Applied Mathematics & Information Sciences
An International Journal

@ 2012 NSP
Natural Sciences Publishing Cor.

A Bi-Directional Security Authentication Architecture for the Internet of Vehicles

Bo Li[1], Yuhong Li[2]*
[1]College of Computer Science, South-Central University for Nationalities, Wuhan, P. R. China
[2] Digital Engineering and Simulation Center, Huazhong University of Science and Technology, Wuhan, China
**E-mail: chuchuemma@163.com, libo_hust@126.com*

Received: 17 Feb. 2012; Revised 14 May 2012; Accepted 15 Jul. 2012

Abstract: The Internet of Vehicles (IoV), which is seemed as an important application of the Internet of Things (IoT) presented widely as the next revolution toward massively distributed information in practice, where any real-world vehicles can automatically participate in the internet and thus be globally queried, is still a new field. Despite the consensus on the great potential of the concept and the significant progress in a number of enabling technologies, there is short of an integrated vision on how to realize it. This paper examines the technologies that will be fundamental for realizing the IoV and proposes a functional architecture that integrates them into a single platform. The functional architecture introduces the use of Bi-directional security authentication framework to encapsulate dedicated short range communication (DSRC) protocol, sensor technologies (On-Board Unit and Road-Side Unit), embedded object logic, and Internet-based information infrastructure. It was applied to evaluate urban transportation dimension and, indirectly, road upkeep, as well as sharing urban population information, in real time, in any place through Intranet and/or Internet, aiding the whole integration of the municipal affairs system. Apart from accessibility advantages for drivers, there are important benefits for municipal administration. Our system outperforms existing industry standards in metrics such as network throughput, delivery ratio and allows different configurations that provide different levels of equipment availability, using fewer resources than a conventional transportation management system, and reducing time and costs. Finally, we demonstrate the feasibility, flexibility, security, and concurrency of the architecture by detailing an implementation, and describe a prototype for the real-time monitoring of traffic flow through an intelligent transportation management system, which can lay a good foundation for the application of IoV in the future.

Keywords: Internet of Vehicles; System Architecture; Bi-directional security authentication; Transportation Management; DSRC.

1. Introduction

Introduced by Ashton in 1991, the Internet of Things (IoT) encompasses a variety of technologies and research areas and is referred to the linkage between the existing internet and the uniquely identifiable real-world objects (Things), see [1] and [2] for details. The gap between the notion of ubiquitous computing and a world of networked, sensing, and intelligent things has been narrowed by advances in fields such as automatic identification, wireless communications, integrated sensing, or distributed data processing. IoT utilizes low-cost information gathering and dissemination devices, such as sensors and RFID tags, that facilitate fast-paced interactions among the objects themselves as well as the objects and persons in any place and at any time.

Nowadays, more and more individuals and businesses can benefit by the realization of IoT in many fields, such as global supply chain logistics, product counterfeit detection, manufacturing automation, smart homes and appliances, e-government (electronic official documents and currency), improved integrated vehicle health management, and e-health (patient monitoring and patient records) etc.

Owing to limited road resources and unscientific management, the rapid increase in automobile ownership has led to higher incidences of traffic congestion and traffic accidents. With the rapid progress of the IoT in the recent years, urban transportation and vehicles management have been given a new meaning, which results in changes of technical methods and management concepts [3].

There are plenty of literatures on the architecture and key technologies for the Internet of Things, such as [4-6]. IoT has been put into practice in some fields [3]. Although Internet of Vehicles is an application of Internet of Things in the Intelligent Transportation System (ITS), nevertheless, there are some problems with Internet of Vehicles in key equipments, protocol and technical implementation. The application of Internet of Vehicles is still in its infancy stage, and how Internet of Vehicles runs is far from being completely understood yet.

