The UMTS-AKA Protocols for Intelligent Transportation Systems*

Hsia-Hung Ou‡ Min-Shiang Hwang† Jinn-Ke Jan‡

Department of Management Information Systems†
National Chung Hsing University
250, Kuo Kuong Road,
Taichung, Taiwan 402, R.O.C.
Email: mshwang@nchu.edu.tw

Department of Computer Science and Engineering‡
National Chung Hsing University
Taichung, Taiwan 402, R.O.C.

July 2, 2009

*This work was supported in part by Taiwan Information Security Center (TWISC), National Science Council under the Grants NSC 96-2219-E-001-001, and NSC 96-2219-E-009-013.

†Corresponding author: Prof. Min-Shiang Hwang.

The UMTS-AKA Protocols for Intelligent Transportation Systems

Abstract

The integration of communication protocols into transport systems is a much adored research area today. Much of seminal work has been reported on the topic of intelligent transportation systems (ITS) in the recent years. Many advanced techniques have been garnered to improve online communication and to promote the security, comfort, and efficiency of ITS. Of primary importance to the effective application of ITS is the communication protocol used. A fascinating development is that the yesterday's Global System for Mobile Communication protocol is being replaced by the Universal Mobile Telecommunication System protocol, which is the third-generation mobile technology. This article attempts to identify a suitable communication system for ITS applications. It is impracticable to substantially modify the original UMTS-IMS-AKA protocol which is in practice because it can disturb the operation of the current system, and thus we explore other possibilities through this research. We investigate a novel protocol to make the original UMTS-IMS-AKA protocol compliant with ITS as well as adaptable into the current UMTS protocol.

Keywords: ITS, AKA, UMTS, IMS, Authentication, Security, Group key, Mobile communication

1 Introduction

According to the US Department of Transportation, "Intelligent transportation systems (ITS) encompass a broad range of wireless and wire line communications-based information and electronics technologies. When integrated into the

transportation system's infrastructure, and in vehicles themselves, these technologies relieve congestion, improve safety and enhance American productivity" [40]. To put it simpler, a vehicle's computer integrates the systems for information, communications and vehicle detection, as well as encompasses the technology needed to carry out these processes. Of the many different applications of ITS, a select few are as follows: 1) it improves the interaction between people, cars, roads, and transportation systems; 2) it promotes security, efficiency, and comfort in conveyance systems, and reduces the impact of transportation upon the environment; 3) it provides a diverse range of services, such as travel and traffic management, public transportation management, electronic payment services, commercial vehicle operations, emergency management, advanced vehicle safety systems, information management, and maintenance and construction management [18]. A much simplified and logical model of ITS is illustrated in Figure 1 [17]. The research on ITS is too vast to be covered in a single article like ours. Thus, this article covers only a small part of the issues surrounding ITS. Our focus is especially on the issues in communication.

1.1 Characteristics of ITS

Signals are delivered to the different elements of ITS with the help of the communications infrastructure. The communications infrastructure consists of an array of diverse systems, which may be classified into wired networks and wireless networks. These networks may be either public or private, such as public land mobile networks, personal communication networks, public land mobile communications systems, private networks, packet switched data networks, integrated services digital networks, public switched telephone networks, and broadcast networks. These network forms should have the following characteristics so as to be suitable for ITS [14], there are: 1) Support communication services including: voice, data, image, video, and signaling; 2) Accommodate a

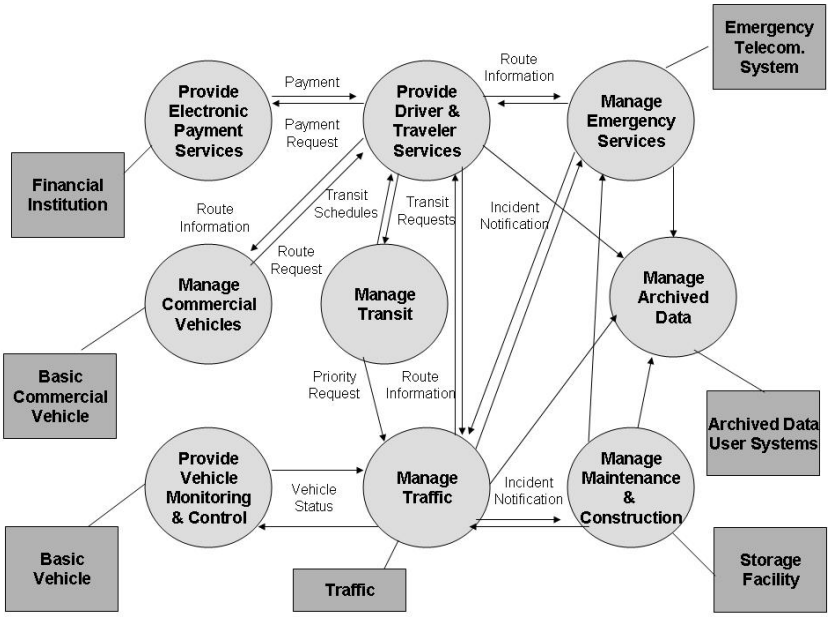

Figure 1: Article describing simplified ITS

wide variety of terminals, e.g., fixed, portable mobile, and in-vehicle mobile; 3) Preserve upward/downward terminal compatibility; 4) Allow mobile and fixed users to utilize the services without geographical barriers (i.e., seamless communication); 5) Provide service flexibility so that any combination of services may be used; 6) Make efficient and economical use of the spectrum; 7) Provide user authentication and billing functions; 8) Provide varied degrees of network security that preserve user privacy; 9) Have modular structures that allow the systems to start from small and simple configurations and then grow as needed in size and complexity; 10) Generally use open architectures that permit easy introduction of advanced technology and support new applications.

Since communication services involve exchanging information between different systems, it is important to integrate the different types of communications systems rather than design an exclusive one. The hierarchical structure for communication services is as shown in Figure 2 [14].

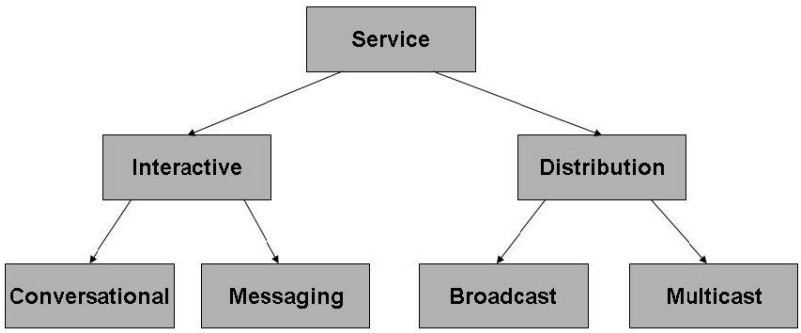

Figure 2: Communication services hierarchy

1.2 MANET and VANET

A major part of current research concerning the communications network in transport systems surrounds Vehicle Ad hoc NETwork (VANET) [14, 20, 24, 26, 27, 31, 44], VANET focuses on messaging, broadcasting, and multicasting, which many think are services difficult to be implemented or accomplished with the existing telecommunications techniques, namely GSM and UMTS. One of the key objects of this research is to identify a communication system that is suitable for ITS. Our focus is to extend on the existing UMTS-AKA (Authentication and Key Agreement) protocol with a view to making it compliant with ITS.

