Traceable and Private Satellite Communication for Emergency Notification in VANET

Chin-Ling Chen[1,2,3], Jin-Xin Hu[4], Chun-Ta Li[5], Yong-Yuan Deng[3], Shunzhi Zhu[1]

[1] School of Computer and Information Engineering, Xiamen University of Technology, China
[2] School of Information Engineering, Changchun Sci-Tech University, China
[3] Department of Computer Science and Information Engineering, Chaoyang University of Technology, Taiwan
[4] School of Computer Science, Shenyang Aerospace University, China
[5] Department of Information Management, Tainan University of Technology, Taiwan
clc@mail.cyut.edu.tw, 573217648@qq.com, th0040@mail.tut.edu.tw, allen.nubi@gmail.com, szzhu@xmut.edu.cn

Abstract

With the rapid development of the Internet of Things (IoT) technology in recent years, and its increasing success in the automotive sector, many research efforts have focused on the issues in Vehicular Ad Hoc Networks (VANETs). Simultaneously, satellite technology is used for reliable emergency notification so that it can cope with significant accidents or disasters which potentially make traditional roadside radio communication infrastructure unavailable. However, these transmitted emergency messages are also vulnerable to unauthorized access, affect the privacy and security of people.

Privacy and confidence of messages exchanged between mobile users are often regarded as two mutually conflicting issues. By using the cryptography, the proposed scheme can defend against known attacks and also solve some security issues such as mutual authentication, confidential communication, non-repudiation, user's privacy, unforgeability etc. The system can also track malicious behaviors and prevent a legal registered mobile user from stealing the network control center's private key to make sure no insider attack possibility. Our schme provides a good application in emergency notification of VANET.

Keywords: Vehicular ad hoc networks, Satellite communication, Security, Privacy

1 Introduction

In recent years information technology has developed very rapidly and the usage rate of the Internet has become extremely widespread. In this scenario, satellite-based communication systems can reveal to be extremely convenient, by allowing vehicles to communicate among each other'sand with vehicle control stations at anytime and in anyplace, regardless the presence of ground-based wireless network coverage, such as cellular, WiMAX or Wi-Fi-based mobile communication systems. The role of satellite systems has been always complementary to ground-based fixed or mobile wireless connectivity. For instance, early satellite communication networks targeted maritime communities, which were not served by any ground-based network for geographical as well as technical reasons. With the evolving need of ubiquitous personal communications, satellites have served as gap fillers, by covering the remote areas not serviced by either landline or cellular networks [1]. Satellite communicationsalso involve on-earth radio stations using satellites as relays and communication facilities for dealing with huge communication distances, and covering extremely wide areas, without ground conditioning and topological constraints.The communication cost is independent of the station distance, as well as the service model is quite flexible, and can offer multiple simultaneous access channels providing greater communication capacity together with immunity from weather factors. Signals emitted from the satellite to the surface, can simultaneously be received by all the in–range antennas. Thus, while traditional terrestrial cable transmission cannot easily match multicast-oriented paradigms, the inherent broadcast nature makes it the best solution for simultaneously distributing the same information to a huge number of end users. This may be of particular interest in emergency notification where many vehicles have to be timely informed about potential dangers also when ground-based coverage infrastructures may be temporarily unavailable. Satellite communication systems are widely used in many areas around the world, and they assume an important strategic value especially in military applications and in all the mission-critical scenarios where connectivity is essential and terrestrial alternatives are unavailable, unreliable or simply too expensive. Moreover, satellite communication has proven to be priceless during

[*] Corresponding Author: Yong-Yuan Deng; E-mail: allen.nubi@gmail.com

DOI: 10.3966/160792642020012101019

specific emergencies or disasters, when and where all other forms of communication fail due to damaged infrastructures [1]. Since communication systems based on Earth's Equatorial Geosynchronous Orbit (GEO) satellites are affected by a significant latency, due to their distance from earth (approximately 35400 Kms), the use of Low Earth Orbit (LEO) Satellite systems is becoming more and more popular mainly when interactive and timely communications in a universal coverage scenario are necessary.

There are two kinds of communication scenarios in VANETs: namely Vehicle to Vehicle (V2V) and Vehicle to Roadside (V2R). Vehicle to vehicle communication usually takes place by using wireless ad-hoc technologies ensuring the short-range propagation of information between near vehicles by using several kind of broadcasting mechanisms. However, their infrastructureless nature and limited coverage range make such communication technique of very limited utility for notifying critical information in advance to vehicles that are several kilometers far from the notifier of for reliably requesting emergency rescue. In Vehicle to Roadside communications, the vehicle/user can access the Internet or other available resources/services by relying on the radio coverage provided by multiple RoadSide Units (RSUs) distributed along the road. V2R communications have been essentially conceived for safety VANET applications, such as road accident notifications and weather warnings, but they have been recently exploited also for providing commodity services to vehicles such as infotainment and Internet access [2-3]. However, in presence of road accidents characterized by a particular severity or natural disasters, such as earthquakes, the roadside infrastructure may become unavailable so that alternate and always-available communication links such as satellite ones can assume a paramount importance for emergency notification and, in general for providing safety-related services. Therefore, securing all the communications and controlling access to services in VANETs has become one of the most important issues. The whole communication system needs to ensure, in addition to reliable authentication, and message confidentiality and integrity, that the pivotal information will not be faked or tampered with by malicious attackers. Mutual authentication and key exchange mechanism between the involved parties are the major preventive methods. Unfortunately, password-based authentication is still the most common method for checking users' identities and grant them access to VANET services. However, in traditional password-based authentication mechanisms [4-20], the validation table with identity codes and password hashes is usually stored by each service provider, so that, if validation table is stolen, disclosed or tampered with, the whole communication system will be compromised. A more robust scheme relying on state-of-the-art cryptographic techniques and hybrid (terrestrial radio/satellite links) is proposed in this work for managing federated authentication for services' access within the VANET and provide improved reliability to communications in emergency notification. Asymmetric Key and symmetric encryption techniques, as well as one-way hash functions have been used to achieve the best results in each phase/activity. The proposed scheme can also ensure the anonymity of honest notifiers together with the identification of malicious ones and protect the involved parties against some known attacks

The remaining sections are as follows: Section 2 analyzes the related works. Section 3 introduces the architecture of the proposed scheme and details the most significant operations. In Section 4, we analyze the security of our scheme and compare our scheme with others. To reveal our scheme's computation and communication costs in Section 5. In Section 6, we offer a conclusion and discuss the direction of further work.

2 Related Works

In recent years, many researchers have proposed a lot of satellite communication systems, as early as 1996, Cruickshank [4] presented a satellite communication system based on public key cryptography (PKC). Cruickshank's scheme failed to support mobile devices because of the high computation cost. In 2003, Hwang et al. [5] proposed a satellite communication system based on symmetric key cryptography (SKC) to solve Cruickshank's problem. However, it still entails high communication cost. Therefore, to reduce both computation and communication cost, Chen et al. [6] presented a self-authentication mechanism for a satellite communication system in 2009, with a lightweight protocol and a session key mechanism to reduce the computation and communication costs. But Chen et al.'s protocol failed to protect the security of users' information, so attackers can easily attack the satellite communications system or steal users' sensitive information. In 2014, Chen et al. [7] and Tsai et al. [8] proposed a novel secure authentication scheme without verification table for satellite communication systems that is based on elliptic curve cryptosystems (ECCs) which can achieve user anonymity in 2015. But it hasn't mentioned identity theft attack. Zhou et al.'s [9] presented a secure authentication method which can validate the new vehicle node to improve the security of the VANET in the same year. But they did not base on mobile users.

Although many researchers [21-23] have discussed the security of the VANET, none has mentioned combining security-related applications and non-security-related applications. When there is an accident, the driver needs to immediately send an emergency notification to the rear vehicles, in case of further collisions. But the notification may expose the driver's privacy; if the communication system can be totally anonymous, it may cause the rear vehicle drivers to question the accuracy of the notification. So, it is very difficult to achieve privacy and anonymity at the same time in the communication system. Besides, even the latest research articles, there are still not considering the satellite connection [24-26]. When an emergency occurs, related information must be reported back to the backend server by the vehicle as soon as possible. Relevant personnel will provide processing and assistance upon receiving the notice.If there is no RSU available for connection, these emergencies will not be passed to the backend server.Therefore, the satellite connection will ensure that when no RSU is available, the emergency information can still be passed to the backend server.

3 The Proposed Scheme

3.1 System Architecture

There are six parties in our scheme. The following descriptions will explain each service feature.

(1) A Mobile user (MU) can use mobile devices to communicate with other users or VANET service providers via RSU-provided services or through a LEO satellite communication system.Each user is associated with a vehicle provided with one or more on-board communication units (OBUs) enabling secure communications within the VANET.

(2) The VANET Network Control Center (NCC), managing emergency notification services, can verify the identity of a VANET user and its legitimacy through the AAAHS and hence has to previously register with it to allow further interactions.

(3) A Low Earth Orbit Satellite (LEO) system can transfer communication messages between mobile users and network control center in case of emergency notification and when no RSUs are available.

(4) A Service Provider (SP): The Service Provider provides mobile users various VANET-related services also NCC is regarded as a special SP, providing emergency notification services.

(5) AAA Home Server (AAAHS): The AAA Home Server can verify the user's identity and issue authorization certificates for legitimate users.

(6) AAA Foreign Server (AAAFS): When foreign mobile users roam into the VANET, the authentication, authorization and accounting foreign server verifies their identities, and communicates with the AAAHS in the local network.

The system architecture is described in Figure 1.

Step 1. Mobile user←→ AAAHS. The mobile user sends registration request messages to AAAHS via secure channel, after computing and then storing the user's details in the database, AAAHS sends back the successful registration message to the mobile user through a secure channel.

Step 2. SP ←→ AAAHS. Service provider sends its registration request messages to AAAHS. Then, the AAAHS issues a private key to the service provider via secure channel.

Step 3. Mobile user→RSU→AAAHS. The mobile user sends the authentication request message via RSU to the AAAHS that processes authentication.

Step 4. AAAHS→RSU→ Mobile user. After receiving the authentication request message, AAAHS verifies the validity of the mobile user and sends via RSU the authorization certificate to the mobile user.

Step 5. Mobile user→RSU→SP. When the mobile user requests a specific service, he/she sends a specific request messages (containing its previous authentication grant) together with his authorization certificate to the service provider.

Step 6. SP→ AAAHS. After receiving the request messages, the service provider sends a mobile user's authentication message to the AAAHS.

Step 7. AAAHS→ SP. After verifying the service provider's validity, AAAHS sends mobile user's information to the service provider.

Step 8. SP→RSU→ Mobile user. After the authentication process, the service provider provides service to the mobile user through RSU (or satellite if NCC). A specific session key is exchanged to allow encryption of service-related information

Step 9. Mobile user→RSU→AAAFS. If the mobile user wants to extend the validity of an authorization certificate, he/she puts forward the request message to the AAAFS.

Step 10. AAAFS←→ AAAHS. Once the mobile user passes the certification process, AAAFS sends mobile user's information to the AAAHS. AAAHS issues a new certificate and sends it back to the AAAFS.

