A Secure and Efficient Communication Scheme with Authenticated Key Establishment and Privacy Preserving for Vehicular Ad Hoc Networks*

Chun-Ta Li[†] Min-Shiang Hwang[‡] Yen-Ping Chu[§]

Department of Management Information Systems[‡]
National Chung Hsing University
250 Kuo Kuang Road, Taichung, Taiwan 402, R.O.C.
Email: mshwang@nchu.edu.tw
Fax: 886-4-22857173

Department of Computer Science[†]
National Chung Hsing University
250 Kuo Kuang Road, Taichung, Taiwan 402, R.O.C.

Department of Computer Science and Information Engineering[§]
Tunghai University
181 Section 3, Taichung Harbor Road, Taichung, Taiwan 407, R.O.C.

October 31, 2012

*This work was supported in part by Taiwan Information Security Center (TWISC), National Science Council under the grants NSC95-2218-E-001-001, NSC95-2218-E-011-015, and NSC96-3114-P-001-002-Y.

[‡]Responsible for correspondence: Prof. Min-Shiang Hwang

A Secure and Efficient Communication Scheme with Authenticated Key Establishment and Privacy Preserving for Vehicular Ad Hoc Networks

Abstract

Privacy and security should be paid much more attention in secure vehicular ad hoc networks (VANETs). However, as far as we know, few researches on secure VANET protocols have addressed both the privacy issues and authenticated key establishment. Therefore, in this work, a lightweight authenticated key establishment scheme with privacy preservation to secure the communications between mobile vehicles and roadside infrastructure in a VANET is proposed, which is called SECSPP. Our proposed scheme not only accomplishes vehicle-to-vehicle and vehicle-to-roadside infrastructure authentication and key establishment for communication between members, but also integrates blind signature techniques into the scheme in allowing mobile vehicles to anonymously interact with the services of roadside infrastructure. We also show that our scheme is efficient in its implementation on mobile vehicles in comparison with other related proposals.

Keywords: Cryptography; Key establishment; Mutual authentication; Privacy; Security; Vehicular ad hoc networks

1 Introduction

Vehicular ad hoc networks (VANETs) with interconnected vehicles and numerous services promise superb integration of digital infrastructure into many aspects of our lives, from vehicle to vehicle, roadside devices, base stations, traffic lights and so forth. A network of a huge number of mobile and high-speed vehicles through wireless communication connections has become electronically and technically feasible and been developed for extending traditional traffic controls to brand new traffic services that offer large traffic-related applications. Applications of vehicular ad hoc networks range from rapid transportation development to civil life-support operations such as electronic toll systems, vehicle-collision avoidance, collection of traffic information, vehicle diagnostics, cooperative driving, and entertainment-related applications. In VANETs, the vehicles act as mobile nodes, and self-organized, wireless communications occur with each other directly, by multi-hop communications, and do not rely on a predefined or centralized infrastructure to keep the network connected such as with MANETs (Mobile Ad Hoc Networks) [1, 3, 22, 25, 28, 30]. Some important characteristics need to be considered for VANETs and are quite different from MANETs shown in Table 1. Jungels et al. [21] simply classify the VANET applications into two types, namely: vehicle-to-vehicle communication and vehicle-to-roadside infrastructure communication, respectively. For the former type, vehicles are able to communicate with others in order to receive some valuable traffic information from them, such as roadway conditions, accidents on the road etc. For the latter type, Dotzer et al. [4] further classify it into two communication modes, namely: 1) transmitting messages from fixed roadside nodes to mobile vehicular nodes (i.e. transmission of traffic signals and entertainment services), 2) transmitting messages from mobile vehicular nodes to fixed roadside nodes (i.e. an ambulance can transmit emergency signals to control the destined traffic lights). In this work, we would like to propose a new secure communication scheme and apply it to above-mentioned two situations for VANETs.

Unlike traditionally wired networks are protected by several lines of defense such as firewalls and gateways, security attacks on such wireless networks may come from any direction and target all nodes. Therefore, VANETs are susceptible to intruders ranging from passive eavesdropping to active spamming, tampering, and interfering due to the absence of basic infrastructure and cen-

Table 1: Comparisons of VANETs and MANETs

Characteristics	MANET	VANET
Network topology	random deployment	deployment stands on the direction of the roadway route
Mobility	normal speed (less than 20km/hr)	high speed (more than 40km/hr)
Route direction	from any direction	driving directions (or reverse of driving direction)
Communication models	peer-to-peer	vehicle-to-vehicle vehicle-to-roadside device
Resource constraints	limited computation ability and power	unlimited computation ability and power
Connected range and nodes	small scale and few nodes (10-100 communication nodes)	large scale and many nodes (more than 100 nodes)
Application areas	military, calamity, emergency, and civil environments	traffic safety, traffic control, and electronic toll systems etc.

tralized administration. Moreover, the main challenge facing vehicular ad hoc networks is user privacy. Whenever vehicular nodes attempt to access some services from roadside infrastructure nodes, they want to maintain the necessary privacy without being tracked down for whoever they are, wherever they are and whatever they are doing. It is considered as one of the important security requirements that should be paid more attention for secure VANET schemes, especially in privacy-vital environment. A number of security threats to vehicular ad hoc networks have been addressed [5, 13, 14, 18]. In [19, 20], Raya et al. introduced three kinds of security threats in VANETs, including attacks on safety-related applications, attacks on payment-based applications, and attacks on privacy. They further proposed certain recommended mechanisms to achieve security issues in VANETs. For example, establishing vehicular public key infrastructure, setting up an Event Data Recording (EDR) machine and tamper-proof hardware in vehicles, etc. In [15], Leinm$\ddot{u}$ller et al. proposed some security requirements and two solutions including reactive and proactive security concepts for securing VANETs. In [17], Moustafa et al. developed an AAA (Authentication, Authorization, and Accounting) scheme for vehicular environments by employing EAP-Kerberos and EAP-TLS authentication protocols, however, an on-line centralized authority (CA) is not suitable for VANETs due to the CA being a single point and it is susceptible to damage the security of the entire network whenever it fails or is compromised.

According to the security threats and privacy issues into consideration, our proposed scheme must maintain the following essential requirements:

- Providing mutual authentication between the two communicating parties such as vehicle-to-vehicle and vehicle-to-roadside device.
- Allowing mobile vehicles to anonymously interact with the roadside devices to access the service.
- The system must have light overheads in terms of computational costs and high efficiency.
- Generating dynamic session key to secure the communications between nodes in VANETs.
- Providing data confidentiality and integrity in applications of vehicle-to-vehicle and vehicle-to-roadside device communications;
- Preventing impersonation attacks, that is, no one can impersonate another authorized member to cause service abuse problems and to damage the security of VANETs.
- Preventing eavesdropping, in other words, an intruder cannot discover some valuable information from communications between members in VANETs.

In summary, our proposed scheme has two main advantages that compared with other related schemes: one is that it allows anonymity of the communications between vehicles and roadside infrastructure, and the other one is that it combines the authenticated key establishment into the scheme by using the following cryptographic techniques including non-interactive key agreement, blind signature, one-way hash function and nonces. To the best of our knowledge, this work is the first attempt to provide a secure communications model with mutual authentication, key establishment protocol, and privacy preservation in vehicular ad hoc networks.

The rest of this article is organized as follows. In Section 2, we describe some basic preliminaries of our scheme. In Section 3 we present our secure communication scheme for VANETs, followed by the security analysis and performance evaluation in Section 4. Finally, we conclude this article in Section 5.

2 Preliminaries

As a preliminary, we used some cryptographic techniques and basic tools in our scheme. The security of our scheme is based on non-interactive ID-based public-key cryptography, blind signature [9, 10], and one-way hash chain. A brief review of three techniques is provided as follows.

