Secure and Authenticate Communication by using SoftSIM for Intelligent Transportation System in Smart Cities

Secure and Authenticate Communication by using SoftSIM for Intelligent Transportation System in Smart Cities

Shalini Yadav[1] and Rahul Rishi[2]

[1]Research Scholar, MDU Rohtak, India
[2]Professor, MDU Rohtak, India
Shalini.yadav99999@gmail.com

Abstract. Intelligent Transportation System is a field which is daily paving way for new technologies. Communication in vehicular devices has paved way for security breaches. Vehicle-to-everything connects each and every device to our vehicle just like Internet of Things connects everything to the internet. Everything which is connected to the internet, is prone to security attack. It is very difficult to track the source of the information. Authentication is a big issue and has to be solved. This paper has provided a cognitive approach to address this problem effectively in ITS. A softSIM- similar to the hardware SIM has been proposed. An architecture of the softSIM is designed. A novel algorithm for authenticating the on-board softSIM with the operator has been developed. The performance analysis of softSIM is compared with regular device users. The paper also incorporates future scope as well as business case of the study. The soft SIM will be part of on-board unit and shall come programmed from manufacturer side. This has provided cost effective solution and saved the space that was needed for the hardware SIM.

1. Introduction

Intelligent Transportation System has changed the way the world travels. Almost everything is accessible by the vehicle. This phenomenon has been termed as Vehicle-to-Everything. Where in each and every device could be connected to the car. It has made life comfortable adding quality to it. Everything is becoming smart, homes are becoming smart, cars are becoming smart, and cities are becoming smart. All this is achievable by connecting everything. The doctor can now monitor the pacemaker of his patient from distance. The farmer can water the fields from his home. The MCD can water the plants on roads or operate the street lights from its office. So everything can be seen as an object or entity in this network. Now if we want to operate these things from the car than it needs to have some sensors, controllers, processors, memory, operating system or any specific component based on the specific needs.

Anything that can be remotely accessed is also prone to security breach. This issue has been addressed in mobiles by the SIM (subscriber identity module) card. The SIM card provides the necessary security for identification and authentication. The eSIM (embedded SIM) proposed by the GSMA is paving way for replacement of the present SIM card as they could be remotely provisioned. The present SIM has a 128 bit key that is used in authenticating the SIM on the network. It has space to store location, messages and some contacts. The SIM card is actually a smart card. The smart card provides security and authentication and comes with an IC (integrated chip). A smart card works on normal request-response commands.

Internet of Things or IoT is defined as a network of things. It is the technique by which physical objects can be connected to each other. IoT provides internet connectivity outside mobile phones, workstations, PCs etc. but to things of everyday use like say a water bottle that can be switched on from a smartwatch or smartphone. It has extended the concept of internet connectivity beyond laptops and mobiles. IoT has emerged as the most used and working technology of today. This popularity is because of its ability to upgrade and improve human life on all areas- transportation, communication, societal, political, business, environment, education, healthcare, entertainment, etc.

Intelligent Transportation System is a result of combination of smart technology applied to the field of traditional transportation systems. It compasses a wide variety of features and parameters that provide ease of communication and commutation in everyday life. It deals with adding life quality or associating a lifestyle to the way people travel. Trying to connect a nearby restaurant while driving and placing an order from the car keeping in mind the distance and time needed to reach that restaurant and paying money can be said to be a perfect example of Intelligent Transportation System and this day is not far away when it will be put in practice and business shall thrive out of it.

Vehicle-to-Everything (V2X) is the term given to the process of connecting everything to the car. Everything ranging from other vehicles to any other object is being connected to the car. The driver can operate any function near or far away with the help of this feature. It basically makes the communication seamless by covering all types of communication techniques like: Vehicle-to-Infrastructure, Vehicle-to-Vehicle, Vehicle-to-Network, Vehicle-to-Device, etc. It is a subset of the ITS. And the above mentioned example has perfectly explained the connectivity of a car to restaurant, bill. Similarly there can be any number of example that can be considered.