Step 11. AAAFS→RSU→Mobile user. AAAFS forwards the authorization certificate to the mobile user via RSU.

Step 12. Mobile user → LEO → NCC. In emergency case, mobile users send location request message to the NCC via LEO.

Step 13. NCC → LEO → Mobile user. After receiving the request message, NCC authorizes the validity of the mobile user and sends location information to the mobile user via LEO.

Step 14. Mobile user → LEO → NCC. The mobile user is now able to send emergency notification details to the NCC.

The following notations will be used in our scheme.

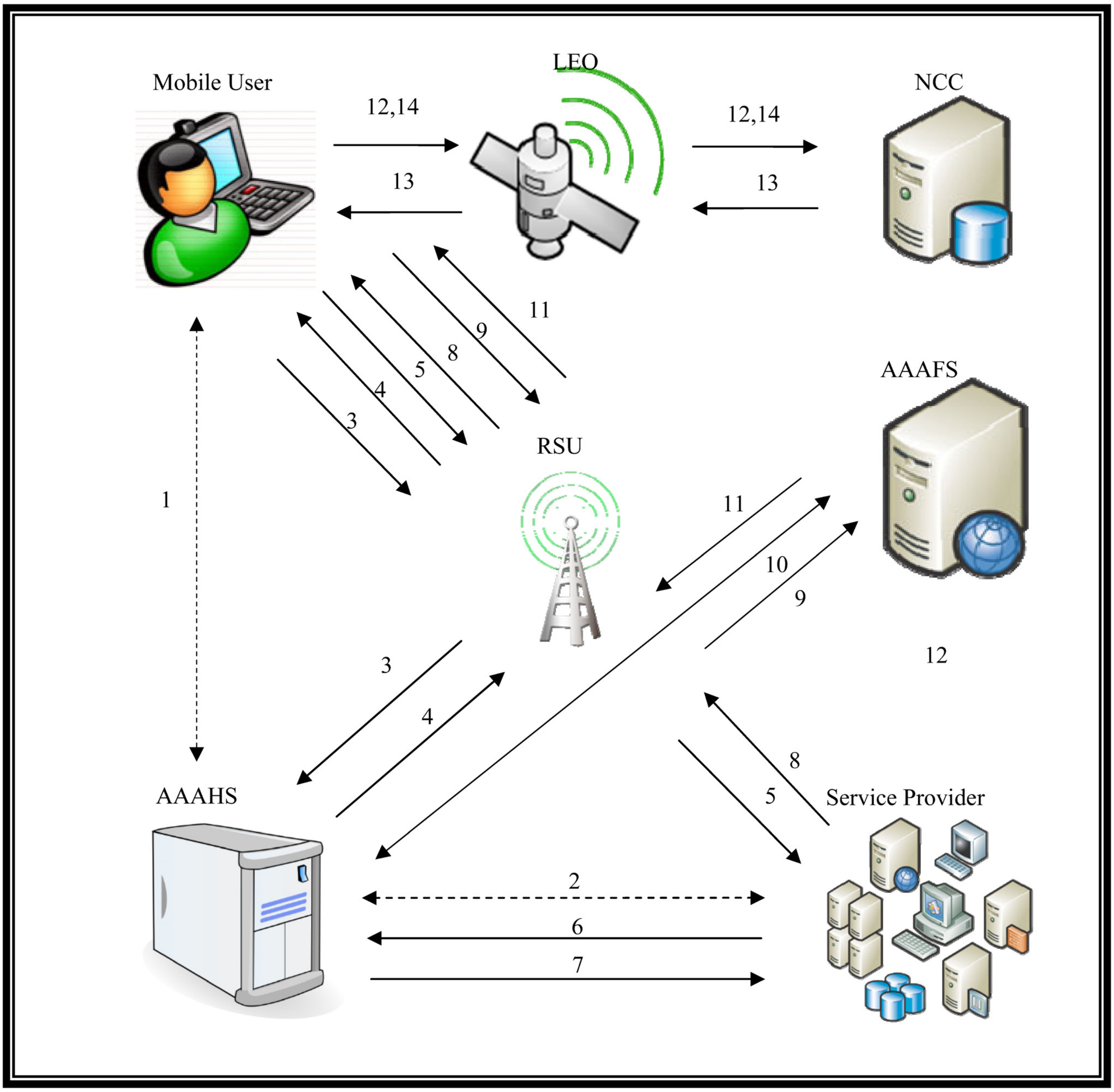


Figure 1. The architecture flow chart

3.2 Registration

Both the mobile user and the service provider, as well as the NCC,must register to the AAAHS.The two scenariosare illustrated in Figure 2.

3.2.1 Mobile user to AAAHS

Step 1. The mobile user chooses its identification credentials consisting of an identity ID_i and a password PW_i, to be passed to the AAAHS together with its driving license number. The VANET access device then computes two hash values A_1 and X_1 as follows:

$$A_1 = h(ID_i \| PW_i) \quad \textbf{(1)}$$

$$X_1 = h(A_1 \| PW_i) \quad \textbf{(2)}$$

Then, the value A_1 and the user's driving license *license* are sent to AAAHS within the registration message and the value X_1 is storedin the access device on volatile memory.

Step 2. After receiving the mobile user's registration message, the AAAHS uses the private parameter Y_i and the private key x to compute the new parameters F_i and G_i:

$$F_i = A_1 \oplus h(Y_i) \quad \textbf{(3)}$$

$$G_i = h(Y_i \| x) \oplus F_i \quad \textbf{(4)}$$

It then generates a random number $nonce_1$ and computes the mobile user's temporary identity code T_{ID} and the value I_i *as follows*:

$$T_{ID} = h(A_1 \| x \| nonce_1) \quad \textbf{(5)}$$

$$I_i = license \oplus x \oplus h(Y_i \| x) \oplus T_{ID} \quad \textbf{(6)}$$

T_{ID}	:	the mobile user's temporary ID code
ID_X	:	*X*'s identity
license	:	the driver license of the mobile user
PW_i	:	mobile user's password
x	:	AAAHS's private key
M_{req}	:	the request for updating authentication message
$M_{LOCATION}$	:	the request message for locating the car which is issued by mobile user
$M_{POSITION}$	:	vehicle's current location information which is issued by NCC
$M_{ACCIDENT}$	:	emergency message
M_{REPORT}	:	report message
Sig_i	:	the i^{th} digital signature
Lifetime	:	the validity period of digital certificate
Cert	:	the digital certificate
$nonce_i$	:	the i^{th} random number
$temp_{puk}/temp_{prk}$	:	a temporary public/private key
$E_X[M]/D_X[M]$	:	use the symmetric key *X* to encrypt/decrypt message *M*
$S_X[M]$	:	use the private key *X* to sign message *M*
$V_X[M]$	:	use the public key *X* toverify message *M*
SK_{MU-X}	:	the session key of mobile user and *X*
TSP_X	:	the timp stamp of *X*
$h(\cdot)$	:	one-way hash function
$\|\|$	:	concatenation operation
$\dashrightarrow$	:	secure channel
$\longrightarrow$	:	insecure channel

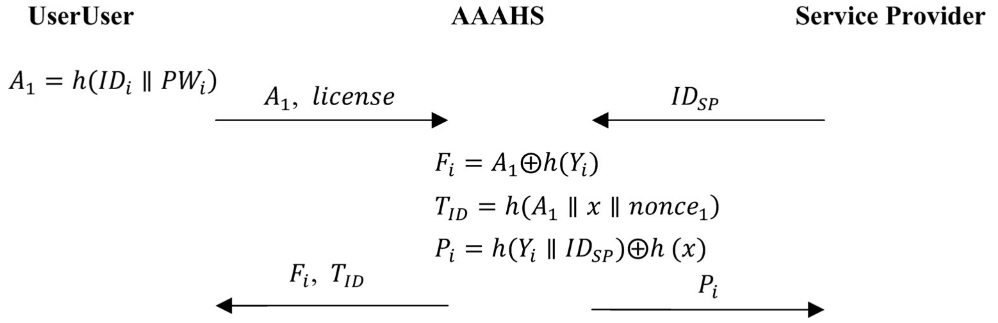

UserUser
AAAHS
Service Provider
$A_1 = h(ID_i \| PW_i)$
$A_1,\ license$
ID_{SP}
$F_i = A_1 \oplus h(Y_i)$
$T_{ID} = h(A_1 \| x \| nonce_1)$
$P_i = h(Y_i \| ID_{SP}) \oplus h\ (x)$
$F_i,\ T_{ID}$
P_i

Figure 2. Scenario of the registration phase

Finally, the AAAHS sends back the successfully registered notification message, containing the parameter F_i and the temporary identity code T_{ID} to the mobile user by completing the registration. These parameters will be used by the access device in securing future interactions with AAAHS (i.e. during the mobile users' authentication process).

3.2.2 Service provider (or NCC) to AAAHS

Step 1. The service provider sends its own identity ID_{SP} to the AAAHS in order to register for future interactions involving remote user identification. The same holds for the NCC that has to interact with AAAHS for coping with users' identities, and hence manage authentications and service requests.

Step 2. After receiving the registration request information, AAAHS uses a private key x and private parameter Y_i to compute P_i:

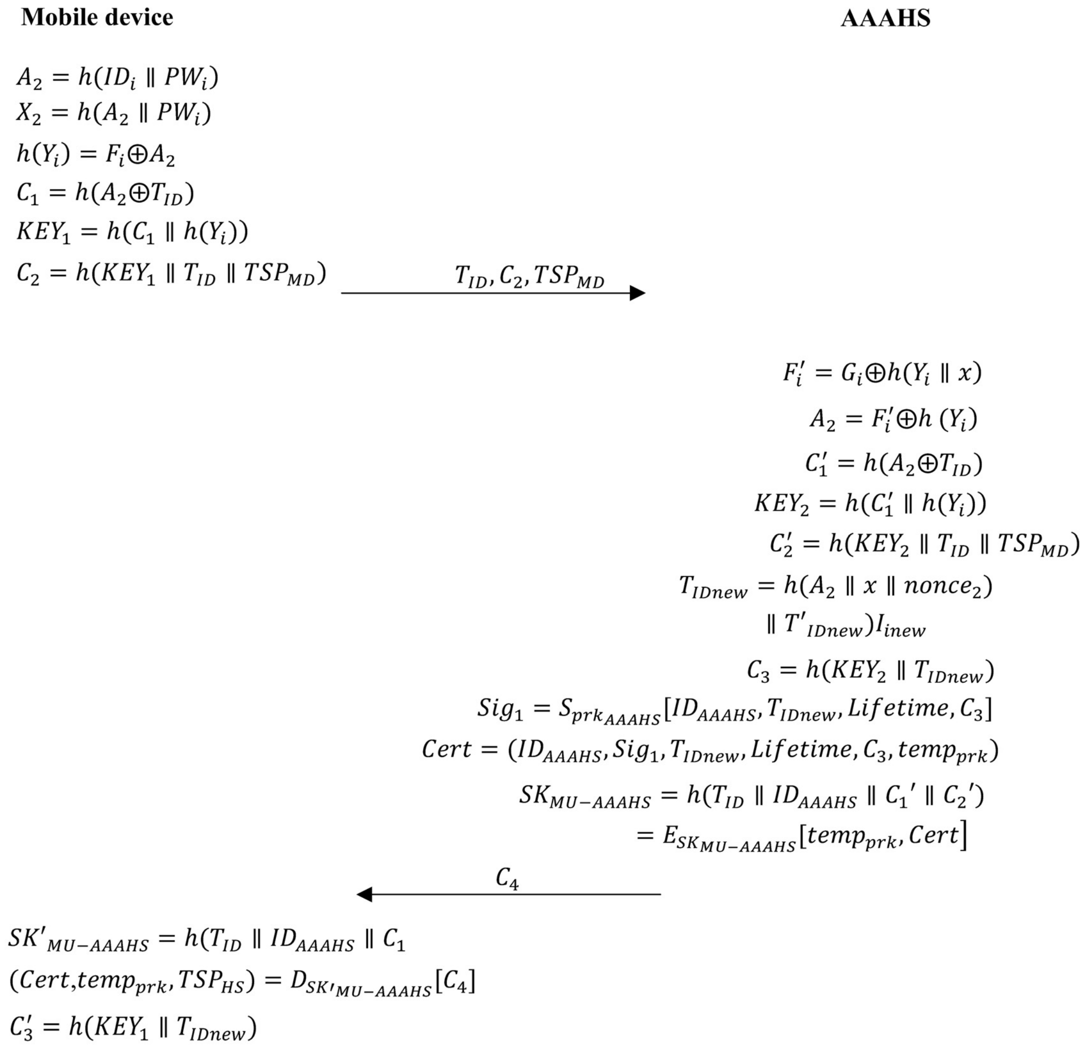
$$P_i = h(Y_i \| ID_{SP}) \oplus h(x) \qquad \textbf{(7)}$$

