The Research of Access Control Based on UCON in the Internet of Things

Zhang Guoping
School of Computer and Communication Engineering in China University of Petroleum, Dong Ying, China
Email: zhanggp@upc.edu.cn

Gong Wentao
Internet and Education Technology Center in China University of Petroleum, Dong Ying, China
Email: gongwt@upc.edu.cn

Abstract—**In this paper, we introduce the internet of things and related architecture and protocols, and the family of usage control (UCON) models, which integrate authorizations (A), obligations (B), and conditions (C). The UCON is a generalization of access control to cover authorizations, obligations, conditions, continuity (ongoing controls), and mutability. In the internet of things' highly dynamic, distributed environment, obligations and conditions are also crucial decision factors for secure controls on usage of resources, such as digital resources for cars and other moving devices and so on. In order to meet the needs of privacy and authorization flexible access control in the internet of things, we propose the access control policies based on UCON to meet the needs of requirements for security authorization and control.**

Keywords—the internet of things, usage control model, access control, authorization policies

I. Introduction

IOT (the internet of things) [1], [2], [3] has developed much faster than ever before, it will bring us opportunities for new personal life styles due to its rapid development of information technology, but it also has raised several new challenging issues [4], [5]for reliable and trusted controls on the usages of resources in IOT throughout their life cycle, and thus the access control has been the important factor to the development of IOT, all the traditional access control models just like MAC (Mandatory access control) [6] and DAC (Discretionary access control) [7] are not suitable for access control in open network environment such as IOT, they are facing a problem as follows: the access control process cannot be carried out smoothly due to their diversity of access policies.

In order to solve the problem above, the security researchers Park and Sandhu propose the UCON (usage control model) in 2002 [6], [7], [8]. UCON proposes a lot of concepts based on the traditional access control, such as subject and object in access control model, and attributes of them, and authorization (A) and obligation (B) and condition (C) [9] and so on. UCON has strong safety performance functions, using a variety of restrictions to make sure the secure in the access control. However, the solution for the access process in IOT is still not enough: firstly, UCON is still lack of exact representation of its precise definition [10] and authorization process [12] in IOT; secondly, UCON doesn't give the detail description [13], [14] for access process in IOT; finally, UCON is only a conceptual model and the actual construction in IOT needs much more research.

In this paper, the architecture of IOT and abstract of each part has been proposed in section 2, and the architecture and abstraction of usage control model in IOT are given in section 3, and assessment of the application service and the overall access process of access control are also proposed in the section, and the small examples are given in section 4, and the whole paper is summarized in section 5.

A. The Internet of Things Viewpoints

IOT (the internet of things) means the network, which contains radio frequency identification (RFID) [1], infrared sensors, global positioning systems, laser scanners and other information sensing device. All things in IOT can be connected to internet according to the agreement, and exchange the information, thus to achieve intelligent identification, location, tracking, monitoring and management of a network. IOT is known as "the sensor network" in the international area, which is the concept of sensor networks in an expansion of things. IOT is proposed in 1999, and the popular concept of IOT is "connected to the Internet of Things", which contains two meanings: firstly, all core and foundation things in IOT are based on Internet and IOT is the expansion and extension of Internet; secondly, IOT develops broader and deeper than that of Internet, it can make things exchange information between themselves anytime and anywhere. IOT represents the new direction of information technology, the research of IOT has involved a wide and broad development prospects.

The concept of Internet of Things (IOT) is proposed by Foundation of Auto-ID center of MIT (RFID technology) [2].In 2003 SUN's article: Toward a Global "Internet of Things" (Via).

The trend of IOT is the rapid generation of information technology, specifically, to embed sensors and equipment to the power grid, railways, bridges, tunnels, roads, buildings, water systems, oil and gas pipelines and other objects, and then the IOT integrate with the existing internet to achieve human society and the integration of

doi:10.4304/jsw.6.4.724-731

physical systems, which is in the integrated network. There is a strong central ability of super-computer cluster to integrate and control the network in real time, such as people, machines, equipment and some other infrastructure network. Meanwhile, IOT also raises many security issues, such as authorization security and privacy protection. In the industry, IOT is recognized as three levels, the underlying perception of sensory data is used to the upper layer, the second layer is the data transmission network layer, and the top is the application layer. The network layer in the access control is in the face of more and more complicated role among the subjects and the objects than ever before. In order to solve the secure problem, the researchers propose access control models to help the resources could only be accessed by the requesters who have passed authorization.

