Wireless Netw
DOI 10.1007/s11276-014-0761-7

Security of the Internet of Things: perspectives and challenges

Qi Jing · Athanasios V. Vasilakos · Jiafu Wan · Jingwei Lu · Dechao Qiu

Abstract Internet of Things (IoT) is playing a more and more important role after its showing up, it covers from traditional equipment to general household objects such as WSNs and RFID. With the great potential of IoT, there come all kinds of challenges. This paper focuses on the security problems among all other challenges. As IoT is built on the basis of the Internet, security problems of the Internet will also show up in IoT. And as IoT contains three layers: perception layer, transportation layer and application layer, this paper will analyze the security problems of each layer separately and try to find new problems and solutions. This paper also analyzes the cross-layer heterogeneous integration issues and security issues in detail and discusses the security issues of IoT as a whole and tries to find solutions to them. In the end, this paper compares security issues between IoT and traditional network, and discusses opening security issues of IoT.

Keywords Internet of Things · Security · Heterogeneous · Wireless sensor networks · RFID sensor networks

1 Introduction

With the rapid development of Internet of Things (IoT), there are a variety of IoT applications, which contribute to our everyday life. They cover from traditional equipment to general household objects, which help make human being's life better. It is of great potential [1–4].

Meanwhile, a number of challenges are in the way of the IoT. In terms of scalability, IoT applications that require large numbers of devices are often difficult to implement because of the restrictions on time, memory, processing, and energy constraints. For example, calculation of daily temperature variations around all of the country may require millions of devices and result in unmanageable amount of data. And the deployed hardware in IoT often have different operating characteristics, such as sampling rates and error distributions, meanwhile sensors and actuators components of IoT are always very complex. All of these factors contribute to the formation of the heterogeneous network of IoT in which the data of IoT will be deep heterogeneous. Moreover, it is expensive to transmit huge volume of raw data in the complex and heterogeneous network, so IoT need data compression and data fusion to reduce the data volume. Consequently, standardization of data processing awareness for future IoT is highly desired. What is more, hackers, malicious software and virus in the communication process might disturb data and information

Q. Jing · J. Lu · D. Qiu
School of Software and Microelectronics, Peking University, Beijing, China

Q. Jing
Laboratory of Information Security, Institute of Information Engineering, CAS, Beijing, China

Q. Jing
Beijing Key Laboratory of IOT Information Security Technology, Institute of Information Engineering, CAS, Beijing, China

A. V. Vasilakos
Department of Computer Science, Kuwait University, Kuwait, Kuwait

J. Wan (✉)
School of Mechanical and Automotive Engineering, South China University of Technology, Guangzhou, China
e-mail: jiafuwan_76@163.com

Published online: 17 June 2014

integrity. With the development of IoT technology, information insecurity will directly threat the entire IoT system.

Nowadays, IoT is widely applied to social life applications such as smart grid, intelligent transportation, smart security, and smart home [5]. Access cards, bus cards and some other small applications also belong to IoT. Applications of IoT can bring convenience to people, but if it cannot ensure the security of personal privacy, private information may be leaked at any time. So the security of IoT cannot be ignored. Once the signal of IoT is stolen or interrupted, it will directly affect the security of the entire information of IoT. With the widely spreading of IoT, it will provide more extensive wealthy of information, the risk of exposure of such information will increase. If IoT cannot have a good solution for security issues, it will largely restrict its development. Thus, above all the problems of IoT, security problem is particularly important.

In this paper, we will firstly introduce our security architecture, divide IoT into layers, and sub layers, and we will extract major technical supports of each sub layer, propose security architecture to the problems of these technologies. Then we will introduce the key technologies of each layer, and propose solutions to special issues and common security and privacy issues. We also analyze cross-layer heterogeneous integration issues and security issues in details and discuss the security issues of IoT as indivisible entity and try to find solutions to them. In the end, we compare security issues between IoT and traditional network, and discuss some opening security issues of IoT.

2 Security architecture of IoT

IoT not only has the same security issues as sensor networks, mobile communications networks and the Internet, but also has its specialties such as privacy issues, different authentication and access control network configuration issues, information storage and management and so on. Data and privacy protection is one of the application challenges of IoT [3]. In IoT, RFID systems, WSNs sensors perceive for the end of the information technology, which protect the integrity and confidentiality of information by the password encryption technology [6–9]. There are many ways to encrypt data and information, such as random hash lock protocol (hash function), hash chain protocol, extract key from an infinite channel, Encrypted identifier and so on [10–13]. Identity authentication and access control can determine the communication between both sides and confirm each other's true identity, prevent disguised attacks to ensure the authenticity, validity of the information and so on [14–17]. There are two major security issues in the transmission process. One risk of the IoT security is from itself, and the other one comes from the related technology of construction and implementation of the network functions [14]. IoT itself is the integration of multiple heterogeneous network, it should deal with compatibility issues between different networks which is prone to security issues, for example, it is difficult to establish the junction of relationship as the relationship of trust between nodes that are constantly changing, but this can be solved by key management and routing protocols [18–20]. Security issues such as DOS/DDOS attacks, forgery/middle attack, heterogeneous network attacks, application risk of ipv6, WLAN application conflicts also affect the transport security of IoT [18, 21, 22]. In the core network, due to the large amount of data during the transmission, it is easy to cause network congestion. We should give full consideration to the capacity and connectivity issues, such as address space, reference network redundancy and security standards [23, 24]. The application security issues include information access and user authentication, information privacy, destroy and track of data stream, IoT platform stability, middleware security, management platform and so on [19, 20, 25–28]. The application of IoT directly connects with people's everyday life, to ensure the technology security, and to strengthen human security awareness and norms of human behavior at the same time. Meanwhile, people associated CPS (cyber-physical systems), and pervasive computing security has also been researched.

We will divide IoT into three layers: perception layer, transportation layer and application layer. In order to analyze the security issues of IoT in more detail, according to the data transmission in the IoT Phases, we divide perception layer into perception nodes and perception network, divide transportation layer into access network, core network, and LAN, and divide application layer into application support layer and IoT applications. Each layer has a corresponding technical support, these technologies at all levels play irreplaceable roles, but these techniques are more or less related to the existence of the range problems that can cause insecurity, privacy and other security issues of data. Security architecture of IoT is shown in Fig. 1.

IoT must ensure the security of all layers. In addition, IoT security should also include the security of whole system crossing the perception layer, transportation layer and application layer. Perception layer includes RFID security, WSNs security, RSN security and any others. Transportation layer includes access network security, core network security and local network security. There are 3G access network security, Ad-Hoc network security, WiFi security and so on for these sub layers. Different network transmission has different technology. Application layer includes application support layer and specific IoT applications. The security in support layer includes middleware

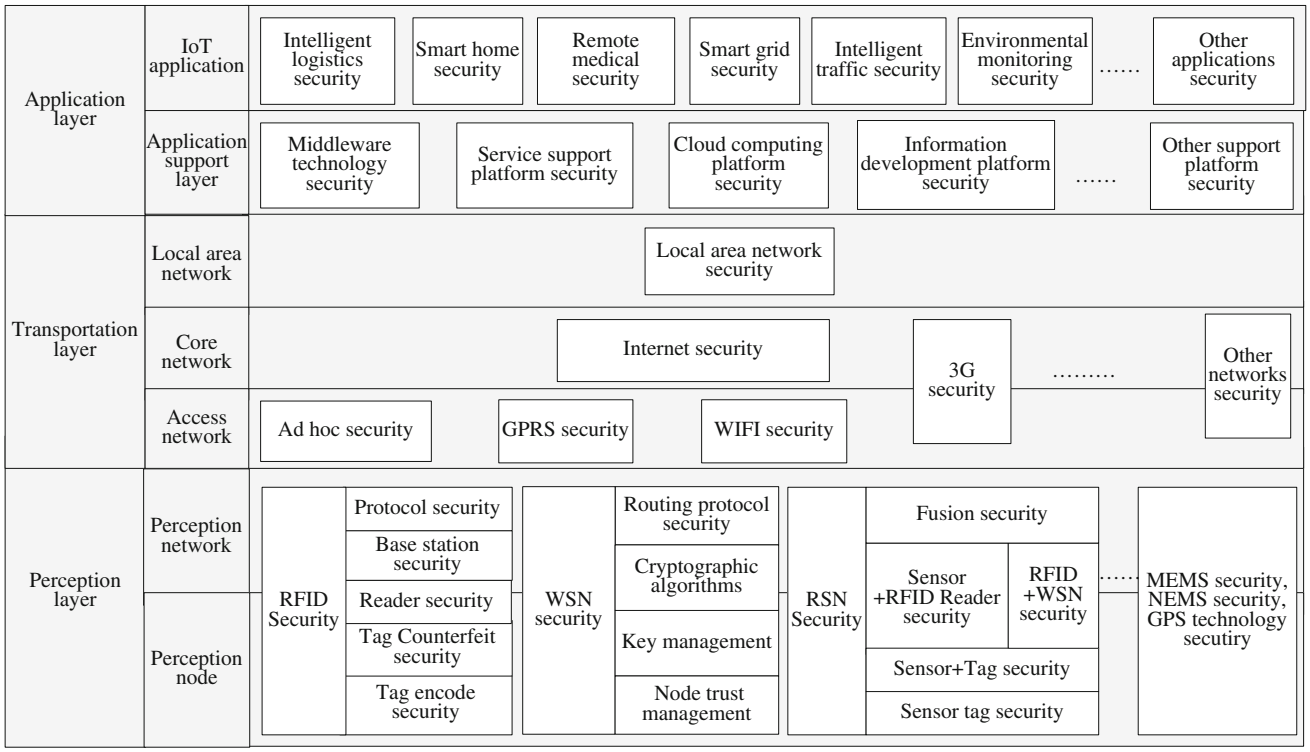

Fig. 1 Security architecture

technology security, cloud computing platform security and so on. IoT applications in different industries have different application requirements. Thus, networking security is a large multi-layered security system, in addition, considering security of each layers also consider cross-layer integration of heterogeneous network security issues (Table 1; Figs. 2, 3).

3 Security issues analysis of IoT

IoT does not have a standard architecture so far. According to the proposed architecture of ITU-T Y.2002, IoT is divided into three layers: perception layer, transportation layer, and application layer [29].

3.1 Perception layer

Perception layer is mainly about information collection, object perception and object control. Perception layer can be divided into two parts: perception node (sensors or controllers, etc.), perception network that communicates with transportation network. Perception node is used for data acquisition and data control, perception network sends collected data to the gateway or sends control instruction to the controller. Perception layer technologies include RFID, WSNs, RSN, GPS, etc.

This section mainly analyzes these technologies for the security issues of perception layer.

3.1.1 Security issues of RFID technology and solutions

RFID (Radio Frequency Identification) is a non-contact automatic identification technology, which can automatically identify the target tag signal to obtain relevant data, identifying the process does not require manual intervention, and can work in harsh environments [30]. While RFID is widely used, it exposes a lot of problems as follows.

3.1.1.1 Uniform coding Currently there is no uniform international encoding standard for RFID tag. The most influential standards are the UID (Universal Identification) standards supported by Japan and the EPC (Electronic Product Code) standard supported by European. As uniform standard has not yet formed, it may cause problems that the reader cannot obtain access to the tag information or errors may occur in the reading process.

