IOT Secure Transmission Based on Integration of IBE and PKI/CA

Liu Yang[1,2*], Peng Yu[2], Wang Bailing[1], Bai Xuefeng[1], Yuan Xinling[1] and Li Geng[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 in Internet of Thing technology, the security issues have become increasingly prominent. There are many problems and shortcomings in applying current security mechanisms to the Internet of Thing. In this article we build network security architecture by presenting combination of IBE and PKI/CA in the Internet acquisition and transport layer. With the KDC security certification, the node open parameters and the security of the private key of the node with the PKG distribution are implemented, and the nodes and node data transmission together are effectively protected. We also enable the secure authentication and encrypted transmission by PKI/CA in the middle of certification in aggregation nodes and network data processing. Moreover we propose the key management strategy of private key generator and realize the publication of PKG parameter and the fast distribution, update, and withdraw process of private key, which further ensure secure data network transmission.

Keywords: *The Internet of Things Security Architecture; Identity Based Encryption; Key Distribution Center；Private Key generate; Public Key Infrastructure/Certificate Authority*

1. Introduction

The Internet of Things (IOT) is a network connecting to the physical world. It integrates RFID and sensor network sensing technology, communication network and Internet technology, intelligent computing technology, realizing overall perception, reliable delivery and intelligent processing. Its main feature is access to the various kinds of information of the physical world through radio frequency identification and sensors, transmit information integrating the Internet and mobile communication network and other network, analyze and process information by intelligent computing. It improves the perception for the physical world and realized intelligent decision-making and control. Internet of Things is widely used in the defense and military, production control, environmental monitoring, urban management, transportation and logistics, education, health care, public safety, home life and other fields. Therefore, the Internet of Things will be another technology and economic tide of the global information industry following the computer, Internet and mobile communication network, and will bring great opportunities and challenges to the life of the high-speed information.