Machine to machine (M2M) refers to the technology where by any one machine interact with any other machine without human interaction. These are very good for situations that require remote monitoring of any work or anything. M2M communication require the use of highly efficient sensors, ID, uninterrupted power and communication connection. These are effective in the tasks that are hazardous to human lives.

Smart cards come with an integrated circuit. These can be used to carry out a wide range of tasks from authentication, security, identification to any particular task which can be application specific. Example: SIM cards, IDs, RFIDs, Metro cards, etc.

2. Literature Survey

Peng Lin, Qian Zang, Mounir Hamdi, A game formulation of duopoly market with coexistence of SoftSim and regular users, 2012. This paper tells the advantages of softSim over regular SIM cards. The paper basically gives an convergence algorithm based on nash equilibrium for the coexistence of regular users and softSIM users [1].

Kaveh B. Kelarestaghi, Mahsa Foruhandeh, Kevin Heaslip, Ryan M Gerdes, Intelligent Transportation System Security: Impact Oriented Risk Assessment of In-Vehicle Networks, 2019. This paper studies in detail the vulnerabilities, security issues in the in-vehicle system. It studies the various attacks on the cyber physical systems in the transportation domain [2].

Zhigang Xu, Xiaochi Li, Xiangmo Zhao, Michael H. Zhang, and Zhongren Wang (2017), Journal of Advanced Transportation, Hindawi, DSRC versus 4G-LTE for Connected Vehicle Applications: A Study on Field Experiments of Vehicular Communication Performance. This paper deals with DSRC RSUs and LTE cellular ststions and OBUs for connected cars. It compares performance of DSRC and LTE in terms of safety applications on the vehicles. [8]

Agchai Sumalee Hung WaiHo, IATSS Research, Vol 42, Issue 2, July 2018, ScienceDirect, Smarter and more connected: Future intelligent transportation system. This paper studies the current trends in ITS, smart cities related AI techniques, connected environment for urban mobility and future of ITS and smart cities. [9]

Understanding SIM evolution, GSMA Intelligence, Gsmaintelligence.com, March, 2015. This paper tells about the evolution of sim. The basic purpose when it came, the functionality it provides and finally the development it has gone through in the decades. [15]

One M2M Requirements Technical Specification oneM2M.org, August, 2014. This document is provided for future development work within oneM2M. Its goal is to provide specifications for common M2M service layer for connecting to various hardware and software connecting myriad of devices. [18]

One M2M: Security Solutions, oneM2M.org, June, 2017. This document tries to give an overview of the security architecture for global machine to machine platform. [20]

Smart Card Handbook, Wolfgang Rankl, Wolfgang Effing, John Wiley & Sons, 2002. This book attempts to cover aspects of smart card technology. Its history, working, operating system, market, everything. Year after year this book continues to cover the subject of smart cards as completely as possible. [23]

One M2M: Proximal IoT Interworking, oneM2M.org, February, 2017. The document is the specification describing interworking methodologies that is defined by oneM2M for the purpose of representing non-oneM2M devices and applications in oneM2M resource architecture. [19]

Embedded SIM study, Ernst & Young survey, ey.com, September, 2015. The paper studies mobile operators and devices to understand technical and market changes. It concludes that slowly the embedded Sims are replacing the removable Sims and studies its advantages over the later. [14]

Card Specification, Committee and working groups of Global Platform, March, 2006. This document provides a detailed study of card- its history, architecture, maintenance, management and security. [11]

Device API Access Control, Committee and working groups of Global Platform, April, 2017. This document defines API in the mobile operating system based on the security access rules. This is primarily for security issuer. [13]

Smart Cards, Remote APDU structure for UICC based applications (Release 11), ETSI, etsi.org, 2013. This document defines the remote management of UICC based on secured packet structure. It specifies APDU format for remote management. [12]

Security in Machine-to-Machine Communication: The role of the Telecommunication Operator, Francois Ennesser, 8th Security Workshop, Sophia Antipolis, 2012. This paper talks about the security attacks in IoT and M2M devices. It states the cost of attacks. It tells device security improvements. [10]

