PROCEEDINGS OF SCIENCE

Resource Authentication Management Model Based on CA and DHT in Internet of Things

Fufang Li[1][2]
School of Computer Science and Educational Software, Guangzhou University,
Guangzhou 510006, China
E-mail: lffgz@163.com

Lina Yuan
South China Institute of Software Engineering.GU, Guangzhou University,
Guangzhouconghua 510990, P.R. China
E-mail: 18971656@qq.com

Lingxi Peng, Wenbin Cheng, Yuanyong Feng[3][a]
School of Computer Science and Educational Software, Guangzhou University,
Guangzhou 510006, China
E-mail:[a]ComerFeng@gmail.com

Research on the Internet of Things (IoT) has been a hot spot in recent years. Resource authentication and management in IoT is a most important and challenging problem and is far to be solved. In this paper, we propose an effective distributed hierarchical IoT resource authentication and management model based on the key technologies of distributed hash table, Chord Ring and public key infrastructure. By using the exceptional advantage of search and query ability of the above technologies, the proposed model owns enhanced security and improved efficiency. Simulation results show that the proposed model can mutually authenticate the IoT end entities each other in more short time compared to other existing approaches.

CENet2017
22-23 July 2017
Shanghai, China

[1] Speaker

[2] This work has been co-supported by: Natural Science Foundation of China under Grant No. 61472092; Guangdong Provincial Science and Technology Plan Fund with grant No. 2013B010401037; Natural Science Foundation of Guangdong Provinceunder Grant No. S2011040003843; GuangZhou Municipal High School Science Research Fund under grant No. 1201421317; State Scholarship Fund by China Scholarship Council under Grant No. [2013]3018-201308440096; and Yuexiu District Science and Technology Plan Fund of GuangZhou City with grant No. 2013-CY-005.

[3] Correspongding Author

1. Introduction and Related Work

The Internet of things (IoT) and its application has been considered as a core scientific strategy by academia, industry and the governments all over the world. The IoT and its related theory and technology have also been widely studied by researchers at home and abroad in recent years. As defined by IoT-GSI of ITU, the Internet of Things (IoT) is a global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies[1]. The IoT allows objects to be sensed or controlled remotely across existing network infrastructure, creating opportunities for more direct integration of the physical world into computer-based systems, and resulting in improved efficiency, accuracy and economic benefit in addition to reduced human intervention[2]. According to the conception of IoT ITU, a thing is an object of the physical world (physical things) or the information world (virtual things), which is capable of being identified and integrated into communication networks[3]. Each thing is uniquely identifiable through its embedded computing system but is able to interoperate within the existing Internet infrastructure. In IoT system or application, the number of things is sharply very large, experts estimate that the IoT will consist of about 30 billion objects by 2020[4]. Facing such a huge number of IoT equipment and resources, how to securely, reliably and credibly manage these equipment and resources with privacy protection is a most urgent, important and challenging problem.

