Applied Mathematics & Information Sciences
An International Journal

http://dx.doi.org/10.12785/amis/092L40

Authentication Scheme based on Biometric Key for VANET Information System in M2M Application Service

Keun-Ho Lee[1] *and Soo Kyun Kim*[2,*]

[1] Division of Information and Communication, Baekseok University, ChungNam, Korea
[2] Department of Game Engineering, Paichai University, Daejeon, Korea

Received: 8 Aug. 2014, Revised: 9 Nov. 2014, Accepted: 10 Nov. 2014
Published online: 1 Apr. 2015

Abstract: Smart machines and devices are rapidly deployed in the future, a secure mobile environment will be mandatory. Smart machines and devices of future are being developed towards smart machine and device based M2M(Machine to Machine) by using IT(Information Technology) technology and new science technology. Wireless machines and devices are increasing greatly in the recent years. M2M has shown the advantages of better coverage and lower network deployment cost. It is expected that smart machines will appear as new convergence service model with other machines and devices. Most numerous rese arches within M2M sectors are carried out in intelligent vehicle sector integrated with IT and science technology. Intelligent vehicle section shows severe changes in position between vehicles and has numerous large scales of networks in its components, therefore, it is required to provide safety by exchanging information between vehicles equipped with wireless communication function via biometric information in VANET (Vehicular Ad hoc Network) and fixed apparatus at roadside regarding the status of road. VANET is much more vulnerable to security attacks than wired networks or infrastructure-based mobile networks. This thesis is to propose scheme that mutually authenticates between vehicles by composing vehicle movement as biometric information. We have successfully included the establishment of the detection and prevention of node identity fabrication using biometric key in VANET information systems.

Keywords: M2M, Intelligent Vehicular, VANET, Authentication, Biometric

1 Introduction

Rapid development of IT and science technology has brought changes in development from personal PC to Smart phone, and new service environment is constructed by converging with other peripheral devices based on smart phone. Now IT is leading rapid changes in society. Internet of things is the combination of the variety of information sensing machines and devices, such as RFID(radio frequency identification devices), infrared sensors, GPS(global positioning system), and Internet, forming a huge network, so that all items are connected to the network to facilitate the identification and management, which ultimately provides the full range of service to people everywhere based on the integration of applications. The most important part in the network of things is the interconnection and interoperability between the machines, which is often called M2M. M2M(Machine to Machine) are a collection of wireless mobile machines forming a temporary network without the aid of any established infrastructure or centralized administration. It is a general term of all that can enhance the communication of machinery equipment and capability of network technology, which organically combined in communication between machines and devices, machine control communications, interactive communication, mobile internet communications and other types of communication technologies, to share information with machine, equipment, application process, background information system and operator. Whenever and wherever information is obtained with no difficult, and M2M, which is for communication between machines and surrounding devices, became a major research topic in technology among researchers and wireless communication entities. It creates new and various service environment by applying with new technologies. Research direction of M2M is to transmit a number of information via various communication environments between devices and machines. M2M sectors are carried out in intelligent vehicle sector integrated with IT and

* Corresponding author e-mail: kimsk@pcu.ac.kr

science technology. Intelligent vehicle section shows severe changes in position between vehicles and has numerous large scales of networks in its components, therefore, it is required to provide safety by exchanging information between vehicles equipped with wireless communication function via biometric information in VANET (Vehicular Ad hoc Network) and fixed apparatus at roadside regarding the status of road[1,2]. And one of these researches is to integrate IT and intelligent vehicles to enable various type of information to be transmitted, which mean, various devices are connected and linked to intelligent vehicles. Intelligent vehicles improve the users safety by implementing advanced technology like machinery and electronics, communication environments, and control environments in the telecommunications of the car, and secure comfortable driving environment. It reduces casualties in case of dangerous car crashes and makes the car more than a basic means of transportation by enabling it to share information and making it a work environment and even leisure environment. To improve the security in the cars of the drivers, it needs to be able to monitor the surrounding and interior conditions and make it easy for the drivers to be alerted of the dangers that occur. An intelligent vehicle can improve the safety and convenience of the driver while enabling the car to operate various information operations that are needed in driving by itself by giving it many advanced technologies. For the future advancement of intelligent cars there needs to be information such as safe driving through the information system of the intelligent vehicles, public services in the transportation sector, and vehicle diagnostics and analysis of the various security threats that can occur in the intelligent information system in the intelligent vehicles to enable the user to quickly and accurately determine the various information transmitted in real time and to make the driving environment safe and comfortable[3]. This thesis aims to examine what security factors exist in M2M and VANET, compose VANET as non-infrastructure and infrastructure in shadow area in cluster configuration architecture, and then propose authentication scheme of shadow area in VANET. Finally, we show the performance evaluation of the proposed authentication scheme based on shadow area in VANET.