Communication and Security in Machine-to-Machine Systems, Iva Bojic et. All. It presents current standards and architecture of M2M systems with the focus on communication and security issues, while also discussing current and future research efforts addressing important open issues. One of the main problems in the area is correlated with heterogeneous devices, which are using different technologies for communication. To solve it a unique identifying scheme that enables device identification regardless of used technology is explained. [16]

3. Motivation

With autonomous driving and intelligent transportation system becoming famous, with popularity in space exploration, the high cost of these kinds of projects needs highest amount of security. The malicious hackers try to venture into the on-board equipment of the vehicle and manipulate the entire project under itself. Therefore on-board security has become a top most priority for the ITS industry. Anything which can be connected to Wi-Fi or any other network is prone to security breach. There is an urgent need to work for the security features in car industry.

In case of mobile phones this feature of authentication and security is being taken care by the SIM card. The SIM card is an integrated chip that is put manually inside the mobile phone. It needs space. The SIM card has been started been replaced by eSIM cards that come embedded with the device and can be remotely provisioned. These require smaller space than SIM.

The size of the on-board devices is getting smaller day by day, developers are moving from system on board to system on chip. Integrating everything on a single circuitry becomes too cumbersome. This drove the research to the concept of an on-board softSIM that can be remotely provisioned and is secure. The on-board softSIM is a complete set of software code that shall be assigned to the equipment and which shall carry all the functionality of eSIM as well as more.

The application area is Intelligent Transportation System. So here there is no need of any hardware sim but a software sim that will not occupy any space on the chip and would be very easy to provision. At the same time it is enhancing security in the domain of connected vehicular network.

The main goals of the paper are to provide security in vehicular communication. It aims to provide authentication in vehicular communication. It works to provide cost effective industry products to end users. It provides a flexible platform, inter operative operating system i.e. platform following traditional security mechanism by ISO/GSMA/3GPP/TIA/ETSI/ANSI_41. These services can be changed over the air which is also known as remote provisioning.

In light of the study, the architecture of the on-board softSIM is designed.

4. Architecture

A software sim or soft SIM for the connected vehicular environment that deals with the security and authentication in the industry. This soft Sim shall be configured over the air. It will be able to serve multiple platform as it shall be made platform independent. It will be configured on the on-board device on the vehicle. The sot Sim shall be assigned by the manufactured of the OBE (on-board equipment). It shall be needed to authenticate the vehicle on the network. The network may be cloud or VANET. It is functional enough to run its own Java applets. It can be prepared by hashing techniques. It can be said to be an advanced version of eSIM (embedded SIM). It shall be able to connect to other nodes in the network and access remote resources. Just like a biometric identifies an individual, the soft SIM shall identify the node (vehicle) individually among all other nodes. Hence making the system more reliable and answerable. It can then be further used to record all the data from the vehicle on a storage space along with the information of the nodes and network that it connects to. This data could be used to predict various information about the car (private) or bus (public), the driver, the inside as well as the neighboring environment and other events and entities in the network.

Here is the designed architecture of the Soft SIM.

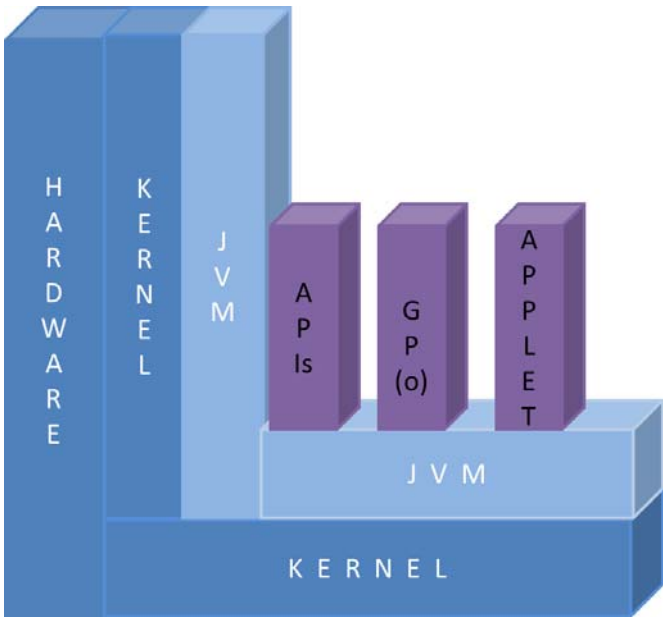

Figure 1. Architecture of the on-board device mounted in vehicle.

