Security in the Internet of Things: A Review

Hui Suo[a], Jiafu Wan[a,b,*]
[a] College of Information Engineering
Guangdong Jidian Polytechnic
Guangzhou, China
suohui79@163.com

Caifeng Zou[a], Jianqi Liu[a]
[b] School of Computer Science and Engineering
South China University of Technology
Guangzhou, China
[*]Corresponding author, jiafu_wan@ieee.org

***Abstract* — In the past decade, internet of things (IoT) has been a focus of research. Security and privacy are the key issues for IoT applications, and still face some enormous challenges. In order to facilitate this emerging domain, we in brief review the research progress of IoT, and pay attention to the security. By means of deeply analyzing the security architecture and features, the security requirements are given. On the basis of these, we discuss the research status of key technologies including encryption mechanism, communication security, protecting sensor data and cryptographic algorithms, and briefly outline the challenges.**

Keywords - internet of things; security; privacy; confidentiality; challenges

I. INTRODUCTION

The term, internet of things (IoT) that refers to uniquely identifiable objects, things, and their virtual representations in an internet-like structure, was first proposed in 1998 [1]. In recent years, the concept of IoT has become particularly popular through some representative applications (e. g., smart electric meter reading, greenhouse monitoring, telemedicine monitoring, and intelligent transportation). Usually, IoT has four major components including sensing, heterogeneous access, information processing, applications and services, and additional components such as security and privacy.

Nowadays, the IoT as a buzzword is widely known, subsequent industry applications related to the IoT will arise, for example cyber-transportation systems (CTS), cyber-physical systems (CPS), and machine-to-machine (M2M) communications [2].

As to the security, the IoT will be faced with more severe challenges. There are the following reasons: 1) the IoT extends the 'internet' through the traditional internet, mobile network and sensor network and so on, 2) every 'thing' will be connected to this 'internet', and 3) these 'things' will communicate with each other. Therefore, the new security and privacy problems will arise. We should pay more attention to the research issues for confidentiality, authenticity, and integrity of data in the IOT.

At this stage, the ambient intelligence and autonomous control are not part of the original concept of IoT. With the development of advanced network techniques, distributed multi-agent control and cloud computing, there is a shift integrating the concepts of IoT and autonomous control in M2M research to produce an evolution of M2M in the form of CPS. CPS mainly focuses on intelligentizing interaction, interactive applications, distributed real-time control, cross-layer optimization, cross-domain optimization, etc. Therefore, some new technologies and methodologies should be developed to meet the higher requirements in terms of reliability, security and privacy [3].

II. PAY ATTENTION TO SECURITY IN IOT

The security of information and network should be equipped with these properties such as identification, confidentiality, integrality and undeniability. Different from internet, the IoT will be applied to the crucial areas of national economy, e.g., medical service and health care, and intelligent transportation, thus security needs in the IoT will be higher in availability and dependability.

A. Secure Archetecture

In general, the IoT can be divided into four key levels [4]. Fig. 1 shows that the level architecture of the IoT.

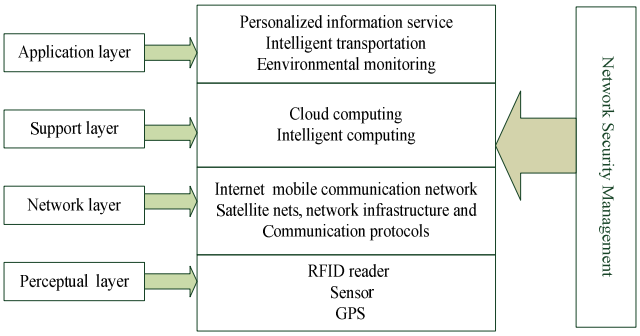

Figure 1. Security architecture

The most basic level is the perceptual layer (also known as recognition layer), which collects all kinds of information through physical equipment and identifies the physical world, the information includes object properties, environmental condition etc; and physical equipments include RFID reader, all kinds of sensors, GPS and other equipments. The key component in this layer is sensors for capturing and representing the physical world in the digital world.

The second level is network layer. Network layer is responsible for the reliable transmission of information from perceptual layer, initial processing of information, classification and polymerization. In this layer the information transmission is relied on several basic networks, which are the

978-0-7695-4647-6/12 $26.00 © 2012 IEEE
DOI 10.1109/ICCSEE.2012.373

internet, mobile communication network, satellite nets, wireless network, network infrastructure and communication protocols are also essential to the information exchange between devices

The third level is support layer. Support layer will set up a reliable support platform for the application layer, on this support platform all kind of intelligent computing powers will be organized through network grid and cloud computing. It plays the role of combining application layer upward and network layer downward.