Lastly, AAAHS sends P_i to the service provider by completing the registration. P_i will be useful to the provider in securing its future interactions with AAAHS.

3.3 Authentication

In this verification, the mobile user and the AAAHS confirm each other's identity via mutual authentication.

Afterward, the AAAHS uses its private key for a signature operation by issuingan authorization certificateto the mobile user. The overview of the authentication phase is displayed in Figure 3, whereas the detailed descriptions are also given in the following.



$$A_2 = h(ID_i \parallel PW_i)$$
$$X_2 = h(A_2 \parallel PW_i)$$
$$h(Y_i) = F_i \oplus A_2$$
$$C_1 = h(A_2 \oplus T_{ID})$$
$$KEY_1 = h(C_1 \parallel h(Y_i))$$
$$C_2 = h(KEY_1 \parallel T_{ID} \parallel TSP_{MD})$$

$$F_i' = G_i \oplus h(Y_i \parallel x)$$
$$A_2 = F_i' \oplus h\,(Y_i)$$
$$C_1' = h(A_2 \oplus T_{ID})$$
$$KEY_2 = h(C_1' \parallel h(Y_i))$$
$$C_2' = h(KEY_2 \parallel T_{ID} \parallel TSP_{MD})$$
$$T_{IDnew} = h(A_2 \parallel x \parallel nonce_2)$$
$$\parallel T'_{IDnew})I_{inew}$$
$$C_3 = h(KEY_2 \parallel T_{IDnew})$$
$$Sig_1 = S_{prk_{AAAHS}}[ID_{AAAHS}, T_{IDnew}, Lifetime, C_3]$$
$$Cert = (ID_{AAAHS}, Sig_1, T_{IDnew}, Lifetime, C_3, temp_{prk})$$
$$SK_{MU-AAAHS} = h(T_{ID} \parallel ID_{AAAHS} \parallel C_1' \parallel C_2')$$
$$= E_{SK_{MU-AAAHS}}[temp_{prk}, Cert]$$

$$SK'_{MU-AAAHS} = h(T_{ID} \parallel ID_{AAAHS} \parallel C_1$$
$$(Cert, temp_{prk}, TSP_{HS}) = D_{SK'_{MU-AAAHS}}[C_4]$$
$$C_3' = h(KEY_1 \parallel T_{IDnew})$$

Figure 3. Overview of the authentication phase

Step 1. The mobile user inputs his identity code ID_i and password PW_i to his VANET access device that computes the values A_2 and X_2 as follows:

$$A_2 = h(ID_i \,||\, PW_i) \quad \textbf{(8)}$$

$$X_2 = h(A_2 \,||\, PW_i) \quad \textbf{(9)}$$

After that, the VANET device checks whether or not X_2 is equal to X_1, which has been previously stored in its non-volatile memory:

$$X_2 \overset{?}{=} X_1 \quad \textbf{(10)}$$

If it holds, the device computes some authentication-related parameters, which includes the time stamp TSP_{MD}:

$$h(Y_i) = F_i \oplus A_2 \quad \textbf{(11)}$$

$$C_1 = h(A_2 \oplus T_{ID}) \quad \textbf{(12)}$$

$$KEY_1 = h(C_1 \,||\, h(Y_i)) \quad \textbf{(13)}$$

$$C_2 = h(KEY_1 \,||\, T_{ID} \,||\, TSP_{MD}) \quad \textbf{(14)}$$

Then, it sends an authentication request message (T_{ID}, C_2, TSP_{MD}) to AAAHS.

Step 2. After receiving the authentication request message, the AAAHS checks the time stamp TSP_{MD} and uses the temporary identity T_{ID} to find the mobile user's information and computes the following values:

$$F_i^{'} = G_i \oplus h(Y_i \,||\, x) \quad \textbf{(15)}$$

$$A_2 = F_i^{'} \oplus h(Y_i) \quad \textbf{(16)}$$

$$C_i^{'} = h(A_2 \oplus T_{ID}) \quad \textbf{(17)}$$

$$KEY_2 = h(C_1^{'} \,||\, h(Y_i)) \quad \textbf{(18)}$$

The AAAHS then computes another hash C_2*'* and checks if it is equal to the value C_2 sent by the mobile device in its authentication request message:

$$C_2^{'} = h(KEY_2 \,||\, T_{ID} \,||\, TSP_{MD}) \quad \textbf{(19)}$$

$$C_2' \overset{?}{=} C_2 \qquad (20)$$

If such condition holds, it means that the mobile user's authentication request message can be approved; otherwise, the AAAHS will deny this request.

After the above authentication check, the AAAHS generates a new random number *nonce*$_2$ and updates the temporary identity T_{IDnew} to the mobile user to be used for the next authentication:

$$T_{IDnew} = h(A_2 \,||\, x \,||\, nonce_2) \qquad (21)$$

$$I_{inew} = I_i \oplus T_{ID} \oplus T_{IDnew} \qquad (22)$$

$$C_3 = h(KEY_2 \,||\, T_{IDnew}) \qquad (23)$$

The AAAHS then issues a pair of temporary public/private keys: *temp*$_{puk}$/*temp*$_{prk}$ to the mobile user and an authorization certificate *Cert* which includes its identityID_{AAAHS}, AAAHS's digital signature *Sig*$_1$, the mobile user's temporary identity code T_{IDnew}, the certificate's validity period *Lifetime*, the hash C_3 and the above temporary private key *temp*$_{prk}$. The AAAHS uses its private key *prk*$_{AAHS}$ to compute the signature as follows:

$$Sig_1 = S_{prk_{AAAHS}}[ID_{AAAHS, T_{IDnew}}, \; Lifetime, C_3] \qquad (24)$$

$$Cert = (ID_{AAAHS}, Sig_1, T_{IDnew}, Lifetime, \; C_3, temp_{prk}) \qquad (25)$$

it also computes a session key $SK_{MU-AAAHS}$ for securing its interaction with the mobile user as follows:

$$temp_i = temp_{prk} \oplus I_{inew} \qquad (26)$$

$$SK_{MU-AAAHS} = h(T_{ID} \,||\, ID_{AAAHS} \,||\, C_1' \,||\, C_2') \qquad (27)$$

Then, the AAAHS uses the session key to encrypt the user's temporary private key $temp_{prk}$, the digital certificate *Cert*, and the time stamp *TSP*$_{HS}$:

$$C_4 = E_{SK_{MU-AAAHS}}[temp_{prk}, Cert, TSP_{HS}] \qquad (28)$$

andfinally, it sends the encrypted message C_4 back to the mobile user, for granting the authentication.

Step 3. After receiving the authentication grantmessage, the mobile user computes the session key by using the previously determined authentication parameters and decrypts the message C_4:

$$SK'_{MU-AAAHS} = h(T_{ID} \,||\, ID_{AAAHS} \,||\, C_1 \,||\, C_2) \qquad (29)$$

$$(Cert, temp_{prk}, TSP_{HS}) = D_{SK'_{MU-AAAHS}}[C_4] \qquad (30)$$

Then, the mobile user verifies if the digital signature is valid or not:

$$V_{puk_{AAAHS}}(Sig_1) \overset{?}{=} (ID_{AAAHS}, T_{IDnew}, \; Lifietime, C_3) \qquad (31)$$

After this, the mobile user computes parameter $C_3{}'$ and verifies if it equals the C_3 value provided by AAAHS:

$$C_3' = h(KEY_1 \,||\, T_{IDnew}) \qquad (32)$$

$$C_3' \overset{?}{=} C_3 \qquad (33)$$

If the condition holds, the mobile user can ensure authentication with AAAHS is approved; otherwise he will terminate unsuccessfully the request process. Lastly, the mobile user will update the temporary identity for the next authentication (i.e., by setting $T_{ID} = T_{IDnew} \; and \; I_i = I_{inew}$).

3.4 Request for Service

When a mobile user requests a specific service, he must be authenticated in advance. The same holds for accessing to emergency services provided by NCC, that in the following will be considered as a service provider for satellite-based notifications. Accordingly, users that want to use notification services have to previously perform service request to the NCC. The mobile user submits the authentication grant message and authorization certificate received by AAAHS to the service provider (or NCC) for verification. If the mobile user's identity and authentication grant message are approved, the requested service will be provided to him. An overview of the service request/approval process and the detailed implementation steps are respectively illustrated in Figure 4 and in the following paragraphs.

Step 1. The mobile user inputs his/her identity ID_i and password PW_i to the VANET access device that computes the values A_2 and X_2 as follows:

$$A_3 = h(ID_i \,||\, PW_i) \qquad (34)$$

$$X_3 = h(A_3 \,||\, PW_i) \qquad (35)$$

After that, the mobile device checks whether or not X_3 is equal to the parameter X_1 which has been stored in the device's nonvolatile memory at the registration time:

$$X_3 \overset{?}{=} X_1 \qquad (36)$$

If it holds, the access device computes the other parameters, which includes the time stamp *TSP*$_{MD2}$:

$$h(Y_i) = F_i \oplus A_3 \qquad (37)$$

$$C_s = h(A_3 \oplus T_{IDnew}) \qquad (38)$$

$$KEY_3 = h(T_{IDnew} \,||\, ID_{SP} \,||\, C_5) \qquad (39)$$

$$C_6 = h(A_3 \,||\, KEY_3 \,||\, TSP_{MD2}) \qquad (40)$$

It then sends the authentication request message ($T_{IDnew}, C_6, TSP_{MD2}$) to the service provider.

