Security Architecture of the Internet of Things Oriented to Perceptual Layer

Weizhe Zhang[1]*, Baosheng Qu**

Abstract

The Internet of Things (IoT) is a ubiquitous Internet-based network. However, the IoT exhibits characteristics that pose considerable risks: inherent openness, heterogeneity, and terminal vulnerability. Thus, a new type of architecture must be established to ensure security. The new architecture should aim to improve the efficiency, reliability, and controllability of the entire security system. It should also cover most security technologies and ensure thorough compatibility of various security mechanisms. Therefore, this study investigates all possible attacks and security threats to the IoT and proposes related security technologies. This study presents a design of a highly refined security subject and universal two-dimensional security architecture integrated with related safety technologies.

Keywords: ubiquitous network; Internet of Things; security subject; perceptual layer

1. Introduction

The Internet of Things (IoT) is an "always-on" communications network built on the Internet, in which massive terminal objects such as radio frequency identification (RFID) equipment, sensors, and intelligent terminals can connect to the Internet by perception of the environment. The IoT has been designed into a type of application paradigm[1][2].

The IoT has been variously defined. Considering the importance of functionality and identity, the International Telecommunications Union briefly defines the IoT as follows: "from anytime, anyplace connectivity for anyone, we will now have connectivity for anything.

The European Commission similarly describes the IoT as "things having identities and virtual personalities operating in smart spaces using intelligent interfaces to connect and communicate within social, environmental, and user contexts."

The technology of the IoT can be widely applied to improve the quality of life as well as industrial production. The IoT involves important applications such as military interoperability, disaster warning, personnel tracking, and intelligent terminal interactions. The IoT is a comprehensive perceptual network interconnection, more popular and more powerfully smart, making the IoT advantageous over other existing Internet or sensing applications.

The application of the IoT is only at its initial stage. Research on security issues related to the IoT remains inadequate. The inherent openness, heterogeneity, and terminal vulnerability of the IoT pose a huge risk. Thus, the design of a series of security mechanisms must be promptly implemented to ensure security.

However, the complexity of the IoT separates related aspects of research. Moreover, the trust mechanism, anonymous privacy, safe route, intrusion detection, and other facets of the IoT are not related. Thus, establishing a new architecture is necessary, which should cover the majority of security technology and ensure thorough compatibility of various security mechanisms to improve the efficiency, reliability, and controllability of the entire security system.

Considering that the greatest difference between the IoT and the Internet lies in perceptual quality, we propose bottom-up security architecture with extensible loose coupling characteristics that are oriented to the perceptual layer. This architecture is expected to satisfy a series of application needs. The main problems are listed as follows:

1). Coupling:

Different technologies such as intrusion detection and trust mechanism are related to each other. However, these technologies use different processing methods and are applied in different layers. Consequently, loose coupling and reasonability as well as structured I/O interactions among security mechanism must be ensured in the design of the security architecture.

2).Completeness:

The existing security mechanism is mostly used for a single application or field. The design of the security architecture should consider future application trends, incorporating any possible security module.

This paper presents an analysis of all attacks and security threats that may arise in the IoT. Accordingly, this study proposes related security technologies and a design of a universal security architecture that integrates logically related technologies.

*Corresponding Author: Weizhe Zhang
(E-mail: wzzhang@hit.edu.cn).
[1] School of Computer Science and Technology,
Harbin Institute of Technology, Harbin, China.

This work also investigates common security architecture problems. Section 2 presents an analysis of the current research status of the security architecture. Section 3 examines the security threats occurring in the perceptual, network, middleware, and application layers. A more refined security principle and two-dimensional (2D) security architecture for the IoT are presented in Section 4. Finally, Section 5 states the conclusion of the paper.

2. Related Studies

Several studies have been conducted on the security architecture of the IoT. However, the architectures described have yet to be refined.

Most studies on the security of the IoT are designed for certain types of applications or aimed at achieving specific security issues. The IoT can be classified according to its users: dedicated IoT network such as cyber physical systems (CPS) and open IoT such as the Web of Things.

1). Securityarchitecture for dedicated IoT[3]

CPS is a typical dedicated IoT that mainly focuses on interactions in a relatively closed system.

