaponry management information system to storage, analysis, processing to achieve the purpose of control and management equipment. In order to ensure the security of electronic labels, hybrid encryption algorithm of DSA-based digital signature and encryption DEA algorithm is studied [5, 6], to ensure security of the electronic tags information.

Specific improved hybrid algorithm is:

1. First regroup 64-bit data according to blocks and put the output into L0, R0 two parts, each of 32 bits, and its replacement rule is that exchange the 58th bit with the first, the 50th bit with the second, ..., and so on, the last one is the original No. 7. L0 and R0 are the two parts after the transposition output, L0 is the left 32-bit of the output, and R0 is the right 32 bits. Example: Set the input value before transposition D1D2D3..... D64, then the results after of the initial transposition: L0 = D58D50 ... D8; R0 = D57D49 ... D7.

2.Sub-key generation algorithm

The 8th, 16th ..... 64th bit is a parity bit according to DES algorithm rule, and is not involved in DES operation. Key actual use 56 bits, this 56 is Divided into two parts C0 and D0, each of 28 bits, and cycle left for the first time, to obtain C1 and D1, then the C1 (28 bits), D1 (28 bits) obtained were combined to form a 56-bit date, and then selection transposition 2 through the narrow, so as to get a key K0 (48 bits). And so on, K1, K2... K15 can be got.

3.Calculated date hash value of the encrypted cipher text using the secure hash algorithm SHA-1. Parameters used in DSA signature are:

p: primes of L bits long. L is a multiple of 64 bits; the range is 512~1024 bits;

q: prime factors of 160bits of p-1;

g: g = h ^ ((p-1) / q) mod p, h satisfy h <p - 1, h ^ ((p-1) / q) mod p> 1;

x: x <q, x is the private key;

y: y = g ^ x mod p, (p, q, g, y) are public keys;
Signature process is:
P generates a random number k, k <q;
P compute r = (g ^ k mod p) mod q
s = (k ^ (-1) (H (m) + xr)) mod q
The result of the signature is (m, r, s).

Where H (m) is the Hash value of m, m is plaintext to be signed or Hash value of the plaintext. The final signature is integers (r, s), which is sent to the authenticator with m.

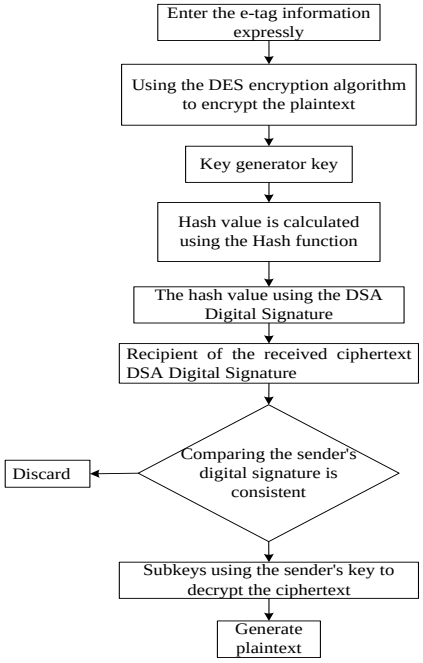
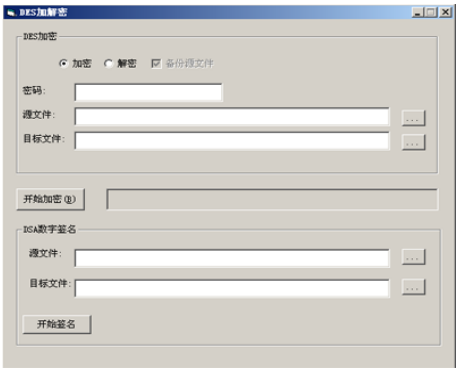


Figure 2 flowchart of hybrid algorithm based on the DES algorithm and DSA digital signature

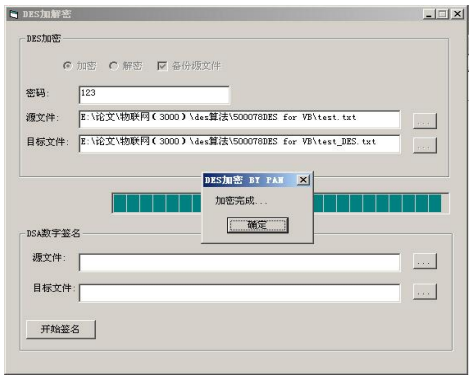
4. Firstly calculate the encrypted digital signature use SHA-1 algorithm after RFID reader receives the cipher text, if the signatures consistent with that provided by the sender, then use decrypt the cipher text with the sub-key generated by the DES algorithm to generate plaintext. Figure 2 is a flow chart of implementation.

6 Simulation results

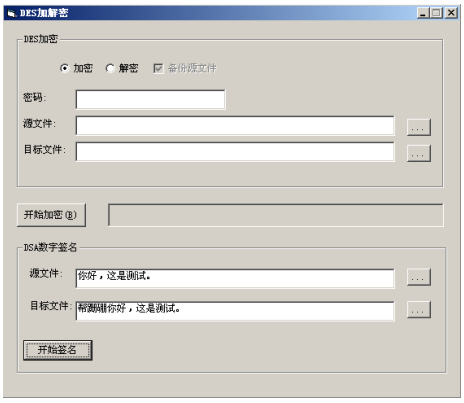
Visual Basic is used to the simulation of the improved hybrid algorithm, through the 16th iterations and inverse IP permutation to encrypt the plaintext, through the DSA sign the encrypted cipher text, the simulation interface is shown in Figure 3:



3.1 simulation interface of the improved hybrid algorithm



3.2 Schematic of encryption algorithm



3.3 the results of the signature algorithm

Figure 3 Simulation interface of the improved hybrid algorithm

When the input plaintext is "你好，进入测试环节", the result cipher text of DES encryption is "“DES 6t:bQ 朵 m 疸撲 Q 巇?i 炩 r 泼", then do DSA digital signature, the result is "宾玢拾 6t:bQ 朵 m 疸撲 Q 巇?i 炩 r 泼", where "宾玢拾" is the cipher text signature.

7 Conclusion

The use of the digital signature of hybrid key algorithm based on DES algorithm and the DSA algorithm in IOT of the equipment management equipment, on ensure one hand the confidentiality of information equipment and the integrity and confirmatory of the process of information transmission on the other hand.

References

1. Zhang Defeng. Cloud Computing Practice. [M].Tsinghua University Press.
2. Wang Zili, Deng Xin. .Things countermeasures system security threats Discussion[J].Modern computers. 2012.(12):7-10.
3. Zhang Daoyin. Thing security threats and countermeasures[J]. Hot technology. 2012,(4):009.
4. Shao hua,Fan hong. Things to achieve overall protection of information security technology research,2011,201(1):09.
5. Chen tong.3-des algorithm based train control system vehicle safely Communications Research and lmplementation [D],Beijing Jiaotong University ,master's degree thesis.2009.
6. Li Qian. Based on the DES encryption algorithm and ECC hybrid research and application of digital signatures[D]. Journal of Xi'an University of Technology,2008.