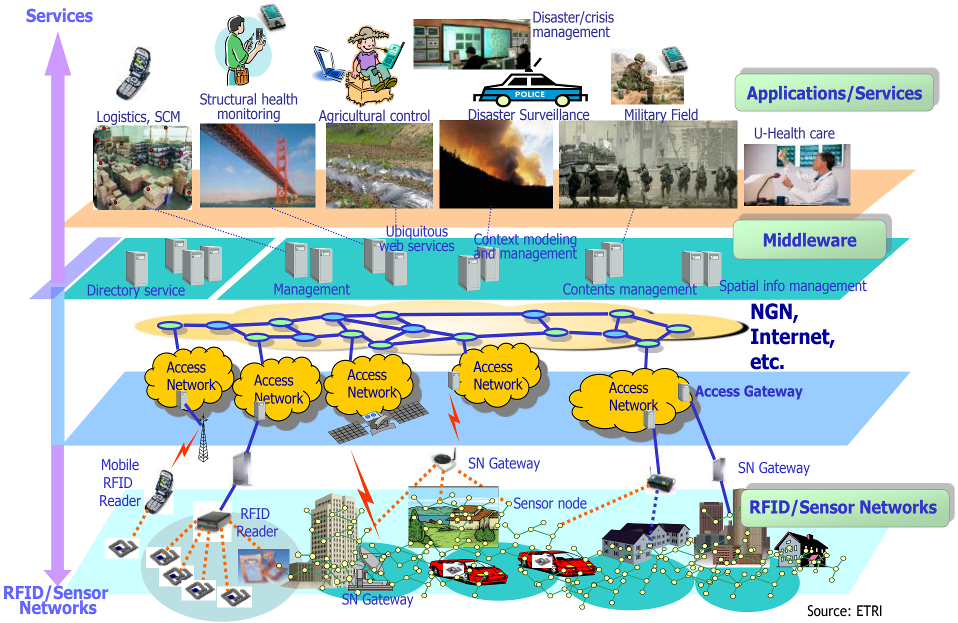


Figure 1. Structure of the Internet of Things

Research and Application of the Internet of Things is at an early stage, many of the theories and key technologies to be a breakthrough. With the all-round development of the Internet of Things, a variety of wireless communication technologies and network structure continuous integrate together, and communication network environment is becoming increasingly complex, basic network security issues are more complex and difficult to solve, a variety of complex heterogeneous communication systems will impact the overall security issues due to its characteristics. Therefore, the information security issue is the core technology relating to the Internet of Things industry safety sustainable development. Internet of Things security is not only related to information security, but also including national security, public safety, protection of intellectual property rights, personal privacy. Internet of Things safety goal is to achieve the collection of information confidentiality, integrity and availability. The trust relationship between the entities within the Internet of Things, secure communications, the extension of secure business and secure system have become an important research focus.

Whether it is in the Internet or wireless sensor network and RFID systems, the encryption processing is always an important means to ensure a secure network transmission. In key management system implementations, method based on the system of symmetric-key and methods based on the symmetric-key are two important encryption method. In symmetric-key encryption methods, Eschenauer proposed a key distribution method based on probability [1]. That program uses key pool and storages part key of the key pool in each node, when any number of nodes have the same key can connect. It reduces the keys stored in node but at the same time reduces the network connectivity. To solve this problem, Pietro et al proposed a random key pre-distribution model [2]. In the key space, the model randomly selects sub-key space, and further extracts a set of key again in the sub-key space and assigns to the node. It communicates through the node common key. But the drawback is that key only meet a certain probability be possible to communicate. On this basis, q-Composite method [3], Multi-key space random key pre-distribution method [4], symmetric polynomial random key pre-distribution method [5], based on geographic information or deployment information random key pre-distribution method [6] *etc.* appeared.

Compared with asymmetric-key system, the symmetric-key system has advantages in computational complexity, but there is lack of key management and security. For example, the difficult to certificate between neighbor nodes and the joining and leaving of nodes are not flexible enough. Especially in the Internet of Things environment, how to achieve the integration of key management systems and other network worth exploring. For this reason, the asymmetric-key system is also applied for wireless sensor networks. TinyPK used the MICA2 nodes on the TinyOS environment to realize the nodes certification outside the sensor network and TinySec key distribution by using RSA algorithm [7]. BENENSON Z realized TinySec key distribution based on ECC (ellipse curve cryptography) on MICA2 nodes for the first time [8]. Richard proposed improved program for the key management based on lightweight ECC, especially as one of the public-key cryptosystem based on circular curve cryptosystem. That has been a great deal of attention in the wireless sensor network key management, and has some theoretical research value and application prospects [9]. In recent years as asymmetric key systems IBE (Identity-Based Encryption) algorithm caused attention. IBE algorithm was first proposed in 1984 by Shamir [10]. The basic idea of this encryption algorithm is a public key can be any unique string, such as the e-mail address, social security number as the user's public key. Its advantage is the public key, can be identified, does not require the usual PKI certificate issued, and the algorithm implementation form of elliptic curve. IBE prototype [11] system is proposed by Boneh and Franklin, 2001, which is a key generation center PKG (Private Key Generate) as the main system. Canetti [12] proposed the use of any chosen plaintext attack security IBE scheme can construct chosen ciphertext attack security IBE scheme, and proposed a specific IBE system. Gentry, *et al.*, [13] proposed a safe and practical hierarchical IBE scheme. Boneh, *et al.*, [14] in the case of not using bilinear pairings, based on quadratic residue assumption, proposed a space-efficient IBE algorithm.

The above study discussed secure transmission most from the point of view of the wireless sensor network. As the Internet of Things consists of RFID, WSN, Internet and other networks, the transmission of information security issues become more complex, using a single network environment safe handling mechanism cannot guarantee secure data transmission of the Internet of Things. This paper analyses on the existing of Things safety issues and research status, establish security architecture model of the Internet of Things, using IBE PKI /CA combination of methods, combining of Key Distribution Center KDC and private key generator PGK in Collection Layer, processing session key, IBE public parameters and node private key distribution. And proposes private key generator key management strategy to solve the problem of the Internet of Things collecting data secure transmission. In the network layer, Using PKI/CA technology to achieve security authentication and encryption transmission between the aggregation node and the Internet of Things data processing center, solve the security transmission of the Internet of the Things, and protect the Internet of Things data privacy, integrity, reliability.