2.1 Non-Interactive ID-Based Public Key Cryptography

To date, a number of non-interactive ID-based public-key schemes have been proposed [12, 16, 27] and the security of these schemes is based on the hardness of factorization of the composite primes. Normally, it consists of three phases, namely: system setup phase, user registration phase and authentication phase, respectively. In the following, we briefly describe each of them in detail.

System setup phase: In this phase, there exists a trusted authority TA which is responsible for choosing four primes p_j such that $(p_j\text{-}1)/2$ are odd and pairwise relatively prime and let $N = p_1 * p_2 * p_3 * p_4$, where $j = 1, 2, 3, 4$. The TA then selects a public key e in $Z^*_{\phi(N)}$ and computes a corresponding private key d such that $e * d \equiv 1(\bmod \phi(N))$, where $\phi(.)$ is the Euler's totient function.

User registration phase: In this phase, both the TA and users are communicated through a secret channel. Whenever a user U_i with his/her identity ID_i wants to join the system, TA computes a secret key $s_i = e{*}log_g(ID_i^2)(\bmod \phi(N))$ for U_i, where g is a primitive element in $GF(p_j)$. Finally, the secret information including four primes p_j and d are kept secret in the TA and the secret key s_i is also kept secret in U_i. Moreover, the public information including N, g, e, and the public key of U_i, that is, ID_i, are known to everyone.

Authentication phase: Whenever a user U_i wants to join the network, he/she must prove his/her identity to a verifier U_j. The detailed authentication procedure is described as follows. U_i first sends his ID_i to the verifier U_j, then U_j computes $X = (ID_j^2)^r(\text{mod}N)$ and sends it to U_i, where r is a random number in Z_N^*. Upon receiving X sent by U_j, U_i computes $Y = X^{s_i}(\text{mod}N)$ and sends it to U_j, where s_i is U_i's secret key. Upon receiving Y sent by U_i, the verifier U_j computes $(ID_i^2)^{r*s_j}(\bmod N)$ and verifies whether $Y = (ID_i^2)^{r*s_j} = (ID_j^2)^{r*s_i}(\text{mod}N)$ holds or not. If it holds, U_j is convinced that U_i's identity ID_i is legal; otherwise, U_j terminates the connection.

2.2 Blind Signature

In Chum's blind signature scheme [2], there are two main participants, namely: the user and the signer, respectively. The user first generates a message m and the signer will generate the digital signature on message m for the user by using signer's private key and the signer will be unable to know the content of signed message and it can be implemented based on existing well-known digital signature schemes, such as RSA [23] and the ElGamal scheme [6]. The user first blinds the message m with a random blind factor r and computes the blinded message $C = r^e m$ and sends C to the signer, where e is signer's public key. Upon receiving the blinded message C sent by the user, the signer signs the message C with his/her private key d and computes $C' = C^d = rm^d$. Then, signer sends the result C' back to the user. Upon receiving the message C' sent by the signer, the user un-blinds it to get the signer's signature on the message by computing $C" = C'/r = m^d$. Finally, the user can verify the integrity of $C"$ by computing $V = C"^e$ and checks whether $V = m$ holds or not. If it holds, the user is convinced that he/she has obtained the signer's signature on the message; otherwise, drop it and stop.

The blind signature technique has been confirmed to ensure non-linkability that prevents the signer from linking a blinded message he/she signed to an un-blinded message and it can be useful in our scheme for fulfilling the user privacy requirement.

2.3 One-Way Hash Chain

One-way hash functions are important tools in the field of cryptographic applications due to their efficiency with regard to computational costs and are suitable for resource-constrained devices [11, 26]. In addition, the security of an one-way hash function $h(.)$ is based on the hardness of inverting the inputs from the outputs; that is, given a and $h(.)$, it is easy to compute $h(a) = b$. However, only given b, it is hard to find a, satisfying $h(a) = b$.

Figure 1 shows the construction of an one-way hash chain. First, we generate an initial value $h^1(m) = h(m)$, where m is a message and $h^1(m)$ represents the message m has been hashed once. Thus, h^n can be regarded as the message m which has been hashed n times such that $h^n(m) = h(h^{n-1}(m))$, where $n = 2, 3, 4, \ldots$. Due to the one-way property, the hash chain can be used in reverse order of generation for authentication; that is, $h^{n-1}(m)$ can be proven to be authentic if $h^n(m)$ has been proven to be authentic. In our scheme, the

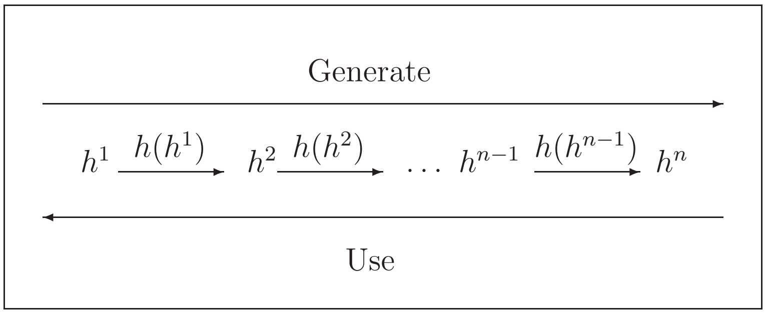

Figure 1: Construction of an one-way hash chain

concept of one-way hash chain would be used to authenticate messages and details of the proposed scheme will be briefly described in next section.

3 The Proposed Scheme

In the proposed scheme, a sample system architecture for a VANET is given in Figure 2. In general, a VANET consists of two types of entities, namely: mobile vehicles and roadside devices, and the proposed scheme would focus on two types of communications in VANETs, namely: vehicle-to-vehicle communication and vehicle-to-roadside device communication. In vehicle-to-vehicle communication scenario (depicted in dotted line), all messages transmitted between vehicles should be verified and protected in the scheme. Therefore, even if an intruder eavesdrops on the communications between vehicles or injects false messages into networks, the scheme can still provide an adequate level of security. Furthermore, in a vehicle-to-roadside device communication scenario (depicted in solid line), an ambulance can send an emergency signal to control the traffic lights on its intended path or a mobile vehicle can safely receive different kinds of entertainment services (such as on-line movies) he/she is authorized to in VANETs anytime from anywhere. However, the method of securely transmitting messages and accessing services with privacy preservation in public environments using vehicle ad hoc wireless networks is challenging. In the following discussion, we present a non-interactive ID-based scheme for vehicle-to-vehicle communications that uses member's ID to establish a secure trust relationship between communicating vehicles and a blind signature-based scheme for vehicle-to-roadside device communication that allows authorized vehicles to anonymously interact with the services from roadside devices without disclosing any of his/her contextual information such as location, user identity etc. Notations used throughout this article are summarized in Table 2 and the details of the proposed scheme are briefly described as follows.