1.1. Related work

Amdouni introduce a layered measurement system for wireless infrastructure discovery, which is integrated in the vehicle's router to build and maintain a database of WiFi APs within the vehicle’s range [7]. Baroody developed a Dynamic Discovery Service (DDS) protocol to discover Internet Gateways which is suitable for the characteristics of future vehicular ad hoc networks [8]. In [9], a novel intelligent Internet of Vehicles administration system was presented to replace traditional traffic management system. Also, a vehicle monitoring system was proposed based on the Internet of Things, through the control of the vehicle in the virtual information space, it achieves accurate and intelligent vehicle management [10]. However, few documents discussed the key equipments, such as on-board unit (OBU), and road side unit (RSU). Also, some important attributes, such as, concurrency of communication and security of the Internet of Vehicles system are few addressed.

This paper introduced the design of Internet of Vehicles system, including the key technologies and system architectures covering key equipments, software and network architecture. In the end, the main improvement for current OBU based on Dedicated Short Range Communications (DSRC) protocol in China was proposed.

1.2. Contributions

Although the concept of Internet of Vehicles is widely accepted in the world, its practice application is still under way. Compared to current literatures on the Internet of Vehicles, this paper solves the problems:

-The models of system architecture covering key equipments, software and network architecture were proposed, which describe the overall view of the Internet of Vehicles. Moreover, the security model was presented to make the system more robust and safety.

-OBU and RSU are the basic equipment for Internet of Vehicles. the key equipment type was carefully compared and selected, and the main improvement for current OBU based on DSRC protocol in China was proposed, to guarantee better system concurrency and real-time. Furthermore, the experimental unit system about key equipments and improved protocol was carried on, to verify the feasibility and validity.

This paper is organized as follows. In Section 2, the key equipments and improvements for current OBU based on DSRC protocol are introduced. Section 3 presents system architecture and security. In section 4, experimental results are shown that the design scheme and improved DSRC proposal are feasible, which can lay a good foundation for the application of Internet of Vehicles in the future. Section 5 includes conclusions and future research task.

2 Communication Protocols and Sensors Architecture

The communication protocol of IEEE 802.11p (Wireless Access in the Vehicular Environment）is designed for Internet of Vehicles, and has been used on the Vehicle-carried Communication System, that is, DSRC systems. Considering the very background of Internet of vehicles system, the key equipments includes On-Board Unit (OBU) and Road-Side Unit (RSU), which must meet the following demands.

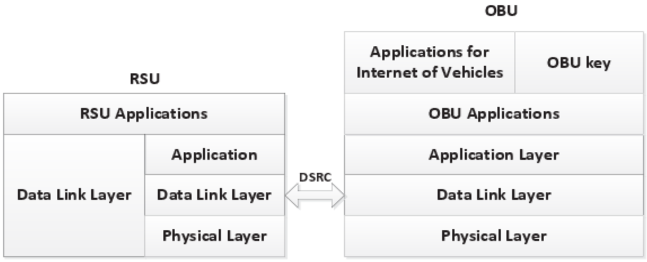


Figure.1. Architecture of OBU and RSU

(1) The equipments meet the requirements of the free flow charging mode, allowing vehicles to pass the checkpoint at higher speed eg. 120km/h;