2. IBE algorithm and PKI/CA

PKI/CA technology whose core is digital certificates encrypts and decrypts the transmission of information on the network, digital signatures and signature verification. It either to ensure that information unless the sender and the receiver themselves are not stolen by other people, can also ensure that the information has not been tampered with during transmission. Sender confirms the identity of the recipient through digital certificates, but also to ensure that the sender cannot deny their own sent messages. Therefore, we can consider use PKI technology which is extensive use in the Internet to protect the security of information transmission and certification in the Internet of Things. IBE core is bilinear map on super singular elliptic curves, and use the algorithm of the Bonelr Franklin. The algorithm consists of four main functions: Setup, Extract, Encrypt and Decrypt, respectively to complete the establishment of the system public parameter, the private key extraction, the encryption and decryption process. Specific methods are as follows:

(1) Initialization process: The initialization process consists of two parts. First, calculate the public parameters, and second calculate nodes key. First calculate the public parameters, and select the master key s; according to the identity of each wireless node ID ,calculate HASH and using the master key to generate the appropriate key K; transmit parameters and the node private key K to the wireless nodes, such that each node has its own public key and the associated parameters.

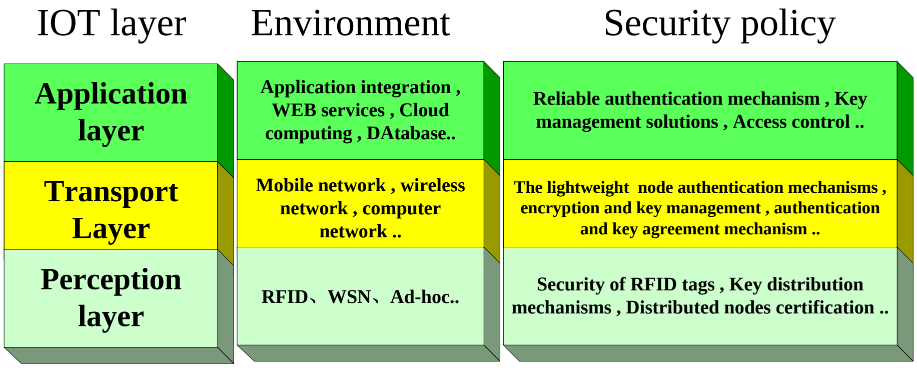
(2) Encryption process: In a wireless sensor network, B's identity ID as public key and random number taken r, using plaintext encryption for the transmitting node A and receiving node B. Of particular note is the IBE-based algorithm may make encryption and authentication combined, take a small price to complete the encryption and authentication. This is also the advantages of IBE algorithm can be further applied to wireless sensor networks.

(3) Decryption process: When node B receipt ciphertext, use key K to decrypt the original.

The program considering the advantages of PKI / CA and IBE algorithm, combining the two to achieve the secure transmission of information in Perception layer and Transport layer of the Internet of Things.

3. Security architecture of the Internet of Things

Based on the above analysis, taking into account the overall needs of the Internet of Things safety mainly combine physical security, information collection security, security of information transmission and information processing security, the ultimate goal of secure is to ensure information confidentiality, integrity, authenticity, and network fault tolerance, so design the security architecture of the Internet of Things is mainly divided into three logical layer, that Perception layer, Transport layer and Application layer.



IOT layer	Environment	Security policy
Application layer	Application integration , WEB services , Cloud computing , DAtabase..	Reliable authentication mechanism , Key management solutions , Access control ..
Transport Layer	Mobile network , wireless network , computer network ..	The lightweight node authentication mechanisms , encryption and key management , authentication and key agreement mechanism ..
Perception layer	RFID、WSN、Ad-hoc..	Security of RFID tags , Key distribution mechanisms , Distributed nodes certification ..