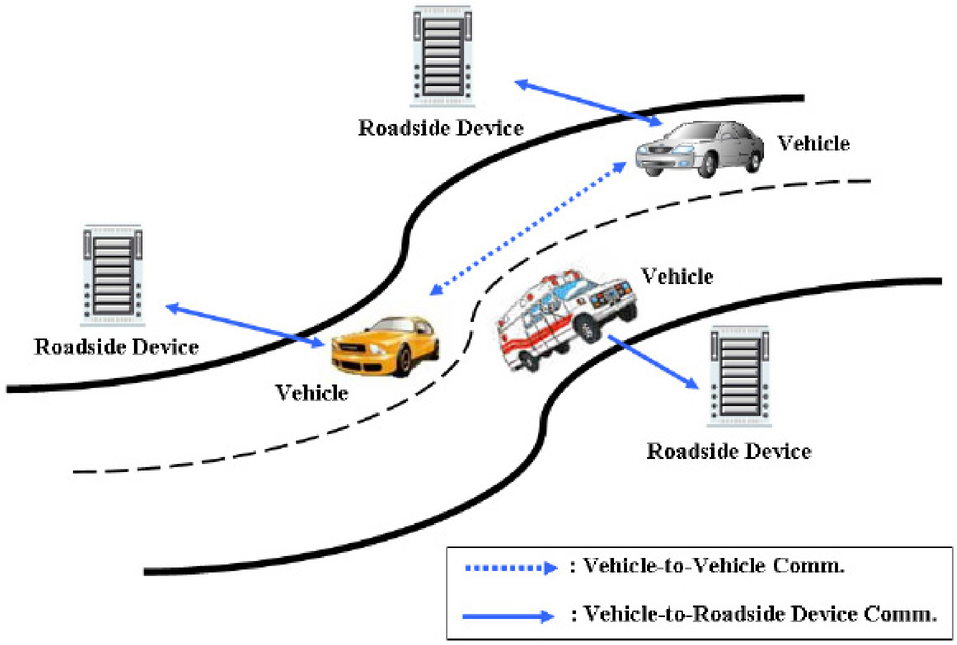

Figure 2: Sample VANET

3.1 Predeployment Phase

Before a vehicular ad hoc network is deployed, we needs the aid of a trusted third party TTP only at the initial network formation. Consider the scenario that a vehicular node wants to be able to dynamically access available services in VANETs. Due to such wireless communication channels in VANETs are more vulnerable to security threats, the authorization of the vehicular node to the particular services he/she requests should be verified. As a result,

Table 2: Notations used through the proposed scheme

VID_i	The identity of vehicular node i.
RID_i	The identity of roadside device node i.
S_i	Service provider.
(PK_{S_i}, SK_{S_i})	A public key and private key of service provider S_i.
$tag\#$	An unique tag number for a request.
hop	The number of hops that a message can transmit.
r_l	The identity of roadway section.
ES_i	An emergency signal, which node i issues.
MAC	The message authentication code and is defined by $MAC = H(K; m)$, where m denotes the message under the protection key of K.
M_i	The receipt of the service access for a user i to register himself as a legal user of destined service that S_i provides.
$H(.)$	A collision-free and public one-way hash function.
$\oplus$	Exclusive OR operation.
$H(SK)$	The group secret key shared among all nodes in the network.
T_i	A timestamp, which node i attaches.
$a\|\|b$	Concatenation of message a and b.
$E_{PK_{S_i}}\{.\}$	The asymmetric encryption function with service provider's PK_{S_i}.
$D_{SK_{S_i}}\{.\}$	The asymmetric decryption function with service provider's SK_{S_i}.

in our proposed scheme, the vehicular node and the service provider need to authenticate each other first and this is done through some out-of-band non-cryptographic technique. For ensuring secure communications in such networks, TTP is used for generating the necessary information for vehicular nodes and the service providers to form a secure VANET environment. The TTP first chooses a set of network parameters, including four primes p_j such that (p_j-1)/2 are odd and pairwise relatively prime and let $N = p_1 * p_2 * p_3 * p_4$, where $j = 1, 2, 3, 4$; the TTP's public key $e \in Z^*_{\phi(N)}$; the TTP's private key d such that $ed \equiv 1(\text{mod}\phi(N))$, and a primitive element g in $GF(p_j)$; r_l, which is the identity of the roadway section and $l = 1$ to n if there are n sections of the roadway; an initial group secret key $H(SK)$ and a hash chain message $H^t(SK)$, where the length t could be adjusted to the proper value depending on the actual frequency of usage (i.e. according to the months in a year, the length of t would be set to 12). In addition, the TTP never shares its private key d with anyone else and it does not get involved in the following network operations. Thus, attackers are unable to attack the TTP to get d.

3.1.1 Handling New Vehicles

For each new vehicular node, when vehicle V_i wants to join in the network, V_i will perform the following phase with TTP. First, V_i must personally go to registration center and provide his/her identification information to the center for registration. Then, the TTP of the registration center presets a set of node parameters and sends them to V_i through a secret channel, including V_i's identity VID_i; the identity of the roadway section r_l; the group's secret key $H^t(SK)$ shared among all nodes in the network; V_i's secret key $VK_i = e * log_g(VID_i^2)(\text{mod}\phi(N))$, where $H(.)$, N, e and g are public parameters. It should be noted that a secret key for a destined node is protected by itself and it never reveals its secret key with anyone else. Similarly, the group secret key $H^t(SK)$ is undisclosed to outsiders that have not participated in a VANET.

3.1.2 Handling New Roadside Devices

In the scheme, new roadside devices can deploy in the network while some roadside devices may leave the network. When a new node of roadside device R_i joins the network, TTP computes a set of node parameters, including R_i's identity RID_i; the identity of the roadway location r_l; the initial group secret key $H^1(SK)$ and the length of t; and a secret key $RK_i = e * log_g(RID_i^2)(\text{mod } \phi(N))$. Thereupon, TTP sends them secretly to the involved roadside device R_i in the network through a secret channel.

3.1.3 Handling New Service Providers

In case a new service provider S_i joins the network, TTP not only issues $(SID_i, H^t(SK), r_l, SPK_{S_i} = e * log_g(SID_{S_i}^2)(\text{mod}\phi(N)))$ but also generates an asymmetric public/private key (PK_{S_i}, SK_{S_i}) to them. The asymmetric public/private key pair would be used in the blind signature technique to ensure inability to link between V_i and S_i in Scenario 3 of the proposed scheme.

3.2 Scenario 1: Secure Communications between Vehicles

In this scenario, when a source vehicular node wants to transmit some confidential messages to a destination vehicular node, in order to protect the network communications between source vehicle to destination vehicle from external or internal security attacks, it must provide a secure vehicle-to-vehicle communication scheme with mutual authentication for applying such security system in this scenario. Based on non-interactive ID-based public key cryptography, we denoted the source vehicular node as V_s and the destination vehicular node as V_d. The secure communication mechanism with mutual authentication between the node V_s and V_d is performed in the following steps and shown in Figure 3.

Step 1: As the data transmission request is originated, the source vehicular node V_s initiates a route discovery process to establish a route and a session key $K_{s,d}$ with the destination node V_d through a number of intermediate vehicular nodes. Thus, V_s first generates a unique $tag\#$ and a random number a for this request.

Step 2: Then, V_s computes $C = (VID_d^2)^{H(T_{V_s}||r_l)*VK_s} (\bmod N)$ and $C\oplus$ $(tag\#$ $||\ VID_s||VID_d||T_{V_s}||a)$, where VK_s is V_s's secret key and T_{V_s} is a timestamp generated by V_s.

Step 3: V_s broadcasts the route discovery message $H^t(SK) \oplus (tag\#, VID_s,$ $VID_d,\ hop,\ T_{V_s},\ r_l, C \oplus (tag\#||VID_s||VID_d||T_{V_s}||a))$ to all vehicular nodes within its wireless transmission range, where the route discovery message is encrypted by the group key $H^t(SK)$ which is shared among all nodes in the network.