Although the ITS communication environment is classified into wired and wireless networks, much of development bottlenecks surround the wireless side. The current wireless networks mainly take IEEE 802.11 (especially 802.11p is still active by IEEE 802.11 working group and scheduled to be published in July 2008) as the standard. Infrastructure and Ad hoc are widely used. All mobile nodes working within the infrastructure must connect to the access point for transmission. Unlike the infrastructure mode, devices in the Ad hoc mode do not need access points for transmission. Ad hoc relies on point-to-point networks that they constitute along with the members of mobile nodes. One such network using Ad hoc framework is MANET. The ITS communication

environment can be simply classified into "car-to-car communication" (C2CC, or inter-vehicle communication, IVC) and "car-to-infrastructure communication (C2IC)" [34, 43]. The Ad hoc network is most suitable for C2CC. An improved version of MANET called VANET has also been proposed [32, 45].

Its security architecture can be found in [13, 22, 23, 28, 25, 30, 35, 37, 38, 42, 46]. VANET has five characteristics that meet the needs of inter-vehicle communication: high mobility, large number of nodes, no centralized infrastructure, user privacy, and no user interaction. VANET must suit increased movement, more nodes, and higher computational overhead (since its mobile node is the vehicle's computer rather than a PDA or a mobile phone). VANET can deliver information over the Ad hoc network formed with neighboring vehicles. Although VANET was designed exclusively for ITS, it comes with innate drawbacks. One is the scalability program [14]. In a large and distributed environment, scalability is crucial. This is especially the case for vehicles that travel very far apart from each other, in which case signal delivery cannot continue between them. Additionally, vehicle obstruction can lead to increased bandwidth overhead. Furthermore, the ease of disclosure of sensitive information over wireless networks [20, 44], general privacy management [16, 29, 31], and location program [21, 41] are subjects relating to VANET that must be urgently resolved.

1.3 Communication Types in ITS

The ITS communications infrastructure can be classified into two major types: wireless and wired communication systems. Wireless communication can be further classified into wide-area and short-range communication systems. Short-range communication has two subdivisions: dedicated short-range (formerly vehicle-to-roadside) and vehicle-to-vehicle communications [39].

Wide-area communication systems are currently used for cellular phone communication, and short-range communication systems are used in VANET.

At present, cellular phone communication systems are very widely used, and network coverage is nearly universal. It is much easier to use the existing cellular phone networks and improve upon them rather than develop a new VANET. The cellular phone network is reliable and will continue to evolve and mature. In addition to being popular and stable, the benefit of cellular phone networks is that the infrastructure is already in place. However, VANET will still be needed for vehicle-to-vehicle communication.

1.4 The rests of the article

The focus of this research is on developing a cell phone-based system to replace VANET and thus eliminate the bottleneck that has developed with regard to improving this form of ITS communication. The remainder of this article is organized as follows. In Section 2, we review the UMTS technology, AKA protocol, and MBMS (Multimedia Broadcast/Multicast Service). In Section 3, we extend the UMTS-IMS-AKA (IMS: IP Multimedia System) protocol which is based on a group key. This proposed protocol is compliant with ITS. In addition, we also propose a dedicated vehicle-to-vehicle communication system in this section. Related discussion and analysis will be presented in Section 4. Finally, we give our conclusions in Section 5.

2 Relevant UMTS Technology

UMTS is the third-generation (3G) mobile telecommunications technology that evolved from GSM of the second generation (2G). UMTS is widely compatible than GSM and has thus gradually replaced it to become the most ideal system for mobile phone communication. Compared with GSM, UMTS contains bigger bandwidth to allow larger downloads and uses reliable safety mechanisms. Its convenience has been widely appreciated, and thus it proliferated all over the globe. GSM does two types of services: CS (circuit switched) service and PS (packet switched) service. CS service is responsible for traditional speech

telecommunication. PS service provides the forerunner's packet switching to support IP. It has the security characteristics [3] required by ITS environments, and can attain the goals outlined earlier. UMTS is also a wide-area wireless infrastructure that can support the delivery of a large number of packets as well as many broadcasts or multicast information. Through a special BS (basic station), it can also support short-range information transfer. In contrast, dedicated wireless systems are not easily supported by UMTS. However, we think our technique can accomplish this. In this section, we first introduce the UMTS-AKA protocol [2], the UMTS-IMS-AKA protocol [1], and the UMTS-MBMS protocol [10, 11]. In the following section, we describe how they are suitable to an ITS environment.

2.1 UMTS-AKA and UMTS-IMS-AKA Protocols

The UMTS-AKA protocol [2] is an authentication and key agreement protocol. It is equipped by the 3GPP (3rd Generation Partnership Project). The objective is to meet the requirements of UMTS so that the mobile device can stay secure both during the authentication process and during the telecommunication session. As shown in Figure 3, the UMTS-AKA protocol has two phases. One is the phase of distribution of authentication vectors from HE (Home Environment) to SN (Service Network). The other is the phase of authentication and key establishment. Table 1 defines the relevant symbols.