B. Traditional Access Control Viewpoints

The concept of access control and related access control technologies were proposed 40 years ago, with the development of web services and data security requirements, access controls have also been introduced into the internet, simply, access control goal is to ensure safe control in web services, that is, all the access requesters and the service providers' services are being under their control, and service providers can only be authorized by the specific service requester.

There are several traditional access control models, such as discretionary access control (DAC) and mandatory access control (MAC), and Role-Based Access Control (RBAC) [7].All the traditional access control models introduced above are not suitable for access control in IOT's open network environment, and all the traditional access controls are facing a problem as follows: the access process cannot be carried out smoothly due to their diversity of access policies. In order to solve the problem above, the security researchers Park and Sandhu propose the usage control model (UCON) and some other researchers propose digital resource management (DRM) [14], [15], [16] and trust management and other access control technologies.

C. Modern Access Control Technology Viewpoints

In order to protect the digital resources, some researchers propose the technologies such as trust management and digital resources management with the help of public-key infrastructure. All the information about resources are stored and managed by the server, and there are some industry initiatives such as Intel-driven Trusted Computing Platform Alliance (TCPA) and Microsoft's Palladium, both TCPA and Palladium have gained serious attention due to their secure potential impacts on privacy, and the protection impacts on security problems as well as DRM. DRM technologies emerged nearly twenty years ago and gained much attention recently, and DRM will provide a foundation for more trusted and secure computing environment with comprehensive modern models (such as UCON) and access control policies.

UCON fundamentally improves the traditional access control models introduced above, it includes the subjects and the objects and the rights of three basic elements, combined with authorization (A) and obligation (B) and condition (C) and so on. UCON has sixteen strong safety performance functions, just as preA and preB and PreC [7] and so on.

In order to meet the needs for open network environment in access control, UCON introduces two new important features: continuity and mutability. In traditional access control models, authorization decisions for access control are generally made prior to the access control, and only very few changes after the access control, such as the decision for the access control in discretionary access control model is based on the existing access control lists, as long as the value in the matrix of access control list is true, the permission for access control is promised, or else the request is denied. The decision for the access control will not be changed during the access control, and the value of matrix can only be changed by the administrator after the access control. In today's IOT access control, in particular, having relatively long-term continuous service to immediately revoke the usage or application service needs permission. The attributes of the subjects and the attributes of the objects are only changed after the access control in the traditional access control models, thus the UCON model introduces concept of mutability, it means the value of subject's attributes and the value of object's attributes could be changed not only after access control, but also during the access control, and the changes in the attributes will affect the permission in the subject's next access behavior. In the traditional access control models, such as in mandatory access control the permission is made before the access control and the decision for access control is made by comparing the security level between the subject and the object, and the permission is made before the access control and couldn't be changed, thus couldn't meet the needs for the strict and secure control in IOT access control, the subjects' access behavior could do harm to the objects in IOT, thus the permission must be changed during the access control.

II. The Architecture of IOT

The IOT is a term which was first introduced by the MIT Auto-ID Center in 1999. IOT has received much attention not only in the industrial but also in academic areas recently. Many key information technologies such as middleware and sensor networking are now available and expected to become widely applied.

The core technologies of The IOT includes radio frequency identification (RFID) devices, WSN(wireless sensors network) networks, infrared sensors, global positioning systems, Internet and mobile networks, network services, industry applications. The IOT is composed of millions of heterogeneous devices, such as sensors, smart cards and so on. These devices will not only simply convey information but also process the information in transition. IOT should have three characteristics, firstly, IOT is easy to fully aware, using RFID and sensors technology, such as two-dimensional code to catch the information about the access to objects at anytime and anywhere; secondly, IOT is reliable delivery, through the integration of telecommunications networks and the internet, real-time information about the object is accurately passed on; thirdly IOT is the kind of intelligent process, IOT makes use of cloud computing and fuzzy recognition and other intelligent computing technology, using the massive data and information analysis to achieve the intelligent control.