Step 4: When a vehicular node receives the message, it decrypts the message $(tag\#, VID_s, VID_d, hop, T_{V_s}, r_l, C \oplus (tag\#||VID_s||VID_d||T_{V_s}||a))$ by computing $H^t(SK) \oplus (tag\#, VID_s, VID_d, hop, T_{V_s}, r_l,\ C\ \oplus\ (tag\#$ $||\ VID_s\ ||VID_d||T_{V_s}||a)) \oplus H^t(SK)$ and checks if $((hop - -) \geq 0)$, if it does not hold, then the system drops it and stops; otherwise, it checks whether the node itself is the destination vehicular node or not. If it does not hold, it forwards the route discovery packet $H^t(SK) \oplus$ $(tag\#, VID_s, VID_d, hop-1, T_{V_s},\ r_l,\ C \oplus (tag\#\ ||\ VID_s\ ||VID_d||T_{V_s}||a))$ to its neighboring nodes within its wireless transmission range; otherwise, the vehicular node is the destination node V_d and it can computes $C' = (VID_s^2)^{H(T_{V_s}||r_l)*VK_d} (\mathrm{mod} N)$ and decrypts the message $C \oplus$ $(tag\#||VID_s||VID_d||T_{V_s}||a)$ by computing $C \oplus (tag\#\ ||\ VID_s\ ||\ VID_d$ $||\ T_{V_s}||a) \oplus C'$ to recover the message $(tag\#||VID_s||VID_d||T_{V_s}||a)$.

Step 5: After V_d has verified the route discovery message, V_d should respond to the source node V_s. V_d selects a random number b and computes the session key $K_{d,s}$ as $K_{s,d} = H(a||b||0)$.

Step 6: Then, V_d sends $H^t(SK) \oplus (tag\#, VID_d, VID_s, hop, T_{V_d}, r_l, C' \oplus (tag\# || VID_d ||VID_s||T_{V_d}||r_l||b||MAC))$ to V_s, where $MAC = H(K_{d,s}; a+1)$ and T_{V_d} is a timestamp generated by V_d.

Step 7: After receiving the response message sent by V_d, V_s first decrypts it by using the keys $H^t(SK)$ and C to recover $(tag\#||VID_d||VID_s||T_{V_d}||r_l || b || MAC)$. Then, V_s can compute the common session key $K_{s,d} = H(a||b||0)$ and verifies the validity of the MAC. If the above holds, the pairwise session keys obtained by V_s and V_d are equal because $K_{s,d} = H(a||b||0) = K_{d,s}$. Finally, V_s and V_d can securely interact with each other by using the pairwise session key $K_{s,d} = H(a||b||i)$, where $i = 1, 2, 3, \ldots$. for securing follow-up interactions between V_s and V_d.

3.3 Scenario 2: Secure Communications between Vehicles and Roadside Devices

Communications in this scenario can be roughly classified into two communication models in VANETs, one being vehicle-to-roadside device communications (for example, a vehicle may send a message to a roadside device to inquire on the trafficability of some area; or a vehicle can send the e-toll for roadside electronic systems) and another one being roadside device-to-vehicle communications (for example, the roadside devices may periodically send the traffic information to vehicles in real time or update the group secret key $H(SK)$ shared among all nodes in the network). Since malicious attackers may attempt to improperly inject false messages, replicate or modify messages to upset the traffic in the networks. To prevent such attacks and ensure secure communication between nodes, networks must provide a mechanism to identify nodes and establish secure relationships among the nodes in VANETS. The detailed steps of above-mentioned two communication models of Scenario

2 are described in the following subsections.

3.3.1 Vehicle-to-Roadside Device Communications

When mobile vehicles join the VANETs and access public services, computing is enabled anytime and from anywhere. Let us consider the following example. It is expected for an urgent task that an ambulance V_i can transmit an emergency signal ES_{V_i} to a roadside device R_j for the purpose of controlling the destined traffic lights on its driving route. However, malicious vehicles may selfishly abuse this service while in a traffic jam. Motivated by the above mentioned, we provide a solution according to the need for a secure communication scheme with mutual authentication for providing reliable services in this model for which detailed steps are shown as follows.

Step 1: V_i generates a random number a and computes $C = (RID_j^2)^{H(T_{V_i}||r_l)*VK_i} \bmod N$, where RID_j is R_j's identity and VK_i is V_i's secret key.

Step 2: Then, V_i sends $H^t(SK) \oplus (ES_i, VID_i, RID_j, T_{V_i}, r_l, C \oplus (ES_i||\, VID_i \,||\, RID_j||T_{V_i}||a))$ to R_j, where ES_i is an emergency signal, which is issued by node V_i.

Step 3: Upon receiving $H^t(SK)\oplus(ES_i, VID_i, RID_j, T_{V_i}, r_l, C\oplus(ES_i||VID_i||RID_j||T_{V_i}||a))$ from V_i, R_j decrypts it with key $H^t(SK)$ by computing $H^t(SK) \oplus (ES_i, VID_i, RID_j, T_{V_i}, r_l, C \oplus (ES_i||VID_i||RID_j||T_{V_i}||a)) \oplus H^t(SK)$ to recover $(ES_i, VID_i, RID_j, T_{V_i}, r_l, C\oplus(ES_i||VID_i||RID_j||T_{V_i}||a))$. Then, R_j checks the validity of VID_i. If the authority of VID_i is correct, R_j computes $C' = (VID_i^2)^{H(T_{V_i}||r_l)*RK_j} (\bmod N)$ to decrypt $C\oplus(ES_i||VID_i||RID_j||T_{V_i}||a)$ to reveal $(ES_i||VID_i||RID_j||T_{V_i}||a)$ by computing $C\oplus(ES_i||VID_i||RID_j||T_{V_i}||a)\oplus C'$.

Step 4: If above messages are valid, and in order to achieve mutual authentication and establish a session key between two communication parties,

R_j generates a random number b and computes the pairwise session key $K_{i,j} = H(a||b||0)$. Then, R_j sends $H^t(SK) \oplus (ES_i, RID_j, VID_i, T_{R_j}, r_l, C' \oplus (ES_i||RID_j||VID_i||T_{R_j}||r_l||b||MAC))$ to V_i, where the $MAC = H(K_{i,j}; a+1)$.

Step 5: Finally, V_i can decrypt the message with the key $H^t(SK)$ and C to reveal $(ES_i||RID_j||VID_i||T_{R_j}||r_l||b||MAC)$ and compute the pairwise session key $K_{i,j} = H(a||b||0)$ to verify the validity of the MAC. If it holds, mutual authentication and session key establishment are accomplished between nodes V_i and R_j; otherwise, communication is stopped.

For applications used in electronic toll systems and traffic flow inquiries, the communication procedure steps are similar to the above proposed scheme and can be directly applied on condition that the vehicular node only needs to replace ES_i with e-toll data (or inquiry requests) in Step 2. Due to the space limitations, remaining steps may be deduced by analogy to simplify the exposition of the procedure.

3.3.2 Roadside Device-to-Vehicle Communications

For applications of roadside devices R_j may periodically send traffic information to vehicles V_i in real time or update the hashed secret key $H^t(SK)$ shared among all nodes in the network, R_j must securely send messages to V_i with some security mechanism in order to withstand malicious outsiders from attacks in this scenario. It is assumed that at this point, involved roadside devices are trusted and non-compromised nodes. Below, we consider an example of updating a group secret key $H^t(SK)$ for the design scheme and detailed steps in the scheme are shown as follows:

Step 1: Assuming that there are m R_js and $H^t(SK)$ is a recent group key shared among all nodes in the network, where $j = 1, 2, 3, \ldots, m$. While a request for updating the group key is required, R_j must notify all the nodes of V_i to replace the recent group key $H^t(SK)$ with $H^{t-1}(SK)$. Since every R_j has an initial group key $H^1(SK)$, it can correctly compute the latest group key $H^{t-1}(SK)$ by hashing $H^1(SK)$ for $t-1$ times. As a result, every R_j generates its own $nonce_j$ and broadcasts the message $H^t(SK) \oplus (Update\_Group\_Key, H^{t-1}(SK), RID_j, r_l, T_{R_j}, nonce_j)$ to all nodes V_i within its wireless transmission range.