2 Related Work

2.1 M2M(Machine to Machine) Service

M2M service is defined as Machine to Machine, Machine to Man, and Man to Machine. As depicted in figure 1, various devices are installed to communicate and collect information from surrounding M2M terminal and sensor nodes. Its concept is to provide information service to people and surrounding machines using network provider. M2M is utilized in the sectors of sensor network, transport, and emerging device. Core technologies in M2M are identification, information collection, communication, intelligence and minimization, and every devices and system should be maintained autonomously and securely through control and information exchange between machines and devices.

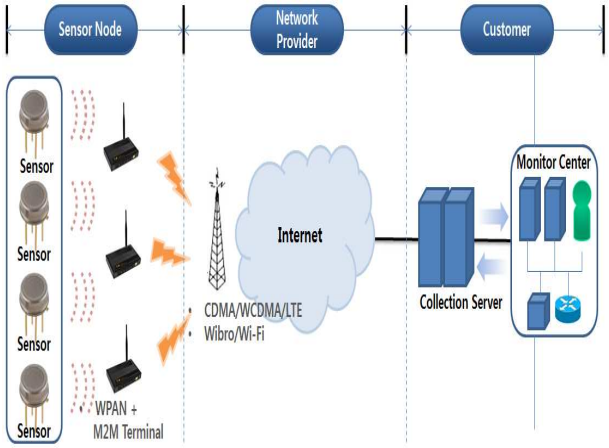

Fig. 1: M2M Architecture

Threatening factors in devices in M2M architecture are bugging between equipment, hijacking, and alteration of privacy in relation with denial. There are possible threatening factor in gateway such as authorization violation by illegal usage and access, physical intrusion, replay attack and main-in-the middle attack. Other types of threatening factors are paralysis through illegal intrusion, service denial, virus, worm, troy wooden horse and depletion of resources[4].

2.2 Intelligent Vehicle Service

Intelligent vehicle service is evolving with various types of services to provide convenience of life by integrating with home network, telematics and intelligent robot thanks to development of convergence technology. As seen in figure2, intelligent vehicle communication network technology is classified with internal network and external network of vehicle from the reference point of vehicle. V2V(Vehicle to Vehicle) establishes vehicle communication network which construct communication network based on vehicletovehicle communication without having infrastructure of transmitting information, whereas V2I(Vehicle to Infrastructure) lets vehicle accesses infra network via wire and wireless communication and provides communication network that supports communication between terminals and servers. V2V provides vehicle collision warning services and group communication based on communication

between vehicles, whereas V2I provides IP based traffic information, safety support and download service to vehicles [9,10,11].