Hardware: The hardware is the device surmounted on the vehicle providing the physical connecting equipment. It is the on-board equipment installed on the vehicle.

Kernel: Kernel has the complete system control over everything. It is the operating system core component. It is the central controlling unit. It carries out all the functionality on the device. It shall handle all the operations on the device.

JVM: Java Virtual Machine (JVM) is actually a byte code that provides the run time environment to the applications and applets that carry the different functionalities. The codes running on JVM can be written in java or any other language.

Applets: Independent applications that are used to perform any functionality on the device.

APIs: Application Programming Interface is a computing or programming interface. It is basically a set of protocols and routines. It specifies how software components or other systems can use it. It is basically an interface between two applications. It sends the request and then returns the response.

GP (o): Global Platform is optional and given for any global platform that shall be defined for these connected devices. It is needed to manage heterogeneous connected technologies and integrate them into one platform. It is needed for standardization and uniform protocols in the industry. This itself is a greater challenge and needs continuous upgradation.

Hardware: It consists of all the hardware components: RAM, firmware, NVM, Secondary Storage.

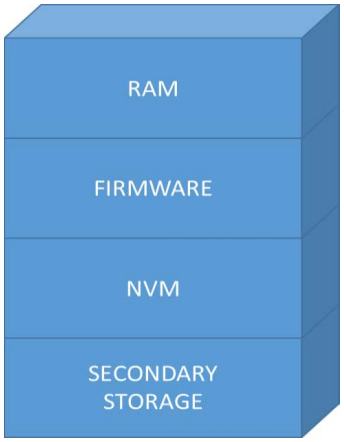

Figure 2.Hardware components

RAM: Random Access Memory is the main memory. It is an erasable memory. It can be written, read, stored and erased at any time. It consists of the working code. Data (information) can be read and written quickly in any order. It is basically a volatile storage.

Firmware: Firmware is the permanent part of ROM. It is a set of software code programmed into the read only memory. It is used to provide low level control for the specific device hardware. It helps in giving instructions on how to communicate with other hardware device components.

Non Volatile Memory: Non Volatile Memory doesn't require a constant power supply and it can operate without power. It provides long term and consistent storage. It need not be refreshed periodically. It is based on semiconductor technology.

Secondary Storage: Secondary storage provides larger permanent data storage needed for the devices to connect to other devices and other information for connection making. It is a non-volatile memory and is used to hold data unless overwritten or explicitly deleted.

The soft SIM is embedded on to the on board device's operating system present in the car. The device consists of its operating system, a java run time environment and device applications in addition to the soft SIM module.

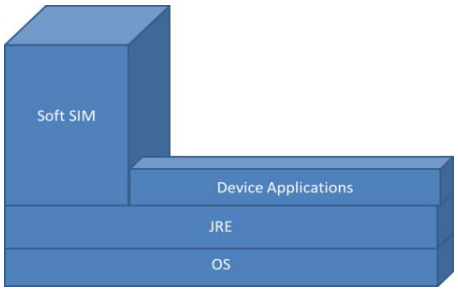

Figure 3. Soft SIM w.r.t. operating system

The soft SIM is installed on the JRE (Java Run-time Environment). The soft SIM can be programmed on any language as there are numerous on board device makers in the market. So keeping this in mind the soft SIM can configured in any language by the manufacturer and run on the java virtual machine.

