International Journal of Future Generation Communication and Networking
Vol.6, No.6 (2013), pp.1-10
http://dx.doi.org/10.14257/ijfgcn.2013.6.6.01

Research on Security Issues of the Internet of Things

Chen Qiang[1,*], Guang-ri Quan[2], Bai Yu[3] and Liu Yang[2]

[1] Heilongjiang Co., Ltd. of China Mobile Communication Corporations,
Harbin, China
[2] Department of Computer Science & Technology
Harbin Institute of Technology at Weihai, Shandong, China
[3] Department of Computer Science & Technology
Harbin Institute of Technology, Haerbin, China
** hlhlj@139.com*

Abstract

There are many problems in security of Internet of Things (IOT) crying out for solutions, such as RFID tag security, wireless security, network transmission security, privacy protection, information processing security. This article is based on the existing researches of network security technology. And it provides a new approach for researchers in certain IOT application and design, through analyzing and summarizing the security of ITO from various angles.

Keywords: *Information processing, Network transmission, Privacy protection, security of IOT*

1. Introduction

The Internet of Things (IOT) is mutual integration of the product of wireless sensor networks (WSN), Ubiquitous network, Pervasive Computing and Internet. In 2005, the World Summit on the Information Society (WSIS) held in Tunis, The International Telecommunication Union (ITU) formally proposed the concept of Internet of Things. The report pointed out that the ubiquitous "Internet of Things" communication era is approaching, Radio frequency identification (RFID) technology, sensor technology, nanotechnology, intelligent embedded technology will be more widely used. According to the description of the ITU, in the era of the Internet of Things, short-range mobile transceivers embedded in a variety of daily necessities, human beings in the world of Information will get a new dimension of communication, from any location at any time communication between people. Communication connection extended to persons and things, and between things. Subsequently, IBM announced the latest strategy called "wisdom of the Earth". Some analysts believe that the idea of IBM's most likely to rise to the national strategy of the United States, and caused a sensation in the world. IBM believes the next phase of the mission of the IT industry is to make full use of the new generation of IT technology in all walks of life among. Specifically, embedding and equipping the sensor (Sensor) to the power grid, railways, bridges, tunnels, roads, buildings, water supply systems, dams, oil and gas pipelines and other objects, and universal connectivity to from IOT. Because of the IOT theoretical system is not sound and the understanding is not in-depth, IOT in this stage is not a precise and generally accepted definition. Same time, because of things and the Internet, mobile communication network, sensor networks are closely related, different areas of researchers thinking IOT based on different starting point, so the short term, there is no consensus. Currently, a more

ISSN: 2233-7857 IJFGCN

comprehensive definition of Internet of Things is: Internet of Things is new network that interconnect the wireless sensors and radio frequency identification (RFID) sensing devices through a wireless network and Internet technologies to achieve the overall perception of information, reliable transmission, and intelligent processing. It connects any article with the Internet through radio frequency identification (RFID) devices, infrared sensors, global positioning systems, laser scanners and other information sensing device in accordance with the agreed protocol to the exchange of information and communication, in order to achieve the intelligent identification, positioning, tracking, monitoring and management.

The main features of the Internet of Things first are comprehensive perception, using RFID, sensor, two-dimensional code to access to the information of the object anytime, anywhere. Scope of data collection terminal connected through the Internet of Things is very broad, involving hundreds of millions of heterogeneous devices ubiquitous access, including mobile phones, computers that already have powerful computing, storage and communication capabilities of the terminal; appliances, railways, bridges, buildings such as the embedded sensor device; radio frequency identification (RFID) devices, infrared sensors, global positioning systems, laser scanners. Followed by a reliable transfer, through the wide variety of data collection terminal including the Internet, mobile Internet and other network interconnection, to achieve real-time acquisition of external environment information, the dynamic information of the object and convert it into a data format suitable for network transmission, and transfer to the data center through network. Finally is intelligent processing, using cloud computing, fuzzy identify and other intelligent computing technology to analyze and process vast amounts of data and information to achieve intelligent control for objects.

At present, the global Internet of Things industry market will show rapid growth, with an estimated 2012 global logistics network the size of the market or more than 170 billion U.S. dollars, in 2015 to nearly $ 350 billion, an average annual growth rate of nearly 25%.