3.1.1.2 Conflict collision As multiple RFID tags may also transmit data information to the reader at the same time, which may cause the reader not able to get data correctly [31]. Using the anti-collision technique can prevent multiple tags from transmitting information to the reader simultaneously.

Table 1 Issues and solutions to the security of IoT

Layers	Features and issues	Technologies		Solutions	Details
Perception layer	Various kinds of sensor devices	Uniform encoding for RFID tag		Uniform encoding	UID supported by Japan and EPC supported by European
	Multiple tags in one reader's working scope	Conflict collision prevention in RFID	Tags' collision	Anti-collision algorithm	Slot ALOHA, improved slot ALOHA, GBT, PGT, etc
			Readers' collision	Scope-based solutions	Avoids overlap of reader working scope
				Time-based solutions	Prevents readers from sending signals simultaneously
	Limited resources (storage capacity and weak computational capabilities), easy tag cracking	Privacy protection in RFID		Physical-based schemes	Deactivation kill command, block tags, clip tags, pseudonyms tags, Faraday nets, signal interference, and antenna energy analysis
				Password-based schemes	Hash locks, random hash lock, hash chain, anonymous ID, re-encryption
				Compromising solution	Store less important information in RFID tag, and store important information in the up level service
	Short password based security mechanisms, easily forgery tag and tag replication, eavesdropping and retransmission	Trust Management in RFID		RFID-CoA	Unique "RFID-fingerprint" for the RFID tag, cheap hardware technology
				RFID security protocol	RFID private authentication protocol, RWP, AFMAP, ultralight weight RFID mutual authentication protocol, etc
				Digital signature technology	Low-cost GPS digital signature system — Tag replication prevention, data authentication
					Lightweight authentication protocol — Efficient data protection
	Data security with limited computing power and storage space	Cryptographic algorithms in WSNs		Symmetric encryption	Inconvenient digital signatures, message authentication, RC4, IDEA, RC5, TinySec
				Public-key encryption	Rabin's scheme, NtruEncrypt, elliptic curve cryptography, etc
	Key distribution, including the distribution of the public key and the secret key, is to ensure key to be transported and distributed securely to legitimate users	Key management in WSN		Key broadcast distribution	Security communications between nodes in the same group
				Group key distribution	Secure communications between nodes in the same group
				Distribution of node master key	Saved into the node before deployment in the form of pre-distribution
				Distribution of the key shared between nodes	Communication between any pair of nodes protection, security communications between adjacent nodes
				Symmetric key algorithms	SPINS, the famous random pre-distribution key scheme, q-composite, Pre-distribution matrix key scheme
				Group key distribution	Public key distribution problems, the issue of using of public key algorithms to assign other keys, abbreviated certificate, implicit certificate, etc
	Limitation of power, computing ability and storage capacity Attacks towards routing protocol	Secure routing protocol in WSN		Secure routing protocols designed specifically for WSN	Authentication protocols should discuss and verify the security of themselves in detail and should take energy management issues of wireless sensor network into consideration carefully
	Limited resources, easy capture of nodes, and unique communication mode	Trust management in WSN		Measurement, evaluation, relationship formalization, formal derivation of trust	Update of trust, cooperation of all nodes, tradeoff between limited resources and network security
	Differences of storage formats, information access formats, and security control mechanisms, data processing methods and data filtering aggregation	Heterogeneous integration technology		WSNs solutions	Random-intensive distributed low-cost static sensor nodes
				RFID solutions	Heterogeneous integration technologies
				WSN in IoT solutions	Multi-hop, intelligent RFID reader/tag, potential privacy exposure, compatibility issues, unified data encoding standard and item information exchange protocol

Table 1 continued

Layers	Features and issues	Technologies	Solutions	Details
Transportation layer				
Access network	WIFI: Phishing site, access attacks, malicious AP and DDos/Dos, etc	Access control and network encryption technologies	Access control	WPA, encryption, authentication technology, etc
			Network encryption	TKIP and AES
	Ad hoc: data security, network routing security, DDos/Dos issue	Encryption mechanisms, authentication and key management, Ad hoc network routing protocol	Ad hoc network routing protocol, authorization protocol	Ad hoc network routing protocol, authorization protocol, key management
	3G network: data security, unlawful attacks, etc	Symmetric encryption, asymmetric encryption and digest algorithm	Key management, data origin authentication and data encryption	Information transmission security
Core network	Large numbers of nodes to access the Internet	6LowPAN technology	6LowPAN	Use ipv6 to provide IP, low power consumption for heterogeneous integration
LAN	Data security issues	Network access control	Network access control	Illegally usage of network resources
The entire layer	Common attacks: Information disclosure, network paralysis, etc	Heterogeneous fusion technology	Heterogeneous fusion	Tight coupling, loose coupling, ACENET, AN net, etc
		Attack detection and prevention technologies	Attack detection and prevention	System update, DDos attack detection and prevention methods
Application layer	Invalid or insecure data	Middleware, service support platform, cloud computing, information development platform, etc	Data security protection	Data isolation/recovery: database management, backup management, etc
	Access control problem		Access control protocols	User management, user authentication, network authentication, information privacy
	Long-term service viability		Service contract management	Contract management
	Service interruption, illegal intervention, equipment lost and DDOS attack, etc		Supervision capability: enhance management	Information disclosure protection, disaster control and recovery, supervision
	Ubiquitous industry, life, environment intelligence	Intelligent logistics, smart home, remote medical, Smart grid, intelligent traffic, etc	Environmental monitoring	Access control, user authorization, privacy protection, platform monitoring, etc

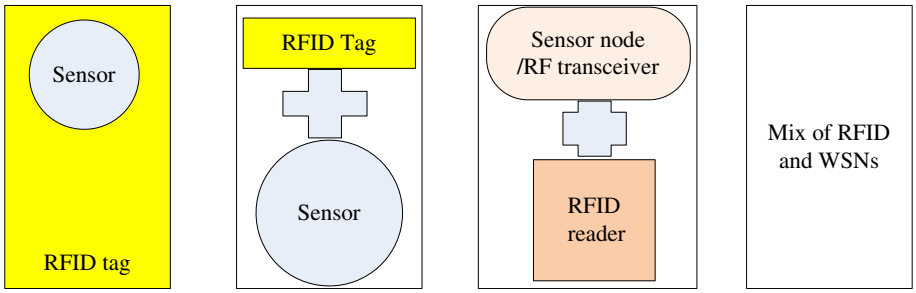

Fig. 2 Four kinds of integration methods

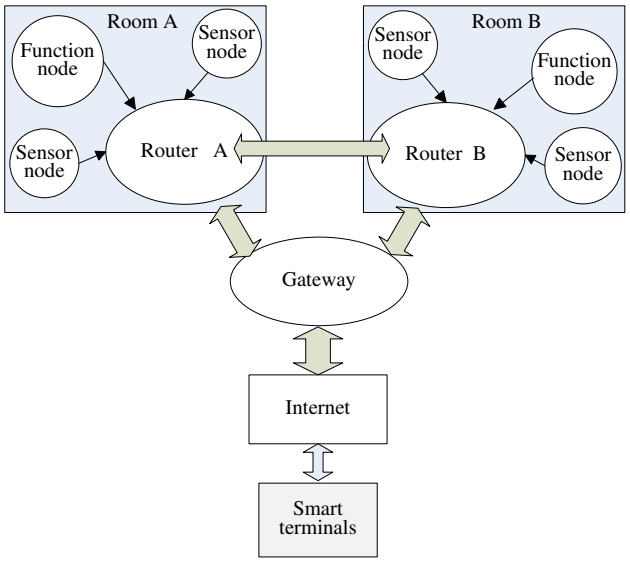

Fig. 3 Smart home architecture

RFID conflict collision can be divided into two categories: tags' collision and readers' collision [32]. When a large number of labels are in the reader's working scope, and the reader cannot access to data correctly, this is called tags' collision. IoT requires wide range of RFID sensor coverage, and multiple readers' cooperative work is particularly important, but the working scope of reader overlaps. So information may become redundant which increases the burden on the transmission of network. This is called readers' collision.

Different collisions have different solutions. Currently, tag anti-collision algorithm has been studied adequately, but research for reader anti-collision algorithm is not enough. Reader anti-collision algorithm is mainly divided into solutions based on the scope-based and time-base solutions [33, 34]. The main idea of the scope-based anti-collision algorithm is to try to avoid overlapping of reader work scope to achieve the purpose of reducing the conflict zone, but this solution requires an additional central control area to calculate the working scope between the readers, which increases the complexity and cost [35].

3.1.1.3 RFID privacy protection Low cost tags led to RFID's limited resources, such as low storage capacity and weak computational capabilities, thus it requires light-weight solutions for privacy protection, which includes data privacy and location privacy.

Data Privacy: RFID security and privacy technologies can be divided into two categories: physical-based schemes and password-based schemes, the former sends deactivation kill command [36], block tags [36, 37], clip tags, pseudonyms tags [38], Faraday nets, signal interference [39], antenna energy analysis [40] etc. The later includes schemes such as hash locks [41], random hash lock [42], hash chain [43], anonymous ID [44], re-encryption [45]. Different organization styles for IoT require different ways of privacy protection agreement. For example, T2TIT architecture of the French national research agency uses HIP [46, 47] protocol to solve the data privacy issues. A compromise solution for data privacy issues is to store less important information in RFID tag, and store important information in the up level service.

Location privacy: Although RFID tags do not store important information, but hackers can still get the tag ID information for the purpose of tracking the position of the tag [48]. For example, when a reader equipped with vehicle GNSS information reads a tag's information, it can easily obtain the approximate location information of the tag according to its effective operational range.

3.1.1.4 Trust management In IoT, we must take node privacy more seriously. So we need to introduce trust management into IoT RFID system. Trust management exists not only just between the readers and RFID tags, but also between the readers and the base stations.

In trust management field, digital signature technology is of great usage. It has been used for data authentication, device authentication and data exchange between different applications for a long time. Cryptographic algorithms and protocols play important roles for digital signature technology. While standard cryptographic algorithms and protocols require storage space and computing resources

more than the available resources of RFID tags, so RFID authentication algorithm must not only take into account security and privacy issues, but also consider the tag storage and computing power. Complexity of security and limited resources of RFID tags would be the focus of ongoing research.

Above all, uniform encoding, conflict collision, privacy protection and trust management are four typical technologies for the security issues of RFID. With uniform encoding standard, we encode tag information uniformly, which can maximize information exchange. With a good conflict collision resolution technology, we can make RFID readers read information correctly, and minimize potential data interference. With a good lightweight data privacy protection, we have helped protect data privacy and location privacy. Finally, with appropriate trust management algorithms, we can enable trust management for readers/RFID tags, readers, and base stations.