To effectively and credibly manage the resources of IoT system or application, many researchers have done a lot of productive work in this area. To acquire secure and efficient access requirement of resources for multi-user in IoT, paper [5] presented a novel hierarchical access control scheme for perceptual layer of the IoT application. By using Merkle tree to guarantee secure and efficient multi-user key material derivation, their model can more effectively manage the multi-user's resource access of perceptual layer in IoT. To solve the growing issues of resource matching and selection in IoT solutions, paper [6] proposed a novel resource model to describe the IoT resources in a multidimensional manner. In their model, they present a resource matching algorithm which selects the well-matched resources by matching the similarity between the proposed resources. Their experiments verified that their resource matching model is more effective and efficient than existing approaches. To realize a virtual computing platform that provides access to heterogeneous group of device resources in our living environments, Takalo[7] proposed a two-level resource management architecture, where the necessary information about applications and resources are represented with machine-interpretable semantic descriptions based on the Semantic Web technologies. By organizing the IoT resources into system level and local level, their proposed architecture can effectively and optimally allocate the IoT resources to the applications based on their criticality, performance and needs. To tackle with the constraints of memory, processing capability and low-power radio standards of devices in the Internet of Things, Sehga[8] investigate how existing IP-based network management protocols can be implemented on resource-constrained devices, and they present the resource requirements for SNMP and NETCONF on an 8-bit AVR based device. To enhance the credibility and privacy protection ability of the resources in IoT system or application is another challenging problem on IoT research area. In order to address the defects of being aided by home domain authentication server to authenticate the identity of roaming mobile nodes, paper [9] proposed a direct anonymous authentication protocol with provable secure mobile nodes in Internet of things, which simplify the legitimacy authentication procedure for the mobile nodes in IoT. Their approach can not only achieved the legitimacy authentication of anonymous identity, but also had shorter time delay and higher operating efficiency and good anti-attack capability. To solve the problem of authentication and data privacy in IoT, paper [10] put forward a new scheme of key management and authentication for IoT. The proposed scheme can better meet the special need of IoT environment, such as low capability resource, high interaction rates, high mobility, and low data volume. In article [11], Tan present a distributed multi-hop certification authority scheme for mobile Ad Hoc network. In their scheme, by using a variety of methods and techniques, they designed a wieldy multi-hop certification authority algorithm and gained sound performance and effectiveness.

In this paper, we propose an effective Resource Authentication and Management Model based on Certificate Authority and Distributed Hash Table (RAM_CA_DHT, for short). In the proposed model, we deploy a hierarchical distributed certificate authority back bone system which complies with the PKI specifications[12,13]. By introducing the architecture of PKI (Public Key Infrastructure) specifications to construct the authentication system for the IoT environment, end entities in the whole IoT system can easily verify their identity to each other securely and efficiently. On the other hand, we use hierarchical Distributed Hash Table (DHT, for short) to organize the IoT authentication system, which will largely improve the speed and efficiency of the mutual and multilateral authentication in the IoT system[14,15].

The rest of the paper is organized as follows: In section II, we talk about the proposed model of RAM_CA_DHT in detail. Section III describes the resource authentication and management schema and algorithm in the model of RAM_CA_DHT. In section IV, we do simulation experiment to show the performance of RAM_CA_DHT and compare it with similar approaches. At last, we conclude the paper in section V.

2. The Proposed Resource Authentication and Management Model of RAM_CA_DHT

As mentioned above, although many work had been done on resource management and authentication in Internet of Things, satisfactory solution on this field is far from reaching. To solve this problem, we try to present an effective Resource Authentication and Management Model based on Certificate Authority and Distributed Hash Table (RAM_CA_DHT, for short). The proposed resource authentication and management model of RAM_CA_DHT is shown in Figure 1. As is shown in Figure 1, the resource management architecture and authentication schema of the proposed resource authentication management model of RAM_CA_DHT is logically organized as four layers. And in each layer of the model of RAM_CA_DHT, the servers of GARCA (abbreviation of Global Area Root Certificate Authority, in Layer IV), WADCA (abbreviation of Wide Area Domain Certificate Authority, in Layer III) and LADCA (abbreviation of Local Area management Domain Certificate Authority, in Layer III) and VN (abbreviation of Virtual Nodes, in Layer II) are respectively organized into three kinds of Chord Rings according to the theory of Distributed Hash Table. By using Chord Ring to organize the above servers and VNs, and benefiting from the sound scalability and high efficiency of Chord

Ring, the above servers and VNs can be easily located and found and thus promote the performance of the resource authentication and management system.

The detailed construction of the proposed layered hierarchical resource authentication and management model of RAM_CA_DHT is described as follows:

(a) The Layer I is the physics layer which is composed of various heterogeneous smart physics equipment and devices, such as computers, smart mobile phones, digital video or audio facilities, scanners, and so on. These equipments and devices are divided into different management domains by the very special applications or geographical regions they belong to. That is to say, we incorporate the equipments and devices into one management domain if they are belong to the same administrative region or the same application. We name these management domains as Local Area management Domain (LAD for short). For the needs of effective authentication management of the resources of the LAD, we deploy a Certificate Authority server for each LAD (LADCA, for short), and let it be the root of the LAD which it belongs to. The LADCA is a special member of the LAD and is responsible for the management of authentication service and other the related information of the nodes in the local area domain.