The soft SIM has three components: Algorithms, KMS, ID

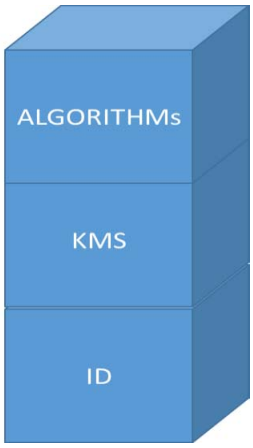

Figure 4. Components of a soft SIM

Algorithms: Algorithms is a step by step procedure defined to attain a task. These are defined for generating the random number for the authentication purpose. It provides a new random number every time that it has to connect to the network or any other node.

KMS: The Key Management System is used to provide keys for secure channel communication. The authorization keys are produced for every session of communication between on board device and the network. It is independent of the equipment. A new session key is generated for every new connection that the device makes.

ID: The soft Sim has a unique Identification Number. It is assigned to the equipment by the equipment manufacturer. It is given only once.

Every application that comes on the device is first authorized by the soft SIM present on the device operating system. Only after authorization, it can execute itself.

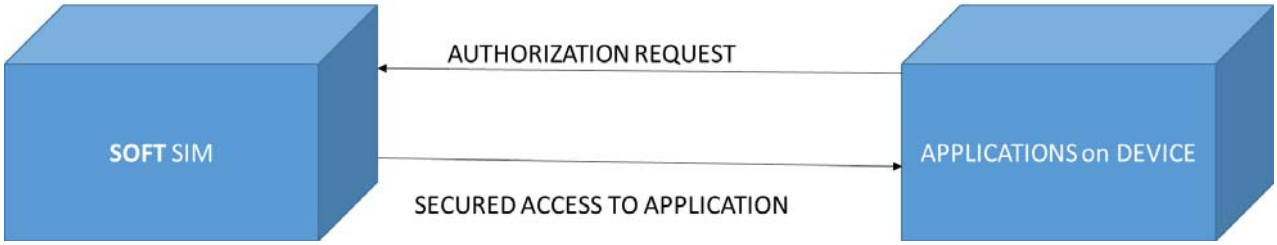

Figure 5. Authentication between soft SIM and application on device

Algorithm 1 : How does the softSIM authenticate itself on the operator:	
1.	SIM sends an ID via the device or the operator stating its identification on the network.
2.	The operator sends a challenge to the SIM.
3.	The SIM has to send an appropriate response to the operator.
4.	Only when the response matches the challenge, a secure connection is established between the SIM and the operator.

The SIM has to authenticate itself on the operator by a sequence of request commands and responses.

ID: The soft SIM identifies itself with the operator. It send its uniquely configured id to the operator.

Challenge: The operator sends a challenge to the SIM. It is made up from the ID hash and a random value. So it is just another random number. This random number is then encrypted by an encryption technique.

Response: It is an authentication signature given by SIM to operator. The authentication algorithm along with challenge and authentication data gives authentication signature.

Connection Established: A secure connection is then established between the SIM and the operator.