3.1.2 Security issues and technical solutions in WSNs

WSNs are self-organizing networks with dynamic network topology, and widely distributed multi-hop wireless networks. Take cost into consideration, WSNs have limited resources including small amount of storage, poor calculation ability, narrow sensing range, which leads to a series of network security risks. One target of perception layer is to implement fully aware the environment. Limited scope of a single node makes network structure complex with a large number of sensing nodes. Perception layer is for collecting information, it is data oriented. So for WSNs research we will focus on data analysis. In the process of collecting data, the message may be subject to eavesdropping, malicious routing, message tampering and other security issues, which affect the security of the entire IoT. Data security issues can be summarized into data confidentiality, data authenticity, data integrity, and data freshness. These four types of security issues can be solved in four aspects: cryptographic algorithms, key management, secure routing, node trust.

3.1.2.1 Cryptographic algorithms in WSNs The main application areas of wireless sensor network are wide which demands high data security, including data confidentiality and data integrity, which can be solved by data encryption [49]. Cryptographic algorithm is a very important method to ensure the physical layer network security, and is the basic for ensuring security of the entire network service.

Data encryption algorithm is divided into two categories: symmetric encryption algorithm and public-key encryption algorithms. Because computing power and storage space of sensor nodes are both limited, asymmetric encryption algorithm's computational complexity and energy consumption makes it difficult to be applied to wireless sensor networks. Symmetric encryption algorithm is widely used in wireless sensor networks because of its simple calculation and small amount of calculation.

Symmetric encryption algorithms have the following problems: (1) the key exchange protocol based on the symmetric cryptosystem is too complex that symmetric encryption algorithm for wireless sensor networks has poor scalability. (2) Confidentiality problem of key [50]. In WSNs, nodes are in unattended environment. Once a node is compromised, it will cause huge security threat to the entire network; and (3) Inconvenient digital signatures and message authentication [50]. In a symmetric encryption algorithm, the message authentication code is usually used for authentication, which increases the communication load, and requires more storage space, causing extra power consumption.

Based on the above issues, people began to consider applying public-key encryption algorithm into wireless sensor network. Each node holds its own private key and base station's public key. While base stations are saving the public key of all nodes. Public key algorithm has good scalability, without complicated key management protocol. It is convenient for node authentication, and can better ensure the security of the entire network [51].

At present, there are three public key encryption algorithms suitable for wireless sensor networks: Rabin's Scheme, NtruEncrypt and Elliptic Curve Cryptography. These three algorithms have been validated on Mica2 series wireless sensor platform, demonstrating that only if there is a well-designed algorithm, by selecting the appropriate parameters to optimize the design, public key encryption algorithm can be used in wireless sensor networks which has limited energy and computing power [50–55].

In order to overcome difficulties of applying public key algorithm into WSNs, there are mainly two research aspects to overcome this. In terms of hardware, we can design customized, low power co-processor to complete most computing work of encryption algorithms. In terms of software, we can use well-designed algorithms and appropriate parameters to reduce the amount of computation.

In conclusion, both symmetric encryption and asymmetric encryption have its own advantages, but still cannot completely solve wireless sensor network security issues. In wireless sensor network applications, symmetric encryption algorithm technology is relatively mature, but security strength is not very high. Asymmetric encryption algorithms can provide high strength security, but current research is just in experimental stage. How to use asymmetric encryption algorithm technology in WSN is a key issue that the underlying security facilities need to be taken into consideration. Energy consumption caused by public

key encryption algorithms and security protocols communication should be the main consideration of future research.

3.1.2.2 Key management in WSNs Key management is a key issue waiting to be solved for the security of wireless sensor network. It is also one of the basic premises to address other security issues. Key management includes secret key generation, distribution, storage, updating and destruction process, where key distribution is the most important issue in key management. Key distribution, including the distribution of the public key and the secret key, is to ensure key to be transported and distributed securely to legitimate users. How to design a lightweight secret key distribution scheme on the basis of the sensor nodes with limited resources, to support all levels of protocols, applications and services security is the main problem in the field.

According to keys' role, WSNs key distribution scheme can be divided into four forms. (1) Key broadcast distribution in the entire network [56–60]: The key is used to protect the security of station broadcasting information to all nodes. Broadcast keys could use public or private ones as needed. As energy consumption of the former in the entire network is too large, symmetric key distribution is commonly used in this scenario. The allocation of broadcast key is to solve the problem of key updates. (2) Group key distribution [61–63]: For some reason, the sensor network generates an internal network group consisting of several nodes. Group key is used to secure communications between nodes in the same group. Group key can be seen as broadcast key of group members. (3) Distribution of node master key: Node master key is the key shared between the node and the base station, which is often saved into the node before deployment in the form of pre-distribution. (4) Distribution of the key shared between nodes [64–68]: The key shared between nodes refers to the key shared between a pair of nodes. It is used for protecting the communication between any pair of nodes. Because of energy-consumption and other factors, key shared between nodes are mainly used to solve security problem in communications between adjacent nodes, to achieve security connectivity of whole network, or security communication rate reaching a threshold. Research in this area is sufficient with quantities of achievements.

For a long time, because of the high energy- consumption of the public key, wireless sensor network key distribution scheme has been designed with symmetric key algorithms, such as centralized key distribution scheme SPINS [65], the famous random pre-distribution key scheme [69], q-composite and a serial of other schemes proposed on the base of random pre-distribution key [60, 68]. The latter is based on the random graph theory, so we can only guarantee the security of the whole network connectivity at a high probability. "Pre-distribution matrix key scheme" [60, 68] ensure the security of the entire network connectivity in form of matrix. Although the key distribution schemes discussed above, based on symmetric key algorithm, have been carefully designed based on the characteristics of sensor networks, but because of the characteristics that symmetric key algorithms has make it not suitable for making key distribution, these key distribution schemes take a lot of energy in complex communication process. Due to recent further in-depth research in sensor hardware acceleration and software optimization [70, 71], key distribution based on public-key algorithm once again attracted public attention. Research in this area can be divided into two categories: public key distribution problems and the use of public key algorithms to assign other keys. As traditional schemes using public key certificate distribution has many drawbacks in sensor networks, so abbreviated certificate [57], implicit certificate [72] and the other certificate management solutions are proposed to reduce energy consumption.

Researches combining public key and symmetric key algorithm, making use of both of their advantages to achieve key distribution scheme has also started [73]. In short, the current key management research direction is to reduce the complexity of key distribution frameworks designed based on the symmetric key algorithm and to further reduce power consumption to improve their usability, and design a specific comprehensive key distribution scheme for wireless sensor networks according to practical contexts, so that various types of key distribution schemes could be combined in specific application contexts.

3.1.2.3 Secure routing protocols for WSNs Network layer routing technology plays a key role in wireless sensor network. Attacks towards routing protocol will lead directly to the collapse of the network. Therefore, the setup of secure and effective routing protocol has always been the focus of research in wireless sensor network [74]. Since the limitation of power, computing ability and storage capacity, traditional network routing protocols cannot be applied in wireless sensor network, even routing protocols commonly studied in the Ad hoc network encounter new problem in WSNs. There are plenty of important differences between Ad hoc networks and wireless sensor network.

On the basis of research on platform cryptographic algorithms and key management issues, network layer data security and integrity can be guaranteed. But the authentication of routing information must be with the help of designing secure routing protocols. Different from traditional end-to-end authentication scheme (such as SSH and SSL), data integration features in sensor network require

that the certification must be made between nodes. So far, research in this area can be divided into the following two categories:

1. Secure routing protocols designed specifically for wireless sensor network [75]. These authentication protocols should discuss and verify the security of them in detail, and take energy management issues of wireless sensor network into consideration carefully to get better results in practical applications.
2. Analysis of potential vulnerabilities of routing protocols. The paper "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures" summarized security routing issues of wireless routing network [74], and analyze the security flaws of existing protocols (such as Wormhole attack, Sinkhole attacks, DoS attacks, etc.), and proposed a number of corresponding solutions according to attacks. The main idea of this research is to study the vulnerability of routing protocols from the attacker's point of view [76–79] and design appropriate solutions against these potential attacks.

Although these studies have their own advantages, they still can't completely solve the security problems of routing protocols. Works based on Ad hoc network protocols always tend to be more complete in the details of the agreement, but can't achieve satisfactory results when it comes to energy aspect. Secure routing protocols designed completely for wireless sensor networks usually simplify some problems, like assuming some premises that may lead to new vulnerabilities. Although it is a great idea to study potential security vulnerabilities of security protocols, but it cannot solve problems of protocol design.

3.1.2.4 Trust management of nodes in WSNs WSN has many special characteristics, such as the limited resources of sensor nodes, easy capture of nodes, and unique communication mode (sensor nodes gather information and report to the base station), etc. These characteristics made sensor network more vulnerable to various attacks. However, it cannot guarantee the security of wireless sensor networks by only relying on password mechanisms and cryptographic algorithms. We need to introduce trust management mechanism to ensure the security of wireless sensor networks.

The concept of trust management can be traced back to 1996 [80]. M. Blaze and others proposed it to solve service security issues of open network. So far, researches on trust management are divided into four sections: trust measurement mechanism, trust evaluation mechanism, trust relationship formalization, and formal derivation of trust. Another important aspect in trust management is the update of trust, which is even more severe in dynamic network. "The effect of rumor for mobile ad-hoc networks" [81, 82] is studied calculation of trust degree based on the interaction between hop neighbors.

It is particularly necessary to introduce trust management mechanisms into sensor networks. First, sensor network relies on cooperation of all nodes to collect effect data. The fragility of a single node makes it easy to be malicious captured thus providing fake or erroneous information result in broken of cooperation between nodes, and finally return false or error data to final users. Therefore, the credibility of a single node is the key to ensure the offer of effective network service delivery. Secondly, cryptographic mechanism like SPIN [65], TINYSec [74] can only provide verification of data consistency and validity, but cannot guarantee data authentication.

Trust management need to give it specific consideration based on the characteristics of wireless sensor network. For example, energy consumption is a critical issue in sensor networks. Trust management system must be able to make the tradeoff between limited resources and network security [61, 83]. "A Security Framework with Trust Management for Sensor Networks" specifically discussed trust management problems in the context of wireless sensor networks and proposed some trust management frameworks and mechanisms to it.

Above all, lightweight cryptographic algorithms, key management, secure routing protocol and trust management of nodes are four typical technologies for the security issues of WSNs. We need good lightweight cryptographic algorithms to fulfill the high data security requirement. Key management is a key issue waiting to be solved for the security of WSNs, as it is also the basis for the security of other IoT components. As attacks toward routing protocol will directly leads to the collapse of WSNs, we need to setup secure and effective routing protocols. Finally in order to ensure the security of the entire wireless sensor network, we need effective trust management solutions to enable the security in the network.

3.1.3 The problems of heterogeneous integration

RSN (RFID sensor network) is widely used in the Internet of Things, which is the integration of RFID and WSNs [62]. We can use RSN technology to solve the problem caused by heterogeneous data.