(b) The Layer II is the virtualization of the hybrid heterogeneous equipments and devices of Layer I. In this layer, we virtualize the hybrid heterogeneous equipments and devices as Virtual Nodes (VN for short). To do this, we deploy a lightweight Node Agent (NA for short) to manage the information of the node, and we let NA be the representative of the node which it reside in. The information of the node managed by the agent includes: ID of the node, IP address of the node, digital CA certificate of the node, other attributes of the node such as CPU main frequency, memory size, network bandwidth, disk apace, etc. The agent of NA should update the above information and store this information into the database in the LADCA server in real time periodically. To carry out the functions of resource authentication management and other related affairs, we deploy a LAD Agent (LADA for short) and design a database table to cooperatively manage the related information of the nodes in the database system which is installed in the LADCA server. The agent of LADA is the delegate of the LAD and is responsible for the affairs of resource authentication management of the LAD which it belongs to. In the local area domain, all agents of NAs and LADA are organized into a Local area Chord Ring (LCR for short) according to the theory of Distributed Hash Table. That is to say, the agent of LADA is a member of the LCR and is the entrance and interface of the local area domain where it reside in as well. Being a member of LCR where it is deployed, the LADCA server is also a member of Wide area domain Chord Ring, and is the representative of the LAD when constructing the Wide area domain resource authentication and management Chord Ring (reference to Layer III).

(c) The Layer III is the Wide Area Domain (WAD for short) resource authentication and management layer of the model of RAM_CA_DHT. The WAD is composed of several LADCAs which are introduced in Layer I and Layer II. As is mentioned above, to mange the hybrid heterogeneous equipments and devices of the wide area domain, we firstly divide the physics nodes into LADs (Local Area Domains) according to the very applications or geographical regions they belong to. In the meantime, to efficiently manage the authentication affairs and other related information of the WAD, we deploy a Wide Area Domain Certificate Authority (WADCA for short) server for each WAD and let it be the root of the WAD where it resides in. In the server of WADCA, we deploy a WAD Agent (WADA for short) in it so as to manage the authentication management affairs of the WADs. Then, by using the agents of LADAs and WADA, we consolidate all the LADCA and WADCA servers into a Wide area domain Chord Ring (WCR, for short) according to the theory of DHT. Being a member of WCR, the WADCA server is also a member of the GCR, and is the representative of each WAD to participate in the organization of the global area domain resource authentication and management Chord Ring of the global IoT system (reference to Layer IV).

(d) The Layer IV is the global area resource authentication and management layer of the model of RAM_CA_DHT. According the above-mentioned Layer III, a WADCA server has been deployed in each WAD, and an agent of WADA has also been deployed in it so as to manage the authentication management affairs of the whole WAD. In order to manage the global area resource authentication affairs effectively and to simplify the trust model of the whole system, we deploy a Global Area Root Certificate Authority (GARCA for short) server, which will help to provide cross domain authentication for the global IoT system. In Layer IV, a Global Area Agent (GAA, for short) is also implemented and deploy in the GARCA server. The agent of GAA is responsible for the management of authentication affairs of the whole system. To manage the authentication affairs of the global area resources more efficiently, all WADCAs and GARCA are also organized as a Global area domain Chord Ring (GCR, for short) according to the theory of Distributed Hash Table. As is shown in figure 1, besides being a member of the GCR, each WADCA server is also a member of the WCR which it belongs to.

By this way, with the WADAs being the representative of the WADs, we use WADAs and GAA to construct all WADCA servers and GARCA server into a hierarchical distributed global area backbone resource authentication system according to PKI architecture specification. Layer IV and Layer III constitute the core of the proposed resource authentication and management system of RAM_CA_DHT IoT.

