An Efficient Authentication and Access Control Scheme for perception layer of Internet of Things

YE Ning[1] , Zhu Yan[1], WANG Ru-chuan[1, 2], Reza Malekian[3], Lin Qiao-min[1]

[1]Department of Computer Science and Technology, NJUPT, Nanjing , China
[2]State Key Laboratory for Novel Software Technology, Nanjing University, Nanjing, China
[3]Department of Electrical, Electronic and Computer Engineering, University of Pretoria, Pretoria, 0002, South Africa

Abstract In view of the security issues for perception layer of Internet of Things (IoT), an efficient authentication and access control method was proposed. Establishing session key based on Elliptic Curve Cryptography (ECC), it realized mutual authentication between the user and sensor nodes, and process is simple. Also, this method solves the resource-constrained problem of perception layer of the IoT. Attribute-based Access Control (ABAC) method to the resources access of legitimate user enables to achieve flexible fine-grained access control.

Keywords Internet of Things; Elliptic Curve Cryptography; Mutual Authentication; Attribute-based Access Control

I. Introduction

IoT connects objects with Internet through information sensing equipment for information-exchange and communication, to achieve intellectualized identifying, positioning, monitoring and managing. Aim is to have all items connected with the Internet for convenient identification and management [1].It is logically divided into perception layer, transport layer and application layer [2]. The perception layer senses, gathers information, and submits the collected information to the higher application layer for intelligent processing via Internet or other transmitted networks.

The development of IoT is based on wireless sensor networks (WSN) whose basic function is to collect information for the authorized user [3],[4]. Sensor nodes acquire, transmit and process the data of the physical world to achieve accessing the information of things. Most of these sensor nodes are deployed in unmanned environment, and due to lacking of effective protection measures, the signal exposed to the public are vulnerable to malicious attacks. Moreover, sensor nodes are usually equipped with limited computing power, storage, and communication modules [5].WSN cannot adopt encryption technology which needs large amount of computing, and lacks of sophisticated security protection. However, the obtained data may contain sensitive and important information, and therefore is essential for the protection of the security and privacy of the data transmission in the network.

Authentication and access control mechanisms [6],[7] are capable of preventing unauthorized users from accessing the data of sensor nodes on the IoT perception layer, and guaranteeing

the data security effectively. User authentication is to allow legitimate user to access resources as well as to decline malicious person or attacker. After authentication, access control is to restrict authenticated user to access the only data that he has the privileges. However, due to the characteristics of WSN, secure access is faced with more severe challenges.

According to the special characteristics of the sensor nodes, as well as the short length and the relatively limited computing, communications and storage overhead of the symmetric key cryptography (SKC), existing studies show that the authentication and access control of the symmetric cryptosystem is more suitable for the WSN. Banerjee et al. [8] proposed a user authentication that fully based on symmetric key in wireless sensor networks. They leverage the underlying pair-wise key pre-distribution technique to support authenticated querying. Chan-Perrig-Song et al. [9] came up with multiple key enhancement protocol which is in the basis of random key pre-distribution scheme, to enhance the self-recovery capabilities of the node captured. However, SKC is not scalable, requires large memory for storing keys and its pre-distribution scheme complex. Therefore, many scholars have proposed authentication and access control based on public key cryptography (PKC) to overcome these challenges. Tseng et al. [10] proposed an improved dynamic user authentication scheme to enhance the security of wireless sensor networks by withstanding the security weaknesses and to allow legitimate users to change their passwords freely. Wang et al. [11] applied an ECC-based wireless sensor network access control scheme which is a prospective method based on public key cryptography. But this scheme can neither provide mutual authentication between nodes nor resist Dos attack. Yeh et al. [12] proposed a secured authentication protocol for WSN using ECC. Its security was based on the intractability of elliptic curve discrete logarithm problem. Compared with other cryptography, ECC provides better performance, because it can use a smaller key size to achieve the same security.

In this paper, we focus on simple-efficient mutual authentication and secure key establishment based on ECC which has much lower storage and communication overheads. For access control policy, we adopt ABAC-based authorization method. ABAC is a more flexible and scalable that abstract identity, role, and resources information of the traditional access control into entity attributes. Additionally, ABAC can support either fine-grained access control in the complex system or dynamic extension of large scale users.