In IoT, there is a large number of widely distributed data needs to be collected. However, data collected in different ways or different protocols is always of different formats. We cannot analyze these data effectively without data unification, and the data will be destroyed, lost, compromising if we cannot get the right integration technology, if nodes are monitored, captured, information would be stolen, resulting in privacy exposure. Security issues in

information integration field occupy a very important position. One of the most important challenges of data integration is the problem caused by heterogeneous data, because WSNs and RFID may use two different protocols, which leads to compatibility issues between data formats, communication protocols. So we need unified data encoding standard and item information exchange protocol for RFID and WSNs in the context of IoT. RFID and WSNs require close collaboration in software level for the integration in the system–level. However, RFID and WSNs have different storage formats, different information access formats, and different security control mechanisms. Because of different data formats and different application directions, RFID and WSNs have different data processing methods for data filtering, aggregation and other data processing, so we need to do research for information access format, data storage format, data processing methods and mechanisms of security control. There are four common integration methods (see Fig. 2): tag integrated with sensor node, tag integrated with wireless sensor node, readers integrated with wireless sensor node and the wireless device, combination of RFID and sensor node [84].

In the IoT environment, RSN face a large number of nodes. For different nodes, the calculation capabilities, transmission capacity, power consumption, and storage resource are different. And sensor networks are often deployed in open environment, and after deployment, it will not be concerned during long period of time. So they may receive physical attacks. In the perception layer, the main constraints are: low data rate, small packet (affecting security protocols to achieve the required additional information transmission), limited capacity (8-bit or 16-bit processor architecture, 8 MHz clock frequency), limited energy resources (battery).

In the perception of the Transportation layer, unreliable transmission collisions in the wireless connection will lead to unreliable transport. Due to the lack of central infrastructure, network density results from large number of sensors are unreliable. Reliable transport has been the focus of our study. The key technologies, key management, certification authority with WSNs and RFID technology are basically the same.

There are still many problems that cannot be effectively resolved. For example, how to support the new node added based on key pre-distribution method; how to store and allocate key; how to achieve lower energy consumption for encryption; how to take advantage of the characteristics of sensor networks, automatic defense security Technology; fault zone automatic discovery technology and network auto-recovery mechanisms; invasion model and intrusion detection methods; against malicious routing information mechanisms; energy efficient lightweight secure routing protocols; RFID sensor network for secure data integration agreements; RFID sensor network privacy protection mechanisms; RFID sensor network trust management mechanisms.

The complexity of the sensor nodes on the Internet of Things is a big challenge [85], firstly, the number of sensor network and terminal equipment associated with IoT cannot be compared by single sensor network; secondly, for the terminal equipment connected to the Internet of Things or device, the processing capacity will have great differences, they may interact with each other. The limited capacity of single-node and multi-node network vulnerability, heterogeneous and complex perception layer caused major problems. In view of the overall structure of the complexity of IoT, even if we ensure the security of perception layer, we cannot guarantee the security of the Internet of Things. This is because several layers of IoT are melt in one large system integration. We will continue to talk about security issues about network transport layer in depth.

3.2 Transportation layer

Transportation layer mainly provides ubiquitous access environment for perception layer, perception of information transmission and storage, and application layer load other related businesses [86]. Transportation layer can be divided into three layers by function: the access network, the core network and local area. It is a combination of a variety of heterogeneous networks. This paper analyzes the Transportation layer security issues by the functional structure of transportation layer, and discusses the issues and solutions by integration of heterogeneous integration.

3.2.1 Functional architecture of the transportation layer of security issues

3.2.1.1 Access network Access network provides ubiquitous access environment for perception layer, the perception layer and the core network will have security issues when the perception layer accesses the core network. Access Network includes wireless networks, Ad hoc network, etc.

According to the differences of the structure of network, wireless networks can be divided into center network and non-center network. In the center network, the communication between the mobile nodes must use fixed bridge (or known as a base station), such as the common cellular networks and wireless local area network. In the non-center network, the communication between need not fixed base station [87]. WiFi is a center network and Ad hoc is a non-center network.

- WiFi security issues analysis

WiFi stands for Wireless Fidelity. It is a wireless network access specification, also known as IEEE802.11, which is currently the most widely used wireless networking standards, refers that the wireless terminal can be connected to each other by wireless technology. WiFi-based applications in IoT include access the Internet via WiFi web, access e-mail, download or watch online video, etc.

Network security is a concern in WiFi. When users access the Internet web page, it is possible to encounter phishing site [88, 89], users' account and password will be compromised. In short, WiFi security risks mainly include two aspects: one is from the network trap; the other is from the network attack. WiFi security issues are access attacks, malicious phishing AP, and DDos/Dos attacks.

In order to solve the security issues of WiFi, access control and network encryption are available. Access control refers that only authorized users can access the WiFi network. Network encryption means that only the recipient who can decrypt correctly can understand the data content. Access control and network encryption technologies include WPA, encryption, authentication technology, etc. WPA technology is a wireless network based on application protocols, WPA provide data protection for the authorized users to access the Internet network resources. Users who have not been authorized can't access the data. Currently the encryption methods of the network are TKIP and AES. Authentication methods of WiFi to access the Internet can guarantee the security of user access to the data. The main certifications are PPPoE authentication, Web authentication, and wireless access authentication, etc.

- Ad hoc security issues analysis

Wireless Ad hoc network is a group of autonomous wireless nodes or terminals cooperated and formed, independent of the fixed infrastructure which use of distributed network management, is a self-creating, self-organization and self-management network [90, 91].

In the IoT, Ad hoc network is a peer-to-peer non-center network, which can eliminate heterogeneous between the perception layer nodes by Ad hoc network routing protocol [91–94]. To a certain extent, if the network nodes change, it is able to adapt to these changes, coordinate inter-node dynamically and perception layer network communication in the core network and will not affect the operation of the entire network. Security threats of traditional Ad hoc network are from the radio channel and networks. Wireless channel is vulnerable to eavesdropping and interference. In addition, non-center and self-organizing networks suffer from vulnerable posing, cheating and other forms of attack. In IoT, Ad hoc networks still have the following security issues:

Illegal node access security issues: each node needs to be able to confirm the identity of other nodes that communicate with the node, otherwise, an attacker can easily capture a node, thus allowing access to critical resources and information, and to interfere with other communication nodes. Authorization and authentication can address this security issue. Certification proves that the identity of the node is legitimate, and then the authorization decides whether this capacity is allowed to do certain things.

Data security issues: Wireless Ad hoc network communication is undirected, sensory data transmitted over the network is easy to leak or malicious users tampering, network routing information is also susceptible to malicious user identification, and thus illegal to get the exact location of the target. Authentication and key management mechanism can solve this security issue [87].

Network routing security, such as DDos/Dos, can be addressed with encryption mechanisms.

- 3G network security issues analysis

When used as an access network, 3G networks have the following security problems: user information leakage, data incompleteness, unlawful attacks and other security issues. Confidential information by the user, the key management mechanism, data origin authentication and data encryption can solve the corresponding secure issues, but the current security mechanisms are still in the research stage [95–99]. In the process of data transfer, it exists following issues: data leakage, illegal node access and unlawful attacks. Through the appropriate security key management mechanisms, behavioral entity authentication can resolve these issues [96].

Through a comparative analysis on the 3G network access and security problems encountered in the core network, the emphasis of the security issues in the 3G network is different. In the access network, 3G network need to be more concerned about the security issues of certification, and its solution is bellows [96]: the password information and lawful intelligent terminal node hardware information (SIM card number or terminal network address) are stored on the server side; when smart terminal access the server, it can provide password; mobile operators provide hardware information to the server; comparing the server-side and the terminal, it can verify the legitimacy and authority of the mobile terminal to determine the control sensor networks. In the core network, 3G network concerns about the security of information transmission, including data confidentiality, integrity, reliability and authenticity. The main means of implementation are symmetric encryption, asymmetric encryption and digest algorithm technology.

Whether in the access network or in the core network, 3G networks have common problems: DDos/Dos attacks, phishing attacks and identity attacks. We don't have good

solutions to solve the DDos/Dos attacks, but we can take behavioral entity authentication and other methods to solve the identity phishing attacks.

3.2.1.2 Core network Core network of IoT is mainly responsible for the data transmission. The core network is mainly Internet. The following is analysis of security issues on the Internet.

Since a large number of nodes need to access to the Internet, which requires a lot of IP addresses, the traditional IPv4-based Internet is unable to meet so many sensor nodes, so the next generation Internet based on IPv6 can solve this problem. In order to use IPv6 sensor networks with low power consumption for heterogeneous integration, we can take 6Lowpan technology to solve the problem of IPv6 addresses.

6LowPAN [100–106] technology adopts PHY layer and MAC layer of IEEE802.15.4, and transportation layer uses the IPv6 protocol. As in IPv6, MAC payload length supported by the underlying can provide much greater than 6LowPAN payload length, in order to achieve the MAC layer and transportation layer seamless connectivity, 6LowPAN Working Group recommends that the transportation layer and MAC layer are added between network adaptation lays, which used to complete the header compression, fragmentation and reassembly, and mesh routing forwarding work.

Adaptation layer is an intermediate layer between IPv6 network and IEEE 802.15.4MAC layer. It makes IPv6 support for IEEE 802.15.4 medium access and the control LoWPAN network construction, topology and MAC layer routing for the MAC layer. The basic functions of 6LoWPAN include the link layer fragmentation and reassembly, header compression, multicast support, network topology construction and address assignments.

3.2.1.3 Local area network In IoT, local area network should take data leakage and server's independent protection security issues more seriously. To adopt the following measures, we can strengthen security management in the local area network [107].

Network access control is to ensure the network resources being used legally, which is the main strategy of network security protection. Others, such as denial of malicious code, closing or deleting unnecessary system services, and constantly updating the operating system patches, using a secure password and the password can be used to protect the security of local area network of IoT.

3.2.2 Common issues of transportation layer analysis

3.2.2.1 Heterogeneous network convergence issues of transportation layer analysis The Transportation layer of IoT is made of a variety of heterogeneous networks (such as Ad hoc network, the Internet, 3G networks, etc.), so there are security issues of heterogeneous fusion [108, 109]. In order to solve the security issues of heterogeneous integration, networking has taken the following four ways: tight coupling, loose coupling, ACENET, AN net, etc.

3.2.2.2 Attacks issues of transportation layer analysis DDos attack [110] is the most common network attacks, especially in the IoT. Because of the heterogeneity and complexity of IoT network, the transportation layer is vulnerable to get attacked. Usually the solution is to upgrade the system and use DDos attack detection and prevention. Currently there is no good solution to solve the network DDos attack.

The transportation layer of IoT is also vulnerable to Trojan horses, viruses, spam and other attacks resulting in information disclosure, network paralysis, others such as middle attacks, replay attacks, access attacks, and phishing sites attacks [88, 89] and combo attacks. Although attacks are very common issues, using the necessary intrusion detection mechanisms and authentication mechanisms can prevent detection timely [86].

In this layer, we mainly focus on security issues for the access network, core network, and local area network. In access network, we analyzed security issues for WIFI, Ad hoc and 3G-network, and their corresponding solution technologies. In core network, we analyzed the security issue of massive number of nodes and introduced 6LowPAN technology. In local area network, we analyzed network access control technology to solve the security issue of illegally network resources usage. We also analyzed some common security issues of the entire transportation layer such as illegally information disclosure, network paralysis, etc. As transportation layer is in the middle of the IoT system, it is of great importance.

3.3 Application layer

3.3.1 Security issues of application support layer

The application support layer, an advanced layer above the transportation layer, supports all sorts of business services and realizes intelligent computation and resources allocation in screening, selecting, producing and processing data. During the whole process, the application support layer can recognize valid data, spam data and even malicious data, and filter them in time. Application support layer can be organized in different ways according to different services. Usually it includes middleware, M2 M, cloud computing platform and service support platform.