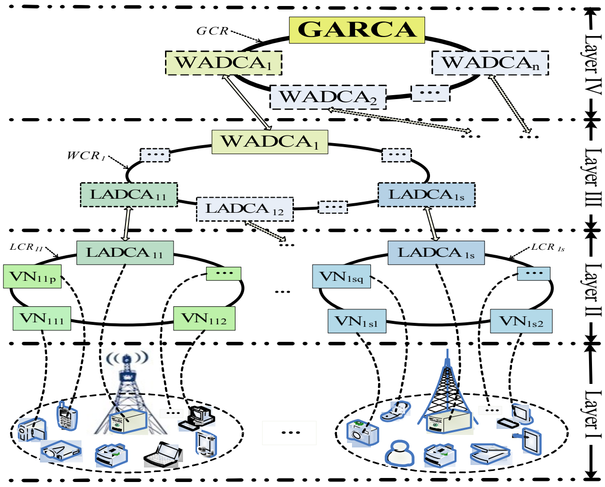

Figure 1: The resource organization architecture and the authentication schema of the model of RAM_CA_DHT

3. The Resource Authentication and Management Schema and Algorithm in the Model of RAM_CA_DHT

3.1 The Resource Authentication and Management Schema of the Model of RAM_CA_DHT

As described in Section III, to accomplish effective resource authentication and management in the global IoT system, we have deployed three kinds of CA servers: LADCAs, WADCAs and GARCA in different layer of the model of RAM_CA_DHT. The LADCAs, WADCAs and GARCA, which own high performance and are linked with high-speed backbone network, are responsible for resource authentication and management in local area domain, wide area domain and cross domain of the whole IoT system respectively. In the model of RAM_CA_DHT, the LADCAs, WADCAs and GARCA constitute the whole hierarchical tree authentication system. The architecture of the proposed resource authentication and management model is as shown in Figure 2.

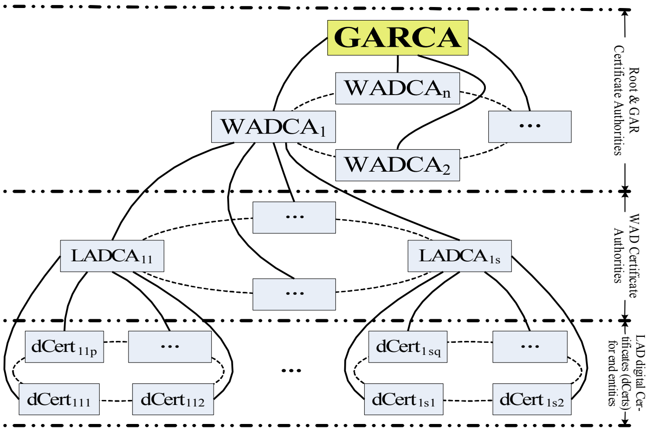

Figure 2: The architecture of the proposed resource authentication model

The detailed procedure of the authentication management of resource in the model of RAM_CA_DHT is divided into three parts:

Part I: To construct the root & GAR certificate authority layer of the basic hierarchical backbone authentication environment for the whole IoT resource authentication management system. Firstly, the GARCA server should be deployed and started running so that it will be able to accept and approve the digital CA Certificates requests from the WADCA servers. After the GARCA server having been running for the first time, and as the root of the hierarchical authentication system, we let GARCA server generate a root CA request and issue the root CA certificate for itself at first. Secondly, all the WADCA servers are also deployed and started up. Meanwhile, we activate all agents of GAA and WADAs that are resided in GARCA and WADCA servers. All the GARCA and WADCA servers are logically linked into GCR (Global area domain Chord Ring) through multi-party collaboration of the agents of GAA and WADAs. After all the WADCA servers and the agent of GAA having been started running, every WADA would begin to collect information of the WADCA server which it reside in and then generate a CA certificate request and submit it to the GARCA server. The agent of GAA should handle the digital certificate requests submitted from WADAs and then issue these WADCA servers' CA certificates. Finally, the agent of GAA should deliver these WADCA servers' CA certificates to its' owner, and all the agents of WADAs should receive and install the CA certificates into the corresponding WADCA server. So far, the WADCA servers can be authenticated with each other by verifying their CA certificates, and thus the root & GAR certificate authority of the basic hierarchical backbone authentication environment for the whole IoT system has been set up.