The application layer is the topmost and terminal level. Application layer provides the personalized services according to the needs of the users. Users can access to the internet of thing through the application layer interface using of television, personal computer or mobile equipment and so on.

Network security and management play an important role in above each level. Then we will analysis the security features.

B. *Security Features*

a) Perceptual Layer: Usually perceptual nodes are short of computer power and storage capacity because they are simple and with less power. Therefore it is unable to apply frequency hopping communication and public key encryption algorithm to security protection. And it is very difficult to set up security protection system. Meanwhile attacks from the external network such as deny of service also bring new security problems. In the other hand sensor data still need the protection for integrity, authenticity and confidentiality.

b) Network Layer: Although the core network has relatively complete safety protection ability, but Man-in-the-Middle Attack and counterfeit attack still exist, meanwhile junk mail and computer virus cannot be ignored, a large number of data sending cause congestion. Therefore security mechanism in this level is very important to the IoT.

c) Support Layer: Do the mass data processing and intelligent decision of network behavior in this layer, intelligent processing is limited for malicious information, so it is a challenge to improve the ability to recognize the malicious information.

d) Application Layer: In this level security needs for different application environment are different, and data sharing is that one of the characteristics of application layer, which creating problems of data privacy, access control and disclosure of information[4,10].

C. *Security Requirements*

According to the above analysis, we can summarize the security requirements for each level in the following, as shown in Fig. 2.

a) Perceptual Layer: At first node authentication is necessary to prevent illegal node access; secondly to protect the confidentiality of information transmission between the nodes, data encryption is absolute necessity; and before the data encryption key agreement is an important process in advance; the stronger are the safety measures, the more is consumption of resources, to solve this problem, lightweight encryption technology becomes important, which includes Lightweight cryptographic algorithm and lightweight cryptographic protocol. At the same time the integrity and authenticity of sensor data is becoming research focus, we will discuss this question more in-depth in the next section.

b) Network Layer: In this layer existing communication security mechanisms are difficult to be applied. Identity authentication is a kind of mechanism to prevent the illegal nodes, and it is the premise of the security mechanism, confidentiality and integrality are of equal importance, thus we also need to establish data confidentiality and integrality mechanism. Besides distributed denial of service attack (DDoS) is a common attack method in the network and is particularly severe in the internet of thing, so to prevent the DDOS attack for the vulnerable node is another problem to be solved in this layer.

c) Support Layer: Support layer needs a lot of the application security architecture such as cloud computing and secure multiparty computation, almost all of the strong encryption algorithm and encryption protocol, stronger system security technology and anti-virus.

d) Application Layer: To solve the security problem of application layer, we need two aspects. One is the authentication and key agreement across the heterogeneous network, the other is user's privacy protection. In addition, education and management are very important to information security, especially password management [4,10].

In summary security technology in the IoT is very important and full of challenges. In other hands laws and regulations issues are also significant, we will discuss this problem in the following.

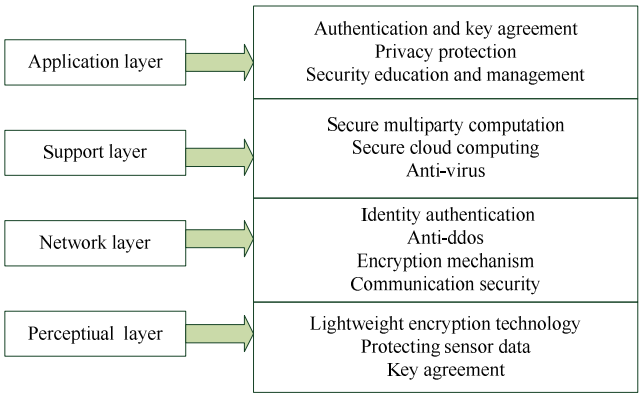

Figure 2. Security requirements in each level

III. RESEARCH STATE OF CRUCIAL TECHNOLOGIES

Now, we will look into the state of research for the security requirements in Section II, and further detail on encryption mechanism, communication security, protecting sensor data, and cryptographic algorithm in the following subsections.

A. Encryption Mechanism

In the traditional network layer we adopt by-hop encryption mechanism, in this way the information is encrypted in the transmission process, but it needs to keep plaintext in each node through the decryption and encryption operations. Meanwhile in the traditional application layer encryption mechanism is end-to-end encryption, that is, the information only is explicit for the sender and the receiver, and in the transmission process and forwarding nodes it will be always encrypted.