In IoT, the middleware is developed on certain core technology, such as traditional middleware servers as

communication component, allow the software to be deployed on different platforms or operation systems. However data in IoT is massive and dynamic, thus middleware of IoT must have huge capacity and can be linearly expanded to store increasing data [111]. The encapsulated function inside middleware of IoT is more complex, such as the controlling of ambient temperature and maintaining of ambient state. It needs to process correlative requests sent from devices in different places simultaneously. These requests form a context, which will last a period of time. Different contexts can perform different functions and provide different services to users. When there are several requests at the same time, it is fair and good to process them according to their arrived time. However IoT involves daily life issues, event issues, or even disaster issues. Those more emergent issues need higher priority of services. The system needs to recognize the emergency degree of these issues and entrust them with corresponding priorities.

M2 M, one of the most popular application models of IoT nowadays, still cannot avoid security risk since the data transferring is based on electric cable, wireless network or mobile network. The security problems that M2 M faces in the application level can be divided into three aspects as follows.

Applications composed by backend terminal system and middleware need to satisfy high security requirements, so as to collect and analyze data immediately and increase the business processing intelligence. Security management of source code and IoT needs also to be satisfied with high standard. Other security issues contain access control, privacy protect, user authorization, data integrity, real-time availability, etc. Meanwhile, privacy and reliability are the most concerned issues of IoT. Recently, most researches begin to pay attention to technologies of protecting privacy, these technologies contain k-anonymity [110], data conversion, data randomization, using terminals with SIM module bounded to IMEI and IMSI, developing interlocking management cards and machines and sending updated key authentication and M2 M platform certification to prevent piracy of cards and machines, ensuring secure code resources. Security risks rise up when personnel changes happen to service operation administrators. There are threats of inappropriate authentication of M2 M users. The data exchange between operators can lead to trade information disclosure and economic losses. So the government should take appropriate legislation to regulate the behavior of operators taking advantage of signing when switching carriers to reduce the risk.

Moreover, operators should provide special process to shift keys and other user information when switching carriers, in order to ensure the security of user information.

Cloud computation platform faces several major security challenges including risk of priority process, risk of management agencies, risk of data premise, risk of data isolation, risk of data recovery, risk of investigation support and risk of long-term development [112].

3.3.1.1 Security threats According to a survey by IDC, security issue is the most concerned aspect in cloud computation. All the respondents have technical security concerns. In fact, the cloud computation platform will encrypt the data and back up users' data that will not be deleted until a certain period of time. So be sure to carry out risk estimation and come up with contingency plans before putting the data into the cloud end.

Cloud computation involves certain key information of enterprises, thus leads enterprises and individuals becoming the targets of hackers. Though it may not be a common problem, security event is possible to happen. Due to the security issue, enterprises sensitive to data such as medical enterprises and financial enterprises are not recommended to adopt cloud computation technology.

3.3.1.2 Service interruption and attack issue According to the past experience of cloud computation service, there are always some common service interruptions happening, including data backup, system shutting down and data center offline. Luckily these failures can be predicted.

There is also DDOS attack beside the service interruption. DDOS attack refers to a kind of attack that can prevent normal users from visiting cloud services, making some critical cloud services consume a lot of system resources such as processes, memory, disk space and network bandwidth, which leads the response of cloud server become extremely slow or completely unresponsive.

3.3.1.3 Investigate audit issues In cloud computation, computation, storage, network bandwidth services can be accesses globally, but account information provided by the users can be counterfeit. Moreover different countries and regions have different requirements on obtaining evidence of illegal behaviors, therefore the network crimes based on the cloud-computing platform are hard to trace. Tracing crimes can be more difficult when the resources of the platform come from varied multi-level third-party vendors.

Enterprises will face various unknown risks if they hastily adopt cloud computing without thorough understanding of the cloud service provider environment, IoT applications, and operation responsibilities (such as responsibilities for the accident, encryption issues, security monitoring).

3.3.2 Security issues of IoT applications

The application layer involves integrated or individual specific application business. The security issues it faces

cannot be solved in other layers of IoT, such as privacy protection issue, which does not occur in perception layer and transportation layer, but can become the real demand in certain special contexts of application layer, or can be also called special security demand of application layer [85].

Certain special contexts of IoT, such as positioning, have the security problem of privacy including location privacy and query privacy. The location here refers to the past or present location of a user, while the query privacy refers to query and mining of sensitive information. If a user often searches the restaurants or hospitals in a certain area, this query records can be taken by some unruly elements to analyze the user's residence location, income, lifestyle, behaviors, heath status and other sensitive information, causing disclosure of personal information. Current protection of privacy includes location camouflage, anonymous space, space encryption, etc. [19].

The applications of IoT are widely applied to social life applications, such as smart grid, intelligent transportation, smart security, smart home and so on [113].

3.3.2.1 Intelligent transportation IoT is widely used in the logistics industry. Information technology, integrated logistics management and process monitoring can not only improve the efficiency of logistics enterprises and help control logistics cost, but also improve information level of the enterprise. Implementation of intelligent logistics system includes receiving, transfer, sorting, sending, transportation and other associated subsystems. Each subsystem achieves inventory management, goods delivery, automated billing and other business functions.

RFID technology has real-time, fast, and accurate features. On the way of objects transported, RFID reader use GPS system through GSM/CDMA network to provide object's current position to the data center. Making the logistics process can help track the information flow and capital flows in real time, and make each business aspects more coordinated and efficient.

But RFID systems are the same as the Internet, so it will get viruses and hacker attacks. The main reason is the chip loading no security module or loading an inadequate protection module due to cost, which leaves convenient channel for hackers to crack the code to get information [114]. In intelligent logistics, the most serious data security risk of RFID system is information leakage. The so-called information leakage refers to leaking information that tag sends. Electronic label may contain internal information or personal privacy information, such as the production batch number, personal identity and shopping habits. If the tag is stolen, the internal information or personal privacy information will get leaked. To prevent data theft, we can use two ways: (1) data encryption; and (2) do not store sensitive data with electronic tags, only store ID information that has no special significance. Critical data scattered in various servers [115].

In addition, in the logistics industry, it is a core issue to ensure the security of goods. The phenomenon of express lost often emerges in major holidays. In this case, the problem of the express's security becomes more and more important. For the problem of items' real-time information feedback, it is hard to find a good solution for a range of security issues items [116]. ZigBee technology is characterized by: low-rate, low power, low cost, self-configuration and flexible network topology. So, it can be used for real-time feedback on the items of information [117].

Each link node relies on RFID reader to identify the information that carried by RFID label. The module of serial communications sends the electronic label information, GPS information and other node's information out through GPRS. By ZigBee protocol architecture, SPI interface connect GPS, GPRS, RFID and other communication module with a data processing unit MCU, which can make the logistics system have positioning, anti-theft anti lost alarm functions. In this way, it can help track express mitigate people's concern psychologically and can greatly reduce system power consumption, making the wireless sensor network platform industrialization possible [116].

3.3.2.2 Smart home Under the tide Internet of Things, Intelligent home industry has broad prospects in China and around the world, and contains a huge potential market [118].

The new intelligent home system [118, 119] consist of sensors, Internet and intelligent control, it can provide people an efficient, comfortable, secure, convenient, environmentally friendly living environment. In the United States, Gates' "Future House" must be a classic intelligent home [120]. All the lighting, music, temperature, humidity can be adjusted by computer according to the guests' needs. Start with the opening of the door, visitors will receive a built-in microchip brooch with which they can pre-set their preferences temperature, humidity, lighting, music, paintings and other conditions, no matter where they go, built-in sensors on these data will be transmitted to a central computer with Windows NT system, it will adjust the environment automatically. When the guests come, the sensor in floor will open illuminated automatically, and turn off when the guests leave [120]. The mainly applied technology of intelligent home system includes network control technology, communications technology and mobile terminal technology [120].

Intelligent home system based on IoT in accordance with the three-tier structure can be summarized as shown in Fig. 3. Setting the sensor nodes and function nodes in each room of the family, environment change captured by the

sensor nodes, the data is passed to the gateway via the route aggregation. Some changes will touch response program designed in advance. And the functional nodes react directly. If we need people to make decisions, then we can notify the gateway to intelligent terminals via the Internet, people came to see the information if you want to take steps, you can issue the command and returns to the home gateway routing node to respond by functional nodes. For example, when the host is not at home, a stranger come, the sensor will pass information to intelligent terminals such as mobile phones. The host of the house receives a notice outside, if he wants to grab the stranger he can give the system a directive, such as "Close all windows and doors", function control node receives instruction and corresponding function hardware execute instruction.

The mainly applied technology of intelligent home system includes network control technology, communications technology and mobile terminal technology [120].

- Network Control Technology

There are EIB, C-Bus, H-Bus, LonWorks, SCS, RS-485 which connected with the interconnect bus of home gateway. Because of the complex arrangement of wired lines, the original cause will bring various damages to the building and maintenance. Expansion will also bring a lot of limitations. So the way of wireless including the RF, carrier, Wi-Fi, ZigBee, Bluetooth and so on.

- Communications Technology

Communications technology is divided into wired communication and wireless communication technologies, most of them have matured, such as ZigBee-based wireless network technology for smart home system. Due to low cost, low power, versatility and farther coverage features, intelligent home systems will become another highlight.

- Mobile Terminal Technology

For Mobile intelligent terminals such as smart phones, tablet PCs, notebooks. The main security issues include privacy-aware layer of theft, illegal eavesdropping and so on. For some hardware devices, indoor and outdoor environment and human impact will be security issues. DDOS attacks at the network layer technologies such attacks during transmission of 3G also bring some security issues.

The application layer security is application specific. Its security issues cannot be solved in other layers of IoT. With different IoT applications, there come different security issues. In this layer, we analyzed security issues of the application support layer, including security threats, service interruption and attack issues, and investigate audit issues. Then, we analyzed security issues of IoT applications and introduced several typical IoT applications such as Intelligent Transportation and Smart Home. And we also analyze their corresponding security issues and technologies.

3.4 Security of IoT as a whole

As IoT is getting more and more popular, there are lots of security issues needing considered as a whole system. The security requirement for IoT cannot be achieved by simply putting the solutions from each sub layers together.

There are different kinds of IoT applications such as: Intelligent Transportation, Smart Home, Intelligent Urban Management, Intelligent Medical, Smart Green, and Smart Grid. For different applications we have different security requirements. For example, the security of data privacy would be of great importance for Intelligent Transportation and Intelligent Medical. But to Intelligent Urban Management and Smart Green, data authenticity would be more important. In order to get the best security, we may need to give them different weight from different applications.

As we know, some security needs cannot be fulfilled by only using one specific technology in a single layer. For example, for a system with weak application layer, no matter how much effort we have done for data privacy security in perception layer, it would be easy for a cracker to get all private data. So in this situation, we need to have some cooperation between different layers. Thus we need to design corresponding technologies for cross layers usage.