Chao Ding et al. divided CPS into two parts: the information field and the control field. They analyzed the new attacks existing in the information field (e.g., clock synchronization attack, data mining privacy leak, and user privacy leak) as well as those affecting control systems (e.g., control commands fake attack and perceptual data tampering). They also proposed IoT/CPS security architecture.

Xin Ma et al. also proposed security architecture. In the design of the security architecture oriented to production security, disaster warning, and other public security, they merged the middleware and application layers with the control layer[4]. This innovation reduces the complexity of the entire security architecture of dedicated IoT and emphasizes control security. However, all aforementioned structures are designed under the hypothetical precondition that the whole environment of perceptual layers is closed. Another condition is that only threats related to openness exist in the middleware and application layers. These conditions ignore new security threats posed by the deployment of dedicated services in the open-awareness network. Privacy issues on the terminal as well as problems on node coordination continue to exist.

2).Security architecture oriented to the open IoT

the IoT is similar to the Internet, which has a distributed, open-application architecture and can control all components, although without a single unit. Compared with the dedicated IoT, the openness of the open IoT includes two challenges: the environment of the perceptual layers is more complex, and the units cannot be fully trusted.

Leusse et al. proposed the new idea of self-managed security cells (SMSC) oriented to the middleware layer, which can undertake a series of functions such as strategic management and access control and establish the security architecture of the IoT based on service-oriented architecture (SOA)[5];

Zhen Qiang Wu et al. proposed the secure transmission system for the IoT for the application layer (Object Name Service applications) and developed a three-layer structure consisting of the management centre, root services, and local services[6]. These services ensure authentication and anonymity of data transmission by designing encryption mechanisms.

Yan Bing Liu et al. considered information collection safety, network and information security, as well as information processing security in the design of the security architecture[7]for RFID applications.

Existing research on the IoT security architecture is generally insufficient. These architectures are incomplete in terms of function; the dedicated IoT structure focuses on ensuring the business process out of attack and control security. However, the architecture for open IoT gives equally high importance on users, institutions, terminal information, identity, and behaviour out of attack, as it does on data security.

On the basis of structure, the abovementioned security architectures remain incomplete. All are based on the layered structure of the IoT. Consequently, the layer-to-layer security mechanism and the inner layer of the security module are isolated, as well as the security flow. The security performance of the entire system is not ensured.

Numerous solutions have been proposed such as identification of identity, data encryption, access control[8], and privacy protection. Although these studies have achieved the security objectives, none of these can practically ensure system security.

On one hand, high resource costs cannot ensure security in time; the same applies to the required intensity of the limited terminal in the entire interaction cycle. On the other hand, the security mechanism cannot effectively withstand common internal attack in the perceptual network.

The details above suggest that more generalizations regarding new security architecture are needed to ensure the security of various applications. Moreover, layer-to-layer and internal layer security flow should be developed to optimize its operation efficiency under the control of layered mechanism.

3. IoT Security Threats

Security threats existing in the IoT are closely associated with its application environment. A detailed discussion is provided as follows.

3.1 Perceptual layer security threats

In the perceptual layer, perceptual nodes usually build an ad hoc network with a dynamic distribution. Given limited node resources, dynamic change in network topology, and distributed organized structure, the main threats that come from the perceptual layer are listed below.

1). Physical capture: Many nodes are statically deployed in the area and can easily be captured by attackers and thus, are physically compromised.

2). Brute force attack: The ability of resource storage as well as the computation of the sensor node are limited and are most likely to suffer from brute force attack.

3). Clone node: The hardware structure of several perceptual nodes is simple, and hence, can be easily copied by the attacker.

4). Impersonation: Authentication in the distributed environment is very difficult for the perceptual node, allowing for malicious nodes to use a fake identity for malicious or collusion attacks.

5). Routing attack: Data forwarding and relay exist in the process of perceptual data collection. Thus, intermediate nodes might attack the data during forwarding.

6). Denial of service (DoS) attack: Nodes can easily be trapped under DoS attack, given their finite processing ability.

7). Node privacy leak: The attacker can passively or actively steal sensitive information in the node.

3.2 Network layer security threats

The network layer of the IoT is usually referred to as the next-generation network integrated by various types of networks, mainly classified into inter-city nets and backbone network. The manufacture of communication equipment for fast self-adaptive configuration and the development of a controllable and manageable security platform within the heterogeneous and interlink network draw considerable interest. Such equipment is often deployed in advance and are not strictly monitored by controllable and safe data routing.