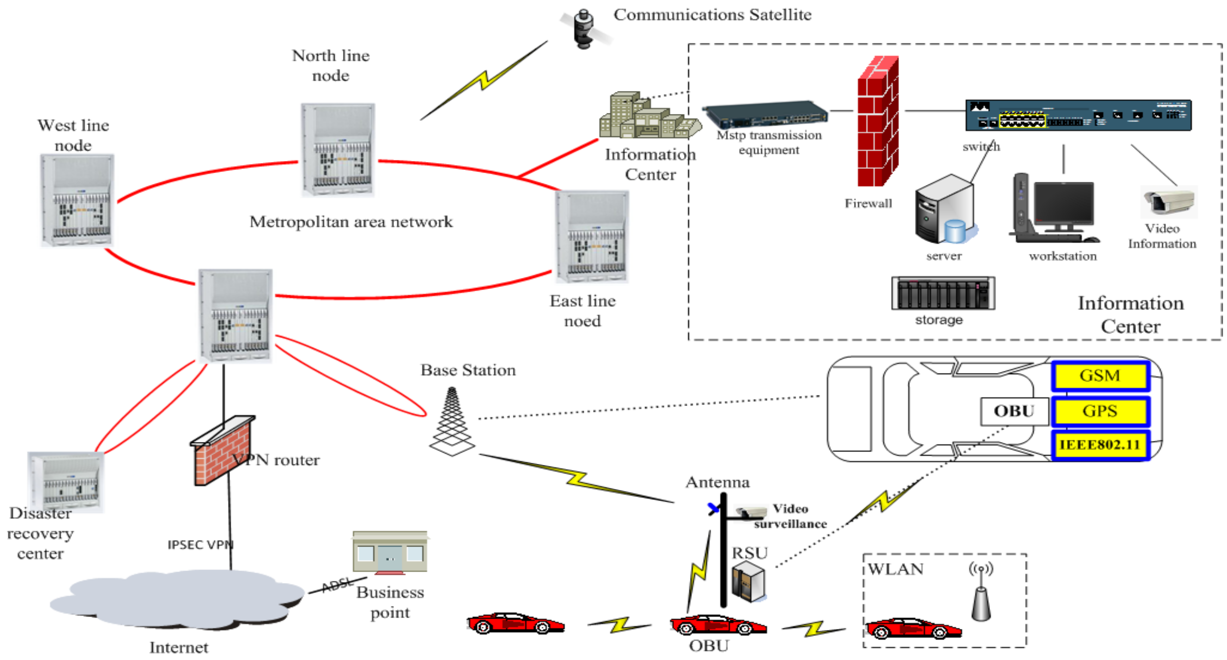


Figure.2. System network topology

(2)The equipments are reliable, stable and durable, possessing at high read-write success rate, and working at a distance about 10 m.

(3)The equipments can solve the problem of interference from adjacent channels and interference from following vehicles.

(4)The equipments are of high security, and can prevent forgery, copy, tampering and so on.

(5)The equipments can concurrent process multi-vehicles communications.

In Internet of Vehicles system, the selection of the types of OBUs is mainly delimitated as follows: single chip and passive power 915MHz electronic tag, single chip and active power 5.8GHz electronic tag, double chip and active power 5.8GHz electronic tag [11].

There are some features for Single-chip and active power electronic tag, for instance, can read and write, active communication working mode, and communication distance can arrive 30 meters, good security (cannot be repudiated), suitable for free flow in high speed, transaction result can be inform on spot, and so on. Therefore, it is appropriate to choose single-chip and active power electronic tag for 5.8GHz frequency bandwidth for Internet of Vehicles.

In our design, there are four layers in the RSU architecture, and five layers in the OBU architecture, as can be shown in Figure 1.

Using DSRC standards on highway application for reference, we put forward some improvements for current OBU products in China. Compared with the existing Chinese products standard, the main improvements of Internet of Vehicles protocol standard are as follows:

(1) The improved protocol provides concurrent operation mechanism of RSU with multi OBU at the same time;

(2) The improved protocol simplifies the transaction flow, reduces transaction time, and improves the performances;

(3)The improved protocol adopts TDES encryption algorithm and simplified double-direction authentication protocol, ensures complete transaction rapidly and safely;

(4) To process multi OBUs concurrent transaction, PSAM generates random number at the same time.