Figure 2. Security architecture of the Internet of Things

The information collection security in Perception layer: In the hierarchical model of the Internet of Things, the physical security layer and information collection security layer corresponding to the Perception layer security of the Internet of Things. Guarantee of the Internet of Things information collection node (physical node) is not to be deceived, controlled, destructed; prevent the collection of information is eavesdropped, tampered, forged and replay attacked.

The security in Transport layer: To ensure that the process of information transmission data confidentiality, integrity, authenticity, and freshness, mainly for telecommunication network security, and corresponds to the security of the network layer of the Internet of Things.

The security in Application layer: Guarantee the privacy of the information and store security, mainly for individual privacy protection, business data security verification.

This paper mainly related to the Internet of Things collection layer and transport layer security issues, the secure communications architecture design as follows:

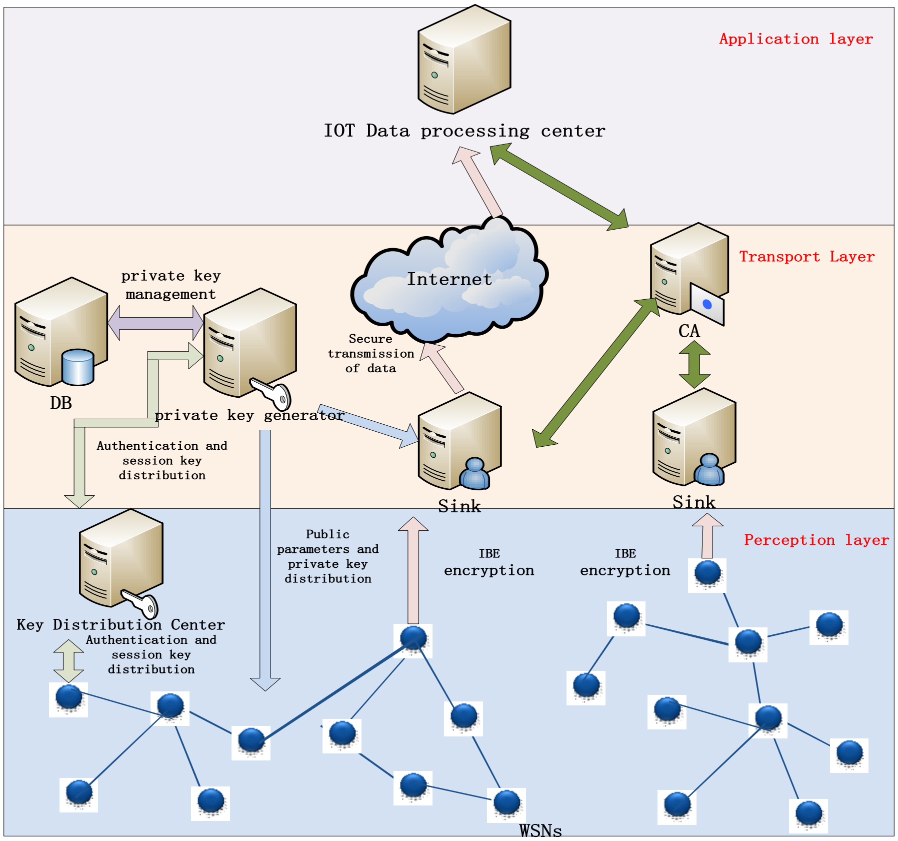

Application layer
IOT Data processing center
Transport Layer
Internet
private key management
CA
Secure transmission of data
DB
private key generator
Authentication and session key distribution
Sink
Sink
Perception layer
Public parameters and private key distribution
IBE encryption
IBE encryption
Key Distribution Center
Authentication and session key distribution
WSNs