Step 2: After receiving the message in Step 1, V_i decrypts the message by computing $H^t(SK) \oplus (Update\_Group\_Key, H^{t-1}(SK), RID_j, r_l, T_{R_j}, nonce_j) \oplus H^t(SK)$ and checking whether $H(H^{t-1}(SK)) = H^t(SK)$ holds or not. If the aforesaid holds, V_i replaces the group key $H^t(SK)$ with $H^{t-1}(SK)$; otherwise, it drops it. Moreover, because of the shared goal of mutual authentication, V_i answers $H^{t-1}(SK) \oplus (VID_i, T_{V_i}, r_l, nonce_j + 1)$ to R_j.

Step 3: Upon receiving the message $H^{t-1}(SK) \oplus (VID_i, T_{V_i}, r_l, nonce_j + 1)$ sent by V_i, R_j reveals $(VID_i, T_{V_i}, r_l, nonce_j+1)$ by computing $H^{t-1}(SK) \oplus (VID_i, T_{V_i}, r_l, nonce_j + 1) \oplus H^{t-1}(SK)$ and becomes convinced that V_i has updated its group key already.

Similarly, for applications of roadside devices R_j may periodically send traffic information to vehicles V_i in real time. The roadside device node only needs to replace $Update\_Group\_Key$ with $Traffic\_Information$ in Step 1. Due to the space limitations, the remaining steps may be deduced by analogy to simplify the exposition of the procedure.

3.4 Scenario 3: A Secure and Efficient Communication Scheme with Privacy Preservation (SECSPP)

A secure and efficient communication scheme implementing privacy preservation (SECSPP) for vehicles to anonymously interact with services encompassing three participants, namely: the vehicular node V_i, the service provider S_i, and the roadside device R_j, respectively. In addition, the scheme consists of

Vehicular user V_i Service provider S_i

1. Compute $AC_i = H(M_i||VID_i||a_1)$

2. Send $(VID_i, SID_i, T_{V_i}, C \oplus (VID_i||SID_i||AC_i'||M_i||T_{V_i}))$

$\longrightarrow$

3. Compute

$C \oplus (VID_i||SID_i||AC_i'||M_i||T_{V_i}) \oplus C'$

$AC_i'' = AC_i'^{SK_{S_i}} = a_2 * AC_i^{SK_{S_i}}$

Mark M_i non-fresh

$C' \oplus (SID_i||VID_i||AC_i''||T_{S_i})$

$\longleftarrow$

4. Compute

$C' \oplus (SID_i||VID_i||AC_i''||T_{S_i}) \oplus C$

$AS_i''/a_2 = AC_i^* = AC_i^{SK_{S_i}}$

Figure 3: Access authorization phase in Scenario 3 of the proposed scheme

two phases in this scenario, namely: access authorization phase and an access service phase. We assumed that V_i has registered and paid the service money to S_i and it has allowed V_i to access the desired services from R_j. Then, S will send a receipt M_i to V_i via a secure channel.

In Figure 3, when V_i wants to anonymously access pay-services from R_j, V_i must get an authorized credential AC_i from S_i by presenting the receipt M_i in the access authorization phase. V_i then uses the authorized credential to access the pay-services without disclosing any information about V_i such as location or personal information. This is done through the access service phase and shown in Figure 4. In order to ensure anonymous communication, we assumed that V_i can manipulate the source addresses of the outgoing Medium Access Control (MAC) frames and the detailed method for implementing this can be found in [7] which is omitted here due exceeding the scope of this article. Detailed steps for the SECSPP are described as follows:

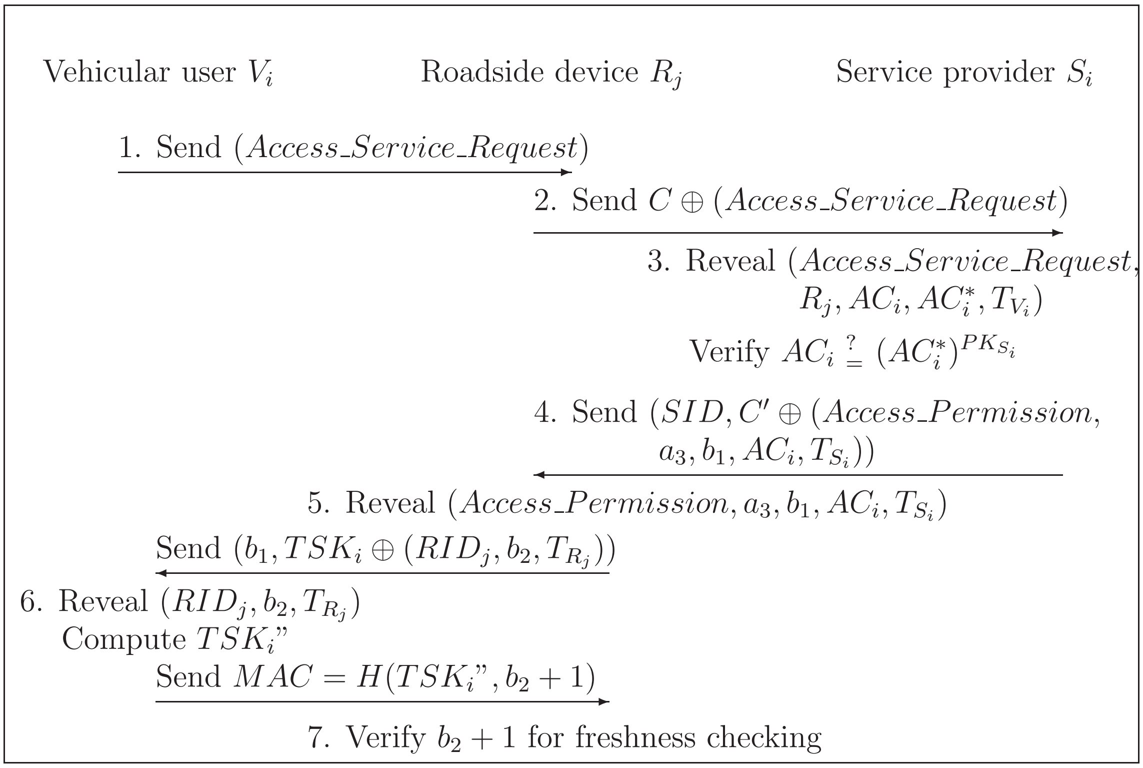

Figure 4: Access service phase in Scenario 3 of the proposed scheme

1. Access Authorization Phase:

Step 1: The mobile vehicular node V_i needs to register itself as a legal user of the desired service and V_i bearing a receipt M_i has only one opportunity to ask the service provider S_i to run the following steps to acquire the authorized credential AC_i. First, V_i selects a random number a_1 and computes the authorized credential AC_i as $AC_i = H(M_i||VID_i||a_1)$.

Step 2: Then, V_i selects a blind factor a_2 to blind AC_i as $AC_i' = a_2^{PK_{S_i}} * AC_i$, where PK_{S_i} is S_i's public key and sends out $(VID_i, SID_i, T_{V_i}, C \oplus (VID_i||SID_i||AC_i'||M_i||T_{V_i}))$ to S_i, where SID_i is S_i's identity and $C = (SID_i^2)^{H(T_{V_i}) * VK_i} (\mathrm{mod} N)$.