Step 2. After receiving the authentication request message, the service provider generates a random number *nonce*$_3$ and computes the parameter *K*, which includes the time stamp *TSP*$_{SP}$:

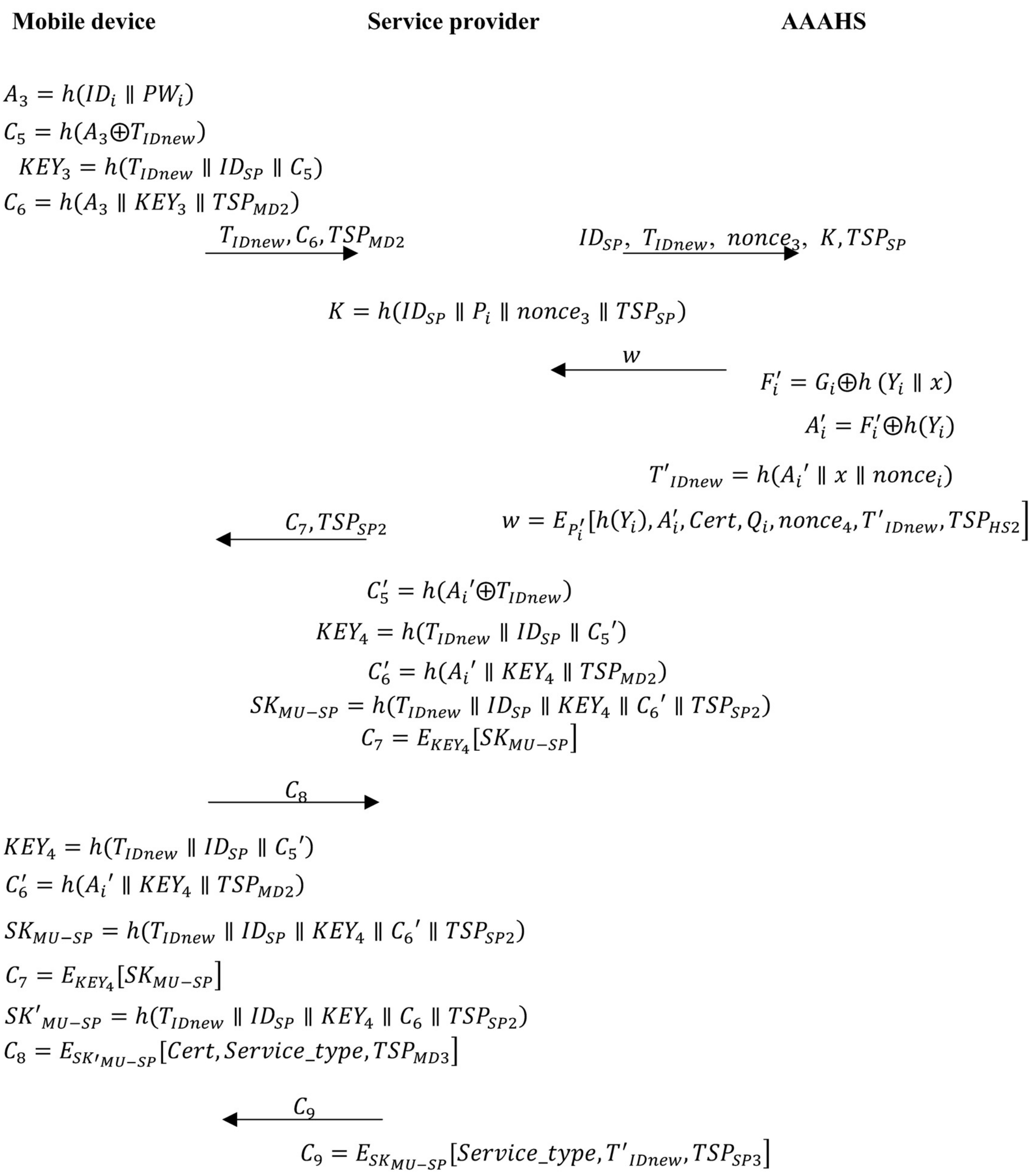

Mobile device
Service provider
AAAHS
$A_3 = h(ID_i \parallel PW_i)$
$C_5 = h(A_3 \oplus T_{IDnew})$
$KEY_3 = h(T_{IDnew} \parallel ID_{SP} \parallel C_5)$
$C_6 = h(A_3 \parallel KEY_3 \parallel TSP_{MD2})$
$T_{IDnew}, C_6, TSP_{MD2}$
$ID_{SP}, T_{IDnew}, nonce_3, K, TSP_{SP}$
$K = h(ID_{SP} \parallel P_i \parallel nonce_3 \parallel TSP_{SP})$
w
$F_i' = G_i \oplus h(Y_i \parallel x)$
$A_i' = F_i' \oplus h(Y_i)$
$T'_{IDnew} = h(A_i' \parallel x \parallel nonce_i)$
C_7, TSP_{SP2}
$w = E_{P_i'}[h(Y_i), A_i', Cert, Q_i, nonce_4, T'_{IDnew}, TSP_{HS2}]$
$C_5' = h(A_i' \oplus T_{IDnew})$
$KEY_4 = h(T_{IDnew} \parallel ID_{SP} \parallel C_5')$
$C_6' = h(A_i' \parallel KEY_4 \parallel TSP_{MD2})$
$SK_{MU-SP} = h(T_{IDnew} \parallel ID_{SP} \parallel KEY_4 \parallel C_6' \parallel TSP_{SP2})$
$C_7 = E_{KEY_4}[SK_{MU-SP}]$
C_8
$KEY_4 = h(T_{IDnew} \parallel ID_{SP} \parallel C_5')$
$C_6' = h(A_i' \parallel KEY_4 \parallel TSP_{MD2})$
$SK_{MU-SP} = h(T_{IDnew} \parallel ID_{SP} \parallel KEY_4 \parallel C_6' \parallel TSP_{SP2})$
$C_7 = E_{KEY_4}[SK_{MU-SP}]$
$SK'_{MU-SP} = h(T_{IDnew} \parallel ID_{SP} \parallel KEY_4 \parallel C_6 \parallel TSP_{SP2})$
$C_8 = E_{SK'_{MU-SP}}[Cert, Service\_type, TSP_{MD3}]$
C_9
$C_9 = E_{SK_{MU-SP}}[Service\_type, T'_{IDnew}, TSP_{SP3}]$

Figure 4. Overview of the request for service phase

$$K = h(ID_{SP} \parallel P_i \parallel nonce_3 \parallel TSP_{SP}) \quad \textbf{(41)}$$

Then, the service provider sends its identity code ID_{SP}, the mobile user's temporary identity T_{IDnew}, the random number $nonce_2$, the time stamp TSP_{SP} and the parameter K to AAAHS by relaying the authentication request.

Step 3. The AAAHS checks if the service provider's identity is valid or not against K:

$$P_i^{'} = h(ID_{SP} \parallel Y_i) \oplus h(x) \quad \textbf{(42)}$$

$$K^{'} = h(ID_{SP} \parallel P_i^{'} \parallel nonce_3 \parallel TSP_{SP}) \quad \textbf{(43)}$$

$$K^{'} \overset{?}{=} K \quad \textbf{(44)}$$

If valid, the AAAHS uses the mobile user's temporary identity T_{IDnew} and searches for his related information, then computes $F_i^{'}$ and $A_i^{'}$:

$$F_i^{'} = G_i \oplus h(Y_i \parallel x) \quad \textbf{(45)}$$

$$A_i^{'} = F_i^{'} \oplus h(Y_i) \quad \textbf{(46)}$$

Then, AAAHS generates a new random number $nonce_4$ and computes an authentication grant hash Q_i for the service provider:

$$Q_i = h(P_i^{'} \parallel nonce_4) \quad \textbf{(47)}$$

It also generates a new temporary identity $T_{IDnew}^{'}$ for the mobile user to perform the next authentication:

$$T_{IDnew}^{'} = h(A_i^{'} \parallel x \parallel nonce_i) \quad \textbf{(48)}$$

Finally, AAAHS uses the private parameters $P_i^{'}$ to encrypt the message:

$$w = E_{P_i^{'}}[h(Y_i), A_i^{'}, Cert, Q_i, nonce_4, T^{'}{}_{IDnew}, TSP_{HS2}] \quad \textbf{(49)}$$

And sends the encrypted authentication grant message *w* to the service provider.

Step 4. After receiving the encrypted message, the service provider obtains the mobile user's information by decrypting the message with its private parameter $P_i^{'}$:

$$(h(Y_i), A_i^{'}, Cert, Q_i, nonce_4, T^{'}_{IDnew}, TSP_{HS2}) = D_{P_i^{'}}[w] \quad \textbf{(50)}$$

$$Q_i^{'} = h(P_i \,||\, nonce_4) \quad \textbf{(51)}$$

$$Q_i^{'} \overset{?}{=} Q_i \quad \textbf{(52)}$$

It then computes another hash $Q_i^{'}$ that is then compared with the authentication grant hash Q_i and ifequal, the validity of the mobile user's identity will be checked as follows:

$$C_5^{'} = h(A_i^{'} \oplus T_{IDnew}) \quad \textbf{(53)}$$

$$KEY_4 = h(T_{IDnew} \,||\, ID_{SP} \,||\, C_5^{'}) \quad \textbf{(54)}$$

$$C_6^{'} = h(A_i^{'} \,||\, KEY_4 \,||\, TSP_{MD2}) \quad \textbf{(55)}$$

$$C_6^{'} \overset{?}{=} C_6 \quad \textbf{(56)}$$

If also this last check is successful, the service provider gets a confirmation that the mobile user is legal. Then, the service provider will generate a session key SK_{MU-SP} for the mobile user and uses KEY_4 to encrypt the session key SK_{MU-SP}:

$$SK_{MU-SP} = h(T_{IDnew} \,||\, ID_{SP} \,||\, KEY_4 \,||\, C_6^{'} \,||\, TSP_{SP2}) \quad \textbf{(57)}$$

$$C_7 = E_{KEY_4}[SK_{MU-SP}] \quad \textbf{(58)}$$

The session key, when the service provider is the NCC (providing emergency notification services) will be used for ensuring the communications occurring through the satellite channel. The service provider then sends (C_7, TSP_{SP2}) to the mobile user. Clearly, if any of the last two verifications fails the entire process is aborted.

Step 5. After receiving the message (C_7, TSP_{SP2}) from the service provider, the mobile user decrypts it and verifies the service provider by checking the session key:

$$SK_{MU-SP} = D_{KEY_3}[C_7] \quad \textbf{(59)}$$

$$SK^{'}_{MU-SP} = h(T_{IDnew} \,||\, ID_{SP} \,||\, KEY_4 \,||\, C_6 \,||\, TSP_{SP2}) \quad \textbf{(60)}$$

$$SK^{'}_{MU-SP} \overset{?}{=} SK_{MU-SP} \quad \textbf{(61)}$$

If verification succeeds, the session key $SK^{'}_{MU-SP}$ is used to encrypt the digital certificate and the type of requested service (*Service_type*):

$$C_8 = E_{SK^{'}_{MU-SP}}[Cert, Service_{type}, TSP_{MD3}] \quad \textbf{(62)}$$

Then, the mobile user sends C_8 to the service provider.