With the all-round development of the Internet of Things, a variety of wireless communication technology and network structure continuous integration, including wireless sensor networks, RFID networks, mobile vehicle network, mobile network, 3G communication network, the WiMAX communication networks and wired broadband. Communication network environment has changed more and more complex, the security issues carrying all kinds of business on the basis of network is are more complex and difficult than existing network system to solve. Manifestations of security issues involved on the Internet of Things application are discussed in the article, from the point of view of the RFID tag information security, information security of wireless communications, network transmission of information security, privacy protection, and information processing security to analyze the hidden dangers in the IOT.

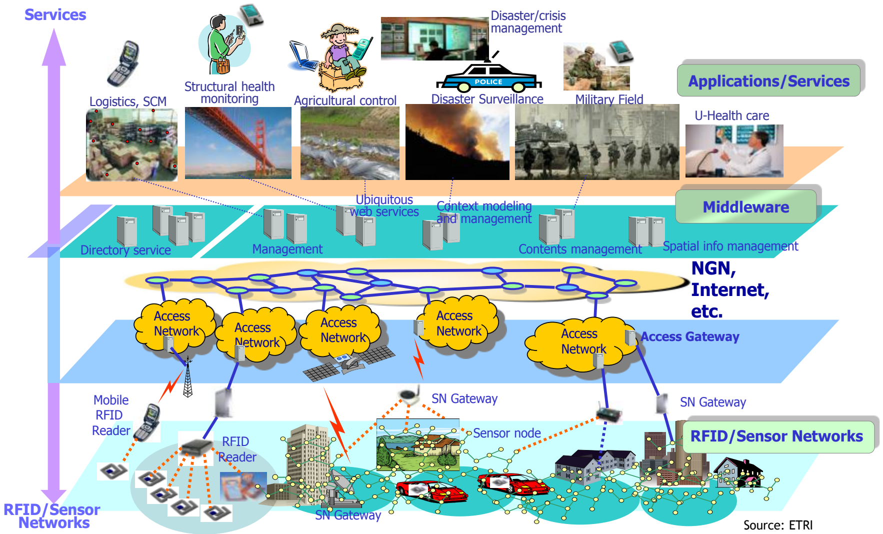
2. Internet of Things Security Requirement

The worm containment propagation model studied the interaction between the parameters composition included in containment strategy and the parameters in the process of containment, then establish a complete mathematical description and draw worm outbreak curve in the process of containment under different conditions, then compared with the behavioral simulation results and correct each other. By comparing worm epidemic curves before and after containment, the worm spread behavior changes and epidemic trends under the different containment strategy can be analyzed, so as to contrast the effectiveness of the containment strategy and the place need to further improve. This article assumes vicious worms using uniform random scanning strategy.

Internet of Things safety issues is mainly manifested in the following points: The first is the physical security, the main is sensor security, including sensor interference, shielded, signal intercepted and it is IOT embody of safety characteristic; The second is the operation safe, it exists in the various elements, related to the normal operation of the sensor, transmission systems and treatment systems, and it is basically same with traditional information systems security; The third is the data security, also exist in various elements, and it demands the information in the sensor, the transmission system and the processing system will not be stolen, tampered, forged repudiation. The security problems faced by the sensor and sensor network (WSN) is more complex than the traditional information security, and sensors and sensor network may not run because of the energy-constrained problem is too complex protection system. Therefore, the Internet of things in addition to facing general information network security issues facing the Internet of Things unique threats and attacks.

If these issues are not handled properly in the Internet of Things is widely used, the country's economic and security will be threatened. Therefore, it is necessary to in-depth study safety issues that may be encountered in the application of things, to design and improve its security problems countermeasures. Only in this way can promote extensive application of the Internet of Things, otherwise, the Internet of Things can only be deployed in a limited and controlled environment, so that it cannot fully play its due role.

Information and network security goal is to reach the confidentiality, integrity and availability of information need to protect. In the early stages of the Internet, people are more concerned about the basis of theoretical and applied research. With the increasing scale of networks and services, the security issues are particularly significant and have aroused people's attention, some security technologies, such as intrusion detection systems, firewalls, PKI are launched. Research and Application of the Internet of Things in its infancy, a lot of theory and key technology need breakthroughs. Internet of things to be widely used in various fields, the importance of information security problems is self-evident. The information security of the Internet of Things has five hidden dangers: the RFID tag information security, wireless communications information security, network transmission of information security, privacy, and information processing security.