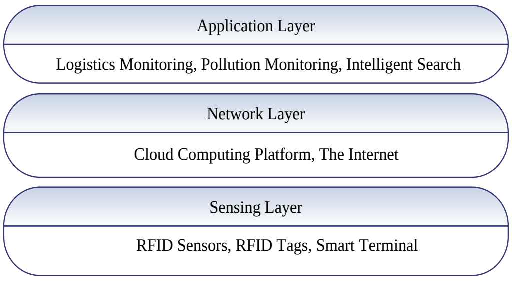
Application Layer
Logistics Monitoring, Pollution Monitoring, Intelligent Search
Network Layer
Cloud Computing Platform, The Internet
Sensing Layer
RFID Sensors, RFID Tags, Smart Terminal

Figure1. Architecture of IOT

In the industry, IOT have generally been recognized as three layers shown in Fig.1: the top is the application layer, it provides the people with the application services; the middle layer is data transmission network layer, it changes the date between the devices; the third layer is sensing layer.

A. Sensing Layer

Sensing layer consists of sensors and some other data acquisition equipment, including access to the data before the sensor network gateway.

Current application in RFID networks draws much more attention than that before, IOT uses RFID scanner to identify the RFID tags on the device and get the information about it. The sensor layer of IOT is the perception of things, and devices in this category were detected by RFID tags. The related technology has been used in highway toll collection systems and supermarket warehouse management systems. RFID also can be used in battlefield information collection for smart dust network; sensing layer consists of smart sensor nodes and access gateways, intelligent node sensing information (including temperature and images and so on).The information in smart dust network is translated to the upper network at the access point, and the sensor information in its gateway will be collected through the network layer and submitted to the background. The related technology has been used in environmental monitoring; pollution monitoring and some other applications.

Perceptual layer is the basis of the development and application in IOT, and the related technology contains such as RFID technology, sensor and control technology, and short-range wireless communication technology and so on. Perceptual layer contains chips, communication protocol, RFID materials, electricity and other subdivision of intelligent nodes. There are some protocol research institutions, such as Berkeley University abroad, and Xi'an advantage of microelectronics in china, and “Tang Core One” is the first piece of domestic self-developed short-range communications chips of things, the company named Perpetuum’s independent power supply for wireless nodes have been developed by collecting vibrational energy-powered products, the company named Powermat also launched a wireless charging platform.

B. Network Layer

The network layer of IOT is built on existing mobile communication network and internet, it contains a variety of mobile communication networks, and its related technology has been used in the internet connected mobile payment systems such as credit card facilities and the RFID phone information collection system. The network layer authentication certificate can also be used to complete the background stock arrives from the bank network.

Network layer also includes information stored query, such as the network management functions and so on. The perception of the network layer of data management and processing technology is a data-center core technology in IOT. Network layer contains many technologies such as aware data management and processing technology, including sensor network data storage, retrieval, analysis, mining, data understanding and perception-based decision-making and behavior theory and technology.

C. Application Layer

The application layer provides users with the services by the perception of data analysis and processing, and the services contains control-type applications (logistics monitoring, pollution monitoring), query type (intelligent retrieval, remote meter reading), control type (intelligent transportation, intelligent home, street light control), scan type (mobile wallet, of highway parking) and so on.

The application layer is the purpose of development of IOT; intelligent control technology will provide users with a variety of physical networking applications. Various industries and home applications will drive the development of the popularity of IOT, and the whole industry chain of IOT will bring profits.

There are already many application areas in application layer, such as through a sensor senses to trigger an object’s information, and then completed by setting a series of moves through the network. When you take the car keys to go to work in the morning, and the sensor standby a computer will detect automatically and launch a series of events: tell you the weather report today and the computer will display the fastest path of driving, and instant-message will be sent to your colleagues that you will soon reach the company. Other examples about the application of IOT have been put into pilot operation of the highway toll collection system and RFID-based mobile wallet payment applications.

III. UCON Model in IOT

The paper’s framework is based on a network layer design between application layer and sensing layer, and set the subject in the usage control as service (service which means application services such as digital sources and information services and so on) which lays in the application layer, and set the object in the usage control as device (device which means cars and the others moving devices contains sensor and so on) which lays in the sensing layer, We pay our attention on the these core subjects and objects, and leaving precise realization of WSN and other important but second-order issues for later work.

The architecture of UCON model and the abstraction of usage control (UCON) model in IOT are given in the section.

A. The Access Control Architecture in IOT

The Access Control Architecture in IOT gets expansion on the basis of Services-Oriented Architecture (SOA) and introduces trust management center and access control model. Therefore, it contains the device (D), service (S), trust management center (TMC), and registration center (RC) and access control model (ACM) which are shown in Fig.2.

