차량 애드 혹 망을 위한 생체 키 기반의 인증 기법

이근호*

Authentication Scheme based on Biometric Key for VANET(Vehicular Ad hoc Network)

Keun-Ho Lee*

요 약 사물지능통신은 낮은 네트워크 비용과 범위에서 이점을 가지고 있다. 사물지능통신의 지능형 자동차는 구성 요소와 망 규모의 비율로 차량간 위치에서 극심한 변화를 보여준다. 지능형 자동차는 무선 통신 기능으로 자동차 장치들 간에 정보를 교환하기 위해 차량 애드 혹 망에서 생체 정보를 통하여 안전성 제공을 요구한다. 본 논문은 자동차 이동시 자동차간의 상호 인증을 위해 생체 정보를 제공하는 기법을 제안한다.

주제어 : 사물지능통신, 지능형자동차, 차량 애드 혹 망, 인증, 생체

Abstract M2M has shown the advantages of better coverage and lower network deployment cost. 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). This thesis is to propose scheme that mutually authenticates between vehicles by composing vehicle movement as biometric information.

Key Words : M2M, Intelligent Vehicular, VANET, Authentication, Biometric

1. Introduction

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. 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 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

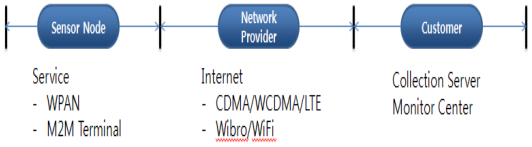
*백석대학교 조교수
논문접수: 2012년 10월 30일, 1차 수정을 거쳐, 심사완료: 2012년 11월 30일

roadside regarding the status of road[1][6].

2. Related Works

2.1 M2M(Machine to Machine) Service

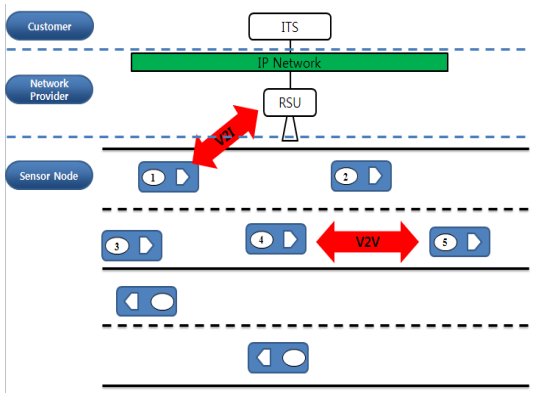
M2M service is defined as Machine to Machine, Machine to Man, and Man to Machine. As depicted in figure 1, various devices are installed to communicate and collect information from surrounding M2M terminal and sensor nodes. Its concept is to provide information service to people and surrounding machines 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[2].



[Figure 1] M2M Architecture

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 vehicle - to - vehicle 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[3][4][5].

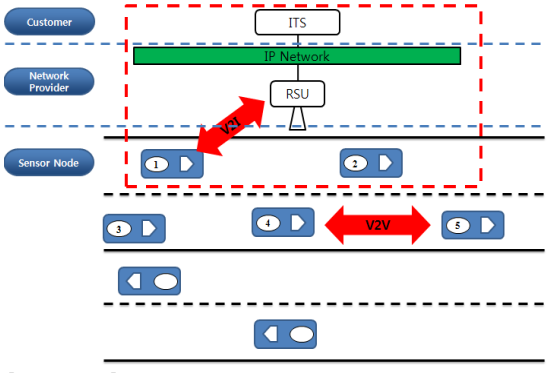


[Figure 2] Intelligent vehicle Architecture

3. Authentication Scheme based on Biometric

3.1 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.



[Figure 3] ITS registration process using BKDC

3.2 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

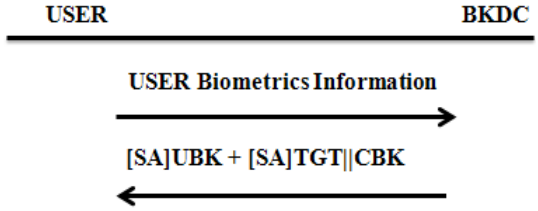
3.3 Authentication Scheme based on Biometrics

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

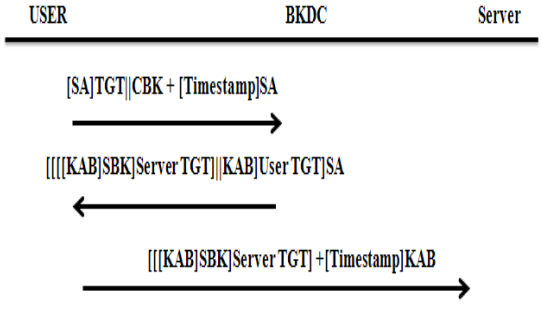
The driver transmits his biometric information to the BKDC, as figure 4. Because personal biometric information is unique, 3rd parties cannot exploit it even if he intercepts. BKDC transmits SA encrypted with UBK and transmits tickets containing SA encrypted with CBK, as figure 4. Through this the user can trust and authenticate the BKDC that has his UBK which is his personal key.



[Figure 4] Biometric information transfer process and User authentication

- User authentication using BKDC

The driver transmits an encrypted timestamp that is used in time syncing to BKDC with the SA acquired through the ticket encrypted with CBK received from BKDC and his UBK, as figure 5. 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.



[Figure 5] User, BKDC and Server 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.

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.

4. Attack Analysis

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 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.

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.

5. 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.

References

[1] 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), 2010, pp.576-579.

[2] Gab-Sang Ryu, Keun-Ho Lee, Authentication based on Cluster in Machine to Machine, Journal of The Korea Knowledge Information Technology Society, Vol 5, No.6, 2010, pp.103-110.

[3] 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, Vol 5, No.6, 2010, pp.124-129.

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

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

[6] You-Boo Jeon, Keun-Ho Lee, Doo-Soon Park, Chang-Sung Jeong, Cluster Authentication Protocol based on VANET in M2M, FTRA AIM2012, 2016, pp. 43~44

이 근 호

- 2006년 8월: 고려대학교 컴퓨터학과 (이학박사)
- 2006년 9월~2010년 2월: 삼성전자 DMC연구소 책임연구원
- 2010년 3월~현재: 백석대학교 정보통신학부 조교수
- 관심분야: M2M 보안, 이동통신 보안, 융합 보안, 개인정보보호
- E-Mail: root1004@bu.ac.kr