Source: ETRI

Figure 1. Structure of the Internet of Things

2.1. RFID Tag Information Security

RFID radio frequency identification is a non-contact automatic identification technology, through radio frequency signal to automatic identify target recognition and access to relevant data, identify fast moving objects and can also identify multiple tags, the identification work without human intervention, and the operation is also very convenient. Same with the traditional Internet, the RFID system is susceptible to various attacks. This is mainly due to the communication between the tag and reader is achieved by the form of electromagnetic waves, the process does not have any physical or visual contact. There is a serious safety hazard in this non-contact and wireless communications. RFID security defects mainly in the following three areas:

1. RFID identification itself to access security issues. Due to the cost of the RFID identification itself, make it difficult to have enough to ensure its safety. In this way, we face a lot of problems. When labels receive the commands and data information from the receiving reader, may result in the error results: (1) Label error in response to reader commands; (2) Confuse the label working condition; (3) Label write error and go to sleep. Due to cost constraints, many labels cannot use a strong programming and encryption mechanisms, so that unauthorized users can take advantage of the legitimate reader or self-configuring a reader to communicate directly with the label, so that the label inside the data extremely vulnerable to theft, for those who can read and write will also face the risk of data is modified.

2. Security issues of the communication channel. RFID uses wireless communication channel, which bring the convenience of attack to unauthorized users. The attacker can unlawful intercept of communications data; The RFID system is mainly used two kinds of frequency signals, one is a low-frequency signal (electromagnetic induction), close transmission. The main frequency has 125 kHz, 225 kHz 13.65 MHz. The other is the high-frequency signal and microwave (electromagnetic propagation), the main frequency has 433 MHz, 915 MH z of 2.45 GHz at z and 5.8 GHz. Now the electromagnetic signals of the respective frequency bands are in the application, the interference between adjacent frequency bands is serious [1]. The direct impact of interfere is data errors in the reader and tag communication process. Therefore, the attacker can block the communication link through the launch of the interference signal, making the reader overload and cannot receive the normal tag data, manufacturing denial of service attacks; also can impostor to send data to the RFID, tamper or fake data.

3. Security issues of the RFID reader. RFID reader can be forged; Communication between the RFID reader and the host can be intercepted by the traditional method of attack [2]. Therefore, the RFID reader is naturally the object of attack for attacker. It can be seen that the RFID encountered security problems are much more complex than the usual computer network security problem. When the reader receive messages sent by label, may result in errors: (1) cannot identify working labels and misjudgment labels fault; (2) Identify a label for additional one and result in recognition errors. So middlemen (Middleware) can modify the configuration file, eavesdropping and interference exchange of data by directly or indirectly between the reader and the host (or application).

2.2. Wireless Communications and Information Security

IOT most use wireless transmission in the information transmission, mainly refers to wireless sensor networks and communication networks and other means of transmission. The exposed radio signals easily become the object of the attacker steal and interference; this will result in a serious impact on information security of IOT. Wireless communication nodes and a large number of devices deployed in an open environment, the energy of the nodes and devices, processing power and communication range are limited, each node in huge number of Internet of things may be destroyed, even though the decipher sensor communication protocol to manipulate them illegally; Internet of Things applications usually need to deploy a large number of sensors to achieve full coverage of a specific area. And for the already deployed sensors, it's usually not recycling or maintenance. Because of the large and one-time characteristics, the sensor must have a lower cost, so large-scale use is feasible. To reduce costs, the sensor is typically limited resources. The sensors generally smaller, its energy, processing power, storage space, transmission distance, the radio frequency and the bandwidth are limited. For example, the MIcA2MPR400cB is current mainstream sensor, its CPU frequency is 4M Hz, memory is 128KB, frequency of 916 Hz and only tens of KB of data transmission per second, the transmission distance is about 500 feet DI [3].