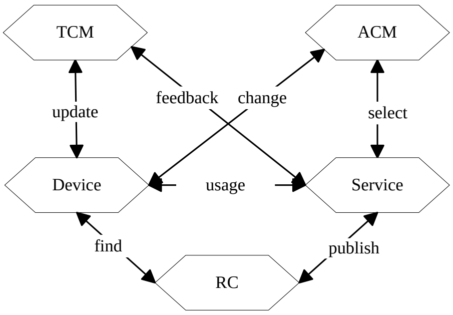

Figure2. Access Control Architecture in IOT

The entire Device's trust degree and Service's trust threshold values are administrated by the trust management center, and all the Service's properties are published at the registration center in the certain wireless sensor network, and all the devices in the same wireless sensor network have to find and apply the service at the registration.

The usage decision for the access control is made between the Device and the Service according to the certain access control policies, using the Device's trust degree and the Service's trust threshold and some other information. Device (the moving car and some others devices which have the sensor) uses the service sources which is provided by the Service (application service such as the information query services which are very useful in mobile and hoc networks and so on) .

There are many kinds of traditional access control models (such as discretionary access control and mandatory access control and so on) in the wireless sensor networks, so it's difficult to make the reasonable decision for the access control between the different wireless sensor networks, in order to solve this problem, access control model is responsible for the management of all the Device's access control properties, and access control model changes them into the unifies usage control model.

Trust management center is responsible for the management of devices' trust value after each time of usage control according to services' feedback, the workflow of usage control comes as following: the device uses the application service provided by the service firstly; the service feedbacks the devices' behavior to the trust management center secondly; the trust management center calculates and updates the device's trust value which applies for the application service according to the certain access control policies.

B. The Usage Control Model in IOT

The abstration of UCON model in IOT is shown in Fig.3.

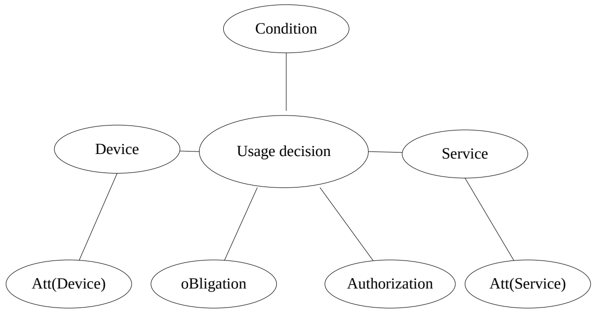

Figure3. Usage Control Model in IOT

The subject(S) of UCON in IOT is the Device(D), which is the control of the application service, such as cars and some other moving devices which contain the sensor to indenty the information.

The attribute(S) of UCON in IOT is the Att(Device), which contains the information about the trust value of the device, and the honest usage times of the application services, and dishonest usage time of the application services, and some other properties and so on.

The subject(O) of UCON in IOT is the Service(S), which lays in the application layer and requests the service information provided by the services locates the wirless sensor network.

The attribute(O) of UCON in IOT is the Att(Service), which contains the service information such as the digital sources for the car and so on.

The condition(C) of UCON in IOT is decided by the policies according to the wireless sensor network, such as the trust value and other decision factors and so on. The condition(C) is the constraints according to the actual situation in wirless sensor network, such as limits of geographical location and so on.

The oBligation(B) of UCON in IOT is according to the needs of the wireless sensor network, if the application services need advertising the information, then the device which uses the information sources has to help the services with advertisment. The obligation of the device should do before or during the usage control in IOT.

The Authorization(A) of UCON in IOT is set by the needs of usage control, and decided by the device and the service. The Authorization(A) is the functional predicates should be evaluated for usage control, and then returns whether the device has rights to use the application service.

The most important properties in the usage contorl based on the trust value, such as Device's trust value and Servce's trust threshold.

In order to make sure the secure of the usage control in the access control in the IOT, UCON model introduces sixteen models, there are seven models for Authorization(A): such as preA(0), preA(1), preA(3), onA(0), onA(1), onA(2), onA(3); and seven models for oBligation(B): such as preB(0), preB(1), preB(3), onB(0), onB(1), onB(2), onB(3); and two models for condition (C):such as preC(0) and onC(0).

The ABC models could be used together according to the wirless sensor network situation in IOT. UCON also introduces the concepts of continuity of decision and mutability of attributes.

C. Assess process of Device and Service

We choose two important factors in The Free-space Model, which means the propagation loss (PL) and propagation distance (PD).