When an MS enters into the service domain of the SN, or VLR (Visitor Location Register), for the first time, it is executing the phase of distribution of authentication vectors from HE to SN and completing a registration procedure. This procedure, in addition to making MS's HE aware of the MS location, can let the SN obtain the AVs (Authentication Vectors) from MS's HE (for authentication with the MS in the future). AVs include the n set of authentication vectors and can provide n time authentication between MS and SN. If MS is always registered and it wants to use a service in SN, it can

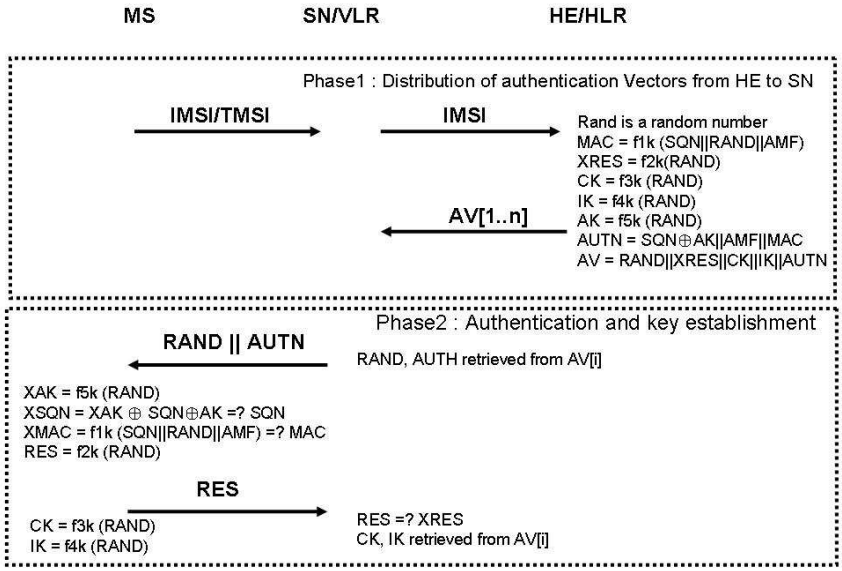

Figure 3: UMTS-AKA-protocol

execute the phase of authentication and key establishment leading to mutual authentication. Thus they confirm the legitimacy of each other. In this protocol, the basis of authentication is a secret key that is shared between MS's HE and MS. Through USIM (Universal Subscriber Identity Module) protection, this key can be recognized only by MS and its HE. SN and HE may be different system operators; this characteristic helps UMTS to expand its service range (and thus make our application ITS-compatible). Once authenticated, both parties can establish the cipher key and the integer key. Using these keys allows their messages to remain private.

UMTS is a huge system constituted by many subsystems to keep abreast of the demands. The UMTS-AKA protocol is the main mechanism for authentication and key establishment. The different subsystems operate a bit differently because of varied demands; however, the same concept is reused for the IP multimedia core network subsystems, where it is called the UMTS-IMS-AKA protocol [1]. Figure 4 illustrates this procedure, while Table 1 defines the relevant symbols.

Table 1: Symbols used in UMTS-AKA-protocol/UMTS-IMS-AKA-protocol

MS, SN, HE	Mobile Station, Service Network, Home Environment
VLR,HLR	Visitor Location Register, Home Location Register
AuC, SQN	Authentication Centre, Sequence Number
USIM	Universal Subscriber Identity Module
IMSI	International Mobile Subscriber Identity
TMSI	Temporary Mobile Subscriber Identity
AV, AUTN	Authentication Vector, Authentication Token
K	Secret Key which share between USIM and AuC
MAC	Messages Authentication Code
AMF	Authentication Management Field
Rand, RES	Random Number, User Response
XRES	Expected User Response
CK, IK, AK	Cipher Key, Integer Key, Authentication Key
$f1 \sim f5$	Authentication and Key Generation Function
UE	User Equipment
IMPI, IMPU	IP Multimedia Private Identity , IP Multimedia Public Identity
P-CSCF	Proxy Call Service Control Function
I-CSCF	Intergating Call Service Control Function
S-CSCF	Service Call Service Control Function
P-CSCF	Proxy Call Service Control Function

Basically UMTS-IMS-AKA and UMTS-AKA are alike and merely run in different environments. IMPI (IP Multimedia Private Identity) corresponds to IMSI (International Mobile Subscriber Identity); IMPU (IP Multimedia PUblic Identity) to TMSI (Temporary Mobile Subscriber Identity); UE (User Equipment) to MS; P-CSCF (Proxy Call Service Control Function) to I-CSCF (Interrogating Call Service Control Function); S-CSCF (Service Call Service Control Function) to SN; and HSS (Home Subscriber Server) to HE - from all these, one can find that UMTS-IMS-AKA and UMTS-AKA are alike with regard to their logic and concepts. Although the method of calculating the parameters of UTMS-AKA and IMS-AKA are identical, their parameters are transported in slightly different ways. Since messages are delivered on IP networks in the UMTS-IMS-AKA protocol, additional parameters must be developed.

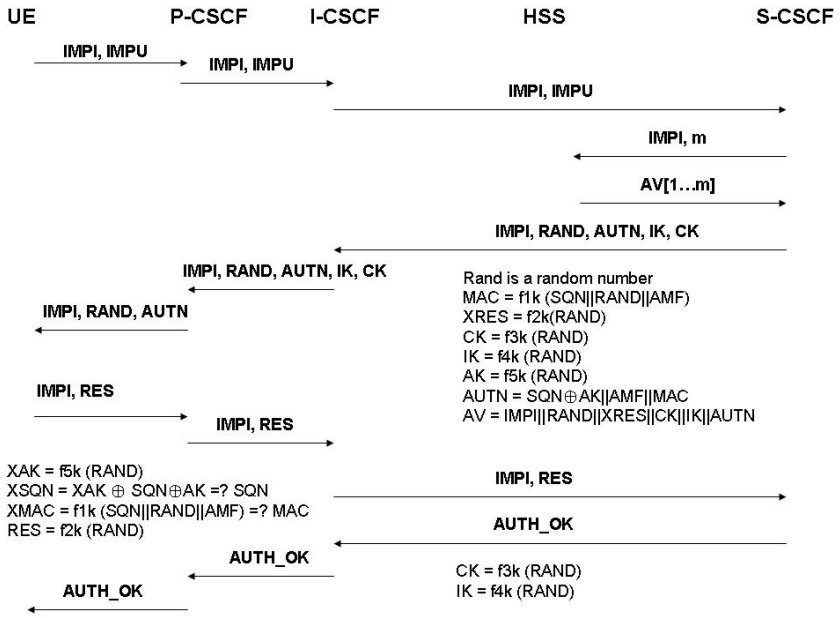

Figure 4: UMTS-IMS-AKA-protocol

2.2 UMTS Multimedia Broadcast/Multicast Service

The Multimedia Broadcast/Multicast Service (MBMS) [10, 11] has been standardized in the 3GPP. It provides a point-to-multipoint service of transmitting multimedia data via the existing UMTS cellular networks. MBMS offers two service modes: broadcast mode and multicast mode. Both of them can share the same data from a single source to multiple recipients. Figure 5 illustrates their architecture [11]. The security architecture of MBMS has been defined elsewhere [12].