Due to the limitations of these reasons, the sensor node cannot use more complex security protocols, and thus these sensor node or device will not be able to have a strong security protection. Therefore, for this weakness of the sensor nodes, the attacker fired a large number of interfering signals, resulting in a large number of repeat visits to the request (Dos attack) will result in active labels run out of energy or gateway aggregation node is submerged and blocked, to plug the perception layer fail, make the perception layer failure; Attacker obtains identity, password information by analyzing the node, tampering with hardware and software, and then capture nodes, masquerading as a legitimate user and can carry out a variety of attacks; Due to the randomness, self-organizing, energy limitations and communication unreliability of nodes are deployed in the Internet of Things, leading to a lack of infrastructure. The topology dynamic changes which offer invaders the possibility to attack IOT through the virtual node, inserting false routing information. In order to offer wireless sensor networks confidentiality, integrity, authentication and other security features, it is a prerequisite to achieve a secure key management protocol, and also is the main problems of sensor network security research. Although key management protocol has been very mature application in the traditional network, however, there is a huge difference between wireless sensor networks and the traditional network in equipment resources and network organizations, which makes it necessary to combine these differences to reconsider the problem on wireless sensor the network key distribution.

Mitrokotsa *et al.,* analyzed attacks and threats of RFID system, and summarizes the corresponding solution from the physical layer, network transport layer, the application layer, the strategy layer four levels [4]. GILBERT think the security issues of the RFID system itself can be summarized as two aspects of privacy and authentication: The main problem is traceability in the privacy, that is how to prevent an attacker from any form of tracking RFID labels; In authentication, it should be ensured that only legitimate reader to be able to interact with the label [5]. At present, there are three major categories to protect the security of the RFID system itself [6]: physical methods (kill command [7], static shielding [8], The active interference and the Blocker Tag method [9] *etc.,*), security protocol (Hash lock, Hash chain, the challenge-response mechanism, re-encryption mechanism [10], *etc.,*), as well as the above-mentioned combination of methods. Rieback proposed the RFID Guardian method to protect privacy. RFID Guardian using a proxy to control the permissions that readers to access label, RFID Guardlan also provides audit, key management, access control, and authentication function [11]. N.w.Lo proposed a mutual authentication protocol based TTP (trusted third party) Server. TCP server releases the key to solve privacy issues as the authority [12].

2.3. Network Transmission of Information Security

The factors endanger the security of the information on Internet can also cause harm on the Internet of Things. Malicious intrusion of Things may result in violation of user privacy and user's actual loss. Cloud computing can collect the global hacker attacks node address, the host computer and other information, to share this information on the Internet, and global ASA firewall can real-time synchronous these libraries to prevent network attacks, Trojan infection and to achieve the implementation of IPS defense [13]. However, the original network communication technology is not fully adapted to IOT. The traditional network routing is fairly simple, and does not put safety on the main objectives. Since IOT nodes arranged as randomness, the self-group, energy constraints and communication unreliability, resulting in IOT has not infrastructure and topology is dynamics. Intruder can attack IOT through virtual nodes, inserting false routing information. The most commonly used routing protocol is SPIN, Flooding, LEACH, PEGASIS, etc. Flooding protocol is simple to be used, using flooding techniques, resulting in a lot of duplication of information and consume large amounts of energy [14]. LEACH protocol family changes will bring additional resource overhead, and single-hop routing networks is small-scale; PEGASIS protocol made improvements on LEACH [15], but the head of the chain will become a bottleneck; SPIN protocol uses a resource negotiation to adapt to changes in resources, but poor reliability is poor, and even some of the data cannot be forwarded [16]. As can be seen, these agreements have little or no safety issues to consider. Therefore, increasing or improving routing security mechanisms become a top priority. Secure routing to adapt to the dynamic and limited resources of IOT, we should consider routing security mainly from the following two ways [17]: First, using point to point encryption, routing and message authentication, intrusion detection and other ways to fight counterfeiting; second is the use of redundancy to provide multi-path routing to improve system error detection and fault tolerance.