Assess process of device and service comes as following:

The first step: Some devices that have the certain usage of the application service are selected in the same wireless sensor network, and based on the reliability of service, the assessment for the application service is given by them, and assessment value of service can be obtained.

The second step: The assessment for the application service is given by the trust management center. Based on the reliability of device, assessment value of service can be obtained.

The third step: According to the assessment value of the trust management center and the assessment value of devices and the weight of trust management center and the device, assessment of the trust management center and device can be obtained.

The fourth step: set certain trust degree to the device that have the usage of the service, and decision for the usage control will be made based on trust and some other combination of policies according to the situation in the wireless sensor network.

Assuming there are M devices (such as car which has sensor, and the information distinguish by the sensor scanner) and N services (such as digital source which services for the moving devices) in the wireless sensor network, then the assessment for the application services comes as followed.

Set the devices' field of assessment for service named F (Field) comes as followed:

$$F = \{ f_1, f_2, \cdots, f_t \} \qquad (1)$$

Indicate that recognition of the extent of device, each one corresponds to a fuzzy subset of the class, t is the number of reviews grade field, t normally takes an odd number to make sure the judgment has an intermediate value.

Set the fuzzy relationship matrix of device named M (Matrix) as following:

$$M = \begin{bmatrix} m_{11} & m_{12} & \cdots & m_{1n} \\ \cdots & \cdots & \cdots & \cdots \\ m_{m1} & m_{m2} & \cdots & m_{mn} \end{bmatrix} \qquad (2)$$

The paper is to assess the application service, and the assessment is given by the moving devices, the fuzzy relationship matrix including the M devices to assess the N application services' trust assessment vector, and set $m_{ij} = (f_{ij1}, f_{ij2}, \cdots, f_{ijt})$ which indicates that the level of trust for the i-th device giving to the j-th application service. The device makes his assessment according to the propagation loss (PL) and propagation distance (PD) of application service's reliability trust, then the credibility assessment of the corresponding components of a vector is 1, and the rest is 0. For example, in five level field named F= {absolute trust, likely trust, not clear, less trust, distrust}, when its counterpart is (1, 0, 0, 0, 0), and the assessment is "absolute trust".

Set the trust fuzzy vector of device named device field (DF) as following:

$$DF_i = (DF_{i1}, DF_{i2}, \cdots, DF_{it}) \qquad (3)$$

DF means the assessment of fuzzy vector for the i-th service, which is given by all of the other devices, and is calculated as following:

$$DF_{ik} = \sum_{j=1}^{m} f_{jik} / \sum_{j=1}^{m} \sum_{k=1}^{t} f_{jik} = \sum_{j=1}^{m} f_{jik} / m \qquad (4)$$

Set the trust fuzzy weight of device named device weight (DW) as following:

$$DW = \{dw_1, dw_2, \cdots, dw_t\} \qquad (5)$$

DW means that peer assessment in the wireless sensor network of each level according to the weights such as (1, 0.8, 0.6, 0.4, 0), set fuzzy weights of the trust as in the five level domain F= {absolute trust, likely trust, not clear, less trust, distrust}, when the assessment is "not clear", the value is 0.6.

Set the trust value of device named device estimation (DE) as following:

$$DE_i = \sum_{k=1}^{t} dw_k * DF_{ik} \qquad (6)$$

The paper contains two kinds of DE values in the wireless sensor network, which are DE_l (means the value of propagation loss) and DE_d (means the value of propagation distance).WDL (Weight of propagation Distance and propagation Loss) means the weight of two factors due to value of device's trust value in the wireless sensor network. The calculation of assessment given by the devices for the application service named DE_{dl} comes as followed:

$$DE_{dl} = DE_d * WDL / (1 + WDL) + DE_l / (1 + WDL) \qquad (7)$$

Set the fuzzy relationship matrix of trust management center named trust matrix (TM) as following:

$$TM = \begin{bmatrix} tm_1 & tm_2 & \cdots & tm_n \end{bmatrix} \qquad (8)$$

The fuzzy relationship matrix of trust management center contains authority for those domain N vectors of the application service the authority of the assessment of TF (Trust management center Field); set $tm_i = (f_{i1}, f_{i2}, \cdots, f_{it})$ to express the assessment to the i-th application service given by the trust management center in the wireless sensor network.

Set the trust fuzzy vector of trust management center named TF as following:

$$TF_i = (TF_{i1}, TF_{i2}, \cdots, TF_{it}) = (f_{i1}, f_{i2}, \cdots, f_{it}) \qquad (9)$$

TF means the evaluation of fuzzy vector for the i-th service given by trust management center, and is defined similar to DF.