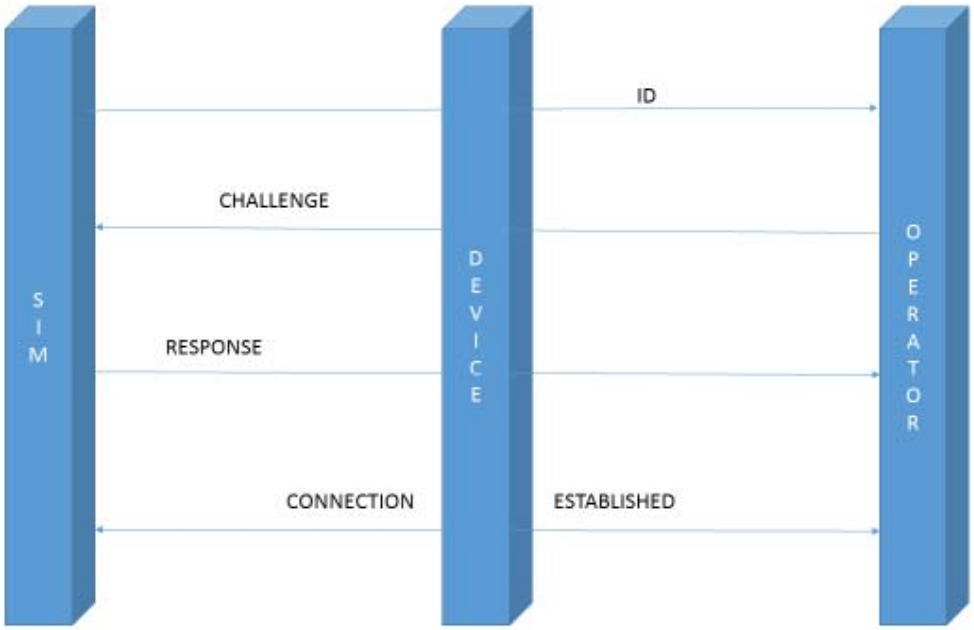

Figure 6 . Authentication flow diagram of soft SIM

5. Analysis

With the growing of more and more cyber physical systems on the connected vehicular environment, the need of safety has increased many folds. The growing of the data day by day has put a question on the authenticity of the data that is being generated. This issue of authenticity has to be addressed urgently. In such a situation the proposed architecture of the on-board softSIM shall definitely address this issues. It by far outweighs the regular on-board devices in terms of security and authentication.

The analysis finds out the unlimited advantages of the on-board softSIM over the regular on-board devices. These are mentioned below:

- It provides cost effective security.
- It is customizable.
- It is reconfigurable.
- It needs no hardware so saves space on the device.
- It provides faster processing.
- It doesn't face the problem of wear leveling.
- It provides flexibility in ecosystem.
- It provides for continuous updating of software.
- There is no need to communicate with the physical smart card vendor for further technical support.
- It doesn't need replacement as needed by physical smart card.
- It could be managed remotely.

6. Conclusion

With the vehicle to everything (V2X) market increasing day by day, every vehicle is getting connected to the internet. These devices that can be connected have a wide variety of range. It may be as small as the tip of the needle or as large as a ship. In such a case where the size of the device is too small, the vendor may want to put minimal required hardware on the device. So here this soft sim shall be highly beneficial in saving space.

The on-board softSIM has a lot of advantages over the hardware sim in providing any authenticate and secure communication in the vehicular environment. It provides all the necessary functionality given in any hardware sim and even does not take any space on the device.

7. Future Scope

The intelligent transportation system has expanded its base from traditional transportation mechanisms to VANET to cloud to artificial intelligence to IoT. When everything gets connected then there is need for security. As security becomes the major concern in the connected world. So arises the techniques and measures that shall govern it. As people wants their data to be private and confidential along with world class quality of service. They also need that they are being connected to the authenticate devices without compromising on service. So authentication and security remain the most popular concern in the time to come. The future work may include- defining and integrating global platform standard for soft SIM in V2X and sharing of RAM between the device and the SIM. The components of operator that support soft SIM shall also be defined. The authorization key- number of bits used, algorithm used, mechanism shall be defined further. The information that will be put on the NVM shall be elaborated. The entire process of how the soft SIM shall communicate with the hardware device shall be established. The kind of information that shall be stored in the soft SIM needs to be carefully planned and put in place. Future developments in the protocol shall be planned. Quick implementation of the project and along with rigorous testing shall be planned. The future holds very bright for the ITS market.

8. Business Case

The business advantages of the on-board soft SIM far out way the efforts put on. It saves manufacturer the cost of production as there is no hardware used to make the sim. So the manufacturing cost is reduced. It saves space on the device chip or board thus helping in space optimization. It provides remote provisioning thus gives vendors a fair competition.

The architecture designed is very light and can be easily adopted into device on-board on cars. Now the business work includes development of the on-board devices with the provision of an in-built softSIM. Testing of the developed product and field testing the same. A sampling plan should be devised to test and also maintain the products. Industries have a lot to contribute in developing and providing for a secure and authenticate way of communication among the vehicular network.