IOT core network should have a relatively complete security protection, but due to the large number of nodes of IOT, there is a cluster arrangement, and therefore result in network congestion on data transmission due to the data transmission of large numbers of machines. Moreover, the existing communication network is a connection-oriented way of working, and the wide application of IOT must be addressed address space vacancies and network security standards and other issues [18]. Judging from the current situation to see, IOT to its core network requirements are far higher than the current capacity provided by IP network, especially in credible, knowable, manageable and controllable. In addition, existing communications network security architecture are made from the perspective of human communication and it is not entirely applicable to the communication between machines, using existing Internet security mechanisms will split IOT logical relationship between machines.

2.4. Privacy Protection

Information privacy is directly reflects for confidentiality of IOT information. Location information of perception terminal is an important information resource of things, and also is one of the sensitive information need to be protected. In addition, there are also privacy issues in data processing, such as behavior analysis based on data mining, *etc.*, [19]. To create access control mechanisms to control IOT in the information collection, transmission and query operations, and cannot result in damage to individuals or organizations because of personal privacy or disclosure of the organization secret. Privacy protection mainly involves the following questions:

1. Data Privacy Protection. The core to protect data privacy is confidentiality of the data itself. Wireless sensor network is a new, data-centric network, and data management is a based, critical important research in wireless sensor network. Data integration, aggregation, storage and other operations make the wireless sensor networks present a unique data privacy protection features based on data management.

2. Location Privacy Protection. Wireless sensor network is an application-specific and task-oriented network issues, and node ID information in general has little significance in wireless sensor networks. Instead, the node location information often played the role of identity, and location privacy has a special and crucial role in wireless sensor networks [20]. Developed in the traditional sense IP address as the center of privacy protection mechanisms are often unable to meet the characteristics of wireless sensor networks; so that the position privacy protection mechanism becomes the urgent needs of wireless sensor networks.

3. Identity Privacy Protection. This problem is particularly important raised in recent years, and are highly relevant to the production and life of human's new wireless sensor networks [21]. In home care, intelligent transportation and other fields, sensors and collected relevant information are often associated with the user entity, resulting in the user's identity leakage [22]. This is one of the key issues that must be addressed to achieve large-scale deployment of wireless sensor network applications.

For privacy protection technology, scholars have many studies. Privacy protection technologies currently focused on data dissemination, data mining, and wireless sensor networks and other areas. Literature [23] reviewed the privacy protection technologies from the data query privacy protection, privacy protection and data aggregation location privacy protection and other aspects of the wireless sensor network, and introduced routing protocols based on encryption technology and privacy protection technologies, in which routing protocol method is mainly used for location privacy protection. Literature [24] summarized privacy protection on the field of data publishing and data mining techniques, and divided them into data distortion based technology, data encryption based technologies and publish limitations technology, in which publish limitations technology is achieved mainly through anonymous technology. Literature [25] used improved k-anonymity algorithm to compute utility that quasi-identifier to sensitive attribute directly through the anonymous data, and meet the user's query services and effective protection of data privacy. Literature [26] proposed a method of data aggregation Privacy CDA, using holomorphic encryption method to make aggregation node can aggregate the encrypted data. Literature [27] used a holomorphic flow encryption algorithm based on additive, making the aggregation node can aggregate the encrypted data. Literature [28] proposed a sink node location privacy protection method that can against the global attack- DCARPS anonymous routing protocol, The protocol proposes a new network topology discovery method: Allowing sink node obtains global topology without leaking its position, and sink is responsible for all route calculation; another great feature of the protocol is to use the label switching method, sensor nodes perform simple label switching when forwarding packets.

2.5. Information Processing Security

Aggregation node and a large number of sensor nodes provide the information that have been monitored, perceived and collected. Internet has a relatively complete security protection, but a huge number of nodes in IOT exist in the way of the cluster, thus will lead to large amounts of data sent simultaneously, the network congestion, resulting in denial of service attacks. As diverse data formats of IOT collected in the perception layer, data from a variety of sensor nodes is massive and multi-source heterogeneous and it will bring more complex network security issues. Therefore, using a method of single node transferring data is obviously not suitable. In order to avoid wasting communication bandwidth and power, it is necessary that to process the source information and combine to meet the needs. At present, the studied for data aggregation heavily concentrates on conservation of resources, and little for security. For example, whether the data is being attacked or polluted is significant for some important occasions (such as military). Therefore, the node should verify the received data to avoid harmful data aggregating or uploading, and to achieve data integrity and reliability. A large and diverse IOT platform necessarily requires a strong and unified security management platform, or an independent platform would be overwhelmed by the applications of IOT, which makes how to manage machine security log of IOT become a new problem, and may split trust relationship between the network and service platform. Currently there are still many technical bottlenecks and difficult to break for massive data processing and operational control strategies of wide range IOT on security and reliability, especially the service control and management, business logic, middleware, business systems crucial interface, *etc*.

