The Internet of Things Security Architecture Based IBE Integration with the PKI/CA[†]

Liu Yang[1,2*], Peng Yu [2],Wang Bailing [1], Bai Xuefeng[1], Yuan Xinling [1], Li Gen[1],

[1] Department of Computer Science & Technology
Harbin Institute of Technology at Weihai, Shandong, China
[2] Automatic Test and Control Institute
Harbin Institute of Technology, Harbin, China
[*] Liuyang322@hit.edu.cn

Abstract. With the rapid development of network technology content, the thing networking security issues have become increasingly prominent, the existing security mechanism in the content networking application has many problems and the insufficiency. This paper constructs the content networking security architecture, put forward the content networking acquisition layer and the transport layer using IBE and PKI/CA, through a combination of KDC security certification, realize the nodes and PKG public parameters and the safety of the private key node distribution, the effective protection of the node and gathering node data safety transmission. In the gathering node and things networking data processing intermediate through the PKI/CA authentication method, realize the security authentication and encryption transmission. Puts forward the private key generator key management strategy, realize the PKG public private key parameters and the rapid distribution, update, cancellation and so on, so as to ensure the physical network data transmission security.

Keywords: Security Architecture; Identity Based Encryption; Public Key Infrastructure/Certificate Authority

1 Introduction

The Internet of Things (IOT) are sensing technologies, such as RFID and sensor networks, communications networks and Internet technologies, intelligent computing technology, integrated, comprehensive perception, reliable messaging, smart characters connect physical world network. Its main characteristics are obtained through methods such as RFID, sensors all kinds of information in the physical world, combined with the Internet, mobile communication networks and other networks for the transmission of information using intelligent analysis technology for information processing, so as to improve the perception of the physical world, for intelligent decision-making and controlling a network. Internet is widely used in military, production control, environmental monitoring, urban management, transport and

[†] Supported by the National Science Nature Foundation of China under Grant No 61170262

logistics, medical, public safety, education, family life and other areas. Therefore, IOT was the computer, Internet and mobile communication network global information industry after another wave of technology and economy, and will bring great opportunities and to high-speed information challenges.

2 Present Research Situation on Security of IOT

Encryption is an important means to ensure the security of network transmission. Symmetric algorithm and asymmetric algorithm are two important methods in Key Management System. Eschenaue put forward a key distribution protocol based on probability[1], the protocol propose the key pool, each node storage parts of the key pool randomly, any numbers of nodes that have the same key can connect to each other, which can reduce the storage of key, however, that decreased the connectivity of nodes. To solve this problem, Pietro put forward a model of random key pre-distribution protocol[2], a group of keys, selected from the sub key space which randomly selected from the key space, assigned to the nodes. The nodes communicate each other with common key, while the shortcomings is that the nodes only can communicate with each other in the condition of a certain probability, based on which, there are other key distribution protocols like q-Composite[3], multiple key space randomly pre-distribution protocol[4], symmetric polynomials randomly pre-distribution protocol[5],randomly pre-distribution protocol based on Geographic Information System and so on.

Above studies is discussed from the point of view of the wireless sensor network secure transmission problems. As the Internet of Things is composed by RFID, WSN, Internet and other network, transmission of information security issues become more complicated .Using traditional security of a single network environment can't guarantee secure data transmission of IOT. In this paper, security architecture model of IOT established based on the analysis on the existing of IOT safety issues and research status. In a combination of the key distribution center KDC and the private key generator PGK in the sensing layer, processing on IBE public parameter , the distribution of the nodes of the private key and the session key, and put forward the private key generator key management strategy, which resolved IOT collecting data secure transmission problems. PKI / CA technology can verify authentication and encryption of transmission between aggregation node and the Internet of Things data processing center at the network layer, which solved network security transfer of Internet of Things, protected the privacy, integrity, and reliability of IOT data.

3 The Internet of Things Security Architecture

3.1 The process of node registered in KDC and distribute session key

The specific process is as follows:

1. Set the authenticated Key Distribution Center (KDC)

2. KDC distributes different symmetric key for each sensor node while registered, KDC knows the key of each node. Each sensor node can communicate with KDC safely using the key. KDC storage the ID of node and ID of PKG, calculating the Hash(ID) for storage.