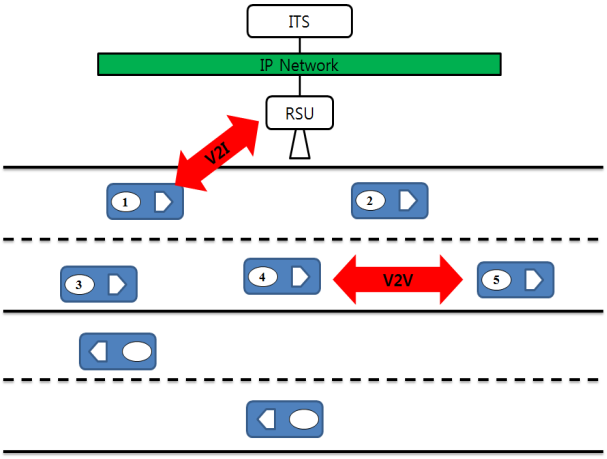

Fig. 2: Intelligent vehicle Architecture

Intelligent Transport System (ITS) is a new age transport system that implements various advanced technology to the current transportation system to manages the congestion of traffic efficiently, to dramatically improve the safety of car crashes and to solve various problems in environmental and energy, time and costs of traffic, and automation of transport systems. There are different categories such as ATMS (Advanced Traffic Management System), ATIS (Advanced Traveler Information System), APTS (Advanced Public Transportation System), CVO (Commercial Vehicle Operation), and AVHS (Advanced Vehicle and Highway System) TMS detects traffic information such as speed and the characteristics of vehicles on the road [3,5]. Mobile ad hoc networks are currently a very active area of academic and industrial research for their foreseeable broad applications. These networks do not have any fixed infrastructure. The vehicles in ad hoc networks are usually limited devices with respect to their energy sources, computational capabilities and communication range. However, it is vulnerable to a wide range of attacks due to the open medium, dynamically changing topology, possible vehicle compromise, difficulty in physical protection, absence of infrastructure, and lack of trust among vehicles[6,7]. There are many security issues which have been studied in recent years. For instance, snooping attacks, wormhole attacks, black hole attacks, routing table overflow and poisoning attacks, packet replication, denial of service (DoS) attacks, distributed DoS (DDoS) attacks, et cetera. Especially, the misbehavior routing problem is one of the popularized security threats such as black hole attacks. Some researchers propose their secure routing idea to solve this issue, but the security problem is still unable to prevent completely [8]. On-board Tampering is executed in a way of modifying speed, position, vehicle interior status information and various sensing information of on-board vehicle [9,12].

3 Intelligent Vehicle Security Threats

There are many security threats such as accessing information using the vulnerabilities that occur between the communications of the intelligent vehicles and ITS and accessing information using inside people.

3.1 Security threats considerations

- DDOS(Distributed Denial Of Service)
By placing a large number of distributed attackers to attack the ITS server, it makes it impossible to provide fast, safe, and pleasant transport system service.

- Authority
By acquiring elevated privileges by figuring out the system administrator password by using the brute force attack, the attacker can alter the speed, characteristics information and traffic information.

- ARP Spoofing
By tampering with the ARP cache memory of the ATIS system, the attacker can set the MAC address to his own MAC address to enable it to check all the information to monitor various data and traffic information.

- SQL Injection
The attacker can use the inner people resources in the APTS system to force insert SQL syntax to leak or alter the data on the server.

- Session Hijacking
The attacker can steal the connection status between the AVHS system and the driver to eavesdrop and alter all the data transmitted and can even acquire authorizations of the server.

3.2 Security considerations

- Encryption
Transmit the information systems data converted to a encrypted code unidentifiable by 3rd parties.

- Hash algorithm
It is impossible to decode input messages with the same hash values so it can figure out if the data has been altered during the transmission to a intelligent vehicle by a 3rd party by hash checks by hash functions.

- Pack analysis
By using packet analysis tools on the information system networks, one can analyze information like packet numbers and TCP, UDP, Port, MAC, and IP to identify, prevent and manage various attacks beforehand.

- Physical security

There needs to be protection of the intelligent vehicle and information system assets for threats like fires, destruction, and theft.

- Biometrics

Biometrics verifies that the person boarding the car is a verified user that is trying to access the information system by comparing the entered characteristic inputs and registered characteristic inputs which are extracted from unique and highly discriminatory characteristics.

4 Authentication Scheme based on Biometric

4.1 Introduction Background

There needs to be a guarantee of confidentiality and integrity from the security threats that can occur in the process of requesting authentication between ITS server to driver, between driver to driver and when using services by using biometric keys and encryption process as figure 3.