7. Conclusion

In summary, with the overall development of IOT, a variety of different wireless communication technologies and network structure are aggregating, and the communication network environment has become increasingly complex, the basic network security issues carried by all kinds of business are more complex and difficult to solve. IOT safety is huge system engineering, network security system is established after the communication system architecture, and a variety of complex heterogeneous communication system may have impact on the overall security issues due to its characteristics. So IOT within the trust relationship between the entities, front-end wireless access authentication and secure communications, security business and systems expansion have become an important research focus. IOT makes the interoperability between virtual world and the physical world not only related to information security, interoperability, but also includes important social functions, intellectual property protection, privacy on important national basic industries and social key services. If these security issues are not addressed, there will be a big risk on the application of IOT. Therefore, IOT security issues is bound to rise to the national level, and it is great significant to promote IOT security.

Acknowledgements

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

References

[1] G. Broll, E. Rukzio and M. Paolucci, “Perci: pervasive service interaction with the Internet of things”, Internet Computing, vol. 13, no. 6, **(2009)**, pp. 74-81.

[2] L. Atzori, A. Iera and G. Morabito, “The Internet of things: a survey”, Computer Networks, vol. 54, no. 15, **(2010)**, pp. 2787-2805.

[3] R. H. Weber, “Internet of Things-New security and privacy challenges”, Computer Law& Security Review, **(2010)**, vol. 26, no. 1, pp. 23-30.

[4] A. Mitrokotsa, M. R. Rieback and A. S. Tanenbaum, “Classfying RFID Attacks and Defenses”, Information Systems Frontiers Special Issue on RFID, **(2009)**.

[5] H. Gilbert, R. Matthew and H. Sibert, “An active attack against HB+: A provably secure lightweight authentication protocol”, IEEElectronics Letters, vol. 41, no. 21, **(2005)**, pp. 1169-1170.

[6] C. Floerkemeier, R. Schneider and M. Langheinrich, "Scanning with a purpose-supporting the fair information principles in RFID protocols", H. Murakami, H. Nakashima, H. Tokuda,and M. Yasumura, editors, International Symposium on Ubiquitous Computing Systems -UCS 2004, LNCS, Tokyo, Japan, Springer, Berlin, vol. 3598, **(2004)** November, pp. 214 231.

[7] S. Weis, S. Sarma, R. Rivest and D. Engels, "Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems", Proceedings of the First Security in Pervasive Computing, LNCS, vol. 2802, **(2004)**, pp. 201-212.

[8] Y. Dong and H. Chang, "An Energy Conserving Routing Algorithm for Wireless Sensor Networks", International Journal of Future Generation Communication and Networking, Washington, vol. 4, no. 1, **(2011)** March, pp. 39-54.

[9] T. Dimitriou, "A Lightweight RFID Protocol to Protect against Traceability and Cloning Attacks", Proceedings of the IEEE Int'l Conference on Security and Privacy for Emerging Areas in Communications Networks (SecureComm), **(2005)**.

[10] A. Juels and R. Pappu, "Squealing Euros: Privacy protection in RFID-enabled banknotes", Proc. Financial Cryptography, R.Wright, Ed. New York: pringer-Verlag, Lecture Notes in Computer Science, vol. 2742, **(2003)**, pp. 103-121.

[11] J. M. Riebaek and B. CrisPo, "RFID Guardian: A battery-Powered mobile device for RFID Privacy management", Australasian Conference on information Security and Privaey, ACISP2005, LNCS3574, **(2005)**, pp. 184-194.

[12] N. W. Lo and K. H. Yeh, "New mutual agreement Protocol to secure mobile RFID-enabled devices", Information Security Technical RePort, **(2008)**, vol.13, no. 3, pp. 151-157.

[13] A. Perrig, "SPINS: security protocols for sensor networks", Wireless Networks Journal (WINE), vol. 8, no. 5, **(2002)**, pp. 521-534.