This paper is organized as follows. Section Ⅱ describes the security foundation for authentication and access control. Section Ⅲ presents our ECC-based mutual authentication and key establishment process, as well as the attribute-based access control policy. Section Ⅳ and Section Ⅴ present security analysis and performance evaluation of the proposed scheme. Finally, section Ⅵ concludes the paper and future research.

II. Security Foundation

1. Authentication

Authentication allows communicating entities to convince the identity of each other and exchange session keys. In WSN, user and terminal nodes in the communication process require mutual authentication to ensure network security, while terminal nodes require authentication mutually to prevent malicious nodes attacks. Encryption mechanism ensures confidentiality to prevent data from being stolen during communication process via encoding

the data. Usually, the authentication is divided into two parts [13] :

a) Authentication: authentication between user and terminal nodes ensures only the legitimate user can access the network.
b) Key establishment: session keys should be created between the user and nodes for secure communication.

2. Access Control Model

Access control is to ensure that resources are only granted to the authorized users [14]. With access control information, it sets the access rights of the subject to the object and protects resources from unauthorized access. To ensure confidentiality and integrity of the system resources is one of the basic security services. Current access control technology can be divided into Role-based Access Control (RBAC) and ABAC [15],[16].

The RBAC [17] defines a set of users and roles. By assigning appropriate role to user to authorize the privileges, the user will have the role permissions to enter the system in a certain role, that is, roles will be associated with the access privileges. The role in the access control plays as a link between the subject and the object. But for IoT perception layer, terminal can be a sensor node or a device. Controlling the resources in the form of user-role is not flexible enough: First, the RBAC itself shows inappropriate aspects in a distributed network environment, such as access control to resources with time constraints. Second, IoT performances the interaction process of information on the perception, and access to resources presents a dynamic and multi-level. But in the RBAC mechanism, once the user is assigned to a certain role, he can just access the resource in a fixed manner.

In ABAC model, the subject and the object all identify through the attributes associated with characteristics. The user is granted appropriate access permissions to the system according to his attributes when he initiates an access request. Unlike RBAC, the ABAC model describes its requestor and the requested resources through attributes, and some restrictions are also described by environmental attributes, which means that all entities in the ABAC can be defined access rights based on any security-relevant characteristics, known as attributes. The associated attributes of each entity can be defined according to the system needs [18].This makes ABAC has sufficient flexibility and scalability to solve fine-grained access control and dynamic expansion of large-scale users in the complex systems, and better adapts to the access control of the Internet of Things.

III. ECC-based Mutual Authentication and ABAC Policy

In this paper, we adopt lightweight ECC to complete the authentication and establish a secure session key. Through mutual authentication between the user and sensor nodes, only legitimate user can access resources. The scheme restricts the privilege of authenticated user by using attribute-based access control policy.

1. Architecture

As shown in Fig. 1, we argue that this architecture is the most suitable model for perception layer of IoT, large number of sensor nodes are deployed in the monitoring area. Pluralities of sensor nodes connect to the transport layer via a respective gateway which is the sensor subnet manager. The main function of the base station (BS) is to gather data and send command to sensor nodes. User is visitor in perception layer, including mobile phones,

notebook computers, personal digital assistant (PDA), etc. The Attribute Authority (AA) exists in perception layer, creating and managing the attribute information. According to the different functions and applications, nodes may have different attributes. Only with appropriate permissions can user access network resources in the case that they through authentication and authorization of the sensor network.