In the IoT network layer and application layer connect so closely, so we should choose between by-hop and end-to-end encryption. If we adopt by-hop encryption, we can only encrypt the links which need be protected, because in the network layer we can apply it to all business, which make different applications safely implemented. In this way, security mechanism is transparent to the business applications, which gives the end users convenience. In the meantime this brings the features of the by-hop full play, such as low latency, high efficiency, low cost, and so on. However, because of the decryption operation in the transmission node, using by-hop encryption each node can get the plaintext message, so by-hop encryption needs high credibility of the transmission nodes [5].

Using the end-to-end encryption, we can choose different security policy according to the type of business, thus it can provide high level security protection to the high security requirements of the business. However, end-to-end encryption can not encrypt the destination address, because each node determines how to transmit messages according to the destination address, which causes it can not hide the source and the destination of the message being transmitted, and bring about malicious attacks [5, 6].

Through the above analysis, we can draw a conclusion: when the security requirement of some business is not very high, we can adopt by-hop encryption protection; when the business needs high-security, then end-to-end encryption is the first choice. So, according to the different requirements we choose alternative encryption mechanism.

Currently, IoT is developing in its primary phase, and the research of safety mechanism is in the blank in the practice, so we have a long way for the research of this domain.

B. Communication Security

At first in communication protocols there are some solutions being established, these solutions can provide integrity, authenticity, and confidentiality for communication, for example: TLS/SSL or IPSec. TLS/SSL is designed to encrypt the link in the transport layer, and IPSec is designed to protect security of the network layer, they can provide integrity, authenticity, and confidentiality in the each layer. And the needs of privacy also have been come up with but unfortunately are not in wide use.

Then communication security mechanisms are also seldom applied nowadays. Because in the IoT small devices are less processing power, this leads that communication security is often weak. Meanwhile in the IoT, the core network is always the current or next-generation Internet, most of the information will be transmitted through the Internet. So DDoS still exists and is a very severe problem. These botnets and DDoS attacks will destroy the availability of communication. When lager-scale or organized DDoS attacks happen, how to do the disaster recovery is highly significant, so we need pay more attention to researching better preventive measures and disaster recovery mechanisms[8].

C. Protecting Sensor Data

Just like that we said in part Ⅱ, the integrity and authenticity of sensor data is becoming research focus, and confidentiality of sensor data is a lower demand because when an attacker can just place its own sensor physically near, he can sense the same values. So at the sensor itself the confidentiality need is relatively low [8].

The other main research target in sensors is privacy, and privacy is also a major problem. We should adopt the mechanisms to protect the privacy of humans and objects in the physical world. Most times people are often unaware of sensors in their life, so we need to set up regulations to preserve the privacy of people. In the literature [7], several guidelines are given to solve this problem in the design phase: at first users must know that they are being sensed, the second users must be able to choose whether they are being sensed or not, the third users must be able to remain anonymous. When the user has no realization of these guidelines, that regulations must be made [8].

D. Cryptographic Algorithms

So far there is a well known and widely trusted suite of cryptographic algorithms applied to internet security protocols such as table 1.

TABLE 1. A SUITE OF CRYPTOGRAPHIC ALGORITHMS

Algorithm	Purpose
Advanced encryption standard (AES)	Confidentiality
Rivest shamir adelman (RSA)/ Elliptic curve cryptography (ECC)	Digital signatures key transport
Diffie-hellman (DH)	Key agreement
SHA-1/SHA-256	Integrality

Usually the symmetric encryption algorithm is used to encrypt data for confidentiality such as the advanced encryption standard (AES) block cipher; the asymmetric algorithm is often used to digital signatures and key transport , frequently-used algorithm is the rivest shamir adelman (RSA); the diffie-hellman (DH) asymmetric key agreement algorithm is used to key agreement; and the SHA-1 and SHA-256 secure hash algorithms will be applied for integrality. Another significant asymmetric algorithm is known as elliptic curve cryptography (ECC), ECC can provide equal safety by use of shorter length key, the adoption of ECC has been slowed and maybe be encouraged recently [9].

To implement these cryptographic algorithms available resources are necessary such as processor speed and memory.

So how to apply these cryptographic techniques to the IoT is not clear, we have to make more effort to further research to ensure that algorithms can be successfully implemented using of constrained memory and low-speed processor in the IoT.

IV. CHANLLENGES

IoT as a very active and new research field, a variety of questions need to be solved, at different layers of the architecture and from different aspects of information security, the following subsections analyze and summarize common challenges for security of IoT.

A. Security Structure

In [10], the IoT will remain stable-persisting as a whole over time, putting together the security mechanism of each logical layer can not implement the defense-in-depth of system, so it is a challenge and important research area to construct security structure with the combination of control and information.