[14] G. Indumathi and K. Murugesan, "A Cross-Layer Design to Improve Spectral Efficiency in Wireless Networks", International Journal of Future Generation Communication and Networking, Washington, vol. 4, no. 1, **(2011)** March, pp. 1-12.

[15] W. Du, "A key management scheme for wireless sensor networks using deployment knowledge", IEEE INFOCOM'04[C], Hong Kong, **(2004)**, pp. 7-11.

[16] D. Liu, "Location-based pairwise key establishments for relatively static sensor networks", ACM Workshop on Security of Ad hoc and Sensor Networks, VA, USA, **(2003)**, pp. 61-77.

[17] Z. Xu and Y. Yin, "A Density-based Energy-efficient Clustering Algorithm for Wireless Sensor Networks", International Journal of Future Generation Communication and Networking, Washington, vol. 6, no. 1, **(2012)** February, pp. 75-85.

[18] A. Perrig, R. Szewczyk and V. Wen, "SPINS: Security protocols for sensor networks", Wireless Networks, vol. 8, no. 5, **(2002)**, pp. 521-534.

[19] C. Blundo, A. D. Santis and A. Herzberg, "Perfectly secure key distribution for dynamic conferences", Proc 12th Annual Int'l Cryptology Conf on Advances in Cryptology, **(1992)**, pp. 471-486.

[20] D. Liu and P. Ning, "Establishing pairwise keys in distributed sensor networks", Proceedings of the 10th ACM Conference on Computer and Communication Security, **(2003)**, pp. 52-61.

[21] Y. Huang and S. P. Shieh, "Adaptive random key distribution schemes for wireless sensor networks", Proc of the Workshop on Advanced Developments in Software and Systems Security, **(2003)**.

[22] A. Perrig, D. Song and J. D. Tygar, "A new protocol for efficient large-group key distribution", Proc. IEEE Symp on Security and Privacy, **(2001)**.

[23] L. Na, Z. Nan and K. Das Sajal, "Privacy preservation in wireless sensor networks: A state-of-the-art survey", Ad Hoc Networks, vol. 7, no. 8, **(2009)**, pp. 1501-1514.

[24] R. L. Rivest, L. Adleman and M. L. Detrouzos, "On Data Banks and Privacy Homomorphism", Foundations of Secure Computation, New York: Academic Press, **(1978)**, pp. 169-179.

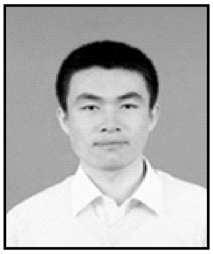
[25] J. Meyerowitz and R. R. Choudhury, "Hiding stars with fireworks: location privacy through camouflage", MobiCom '09 Proceedings of the 15th annual international conference on Mobile computing and networking, Beijing, 2009. New York, USA: ACM, **(2009)**, pp. 345-356.

[26] D. Westhoff, J. Girao and M. Acharya, "Concealed data aggregation for reverse multicast traffic in sensor networks: encryption, key distribution, and routing adaptations", IEEE Transactions on Mobile Computing, vol. 5, no. 10, **(2006)**, pp. 1417-1431.

[27] C. Castelluccia, C. Acf and E. Mykletun, "Efficient and provably secure aggregation of encrypted data in wireless sensor networks", ACM Transactions on Sensor Networks (TOSN), vol. 5, no. 3, **(2009)**, pp. 20:1-20:36.

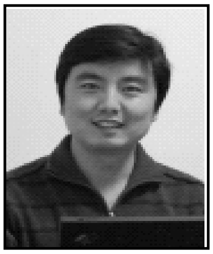
[28] A. A. Nezhad, A. Miri and D. Makrakis, "Location privacy and anonymity preserving routing for wireless sensor networks", Computer Networks, vol. 52, no. 18, **(2008)**, pp. 3433-3452.

Authors



Chen Qiang, his research fields include Image Coding, Image Compression, Wireless Sensor Network, Internet of Things Security Technology, etc. He has participated in many projects of Ministry of National Science, and he has published over 10 academic papers in journals and conferences both home and abroad.

Liu Yang, 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, he 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.