We not only should deal with single-layer heterogeneous issues, but also need to deal with cross-layer heterogeneous integration issues. We need to find out new technologies to build system autonomy and heterogeneous integration model to meet the cross-layer requirement, so that we can get uniform data across different layers. Thus for large-scale heterogeneous network, we can use cross-layer heterogeneous technology to build IoT systems with large-scale heterogeneous network. In Table 1, we give the issues and solutions to the security of IoT.

4 Security issues comparison between IoT and traditional network

As we can tell from the issues and solutions to the security of IoT mentioned above, IoT and traditional network security issues are different in many ways as follows.

IoT is composed of RFID nodes and WSN nodes, whose resources are limited, while the Internet is composed of PC, severs, smart phones whose resources are rich. So in the Internet, we can use combinations of complex algorithms and lightweight algorithms to maximize security with less considerations of resource usage such as computation power. While in IoT, most of the cases, we can only use

lightweight algorithms to find the balance between security and power consumptions.

As stated above, the connection between IoT nodes are always through slower, less secure wireless media, which results in easy data leakage, easily node compromising and all other insecure issues. While in the Internet, most communications are through faster, more secure wire or wireless communications. Even with the Mobile Internet, the wireless connections are built on top of complex secure protocols which are almost impossible to implement for resource limited IoT nodes.

Although there are various devices in the Internet, but with the abstraction of operating system, their data formats are almost the same with Window Family and Unix-like operating systems. However, in IoT, what we have is just bare wireless node. There is no operating system, just a simple embedded program for the chip. With the diversity of nodes perception goal, there comes different chip hardware which result in heterogeneous data contents and data formats.

As stated in application layer, there are all kinds of IoT applications. These applications are used in our everyday life, and they gather our private information every second automatically to make our life easier. With IoT, these applications can even control our everyday life environment. It would be of great potential security problems if we lose control of IoT system. While in the Internet, if we do not provide our information ourselves, there is no way for attackers to get our information. And with the help of operating system and plenty of security software, the environment is more secure.

So in one word, IoT system lives in a more dangerous environment with limited resources and less network guards. So we need to implement lightweight solutions to deal with this more dangerous environment.

5 Open security issues of IoT

In IoT, we are more concerned about the security of the entire system, rather than just the security of a single piece of software or a single IoT layer. What we need to do is to treat the entire IoT system as an integrated entity and figure out how to build integrated cross-layer security solution, how to deal with the heterogeneous security architectures of IoT and how to securely fuse the heterogeneous data generated by different sources.

5.1 Overall security architecture for the entire IoT system

As IoT security issues are application specific, so are their solutions. With different application contexts and different security requirements, we can provide different security architectures to solve the corresponding security issues. This means IoT security architectures are customizable that we may not be able to make a single framework handle all cases. However we can borrow some ideas from software engineering, in which we can abstract the similarities among these IoT applications. And then we design the abstract security architecture on which we provides all the basic security solutions to common IoT applications. In the meantime, the top-level security architecture provides security adapters with which different applications can provide application specific algorithms to exchange data with existing top level security algorithms. We can also use the strategy pattern from the 23 design patterns for software engineering in which the top level architecture provides the interface to different strategies and the application specific system implements these interface. In this way we can abstract the differences between different IoT applications.

5.2 Lightweight security solutions

According to the specific characteristics of IoT, lightweight solutions would always be our future research direction. So we have to study lightweight solutions for IoT system such as key management, access authentication, access control and so on. We also need to make sure these lightweight solutions meet the specific requirements of our specific application. We can divide the application computation requirements and security requirements into several levels. Different level implies different computation complexity requirement and different security requirements. And in each level we provide some default solutions, which fulfill the specific requirements of the corresponding levels. In the way, we can characterize the algorithms that have been proposed into one of these levels. In this way we might be able to provide a overall abstract IoT security framework.

5.3 Efficient solutions for massive heterogeneous data

In addition, IoT system generates massive heterogeneous data every minute, so it is also one of our mainly exploration direction to find an efficient way to deal with these massive data generated by IoT system. We need to provide secure protocols to efficiently handle and organize all these mass information so that we can finally obtain a more comprehensive security solution for the entire application-related IoT system. This is similar to the Internet, which right now enters the age of big data. However the heterogeneity of IoT data makes it quite different from the Internet. So it might be a good idea to take a peek at the solutions of the Internet for big data and apply them to IoT system.

6 Conclusions

In this survey, we have been focused on the security architecture and security issues of IoT, and have divided IoT into three layers: perception layer, transportation layer and application layer. We analyzed the features and security issues of each layer, and introduced the corresponding typical solutions for these issues. In the meantime, we also compared the features of these different solutions by analyzing the technology involved. For perception layer, WSNs and RFID technology is of great importance, we analyzed the security issues of RFID technologies and their corresponding solutions including: Uniform Coding, Conflict Collision, RFID Privacy Protection, Trust Management, then we analyzed security issues and technical solutions in WSNs including: Cryptographic Algorithms in WSNs, Key Management in WSNs, Secure Routing Protocols for WSNs, Trust Management of Nodes in WSNs. After analysis of RFID and WSNs, we analyzed the new challenges for the RSN, which is the integration of RFID and WSNs. As IoT system needs to handle massive heterogeneous data from different sources, we also analyzed cross-layer heterogeneous integration issues and security issues in detail. Transportation layer is consists of access network, core network, and local area network. In access network, we analyzed security issues for WiFi, Ad hoc and 3G-network, and their corresponding solution technologies. In local area network, we analyzed network access control technology to solve the security issue of illegally network resources usage. We also analyzed its functional architecture of security issues and common security issues in detail. The application layer is consists of application support layer and IoT application layer. We have discussed security issues of application support layer such as security threats, service interruption and attack issue, and investigate audit issues. As application layer security is application related, so its security issues cannot be solved in other IoT layers. So we have introduced some typical IoT applications such as Intelligent Transportation and Smart Home, and analyzed their corresponding security issues and related technologies such as network control technology, communications technology and mobile terminal technology.

In the end, we compared security issues between IoT and traditional network, and concluded that IoT system lives in a more dangerous environment with limited resources and less network guards, thus lightweight solutions would always be our first choices for IoT security. We also discussed opening security issues of IoT as an indivisible entity, and give some potential directions for these issues: overall security architecture for the entire IoT system, lightweight security solutions and efficient solutions for massive heterogeneous data.

Acknowledgments The work was supported in part by the National Natural Science Foundation of China (No. 61100066, 61262013), the Open Fund of Guangdong Province Key Laboratory of Precision Equipment and Manufacturing Technology (No. PEMT1303), the National High Technology Research and Development Program of China (No. 2013AA014002), the Innovation Base Cultivating and Developing Engineering Program, Beijing Scientific and Technological Commission (No. Z131101002813085), and the "Strategic Priority Research Program" of the Chinese Academy of Sciences (No. XDA06040100).

References

1. Tsai, C., Lai, C., & Vasilakos, V. (2014). Future internet of things: Open issues and challenges. *ACM/Springer Wireless Networks,*. doi:10.1007/s11276-014-0731-0.
2. Wan, J., Yan, H., Suo, H., & Li, F. (2011). Advances in cyber-physical systems research. *KSII Transactions on Internet and Information Systems, 5*(11), 1891–1908.
3. International Telecommunication Union. (2005). *Internet reports 2005: The internet of things*. Geneva: ITU.
4. Hachem, S., Teixeira, T., & Issarny, V. (2011). *Ontologies for the internet of things* (pp. 1–6). New York: ACM.
5. Sundmaeker, H., Guillemin, P., Friess, P., & Woelfflé, S. (2010). *Vision and challenges for realising the internet of things. Cluster of European Research Projects on the Internet of Things—CERP IoT*.
6. Akyildiz, I. F., Su, W., Sanakarasubramaniam, Y., & Cayirci, E. (2002). Wireless sensor networks: A survey. *Computer Networks, 38*(4), 393–422.
7. Hamad, F., Smalov, L., & James, A. (2009). Energy-aware security in M-Commerce and the internet of things. *IETE TechmeM review, 26*(5), 357–362.
8. Tsudik, G. (2006). YA-TRAP: Yet another trivial RFID authentication protocol. In *Proceedings of fourth annual IEEE international conference on pervasive computing and communications workshops* (pp. 196–200).
9. Mathur, S., Trappe, W., Mandayam, N., Ye, C., & Reznik, A. (2008) Radio-telepathy: Extracting a secret key from an unauthenticated wireless channel. In *Proceedings of MobiCom* (pp. 128–139).
10. Montenegro, G., & Castelluccia, C. (2004). Crypto-based identifiers (CBIDs): Concepts and applications. *ACM Transactions on Information and System Security, 7*(1), 97–127.
11. Xu, X. H. (2013). Study on security problems and key technologies of the internet of things. In *Proceedings of the IEEE international conference on computing and information sciences (ICCIS)* (pp. 407–410).
12. Ouafi, K., & Vaudenay, S. (2009). Pathchecker: An RFID Application for tracing products in suply-chains. In *Proceedings of the workshop on RFID Security–RFIDSec* (vol. 9, pp. 1–14).
13. Blass, E. O., Elkhiyaoui, K., & Molva, R. (2011). Tracker: security and privacy for RFID based supply chains. In *Proceeding of the 18th network and distributed system security symposium*.
14. Elkhiyaoui, K., Blass, E. O., & Molva, R. (2012). CHECKER: On-site checking in RFID-based supply chains. In *Proceedings of the fifth ACM conference on security and privacy in wireless and mobile networks*.
15. Chen, M., Kwon, T., Mao, S., & Leung, V. (2009). Spatial–temporal relation-based energy-efficient reliable routing protocol in wireless sensor networks. *International Journal of Sensor Networks, 5*(3), 129–141.

