Research Article
A Novel Authentication Scheme for V2I Communication Based on WAVE Unicast Services

Atthapol Suwannasa, Somnuk Puangprongpitag, and Wirat Phongsiri
Faculty of Informatics, Mahasarakham University, Mahasarakham 44150, Thailand
Correspondence should be addressed to Somnuk Puangprongpitag; somnuk.p@msu.ac.th
Received 15 July 2013; Revised 8 October 2013; Accepted 23 October 2013

One of the most challenging issues in vehicular network designs is security matter. Particularly, there have been several potential attacks (e.g., message alteration, eavesdropping, privacy violation, and replay) on Vehicle to Infrastructure (V2I) communication. Most previous studies have based on Public Key Infrastructure (PKI) and authentication in broadcast services. By relying on the PKI solutions, cryptographic overhead and the management difficulties of public key certificates can be problematic. Furthermore, broadcast services can cause network flooding. Hence, this paper proposes a novel authentication scheme based on WAVE unicast services to reduce the PKI overhead between vehicles and Road Side Units (RSU). The new scheme is based on Pairwise Transient Key (PTK) procedures with a few extra authentication steps. To evaluate the new scheme, we have experimented on a Network Simulator (NS-2) under both city and highway scenarios. The experimental results have demonstrated that our new scheme introduces only small WAVE Short Message (WSM) delay. The new scheme is also flexible to use in various scenarios under different road situations.

1. Introduction

In recent years, vehicular networks have been investigated by academic researchers and industrial laboratories. The creation of vehicular networks is to provide connectivity among vehicles, resulting in road safety improvement and traffic management. These features are very significant in Intelligent Transport Systems (ITS). In a vehicular network, there are two wireless terminals, namely, Road Side Unit (RSU) and On-Board Unit (OBU). The RSUs may be connected with their infrastructures or other RSUs and located at important parts along roadside. The OBUs are wireless devices, equipped in vehicles to communicate with RSUs and other OBUs. To support ITS, the IEEE 802.11p Dedicated Short Range Communications (DSRC) [1] has been standardized for Wireless Access in Vehicular Environments (WAVE), including Vehicle to Vehicle (V2V) and Vehicle to Infrastructure (V2I). WAVE Short Message Protocol (WSMP) [2] specifies the format of WAVE Short Messages (WSM), exchanged over V2V and V2I.

Security issues in vehicular networks are very crucial due to the sensitivity of WAVE messages in daily life (e.g., accident alerting, traffic jam warning, and traffic light notification). A few malicious WSMs can even create an enormous damage to people and vehicles. Furthermore, privacy must be preserved to protect user private information (e.g., driver's name and license number). The privacy preservation requires some security schemes. Nevertheless, providing the WAVE security is still a challenging task due to the characteristics of vehicular networks (e.g., high speed mobility and large coverage area).

Generally, security schemes are considered separately between V2V and V2I [3] due to the differences of communication models. In particular, sender authentication, message integrity check, and message encryption for V2I have recently been focused by several previous studies. However, there are still several unsolved issues.

Most previous V2I authentication and privacy schemes [3–6] have mainly relied on broadcast communication, which causes network flooding. Boban et al. [7] have evaluated the achievable unicast performance over WAVE services under both city and highway environments. Their evaluation results have demonstrated that unicast communication has the ability to provide a reliable WAVE service and prevents the network flooding. Furthermore, Huang-Fu et al. [8] have
proposed mechanisms based on the unicast service that can reduce 40–90 percent of network traffic overhead. However, there is no security scheme defined in all previous unicast-based mechanisms to protect against several security threats.

So far, there have been a lot of security protocols to prevent several potential attacks in vehicular networks, such as IEEE 1609.2 [9], GSIS [3], IBV [6], and so on. Yet, most of them still have some drawbacks. The IEEE 1609.2 standard with the support of Elliptic Curve Digital Signature Algorithm is designed to support security services on WAVE. However, cryptographic overhead and the management difficulties of public key certificates are still the big concerns [5, 10]. GSIS can only support the authentication between RSUs and the OBUs of some emergency vehicles. It has not been designed for the OBUs of any normal vehicles. In IBV, an OBU’s private key is generated by a tamperproof device (deployed at each vehicle) to sign a message, lunched by an OBU. Yet, IBV has not defined a method to secure a message from an RSU.

Hence, in this paper, we mainly focus on V2I authentication scheme to solve the cryptographic overhead problem and the management difficulties of public key certificates problem. Furthermore, we focus on securing and authenticating WSMs from both directions (RSUs to OBUs and OBUs to RSUs). Our design is also based on WAVE unicast services to avoid network flooding. This work is also an extended work from our previous work in [11] to enhance the vehicle driver’s privacy issues. To evaluate the flexibility of our scheme in different communication scenarios, we simulate our new design in both city and highway environments using NS-2.