Figure 3. The Internet of Things Security Architecture

Collection layer mainly related to the Key Distribution Center (KDC) as nodes and Private Key Generator (PKG) allocating session key, PGK public parameter generation and node private key generation, distribution, encryption and decryption, update, revocation processing; In Transport layer, mainly use PKI/CA technology to achieve the date transmission security from aggregation node to data processing centers of the Internet of Things. The specific process is as follows:

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

1. Set the Key Distribution Center (KDC), KDC is certified.
2. When sensor nodes are registered, KDC allocate different symmetric key for each sensor node, and KDC know the key for each sensor node. Each sensor node can use this key to communicate safely with KDC; KDC store node ID and the ID of PKG to computing 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 need to communicate with PKG, A sends K_A(A->PKG|| ID_A || Hash(ID_A)) to the KDC.
5. When KDC receipt information, it decrypts information by KA to get A->PKG|| ID_A || Hash (ID_A). It recalculates Hash (ID_A) and compares to Hash (ID_A) stored in database, and get authentication if the same. Otherwise to mark the ID with counterfeit.
6. KDC generates a random number R as a session key (KDC distributes the session key R for the nodes is the one-time pad), using K_A to encrypt the follow information K_A (R $\oplus$ Hash(ID_A)|| K_{PKG} (R $\oplus$ Hash(ID_{PKG}))).
7. When A receipt information, decrypt the information by K_A to get R $\oplus$ Hash(ID_A)|| K_{PKG} (R $\oplus$ Hash(ID_{PKG})), A XOR R by Hash(ID_A) R $\oplus$ Hash(ID_A) to get the session key R and forwarding K_{PKG}(R $\oplus$ Hash(ID_{PKG})) to PKG.
8. When PKG receipt information, decrypt the information by K_{PKG} to get R $\oplus$ Hash (ID_{PKG}). PKG XOR R by Hash (ID_{PKG}) R $\oplus$ Hash(ID_{PKG}) to get the session key R and store the session key of different nodes.

PKG public parameters and node private key generation, update, revocation:

1. PKG generates public parameters.
2. PKG generates node private key. KDC sends node ID information which is certified to PKG by R encryption. PKG decrypts and stores node ID information in database, while PKG initialize the key server to generate public parameter P and master key s, where s is secret shared by way of s*P. Use the master key s and node ID to generate private key s*PID for node.(PID is a point on the elliptic curve by the node ID through a hash function converted from), store the private key corresponding to the ID and set a time-out TTL.
3. The PKG can use the session key R to distribute public parameters P and node private key s*$P_{IDA.}$ When nodes receive the information, they decrypt by R to obtain the public parameters P and node private key s*$P_{IDA.}$
4. If the TTL timeout, the PKG generates a random number r 'and XOR master key s to generate s'=s $\oplus$ r' as a new master key, and recalculate the private key corresponding node ID, and distribute new private key and public parameters after storage. Node receives a new node key, should be allowed within a certain time the presence of the private key of the original node, ensure that some of the nodes using the original public parameter, ID.
5. PKG encrypts using session key R1 and sends public parameters and private key of A which is generated by PKG to sensor node A.

6. If the events such as counterfeit, symmetric key are compromised, the session key is compromised, KDC or PKG should immediately revoke the original node, update the session key, the PKG master key, node private key information timely, and distribute new session key, symmetric key and other information in inner network. Meanwhile, the aggregation node should refuse the ID information after it receipt the revocation information, and wait for update information.

Wireless sensor network encryption and decryption process in Perception layer:

1. Encryption: The sender of the message using the public parameter P calculated aggregation node Sink P_{ID}, and then select a random number r to calculate the encryption key K, K=Pair($r*P_{ID}$， s*P), then encrypt the plaintext M, send the ciphertext together with r*P to the aggregation node Sink.
2. Decryption: After aggregation node Sink receipts the ciphertext, uses the nature of bilinear mapping to calculate the decryption key K by its private key $s*P_{ID}$, K=Pair($r*P_{ID}$， s*P), thereby restore information M.