Part II: To construct the WAD certificate authority layer of the proposed authentication environment of the model of RAM_CA_DHT. At first, as is mentioned above, we deploy a

LADCA server in each LAD, and let it be the root of the LAD. Then all LADCA servers should be started up, and in the meantime all agents of LADAs are activated. In each WAD, with the agents of WADA being activated ahead, all agents of WADA and LADAs will cooperatively combine the WADCA server and all LADCA servers into a logical WAD Chord Ring (WCR, as mentioned above). After the WCR being established, every agent of LADAs should begin to collect information of the LADCA server which it reside in and then generate a LAD sub-root CA certificate request and submit it to the WADCA server. The agent of WADA should accept the LADCA server's CA certificate request, issue their CA certificates, and send these CA certificates to its' owner (i.e. the corresponding LADCA server). In the end, every agent of LADAs will get the corresponding CA certificate, and then they should install these CA certificate into corresponding LADCA server. To this point, all LADCA servers can mutually authenticated with each other by verifying their CA certificates, that is to say the WAD certificate authority subsystem has been set up.

Part III: To construct the LAD certificate authority layer of the proposed authentication environment for the whole IoT system. In this part, all agents of NAs should be firstly started running. In each LAD, with participation of the agent of LADA, all agents of NAs and LADA must collaborative linked themselves into a LAD Chord Ring (LCR, as mentioned before). After the NAs having been running, they must immediately begin to detect and collect the information of the end entity equipment. When all information of the end entity having been gathered and the LCR ring having been established, each agent of NAs will generate an end entity CA certificate request and submit it to the LADCA server that they belong to. The agent of LADA should accept the end entities' CA certificate request and issue their CA certificates. At last, in every LAD, the agent of LADA should hand out these issued CA certificate to the corresponding owner of end entity nodes, and then every agent of NAs should receive and install the corresponding CA certificate into the end entity node which it reside in. So far, every end entity owns a CA certificate, and they can use their CA certificate to verify their membership of the whole IoT system. Hence, the LAD certificate authority layer has been built.

3.2 The Resource Authentication and Management Algorithm of the Model of RAM_CA_DHT

As mentioned above, according to the procedure of the authentication management of resource of the proposed model of RAM_CA_DHT, the detail description of the corresponding resource authentication management algorithm is as follows:

```
Step 1: construct the root & GAR certificate authority management backbone system {
    Step 1.1: start up the GARCA server and let it issue the root CA certificate for itself;
    Step 1.2: start up the WADCA servers and activate the agent of GAA and all agents of
        WADAs;
    Step 1.3: link the GARCA server and all WADCA servers into GCR through multi-party
        collaboration of the agents of GAA and WADAs;
    Step 1.4: let the agent of WADA generate a CA certificate request and submit it to the
        GARCA server;
    Step 1.5: the agent of GAA handle WADCA servers' certificate requests, issue their CA
        certificates, and send the corresponding CA certificates to the requesters;
    Step 1.6: all the agent of WADA install their CA certificate into the WADCA server which it resides in;
    }
Step 2: construct the WAD certificate authority management subsystem {
    Step 2.1: start up all LADCA servers, and activate all agents of LADAs;
    Step 2.2: let all agents of WADA and LADAs cooperatively combine the WADCA server and all LADCA servers into a logical WAD Chord Ring (WCR);
    Step 2.3: let the agent of LADAs collect information of the LADCA server and generate a LAD CA certificate request and submit it to the WADCA server;
    Step 2.4: the agent of WADA handle the LADCA server's CA certificate request, issue their CA certificates, and deliver the corresponding CA certificates to the requesters;
    Step 2.5: all the agent of LADAs install their CA certificate into the LADCA server which it resides in;
    }
Step 3: construct the LAD certificate authority management subsystem {
    Step 3.1: activate all agents of NAs;
    Step 3.2: all agents of NAs and LADA collaborative link themselves into a LAD Chord Ring (LCR);
    Step 3.3: let all agents of NAs collect information of nodes which they reside in;
    Step 3.4: each agent of NAs generate an end entity CA certificate request and submit it to the LADCA server that they belong to;
    Step 3.5: the agent of LADA accept the end entities' CA certificate request, issue their CA certificates, and dispatch the corresponding CA certificates to the requesters;
    Step 3.6: all the agents of NA install their CA certificate into the node which it resides in;
    }
Step 4: different end entities of the whole IoT system use their CA certificates to mutually verify their identity.
```