Set the trust fuzzy weight of trust management center named TW as following:

$$TW = \{tw_1, tw_2, \cdots, tw_m\} \qquad (10)$$

TW means that assessment in the domain of each level corresponding to the weights given by the trust management center, and is defined similar to DW.

Set the trust value of trust management center named TE, and TE is calculated as following:

$$TE_i = \sum_{k=1}^{m} tw_k * TF_{ik} \qquad (11)$$

The paper contains two kinds of TE values in the wireless sensor network, which are TE_l (means the value of propagation loss) and TE_d (means the value of propagation distance).WDL is defined before, then the calculation of assessment given by the trust management center for the application service named TE_{dl} comes as followed:

$$TE_{dl} = TE_d * WDL/(1+WDL) + TE_l/(1+WDL) \qquad (12)$$

DTT (weight of Device To Trust management center) means the weight of device factors to trust management center in the wireless sensor network. Assessment of device and the trust management center for application service named TDT (Trust value of Device and Trust management center) is calculated by the following formula:

$$TDT = DE_{dl} * DTT/(1+DTT) + TE_{dl}/(1+DTT) \qquad (13)$$

And TDT will be granted to the application service as their trust threshold, only when the device's trust degree is higher than that of the application service, the device is able to access the service, or else the usage control will be denied. Taking consideration of the length of this paper, no further discussion goes on.

D. Process of Access Control in IOT

The process of access control in IOT is shown in Fig.4, the core objects contains device, which is the subject of usage control in IOT, such as moving car and some other devices; the core objects also contains application service, which is the object of usage control in IOT, such as the digital information provided by the wireless sensor network.

The process of the access control comes as following:

The first step: The device queries the application service in WSN, and requests for the usage control in the registration center. Comparing the trust value of the device and trust threshold of the application service, and if the condition meets (the device's trust value is higher than that of the application service's trust threshold), then the request is promised, turn to the second step; or else, turn to the seventh step.

The second step: The device uses the application service, and the information get from the device is used by the sensor, and the application service sends the device's feedback to the trust management center after the usage control.

The third step: The trust management judges whether the access control is honest according to the feedback of the application service, and if the access control is honest, turn to the fourth step, or else turn to the fifth step.

The fourth step: The usage controls is honest, and trust management center records the information about the application service and the device, including the honest times of the usage control and the value of the trust value, and the online time using the device.

The fifth step: The usage controls is dishonest, and trust management center records the information about the application service and the device, including the dishonest times of the usage control and the value of the trust value, and the time online using the device.

The sixth step: The trust management center updates the device's information and the application service's information, such as the trust value of the device.

The seventh step: The usage control is end.

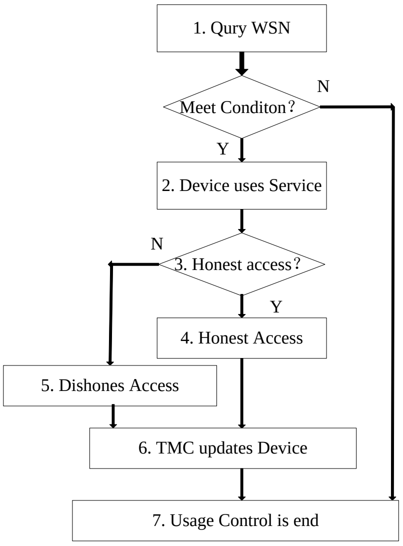

Figure4. Assess process of Device and Service in IOT

IV. The Experiments

Two experiments are introduced here, the first experiment is about the assessment of the trust value of the service application in the wireless sensor network; and the second experiment is about the usage control model description in usage control function models in IOT.