The main security threat in the network layer consists of routing attacks such as malicious behaviours against right path topology and forwarding data, DoS attack, and so on because of the strong closure of the backbone network. The wired or wireless terminal transmission of the network layer makes routing attacks that are different from those in the perceptual layer.

3.3 Middleware layer security threats

The IoT middleware layer mainly provides services for basic tasks such as Web service and application program interface. Hence, the measures taken against Web service attack can also be used for those occurring in the middleware layer. In addition, more attacks may arise as the middleware layer becomes more open.

1). DoS attack: The DoS or distributed DoS attack can destroy service availability because Internet attack entails low cost.

2). Non-permission to access: In an open architecture, if unreasonable access configuration, malicious intrusion, or trapping users with higher permissions into improper operation are present, attackers can easily threaten security by denying permission to access the related service.

3). Data attacks: Attackers focus on attacks for data service. For example, attackers redo service requests, change data on request headers, and execute parts of data dictionary attacks or middleman attacks.

4). Session attacks: With a state attached to it, the service access can be viewed as a conversation. Thus, the attacker can hijack or redo sessions to gain illegal access.

3.4 Application layer security threats

The attacker is likely to destroy privacy in the application layer by a known vulnerability (e.g., buffer overflow, cross site scripting, and SQL injection), error configuration (e.g., simple password), or improperly obtained higher permission access.

1). Privacy leak: Given that the application of IoT is executed on common operating systems and hosting services, the attacker can easily steal user data (e.g., user password, historical data, and social relations) by known vulnerabilities. The attacker can also analyze terminal location and identity privacy by the query results, unless the software is promptly updated.

2). DoS attack: This attack is similar to that in the middleware layer, in which attackers can destroy the availability of the application itself.

3). Malicious code: Attackers can upload malicious codes through the known vulnerabilities, leading to fetcher software infections.

4). Social engineering: A certain relationship exists among IoT users. However, attackers can easily analyze

or obtain additional information that can be used for attacks by social engineering.

In summary, the IoT shares numerous similarities with the Internet in terms of application layer threats. However, the former is likely to face more difficulties in response to network attacks because of its sociability and regional locality.

4. Security Architecture of the IoT

We propose a refining security subject and then construct the security architecture based on this subject.

4.1 Refining security subject

Leusse et al. proposed a security model called SMSC [5]. As shown in Figure 1, the model includes a complete security function and applies the SOA architecture. The scheme potentially establishes the foundation of future security architecture, considering its great autonomy and customization. This model can be easily designed into security as a service and integrated into all kinds of software as a service, platform as a service, and infrastructure as a service SOA. However, the SMSC design is relatively unfinished and disregards the relationship among modules, data, and control, regardless of the use of the message bus to connect all security modules.

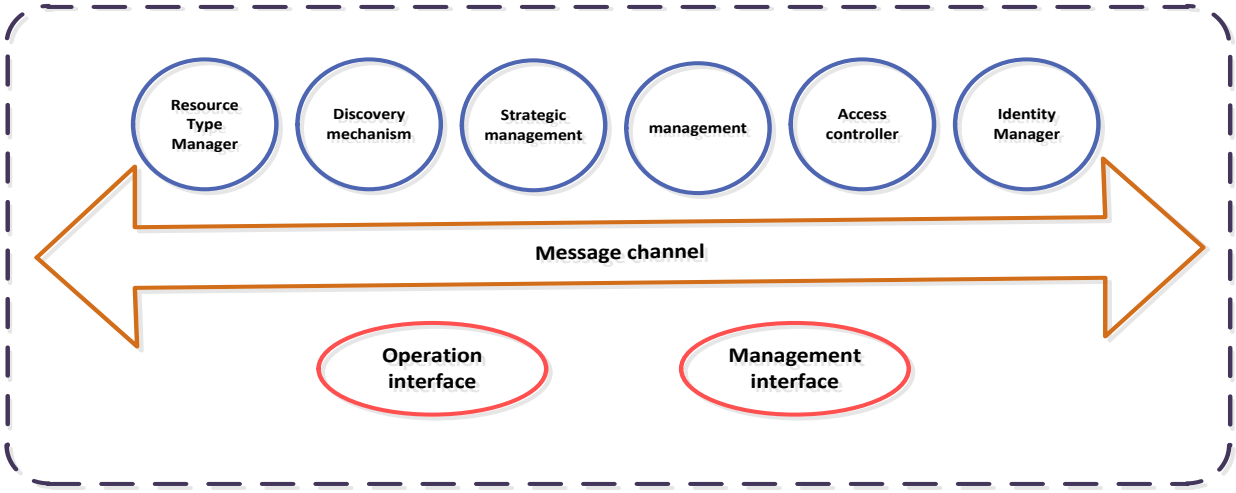

Fig. 1 A coarse-grained secure cell.