B. Key Management

Because key management is the important basis of more security mechanism, it is always the hot research area. It is still the most difficult aspect of cryptographic security. Currently the researchers don't find ideal solutions. Lightweight cryptographic algorithm or higher performance of sensor node is still not applied. So far the real large-scale sensor network is always seldom put into practice. The problems of network security will be paid more attention to and become key points and difficulties of research in this network environment [4, 9].

C. Security Law and Regulations

Currently security law and regulations is still not the main focus, and there is no technology standard about the IoT. The IoT is related to national security information, business secrets and personal privacy. Therefore, our country needs the legislative point of view to promote development of the IoT. Policies and regulations are urgently needed. In this aspect we have a long way to go [5].

D. Requirements for Burgeoning Applications

With the development of WSNs, radio frequency identification (RFID), pervasive computing technology, network communication technology, and distributed real-time control theory, CPS, an emerging form of IoT, is becoming a reality [11, 12]. In this system, the high security is necessary for guaranteeing system performance.

As all said above, the security challenges for the IoT are severe. It is necessary to establish sound security structure. The key management in the real large-scale sensor network is always a challenge, and the policies and regulations related to the IoT will also be a challenge.

V. CONCLUSIONS

In the last few years, this emerging domain for the IoT has been attracting the significant interest, and will continue for the years to come. In spite of rapid evolution, we are still facing new difficulties and severe challenges. In this literature, we concisely reviewed security in the IoT, and analyzed security characteristics and requirements from four layers including perceptual layer, network layer, support layer and application layer. Then, we discussed the research status in this field from encryption mechanism, communication security, protecting sensor data, and encryption algorithm. At last we summarize several challenges. All in all the development of the IoT will bring more serious security problems, which are always the focus and the primary task of the research.

ACKNOWLEDGMENT

This work was supported in part by the National Natural Science Foundation of China (No. 50905063), the Fundamental Research Funds for the Central Universities, SCUT (No. 2011ZM0070), the China Postdoctoral Science Foundation (No. 20090460769), the Natural Science Foundation of Guangdong Province, China (No. S2011010001155), and the High-level Talent Project for Universities, Guangdong Province, China (No. 431, YueCaiJiao 2011).

REFERENCES

[1] R. H. Weber, "Internet of things – new security and privacy challenges," Computer Law & Security Review, vol. 26, pp. 23-30, 2010.

[2] J. F. Wan, H. H. Yan, H. Suo, and F. Li, "Advances in cyber-physical systems research," KSII Transactions on Internet and Information Systems, 2011, 5(11): 1891-1908.

[3] M. Chen, J. F. Wan, and F. Li, "Machine-to-machine communications: architectures, standards, and applications," KSII Transactions on Internet and Information Systems, to appear, January 2012.

[4] G. Yang, J. Xu, W. Chen, Z. H. Qi, and H. Y. Wang, "Security characteristic and technology in the internet of things," Journal of Nanjing University of Posts and Telecommunications (Natural Science), vol. 30, no. 4, Aug 2010.

[5] Z. H. Hu, "The research of several key question of internet of things," in Proc. of 2011 Int. Conf. on Intelligence Science and Information Engineering, pp. 362-365.

[6] G. Gan, Z. Y. Lu, and J. Jiang, "Internet of Things Security Analysis," in Proc. of 2011 Int. Conf. on Internet Technology and Applications (iTAP), Aug. 2011.

[7] M. Langheinrich, "Privacy by design-principles of privacy-aware ubiquitous systems," In Proc. of Ubicomp, pp. 273-291, Oct. 2001.

[8] C. P. Mayer, "Security and privacy challenges in the internet of things," Electronic Communications of the EASST, vol. 17, 2009.

[9] T. Polk, and S. Turner. "Security challenges for the internet of things," http://www.iab.org/wp-content/IAB-uploads/2011/03/Turner.pdf

[10] C. Ding, L. J. Yang, and M. Wu, "Security architecture and key technologies for IoT/CPS", ZTE Technology Journal, vol. 17, no. 1, Feb. 2011.

[11] J. F. Wan, H. Suo, H. H. Yan, and J. Q. Liu, "A general test platform for cyber-physical systems: unmanned vehicle with wireless sensor network navigation," in Proc. of 2011 Int. Conf. on Advances in Engineering, Nanjing, China, December, 2011.

[12] J. H. Shi, J. F. Wan, H. H. Yan, and H. Suo, "A survey of cyber-physical systems," in Proc. of the Int. Conf. on Wireless Communications and Signal Processing, Nanjing, China, November, 2011.