A. Experiment One

In experiment one, assuming the initial DW= {1.0, 0.8, 0.5, 0.4, 0.2}; TW={1.0, 0.7, 0.6, 0.5, 0.3}; and set five levels domain F= {absolute trust, likely trust, not clear,

less trust, distrust}, and there are five devices named D1, D2, D3, D4, and D5 respectively, and there are five application services named S1, S2, S3, S4 and S5 in the wireless sensor network respectively, an example for application service trust threshold assessment of trust management center and devices comes as following:

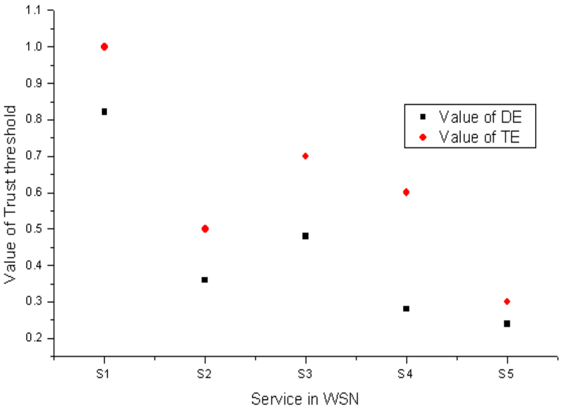

Figure5. Assess process of Service

Set the fuzzy relationship matrix of device named M as: device D1 sets S1 as “absolute trust”; device D1 sets S2 as “not clear”; device D1 sets S3 as “not clear”; device D1 sets S4 as “distrust”; device D1 sets S5 as “distrust”.

Device D2 sets S1 as “absolute trust”; device D2 sets S2 as “distrust”; device D2 sets S3 as “not clear”; device D2 sets S4 as distrust”; device D2 sets S5 as “distrust”.

Device D3 sets S1 as “likely trust”; device D3 sets S2 as “not clear”; device D3 sets S3 as “not clear”; device D3 sets S4 as “less trust”; device D3 sets S5 as “distrust”.

Device D4 sets S1 as “likely trust”; device D4 sets S2 as “less trust”; device D4 sets S3 as “not clear”; device D4 sets S4 as “less trust”; device D4 sets S5 as “less trust”.

Device D5 sets S1 as “not clear”; device D5 sets S2 as “distrust”; device D5 sets S3 as “less trust”; device D5 sets S4 as “distrust”; device D5 sets S5 as “distrust”.

Based on the process introduced above we can get: DF1= {0.4, 0.4, 0.2, 0, 0}; DF2= {0, 0, 0.4, 0.2, 0.4}; DF3= {0, 0, 0.8, 0.2, 0}; DF4= {0, 0, 0, 0.4, 0.6}; DF5= {0, 0, 0, 0.2, 0.8}; and then we can get: DE1= 0.82; DE2= 0.36; DE3=0.48; DE4=0.28; DE5=0.24.

Trust management center sets S1 as “absolute trust”; set S2 as “less trust”; sets S3 as “likely trust”; sets S4 as “not clear ”; sets S5 as “distrust”; then we can get: TE1=1; TE2=0.5; TE3=0.7;TE4=0.6; TE5=0.3; and we can get values of the TE and DE shown in Fig.5.

B. Experiment Two

The second example shows the rich expression of the usage control models in IOT.

Suppose there are the device and the application service in the certain wireless sensor network, and both of them have the properties about trust value, the paper gives the explanation about the access process and the usage control functions, and formal description of this case are as follows:

Subject of UOCN in IOT: Device

Object of UCON in IOT: Service

Attributes (Device): {Device’s trust degree, Device’s money, Device’s honest times, Device’s dishonest times}

Attributes (Service): {Service’s threshold, Service’s number, Service’s money}

Obligation: {feedback the device’s information}

Condition :{ Device.money⩾0∩Device.trustdegree⩾Service.threshold}

Times: Device’s usage times using Service

OLTime: Device’s online time using Service

Expense: Service’s expense each time using Service

Punish: the punishment for device’s trust degree after each dishonest access control

Allowed(Device,Service,R)=>(Device.money ⩾ 0 ∩ Device.trustdegree⩾Service.threshold)

preUpdate(Device.money):Device.money=Device.money- OLTime * Expense

postUpdate(Service.money):Service.money=Service.money+OLTime * Expense

postUpdate (Device. dishonest times): Device.dishonest times = Device.dishonest times +1

postUpdate (Device.trustdegree): Device.trust degree = Device.trust degree- Punish

postUpdate (Service’s number): Service’s number = Service ’s number+1

In this usage control case, the specific attributes of the logical description of a dishonest is presented, the properties of the device and the service can be changed not only after the usage control by Post functions, but also before the usage control by Pre functions.

Money flow properties are updated in real time, the device’s money decreases and the service’s money increases, and the usage time of the services is added one after usage control, the number of the device’s dishonest times is added due to the dishonest feedback given by the service. The properties of the service and the device can be changed in real time, and not only changed before the usage control but also after the usage control and will impact the future permission of usage control, thus authorization of usage control can be more flexible, and more strictly enforce security of the access control in IOT.