4. Simulation experiments and Discussion

In order to verify the effectiveness and performance of the proposed model, we compare our model with similar models proposed by paper [9] and [10]. We measure the mutual authentication time between end entities of inner local area domain and cross different local area domains. We also measure the change of above authentication time as the number of the nodes in the domain increased. Considering the crucial factor that has the greatest impact on the certification time is the scale of the local area domain, we simplified the simulation experiments by simulating five LADs in the network simulator of NS-2, and we set a variety of large numbers of nodes in each LAD so as to fulfill the experiments. The experimental procedure is as follows: (1)we firstly set the numbers of end entities in the five LADs respectively be 50; (2)then, to compare our proposed model with other two similar approaches, by using methods of RAM_CA_DHT, paper [9] and paper [10] in turn, we randomly select 100 inner domain pairs of end entities in the above five LADs and let them do authentication with each other and measure their authentication time; (3) calculate and record the average inner domain authentication time of the 100 inner domain pairs of end entities; (4) randomly select 150 cross domain pairs of end entities cross the above five LADs and do similar experiments of step (2) and (3), and obtain the average cross domain authentication time of the 150 cross domain pairs of end entities; (5) in succession, by changing the numbers of end entities in the five LADs respectively to 100, 150, 200, 250, 300, and 350, do the same experiments of step (2) to (4). The experimental results of inner domain authentication time are as shown in Figure 3, and the cross domain authentication time as shown in Figure 4.

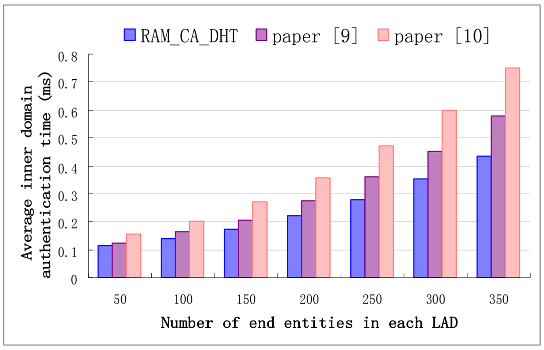

Figure 3: Average inner domain authentication time vs Number of end entities in each LAD

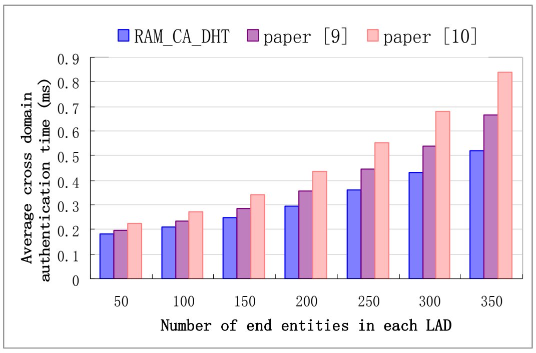

Figure 4: Average cross domain authentication time vs Number of end entities in each LAD

As is shown in Figure 3 and 4, both the average inner domain authentication time and the average cross domain authentication time will increase when the number of end entities increase in each LAD. And from Figure 3 and 4, we can see that both the inner domain authentication time and cross domain authentication time of the proposed model of RAM_CA_DHT are shorter than the other two compared approaches. In summary, in our proposed model of RAM_CA_DHT, the authentication time between end entities is shorter than existing methods, which shows that the proposed model in this paper works better than exiting models.