16. Suo, H., Wan, J., Zou, C., & Liu, J. (2012). Security in the internet of things: a review. In *Proceedings of the IEEE international conference on computer science and electronics engineering (ICCSEE)*, (vol. 3, pp. 648–651).
17. Ye, T., Peng, Q. M., & Ru, Z. H. (2012). *IoT's perception layer, network layer and application layer security analysis.* http://www.iot-online.com/jishuwenku/2012/1029/22888.html. Accessed 12 Oct 2013.
18. Liu, B., Chen, H., Wang, H. T., & Fu, Y. (2012). Security analysis and security model research on IoT. *Computer & Digital Engineering, 40*(11), 21–24.
19. Suo, H., Liu, Z., Wan, J., & Zhou, K. (2013). Security and privacy in mobile cloud computing. In *Proceedings of the 9th IEEE international wireless communications and mobile computing conference* (pp. 655–659), Cagliari, Italy.
20. Wan, J., Chen, M., Xia, F., Li, D., & Zhou, K. (2013). From machine-to-machine communications towards cyber-physical systems. *Computer Science and Information Systems, 10*(3), 1105–1128.
21. De Turck, F., Vanhastel, S., Volckaert, B., & Demeester, P. (2002). A generic middleware-based platform for scalable cluster computing. *Future Generation Computer Systems, 18*(4), 549–560.
22. Tan, Y. S., & Han, J. J. (2011). Service-oriented middleware model for internet of things. *Computer Science, 38*(BIO), 3.
23. ITU-T. Recommendation Y. 2002. (2010). *Overview of ubiquitous networking and of its support in NGN.* Geneva: ITU.
24. Want, R. (2006). An introduction to RFID technology. *IEEE Pervasive Computing, 5*(1), 25–33.
25. Yang, G., Xu, J., Chen, W., Qi, Z. H., & Wang, H. Y. (2010). Security characteristic and technology in the internet of things. *Journal of Nanjing University of Posts and Telecommunications (Natural science), 4*, 20–29.
26. Wan, J., Zou, C., Ullah, S., Lai, C., Zhou, M., & Wang, X. (2013). Cloud-enabled wireless body area networks for pervasive healthcare. *IEEE Network, 27*(5), 56–61.
27. EPC Global. *(2004). EPC radio-frequency identity protocol Class-1 Generation-2 UHF RFID protocols for communications at 800 MHz-960 MHz*, Ver. 1.0.9, EPC Global.
28. Wan, J., Zhang, D., Sun, Y., Lin, K., Zou, C., & Cai, H. (2014). VCMIA: A novel architecture for integrating vehicular cyber-physical systems and mobile cloud computing. *ACM/Springer Mobile Networks and Applications, 19*(2), 153–160.
29. Liu, L. A., & Lai, S. L. (2006). ALOHA-based anti-collision algorithms used in RFID system. In *Proceedings of the IEEE international conference on networking and mobile computing* (pp. 1–4).
30. Hu, F., & Wang, F. (2010). Study of recent development about privacy and security of the internet of things. In *Proceedings of the international conference on web information systems and mining* (pp. 91–95).
31. Lv, B. Y., Pan, J. X., Ma, Q., & Xiao, Z. H. (2008). Research progress and application of RFID anti-collision algorithm. In *Proceedings of the international conference on telecommunication engineering* (vo1. 48, no. 7, pp. 124–128).
32. Finkenzeller, K. (2003). *RFID handbook fundamentals and applications in contactless smart cards and identification* (2nd ed.). West Sussex: Wiley.
33. Wang, D., Wang, J. W., & Zhao, Y. P. (2006). A novel solution to the reader collision problem in RFID system. In *Proceeding of the IEEE wireless communications, networking and mobile computing (WiCOM 06)* (pp. 1–4).
34. Song, I. C., Hong, S. H., & Chang, K. H. (2009). An improved reader anti-collision algorithm based on pulse protocol with slot occupied probability in dense reader mode. In *Proceeding of the IEEE 69th vehicular technology conference* (pp. 1–5).
35. Kim, J., Lee, W., Yu, J., Myung, J., Kim, E., & Lee, C. (2005). Effect of localized optimal clustering for reader anti-collision in RFID networks: Fairness aspects to the readers. In *Proceeding of the IEEE international conference on computer communications and networks* (pp. 497–502).
36. Weis, S. A., Sarma, S. E., Rivest, R. L., & Engels, D. W. (2004). Security and privacy aspects of low-cost radio frequency identification systems. *Security in Pervasive Computing, 2802*, 201–212.
37. Blaskiewicz, P., Klonowski, M., Majcher, K., & Syga, P. (2013). Blocker-type method for protecting customers' privacy in RFID systems. In *Proceedings of the IEEE international conference on cyber-enabled distributed computing and knowledge discovery (CyberC)* (pp. 89–96).
38. Chen, M., Gonzalez, S., Zhang, Q., & Leung, V. (2010). Code-centric RFID system based on software agent intelligence. *IEEE Intelligent Systems, 25*(2), 12–19.
39. Spiekermann, S., & Berthold, O. (2005). *Maintaining privacy in RFID enabled environments. Privacy, security and trust within the context of pervasive computing* (pp. 137–146). Berlin: Springer.
40. Castelluccia, C., & Avoine, G. (2006). *Noisy tags: A pretty good key exchange protocol for RFID tags. Smart Card Research and Advanced Applications* (pp. 289–299). Berlin: Springer.
41. Juels, A., Rivest, R. L., & Szydlo, M. (2003). The blocker tag: Selective blocking of RFID tags for consumer privacy. In *Proceedings of the 10th ACM conference on computer and communications security (CCS 2003),* (pp. 103–111).
42. Ohkubo, M., Suzuki, K., & Kinoshita, S. (2003). *Cryptographic approach to privacy- friendly tags. RFID privacy workshop* (p. 82). Cambridge, MA: MIT.
43. Kinos, S., Hoshino, F., Komuro, T., Fujimura, A., & Ohkubo, M. (2003). Nonidentifiable anonymous—ID scheme for RFID privacy protection. *Computer Security Symposium.*
44. Duels, A., Pappu, R., & Euros, S. (2003). Privacy protection RFID-enabled banknotes. In *Proceedings of seventh international financial cryptography conference* (pp. 103–121).
45. T2TIT Research Group. (2006). *The T2TIT—Thing to thing in the internet of things-project*. ANR.
46. T2TIT project. (May 2010). http://www.infres.enst.fr/wp/blog/2009/11/20/t2titthings-to-things-in-the-internet-of-things-sesames-award-2009/. Accessed 12 Oct 2013.
47. Toumi, K., Ayari, M., Saidane, L., A., Bouet, M., & Pujolle, G. (2010). HAT: HIP address translation protocol for hybrid RFID/IP internet of things communication. *TUNISIA: International conference on wireless and ubiquitous systems* (pp. 1–7).
48. Lakafosis, V., Traille, A., & Lee, H. (2011). RFID-CoA: The RFID tags as certificates of authenticity. In *Proceedings of the IEEE international conference on RFID* (pp. 207–214).
49. Karlof, C., Sastry, N., & Wagner, D. (2004). TinySec: A link layer security architecture for wireless sensor networks. *In Proceedings of the second ACM conference on embedded networked sensor systems* (pp. 162–175).
50. Chen, M., Lai, C., & Wang, H. (2011). Mobile multimedia sensor networks: Architecture and routing. *EURASIP Journal on Wireless Communications and Networking, 2011*(1), 1–9.
51. Han, K., Luo, J., Liu, Y., & Vasilakos, V. (2013). Algorithm design for data communications in duty-cycled wireless sensor networks: A survey. *IEEE Communications Magazine, 51*(7), 107–113.
52. Malan, D. J., Welsh, M., & Smith, M. D. (2004). A public-key infrastructure for key distribution in tinyOS based on elliptic curve cryptography. In *Proceedings of the IEEE international*

conference on sensor and ad hoc communications and networks SECON04 (pp. 71–80).
53. Li, M., Li, Z., & Vasilakos, V. (2013). A survey on topology control in wireless sensor networks: Taxonomy, comparative study, and open issues. *Proceedings of the IEEE, 101*(12), 2538–2557.
54. Bohge, M., & Trappe, W. (2003). An authentication framework for hierarchical Ad Hoc sensor networks. In *Proceedings of the 2nd ACM workshop on wireless security* (pp. 79–87).
55. Zhu, S., Setia, S., & Jajodia, S. (2003). LEAP: efficient security mechanisms for large-scale distributed sensor networks. In *Proceeding of ACM CCS* (pp. 62–72).
56. Hu, Y. C., Johnson, D. B., & Perrig, A. (2003). SEAD: Secure efficient distance vector routing for mobile wireless Ad Hoc networks. *Ad Hoc Networks, 1*(1), 175–192.
57. Sengupta, S., Das, S., Nasir, M., Vasilakos, V., & Pedrycz, W. (2012). An evolutionary multiobjective sleep-scheduling scheme for differentiated coverage in wireless sensor networks. *IEEE Transactions on Systems, Man, and Cybernetics, Part C, 42*(6), 1093–1102.
58. Huang, C. H., & Du, D. Z. (2005). New constructions on broadcast encryption and key pre-distribution schemes. *IEEE INFOCOM, 1*, 515–523.
59. Wander, A. S., Gura, N., Eberle, H., Gupta, V., & Shantz, S. C. (2005). Energy analysis of public-key cryptography for wireless sensor networks. In *Proceedings of the IEEE international conference on pervasive computing and communications* (pp. 324–328).
60. Chan, H., Perrig, A., & Song, D. (2003). Random key predistribution schemes for sensor networks. In *Proceeding of the IEEE symposium on security and privacy* (pp. 197–213).
61. Al-Turjman, F. M., Al-Fagih, A. E., Alsalih, W. M., & Hassanein, H. S. (2013). A delay-tolerant framework for integrated RSNs in IoT. *Computer Communications, 36*(9), 998–1010.
62. Ren, F. Y., Huang, H. N., & Lin, C. (2003). Wireless sensor networks. *Journal of Software, 7*, 1282–1290.
63. Liu, H., Bolic, M., Nayak, A., & Stojmenovic, I. (2008). Taxonomy and challenges of the integration of RFID and wireless sensor networks. *IEEE Network, 22*(6), 26–35.
64. Chan, H. W., & Perrig, A. (2005). PIKE: Peer intermediaries for key establishment in sensor networks. In *IEEE Infocom 2005* (vol. 1, pp. 524–535).
65. Eschenauer, L., & Gligor, V. D. (2002). A key-management scheme for distributed sensor networks. In *Proceedings of the 9th ACM conference on computer and communications security* (pp. 41–47).
66. Liu, D. G., & Ning, P. (2003). Location-based pairwise key establishments for static sensor networks. In *Proceeding of 1st ACM workshop on security of ad hoc and sensor networks* (pp. 72–82).
67. Perrigy, A., Canetti, R., Tygar, J. D., & Song, D. (2000). Efficient authentication and signing of multicast streams over lossy channels. In *Proceedings of 2000 IEEE symp on security and privacy (S&P 2000)* (pp. 56–73).
68. Perrig, A., Szewczyk, R., Tygar, J. D., Wen, V., & Culler, D. E. (2002). SPINS: Security protocols for sensor networks. *Wireless Networks, 8*(5), 521–534.
69. Gaubatz, G., Kaps, J., Ozturk, E., & Sunar, B. (2005). State of the art in ultra-low power public key cryptography for wireless sensor networks. In *Proceedings of the third IEEE international conference on pervasive computing and communications* (pp. 146–150).
70. Zhu, S. C., Setia, S., & Jajodia, S. (2003). LEAP: efficient security mechanisms for large-scale distributed sensor networks. In *Proceeding of ACM CCS* (pp. 62–72).
71. Pietro, R. D., Mancini, L. V., Law, Y. W., Etalle, S., & Havinga, P. J. M. (2003). LKHW: A directed diffusion-based secure multicast scheme for wireless sensor networks. In *Proceedings of the 32nd international conference on parallel processing workshops (ICPP)* (pp. 397–406). IEEE Computer Society Press.
72. Kotzanikolaou, P., & Magkos, E. (2005). Hybrid key establishment for multiphase self-organized sensor networks. In *Proceedings of the sixth IEEE international symposium on a world of wireless mobile and multimedia networks (WoWMoM'05) and pervasive computing and communications workshops* (pp. 146–150).
73. Karlof, C., & Wagner, D. (2003). Secure routing in wireless sensor networks: attacks and countermeasures. In *Proceedings of the first IEEE international workshop on sensor network protocols and applications* (vol. 1(2), pp. 293–315).
74. Cao, Z., Hu, J. B., Chen, Z., Xu, M. X., & Zhou, X. (2006). Feedback: towards dynamic behavior and secure routing in wireless sensor networks. In *Proceedings of the IEEE workshop on pervasive computing and ad-hoc communication (PCAC'06)* (vol. 2, pp. 160–164).
75. Wood, A. D., & Stankovic, J. A. (2002). Denial of service in sensor networks. *IEEE Computer, 35*(10), 54–62.
76. Douceur, J. R. (2002). The sybil attack. In *Proceeding of the 1st international workshop on peer-to-peer systems (IPTPS'02)* (pp. 251–260).
77. Hu, Y. C., Perrig, A., & Johnson, D. B. (2003). Packet leashes: a defense against wormhole attacks in wireless networks. In *Twenty-second annual joint conference of the IEEE computer and communications, INFOCOM 2003* (vol. 3, pp. 1976–1987).
78. Hu, Y. C., Perrig, A., & Johnson, D. B. (2002). Wormhole detection in wireless ad hoc networks. Department of Computer Science, Rice University, Tech. Rep. TR01-384.
79. Blaze, M., Feigenbaum, J., & Lacy, J. (1996). Decentralized trust management. In *Proceedings of IEEE conference security and privacy* (pp. 164–173).
80. Buchegger, S. J., & Le, J. Y. (2003). The effect of rumor for mobile ad-hoc networks. In *Proceedings of the modeling and wireless networks (WiOpt).*
81. Kamvar, S. D., Schlosser, M. T., & Garcia-Molina, H. (2003). The elgentrust algorithm for reputation management in p2p networks. In *Proceedings of the twelfth international world wide web conference* (pp. 640–651).
82. Yao, Z. Y., Kim, D. Y., Lee, I., Kim, K. Y., & Jang, J. S. (2005). A security framework with trust management for sensor networks. In *Proceeding of the IEEE workshop of the 1st international conference on security and privacy for emerging areas in communication networks* (pp. 190–198).
83. Ganeriwal, S., & Srivastava, M. B. (2004). Reputation-based framework for high integrity sensor networks. In *Proceeding of the ACM workshop on security in ad-hoc & sensor networks (SASN)* (pp. 66–67).
84. KSW microtec AG. *KSW—TempSens.* http://www.ksw-microtec.de/www/doc/overviewtempsens1124436343en.pdf. Accessed 12 Oct 2013.
85. Wang, K., Bao, J., Wu, M., & Lu, W. (2010). Research on security management for internet of things. In *Proceeding of the IEEE international conference on computer application and system modeling (ICCASM)* (vol. 15, pp. 133–137).
86. Zhang, L., & Wang, Z. (2006). Integration of RFID into wireless sensor networks: architectures, opportunities and challenging problems. In *Proceeding of the IEEE fifth international conference on grid and cooperative computing workshops GCCW '06* ((58), pp. 463–469).