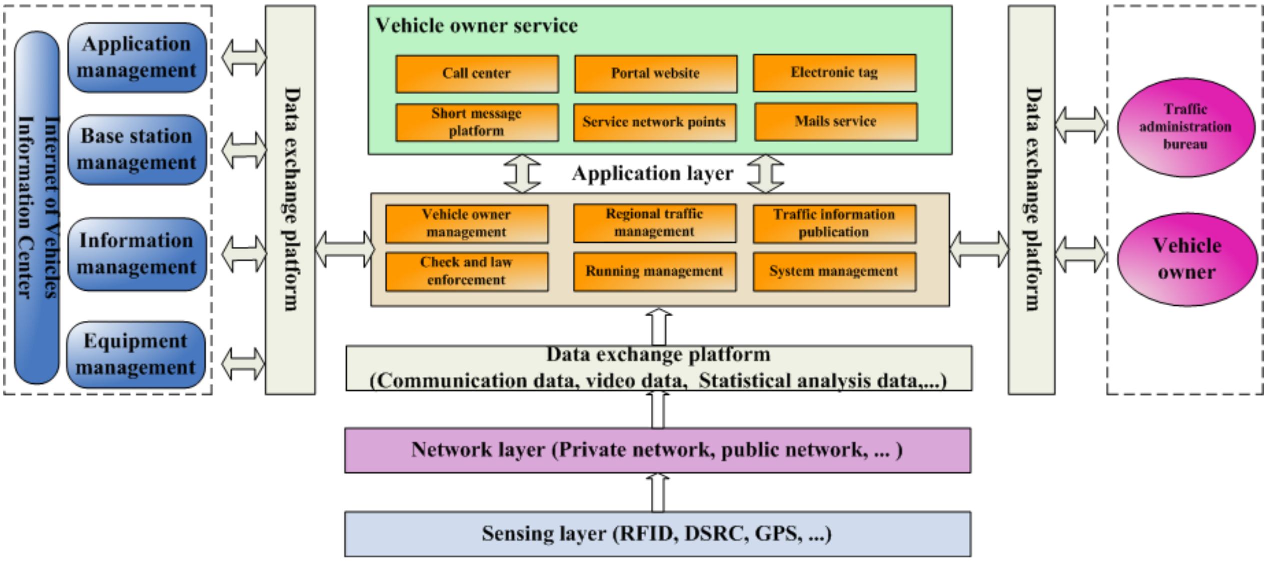


Figure.3. System architecture

3 Bi-Directional Security Authentication System Architecture

3.1System Architecture of IoV

For Internet of Vehicles system, some demands of system architecture must be taken into account: high reliability, high stability, high security, retractility and real-time.

-High reliability

Because the system covers millions of users, involving many behalf sides, it is important to ensure a high reliability. Some mature and advanced technologies must be adopted; some pivotal equipment must meet off-site backup recovery, and possess necessary redundancy and error tolerant capacity as well. And for key equipments, it is necessary to dual-system hot backup. Also, high precision and high read-write success rate are crucial to RSU and OBU.

-High stability

Owing to the fact that equipments must and the data traffic between the systems and modules in all levels is very heavy, it is very important to ensure the high stability in the system.

-High security

One of the objectives of Internet of Vehicles system is involving privacy information of drivers, hence, the Internet of Vehicles system must consider many cases such as destroying, invading, disturbing, and ensuring the system security.

-Retractility

Internet of Vehicles system must fully consider all the factors involving the policy, technology trend and operating demand. Consequently, when designing the system architecture, it is important to take into account the retractility of the system.

-Real-time

The Internet of Vehicles system aims at free flow transportation control, which means many functions are time-limited.

When a vehicle passes RSU lane, OBU and RSU establish communication link, so that the tag vehicle transaction node is formed. The transaction node is then uploaded to the information management center based on the transaction node. On the other hand, the license plate information is captured by vidicon.

Business net spots system provides system customer service. Internet of Vehicles system provides many custom service modes, including custom service website, mail service center and traffic information publication. Every business net spot is connected to the information management center by VPN.

Information management center takes charge of the process, storage, analysis, and checking of all data from front end system. The software systems include customer management system, OBU issue management system, transaction management system, traffic information publication management system, running management system, regional traffic management system, and network management system.

The system network topology can be shown as Figure 2.

System functional architecture can be divided into four layers, that is, sensing layer, network layer, data layer, and application layer. The data layer stores and processes data, while support layer consisting of middle-ware, basic component, and advanced component is to provide service and support. Above the data exchange layer is the application layer, which is all application functional software, including traffic information publication and vehicle owner service, and so on. The data exchange between these operation layers must be conducted by data exchange platform.

The system architecture in the Internet of Vehicles can be shown as Figure.3.

3.2 Bi-Directional Security Authentication

System security architecture comprises physics layer, data link layer, network layer, operation system layer, layer of system software and application layer security. System security architecture is shown as Figure 4.

(1)Electronic transactions

The safety precautions of OBU transactions include: issuing cards of PSAM in RSU and ESAM in OBU, double direction safety authentication.