Figure 2 presents a refining security subject that marks the control and data flow among security modules as well as the interactions among security modules. After accepting a security subject and inputs, it conducts a series of security mechanism processing, and then outputs the related response information. Although the security subjects differ from one another for different environments or different layers, the networking scene can be drawn for abstraction. In detail, the input of an agent can be simplified as a triple (i.e., object, behaviour, and data) and its output as the error message in case of failure or another triple (i.e., subject, behaviour, and data) in case of success. Then, the security business processing can be reduced to the processing of several modules for data stream.

A safe subject can be divided into four parts in terms of function: identity security module, data security module, control security module, and behaviour safety module.

Identity security module mainly includes identity credibility and identity privacy. In identity credibility, the subject in the authentication mechanism verifies whether the object has legal and effective certification by requesting for a Certification Authority or by peer sharing. The authorization management simultaneously confirms whether the object has sufficient access to complete the request operation. To hide their identity, attackers can generate a fake name, which the subject presents outside by the privacy protection mechanism.

Fig. 2 A refined secure subject.

The control security module mainly includes security control management and security decisions. The subject searches the security policy repository for a matched rule and verifies whether the input of the object can be trusted under security decisions.

After ensuring the credibility input, the subject captures the processing results by applying relevant logical processing, i.e., the subject output corresponding to the object input. The subject then conducts security protection of output data in the data security module.

The data security module mainly guarantees the integrity, privacy, and non-repudiation of input/output data. The security subject uses an encryption algorithm to ensure that the data during transmission are not accessed by attackers. The security subject also employs the anonymous group method to its location information in privacy protection.

The behaviour security module can be explained as follows: In the detection of malicious incident, the subject analyzes the possibility of malicious events in the attack mode library by analyzing the actions and the data of the target; after which, the subject builds the interactive knowledge base. In accordance with the direct interaction base, the subject analyzes the credibility of the input, which subsequently acts as a partial basis for security decision, combined with the credibility information and subject correlation collected from the cooperation among several subjects.

Despite different knowledge bases and security mechanisms created by different environments for the subject, the uniform security subject model can solve similar security issues arising in various environments. Consequently, the security subject model can simplify the security system.

For example, in the calculation of the routing trust model in the perceptual layer, the subject association database mainly perceives the topological information among nodes. The trust model investigates the credibility of the path and the nodes by the announced topological consistency among objects.

However, in calculating the application trust model in the middleware layer, the subject association database is mainly referred to as the relationship between the trust mechanism and the reputation mechanism estimates for credit on the objects. The degree of intimacy of the institutions is inspected.

The calculation methods and library content used in these subjects are clearly different; however, these subjects have the same goal. Therefore, the refining security module and the security flow describe the security subject as having a very good effect.

4.2 2D Security architecture

We proposed a type of security architecture against security threats, as shown in Figure 3. In the longitudinal 2D security architecture, security is further categorized based on the environment: perceptual layer security, network layer security, middleware layer; and application layer security. Laterally, division by function on each layer consists of identity security, data security, control safety, and safety behaviour.

Among them, identity security mainly guarantees the subject of authentication and identifiability. Data

security ensures secrecy, integrity, non-repudiation, and reversibility of input/output data. Control security and behaviour security establish their security control platform, which can identify malicious behaviours and evaluate system security, thus forming 2D security architecture.

In this security architecture, the security flow starts from left to right in every module within the security subject to complete corresponding security functions. Security data produced from the lower layer module flow from the bottom toward the knowledge base of higher-layer modules, whereas control information flows toward the strategy base of lower-layer modules.

1). Security module in the perceptual layer

The security module in the perceptual layer maintains the physical and logical security of network facilities and terminal, labels the equipment, and so on.