Step 3: Upon receiving $(VID_i, SID_i, T_{V_i}, C \oplus (VID_i||SID_i||AC_i'||M_i||T_{V_i}))$ sent out by V_i, S_i reveals $(VID_i||SID_i||AC_i'||M_i||T_{V_i})$ by computing $C \oplus (VID_i||SID_i||AC_i'||M_i||T_{V_i}) \oplus C'$ and verifies the validity of M_i, where $C' = (VID_i^2)^{H(T_{V_i})*SPK_{S_i}}(\mathrm{mod}N)$. If it holds, S_i will record (VID_i, M_i, T_{V_i}) in its DB and marks M_i as non-fresh, and then signs AC_i' with its private key SK_{S_i} by computing $AC_i” = AC_i'^{SK_{S_i}} = a_2 * AC_i^{SK_{S_i}}$ and $C' \oplus (SID_i||VID_i||AC_i”||T_{S_i})$ which is then sent back to V_i.

Step 4: After V_i has received $C' \oplus (SID_i||VID_i||AC_i”||T_{S_i})$, it computes reveals $(SID_i||VID_i||AC_i”||T_{S_i})$ by computing $C' \oplus (SID_i||VID_i||AC_i”||T_{S_i}) \oplus C$. Finally, $AC_i”$ can be unblinded by computing $AC_i”/a_2$ and V_i can obtain $AC_i^* = AC_i'^{SK_{S_i}}$. To confirm that AC_i is certified, V_i can verify the validity of authorized credential by checking whether $AC_i = (AC_i^*)^{PK_{S_i}}$ holds or not. If it holds, V_i holds a authorized credential AC_i and its signature AC_i^*; otherwise, drop it and stop.

2. Access Service Phase:

Step 1: When a legal user V_i wants to access the pay-service from the roadside device R_j, V_i sends a service request messages $Access\_Service\_Request$ and $E_{PK_{S_i}}\{Access\_Service\_Request, RID_j, AC_i, AC_i^*, T_{V_i}, a_3\}$ to R_j, where a_3 is a random number generated by V_i.

Step 2: When R_j receives service request messages, it has no responsibility for user authentication and forwards $(RID_j, T_{R_j}, C \oplus (E_{PK_{S_i}}\{Access\_Service\_Requ$ to its back-end service provider S_i, where $C = (SID_i^2)^{H(T_{R_j})*RK_j}(\bmod N)$.

Step 3: Upon receiving the messages, S_i computes $C' = (RID_j^2)^{H(T_{R_j})*SPK_{S_i}}(\bmod N)$ and $C \oplus (E_{PK_{S_i}}\{Access\_Service\_Request, RID_j, AC_i, AC_i^*, T_{V_i}, a_3\}) \oplus C'$ to reveal $E_{PK_{S_i}}\{Access\_Service\_Request, RID_j, AC_i, AC_i^*, T_{V_i}, a_3\}$. Furthermore, S_i reveals $(Access\_Service\_Request, RID_j, AC_i, AC_i^*, T_{V_i})$ by computing $D_{SK_{S_i}}\{E_{PK_{S_i}}\{Access\_Service\_Request, RID_j, AC_i, AC_i^*, T_{V_i}\}\}$

and verifies the validity of authorized credential by checking whether $AC_i = (AC_i^*)^{PK_{S_i}}$ holds or not. If it holds, V_i is granted to access pay-services from R_j; otherwise, the access request is denied.

Step 4: S_i generates a random b_1 and computes the temporary service key TSK_i as $TSK_i = H(a_3||b_1||AC_i||0)$. Then, S_i sends $(SID_i, C' \oplus (Access\_Service\_Permission, a_3, b_1, AC_i, T_{S_i}))$ to R_j.

Step 5: Upon receiving the messages, R_j reveals $(Access\_Service\_Permission, a_3, b_1, AC_i, T_{S_i})$ by computing $C' \oplus (Access\_Service\_Permission, a_3, b_1, AC_i, T_{S_i}) \oplus C$, where $C = (SID_i^2)^{H(T_{R_j})*RK_j}(\mathrm{mod}N)$. Then, R_j can also compute the temporary service key TSK_i and TSK_i can be used for securing the following data traffic for accessing pay-services between V_i and R_j. In order to achieve mutual authentication with V_i, R_j then generates a random number b_2 and sends $(b_1, TSK_i \oplus (RID_j, b_2, T_{R_j}))$ to V_i.

Step 6: Upon receiving the messages, V_i can compute $TSK_i' = H(a_3||b_1||AC_i||0)$ and reveal (RID_j, b_2, T_{R_j}) by computing $TSK_i \oplus (RID_j, b_2, TR_j) \oplus TSK_i'$. Also, for the purpose of mutual authentication with R_j, V_i sends $MAC = H(TSK_i", b_2{+}1)$ to R_j, where $TSK_i" = H(a_3||b_1||AC_i||1)$.

Step 7: When R_j receives the message MAC, R_j verifies it and is then convinced that V_i is a legal user for purposes of accessing the pay-service when the value $b_2 + 1$ is replied; otherwise, the procedure is stopped. Finally, V_i and R_j can use $TSK_i = H(a_3||b_1||AC_i||k)$ for securing the following data traffic in the access service phase, where $k = 2, 3, 4, \ldots$.

4 Discussions

In this section, we shall analyze the essential requirements and the security aspects of our scheme. Furthermore, we shall evaluate and compare the performance of our scheme with other related works in terms of computational costs. The details of the above-mentioned analysis are briefly described in the following subsections.

4.1 Security Analysis

In the following, we will provide proof of the requirements presented in Section 1 and our SECSPP scheme should satisfy the following theorems.

Theorem 4.1. *SECSPP is secured against eavesdropping and impersonating attacks and maintains data confidentiality of the nodes that participants in VANETs including vehicular users, roadside devices, and the service providers.*

Proof. During the authorization access phase, a vehicular node V_i sends the authorized credential message to its service provider S_i and the message is encrypted with the common secret key $C = (SID_i^2)^{H(T_{V_i})*VK_i}(\text{mod}N)$ that is shared only between the vehicular node and the service provider. Thus, starting from the vehicular node, only the service provider can derive the common secret key $C' = (VID_i^2)^{H(T_{V_i})*SPK_{S_i}}(\text{mod}N)$ to decrypt the message and the security of the secret key can be provided based on non-interactive ID-based public key cryptography. By expanding on C and C', we learn that $C = (SID_i^2)^{H(T_{V_i})*VK_i}(\text{mod}N) = (VID_i^2)^{H(T_{V_i})*SPK_{S_i}}(\text{mod}N) = C'$ if VK_i is the correct secret key of V_i issued by TTP at the pre-deployment phase. As a result, S_i can authenticate the validity of V_i, and vice versa. Hence, the data confidentiality and integrity are well protected under the proposed scheme to prevent security attacks such as eavesdropping. Moreover, for impersonating attacks, the attacker might intercept the authorized credential message and then replay it again. However, these attacks can be prevented with the technique of timestamps whereby the timestamps are used in our scheme to guarantee the freshness of transmission messages. In addition, there is only one opportunity for vehicular users to ask the service provider to run the authorized access procedure. When the service provider sends AC_i" back to the user, the M_i would be marked as not fresh and there is subsequently no way for attackers to use the same M_i to request the authorized credential. As a result, service abuse and double spending problems can be avoided in this phase.