References

[1] Peng Lin, Qian Zang, Mounir Hamdi December, 2012 IEEE Global Comunications Conference (GLOBECOM), A game formulation of duopoly market with coexistence of SoftSim and regular users.

[2] Kaveh B. Kelarestaghi, Mahsa Foruhandeh, Kevin Heaslip, Ryan M Gerdes 2019, IEEE Intellignt Transportation Systems Magazine, PP(99):1-1 – January 2019, Intelligent Transportation System Security: Impact Oriented Risk Assessment of In-Vehicle Networks.

[3] Elyes ben Hamida, Hassan Noura, Wassim Znaidi 2015, Electronics, MDPI journals, Security of Cooperative Intelligent Transport Systems: Standards, Threats Analysis and Cryptographic Countermeasures.

[4] M. Benella, B. Achchab, H Hrimech 2020, Journal of Advanced Transportation, Hindawi, Improving Driver Assistance in Intelligent Transportation Systems: An Agent-Based Evidential Reasoning Approach.
[5] Rui Li, Xin Xue, and Hua Wang 2020, Journal of Advanced Transportation, Hindawi, Characteristics Analysis of Bus Stop Failure Using Automatic Vehicle Location Data Characteristics Analysis of Bus Stop Failure Using Automatic Vehicle Location Data.
[6] Tanveer Muhammad, Faizan Ahmad Kashmiri, Hassan Naeem, Xin Qi, Hsu Chia-Chun, and Huapu Lu (2020), Journal of Advanced Transportation, Hindawi, Simulation Study of Autonomous Vehicles' Effect on Traffic Flow Characteristics including Autonomous Buses.
[7] Zhongtao Cheng, Mao Su, Lei Liu, Bo Wang, and Yongji Wang 2020, Journal of Advanced Transportation, Hindawi, A Coordination Law for Multiple Air Vehicles in Distributed Communication Scenario.
[8] Zhigang Xu, Xiaochi Li, Xiangmo Zhao, Michael H. Zhang, and Zhongren Wang 2017, Journal of Advanced Transportation, Hindawi, DSRC versus 4G-LTE for Connected Vehicle Applications: A Study on Field Experiments of Vehicular Communication Performance.
[9] Agchai Sumalee Hung WaiHo, IATSS Research, Vol 42, Issue 2, July 2018, ScienceDirect, Smarter and more connected: Future intelligent transportation system.
[10] Francois Ennesser 8th Security Workshop, Sophia Antipolis 2012, Security in Machine-to-Machine Communication: The role of the Telecommunication Operator.
[11] Committee and working groups of Global Platform April, 2017, Card Specification.
[12] Committee and working groups of Global Platform April, 2017, Smart Cards, Remote APDU structure for UICC based applications (Release 11).
[13] Committee and working groups of Global Platform April, 2017, Device API Access Control.
[14] Ernst & Young survey Ey.com September, 2015, Embedded SIM Study.
[15] GSMA Intelligence Gsmaintelligence.com March, 2015, Understanding SIM evolution.
[16] Iva Bojic et. al at MIT in year 2012,Communication and Security in Machine-to-Machine Systems.
[17] Koji Nakao 2019, Standardization Trends in Security Technologies for Connected Cars at ITU-T. New Breeze Summer.
[18] One M2M oneM2M.org August 2014, One M2M Requirement Technical Specification.
[19] One M2M oneM2M.org June, 2017, One M2M Security Solutions.
[20] One M2M oneM2M.org February 2017, One M2M: Proximal IoT Interworking.
[21] One M2M oneM2M.org May, 2019, Study on ontologies for Smart City Services.
[22] ITU-R Radiocommunication Sector of ITU 2018, Report ITU-R M.2445-0 Intelligent Transport Systems(ITS) usage M Series.
[23] Wolfgang Effing, Wolfgang Rankl John Wiley & Sons 2002, Smart Card Handbook.