The entire bottom layer acts as the hardware security mechanism, including the security cycle analysis of the terminal. The bottom layer self-destroys or invalidates the mechanism after a physical capture (e.g., the KILL-command trigger mechanism of the EPC Global standards). This part closely relates to the realization of application and terminal; upon this is the logic security mechanism protected with several algorithms.

The base module of the logic security mechanism consists of the encryption mechanism and security algorithm. Both perform three functions: allow terminal identity authentication mechanism by the hash algorithm and asymmetric encryption algorithm; hide terminal identity such as the group signature by certain anonymous algorithm; and preserve data secrecy by symmetric or asymmetric encryption algorithm.

Regarding encryption algorithm, security in the perceptual layer can be categorized into terminal identity security and interactive data security.

Terminal identity security, aided by the cooperation of the distributed node and products, manages and destroys the terminal key for fast identification of any terminal. The anonymous algorithm can be used to hide the terminal real identity if timeliness and legality are ensured. The agency may rollback and inspect its identity if necessary.

Interactive data security ensures that the data generated or forwarded by the terminal are not intercepted by unauthorized access. The common information with encryption algorithm protection prevents data that are cracked, abandoned, replayed, and so on, which come from middle attackers during the relay process. Sensitive information of some nodes (e.g., the current position) can be hidden by anonymous algorithm in case of a crack from the attacker.

Measures to secure the identity of the terminal and guarantee data security are not only inadequate. These measures also need to develop ways to control and manage easily the behaviour of the object. Such methods are necessary especially in the perceptual layer, which has incomplete control. This part is referred to as control and behaviour security. In this study, we define behaviour as a combination of object identity, data, and operation.

To achieve security behaviour, several steps must be undertaken. The first step is risk assessment, which examined every possible threat and weakness within security mechanisms and nodes. After completing the identity security and data security mechanisms discussed above, we use an effective intrusion detection mechanism to detect malicious behaviours. Fast processing of detected abnormal events is key to achieving control security and lowering the weight of malicious nodes and mechanisms. In this manner, the known and unknown malicious attacks can be inhibited, and the availability of the system can be ensured.