BM-SC is a Broadcast/Multicast Service Centre which is a source for MBMS data, or scheduling and receiving MBMS data from third parties. It offers an interface for content providers to deliver the requested data to allocated users. SGSN performs user individual service control functions and provides MBMS data transmissions to UTRAN/GERAN. It also provides support for intra- and inter-mobility procedures and indicates its MBMS support to the UE. Moreover, SGSN maintains a single connection with the source of MBMS data and concentrates all users of the same MBMS service into a single MBMS

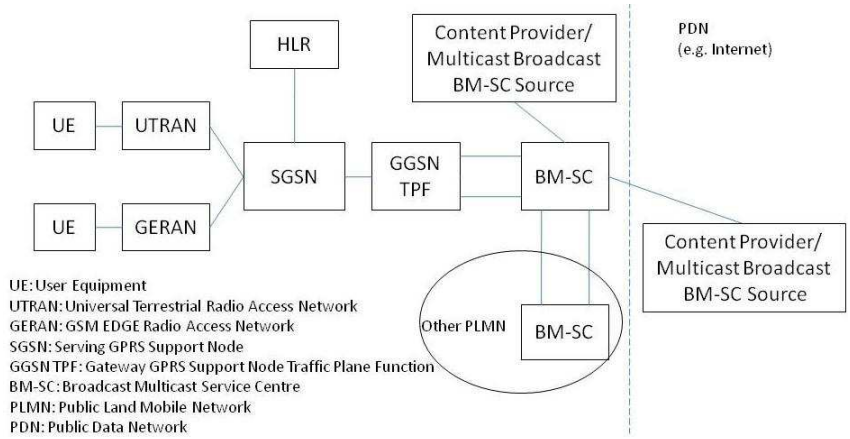

Figure 5: The UMTS MBMS Architecture

service. The role of GGSN within the MBMS architecture is that of a gateway for MBMS data. It links the tunnels from SGSN with MBMS data source via IP multicast.

With respect to the security, BM-SC uses the HTTP digest authentication mechanism [7, 33] to authenticate the UEs, and the Generic Bootstrapping Architecture (GBA) [9] to establish the secret share key with the UEs. HTTP digest authentication mechanism is defined in RFC 2617. UMTS-MBMS is specified in the clause "Procedures using the bootstrapped Security Association" [7]. It is run between BM-SC and ME just as the UMTS-IMS-AKA protocol is executed between SN and MS, and their methods are the same in essence. In order to keep the privacy of MBMS data while conveying, four keys, MRK (MBMS Request Key), MUK (MBMS User Key), MSK (MBMS Service Key), and MTK (MBMS Traffic Key), must be established. MRK is used to authenticate UE to BM-SC when performing key requests; MUK is the MBMS user individual key used by BM-SC to protect MSK transferred to UE; MSK is used to protect the delivery of MTK; and MTK is used to decrypt the received MBMS data on UE.

3 The Proposed Scheme

In mapping the ITS communication characteristics to the existing UMTS environment the following requirements are met:

- A deal of messages delivered and their contents are public and homologous. ITS must deliver many of messages, and the contents of the data are homologous. Some examples are road conditions, multimedia, and navigation information. The primary characteristic of these messages is that they are public and homologous. In order to maintain fairness and privacy, all messages must be encrypted and conveyed. In view of this, UMTS-MBMS provides a point-to-multipoint service for transmitting multimedia data via existing UMTS cellular networks, but it is not fully applicable to the ITS environment. The MBMS is suitable for stable and continuous point-to-multipoint relationship, which includes members and message content. In ITS communication, vehicles are fast-moving on the roads. The original MBMS will meet two kinds of situations. One is the fast movement caused by rapid changes in message routing. The other is the multicasting members of the frequent changes. These particular situations of ITS will cause a heavy load on the MBMS.

- Smaller messages delivered and their contents are private. These messages generally suit a specific purpose, such as paying tolls. Privacy and non-repudiation are necessary characteristics. The current UMTS does a good job in this aspect. Especially IMS, a subsystem of UMTS, provides a complete solution with packet transmission by unicasting. With the support of the IMS, UMTS can provide full service to ITS in this respect.

- Messages are exchanged between two parties as in vehicle-to-vehicle communication. This is accomplished by vehicles detecting each other and communicating directly. Currently, UMTS has no related technique to

support this communication.

Since UMTS is already a popular technique, modifying this protocol substantially can endanger its compatibility. It is not our intention doing so; rather we have merely extended and improved the existing protocol to make the UMTS fully applicable to the ITS. Considering the above needs, this article proposes two expansion protocols to overcome the shortcomings in the original UMTS. One is a group key extension of the UMTS-IMS-AKA protocol. The concept of this protocol is to combine MBMS and IMS into a more streamlined AKA protocol to solve the bottleneck of data transfer. Another is a vehicle-to-vehicle communication system for UMTS. This is to fill the gaps in UMTS in favor of ITS. This protocol shall make possible that vehicles directly exchange messages under the framework of UMTS.

3.1 Group Key Extension of the UMTS-IMS-AKA Protocol

IMS is an extension subsystem of the UMTS to support IP-based multimedia services. It has been designed to support the point-to-point connection with unicasting transmission. Moreover, MBMS facilitates the point-to-multipoint transmission of broadcast and multicast. The earlier release of the 3GPP standard did not provide the integration of IMS and MBMS. Although IMS and MBMS are separate from the system, MBMS must be used with IMS. This will cause duplication of resources wasted. Fortunately, it has been considered and integrated in the latest release. Moreover, some reports [15, 36, 47] provided the integration of IMS and MBMS. The release and the literatures favor the integration of their functionalities and not their security mechanism. However, in the ITS environment, vehicles move so fast that special focus need to be given to the response and performance on communication. For this reason, the proposed protocol attempts to expand on the existing IMS-AKA protocol to enable it to support the group key on MBMS. In addition, considering

the compatibility of the original system, we try to minimize the movement of integration.

First, observe the special situations for MBMS in ITS environment and classify them into two kinds. One is the transmission of multimedia, such as audio, video, or movie. This kind of transmission is very suitable for the original UMTS-MBMS because the source is fixed and the connection is continuing. Another is the transmission of messages, such as traffic information, travel information, traffic control messages, and traffic management messages. This kind of transmission has a feature that the contents of the messages are regional. That is, the contents of the messages change with the location of the vehicle. The original UMTS-MBMS is unable to meet this demand because of the following:

1. The information source is not a fixed point but the distribution is. On the UMTS-MBMS, all the multicast/broadcast messages concentrate on BM-SC and then are forwarded to the recipient. This will result in round-trip transmission that messages provided from the vehicle's location to the BM-SC return to the vehicles in the region.