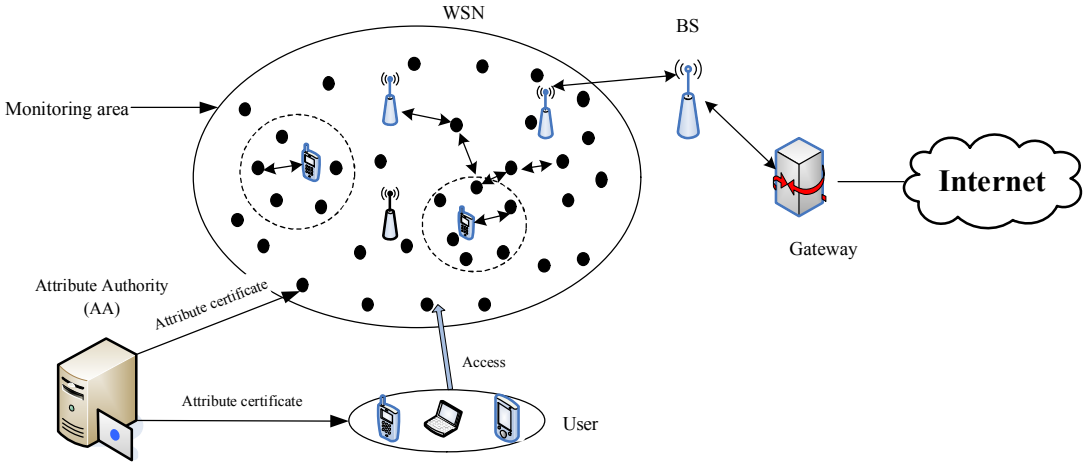

Fig.1. The structure of perception layer of Internet of Things

2. Mutual Authentication based on ECC

Under the same intensity of security, comparing with other cryptography, ECC[19]has many advantages such as less memory occupation and strong ability against the attack .We put forward a method of mutual authentication based on ECC to establish public-private key pairs. What's more, our method can confirm identity in both sides of communication and establish a session key. The authentication includes two phase: initialization phase, mutual authentication and key establishment phase. Notations used are explained in table 1.

Table 1. Definition and Notation

Notation	Definition
U	User
N_i	The i th node
BS	The base station
ID_U /ID_i	The identify of user/ N_i
S_U /Q_U	A secret key/public key of user
S_i/Q_i	A secret key/public key of N_i
F_q	A finite field
E	An elliptic curve defined F_q over a finite field
P	A point on E
K	Session key
s	The secret key of base station
$h()$	A one-way hash function
$\|\|$	Concatenation operation

(1) Initialization Phase

As we known, before the deployment of the WSN, nodes should be initialized [20].Assumed that there are r neighborhood nodes $N_1,N_2,\ldots,N_r$ in the subnet area. The BS generates necessary keys and parameter information: identity, private key, public key, the hash function, elliptic curve and its parameters. First of all, user needs to negotiate with the BS for the secret information used for authentication when he accesses the sensor network. Before presenting our mutual authentication, we describe how the two entities (either two individual sensor nodes or a user and a sensor node) in our network establish their key pairs. The details are as follows:

Initially BS selects a security elliptic curve E over finite field F_q where q is a prime, and selects a base point P with large order p (where p is also a prime).Then BS makes it public to all sensor nodes and users and selects random number $s \in F_q$ as private key, and calculates its public key $P_s = sP$. BS is also responsible to generate all the IDs to the entities in the WSN, each of which has an $ID \in F_q$ through a secure communication channel.

(2)Mutual Authentication and Key Establishment Phase

When user sends a request for information from the WSN, the authentication process is as follows:

Step 1. User U selects an ephemeral key $a \in F_q$, computes $P_U = h(ID_U)$.Private key is generated by user as $S_U = sP_U$, and corresponding public key is $Q_U = aS_U$. Then user sends $\{request, ID_U, Q_U, T_U\}$ to sensor node N_i within his communication range. T_U is generated as a current timestamp by the user. It is assumed that synchronization is guaranteed through appropriate mechanisms.

Step 2. Upon receiving the request from user U, node N_i first checks if the timestamp is valid (i.e by verifying if $T_U \prec T_{now}$, T_{now} is current timestamp).If it is valid, then N_i chooses a ephemeral key $b \in F_q$ and computes $P_i = h(ID_i)$.Then the private key of N_i is $S_i = sP_i$ and the public key is $Q_i = bS_i$. Finally, N_i sends $\{ID_i, Q_i, T_i\}$ to user.

Step 3. When user U receives the message, it check if T_i is valid. If valid, he calculates $Q_U^{'} = aP$ and sends the message $h(ID_U \| ID_i \| Q_U \| Q_U^{'})$ to the N_i.

Step 4. After receiving the message, N_i verifies $h(ID_U \| ID_i \| Q_U \| Q_U^{'})$ .For example, N_i computes $Q_U^{''} = s^{-1}Q_U$, then checks whether $h(ID_U \| ID_i \| Q_U \| Q_U^{''})$ is equal to $h(ID_U \| ID_i \| Q_U \| Q_U^{'})$ or not. If they are equal so N_i completes the authentication of the user. Otherwise, authentication fails. After that, N_i computes $Q_i^{'} = bP$, then it sends $h(ID_i \| ID_U \| Q_i \| Q_i^{'})$ to the user. At the same time, N_i generates the session key $K(h(abP))$.