The security transfer process in the network layer:

1. The IOT data processing center and aggregation nodes Sink first register in the CA Certification Center. The CA certificate Center generates digital certificates (CA private key encryption) and private key and send them to the IOT data processing center and aggregation nodes through a secure channel.
2. The aggregation node Sink will first decrypt the ciphertext transmitted in the wireless sensor node into plaintext M, obtain the message digest H (M) by Hash function, and use aggregation node Sink private key k_s^- to encrypt Message Digest k_s^- (H(M)) to complete the verification of digital signature and data integrity of the recipient.
3. The aggregation nodes Sink using a random number generator to generate a session key kd, using the session key to encrypt the plaintext to provide encryption efficiency and confidential of the information.
4. The aggregation node Sink sends the digital certificate which is got from the IAT data processing center to CA to verify, so that can identify the public key k_{dc}^+ authenticity of the IOT data processing center.
5. The aggregation node Sink uses k_{dc}^+ encrypt session key k_d, based on the authenticity of the public key k_{dc}^+ of the IOT data processing center, $k_{dc}^+(k_d)$.
6. The aggregation nodes Sink encrypts information with the session key, $k_d(M)||\ k_s^-(H(M))||\ k_{dc}^+(k_d)$, sending to the IOT data processing center.
7. The IOT data processing center sends the digital certificate of the aggregation node to the CA to verify, in order to identify the authenticity of the the Sink public key ks+ so that nodes can be identified.
8. The IOT data processing center use their private key k_{dc}^- to decrypt $k_{dc}^+(k_d)$ and obtain the session key k_d, to restore the plaintext M. Recalculate the message digest H(M’) of the plaintext M, simultaneously use aggregation node Sink public key k_s^+ decrypt k_s^- (H(M)) to restore H(M), so that complete non-repudiation identification. And compare to H(M’) to determine the integrity of the information M.

4. Safety analysis

As PKI/CA technology is used in Transport layer of the Internet of Things, it has advantages in terms of security and robustness. Now we analyses the approach of the collection layer.

Sensor network nodes have the characteristics of low computing power, small memory, and small battery energy and so on. Traditional asymmetric encryption algorithm has great difficulty in the direct application of wireless sensor network, so the algorithm must be extended effectively. In the PKG distributed node private key process, we use the way that symmetric key distribute session key. Because the key is easy to leak, the program uses the way that KDC first authenticate the node information, process node information by Secure Hash Algorithm. This realizes the authentication between the nodes, and has a low complexity of the algorithm.

Although IBE-based encryption method is the asymmetric encryption method, the complexity of the algorithm mainly depends on the calculation of the bilinear map and hash function, no matter in the encryption process or the decryption process. IBE algorithms core is to use a bilinear map on super singular elliptic curve, calculate the input date with limited times. As a result of using Hash algorithm, it has the asymmetric key system flexibility, but also has simplicity with symmetric key system. Therefore, on the complexity, the algorithm based on the IBE method is between symmetric key system and asymmetric key system, and far less than the RSA method in asymmetric key system.

On robustness of the key system, for IBE scheme, the public key is the other's identity ID, the generated key is only owned itself. When a node is cracked, does not involve the safety of the other nodes. It has nothing to do with the size of the network, thus ensuring strong network robustness. Therefore, the algorithm given in the robustness and security aspects has more advantages than the current random algorithm.

In IBE-based method, each wireless node only needs to store the public parameters, its own identity ID and key K. And storage capacity has nothing to do with the size of the network, and can ensure the key pair communication with any node, rather than in the form of a probability to ensure that key pair shared between the nodes. At this point, also shows the superiority based on IBE's key method.

5. Conclusion

This paper establishes a security architecture on the collection layer and transport layer of the Internet of Things using a method that IBE and PKI/CA combined, realizes the secure distribution for nodes and PKI public parameters and nodes private key, protecting the secure transmission of the nodes and aggregation nodes effectively; In the aggregation nodes and data processing of the Internet of Things, realizes the security authentication and encryption transmission through PKI/CA certification; Proposes private key generator key management strategy, and realizes PKG's public parameters and private key distribution, update, revocation processing, thus ensure secure transmission of data in the Internet of Things. The algorithm complexity of this program is low, having a greater advantage in the robustness and security aspects.