Step 6. After receiving the request message sent by the mobile user, the service provider (or NCC) uses the session key to decrypt the digital certificate *Cert* and checks if the authorization certificate is valid or not:

$$(Cert, Service_{type}, TSP_{MD3}) = D_{SK_{MU-SP}}[C_8] \quad \textbf{(63)}$$

After successful verification of the certificate's validity period *Lifetime*, the service provider is able to provide the requested service *Service_type* to the mobile user and uses the session key to encrypt the service type and the mobile user's temporary identity code $T^{'}_{IDnew}$, which includes the time stamp TSP_{SP3}:

$$C_9 = E_{SK_{MU-SP}}[Service_{type}, T^{'}_{IDnew}, TSP_{SP3}] \quad \textbf{(64)}$$

Then, the provider sends C_9 to the mobile user.

3.5 Update Authorization Certificate from the Foreign Network

When a foreign mobile user roams into VANET roadside network, if his authorization certificate is still valid, there is no need to request for a new one, if his authorization certificate is expired,a re-authentication is needed to get a new authorization certificate, so that he/she can continue roaming and get related services. The overview of the whole process is illustrated in Figure 5, followed by a detailed description of the involved steps.

Step 1. The mobile user inputs his/her identity ID_i and password PW_i to the mobile device; the mobile device then computes A_4 and X_4 as follows:

$$A_4 = h(ID_i \,||\, PW_i) \quad \textbf{(65)}$$

$$X_4 = h(A_4 \,||\, PW_i) \quad \textbf{(66)}$$

After that, the mobile device checks whether the X_4 is equal to X_1, which has been previously stored intoit:

$$X_4 \overset{?}{=} X_1 \quad \textbf{(67)}$$

If equality holds, the mobile device updates the authorization certification message M_{req} and computes other parameters as follows:

$$h(Y_i) = F_i \oplus A_4 \quad \textbf{(68)}$$

$$C_{10} = h(A_4 \oplus T^{'}_{IDnew}) \quad \textbf{(69)}$$

$$KEY_5 = h(C_{10} \,||\, h(Y_i)) \quad \textbf{(70)}$$

$$C_{11} = h(KEY_5 \,||\, T^{'}_{IDnew} \,||\, TSP_{MD4}) \quad \textbf{(71)}$$

Then, the mobile device will send the authentication message $(T^{'}_{IDnew}, C_{11}, M_{req}, TSP_{MD4})$ to AAAFS.

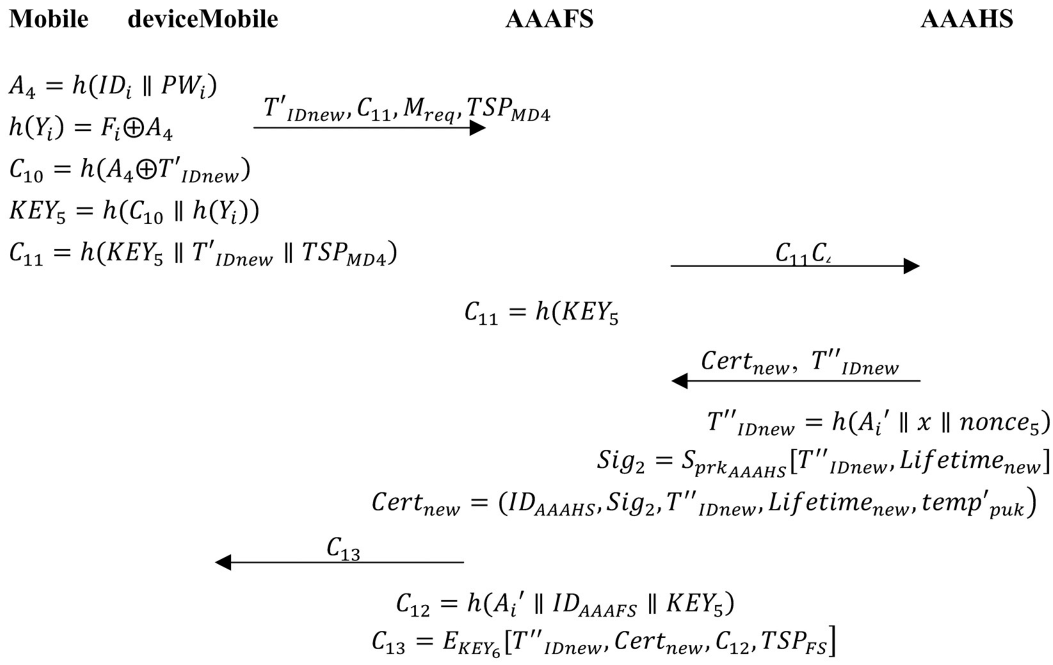

Mobile deviceMobile
AAAFS
AAAHS
$A_4 = h(ID_i \parallel PW_i)$
$h(Y_i) = F_i \oplus A_4$
$C_{10} = h(A_4 \oplus T'_{IDnew})$
$KEY_5 = h(C_{10} \parallel h(Y_i))$
$C_{11} = h(KEY_5 \parallel T'_{IDnew} \parallel TSP_{MD4})$
$T'_{IDnew}, C_{11}, M_{req}, TSP_{MD4}$
$C_{11}C_{\iota}$
$C_{11} = h(KEY_5$
$Cert_{new}, T''_{IDnew}$
$T''_{IDnew} = h(A_i' \parallel x \parallel nonce_5)$
$Sig_2 = S_{prk_{AAAHS}}[T''_{IDnew}, Lifetime_{new}]$
$Cert_{new} = (ID_{AAAHS}, Sig_2, T''_{IDnew}, Lifetime_{new}, temp'_{puk})$
C_{13}
$C_{12} = h(A_i' \parallel ID_{AAAFS} \parallel KEY_5)$
$C_{13} = E_{KEY_6}[T''_{IDnew}, Cert_{new}, C_{12}, TSP_{FS}]$

Figure 5. Overview of certificate update from the foreign network phase

Step 2. After receiving the message, AAAFS verifies if the mobile user is approved or not:

$$F_i' = G_i \oplus h(Y_i \parallel x) \quad \textbf{(72)}$$

$$A_i' = F_i' \oplus h(Y_i) \quad \textbf{(73)}$$

$$C_{10} = h(A_i' \oplus T'_{IDnew}) \quad \textbf{(74)}$$

$$KEY_6 = h(C_{10}' \parallel h(Y_i)) \quad \textbf{(75)}$$

$$C_{11}' = h(KEY_6 \parallel T'_{IDnew} \parallel TSP_{MD4}) \quad \textbf{(76)}$$

AAAFS checks if C_{11}' equals the authentication message C_{11} sent by the mobile user:

$$C_{11}' \overset{?}{=} C_{11} \quad \textbf{(77)}$$

If it is true, AAAFS sends it to AAAHS through a secure channel.

Step 3. AAAHS generates a new temporary identity T''_{IDnew}, validity period $Lifetime_{new}$ and authorization certificate $Cert_{new}$ to the mobile user:

$$T''_{IDnew} = h(A_i' \parallel x \parallel nonce_5) \quad \textbf{(78)}$$

$$I_{inew}' = I_{inew} \oplus T'_{IDnew} \oplus T''_{IDnew} \quad \textbf{(79)}$$

$$temp_i' = I_{inew}' \oplus temp'_{puk} \quad \textbf{(80)}$$

$$Sig_2 = Sprk_{AAAHS}[T''_{IDnew}, Lifetime_{new}] \quad \textbf{(81)}$$

$$Cert_{new} = (ID_{AAAHS}, Sig_2, T''_{IDnew}, Lifetime_{new}, temp'_{puk}) \quad \textbf{(82)}$$

Then, AAAHS sends the new authorization certificate $Cert_{mew}$ and temporary identity T''_{IDnew} to AAAFS through a secure channel.

Step 4. AAAFS computes a new parameter C_{12} and uses the mobile user's key KEY_6 to encrypt the authorization certificate $Cert_{new}$, the mobile user's temporary identity T''_{IDnew} and parameter C_{12}, which includes the time stamp TSP_{PS}:

$$C_{12} = h(A_i' \parallel ID_{AAAFS} \parallel KEY_5) \quad \textbf{(83)}$$

$$C_{13} = E_{KEY_6}[T''_{IDnew}, Cert_{new}, C_{12}, TSP_{FS}] \quad \textbf{(84)}$$

AAAFS sends C_{13} to the mobile user.

Step 5. After receiving the message, the mobile user uses the key KEY_5 to decrypt C_{12}, and verifies the AAAFS:

$$(T''_{IDnew}, Cert_{new}, C_{12}, TSP_{FS}) = D_{KEY_5}[C_{13}] \quad \textbf{(85)}$$

$$V_{puk_{AAAFS}}(Sig_2) \overset{?}{=} (T''_{IDnew}, Lifetime_{new}) \quad \textbf{(86)}$$

$$C_{12}' = h(A_i' \parallel ID_{AAAFS} \parallel KEY_6) \quad \textbf{(87)}$$

$$C_{12}' \overset{?}{=} C_{12} \quad \textbf{(88)}$$

If successful, the AAAFS is approved. The mobile user then updates his temporary identity T''_{IDnew} and his authorization certificate with $Cert_{new}$.

3.6 Transfer Emergency Information

In presence of an accident occurred on the road, when one of the involved drivers or a generic mobile user on another vehicle has to inform the other ones coming from behind, in order to prevent further collisions, he can send an emergency notification message to notify the rear vehicles about the accident by relying on cryptographic techniques to protect the privacy of notifiers through anonymity and simultaneously ensure trustability of the notifications. The overview and the detailed steps describing the process are respectively illustrated in both Figure 6 and the following paragraph.

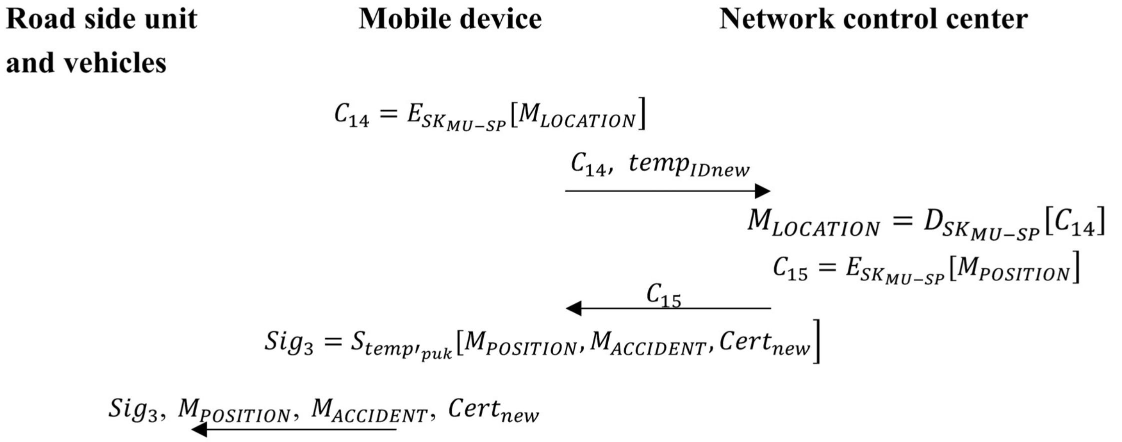

Road side unit and vehicles
Mobile device
Network control center
$C_{14} = E_{SK_{MU-SP}}[M_{LOCATION}]$
$C_{14},\ temp_{IDnew}$
$M_{LOCATION} = D_{SK_{MU-SP}}[C_{14}]$
$C_{15} = E_{SK_{MU-SP}}[M_{POSITION}]$
C_{15}
$Sig_3 = S_{temp'_{puk}}[M_{POSITION}, M_{ACCIDENT}, Cert_{new}]$
$Sig_3,\ M_{POSITION},\ M_{ACCIDENT},\ Cert_{new}$

Figure 6. Overview of transfer emergency information phase

Step 1. When there is an accident, a mobile user (also the involved driver) can use the session key SK_{MU-SP}, previously obtained through a

Step 2. service request to NCC, to request location of the vehicle to the NCC through a specific message:

$$C_{14} = E_{SK_{MU-SP}}[M_{LOCATION}] \qquad \textbf{(89)}$$

Then, the mobile device sends C_{14} and the mobile user's temporary identity $temp_{IDnew}$ to the network control center. Communications take place through the satellite link.