Step 5. Soon as user receives the message, it computes $Q_i^{''} = s^{-1}Q_i$ and verifies if $h(ID_i \| ID_U \| Q_i \| Q_i^{''})$ is equal to $h(ID_i \| ID_U \| Q_i \| Q_i^{'})$ .If so, N_i is authenticated to user.

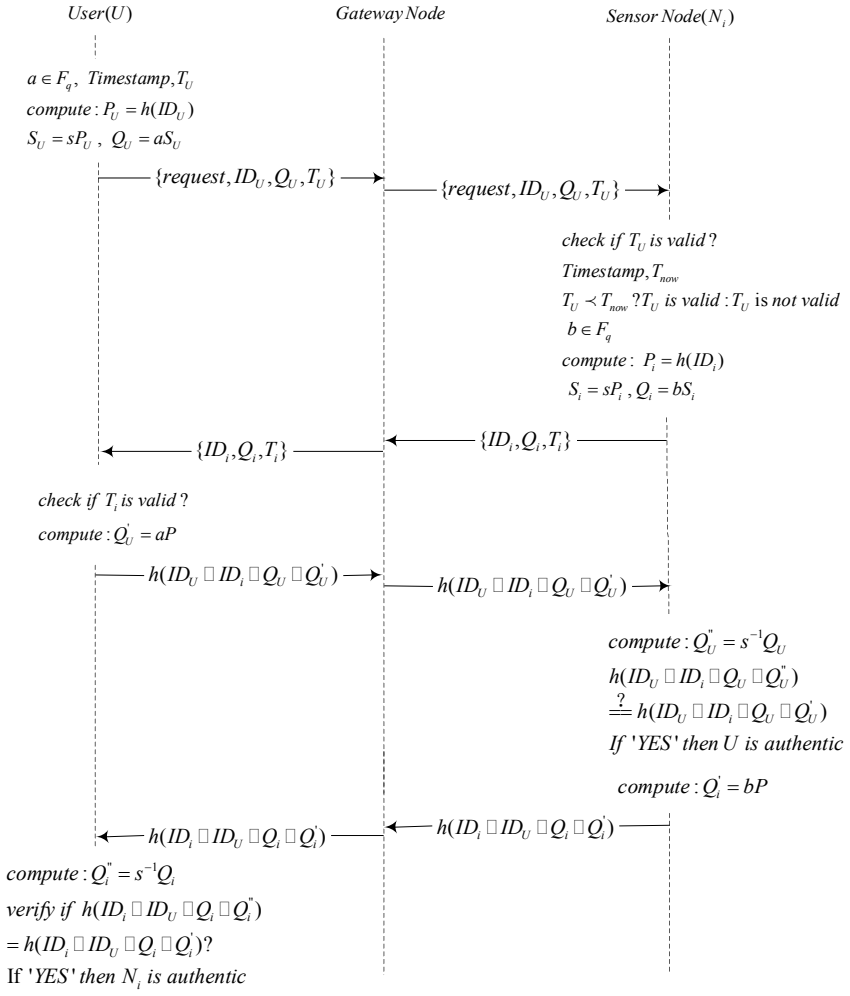

Fig.2. Mutual Authentication Key Establishment Phase

In this way, user U and node N_i are verified the legal identity of each other to achieve mutual authentication and key establishment process, as shown in Fig.2. After authentication, access control will carry on. So the next question is how to authenticate access privilege of

the legitimate user in the IoT. In our paper, we introduce attribute-based access control policy to ensure that only authorized user are given access to certain data or resources.

3. Attribute-based Access Control policy

The main purpose of access control is to restrict the access of the subject to the object, so as to protect the data resources to be used and managed effectively within the legal range[21] .ABAC treat role and identity as characteristics to describe. Moreover, it considers resource attributes, such as the sensitive information. Therefore, we believe that ABAC policy is more fine-grained because it can base on any combination of subject entities, resource and environment attributes.