2. Vehicles quickly move through different service network coverage. On the UMTS-MBMS, the problem of signal transmission can be solved through correcting the routing tables [10]. Two possible options for data path exist for this case. Option 1 is via the original SRNC (Serving Radio Network Controller). Option 2 is via a new DRNC (Drift Radio Network Controller). The original SRNC is a dedicated point to forward the signal to the vehicles in the new location. It has the advantage of easy operation, but it increases communication delay. Via a new DRNC, BM-SC will define a new multicast signaling channel for vehicles to receive data directly. This can reduce some signaling complexity but increases the difficulty in operation. Both of them will increase communication

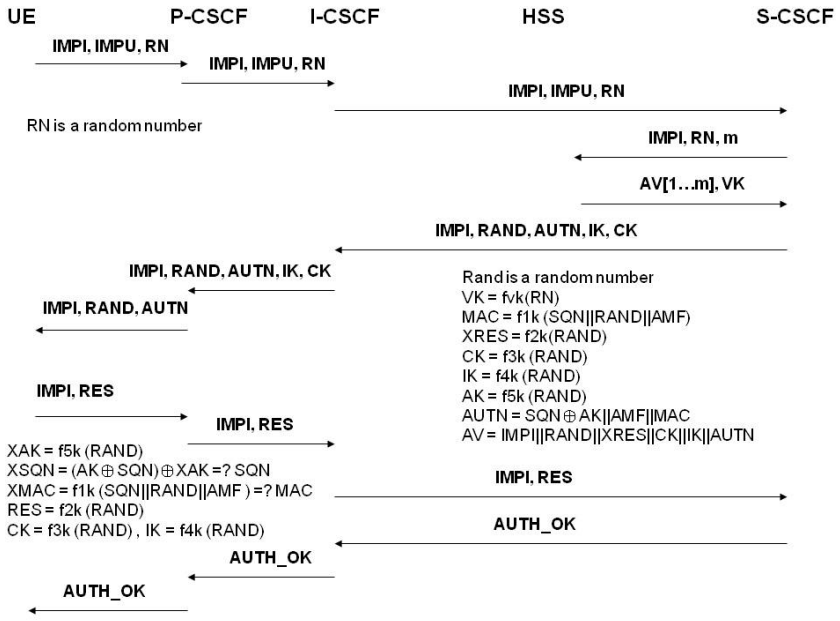

Figure 6: The proposed IMS-AKA-protocol

delay and difficulties in delivery.

For the above reasons, this article proposes to combine a group key with the UMTS-IMS protocol to making it compatible with ITS. The proposal, however, does not affect compatibility with the original protocol since it only increases some parameters with the original behind. Figure 6 outlines our proposal.

Our protocol is very similar to the original IMS-AKA protocol; an obvious characteristic is that our proposal joins a vehicle key, VK, and a random number, SN. VK is an exclusive key allocated to each vehicle that enters the P-CSCF service range; it is used to protect the delivery of GK, and GK is a group key used to decrypt the received data on the vehicle. SN is a random number selected by the vehicle; it is used to generate VK. Their relationship is

$$VK = fv_k(SN). \tag{1}$$

Here fv s a key-generating function, like the $f*$ on the UMTS. It may replace

$f3$ or $f4$ on the UMTS. The details of our proposal are as follows:

1. The vehicle (as UE) sends its IMPI, IMPU, and a random number, SN, to the P-CSCF. IMPI/IMPU is used in the same manner as IMSI/TMSI - to identify vehicles. A vehicle can only have only one IMPI but can be assigned many IMPU so as to hide its movements. After that the vehicle calculates $VK = fv_k(SN)$ and stores the results for future use to decrypt the encrypted GK.

2. P-CSCF sends messages via I-CSCF to the S-CSCF. When S-CSCF receives the messages, it first checks in a database to see if it has unused authentication vectors with the vehicle. If yes, it jumps to Step 6; otherwise, S-CSCF sends the IMPI, m, and SN to the vehicle's HSS requesting m sets of authentication vectors.

3. After HSS has received the request from S-CSCF, HSS uses the secure key K which is shared between the vehicle's ISIM (IP Multimedia Services Identity Module) and the HSS to compute the following (f* is the key-generating function [4, 5, 6]):

    - Randomly select a RAND.
    - Cipher key, $CK = f3_K(RAND)$.
    - Integrity key, $IK = f4_K(RAND)$.
    - Anonymity key, $AK = f5_K(RAND)$.
    - Expected response, $XRES = f2_K(RAND)$.
    - Message authentication code, $MAC = f1_K(SQN||RAND||AMF)$, where SQN is a sequence number that maintains consistency between vehicle's ISIM and its HSS; AMF (authentication and key management files) is used to indicate the algorithm and key used to generate a particular authentication vector.

- Authentication token, $AUTN = SQN \bigoplus AK||AMF||MAC$.
- Authentication vector, $AV = IMPI||RAND||XRES||CK||IK||AUTN$.
- Repeat the above step until m sets of AVs are produced.
- Vehicle key, $VK = fv_k(SN)$.

4. HSS delivers m sets of AVs and VK to S-CSCF once the computation is complete.

5. S-CSCF receives the authentication vector and makes use of it in follow-up connection.

6. The step after here is the same as in the UMTS-IMS-AKA protocol. S-CSCF retrieves a tuple of unused authentication vectors from the AV, and sends $(IMPI, RAND, AUTN, CK, IK)$ via I-CSCF to P-CSCF. After that P-CSCF sends $(IMPI, RAND, AUTN)$ as the challenge to the vehicle.

7. Upon receiving $(IMPI, RAND, AUTN)$, the vehicle computes the following:
   - Cipher key, $XCK = f3_K(RAND)$.
   - Integrity key, $XIK = f4_K(RAND)$.
   - Anonymity key, $XAK = f5_K(RAND)$.
   - Response, $RES = f2_K(RAND)$.
   - Verify the vehicle's sequence number, $SQN' \stackrel{?}{=} (SQN \bigoplus AK) \bigoplus XAK$.
   - Calculate $XMAC = f1K(SQN'||RAND||AMF)$.
   - Verify $XMAC \stackrel{?}{=} MAC$.

8. If the identification is correct, the vehicle delivers $(IMPI, RES)$ to P-CSCF, and P-CSCF sends it via I-CSCF to the S-CSCF.

9. S-CSCF compares RES and $XRES$ in AV to make sure the vehicle is a legal user.

10. If the identification is correct, the S-CSCF delivers a message $AUTH_{OK}$ via I-CSCF to P-CSCF and the vehicle. After that P-CSCF can initiate communication with the vehicle by the CK and IK.

11. When S-CSCF sends a group of messages (as multicasting/broadcasting) to the vehicle, it encrypts the group key, GK, with that of the vehicle's, VK, and then sends to the vehicle via the I-CSCF and P-CSCF. After receiving the encrypted GK, the vehicle decrypts with the VK, and gets the GK to decrypt the encrypted group messages.