V. The Conclusion

In this paper, the several traditional access control models are analyzed. The architecture of IOT model is discussed, and each part of the IOT model is introduced. The abstraction of UCON model in IOT is given, and assessment model based on fuzzy theory in IOT is introduced, and the access control policies and process are proposed. In the end, several small examples are given to verify the strong expression of the usage control model compared with the traditional access control models in the background of IOT.

In our future work, we will explore how to make the usage control model in IOT more effective, further research of the usage control model in IOT will lead to comprehensive and more practical solution for the security in IOT, which can make the authorization for the access control in IOT become easy and feasible.

References

[1] T. Wiechert, F. Thiesse, F. Michahelles, P. Schmitt, E. Fleisch: “Connecting Mobile Phones to the Internet of Things: A Discussion of Compatibility Issues between EPC and NFC”, AMCIS’ 07, Keystone, Colorado, USA, 2007.

[2] T. Kriplean, E. Welbourne, N. Khoussainova, V. Rastogi, M. Balazinska, G. Borriello,T. Kohno, D. Suciu: “Physical Access Control for Captured RFID Data”, IEEE Pervasive Computing ,vol. 6, no. 4, pp. 48-55, 2007.

[3] A. Juels, “RFID Security and Privacy: A Research Survey”, IEEE Journal of Selected Areas in Communications, vol. 24, pp. 381- 394, 2006.

[4] M.Mealling.Dynamic Delegation Discovery System (DDDS)Part Five: URI.ARPA Assignment Procedures.RFC 3401,IETF,October 2002.

[5] R.Moats,“URN Syntax”,RFC 2141,November 1998.

[6] J.Park,R.Sandhu . The UCONABC usage control model[J].ACM Transactions on Information and Systems Security,7(1):128-174,2004.

[7] Xinwei Zhang. Formal Model and Analysis of Usage Control[D].Virginia:George Mason University, 2006.

[8] J.Park,R.Sandhu. Towards usage control models：beyond traditional access control[C].ACM Symposium on Acesscontrol Models and Technologies,2(3) ： 57-64,2002.

[9] J.Park,R.Sandhu . Originator Control in Usage Control[J],Proceedings of the Third International Workshop on Policies for Distributed Systems and Networks(POLICY02),IEEE,60-66,2002.

[10] J.Park,R.Sandhu.Security Architecture for Controlled Digital Information Dissemination, Proceedings of the Sixteenth Annual Computer Security Applications Conference(ASSAC), pp. 224-233, 2000.

[11] Fengying Wang,Fei Wang. The Research and Application of Resource Dissemination Based on Credibility and UCON. 2007 International Conference on Computational Intelligence and Security, pp. 584-588, 2007.

[12] R. Sandhu, E. Coyne, H. Feinstein, C. Youman. Role-Based Access Control Models [J]. Computer, 1996

[13] Somchart Fugkeaw. AmTRUE: Authentication Management and Trusted Role-based Authorization in Multi-Application and Multi-User Environment[C]. International Conference on Emerging Security Information, Systems and Technologies, IEEE, 2007

[14] Ahn GH, Arvisandhu.Role-based Authorization Constrans Specification [L]. ACM Transcactions on Information and System Security, pp. 207-226, 2002

[15] A. Jøsang, R. Ismail, and C. Boyd. A survey of trust and reputation systems for online service provision [J]. Decision Support Systems, 43(2): 618-644, 2007

[16] Su Jin-dian, Guo He-qing, Liu Miao. Trust and Reputation Evaluation Model in Web Services [J]. Computer Engineering and Applications, pp. 127-130, 2006,

Zhang Guoping He is an associate professor in school of computer and communication engineering in China University of Petroleum, Dong Ying, China, he was born in Tangshan, Hebei Province in 1970.He is a master instructor, he gets the computer master in application technology at China University of Petroleum in 2001; he is in the PhD at Ocean University of China in 2010.

He has published many articles which have been indexed by EI, and his main research directions are engaged: information systems integration and information technology, database and data grid.

Gong Wentao He is an assistant engineer in internet and education technology center in China University of Petroleum, Dong Ying, China, he was born in Qianjiang,Hubei Province in 1984. He gets the computer master in application technology at China University of Petroleum in 2010.

He has published several articles which have been indexed by EI, and his main research directions are engaged: access control and date security.