(1) The Definition of ABAC

Here this paper formally defines the (basic) ABAC policy:

Definition1. IoT entities: User(U)，Resource(R)，Environment(E). User (i.e. mobile users, PDA, notebook computers, client, etc.) is the entity which sends the request of the action to the certain resources. Resources are the requested entities that subject takes action on, such as sensor nodes resources. Environment is context information or situational environment for making a policy decision that may be the current system time.

Definition2. Attributes (A): the set of attributes of users, resources and environments. How to define A is closely related to the specific characteristics of safety. Attributes include identity, name, role, location, data, time etc. Attribute Authority is responsible to the establishment and management of the attributes of users, resources and environment.

$$A=\bigcup_{i=1}^{I} attr_i = \{identity, name, role, date, time, location, ...\},$$

i is all the attributes defined in the Internet of Things

Definition3. User Attributes .User Attributes refers to the user's identity and its own characteristics, indicated by $UA_k (1 \le k \le K)$ .The distribution relationship of the user attributes is expressed in $ATTR(u)$.

$$ATTR(u) \subseteq UA_1 \times UA_2 \times \ldots \times UA_K \text{ , } k \text{ is the all users of the IoT}$$

Definition4. Resource Attributes. Resource Attributes are also called node attributes that is acted upon by the user who can access the resources, express in term of $RA_m (1 \le m \le M)$. The relationship of distribution among the resource attributes is expressed in $ATTR(r)$.

$$ATTR(r) \subseteq RA_1 \times RA_2 \times \ldots \times RA_M \text{ . } m \text{ is all resources of the IoT}$$

Definition5. Environment Attributes. These Attributes describe the context information or situational environment which occurs with $EA_n (1 \le n \le N)$. $ATTR(e)$ indicates attribute assignment relationship for environment.

$$ATTR(e) \subseteq EA_1 \times EA_2 \times \ldots \times EA_N = \left\{ \left(e_{date_1}, e_{time_1}, e_{location_1} \right), \left(e_{date_2}, e_{time_2}, e_{location_2} \right), \ldots, \left(e_{date_N}, e_{time_N}, e_{location_N} \right) \right\},$$

n is defined as all environment attributes in IoT perception layer

Definition6. Access Control Rule. Corresponding to the access request, Policy rule determines whether a user U can access a resource R under particular environment E, and it is a Boolean function. If the Boolean value is true, the user can access the resource. Otherwise, access is refused. We define the rule function as follows:

$$Rule: can\_access(u, r, e) \leftarrow f(ATTR(u), ATTR(r), ATTR(e))$$

(2) Access Control Policy Process

When User U enters into the network, he needs to register in the gateway node so that he can access the data of network nodes.

1) U sends registration requests $\{request, UA_k\}$ to the gateway node.

2) The gateway node verifies whether attribute UA_k is legal. If $UA_k \subseteq A$, user attribute is legal, or the user requests will be refused.

When user launches a request to access node resources in the IoT, he needs to submit his own attribute certificate. According to pre-assigned attributes and user attribute certificate, Nodes determine whether the user is authorized to access the data. If the attributes presented by the user matches with the attributes stored in the nodes, access is granted. Judgment is as follows: The system pre-set threshold value d, and in the circumstances of environment attributes $EA_n = \left(e_{date_n}, e_{time_n}, e_{location_n} \right)$, the same attributes of user and resources (such as sensor node resources) are greater than or equal to d. That is $|UA_k \cap RA_m\} \geq d$ (d is the threshold defined by the system), then the user is authorized to access the resources. Otherwise, the user access is denied.

1) U sends a request to the node N_i with $\{request, UA_k\}$.

2) Once the node N_i who receives the request, it judges whether the user is already authenticated or there is a valid session key, then N_i checks whether the requesting user's attributes are satisfied with that the node owned, namely $|UA_k \cap RA_m\} \geq d$. Finally, node N_i sends a response that includes the requested data $T_B = E_K(m)$ to U. Otherwise it will not give response.

3) When U receives T_B, he decrypt it to achieve $m = DE_K(T_B)$ by using the session key K.

IV. Security Analysis

A. Provide mutual authentication

In this paper, user initiates a request and node completes the authentication of the user to prevent malicious attacks (step 4), while in step 5 user authenticates node. Through mutual authentication, the trust relationships between user and nodes will be established.