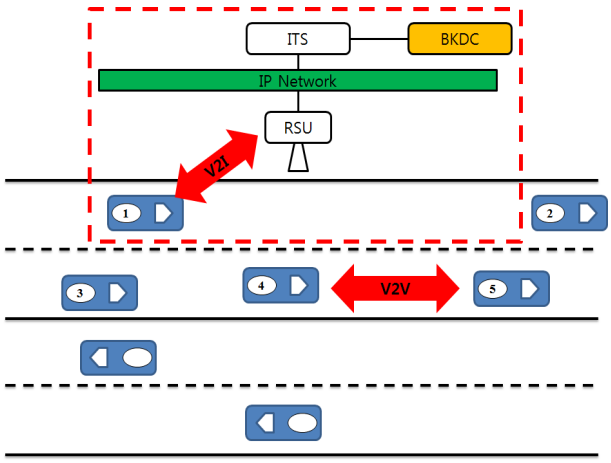

Fig. 3: ITS registration process using BKDC

4.2 Notation

We use the notation listed in Table 1 to describe the proposed scheme.

Table 1: Notation in authentication scheme

BKDC(Biometrics Key Distribution Center)	A reliable biometric key distribution center that can provide biometric information on all drivers and users account management
CBK(Center Biometrics Key)	Biometrics based personal key of the BKDC
UBK(User Biometrics Key)	Biometrics based personal key of the user
SBK(Server Biometrics Key)	Biometrics based personal key of the server
TGT(Ticket-Granting Ticket)	A ticket that contains information like the driver's name and expiration time
SA	A session key between the driver and BKDC
KAB	A session key between the ITS server and BKDC

4.3 Authentication Scheme based on Biometrics

The BUKAS (Biometrics unified Kerberos Authentication scheme) scheme is a method integrating biometric authentication method to the Kerberos authentication method for existing users and it is a mechanism suggested to protect intelligent vehicles from security threats. In the Kerberos authentication method that uses the existing symmetric key passwords, there exists a reliable KDC (Key distribution center). In the KDC there are 3 personal keys KA, KB, and KKDC to mutually authenticate the server and the user. However in the BUKAS scheme the KDC is replaced by BKDC, the key distribution center based on biometrics, and the personal keys of the user, server, and KDC is replaced by UBK, SBK, and CBK acquired from biometric authentication. The process of the BUKAS authentication scheme is as follows.

- New biometric information registration

The driver transmits his biometric information to the BKDC, as figure 4. Because personal biometric information is unique, 3rd parties cannot exploit it even if he intercepts.

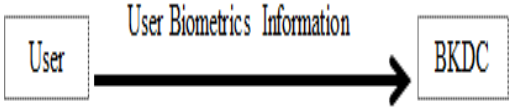

Fig. 4: Biometric information transfer process

BKDC transmits SA encrypted with UBK and transmits tickets containing SA encrypted with CBK, as figure 5. Through this the user can trust and authenticate the BKDC that has his UBK which is his personal key.

- User authentication using BKDC

The driver transmits an encrypted timestamp that is used

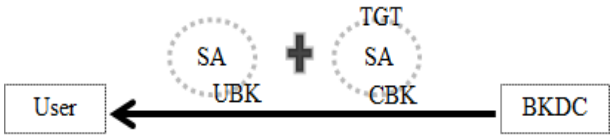

Fig. 5: User authentication

in time syncing to BKDC with the SA acquired through the ticket encrypted with CBK received from BKDC and his UBK, as figure 6. BKDC decodes the ticket with its own CBK to acquire SA and through the acquired SA acquires the time stamp. BKDC can verify that the driver is legitimate by confirming that the driver acquired SA from decoding through the UBK and that he sent the time stamp encrypted by the SA. Through this the user and the BKDC can verify each other as legitimate.

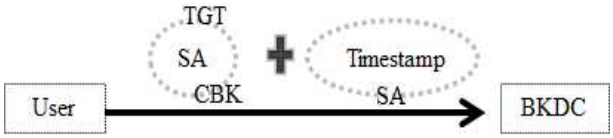

Fig. 6: BKDC authentication

BKDC sends the server ticket containing the session key between the BKDC and server, KAB, encrypted by SBK in the driver ticket containing KAB all encrypted by SA to the driver. The driver acquires server ticket and session key KAB by decoding through the SA.