Upon completing the above steps, the vehicle and the CSCF can initiate communication in two ways. Private data is encrypted by the original IK and CK, and the group data is encrypted by the GK. This scheme governs the private communication provided by the original UMTS-AKA protocol, as well as provides the group communication scheme. Moreover, it can be applied to environments that use wide-area wireless and vehicle-to-roadside communications.

3.2 Vehicle-to-Vehicle Communication Systems for UMTS

To provide a more complete scheme for ITS, we devised a new AKA protocol to be applied to the vehicle-to-vehicle communication systems. Figure 7 illustrates this protocol.

When neighboring vehicles want to communicate, they must obtain the IMPU of the other party first, as in Stage 1. IMPU resembles alias that can temporarily identify the user and can hide his true identity to achieve anonymity. In this stage, vehicles obtain the IMPU of the other party by other techniques such as sensor networks or wireless networks. UMTS also provides location techniques [8] that are helpful in this case. In Stage 2, the two parties

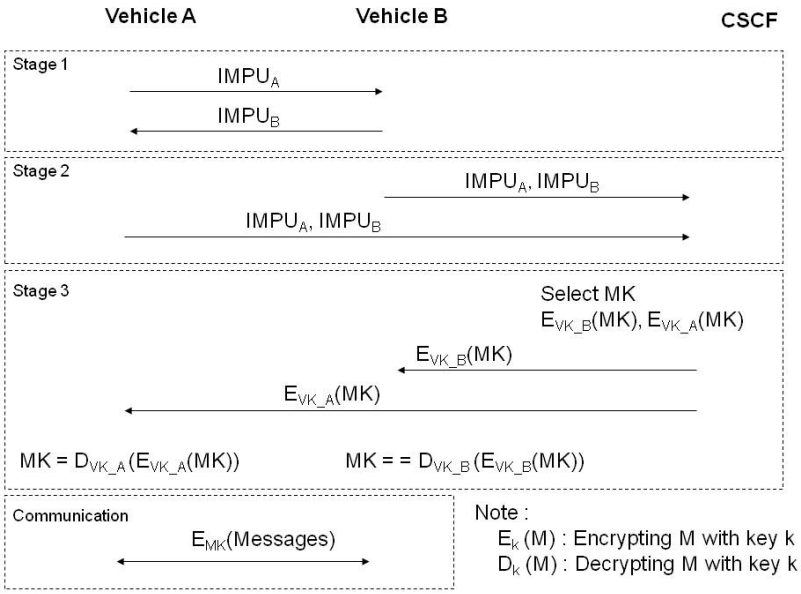

Figure 7: The proposed V2V-AKA-protocol

exchange IMPU and convert them to CSCF. Since the vehicles always stay within the service range of the CSCF, they will pass through Phase 1 of our IMS-AKA protocol. CSCF has already confirmed both parties' IMPI, and selected a meeting key, MK, which encrypts the messages exchanged between both parties. Then, take both parties' VK to encrypt the MK and send back during Stage 3. The purpose of encrypted MK with the respective VK is to hide the MK of both parties; so they cannot be obtained by outside parties while allowing both authorized parties to decrypt the encrypted MK with his VK.

We have proposed two AKA protocols that allow UMTS to configure the ITS environment. One applies to wide-area and vehicle-to-roadside communication systems. The other applies to vehicle-to-vehicle communications. In other words, our proposal helps apply the UMTS to ITS environments.

4 Discussion and Analysis

ITS has a wide range of applications, but not all of them are currently practical. Many applications are still at the conceptual stage. Much research has focused on Ad-hoc networks concerning ITS communication. But the Ad-hoc network had some problems still to remain unresolved. UMTS is a universal and reliable technology but does not fully applicable to the ITS. Because such that the article attaches importance to the realization of these applications. We have introduced some useful characteristics to be applied to ITS in the field of telecommunications, and we utilized the existing UMTS techniques to support them. However, we proposed two practical protocols to service the needs of ITS.

In this section, we will analyze and discuss the benefits of our proposal. We will first simply reiterate the basic characteristics of ITS communication, and then explain why our proposal is suitable in ITS environments. In conclusion, security is taken as a point to discuss briefly.

4.1 Property

According to the recipient of the message, ITS wireless communication can be classified into two types.

1. Vehicle-to-roadside communication: It indicates that the vehicle and ITS deliver data by means of wireless infrastructure. Generally it is the ITS that delivers relevant data to the vehicle. Those data may regard road conditions, video, or audio.

2. Vehicle-to-vehicle communication: It indicates that the relevant data is delivered between vehicles. In this mode, one can view the vehicle as the router. It resembles the Ad hoc network as it can automatically search and link the neighboring vehicles to form a topology. Moreover, neighboring vehicles also can link themselves together to exchange messages.

ITS wireless communication can also be classified according to the data contents.

1. Common messages: This type of message is usually when many vehicles transmit the same message, such as traffic reports or multimedia. Some common messages must be kept private from non-authorized users; only a legal user may receive them. This is due to the fact that legal users must pay for the contents of the data, and non-authorized users may want to steal it. According to the data provider, data can be classified into two types.

   (a) Content provider is the centralization. Their data source is fixed and the connection is continuing, such as audio, video, or movie.

   (b) Content providers are the localization. Their data source is not fixed but will follow the vehicle location to change, such as traffic information, travel information, traffic control messages, or traffic management messages.

2. Private messages: These must always be kept confidential.

These characteristics help us understand the suitability of our scheme.

4.2 Realization

Currently, developments in wireless communication on ITS concern an exclusive network called VANET. VANET was constituted by an Ad-hoc network which automatically links the neighboring vehicles to form a topology. However, Ad-hoc is an exclusive network technique under development. The biggest problem is that it is not stable. Its topology is constituted by mobile nodes (vehicle) that may change at any time. An inherent drawback is that vehicles that are too close or too far cannot communicate. To solve this defect, fixed access points have been used to strengthen the signal, since the

outdoor wireless network's coverage is still not comprehensive. However, it will be quite expensive to build the necessary infrastructure to solve this problem. These problems are completely avoided with UMTS. More importantly, its infrastructure is nearly complete, thus avoiding the problems of lack of signal coverage.

Seamlessly UMTS is the best platform to use with ITS. It can support vehicle-to-roadside as well as vehicle-to-vehicle communications when our modifications are used. The original UMTS was supported by IMS and MBMS to transfer private and common messages. However, when applied to the environment of ITS, it will have some additional considerations, especially the fast movement caused by rapid changes in message routing and multicasting members of the frequent changes. Both of them will cause a heavy load on the MBMS. For this, our protocol introduces the concept of group keys. Moreover, in the UMTS, IMS and MBMS are two separate systems, and the MBMS must be used with the IMS. This has caused wastage of resources and authentication delays. For this, our protocol integrates them into a single protocol. However, to solve the bottlenecks, our protocol is an expansion of the existing IMS-AKA protocol using support group key. This not only combines IMS and MBMS but also solves the problems of MBMS in the ITS.