5. Conclusion

In this paper, we presented a distributed hierarchical resource authentication and management model of RAM_CA_DHT for Internet of Things. As is known to all that the distributed hash table and Chord Ring has the advantage of exceptional search and query ability, so we introduced the technique of distributed hash table and Chord Ring to organize the IoT resource authentication and management model so as to obtain sound efficiency and performance. To strengthen the robustness and reliability of the model, we construct the backbone resource authentication and management system in distributed hierarchical way. To improve the security function of the resource authentication and management platform, we build the resource authentication and management platform according to PKI specifications. Simulation results showed that the proposed model of RAM_CA_DHT has sound security and improves efficiency and performance compared to the previous approaches.

References

[1] ITU. IoT-GSI. *Internet of Things Global Standards Initiative*. http://www.itu.int/en/ITU-T /gsi/iot/Pages/default.aspx. Retrieved 26 June 2015.

[2] Harvard Business Review. *Internet of Things: Science Fiction or Business Fact?*. Harvard Business Review. November 2014. Retrieved 23 October 2016.

[3] ITU, *Overview of the Internet of things*, Recommendation ITU-T Y.2060, June 2012.

[4] Nordrum, Amy. *Popular Internet of Things Forecast of 50 Billion Devices by 2020 Is Outdated*. 18 August 2016, IEEE spectrum: http://spectrum.ieee.org/tech-talk/telecom/internet/popular- internet-of-things-forecast-of-50-billion-devices-by-2020-is-outdated.

[5] Ma Jun,Guo Yuan bo,et al. *Multi useraccesscontrol Scheme Based on Resources Hierarchies for Perceptual Layer of IoT*. Acta Electronica Sinica, Vol.42 No.1, p:28-36 Jan.2014 (in Chinese).

[6] Zhao Shuai, Zhang Yang,Yu Le1, et al. *A multidimensional resource model for dynamic resource matching in internet of things.* Concurrency Computation, vol 27, no 8, p:1819-1843, June 10, 2015.

[7] Takalo-Mattila, Janne; Kiljander, Jussi; Pramudianto, Ferry; Ferrera, Enrico. *Architecture for mixed criticality resource management in Internet of Things*. Proceedings - 2014 TRON Symposium, TRONSHOW 2014; Akasaka, Minato, Tokyo, Japan. p:313-324. January 22, 2015

[8] Sehga, Anuj; Perelman, Vladislav; Küryla, Siarhei; Schönwälder, Jurgen. *Management of resource constrained devices in the internet of things*. IEEE Communications Magazine, v 50, n 12, p 144-149, 2012.

[9] ZHOU Yan-Wei, YANG Bo. *Provable Secure Authentication Protocol with Direct Anonymity for Mobile Nodes Roaming Service in Internet of Things*. Journal of Software, 2015, Vol.26, No.9, p:2436-2450, September 2015.

[10] QI Yong, XU Yang, LI Qian-mu. *A New Scheme of Key Management and Authentication for IOT.* Jisuanji Yu Xiandahua, Vol.2014 No.12, p:91-96, December 2014.

[11] Tan Xuezhi; Wu Shaochuan; Jia Shilou. *A distributed adaptive multi-hop certification authority scheme for mobile Ad Hoc networks*. Journal of Systems Engineering and Electronics, Vol.16,No.2, p:265-272, June 2005.

[12] Techotopia. *An Overview of Public Key Infrastructures (PKI).* http://www.techotopia.com/ index.php/An_Overview_of_Public_Key_Infrastructures_(PKI), Techotopia. Retrieved 26 March 2015.

[13] Ubaidullah Rajput,Fizza Abbas, Jian Wang, Hasoo Eun and Heekuck Oh. *CACPPA: A Cloud-Assisted Conditional Privacy Preserving Authentication Protocol for VANET*. 2016 16th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGrid), Cartagena, Colombia, p:434-442, 16-19 May 2016.

[14] Ribe-Baumann Liz, *Combining resource and location awareness in DHTs*, Lecture Notes in Computer Science, Vol.7044, p:385-402, 2011.

[15] Shimano Yuta and Sato Fumiaki, *Reconfiguration of Chord ring based on communication delay for lookup performance improvement,* Proc. 2011 International Conference on Network-Based Information Systems (NBiS 2011), Vol. 1, p:236-242, 2011.