B. Defend against man-in-the-middle attack

In user-nodes authentication process, each session will generate a random value, such as ephemeral key a or b. Even if attacker captures the private key s of the base station, he still can not calculate the session key. Meanwhile due to the secret of ephemeral key a or b, our mechanism is provided with forward security. The mutual authentication in our paper can resist the man-in-the-middle attack.

C. Defend against eavesdropping attack

Every authentication process of communication, user and nodes will generate a new session key which can not be same with the previous session key. In our protocol, session key $h(abP)$ is calculated by the hash function and the secret value. Even if the previous session key is intercepted, the attacker can not get other session key.

D. Defend against node capture attack

In communication authentication process, the entity chooses a random value to generate a session key that will be discarded when the session terminates.

E. Mitigate Dos attack

Information requests received by the entity are able to authenticate promptly using timestamps, so as to resist DoS attacks.

F. Defend against replay attacks

If a malicious attacker obtain a session key or capture the network traffic of IoT, the session key can identify malicious visitors and authenticate their identity is not legitimate. Resend message will be discarded because of illegal identity.

V. Performance Evaluation

In this section, we summarize the performance of our proposed scheme. Since user and gateway node are powerful devices, computational overhead is negligible compared to the sensor nodes. Therefore, we only consider the computation overhead of sensor nodes. We use the computational overhead (the computation time required for sensor nodes, denoted by T) to analyze the performance. For facilitate of evaluating the computational overhead, we define some notions as follows:

R : the time of random number generation

T_H : the time of executing a one-way hash function SHA-1

T_{ADD} : the time of executing an addition operation of points

T_{MUL} : the time of executing ECC point multiplication

T_{MTPH} :the time of performing a map to point hash function

Table 2. Comparison of computational time

	Our Proposed Scheme	Yeh et al.'s protocol
User Authentication	$R+T_{MUL}+2T_H$	$2T_{MUL}+R+T_{ADD}+4T_H$
Node Authentication	$R+T_{MUL}+2T_H$	$3T_{MUL}+R+T_{MTPH}+T_H$
Total	$R+T_{MUL}+2T_H$	$3T_{MUL}+R+T_{MTPH}+T_H$

The computational cost of our proposed scheme and Yeh et al.'s protocol [12] are shown in table 2. From the table, we know that both the authentication of user and the sensor nodes take $R+T_{MUL}+2T_H$ in our scheme. Meanwhile, for user authentication, Yeh et al.'s protocol takes $2T_{MUL}+R+T_{ADD}+4T_H$, and requires $3T_{MUL}+R+T_{MTPH}+T_H$ while for the node authentication. From the theoretical analysis [19] and the experimental results [5],[6], we know that the cost is mainly related to the evaluation of ECC point multiplication. Besides, the computation cost of T_{MUL} is higher than R and T_H. The computational costs of the user and the sensor nodes in Yeh et al.'s protocol are about $2T_{MUL}$, $3T_{MUL}$, separately. In our proposed scheme, the computation costs of the user and the sensor node are about T_{MUL}, T_{MUL} .Then our scheme has better performance at the sensor node side.

VI. Conclusion

With the gradual popularization of the Internet of things in people's lives, security of IoT is facing more and more challenges. As a stand-by of IoT perception layer, WSN need more reasonable authentication and access control method to ensure security of the data. Traditional cryptographic algorithms can not reach the lightweight, lack of mutual authentication between user and nodes, not suit to the open environment of IoT. An efficient ECC-based authentication and the attribute-based access control policy were proposed in order to achieve mutual authentication between user and nodes and fine-grained access control. Mutual authentication ensures the security of the communication between user and nodes, whose process is simple to solve the resource-constrained problem of the IoT perception layer. Accessing the data on the basis of user attribute certificate in access control authority can achieve flexible fine-grained access control. However，this paper discusses attribute-based access control policy which needs further studies.

Acknowledgment The research is support by National Natural Science Foundation of P. R. China (Grant No. 61170065 and 61003039), Peak of Six Major Talent in Jiangsu Province (Grant No.2010DZXX026), Project sponsored by Jiangsu provincial research scheme of natural science for higher education institutions (Grant No.12KJB520009), Science & Technology Innovation Fund for higher education institutions of Jiangsu Province (Grant

No.CXZZ11-0405).

References

[1] D. Chen, G. Chang, L. Jin, *et al*. A Novel Secure Architecture for the Internet of Things. In Proc. 5th Int. Genetic and Evolutionary Computing (ICGEC), Xiamen, Aug. 2011,311-314.