Two protocols are proposed in this paper. One is an improvement over the IMS-AKA protocol; another is a novel V2V-AKA protocol. The improvement over the IMS-AKA protocol was achieved by integrating a vehicle key on the UMTS-IMS-AKA protocol. The V2V-AKA protocol is an innovative design. It makes direct communication between vehicles possible on the UMTS. The suitable collocation of our IMS-AKA protocol with our V2V-AKA protocol can get all-round development on ITS. Generally messages delivered by our IMS-AKA protocol and interaction with vehicles are shared with our V2V-AKA protocol. Some of the applications can be accomplished with slight

revision. For example, ETC (Electronic Toll Collection) system can to regard our protocol as their charging solution. In this scenario, P-CSCF corresponds to the tollbooth. When a vehicle passes through the tollbooth, the tollbooth sends the authentication request to the vehicle. Our IMS-AKA protocol can be adopted in this scenario. With our protocol, authentication and authorization are assured, and the billing program can also be solved.

4.3 Security Analysis

Our proposal has the structure of the original IMS-AKA protocol and inherits its security features. All the fundamental conditions of security [3] on the IMS-AKA protocol are also attained in our protocol, including anonymity and untraceability. Moreover, our protocol can achieve three objectives (confidentiality, integrity, and availability) [19] of ITS to resist four general threats (deception, disruption, usurpation, and unauthorized disclosure) [19]. Only authorized vehicles can have the secure key K and pass the authentication and get the relational key CK, IK, and VK. All unauthorized vehicles intercept unreadable secret content. Moreover, as in the IMS-AKA protocol, our protocol has the enhanced feature of mutual authentication.

On vehicle-to-roadside communication, in order to retain compatibility with the original IMS-AKA protocol, we have fine-tuned the original protocol. The main change is that we have joined a vehicle key, VK. VK is generated by RN and K; SN is a random number selected by the vehicle; and K is a secret key shared between the vehicle and HSS. By the way, the vehicle has participated in the decision of VK because SN is offered by him. The advantage is that a vehicle can very easily identify fresh VK, and prevent a malicious attacker from stealing VK and reusing it. The group key, GK, used for encrypting the group messages is encrypted by VK and delivered to the corresponding vehicle. Therefore, GK will not leak it in the process of transaction, and group messages can also maintain secrecy.

On the vehicle-to-vehicle communication, our protocol combines UMTS and Ad-hoc. Both the technologies rely on the UMTS authentication mechanism that verifies the identity of vehicles and uses the Ad-hoc network architecture to communicate between the vehicles. It has the advantage of UMTS's security and Ad-hoc network's convenience. Moreover, vehicles know each other, and only the IMPU can ensure the anonymity of the two sides. Use VK to encrypt the meeting key, MK, and the transaction can guarantee that MK will not leak during the transmission.

Keeping with these discussions, a conclusion can be derived that our proposed is based on the original IMS-AKA protocol and continues to develop. In our expanding function, the random number, SN, and the secret key, k, making the vehicle key, VK, has privacy and security. Since the VK is secure, GK and MK protected by VK are also secure; therefore, our protocol is secure.

5 Conclusions

In this article, we have proposed a function for ITS wireless communication mechanisms. Much research has focused on Ad-hoc networks concerning ITS communication. This article provides a new idea on how to use UMTS to replace exclusive Ad hoc networks. To make UMTS more suitable for ITS, we slightly modified the UMTS-AKA protocol without reducing its effectiveness, and our results were excellent.

We will continue researching this subject in the future. We believe this new direction can promote significant ITS implementation.

References

[1] 3GPP, "3rd generation partnership project, technical specification group services and systems aspects, 3G security, access security for IP-based services," *3GPP TS 33.203*.

[2] 3GPP, "3rd generation partnership project, technical specification group services and systems aspects, 3G security, security architecture," *3GPP TS 33.102*.

[3] 3GPP, "3rd generation partnership project, technical specification group services and systems aspects, 3G security, security thraets and requirements," *3GPP TS 21.133*.

[4] 3GPP, "3rd generation partnership project, technical specification group services and systems aspects, 3G security, specification of the MILENAGE algorithm set, document 1: General," *3GPP TS 35.205*.

[5] 3GPP, "3rd generation partnership project, technical specification group services and systems aspects, 3G security, specification of the MILENAGE algorithm set, document 2: Algorithm specification," *3GPP TS 35.206*.

[6] 3GPP, "3rd generation partnership project, technical specification group services and systems aspects, 3G security, specification of the MILENAGE algorithm set, document 5: Summary and results of design and evaluation," *3GPP TS 35.909*.

[7] 3GPP, "3rd generation partnership project, technical specification group services and systems aspects, bootstrapping interface (ub) and network application function interface (ua), protocol details (release 7)," *3GPP TS 24.109*.

[8] 3GPP, "3rd generation partnership project, technical specification group services and systems aspects, functional stage 2 description of location services in UMTS," *3GPP TS 23.171*.

[9] 3GPP, "3rd generation partnership project, technical specification group services and systems aspects, generic authentication architecture (GAA), generic bootstrapping architecture (release 7)," *3GPP TS 33.220*.

[10] 3GPP, "3rd generation partnership project, technical specification group services and systems aspects, multimedia broadcast/multicast service (MBMS), architecture and functional description (release 6)," *3GPP TS 23.846*.

[11] 3GPP, "3rd generation partnership project, technical specification group services and systems aspects, multimedia broadcast/multicast service (MBMS), architecture and functional description (release 7)," *3GPP TS 23.246*.

[12] 3GPP, "3rd generation partnership project, technical specification group services and systems aspects, security of multimedia broadcast/multicast service (MBMS)," *3GPP TS 33.246*.

[13] Ahmed Abdel-Hafez, Ali Miri1, and Luis Orozco-Barbosa, "Authenticated group key agreement protocols for ad hoc wireless networks," *International Journal of Network Security*, vol. 4, pp. 90–98, Jan. 2007.

[14] C.J. Adler, S. Eichler, T. Kosch, C. Schroth, , and M. Strassberger, "The scalability problem of vehicular ad hoc networks and how to solve it," *IEEE Wireless Communications*, vol. 13, pp. 22–28, October 2006.