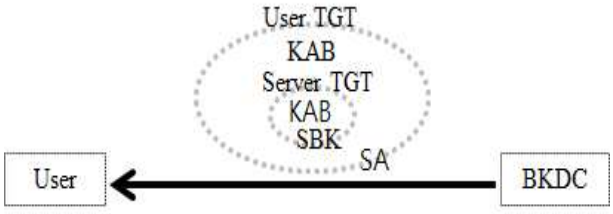

Fig. 7: User and server mutual authentication

The server is ITS. The user sends the acquired server ticket to the server and transmits the time stamp, used in time syncing, encrypted with session key KAB. The server acquires KAB through decoding with its personal key SBK and through decoding with the acquired KAB acquires the time stamp. The server can verify the user that owns KAB and also can verify the legitimacy of the BKDC as a valid biometric key distribution center that it sent with personal key SBK. Thus BKDC, the user, and the server can mutually verify each other.

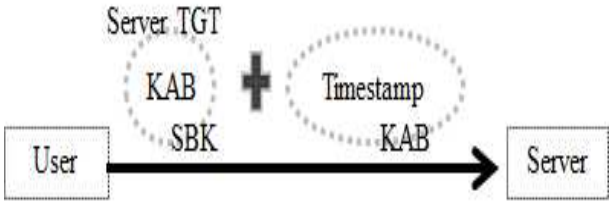

Fig. 8: Server authentication

5 Attack Analysis

In this section, we discuss how authentication scheme based on biometrics is able to deny possible attacks in VANET information system. As scheme establishes authentication based on a trusted layer, it guarantees end-to-end security and V2V. We evaluated the performance of our scheme and identified the advantages and limitations of our proposed approach. In our scheme, a BKDC establishes a vehicle that is worthy of trust by the other members of the ITS. Falsehood detection in the certification process is achieved. Authentication scheme and protocol is more reliable during the certification of a BKDC because it uses a server and it has fewer processing operations. The scheme and protocol enforces stronger security as it uses a server to obtain a higher level of security than can be realized by other normal ITS authentication systems. An analysis of its performance verified its authentication, efficiency, safety, and scalability. Authentication and non-repudiation use a cryptographic certificate. Each vehicle receives a certificate from its trusted BKDC. We evaluated four performance metrics:

- Modification Attacks

Attacks using modification are generally targeted against the integrity of routing computations. By modifying routing information, an attacker can cause network traffic to be dropped, redirected to a different destination, or to take a longer route to its destination, resulting in increased communication delays. Proposed BUKAS scheme can use the session keys to encrypt the traffic flow of both data and control packets. Therefore, since the Kerberos authentication method of the message contents is included in every packet transmitted, the integrity of the contents is guaranteed, along with confidentiality using BKDC by biometric information key.

- Fabrication Attack

Fabrication attacks involve generating false routing

messages. These attacks are difficult to recognize as they are received as genuine routing packets. The authenticity of the received control and data packets can be verified using the session keys and the ITS server and BKDC. As the session keys are unique, fabricated packets can easily be detected and hence discarded.

- Spoofed Route Attack

A malicious vehicle can launch several attacks in a network by masquerading as another vehicle (spoofing). Spoofing occurs when a malicious vehicle misrepresents its identity by altering its MAC or IP address in order to fool a benign vehicle into arriving at an inaccurate picture of the network topology. Proposed scheme participation accepts only packets that have been signed with a certified key issued by a trusted authority using a BKDC. There are many mechanisms for authenticating users to a trusted certificate authority. Since only the source vehicle can sign using its own private key, vehicles cannot spoof other vehicles in route instantiation. Consequently, the legitimacy of all packets is verified automatically during the decryption phase, ensuring that any packets that were spoofed are discarded.

6 Conclusion

This research analyzes the existing security vulnerabilities of the intelligent vehicle information system technology to enable the technology to achieve speed, accuracy, and safety. Also it suggests directions to set standards to implementing the prevention methods and solutions by analyzing the security threats that can surface. Through this it is expected that it would broaden the perspective on security awareness and explore more effective and safe prevention methods and solutions by identifying the relevance various possible security issues.