The rest of this paper is organized as follows. We first introduce the background and related work in Section 2. In Section 3, our scheme is proposed. Section 4 analyzes our scheme in several security requirements including authentication, nonrepudiation, integrity, and availability. In Section 5, our scheme has been simulated and evaluated on NS-2. Finally, Section 6 concludes this paper.

2. Background and Related Work

2.1. Vehicular Network Communication. In vehicular networks, the IEEE 802.11p [1] has been standardized to support a wide range communication. The IEEE 802.11p is designed for DSRC radio to support WAVE data transmission in ranges up to 1,000 m with vehicle velocities in several environments (e.g., urban, highway, and rural). WAVE is a multichannel system that operates among one Control CHannel (CCH) and multiple Service CHannels (SCHs). WAVE management messages and WSMs are transmitted by using the CCH. IP data packets (e.g., Internet access, voice over IP, and video streaming) are transferred under a SCH. WSMs can also be delivered over both CCH and SCHs.

The WSMP is used to rapidly deliver a WSM for data transmission and a WAVE Service Advertisement (WSA) for signal controlling [2, 12]. The WSA is broadcasted to provide the information of available ITS services, offered by an RSU. A Provider Service Identifier (PSID) is used to identify each ITS service.

2.2. WAVE Unicast Services. In the WAVE unicast services, each ITS server must track the addresses of OBUs. Hence, a mobility management technique is also necessary for tracking.

Basic Mobility Management (BMM) and Location Estimation-based Mobility Management (LEMM) have been proposed to provide WAVE unicast services in [8, 13]. For BMM, all RSUs are partitioned into several Location Areas (LAs) [8]. The LA consists of one or more RSUs and it is identified by a Location Area Identity (LAI) [14]. A Location Server is deployed to maintain the RSUs and LAs mapping. In an LA, RSUs broadcast a WSA (PSID service) to OBUs. If the OBU has subscribed to the PSID service, it then identifies this service over the SCH. After that, the RSUs allocate radio resources to support this service operation. The OBU then sends a registration WSM under the unicast mode through the RSU to the Location Server. It then maps the OBU’s MAC address to the LAI, which is covered within the RSU. Finally, this mapping information is stored in the Location Server’s database. The Location Server can send WSMs to the OBU using this LAI. If the OBU enters a new LA, it performs another registration to update new LAI. For LEMM, positioning systems (e.g., GPS) are deployed to estimate the OBU’s location of a high-speed vehicle.

Although both mechanisms can effectively reduce the network overhead of the broadcast behavior, there is no proposed authentication scheme to secure the unicast WSMs. So, it is vulnerable to several attacking techniques.

2.3. Security Issues between OBUs and RSUs. According to Raya et al. [10], vehicular networks are vulnerable to several security threats. In a communication without cryptographic mechanisms, an attacker can deliberately generate false information and transmit to victims. The attacker can also eavesdrop the victims’ personal data. Furthermore, message modification, fabrication, and replay can cause misunderstanding to a victim. Hence, security schemes are very crucial to protect against all aforementioned problems.

The IEEE 1609.2 standard [9] is a set of security services for WSM data and applications. In the IEEE 1609.2, security systems rely on Public Key Infrastructure (PKI) with the support of Elliptic Curve Digital Signature Algorithm (ECDSA). However, an RSU can communicate with hundreds of OBUs in a high density traffic road, in which there may be roughly 180 vehicles keeping within the RSU’s coverage area [6]. So, the management difficulties of public key certificates under PKI may be unacceptable. In addition, driver identification, certificate revocation, cryptography overhead, and privacy protection are additional concerns about the standard. Moreover, the hardware costs would be very expensive to verify a digital signature for every incoming message [4].

Lin et al. [3] have proposed a security protocol (viz., GSIS), based on a group signature and an identity-based signature. The group-based signature is deployed to provide security in V2V, while the identity-based is deployed to secure communication in V2I. This protocol integrates identity-based signature [15] to sign messages, lunched by RSUs. After receiving the messages, OBUs verify the signature to ensure...
its authenticity. However, the protocol is not defined how to verify messages created by general OBUs. In fact, the general OBUs can contact an RSU to request or report some information, such as traffic jam, road under accident, and so on.

Zhang et al. [6] have proposed an Identity-based Batch Verification (IBV) scheme to sign messages created by OBUs. A tamperproof device is equipped in a vehicle to generate an OBU’s private key for signing each message, lunched by the OBU. A Real IDentity (RID) and a password are used to authenticate and activate the tamperproof device. The password can be the signature of the RID signed by a Trust Authority (TA). However, drivers have to contact the TA, if they want to change the device’s password. So, it is probably infeasible to use. Furthermore, this technique has not yet defined a method to sign a message, lunched by an RSU.