[2] L. Atzori, A. Iera, G. Morabito. The internet of things: A survey. *Computer Networks*, **54**(2010)15,2787-2805.

[3] R. H. Weber. Internet of Things–New security and privacy challenges. *Computer Law & Security Review*, **26**(2010) 1,23-30.

[4] G. Zhao, X. Si, J. Wang, *et al*. A novel mutual authentication scheme for Internet of Things. In Proc. Modelling, Identification and Control (ICMIC), Shanghai, China, Jun.26-29,2011, 563-566.

[5] A. Mnif, O. Cheikhrouhou, M. Ben Jemaa. An ID-based user authentication scheme for Wireless Sensor Networks using ECC. In Proc. Microelectronics (ICM), Hammamet, Dec. 19-22, 2011, 1-9.

[6] X. H. Le,M. Khalid, R. Sankar, *et al*. An efficient mutual authentication and access control scheme for wireless sensor networks in healthcare. *Journal of Networks*, **6**(2011)3,355-364.

[7] J. Liu, Y. Xiao, C. L. P. Chen. Authentication and Access Control in the Internet of Things. In Proc. 32nd Int. Distributed Computing Systems Workshops, Macau, Jun. 18-21, 2012, 588- 592.

[8] S. Banerjee, D. Mukhopadhyay. Symmetric key based authenticated querying in wireless sensor networks. In Proc. first Int. Integrated internet ad hoc and sensor networks.ACM, New York, NY, USA ,May, 2006,1223-1227.

[9] H. Chan,A. Perrig. Security and privacy in sensor networks. *Computer*, **36**(2003)10,103-105.

[10] H. R. Tseng, R. H. Jan, W. Yang. An improved dynamic user authentication scheme for wireless sensor networks. In Proc. IEEE Conf. Global Telecommunications, Washington, DC ,Nov. 2007, 986-990.

[11] H. Wang, B. Sheng, Q. Li. Elliptic curve cryptography-based access control in sensor networks. *International Journal of Security and Networks*, **1**(2006)3, 127-137.

[12] H. L. Yeh, T. H. Chen, P. C. Liu, *et al*. A secured authentication protocol for wireless sensor networks using Elliptic Curves Cryptography, *Sensors*, **11**(2011)5,4767–4779.

[13] H. F. Huang. A novel access control protocol for secure sensor networks. *Computer Standards & Interfaces*, **31**(2009)2, 272-276.

[14] Y. Wei, C. Shi, W. Shao. An attribute and role based access control model for service-oriented environment. In Proc. IEEE Conf. Control and Decision (CCDC), Xuzhou, Chinese, May, 2010, 4451-4455.

[15] E. E. Mon, T. T. Naing. The privacy-aware access control system using attribute-and role-based access control in private cloud. In Proc. IEEE Int. Conf. Broadband Network and Multimedia Technology, Shenzhen ,Oct. 2011, 447-451.

[16] S. Xin-fang, H. Xiao-hua. A new access control scheme based on protection of sensitive attributes. In Proc. 7th IEEE Int. Conf. Computer Science & Education (ICCSE),

Melbourne, VIC, Jul. 2012, 1021-1024.
[17] G. Zhang, J. Tian. An extended role based access control model for the Internet of Things. In Proc. ICINA, Kunming ,Oct. 2010, V1-319.
[18] Q. Han, J. Li. An Authorization Management Approach in the Internet of Things*. 2012.
[19] P. N. Mahalle, B. Anggorojati, N. R. Prasad, *et al*. Identity establishment and capability based access control (IECAC) scheme for Internet of Things. In Proc.15th Int. WPMC, Taipei ,Sept. 2012, 187-191.
[20] P. Zeng, K. K. R. Choo, D. Z. Sun. On the security of an enhanced novel access control protocol for wireless sensor networks. *IEEE Transactions on Consumer Electronics*, **56**(2010)2,566-569.
[21] Y. Che, Q. Yang, C. Wu, *et al*. BABAC: An access control framework for network virtualization using user behaviors and attributes. In Proc. IEEE/ACM Int. Conf. Green Computing and Communications & Int. Conf. Cyber, Physical and Social Computing, Washington, DC, USA, Dec. 2010, 747-754.