(2)Bi-directional security authentication

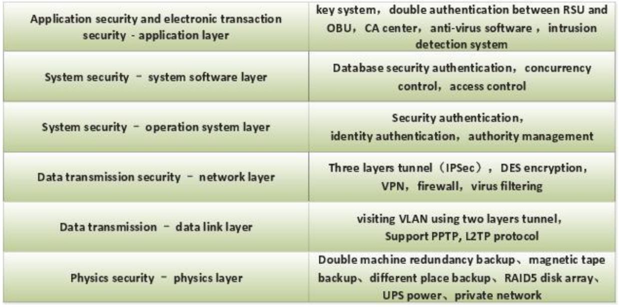
Access credential: RSU must provide correct access credential, and after OBU validating, RSU can access specific OBU. Information authentication: RSU validates the data from OBU through information authenticator sent by OBU. Data encryption: The data between RSU and OBU must encrypt.

(3)TAC code Non-repudiation

In the transaction, OBU generates TAC off-line authentication information, which is sent to lane controller. Then the information is transmitted to the center system, which conducts the authentication of transaction information by off-line authentication encryption machine.

(4)OBU issuing security

The transaction key stored in lane PSAM and OBU-SAM are generated by Internet of Vehicles key management system. The system adopts one card corresponding to one key.



Application security and electronic transaction security - application layer	key system，double authentication between RSU and OBU，CA center，anti-virus software ，intrusion detection system
System security － system software layer	Database security authentication，concurrency control，access control
System security － operation system layer	Security authentication，identity authentication，authority management
Data transmission security － network layer	Three layers tunnel（IPSec），DES encryption，VPN，firewall，virus filtering
Data transmission － data link layer	visiting VLAN using two layers tunnel, Support PPTP, L2TP protocol
Physics security － physics layer	Double machine redundancy backup、magnetic tape backup、different place backup、RAID5 disk array、UPS power、private network

Figure.4. System security architecture

Issuing OBU, the encryption key and authentication key are dispersed and deduced from the contract sequence number. Owing to every contract sequence number is different, the encryption key and authentication key of every OBU-SAM is also different.

The main operation key for issuing lane PSAM and OBU-SAM is stored in a hardware encryption machine, which can provide random number for generating key by hardware circuit. It possess some anti-physics assault ability in hardware and privilege control ability for key generation, storage, operation, and can adopt some strategy to audit, so, key can be stored in hardware encryption machine in low cost.

Desktop issuing device of issuing card are all used under the control of PSAM card authentication. The system read the PSAM ID of terminal authentication PSAM card, look over whether the ID stored in terminal authentication card database or not, if look over successfully, then can be permitted to use desktop issuing device.

4 EXPERIMENTS

The newly developed products such as OBU, RSU based on an improved Bi-directional security authentication DSRC protocol, were examined in details. The stability test, security test and OBU wearing test under hundred thousands of transaction, as well as transaction test under the vehicle speed of 120km/h are verified.

(a)Three OBU parallel driving test: fix 3 OBUs in one vehicle, and test ten times, respectively under different vehicle speed of 30km/h, 40km/h, and 50km/h, altogether 30 times.

(b)OBU following driving test: fix an OBU in a bus and a car, passing communication region at 5km/h in vehicle distance of 1-2m, and test 10 times.

(c)Interference from adjacent test: two vehicles along left and right lane respectively at 20 km/h, 40km/h, 50km/h, 60km/h at the same time, altogether 10 times.

(d)OBU recognition under different vehicle speed of 60km/h, 80km/h, 100m/h, 120m/h, respectively testing 5 times, altogether add up 20 times.

The experimental unit was carried on. The success rate of transaction by means of DSRC is as high as 99%. The experiments show that the design scheme and improved DSRC proposal are feasible, able to serve as a good basis to Internet of Vehicles system in the future.

About video surveillance in Internet of Vehicles system, there are two designs for moving vehicle detection---one is by touch loop, the other is based on video detection. In the test, we first used video detection system, a system developed on basis of some video detection algorithm such as background reconstruction and updating, and difference with background. The hardware platform is built on ARM. We found that the output of moving vehicle detection is far from perfect, because about 30% of moving vehicles cannot be detected correctly, though for the vehicle images captured, the correct rate of recognition is 95% in daytime, and 85% in night.