A lightweight authentication scheme has been proposed in [16] to secure the handoff process in IEEE 802.11p for nonsafety related application. However, there are enormous numbers of keys appearing at RSUs. This scheme has not defined key management processes after completing communication. Hence, the RSU may store hundreds of keys that can hugely degrade the RSU performance.

In [11], we have proposed an authentication scheme in V2I communication based on WAVE unicasts services under a city environment. To exchange WSMs with minimum cryptographic overhead, a symmetric encryption is deployed by creating Pairwise Transient Keys (PTKs). We have designed two PTKs, namely, pre-ptk and ptk. The pre-ptk has been designed for the authentication procedures, while the ptk has been designed to secure unicast WSMs. A driver’s license plate number is used as a component to generate a pre-ptk key. This part of the design can be a security weakness since attackers can easily eavesdrop the license plate number in plaintext.

3. Proposed Design

To countermeasure the potential security threats with minimum authentication overhead, we propose a novel authentication scheme for V2I communication based on WAVE unicast services. In our scheme, there are two types of unicast WSMs, including authentication WSMs and ITS WSMs. The authentication WSM is to authenticate a legitimate driver and a vehicle (an OBU). The ITS WSM is to transfer information for supporting the ITS (e.g., traffic jam alerting messages) and to update the OBU’s address for location tracking according to WAVE unicast services. The notations in our proposed scheme are listed in Table 1. Figure 1 presents an overview scenario of our scheme.

To reduce authentication operations at an RSU and the workload of an authentication server, all RSUs in the scenario are partitioned into several LAs. We assume that the communication of RSUs with their infrastructures and the communication between RSUs are secure and trustable. The details of our keys procedures are discussed as follows.

In our design, there are three key types, namely, pre-pairwise transient key (pre-ptk), pairwise transient key (ptk), and random short key (rsk). When an OBU enters a first LA in a vehicular network, a first pre-ptk (pre-ptk) is created to secure an rsk from the OBU. The second pre-ptk is then generated to secure an rsk from an RSU. After that, the OBU and the RSU exchange the keys (rskOBU and rskRSU). By using the exchanged keys as a component, a ptk is then generated to secure unicast WSMs in the LA. By using this technique, there is no extra operation for the authentication server when the OBU travels to RSUs in the same LA. The key rsk is randomly generated into six characters, consisting of numbers and alphabet characters. When the OBU moves to a new LA, it has to perform a new authentication to generate another ptk, for

| Notations | Descriptions |
|-----------|--------------|
| LA        | Location Area |
| ptk       | OBU’s Pairwise Transient Key |
| pre-ptk   | OBU’s pre-ptk, OBU is pre-ptk_b |
| driver_i  | The driver’s license plate number |
| rskOBU    | Random short key from an OBU |
| rskRSU    | Random short key from an RSU |
| t_i       | The timestamp of ptk_i |
| AM        | Address Mapping service |
| IDUC      | WAVE unicast service ID (PSID) |
| IDRSU     | Road Side Unit ID |
| IDOBU     | Vehicle ID |
| H ()      | Hashing function |
| ptk_i()   | Encrypted data using pre-ptk_i |
| pre-ptk-a_i() | Encrypted data using pre-ptk-a_i |
| pre-ptk-b_i() | Encrypted data using pre-ptk-b_i |

Figure 1: An overview of system architecture in our scheme.
that LA. The keys used in our scheme are based on symmetric encryption with username and password concept. Hence, there is no extra PKI encryption and certificate management overhead. Furthermore, by using unicast services, our design can effectively reduce the undesirable effects of the broadcast behaviors.

In [11], a driver’s license plate number is transferred in plaintext under WSMP from a source OBU to a destination RSU. This license plate number is deployed to query its password for generating the RSU side $\text{pre-}ptk_a_i$. This weakness of this procedure is that the driver’s personal data (driver’s license plate number) can be eavesdropped. This problem can cause a serious concern of his/her privacy. In this paper, the new authentication procedures have been therefore designed to solve this problem.

In our authentication scheme, there are two main security procedures as follows.

### 3.1. Authentication Procedures

In our design, a legitimate driver must register to subscribe ITS services from an ITS website. This website is protected by traditional web security. It may be a government’s website operated with a transportation database. This database stores important information of the driver (e.g., the driver’s license plate number and its password pair) and the information of his/her vehicle (e.g., vehicle ID and its password pair). After completing the registration process, the legitimate driver has username and its password pair to access the ITS services in each RSU.