Step 3. After receiving the location request message sent by the mobile user, the network control center decrypts C_{14} to get the location of the sender and uses the previous session key to encrypt the sender's current position information:

$$M_{LOCATION} = D_{SK_{MU-SP}}[C_{14}] \qquad \textbf{(90)}$$

$$C_{15} = E_{SK_{MU-SP}}[M_{POSITION}] \qquad \textbf{(91)}$$

The network control center then sends C_{15} to the mobile user.

Step 4. The mobile user decrypts C_{15} to get the position information and uses the temporary private key to sign the accident information:

$$M_{POSITION} = D_{SK_{MU-SP}}[C_{15}] \qquad \textbf{(92)}$$

$$Sig_3 = S_{temp'_{puk}}[M_{POSITION}, M_{ACCIDENT}, Cert_{new}] \qquad \textbf{(93)}$$

Then, the mobile device sends the emergency notification message (Sig_2, $M_{POSITION}$, $M_{ACCIDENT}$, $Cert_{new}$) to the NCC, to the roadside unit and eventually broadcasts to the near vehicles through V2V communications. If there is no available roadside unit to send out the notification, the other mobile device that have not been already alerted via V2V will be alerted by the NCC through their RSUs (if any) or satellite links.

After the other vehicles get the emergency notification message, their driver can obtain the public key from the authorization certificate in the message and use such public key to verify the effectiveness and integrity of the signature Sig_2. Also, the driver checks if the certificate is still valid or not and uses the issued party's public key to check the mobile user's validity:

$$V_{temp'_{puk}}(Sig_3) \overset{?}{=} (M_{POSITION}, M_{ACCIDENT}, Cert_{new}) \qquad \textbf{(94)}$$

$$V_{puk_{AAAH}}(Sig_2) \overset{?}{=} (T''_{IDnew}, Lifetime_{new}) \qquad \textbf{(95)}$$

3.7 Track Malicious Behavior

If a malicious entity appears in the vehicle network communication system to attack it, AAAHS can track the malicious behavior and send the malicious attackers' driving license information to the police station. The police can then punish the attackers. The overview is illustrated in Figure 7, followed by detailed descriptions of the steps.

Step 1. After authorizing the message, the rear vehicle's driver can help with sending the emergency notification message to AAAHS.

Step 2. AAAHS requests the police to go to the position of the accident to deal with the vehicles involved in the accident and provide related information (Sig_3, $M_{POSITION}$, $M_{ACCIDENT}$, $Cert_{new}$).

Step 3. When the police arrive at the accident site and find no accident, they will send the message M_{REPORT} to AAAHS and request the sender's real identity.

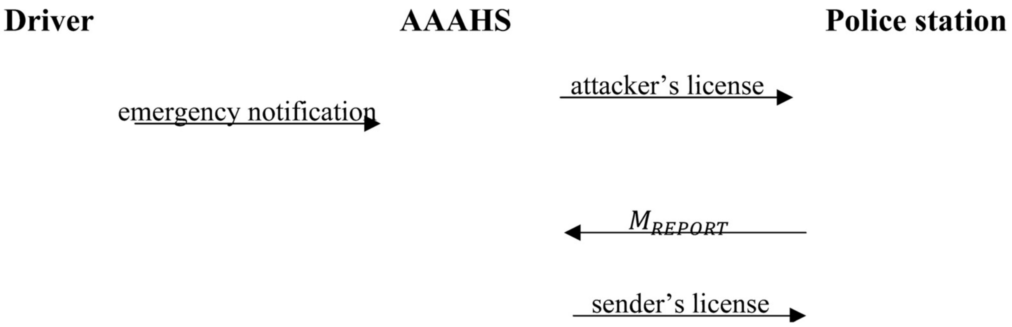


Figure 7. Overview of track malicious behavior phase

Step 4. After receiving the message sent by the police, AAAHS uses the corresponding information (T''_{IDnew}, $temp'_{puk}$) to search for the sender's real identity:

$$I'_{inew} = temp'_i \oplus temp'_{puk_i} \quad \textbf{(96)}$$

$$license = I'_{inew} \oplus T''_{IDnew} \oplus x \oplus h(Y_i \| x) \quad \textbf{(97)}$$

Lastly, AAAHS provides the sender's driver's license to the police and the malicious attacker will have to answer for sending a false alarm.

4 Security Analysis

In this section, we present a security analysis and discuss how our scheme meets the security requirements and defends against various attacks.

4.1 Mutual Authentication

We use BAN logic to prove that our scheme achieves mutual authentication between Mobile user and AAAHS in authentication phase.

In the authentication phase, the target of the scheme is to make sure whether the legality is authenticated by Mobile user *U* and AAAHS *S*.

G1: $U \mid\equiv U \overset{C_3}{\leftrightarrow} S$

G2: $U \mid\equiv S \mid\equiv U \overset{C_3}{\leftrightarrow} S$

G3: $S \mid\equiv U \overset{C_2}{\leftrightarrow} S$

G4: $S \mid\equiv U \mid\equiv U \overset{C_2}{\leftrightarrow} S$

G5: $U \mid\equiv Y_i$

G6: $U \mid\equiv S \mid\equiv Y_i$

G7: $S \mid\equiv ID_i$

G8: $S \mid\equiv U \mid\equiv ID_i$

According to the authentication phase, the BAN logic is applied for making an idealized form as follows:

M1: $(<ID_i, PW_i, T_{ID}>_{Hash})$

M2: $(<Y_i, x, T_{IDnew}>_{Hash})$

We use the assumptions to analyze our proposed scheme as follows:

A1: $U \mid\equiv \#(KEY_1)$

A2: $S \mid\equiv \#(KEY_1)$

A3: $U \mid\equiv \#(KEY_2)$

A4: $S \mid\equiv \#(KEY_2)$

A5: $U \mid\equiv S \mid\Rightarrow U \overset{C_3}{\leftrightarrow} S$

A6: $S \mid\equiv U \mid\Rightarrow U \overset{C_2}{\leftrightarrow} S$

A7: $U \mid\equiv S \mid\Rightarrow Y_i$

A8: $S \mid\equiv U \mid\Rightarrow ID_i$

The following are the BAN logic proof process of the authentication phase which according to the above rules and the related assumptions:

AAAHS *S* authenticates Mobile user *U*. We make the following statement through *M1* and the *seeing rule*:

$$S \triangleleft (<ID_i, PW_i, T_{ID}>_{Hash}) \quad (\textit{Statement 1})$$

We make the following statement through *A2* and the *freshness rule*:

$$S \mid\equiv \#(<ID_i, PW_i, T_{ID}>_{Hash}) \quad (\textit{Statement 2})$$

We make the following statement through (*Statement 1*), *A4* and the *message meaning rule*:

$$S \mid\equiv U \mid\sim (<ID_i, PW_i, T_{ID}>_{Hash}) \quad (\textit{Statement 3})$$

We make the following statement through (*Statement 2*), (*Statement 3*), and the *nonce verification rule*:

$$S \mid\equiv U \mid\equiv (<ID_i, PW_i, T_{ID}>_{Hash}) \quad (\textit{Statement 4})$$

We make the following statement through (*Statement 4*) and the *belief rule*:

$$S \mid\equiv U \mid\equiv U \overset{C_2}{\leftrightarrow} S \quad (\textit{Statement 5})$$

We make the following statement through (*Statement 5*), *A6* and the *jurisdiction rule*:

$$S \mid\equiv U \overset{C_2}{\leftrightarrow} S \quad (\textit{Statement 6})$$

We make the following statement through (*Statement 6*) and the *belief rule*:

$$S \mid\equiv U \mid\equiv ID_i \quad (\textit{Statement 7})$$

We make the following statement through (*Statement 7*), *A8* and the *jurisdiction rule*:

$$S \mid\equiv ID_i \qquad (Statement\ 8)$$

The mobile user should compute the validity authentication message (T_{ID}, C_2) to pass the AAAHS's authentication. Then, AAAHS verifies the correctness of the authentication message via Eq.20 $(C_2' \overset{?}{=} C_2)$. If it holds, AAAHS authenticates the mobile user's identity.

Mobile user *U* authenticates AAAHS *S*. We make the following statement through *M2* and the *seeing rule*:

$$U \triangleleft (<Y_i, x, T_{IDnew}>_{Hash}) \qquad (Statement\ 9)$$

We make the following statement through *A1* and the *freshness rule*:

$$U \mid\equiv \#(<Y_i, x, T_{IDnew}>_{Hash}) \qquad (Statement\ 10)$$

We make the following statement through (*Statement 9*), *A3* and the *message meaning rule*:

$$U \mid\equiv S \mid\sim (<Y_i, x, T_{IDnew}>_{Hash}) \qquad (Statement\ 11)$$

We make the following statement through (*Statement 10*), (*Statement 11*), and the *nonce verification rule*:

$$U \mid\equiv S \mid\equiv (<Y_i, x, T_{IDnew}>_{Hash}) \qquad (Statement\ 12)$$

We make the following statement through (*Statement 12*) and the *belief rule*:

$$U \mid\equiv S \mid\equiv U \overset{C_3}{\leftrightarrow} S \qquad (Statement\ 13)$$

We make the following statement through (*Statement 13*), *A5* and the *jurisdiction rule*:

$$U \mid\equiv U \overset{C_3}{\leftrightarrow} S \qquad (Statement\ 14)$$

We make the following statement through (*Statement 14*) and the *belief rule*:

$$U \mid\equiv S \mid\equiv Y_i \qquad (Statement\ 15)$$

We make the following statement through (*Statement 15*), *A7* and the *jurisdiction rule*:

$$U \mid\equiv Y_i \qquad (Statement\ 16)$$

The mobile user decrypts the message C_4 sent by AAAHS to get the authentication parameter C_3 and checks if C_3 is valid or not. If it holds, the mobile user authenticates AAAHS's identity.

We prove that the mutual authentication achieved between Mobile user *U* and AAAHS *S* in our scheme through (*Statement 6*), (*Statement 8*), (*Statement 14*), and (*Statement 16*).According to the above two cases, our protocol provides mutual authentication between the mobile user and AAAHS.