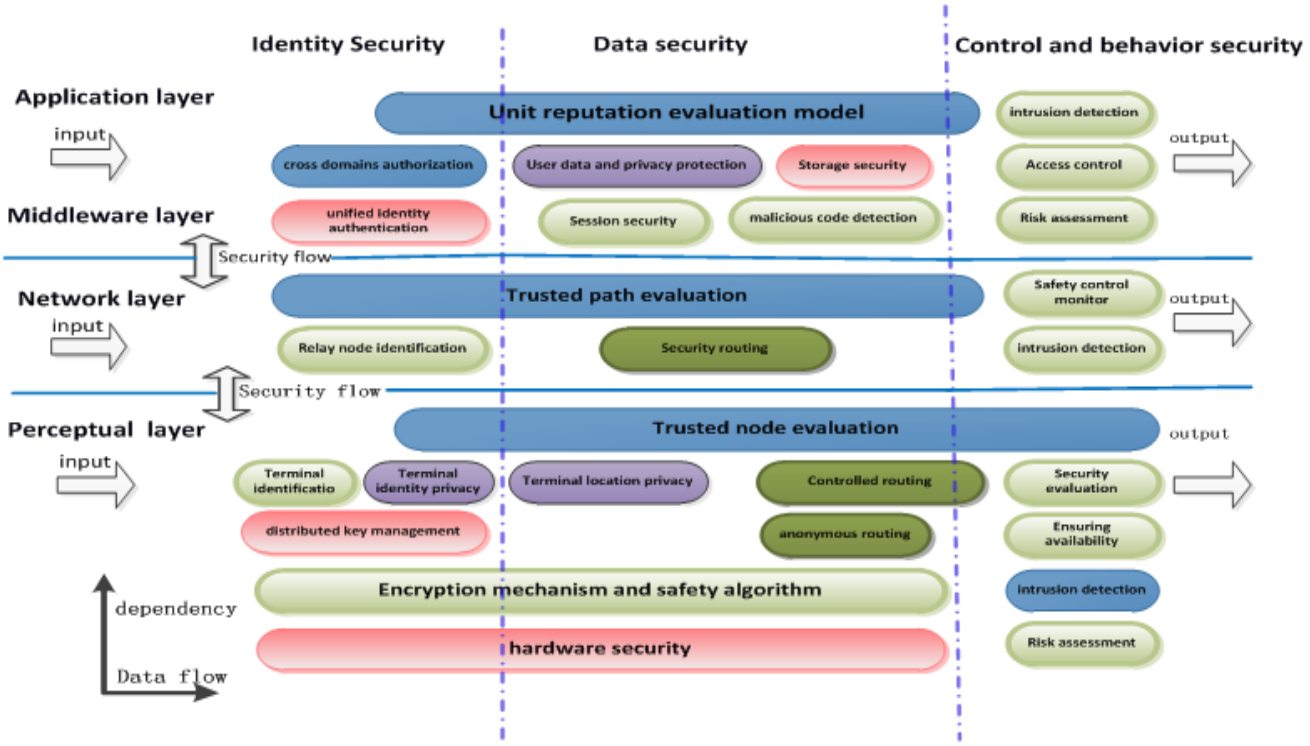

Fig. 3 A hierarchical security architecture.

2). Security module in the network layer

The security module in the network layer solves routing security problems in heterogeneous and integrating networks. The intermediate node selects a reliable path by using the local information in distributed environment. First, the authentication technology ensures the identity legitimacy of the middle transmitting node. Security routing technologies are then employed to ensure data secrecy and integrity in the forwarding process. Intrusion detection and security monitoring management platform are employed to detect and avoid any malicious incident.

Increased attention should be given to logical inconsistency and heterogeneity. These characteristics are observed in the fusion of multi-source networks although the general security technology stays the same in this layer.

3). Security in the application and middleware layers

Here, the application layer and the middleware layer are merged and use relatively unified protective mechanism as their environment. These layers ensure that the interaction of institutions and applications is legal and can be trusted. The identity security of these layers is similar to that in the network layer, which focuses on identity identifiability. The difference is that these layers focus on the cooperation authentication between multiple services. To illustrate, service a needs to check whether the user of service B exists and has related access. This situation is similar to having an open ID that is well supported by popular Internet services.

Various aspects of data security are considered in these two layers. First, service needs to use several technologies such as safe programming and anti-virus software testing. The purpose is to identify service loopholes and all kinds of malicious codes from malicious attacks as well as to qualify the security of the service itself. Second, the data are verified and a temporary cache is developed to prevent attackers with malicious operations or request data attacks. Third, in attacks of hijacking and redo sessions, a session inspection mechanism is established for two or more requests from the same source. Fourth, boundary inspection, data encryption, access control, and similar measures are employed to avoid privacy leakage within the user data to attackers. Regarding control security, risk assessment, access control, and intrusion detection analyse, match, and control for service loopholes and malicious behaviour modes.

However, the main challenge faced by securities in these two layers is the introduction of new techniques in mass application (e.g., cloud computing and virtualization). These techniques have caused substantial changes in the traditional security mode. For example, the user data of a previous independent server may be isolated. However, once virtualized, attackers can use loopholes in virtualization facilities to acquire illegal access to data belonging to another user. Such access consequently violates data privacy and integrity. This area of study belongs to cloud computing security.

The availability of equipment, data, and service is an important aspect of IoT application. The control mechanism of the vertical structure can protect layers from DoS attack. The lateral preventive mechanism in the three layers roughly follows a similar pattern in which intrusion detection (e.g., the honeypot technology, statistical analysis, and anomaly detection caste system) is first employed to determine the presence of an invader. Corresponding measures are then applied using the predefined or dynamic security management strategy.

In the subsequent section, we present the entire frame, marking each module by colours. Light green indicates that mature research results studies have been obtained, providing the foundation, Red indicates widely researched modules. Dark colours are used to mark the remaining modules, indicating a limited number of studies. However, these modules are the vital parts of the entire architecture.

4.3 Brief summary of security architecture

Vertically, the hierarchical security architecture can isolate different subjects in a complicated environment and can analyze relevant safety technology in a relatively closed application and attack scene. Horizontally, in the same layer, security mechanism sorted by the processing sequence of the flow of data consists of identity security, data security, and control security.

A brief analysis of the structure of the security architecture is as follows: First, compared with those in other layers, the security in the network layer is the simplest because of its controllable and closed backbone network and ripe technology. Second, although the environment of the application layer is open, its mature infrastructure (e.g., Web and database server and the operating system) as well as the absence of a unified security mode for its relationship with the realization prompted numerous studies on its security technology.