During the access service phase, an authorized user would send the access service request to the service provider to request service through the roadside device. The access service requested is protected by service provider's public key and only the service provider can use the corresponding private key to decrypt the message to get AC_i, AC_i^* and T_{V_i}, where T_{V_i} is used to prevent replaying attacks and AC_i and AC_i^* are used to identify whether the authorized credential is valid or not. No one has the ability to acquire and derive the user's authorized credential and all the subsequent interactions between participants involved are well protected by the temporary service keys TSK_i. Therefore, some passive and active attacks can be prevented in the SECSPP. □

Theorem 4.2. *SECSPP maintains and ensures anonymous communication for authorized vehicular users and neither the service provider nor outsiders can ascribe any session to a particular user when the user accesses the service from the service provider.*

Proof. During the authorization access phase, a user's VID_i and M_i are hashed together with a random number a_1 to form a authorized credential AC_i and the user's identity is protected based on the security of the one-way hash functions in Step 1. In Step 2, based on the technique of using blind signatures, a blind factor a_2 is used to protect AC_i, and thus the service provider is unable to link it to a specific user. In Step 4, after a user receives the $AC_i" = a_2 * AC_i^{SK_{S_i}}$, he/she computes $AC_i"/a_2 = AC_i^* = AC_i^{SK_{S_i}}$ and verifies whether AC_i is equal to $AC_i^{*PK_{S_i}}$. If so, the user believes that he/she holds an authorized credential AC_i and its signature AC_i^*.

During the access service phase, when a user sends a service request $E_{PK_{S_i}}\{Access\_Service\_Requ$

to the service provider, only the service provider can decrypt the message and outsiders can know the content of authorized credentials AC_i and AC_i^* in Step 3. Furthermore, if the same user sends two different service requests, due to encrypted service requests containing a different T_{V_i}, outsiders cannot ascribe two sessions to the same user except for the service provider. However, based on the security of using blind signature techniques, the service provider has no way to link an authorized credential to a specific user. As a result, authorized vehicular users can anonymously interact with the service provider without disclosing their personal information and the integral property of user privacy is achieved for the VANETs in our proposed SECSPP. □

Theorem 4.3. *SECSPP is able to provide mutual authentication and dynamic session key between two communication nodes in VANETs.*

Proof. Let A and B are two communication entities, namely: the user and the service provider. Let $A \xleftrightarrow{K_{ab}} B$ denotes the fresh session key K_{ab} shared between A and B, and (PK_b, SK_b) are the public/private key pairs of entity B. Hence, the mutual authentication is achieved between A and B if there exists a session key K_{ab}, and A believes $A \xleftrightarrow{K_{ab}} B$ and B believes $A \xleftrightarrow{K_{ab}} B$. As a result, we state that a strong mutual authentication should satisfy the following statements:

$$A \;\; believes \;\; B \;\; believes \;\; A \xleftrightarrow{K_{ab}} B. \tag{1}$$

$$B \;\; believes \;\; A \;\; believes \;\; A \xleftrightarrow{K_{ab}} B. \tag{2}$$

In Step 3 of the access service phase, after B receives the message $E_{PK_b}\{Access\_Service\_Request, RI$ he will decrypt $(Access\_Service\_Request, RID_j, AC_i, AC_i^*, T_i, a)$ by using the corresponding private key SK_b of B. Then B can check if the message AC_i is equal to $AC_i^{*PK_b}$. If it holds, B generates a random number b in Step 4 of the access service phase. B then computes the session key $K_{ab} = H(a||b||AC_i||0)$

and believes $A \overset{K_{ab}}{\longleftrightarrow} B$. Also, messages b and $K_{ab} \oplus (A, b', T_a)$ will be sent to A, where b' is a challenge and T_a is a timestamp.

In Step 6 of the access service phase, A computes the session key $K_{ab} = H(a||b||AC_i||0)$ and decrypts the message $K_{ab} \oplus (A, b', T_a) \oplus K_{ab}$ to confirm if this message contains (A, T_a). If so, A believes $A \overset{K_{ab}}{\longleftrightarrow} B$. Since a is chosen by A, A believes B believes $A \overset{K_{ab}}{\longleftrightarrow} B$.

In Step 7 of the access service phase, after B has received $MAC = H(K_{ab}; b'+1)$, B will check if the MAC message contains a response $b' + 1$. If so, B believes $A \overset{K_{ab}}{\longleftrightarrow} B$. Since b' is chosen by B, B believes A believes $A \overset{K_{ab}}{\longleftrightarrow} B$. Finally, Statements (1) and (2) are satisfied and together accomplish the good properties of mutual authentication and dynamic session key establishment in the SECSPP. □

4.2 Performance Analysis

In this subsection, we compared our proposed scheme with other similar works that are intended to ensure anonymous interactions between the users and the service provider [8, 29]. In [8], He et al. proposed an authorized-anonymous-ID-based scheme. The security of their scheme is based on blind signature and RSA cryptosystem. Later, in [29], Yang et al. proposed a secure scheme for providing anonymous communications in wireless systems without using asymmetric cryptosystems. The results of a comparison of efficiency between our scheme in Scenario 3, Yang et al.'s scheme and He et al.'s scheme are shown in Table 3. For evaluation of performance, we defined some computational parameters as follows.

- T_{exp} denotes the time for the modular exponentiation.
- T_{hash} denotes the time for the hashing operation.
- T_{sym} denotes the time for the symmetric encryption/decryption operation.

Table 3: Efficiency comparisons between our scheme and other related schemes

	Our scheme	Yang et al.'s scheme	He et al.'s scheme
Authorization Phase	4 T_{xor}+3 T_{hash}+ 2 T_{asym}+ 2 random numbers	4 T_{xor}+4 T_{sym}+ 13 T_{exp}+ 6 random numbers	2 T_{asym}+1 T_{hash}+ 2 random numbers
Access Service Phase	5 T_{xor}+6 T_{hash}+ 3 T_{asym}+ 3 random numbers	4 T_{exp}+4 T_{sym}+ 4 random numbers	4 T_{asym}+4 T_{hash}+ 2 T_{sym}
Computation Costs	$\approx$ 500 T_{sym}	$\approx$ 1028 T_{sym}	$\approx$ 602 T_{sym}
Computation Time	4.35 seconds	8.944 seconds	5.237 seconds

Note: In the efficiency comparisons of the above three schemes, there are some shared secret keys used between nodes. For fairness of comparisons, we omitted the computational operations required for establishing secret keys in all of the three schemes.

- T_{asym} denotes the time for the asymmetric encryption/decryption operation.
- T_{xor} denotes the time for the XOR operation.

For instance, a symmetric encryption/decryption is at least 100 times faster than an asymmetric encryption/decryption in software and an exponential operation is approximately equal to 60 symmetric encryptions/decryptions [12, 24]. Moreover, it requires 0.0005 seconds to perform a one-way hashing operation and 0.0087 seconds to perform a symmetric encryption/decryption.

Computational overhead: From the above description, of the authorization phase, it requires nearly 784 symmetric encryptions/decryptions in Yang et al.'s scheme, while that requires about 200 symmetric encryptions/decryptions in He et al.'s and ours. Additionally, in the access service phase, it requires nearly 244 symmetric encryptions/decryptions in Yang et al.'s, 402 symmetric encryptions/decryptions in He et al.'s scheme, and 300 symmetric encryptions/decryptions in our scheme. We ignored the computational costs of the one-way hash function and the XOR operations since these two kinds of operations are quite lighter in terms of load than that of a symmetric encryption/decryption. The sum of the computational time for our scheme, Yang et al.'s, and He et al.'s are 4.35 seconds, 8.944 seconds, and 5.237 seconds, respectively. As a result, the computational costs of our scheme can be reduced by 49% and 83% in comparison with Yang et al.'s and He et al.'s scheme, respectively. Therefore, the proposed scheme is highly efficient in the terms of computational overheads.

Communication overhead: Any two parties in the access service phase of proposed SECSPP scheme requires two communication rounds to accomplish mutual authentication and session key establishment. Note that two rounds is the minimum number needed for any authenticated communication scheme with mutual authentication to fulfill its goal. As a result, the proposed SECSPP scheme is highly efficient in limited computation and communication resource environments to access the remote information systems.