4.2 Confidential Communication

In our scheme, the emergency communication system can ensure the confidentiality by encrypting messages via the one-way hash function and symmetric key. In the authentication phase and certificate issuing phase, AAAHS and the mobile user can use the session key $SK_{MU-AAAHS} = h(T_{ID} \,\|\, ID_{AAAHS} \,\|\, C_1' \,\|\, C_2')$ to ensure the security of the communication. Even if a malicious attacker intercepts the session key $SK_{MU-AAAHS}$, he/she cannot use it to obtain the mobile user's real identity ID_i or the password PW_i. Nobody can use the same session key to trick the legal mobile user to communicate with AAAHS.

(1) During the authentication phase, AAAHS computes the session key $SK_{MU-AAAHS}$ and uses it to encrypt messages as follows:

$$SK_{MU-AAAHS} = h(T_{ID} \,\|\, ID_{AAAHS} \,\|\, C_1' \,\|\, C_2') \qquad \textbf{(27)}$$

$$C_4 = E_{SK_{MU-AAAHS}}[temp_{prk}, Cert, TSP_{HS}] \qquad \textbf{(28)}$$

Then, the mobile user computes a session key and decrypts the message:

$$SK'_{MU-AAAHS} = h(T_{ID} \,\|\, ID_{AAAHS} \,\|\, C_1 \,\|\, C_2) \qquad \textbf{(29)}$$

$$(Cert, temp_{prk}, TSP_{HS}) = D_{SK'_{MU-AAAHS}}[C_4] \qquad \textbf{(30)}$$

(2) During the request for service phase, the service provider and AAAHS use a symmetric key and one-way hash function to encrypt the information:

$$A_3 = h(ID_i \,\|\, PW_i) \qquad \textbf{(34)}$$

$$h(Y_i) = F_i \oplus A_3 \qquad \textbf{(37)}$$

$$A_i' = F_i' \oplus h(Y_i) \qquad \textbf{(46)}$$

$$Q_i = h(P_i' \,\|\, nonce_4) \qquad \textbf{(47)}$$

$$T_{IDnew}' = h(A_i' \,\|\, x \,\|\, nonce_i) \qquad \textbf{(48)}$$

$$w = E_{P_i'}[h(Y_i), A_i', Cert, Q_i, nonce_4, T'_{IDnew}, TSP_{HS2}] \qquad \textbf{(49)}$$

$$(h(Y_i), A_i', Cert, Q_i, nonce_4, T'_{IDnew}, TSP_{HS2}) \quad = D_{P_i'}[w] \qquad \textbf{(50)}$$

$$KEY_4 = h(T_{IDnew} \,\|\, ID_{SP} \,\|\, C_5') \qquad \textbf{(54)}$$

$$C_6' = h(A_i' \,\|\, KEY_4 \,\|\, TSP_{MD2}) \qquad \textbf{(55)}$$

$$SK_{MU-SP} = h(T_{IDnew} \,\|\, ID_{SP} \,\|\, KEY_4 \,\|\, C_6' \,\|\, TSP_{SP2}) \qquad \textbf{(57)}$$

$$C_7 = E_{KEY_4}[SK_{MU-SP}] \qquad \textbf{(58)}$$

$$SK_{MU-SP} = D_{KEY_3}[C_7] \qquad \textbf{(59)}$$

$$C_8 = E_{SK'_{MU-SP}}[Cert, Service_{type}, TSP_{MD3}] \qquad \textbf{(62)}$$

$$(Cert, Service_{type}, TSP_{MD3}) = D_{SK_{MU-SP}}[C_8] \quad \textbf{(63)}$$

(3) During the update authorization certificate phase, the mobile user uses the temporary identity code to update the authorization certificate; AAAFS then sends back the encrypted message. Only the mobile user can decrypt the message to obtain the sensitive information:

$$C_{13} = E_{KEY_6}[T^{"}_{IDnew}, Cert_{new}, C_{12}, TSP_{FS}] \quad \textbf{(84)}$$

$$(T^{"}_{IDnew}, Cert_{new}, C_{12}, TSP_{FS}) = D_{KEY_5}[C_{13}] \quad \textbf{(85)}$$

(4) During transfer emergency information phase, the mobile user uses the session key to encrypt/decrypt the request and notification as follows:

$$C_{14} = E_{SK_{MU-SP}}[M_{LOCATION}] \quad \textbf{(89)}$$

$$M_{LOCATION} = D_{SK_{MU-SP}}[C_{14}] \quad \textbf{(90)}$$

$$C_{15} = E_{SK_{MU-SP}}[M_{POSITION}] \quad \textbf{(91)}$$

$$M_{POSITION} = D_{SK_{MU-SP}}[C_{15}] \quad \textbf{(92)}$$

Therefore, our protocol can achieve confidential communication.

4.3 User's Privacy

The mobile user always uses the temporary identity to communicate with AAAHS or the service provider (and NCC) for any service request or verification as well as for emergency notification. In our scheme, the mobile device only stores the mobile user's temporary identity T_{ID} and parameter F_i. If the mobile user lost his/her device and a malicious attacker found it, the user need not worry about sensitive information being exposed.

4.4 Non-Repudiation

In the authentication phase, AAAHS uses the private key to generate a digital signature Sig_1 for the mobile user. In the emergency notification phase, the mobile user needs the temporary private key to sign the emergency message. So, both AAAHS and the mobile user cannot deny the communication and authentication. We show the non-repudiation proof in Table 1.

Table 1. The non-repudiation proof

Non-repudiation Proof	Issuer	Holder	Non-repudiation Verification
$(ID_{AAAHS}, Sig_1, T_{IDnew}, Lifetime, C_3)$	AAAHS	MU	$V_{puk_{AAAHS}}(Sig_1) \overset{?}{=} (ID_{AAAHS}, T_{IDnew}, Lifetime, C_3)$
$T^{"}_{IDnew}, Lifetime_{new}$	MU	Other MU	$V_{puk_{AAAH}}(Sig_2) \overset{?}{=} (T^{"}_{IDnew}, Lifetime_{new})$
$(Sig_3, M_{POSITION}, M_{ACCIDENT}, Cert_{new})$	MU	Other MU	$V_{temp'_{puk}}(Sig_3) \overset{?}{=} (M_{POSITION}, M_{ACCIDENT}, Cert_{new})$

4.5 Unforgeability

Unforgeability means malicious attackers, or even the mobile user or the service provider cannot fake a legal digital signature. In our scheme, AAAHS issues the authorization certificate to the legal mobile user as follows:

$$Sig_1 = S_{prk_{AAAHS}}[ID_{AAAHS, T_{IDnew}}, Lifetime, C_3] \quad \textbf{(24)}$$

$$Cert = (ID_{AAAHS}, Sig_1, T_{IDnew}, Lifetime, C_3, temp_{prk}) \quad \textbf{(25)}$$

In the authentication phase, the mobile user can use AAAHS's public key to authorize the validity of the certificate. The malicious attacker cannot fake a legal authorization certificate to request service from the service provider or issue a fake emergency notification.

4.6 One-time Session Key Protection

In our scheme, we mainly use the session key $SK_{MU-AAAHS}$ to protect the communication security of the mobile user and AAAHS. In order to communicate with AAAHS, the mobile user must use the session key to encrypt the message. The session key $SK_{MU-AAAHS}$ includes the mobile user's temporary identity T_{ID} and private parameters ($C_1^{'}, C_2^{'}$). So, this one-time session key cannot be used for the next communication.

4.7 Defend Against Attacks

Stolen mobile device attack. In our scheme, if the malicious attacker can get the mobile device, he/she cannot easily get any parameters, even if he/she can access the parameter (F_i, A_i, T_{ID}), he/she cannot use these parameters to derive the mobile user's identity code ID_i and his/her password PW_i because the sensitive information is protected by the one-way hash function.

Fake user attack. In the authentication phase, AAAHS uses the temporary identity to search the related information of the mobile user and computes ($F_i^{'}, A_i^{'}, C_1^{'}, C_2^{'}$) to authorize the validity of the mobile user. If the malicious attacker wants to pass the authentication by faking the legal mobile user, he/she must compute the authentication message (T_{ID}, C_2). The authentication message includes two unknown parameters A_i and $h(Y_i)$, so that the malicious attacker cannot request service or attack the whole system by faking a legal mobile user.

Identity theft attack. During the communication, other legal mobile user, the service provider and AAAHS cannot access the mobile user's real identity. The mobile user always uses the temporary identity T_{ID} to communicate with the service provider or AAAHS. In the registration phase, the mobile user computes parameter A_i rather than real identity ID_i, so that AAAHS will not get his/her real identity code ID_i. Therefore, our scheme can defend against an identity theft attack even if the malicious attacker sabotages the service provider or AAAHS.

Mobile user 'steals server's private key' attack. In our communication system, the mobile user has a temporary identity T_{ID} and parameter F_i, but he/she cannot access AAAHS's sensitive information. Even the mobile user invades AAAHS to get (F_i, G_i, T_{ID}), he/she cannot get AAAHS's private key x which can defend against both inside and outside attack.

Replay attack. Because the session key $SK_{MU-AAAHS}$ includes the mobile user's temporary identity T_{ID} and it will be updated after each authentication, the malicious attacker cannot use the current authentication message (T_{ID}, C_2) to perform the replay attack.

5 Discussions

5.1 Security Features Comparison

According to the security issue, we make a comparison with others' schemes in Table 2. As shown in Table 2, it is clear that our scheme can satisfy all the security requirements and defend against many kinds of attack.

Table 2. The security comparison of related works

	Chen et al. [7]	Tsai et al. [8]	Zhou et al. [9]	Our scheme
Mutual authentication	Yes	Yes	Yes	Yes
Confidential communication	Yes	No	N/A	Yes
User's privacy	Yes	Yes	Yes	Yes
Non-repudiation	N/A	N/A	N/A	Yes
Unforgeability	N/A	N/A	Yes	Yes
One-time session key protection	Yes	No	No	Yes
Stolen mobile device attack	Yes	Yes	N/A	Yes
Fake user attack	Yes	Yes	N/A	Yes
Identity theft attack	Yes	No	Yes	Yes
Mobile user steal server's private key attack	Yes	N/A	Yes	Yes
Replay attack	Yes	Yes	Yes	Yes

5.2 Computational Cost Analysis

In this subsection, we discuss the proposed scheme's computation cost in Table 3. The hash function, symmetric encryption and public key cryptography are used in our scheme.

Table 3. The computation cost of our scheme

Phase Party	Authentication	Request for service	Update certificate from the foreign network	Transfer emergency information	Track malicious behavior
Mobile User	$9T_H + 2T_\oplus + T_S + T_{sign}$	$6T_H + 2T_\oplus + 2T_s$	$7T_H + 2T_\oplus + T_S + T_{sign}$	$2T_S + T_{sign}$	N/A
AAAHF	N/A	N/A	$7T_H + 3T_\oplus + T_S$	N/A	N/A
AAAHS	$T_S + 9T_H + 6T_\oplus + T_S + T_{sign}$	$7T_H + 3T_\oplus + T_S$	$T_H + 3T_\oplus + T_{sign}$	N/A	$T_H + 4T_\oplus$
Network Control Center	N/A	N/A	N/A	$2T_S$	N/A
Service Provider	N/A	$6T_H + T_\oplus + 4T_S$	N/A	N/A	N/A
Other Mobile User	N/A	N/A	N/A	$2T_{sign}$	N/A

Note. T_H: the time to execute a one-way hash function; $T_\oplus$: the time to execute an exclusive OR operation; T_{sign}: the time to execute/verify a signature; T_S: the time to execute a symmetric encryption/decryption operation.