With regard to the middleware layer, the important technology is cloud computing. Whereas the technology itself remains incomplete, security technology (especially for user data and privacy protection) is the focus of related field research.

By contrast, the environment of the perceptual layer is the most complicated for several reasons. First, various perceptual network determine the difficulty of using only one kind of security technology. Second, the perceptual environment is open, and thus, security measures previously used in closed environments can cause problems in the open environment. Finally, limited resources, weak performance, and heterogeneity of several perceptual nodes can lead to numerous security problems. Therefore, the security technology in the perceptual layer is the most urgent aspect of the entire research and crucial to ensuring security of the entire system. However, related studies on these characteristics of the perceptual layer are limited. Thus, security research on the perceptual network is essential.

From the perspective of application logic, the perceptual layer and the application layer of the mechanism are closely related. Therefore, perceptual security must be viewed along with the security of the entire system, instead of separating such from the security of other layers. For example, privacy protection, terminal identity privacy, and location privacy of the perceptual layer are closely associated with storage security and user data privacy protection in the application layer. Intrusion detection also needs the subject cooperation of crossing layers to identify malicious terminals, facilities, and institutions effectively.

5 Conclusion

In this study, we analyze the possible security threats in each IoT layer. We then present a refining security subject that can guarantee application security corresponding to identity, data, behaviour, and control. We describe a detailed process of module security interaction. We also propose a 2D security architecture in which the vertical division narrows down the complexity of the cross-layer security interaction, and the transverse division based on data flow clears the processing logic of the security mechanism. This study elucidates the core of the entire security technology of IOT.

Acknowledgment

The authors would like to thank the anonymous reviewers for their invaluable feedback. This work is supported by National Natural Science Foundation of China (NSFC) under grant No. 61173145, the National Grand Basic Research Program (973 Program) of China under grant No. 2011CB30260.

Reference

[1] P. Castillejo, J.F. Martinez, L. Lopez, G. Rubio, An Internet of Things Approach for Managing Smart Services Provided by Wearable Devices, International Journal of Distributed Sensor Networks, Volume 2013 (2013), Article ID 190813, 9 pages, http://dx.doi.org/10.1155/2013/190813

[2] H. Rowaihy. Location Privacy and Energy Preservation in Sensor Allocation Systems. International Journal of Distributed Sensor Networks Volume 2012 (2012), Article ID 197592, 10 pages doi:10.1155/2012/197592

[3] Ding Chao, Lijun Yang, Meng Wu, Security Architecture and Key Technologies for IoT/CPS, ZTE Communication, 2011,17(1):11-16

[4] Xin Ma, Quanyi Huang, Xueming Shu, Wei Ma, Quanlai Zhao, Study on the Applications of Internet of Things in the Field of Public Safety, China Safety Science Journal, 2010, 20(007):170-176

[5] Leusse P, Periorellis P, Dimitrakos T, Nair S K, Self-Managed Security Cell, a security model for the Internet of Things and Services, in Advances in Future Internet, 2009 First International Conference on, 2009:47-52

[6] Zhenqiang Wu, Yanwei Zhou, Jianfeng Ma, A Security Transmission Model for Internet of Thing, Chinese Journal of Computer, 2011, 34(8):1351-1364

[7] Yanbing Liu, Wenping Hu, Jiang Du, Network Information Security Architecture Based on Internet of Things , ZTE Communication, 2011, 17(1):17-20

[8] Li Guo, Bo Yan, Yan Shen, Study on Secure System Architecture of IOT, Information Security and Communications Privacy, 2010, 73-75

[9] Hong Yu and Jingsha He, Authentication and En-route Data Filtering for Wireless Sensor Networks in the Internet of Things Scenario, International Journal of Grid and Distributed Computing, 2013, Vol. 6, No. 1, 1-12,

[10] Hui Xu, Chunzhi Wang, Wei Liu and Hongwei Chen, NETCONF-based Integrated Management for Internet of Things using RESTful Web Services, International Journal of Future Generation Communication and Networking, 2012, Vol. 5 No.3, 73-82

[11] HuiDan Gao,YaJun Guo, JianQun Cui, HengGeng Hao and Hui Shi, A Communication Protocol of RFID Systems in Internet of Things, International Journal of Security and Its Applications, 2012, Vol. 6, No.2, 91-102