3. Write K_A and Hash(ID_A) to node A, write K_{PKG} and Hash(ID_{PKG}) to PKG

4. When node A wants to communicate with PKG, node A sends K_A (A->PKG|| ID_A || Hash(ID_A)) to KDC

5. When KDC received the message, it decrypts information by K_A, and gets A->PKG|| ID_A || Hash(ID_A),calculates Hash(ID_A) with ID_A and compares with Hash(ID_A) that stored in database, If they are same then through the authentication. Otherwise, the ID counterfeit marked.

6. KDC generates random number r as session key(the session key that distributed by KDC is one-time pad), encrypts R$\oplus$Hash(ID_A)|| K_{PKG} (R$\oplus$Hash(ID_{PKG})) by using KA

7. After A receives the information, decrypts and gets R$\oplus$Hash(ID_A)|| K_{PKG} (R$\oplus$ Hash(ID_{PKG})) by K_A. A XOR R$\oplus$Hash(ID_A) and Hash(ID_A) that has stored , gets the session key R, and transfers K_{PKG} (R$\oplus$Hash(ID_{PKG})) to PKG

8. After PKG receives the message, decrypts it by K_{PKG}, and gets R$\oplus$Hash(ID_{PKG}). PKG XOR R$\oplus$Hash(ID_A) and Hash(ID_A) that has stored, gets the session key R, and store the session key of different nodes.

3.2 The process of transmission of IOT network layer security

The specific process is as follows:

1. The IOT data processing center and aggregate node Sink are resisted in the Certification Center(CA) firstly, the CA generates a digital certificate (CA encrypt by the private key) and the private key, then sends it via a secure channel to the IOT data processing center and aggregate nodes.

2. The integrate node Sink will first decrypt the ciphertext of the wireless sensor node transmitted into plaintext M, and using Hash function to obtain the abstract H (M), and using the private key $K_s^-$of integrate node to encrypt the abstract K_s^- (H (M)), to complete the receiving side to verify the integrity of the data and digital signature

3. The integrate node Sink uses a random number generator to generate a session key k_d to encrypt the plaintext, in order to achieve the confidentiality of the information.

4. The integrate node Sink sends the digital certificate of the the IOT data processing center to CA center for validation to identify the public key k_{dc}^+ of the IOT data processing center .

5. The integrate node Sink recognizes the authenticity of public key k_{dc}^+ of IOT data processing center, and encrypts session key k_d, k_{dc}^+ (k_d)

6. The integrate node Sink encrypts information using the session key, k_d(M)|| k_s^- (H(M))|| k_{dc}^+(k_d),and sends to the IOT data process center.

7. The IOT data processing center sends the digital certificate of integrate node Sink to the CA center for validation, in order to identify the authenticity of public key k_s^+ of the integration node Sink.

8. The IOT data processing center uses its own private key k_{dc} to decrypt $k_{dc}^+ (k_d)$ to get the session key k_d and then restitutes the plaintext M, recalculates the abstracts of the plaintext M, H (M '), and decrypts k_s^-(H(M)) to restitute the H (M) using public key of the integrate node, to complete the non-repudiation differential, and compared with H(M’) to determine the integrity of the information M .

4 Conclusions

In this paper, the security architecture of IOT is based on sensing layer and the transport layer, which combined with IBE and PKI/CA. In the sensing layer, the private key secure and public parameters distributed to the node safely via safety certification of KDC, which effectively protect the transmission of nodes and aggregation nodes. The information of security authentication and encryption can be transported safely via PKI/CA certified in the middle of the sink node and the Internet of Things data processing, put forward the private key generator key management strategy, and realized that PKG's public parameters and the rapid distribution of the private key, updater, evocation and so on, which ensured the transmission of the data security of the Internet of Things acquisition. In this scheme, algorithm complexity is low, and has a greater advantage in the robustness and security aspects**.**

References

1. Eschenauer L,Gligor V.A key-management scheme for distributed sensor networks.Proceedings of the9th ACM Conference on Computer and Communications Security.Washington DC,USA:ACM Press,2002.41-47.
2. Pietro R D,Mancini L.Random key assignment for secure wireless sensor networks.ACM Workshop on Security in Ad Hoc and Sensor Networks (SASN’03).Washington DC,USA:ACM Press,2003.62-71.
3. Chan H,.Random key predistribution schemes for sensor networks.IEEE symposium on Research in Security and Privacy.New York:IEEE publishing,2003.197-213.
4. LIU D,.Establishing pairwise key in distributed sensor network.ACM Transactions on Information and System Security,2005,8(1):41 77.
5. DU W,DENG J.A pairwise key pre-distribution scheme for wireless sensor networks.Proc. of the 10th ACM Conf. on Computer and Communications Security, 2003:42 51.