5.3 Communication Cost Analysis

In this subsection, we show the communication cost of the proposed scheme in Table 4. The greatestcommunication cost in our scheme is the track malicious behavior phase:

$T_{sign}{}' + 3T_M + T_{cert} + T_{LICENSE}$=1*1024+3*1024+8192+4096 =16348 bits. The time of transmitting these messages is 45,760/20*10^{-6}=0.32693 ms under the 20 Mbps bandwidth network environment.

Table 4. The communication cost of our scheme

Phase	Communication Cost
Authentication	$T_{ID} + T_H{}' + T_S{}'$
Request for service	$3T_{ID} + 2T_H{}' + T_{NUM} + 4T_S{}'$
Update certificate from the foreign network	$2T_{ID} + 2T_H{}' + T_M + T_{cert} + T_S{}'$
Transfer emergency information	$2T_S{}' + 2T_{sign}{}' + 2T_M + T_{cert}$
Track malicious behavior	$T_{sign}{}' + 3T_M + T_{cert} + T_{LICENSE}$

Note. T_{ID}: the time to transmit the identity (80 bits); $T_H{}'$: the time to transmit the result of one-way hush function (256 bits); $T_S{}'$: the time to transmit a symmetric encryption - ciphertext (256 bits); T_{NUM}: the time to transmit a random number (32 bits); $T_{sign}{}'$: the time to transmit a signature (1024 bits); T_{cert}: the time to transmit a certificate (8192 bits) T_M: the time to transmit an accident/request/location/ position/report message (1024 bits) $T_{LICENSE}$: the time to transmit the digital license (4096 bits).

6 Conclusions

In recent years information technology has developed very rapidly and the usage rate of the Internet has become extremely widespread, VANET is one of these applications. The main application of VANET is to improve road safety and to transmit emergency notification. However, these transmitted emergency messages are also vulnerable to unauthorized access, affect the privacy and security of people. Due to the VANETs' openness, the system needs to face many security risks and privacy problem. To solve these issues, we proposed an emergency notification solution for VANETs based on satellite communication to ensure the security and privacy of the system and the mobile user. The proposed scheme can defend against known attacks (stolen mobile device attack, fake user attack, identity theft attack, stolen private key attack and replay attack). It also provides a mutual authentication via BAN logic proof, confidential communication, non-repudiation, and protect user's privacy. After each party registers into the system, the user's information will be stored in the network control center, the service provider will provide related services to the user and transfer emergency message. The system can also track malicious behaviors and prevent a legal registered mobile user from stealing the network control center's private key to make sure no insider attack possibility. The prosed scheme gives a good solution in emergency status of VANET applications.

Acknowledgements

This research was supported by the Ministry of Science and Technology, Taiwan, R.O.C., under contract number MOST 107-2410-H-165-001.

References

[1] M. Sadek, S. Aissa, Personal Satellite Communication: Technologies and Challenges, *IEEE Wireless Communications*, Vol. 19, No. 6, pp. 28-35, December, 2012.

[2] K. M. Alam, M. Saini, A. E. Saddik, Toward Social Internet of Vehicles: Concept, Architecture, and Applications, *IEEE Access*, Vol. 3, pp. 343-357, March, 2015.

[3] R. G. Song, Advanced Smart Card Based Password Authentication Protocol, *Computer Standards & Interface*, Vol. 32, No. 5-6, pp. 321-325, October, 2010.

[4] H. S. Cruickshank, A Security System for Satellite Networks, *Fifth International Conference on Satellite Systems for Mobile Communications and Navigation*, London, UK, 1996, pp. 187-190.

[5] M. S. Hwang, C. C. Yang, C. Y. Shiu, An Authentication Scheme for Mobile Satellite Communication Systems, *ACM Sigops Operating Systems Review*, Vol. 37, No. 4, pp. 42-47, October, 2003.

[6] T. H. Chen, W. B. Lee, H. B. Chen, A Self-verification Authentication Mechanism for Mobile Satellite Communication Systems, *Computers & Electrical Engineering*, Vol. 35, No. 1, pp. 41-48, January, 2009.

[7] C. L. Chen, K. W. Cheng, Y. L. Chen, An Improvement on the Self-verification Authentication Mechanism for A Mobile Satellite Communication System, *Applied Mathematics & Information Sciences*, Vol. 8, No. 1, pp. 97-106, April, 2014.

[8] J. L. Tsai, N. W. Lo, T. C. Wu, Secure Anonymous Authentication Scheme without Verification Table for Mobile Satellite Communication Systems, *International Journal of Satellite Communications & Networking*, Vol. 32, No. 5, pp. 443-452, November, 2015.

[9] A. Zhou, J. Li, Q. Sun, A Security Authentication Method Based on Trust Evaluation in VANETs, *Eurasip Journal on Wireless Communications & Networking*, Vol. 2015, No. 1, pp. 59, December, 2015.

[10] C. L. Chen, J. Shin,W. J. Tsaur, C. Gong, L. Zhao, A SaaS-Model-Based Approach to An Environment Monitoring System, *the Special Issue of "Emerging Topics in Mobile & Wireless Networks" of Journal of Internet Technology*, Vol. 18, No. 2, pp. 347-359, March, 2017.

[11] R. G. Song, Advanced Smart Card Based Password Authentication Protocol, *Computer Standards & Interface*, Vol. 32, No. 5, pp. 321-325, October, 2010.

[12] C. C. Chang, C. Y. Lee, Y. C. Chiu, Enhanced Authentication Scheme with Anonymity for Roaming Service in Global Mobility Networks, *Computer Communications*, Vol. 32, No. 4, pp. 611-618, March, 2009.

[13] L. Y. Yeh, Y. C. Chen, J. L., Huang, PPACP: A Portable Privacy-preserving Authentication and Access Control

Protocol in Vehicular Ad Hoc Networks, *Computer Communications*, Vol. 34, No. 3, pp. 447-456, March, 2011.

[14] C. C. Lee, Y. M. Lai, P. J. Cheng, An Efficient Multiple Session Key Establishment Scheme for VANET Group Integration, *2015 IEEE Intelligent Vehicles Symposium (IV)*, Seoul, Korea, 2015, pp. 1316-1321.

[15] C. L. Chen, T. F. Shih, K. H. Wang, C. H. Chen, W. J. Tsaur, An Investigator Unearths Illegal Behavior via A Subliminal Channel, *Journal of Internet Technology*, Vol. 19, No. 2, pp. 573-580, March, 2018.

[16] J. Nam, S. M. Kin, S. G. Min, Extended Wireless Mesh Network for VANET with Geographical Routing Protocol, *11th International Conference on Wireless Communications, Networking and Mobile Computing (WiCOM 2015)*, Shanghai, China, 2015, pp. 1-6.

[17] R. V. Alexandrescu, M. C. Surugiu, I. Petrescu, Study on the Implementation of Protocols for Providing Security in Average VANET Intervehiculary Network Communication Systems, *2015 7th International Conference on Electronics, Computers and Artificial Intelligence (ECAI)*, Bucharest, Romania, 2015, pp. 1-6.

[18] C. L. Chen, C. C. Lee, N. C. Wang, C. Y. Hsu, Using a PTD to Strengthen Remote Authentication from an Untrusted Computer, *Journal of Internet Technology*, Vol. 13, No. 5, pp. 725-736, September, 2012.

[19] N. W. Wang, Y. M. Huang, W. M. Chen, A Novel Secure Communication Scheme in Vehicular Ad Hoc Networks, *Computer Communications*, Vol. 31, No. 12, pp. 2827-2837, July, 2008.

[20] T. Fu, Z. Wang, Y. We, A Certificateless Authentication VANET Protocol Based on Non-bilinear Pairings, *Proceedings of the 9th International Symposium on Linear Drives for Industry Applications*, Hangzhou, China, 2013, pp. 681-687.

[21] R. Mishra, A. Singh, R. Kumar, VANET Security: Issues, Challenges and Solutions, *IEEE International Conference on Electrical, Electronics, and Optimization Techniques*, Chennai, India, 2016, pp. 1050-1056.

[22] B. Aslam, P. Wang, C. C. Zou, Extension of Internet Access to VANET via Satellite Receive-only Terminals, *International Journal of Ad Hoc & Ubiquitous Computing*, Vol. 14, No. 3, pp. 172-190, December, 2013.

[23] C. L. Chen, M. S. Lu, J. W. Li, C. Gong, L. Zhao, A Secure Public Transport Multimedia on Demand System for VANET, *Journal of Internet Technology*, Vol. 16, No. 7, pp. 1177-1188, December, 2015.

[24] S. Sharma, A. Kaul, A Survey on Intrusion Detection Systems and Honeypot Based Proactive Security Mechanisms in VANETs and VANET Cloud, *Vehicular Communications*, Vol. 12, pp. 138-164, April, 2018.

[25] Q. G. K. Safi, S. Luo, C. Wei, L. Pan, G. Yan, Cloud-based Security and Privacy-aware Iinformation Dissemination over Ubiquitous VANETs, *Computer Standards & Interfaces*, Vol. 56, pp. 107-115, February, 2018.

[26] J. Kang, D. Lin, W. Jiang, E. Bertino, Highly Efficient Randomized Authentication in VANETs, *Pervasive and Mobile Computing*, Vol. 44, pp. 31-44, February, 2018.

Biographies

Chin-Ling Chen received his Ph.D. from National Chung Hsing University, Taiwan in 2005. From 1979 to 2005, He was a senior engineer at Chunghwa Telecom Co., Ltd. He is a professor. His research interests include cryptography, network security and electronic commerce. He has published over 90 articles in SCI/SSCI international journals.

Jin-Xin Hu received the B.S. degree and M.S. degree in Computer Science from Shenya ng Aerospace University, China, in 2015 and 2018 respectively. Her main research interests include deep learning, network security and cryptography.

Chun-Ta Li received the Ph.D. degree in Computer Science and Engineering from National Chung Hsing University, Taiwan, in 2008. He is currently an Associate Professor with the Department of Information Management at Tainan University of Technology, Taiwan. His research interests include information and network security, wireless sensor networks, mobile computing, and security protocols for RFID, IoTs and cloud computing.

Yong-Yuan Deng is a postdoctoral researcher at the Institute of Information Engineering and Computer Science, Chaoyang University of Technology since 2017. He received his Ph.D. at the Institute of Information Management, Chaoyang University of Technology, Taichung, Taiwan in 2016. His research interests include cryptography, sensor network, mobile commerce and radio frequency identification system.

Shunzhi Zhu is a professor, received the Ph.D. degree in School of Information Science and Engineering from Xiamen University. His research interests include data mining, information recommendation, and privacy protection.