Hence, we adopted the touch loop detection way, the success detection rate of which is higher more than 95%. Of course, there is a problem about touch loops, the loops are easily to be spoiled.

5 Conclusion

This paper illustrates a Bi-directional security authentication framework for a realization of IoV, which encapsulates dedicated short range communication (DSRC) protocol, sensor technologies (On-Board Unit and Road-Side Unit), embedded object logic, and Internet-based information infrastructure. The feasibility, flexibility, security, and concurrency of the architecture is demonstrated by a detailed prototype implementation in a urban transportation management system. The real-time monitoring for the traffic flow can be realized as well, which lays a good foundation for the application of IoV in the future.

Acknowledgements

This work is partially supported by the National Nature Science Foundation of China under grant No.91130003, the Fundamental Research Funds for the Central Universities(HUST2011QN067), and the Special Fund for Basic Scientific Research of Central Colleges, South-Central University for Nationalities (Grant No. CZQ11026).

References

[1] T. S. Lopez, D. C. Ranasinghe, M. Harrison and D. McFarlane, *Adding sense to the Internet of Things An architecture framework for Smart Objective systems*, Personal and Ubiquitous Computing, 16 (3), (2012) 291-308.

[2] K. Ashton, *That 'Internet of Things' Thing*, RFID Journal, 22, (2009) 1-6.

[3] L. Atzoria, A. Ierab and G. Morabitoc, *Internet of Things: A survey*, Computer Networks, 54 (2010) 2787-2805.

[4] L. Atzori, A. Iera and G. Morabito. *SIoT: Giving a Social tructure to the Internet of Things*. IEEE Communications Letters, 15 (2011) 1193-1195.

[5] L.Zheng et al.,*Technologies, applications, and governance in the Internet of things, Internet of Things-Global Technological and Societal Trends*. River Publisher Ed. (2011).

[6] H.Ning and Z.Wang. *Future Internet of things architecture: like mankind neural system or social organization framework?* IEEE Commun. Lett., 15 (2011) 461-463.

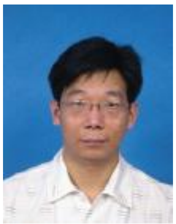
[7] I. Amdouni, F. Filali. *On the Feasibility of Vehicle-to-Internet Communications using Unplanned Wireless Networks*, 2010 17th International Conference on Telecommunications, (2010) 393-400.

[8] R. Baroody, A. Rashid, N. Al-Holou, S. Hariri, *Next Generation Vehicle Network (NGVN): Internet Access Utilizing Dynamic Discovery Protocols*. Proceedings of the IEEE/ACS International Conference on Pervasive Services (2004).

[9] Y. Leng, L. Zhao. *Novel Design of Intelligent Internet-of-Vehicles Management System Based on Cloud-Computing and Internet-of-things*. 2011 International Conference on Electronic & Mechanical Engineering and Information Technology. (2011) 3190-3193.

[10] L. Hu, H. Li,X. Xu,J. Li. *An Intelligent Vehicle Monitoring System based on Internet of Things*. 2011 Seventh International Conference on Computational Intelligence and Security. (2011) 231-233.

Bo Li is presently employed as a lecturer at College of Computer Science, South-Central University For Nationalities, P.R. China. He obtained his M.S majoring in System Analysis and Integration and obtained his PhD majoring in Space Information Science and Technology from Huazhong University of Science and Technology, China. His research area includes digital Image processing, pattern recognition and intelligent transportation system.



Yuhong Li is an active figure both in mathematics and systems science, and is presently employed as the assistant of the dean and Associate Professor at School of Hydropower and Engineering Information, Huazhong University of Science and Technology, China. He obtained his PhD in pure mathematics from the University of Hull(UK) and PhD in systems science from Wuhan University (China). He obtained his M.S. degree from Wuhan Institute of Physics and Mathematics, Chinese Academy of Sciences, Wuhan, China. He is an active researcher coupled with the teaching experience. His research interests include but are not limited to complex systems analysis and its applications, object recognition, graph and shape matching, image parsing, and visual tracking.