Storage overhead: In the access authorization phase, the proposed SECSPP scheme achieves low storage overheads because the service provider does not need to maintain authorized credential per user and each credential is still secure against malicious attacks as discussed in the previous subsection. In addition, each user only needs to store its own credential AC_i^* it belongs to. While the access service phase is running, for involved participants, including the vehicular node, the service provider and the roadside device only need to maintain one credential AC_i and two random numbers $(a_3,\ b_1)$ for each currently in-use credential and thus the storage overhead of SECSPP scheme is only half of Yang et al.'s scheme.

5 Conclusions

In this article, a secure and efficient communication scheme for vehicular ad hoc networks is proposed. By comparison with other related schemes, the proposed scheme not only maintains good and sought after properties (e.g. low computational costs, establishment of fresh session keys, mutual authentication) but also provides the advantage of user privacy preservation. Hence, a vehicular node can anonymously access the service from roadside devices that a service provider provides and nobody can learn information about the user (e.g. location/user identification/transaction privacy). Moreover, in comparison with Yang et al.'s and He et al.'s schemes, the computational costs of involved nodes in our scheme are lower and can be reduced by 49% and 83%, respectively. As a result, our proposed scheme is suitable for various ad hoc networks and privacy-vital applications in pervasive computing environments since it ensures and provides security, reliability, and efficiency.

References

[1] Mohamed Salah Bouassida, Isabelle Chrisment, and Olivier Festor. Group key management in MANETs. *International Journal of Network Security*, 6(1):67–79, 2008.

[2] D. Chaum. Blind signature systems. In *Proceedings of advances in Crypto'83*, page 153, New York, USA, 1983.

[3] Ashok Kumar Das. An identity-based random key pre-distribution scheme for direct key establishment to prevent attacks in wireless sensor networks. *International Journal of Network Security*, 6(2):129–139, 2008.

[4] F. Dotzer, F. Kohlmayer, T. Kosch, and M. Strassberger. Secure communication for intersection assistance. In *Proceedings of the 2nd International Workshop on Intelligent Transportation*, Hamburg, Germany, 2005.

[5] S. Eichler, F. Dotzer, C. Schwingenschlogl, F. J. F. Caro, and J. Eberspacher. Secure routing in a vehicular ad hoc network. In *IEEE 60th Vehicular Technology Conference*, pages 3339–3343, 2004.

[6] T. ElGamal. A public-key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Transactions on Information Theory*, IT-31(4):469–472, July 1985.

[7] M. Gruteser and D. Grunwald. Enhancing location privacy in wireless LAN through disposable interface identifiers. In *Proceedings of WMASH*, San Diego, CA, 2003.

[8] Qi He, Dapeng Wu, and Pradeep Khosla. The quest for personal control over mobile location privacy. *IEEE Communications Magazine*, 42(5):130–136, 2004.

[9] Min-Shiang Hwang, Cheng-Chi Lee, and Yan-Chi Lai. Traceability on low-computation partially blind signatures for electronic cash. *IEICE Transactions on Fundamentals on Electronics, Communications and Computer Sciences*, E85-A(5):1181–1182, 2002.

[10] Min-Shiang Hwang, Cheng-Chi Lee, and Yan-Chi Lai. An untraceable blind signature scheme. *IEICE Transactions on Fundamentals on Electronics, Communications and Computer Sciences*, E86-A(7):1902–1906, 2003.

[11] Cheng-Chi Lee, Li-Hua Li, and Min-Shiang Hwang. A remote user authentication scheme using hash functions. *ACM Operating Systems Review*, 36(4):23–29, 2002.

[12] Jung-San Lee and Chin-Chen Chang. Secure communications for cluster-based ad hoc networks using node identities. *Journal of Network and Computer Applications*, 2006.

[13] Tim Leinmüller, Christian Maihöfer, Elmar Schoch, and Frank Kargl. Improved security in geographic ad hoc routing through autonomous position verification. In *Proceedings of the 3rd international workshop on Vehicular ad hoc networks*, pages 57–66, Los Angeles, USA, 2006.

[14] Tim Leinmüller, Elmar Schoch, and Frank Karql. Position verification approaches for vehicular ad hoc networks. *IEEE Wireless Communications*, 13(5):16–21, 2006.

[15] Tim Leinmüller, Elmar Schoch, and Christian Maihöfer. Security requirements and solution concepts in vehicular ad hoc networks. In *Proceedings of the 4th Annual Conference on Wireless on Demand Network Systems and Services*, pages 84–91, 2007.

[16] U.M. Maurer and Y. Yacobi. A non-interactive public-key distribution system. *Designs, Codes and Cryptography*, 9(3):305–316, 1996.

[17] Hasnaa Moustafa, Gilles Bourdon, and Yvon Gourhant. Aaa in vehicular communication on highways with ad hoc networking support: a proposed architecture. In *Proceedings of the 2nd ACM international workshop on Vehicular ad hoc networks*, pages 79–80, 2005.

[18] K. Plossl, T. Nowey, and C. Mletzko. Towards a security architecture for vehicular ad hoc networks. In *The First International Conference on Availability, Reliability and Security*, 2006.

[19] M. Raya and J. P. Hubaux. Security aspects of inter-vehicle communications. In *Proceedings of the 5th Swiss Transport Research Conference (STRC 2005)*, Ascona, Switzerland, 2005.

[20] M. Raya and J. P. Hubaux. The security of vehicular ad hoc networks. In *Proceedings of the 3rd ACM workshop on Security of ad hoc and sensor networks*, pages 11–21, Alexandria, USA, 2005.

[21] Maxim Raya, Daniel Jungels, Panos Papadimitratos, Imad Aad, and JeanPierre Hubaux. Certificate revocation in vehicular ad hoc networks. Technical LCA-Report-2006-006, LCA, 2006.

[22] Wei Ren. Pulsing RoQ DDoS attacking and defense scheme in mobile ad hoc networks. *International Journal of Network Security*, 4(2):227–234, 2007.

[23] R. L. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public key cryptosystems. *Communications of the ACM*, 21(2):120–126, 1978.

[24] B. Schneier. *Applied Cryptography, Protocols, Algorithms, and Source Code in C*. John Wiley and Sons Inc., second edition, 1996.

[25] Bartlomiej Sieka and Ajay D. Kshemkalyani. Establishing authenticated channels and secure identifiers in ad-hoc networks. *International Journal of Network Security*, 5(1):51–61, July 2007.

[26] Chwei-Shyong Tsai, Chih-Wei Lin, and Min-Shiang Hwang. A new strong-password authentication scheme using one-way hash functions. *International Journal of Computer and Systems Sciences*, 45(4):623–626, 2006.

[27] Yuh-Min Tseng and Jinn-Ke Jan. ID-based cryptographic schemes using a non-interactive public-key distribution system. In *Proceedings of the 14th Annual Computer Security Applications Conference (IEEE ACSAC98)*, pages 237–243, Phoenix, Arizona, Dec. 1998.

[28] Johann van der Merwe, Dawoud Dawoud, and Stephen Mcdonald. A survey on peer-to-peer key management for mobile ad hoc networks. *ACM Computing Surveys*, 39(1):1–45, 2007.

[29] Chou-Chen Yang, Yuan-Liang Tang, Ren-Chiun Wang, and Hung-Wen Yang. A secure and efficient authentication protocol for anonymous chan-

nel in wireless communications. *Applied Mathematics and Computation*, 169(2):1431–1439, 2005.

[30] Yanchao Zhang, Wei Liu, Wenjing Lou, and Yuguang Fang. Securing mobile ad hoc networks with certificateless public keys. *IEEE Transactions on Dependable and Secure Computing*, 3(4):386–399, 2006.