Acknowledgement

This research was supported by Basic Science Research Program through the National Research Foundation of Korea(NRF) funded by the Ministry of Education, Science and Technology(No.2012-0003141)

References

[1] You-Boo Jeon, Keun-Ho Lee, Doo-Soon Park, Chang-Sung Jeong, Cluster Authentication Protocol based on VANET in M2M, FTRA AIM2012, pp. 43-44 (2012)

[2] Du Jiang, CHAO ShiWei, A Study of Information Security for M2M of IOT, in Proceedings of the 2010 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE), pp.576-579 (2010)

[3] Tae Yang Kim, Keun-Ho Lee, Information System based Authentication Scheme Intelligent Vehicles, The 2nd International Conference on Convergence Technology2012, pp.282-285 (2012)

[4] Gab-Sang Ryu, Keun-Ho Lee, Authentication based on Cluster in Machine to Machine, Journal of The Korea Knowledge Information Technology Society, **5**, 103-110 (2010)

[5] Do Baek Na, Sang Beom Lee, Intelligent Vehicle Information Systems Technology. Korea Society of Machine Tool Engineers, **13**, pp.2-98 (2004)

[6] Mohsen Imani, Mahdi Taheri, M.Naderi, Security enhanced routing protocol for ad hoc networks, JoC(Journal of Convergence), **1**, 43-48 (2010)

[7] Surasee Prahmkaew, Performance Evaluation of Convergence Ad Hoc Networks, JoC (Journal of Convergence), **1**, 101-106 (2010)

[8] Fan-Hsun Tseng, Li-Der Chou, Han-Chieh Chao, A survey of black hole attacks in wireless mobile ad hoc networks, HCI(Human-centric Computing and Information Sciences), 1:4, (2011)

[9] Gi-Weon Kim, Soo-Kyun Kim, Keun-Ho Lee, The Security Requirement based on Intelligent Vehicular Network in M2M Environment, Journal of The Korea Knowledge Information Technology Society, **5**, 124-129 (2010)

[10] Maxim Raya, Panos Papadimitratos, and Jean-Pierre Hubaux, Securing Vehicular Communications, In Magazine of IEEE Wireless Communications IVC Specials, EPFL, pp.8-15 (2006)

[11] Inhyok Cha, Yogendra Shah, Andreas U. Schmidt, Andreas Leicher, and Michael Victor (Mike) Meyerstein, Trust in M2M Communication, IEEE VEHICULAR TECHNOLOGY MAGAZINE, pp. 69-75 (2009)

[12] Dong-Hoon Kim, Jun-Yeob Song and Seuk-Keun Cha, Introduction of Case Study for M2M Intelligent Machine Tools, Proceedings of 2009 IEEE International Symposium on Assembly and Manufacturing, pp. 17-20 (2009)

Keun-Ho Lee is a professor in the division of information and communication at Baekseok University. He received the B.S. degree in computer science from Soonchunhyang University, Korea in 1998, the M.S. degree in electronic commerce from Soonchunhyang University, Korea in 2001, the Ph.D. degree in Computer Science from Korea University in 2006. He was the manager of the Samsung Electronic in 2006-2010. His research interests include ad hoc, sensor, ubiquitous, m2m, intelligent vehicle, and mobile communication security. He is a member of IEEE Computer Society.

Soo Kyun Kim received Ph.D. in Computer Science & Engineering Department of Korea University, Seoul, Korea, in 2006. He joined Telecommunication R&D center at Samsung Electronics Co., Ltd., from 2006 and 2008. He is now a professor at Department of Game Engineering at Paichai University, Korea. Professor Kim has published many research papers in international journals and conferences. Professor Kim has been served as Chairs, program committee or organizing committee chair for many international conferences and workshops; Chair of ICCCT11, ITCS10, HumanCom10, EMC10, ICA3PP10,,FutureTech10, ACSA09, Em-Com09, CSA09, CGMS09, ISA09, SIP08,FGCN08 and so on. Also Professor Kim is guest editor of the International Journal of IET Image Processing and Multimedia Tools and Applications. His research interests include multimedia, pattern recognition, image processing, mobile graphics, geometric modeling, and interactive computer graphics. He is a member of ACM, IEEE, IEEE CS, KACE, KMMS and KIIT.