Acknowledgements

This research was supported by the National Science Nature Foundation of China under Grant No 61170262.

References

[1] L. Eschenauer and V. Gligor, "A key-management scheme for distributed sensor networks", Proceedings of the9th ACM Conference on Computer and Communications Security, Washington DC, USA: ACM Press, **(2002)**, pp. 41-47.

[2] R. D. Pietro and L. Mancini, "Random key assignment for secure wireless sensor networks", ACM Workshop on Security in Ad Hoc and Sensor Networks (SASN'09), Washington DC, USA: ACM Press, **(2009)**, pp. 62-71.

[3] Q. Y. Dai, R. Y. Zhong, M. L. Wang, X. D. Liu and Q. Liu, "RFID-enable Real-time Multi-experiment Training Center Management System", International Journal of Advanced Science and Technology, vol. 7, **(2009)** June, pp. 27-48.

[4] H. Chan, "Random key predistribution schemes for sensor networks", IEEE symposium on Research in Security and Privacy, New York, IEEE publishing, **(2009)**, pp.197-213.

[5] D. Liu, "Establishing pairwise key in distributed sensor network", ACM Transactions on Information and System Security, vol. 8, no. 1, **(2009)**, pp.41-77.

[6] W. Du and J. Deng, "A pairwise key pre-distribution scheme for wireless sensor networks", Proc. of the 10th ACM Conf. on Computer and Communications Security, **(2009)**, pp. 42-51.

[7] Y. Zhen, "A key management scheme using deployment knowledge for wireless sensor networks", IEEE Transactions on Parallel and Distributed Systems, vol. 19, no. 10, **(2008)**, pp.1411-1425.

[8] H. D. Gao, Y. J. Guo, J. Q. Cui, H. G. Hao and H. Shi, "A Communication Protocol of RFID Systems in Internet of Things", International Journal of Security and its Applications, vol. 6, **(2012)** April, pp.91-102.

[9] D. Zhenhua, L. Jintao and F. Bo, "Research on Hsah-based RFID security authentication protocol", Journal of Computer Research and Development, vol. 4, **(2009)**, pp.583-592.

[10] R. Watro and D. Kong, "TinyPK:Securing Sensor Networks with Public Key Technology", SASN'04(ACM), Washington DC, **(2010)**,pp. 322-339.

[11] Z. Benenson, "Realizing robust user authentication in sensor networks", Proceedings of the Work shop on Real-World Wireless Sensor Networks (REALWSN 2009), Stockholm, **(2009)**, pp.135-142.

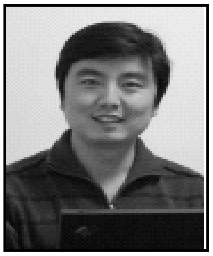
[12] S. Richard, "A Low-power design for an elliptic curve digital signature chip", Lecture Notes in Computer Science, **(2011)**, pp.366-380.

[13] A. Shamir, "Identity-based cryptography and signature schemes", Advances in Cryptology, CRYPTO'08, Lecture Notes in Computer Science, **(2008)**, pp.47-53.

[14] D. Boneh and F. Franklin, "Identity-based Encryption from the Weil Pairing", Advances in Cryptology-Crypto'2001, LNCS 2139, Springer-Verlag, Berlin, **(2001)**, pp.213-229.

Authors

Liu Yang is an Associate Professor; his research fields include Network information Security Technology, Internet of Things Security Technology, etc. He has participated in many projects of Ministry of Information Industry and National Science, and he has published over 20 academic papers in journals and conferences both home and abroad.



Wang Bailing is working for Harbin Institute of Technology (abstract as HIT) as an associate professor. He got the Ph.D. degree from HIT in 2006. His research is mainly on information security, network security, parallel computing.