[15] Adel Al-Hezmi, Michael Knappmeyer, Bjorn Ricks, Filipe Cabral Pinto, and Ralf Tonjes, "Enabling ims with multicast and broadcast capabilities," in *IEEE 18th International Symposium on Personal, Indoor and Mobile Radio Communications(PIMRC 2007)*, pp. 1–5, Sept. 2007.

[16] A. Alrabady, M. Gruteser, B. Hoh, and H. Xiong, "Enhancing security and privacy in traffic-monitoring systems," *IEEE Pervasive Computing*, vol. 5, pp. 38 – 46, Oct.-Dec 2006.

[17] Architecture Development Team, "ITS executive summary," *Research and Innovation Technology Administration (RITA), US Department of Transportation*, January 2005.

[18] Architecture Development Team, "ITS user services document," *Federal Highway Administration, US Department of Transportation*, May 2007.

[19] Architecture Development Team, "National ITS architecture - security," *Research and Innovation Technology Administration (RITA), US Department of Transportation*, May 2007.

[20] M.M. Artimy, W.J. Phillips, and W. Robertson, "Connectivity with static transmission range in vehicular ad hoc networks," in *3rd Annual Communication Networks and Services Research Conference*, pp. 237–242, Maye 2005.

[21] A. Benslimane, "Localization in vehicular ad hoc networks," in *Systems Communications 2005*, pp. 19 – 25, Aug. 2005.

[22] J.-J. Blum, A. Eskandarian, and L.-J. Hoffman, "Challenges of intervehicle Ad Hoc networks," *IEEE Transactions on Intelligent Transportation Systems*, vol. 5, pp. 347–351, December 2004.

[23] Mohamed-Salah Bouassida, Isabelle Chrisment, and Olivier Festor, "Group key management in manets," *International Journal of Network Security*, vol. 6, pp. 67–79, Jan. 2008.

[24] Mohamed Salah Bouassida, Gilles Guette, Mohamed Shawky, and Bertrand Ducourthial, "Sybil nodes detection based on received signal strength variations within vanet," *International Journal of Network Security*, vol. 9, pp. 22–33, July 2009.

[25] Ching-Wen Chen, Ming-Chin Chuang, and Chwei-Shyong Tsai, "An efficient authentication scheme between manet and wlan based on mobile

ipv6," *International Journal of Network Security*, vol. 1, pp. 14–23, July 2005.

[26] F. Dotzer, F. Kohlmayer, T. Kosch, and M. Strassberger, "Secure communication for intersection assistance," in *2nd International Workshop on Intelligent Transportation*, Hamburg, Germany, 2005.

[27] F. Dotzer, F. Kohlmayer, T. Kosch, and M. Strassberger, "VARS: A vehicle Ad-Hoc network reputation system," in *Sixth IEEE International Symposium on a World of Wireless Mobile and Multimedia Networks*, 2005.

[28] M. Gerlach, "VaneSe-an approach to VANET security," in *V2VCOM 2005*, 2005.

[29] M. Gerlach, "Assessing and improving privacy in VANETs," in *Fourth Workshop on Embedded Security in Cars (ESCAR)*, November 2006.

[30] M. Gerlach, A. Festag, T. Leinmuller, G. Goldacker, and C. Harsch, "Security architecture for vehicular communication," in *5th International Workshop on Intelligent Transportation (WIT)*, Hamburg, Germany, March 2007.

[31] J.P. Hubaux, S. Capkun, and Jun Luo, "The security and privacy of smart vehicles," *IEEE Security and Privacy Magazine*, vol. 02, pp. 49–55, May-June 2004.

[32] IEEE P1609.3/D18, "Committee SCC32 of the IEEE intelligent transportation systems council. draft standard for wireless access in vehicular environments (WAVE) - networking services," December 2005.

[33] IETF RFC 2617, "HTTP digest authentication,".

[34] D. Jungels, "Certificate revocation in vehicular ad hoc networks," *Technical report of LCA*, 2006.

[35] Ramanarayana Kandikattu and Lillykutty Jacob, "Comparative analysis of different cryptosystems for hierarchical mobile ipv6-based wireless mesh network," *International Journal of Network Security*, vol. 10, pp. 139–152, 2010.

[36] M. Knappmeyer, B. Ricks, R. Tonjes, and A. Al-Hezmi, "Advanced multicast and broadcast content distribution in mobile cellular networks," in *IEEE Global Telecommunications Conference(GLOBECOM '07)*, pp. 2097 – 2101, Nov. 2007.

[37] Chun-Ta Li and Yen-Ping Chu, "Cryptanalysis of threshold password authentication against guessing attacks in ad hoc networks," *International Journal of Network Security*, vol. 8, pp. 166–168, 2009.

[38] Hongwei Li and Atam P. Dhawan, "Mosar: A secured on-demand routing protocol for mobile multilevel ad hoc networks," *International Journal of Network Security*, vol. 10, pp. 125–138, 2010.

[39] Lockheed Martin Federal Systems, Odetics Intelligent Transportation Systems Division, "ITS communictions document," *Federal Highway Administration, US Department of Transportation*, January 1997.

[40] US Department of Transportation *http://www.its.dot.gov*.

[41] B. Ostermaier, F. Dotzer, and M. Strassberger, "Enhancing the security of local dangerwarnings in VANETs - a simulative analysis of voting schemes," in *Second International Conference on Availability Reliability and Security (ARES 2007)*, pp. 422 – 431, April 2007.

[42] A. Patcha and J.-M. Park, "A game theoretic formulation for intrusion detection in mobile ad hoc networks," *International Journal of Network Security*, vol. 2, pp. 131–137, Mar. 2006.

[43] M. Raya and J.P. Hubaux, "Security aspects of inter-vehicle communications," in *5th Swiss Transport Research Conference (STRC)*, Ascona, Switzerland, March 2005.

[44] M. Raya and J.P. Hubaux, "The security of vehicular ad hoc networks," in *3rd ACM workshop on Security of ad hoc and sensor networks*, Alexandria, VA, USA, 2005.

[45] IEEE Draft Amendment to Standard for Information Technology, "Telecommunications and information exchange between systems - LAN/MAN specific requirements - part 11: Wireless lan mecium access control (MAC) and physical layer (PHY) specifications: Amendment 3: Wireless access in vehiclular environments (WAVE)," January 2006.

[46] Chang-Kuo Yeh and Wei-Bin Lee, "An overall cost-effective authentication technique for the global mobility network," *International Journal of Network Security*, vol. 9, pp. 227–232, 2009.

[47] M. Zafar, N. Baker, M. Fuchs, J. Santos, A. Ikram, and S. Sargento, "Ims - mbms integration: Functional analysis & architectural design," in *16th IST Mobile and Wireless Communications Summit*, pp. 1–5, July 2007.