87. Li, C., & Chen, C. L. (2011). A multi-stage control method application in the fight against phishing attacks. In *Proceeding of the 26th computer security academic communication across the country* (p. 145).
88. Anti-Phishing Working Group. (2009). *Phishing activity trends report.* Q42.
89. Liu, J., An, X. B., & Li, C. S. (2002). *Wireless network communication principle and application* (pp. 386–407). Beijing: Tsinghua University Press.
90. Liu, Z. Y., & Yang, Z. C. (2006). Ad hoc network and security analysis. *The Computer Technology and Development, 16*(1), 231.
91. Avudainayagam, A., Lou, W., & Fang, Y. (2003). DEAR: A device and energy aware routing protocol for heterogeneous Ad hoc networks. *Parallel and Distributed Computing, 63*(2), 228–236.
92. Ryu, J. H., & Cho, D. H. (2001). A new routing scheme concerning energy conservation in wireless home ad-hoc networks. *IEEE Transactions on Consumer Electronics, 47*(1), 1–5.
93. Biyiklioglu, F., & Buzluca, F. (2007). A new mobility aware technique for heterogeneous mobile Ad hoc networks. In *12th Proceeding of the IEEE symposium on computers and communications* (pp. 45–50).
94. Li, X., Bao, Y. Z., & Zhen, Y. (2004). Power and mobility-aware adaptive dynamic source routing in MANET. In *Proceeding of IEEE TENCON 2004 conference on analog and digital techniques in electrical engineering,* (vol. B, vol. 2, pp. 652–655).
95. Sun, Y. Y., Liu, Z. H., Li, Q., & Sun, L. M. (2010). A IoT security architecture for 3G access. *Research and Development of the Computer, 47*, 327–332.
96. Yang, Z. W. (2010). Look the internet of things from the internet and 3G. *Radio frequency (rf) in the world*, (01).
97. Xiong, Z. (2012). Based on analysis of internet security of 3G networks. *Digital Technology and Application, 3*, 231.
98. Sun, C. M., Sun, Y. P., & Zhou, J. (2005). Based on the 3G internet security mechanism research. *Computer knowledge and technology, 7*(31), 7632–7635.
99. Jin, R. (2010). *Discussion of 6LowPan technology.* http://blog.csdn.net/rizejin/article/details/5548520. Accessed 12 Oct 2013.
100. Montenegro, G., Kushalnagar, N., Hui, J., & Culler, D. (2007). *Transmission of IPv6 packets over IEEE 802.15.4 networks.* http://tools.ietf.org/html/rfc4944. Accessed 12 Oct 2013.
101. Kushalnagar, N., Montenegro, G., & Schumacher, C. (2007). *IPv6 over low-power wireless personal area networks (6LoWPANs): Overview, assumptions, problem statement, and goals.* http://tools.ietf.org/html/rfc4919. Accessed 12 Oct 2013.
102. Khoshdelniat, R., Sinniah, G., R., Bakar, K. A., Shahari, M. H. M., Suryady, Z., & Sarwar, U. Performance evaluation of IEEE802. 15.4 6LoWPAN gateway. In *Proceeding of the IEEE Asia-Pacific conference on communications (APCC)* (pp. 253–258).
103. Wu, J. (2006). 6Lowpan technical analysis. *Railway communication signal, 42*(12), 38–40.
104. Gu, J. (2008). 6lowpan adaptation layer network self-organizing ability of the simulation and research. *Computer Applications and Software, 20*(10), 42–45.
105. Lu, G. (2008). 6Lowpan neighbor discovery protocol research. *Computer Applications and Software, 20*(4), 51–53.
106. Bandyopadhyay, D., & Sen, J. (2011). Internet of things: Applications and challenges in technology and standardization. *Wireless Personal Communications, 58*(1), 49–69.
107. Zhang, B., Zou, Z., & Liu, M. (2011). Evaluation on security system of internet of things based on fuzzy-AHP method. In *Proceeding of the IEEE international conference on E -Business and E-Government (ICEE)* (pp. 1–5).
108. Wang, Z. L., & Wang, F. H. (2011). *Introduction to the internet of things engineering*. Beijing: Mechanical Industry Press.
109. Zhang, G. G., Bi, Y., & Li, C., et al. (2013). Massive internet data security processing model research. *Small Microcomputer System, 34*(9), 2090–2094.
110. Yi, K. M. (2010). Preliminary study of IoT security. *Internet Police Detachment of Public Security Bureau in Taian City*.
111. Sweeney, L. (2002). K-anonymity: A model for protecting privacy. *International Journal of Uncertainty, Fuzziness, and Knowledge-Based Systems, 5*, 557–570.
112. A. de Saint-Exupery. *Internet of things [EB/OL].* http://www.sintef.no/upload/IKT/9022/CERP-IoT%20SRA_IoT_vll_pdf.pf. Accessed 12 Oct 2013.
113. Sheng, N. H., Yu, Z., Li, L. F., Ming, L. W., & Feng, Q. S. (2006). Research on China internet of things' services and management. *Chinese of Journal Electronics, 34*(12A), 2514–2517.
114. Zhang, D., Zhou, J., Guo, M., Cao, J., & Li, T. (2011). TASA: Tag-free activity sensing using RFID tag arrays. *IEEE Transactions on Parallel and Distributed Systems, 22*(4), 558–570.
115. Gu, D. C., Chen, L., & Zhang, Z. Q. (2013). Logistics monitoring design based on ZigBee technology. *The Internet of Things Technology, 2*, 79–86.
116. Zai, L., Liu, S. D., & Hu, X. B. (2007). *ZigBee technology and application* (p. 2007). Beijing: Beijing University of Aeronautics and Astronautics Press.
117. Shao, P. F., Wang, Z., & Zhang, B. R. (2012). Smart home system research for the mobile internet. *The Computer Measurement and Control, 20*(2), 474–476.
118. Chen, M., Wan, J., González, S., Liao, X., & Leung, V. (2014). A survey of recent developments in home M2 M networks. *IEEE Communications Surveys and Tutorials, 16*(1), 98–114.
119. Chen, Y. P. (2013). The internet of things technology in the application of the smart home. *China Public Security, 16*, 61–63.
120. Bao, Y. Q. (2013). The smart home system based on internet of things technology research and discussion. *The Internet of Things Technology, 7*, 38–41.

Qi Jing received the M.S. degree from Harbin Institute of Technology, China in 2003, and the Ph.D. degree from School of Electronics Engineering and Computer Science of Peking University in 2009. She is also a postdoctoral fellow with the Beijing Key Laboratory of IOT information security technology, Institute of Information Engineering, CAS, China. She is currently an Associate Professor of School of Software and Microelectronics, Peking University. She is focused on information security, Internet of Things.

Athanasios V. Vasilakos is currently a Professor with the Kuwait University. He served or is serving as an Editor or/and Guest Editor for many technical journals, such as the IEEE Transactions on Network and Service Management; IEEE Transactions on Cloud Computing, IEEE Transactions ON Information Forensics and Security, IEEE Transactions on Nanobioscience, IEEE Transactions on Cybernetics; IEEE Transactions on Information Technology in Biomedicine; ACM Transactions on Autonomous and Adaptive Systems; the IEEE Journal on Selected Areas in communications. He is also General Chair of the European Alliances for Innovation (www.eai.eu).

Jiafu Wan is an Associate Professor in School of Mechanical and Automotive Engineering, South China University of Technology (SCUT), China. He received the Ph.D. degree in Mechatronic Engineering from SCUT in Jun 2008. In 2010, he became a Provincial Talent Cultivated by "Thousand-Hundred-Ten" Program of Guangdong Province, China. He is a project leader of several projects (e.g., NSFC). Up to now, Dr. Wan has authored/co-authored one book and more than 60 scientific papers. His research interests include cyber-physical systems (CPS), Internet of Things, machine-to-machine (M2M) communications, mobile cloud computing, and embedded systems. He is a CCF senior member, and a member of IEEE, IEEE Communications Society, IEEE Control Systems Society, and ACM.

Jingwei Lu received her B.E. degree in Computer Science and technology from Liaoning Normal University, Dalian, China. She is studying for her M.E. degree in School of Software and Microelectronics, Peking University, Beijing, China. Her research interests in machine learning, cloud computing and IoT.

Dechao Qiu got his bachelor's degree of Software Engineering and master's degree of Software Engineering from Wuhan University and Peking University of China respectively. His research interests are Software Technology, Software Development and the Internet of Things.