There are two pairs of username/password, which are used to generate a key $\text{pre-}ptk_b_i$ and $ptk_i$. A driver, and its password pair and an ID$_{OBU}$ and its password pair are defined in (2) and (3). This technique can mitigate nonrepudiation problem because of the specific authentication data of the driver and his or her vehicle (the non-repudiation will be further discussed in Section 4). When an OBU enters an LA (e.g., LA$_i$ at time $t_i$ in Figure 1), the OBU has to complete the following steps (as shown in Figure 2) to generate a $ptk_i$.

#### Step A.1
The OBU initiates a unicast service by recoding the service PSID (i.e., ID$_{UC}$). The OBU has to be a member of this service. If an RSU supports this service, it allocates radio resources and announces the service ID$_{UC}$ by sending a WSA to the OBU (described further in Step A.2).

#### Step A.2
The RSU intermittently broadcasts the WSA to the OBU in Step A.2.1. In this WSA, the source address (src) is the RSU’s MAC address (MAC$_{RSU}$). The destination address (dst) is the broadcast MAC address (MAC$_{BROADCAST}$). The RSU’s ID is ID$_{RSU}$. The PSID is ID$_{UC}$, and the last field is a SCH number. The OBU can then receive the WSA for matching with the unicast service ID$_{UC}$ in Step A.2.2. In this matching process, if the OBU is a member of the service, the SCH is identified for this service. When the OBU enters a new LA, it has to perform this step again for initiating a unicast service in that LA.
Step A.3. In path (1) Figure 1, \(pre-pGTK_a\) is generated to encrypt an authentication request message, driver\(_i\) and rsk\(_{OBU}\). The encrypted value is placed into the data payload of an authentication WSM in Step A.4. The key \(pre-pGTK_a\) is based on a hashing function as shown in the following equation:

\[
pre-pGTK_a = H ((ID_{OBU}, password), ID_{RSU}, ID_{UC})
\]

\[
pre-pGTK_b = H ((driver\_i, password), (ID_{OBU}, password), ID_{RSU}, ID_{UC}, rsk_{OBU}) .
\]

Step A.4. The OBU sends the authentication WSM to authenticate at the RSU. The data payload also contains an ID\(_{OBU}\) and the encrypted value, including the authentication request message (i.e., type "AUTH REQUEST"), the driver\(_i\), and the rsk\(_{OBU}\). The RSU forwards this authentication WSM with its ID\(_{RSU}\) to the authentication server. After that, the authentication server generates \(pre-pGTK_a\) by querying the password of the ID\(_{OBU}\) from its database to decrypt the authentication WSM to get the driver\(_i\). The authentication server then queries the password of the driver\(_i\) and replies the driver\(_i\) and its password pair and the ID\(_{OBU}\) and its password pair back to the RSU. In this step, the information from the driver's license plate number (driver\(_i\)) is encrypted before sending from the OBU to the RSU. In our new design, although an attacker can eavesdrop the authentication WSM, the attacker cannot decrypt it to get the driver\(_i\) and the rsk\(_{OBU}\) due to having no valid key. This technique can effectively reduce the privacy concern comparing to the proposed scheme in [11].

Step A.5. The RSU receives the driver\(_i\) and its password pair and the ID\(_{OBU}\) and its password pair from the authentication server. The RSU then has all required data to generate the key \(pre-pGTK_a\). This key is finally generated to decrypt for obtaining rsk\(_{OBU}\).

Step A.6. The RSU-side ptk\(_i\) is generated as defined in (3). This ptk\(_i\) with a timestamp \(t_i\) is distributed to all RSUs (such as RSU\(_j\) and RSU\(_k\)) in LA\(_n\) in Figure 1 to secure the unicast service ID\(_{UC}\) in the LA. The key ptk\(_i\) is used until the OBU enters a new LA or until it expires. The timestamp \(t_i\) is used to check an expiration time of the ptk\(_i\). This expiration time is predefined as threshold \(L\). When the difference of \(t_i\) and current timestamp is larger than threshold \(L\), the ptk\(_i\) is obsoleted. After that, the OBU has to reauthenticate to receive a new key. In our scheme, we define threshold \(L = 20\) minutes. If it is too small, the key will be frequently changed. So, it can increase the security. However, it may affect the RSU performance. To be used in a real world environment, threshold \(L\) should be configured as a suitable value depending on an RSU’s performance:

\[
ptk_i = H ((driver\_i, password), ID_{OBU}, password), ID_{RSU}, ID_{UC}, rsk_{OBU}, rsk_{RSU}, t_i).
\]

Step A.7. To send a reply message back to the OBU, ptk\(_i\) is not used in this step because the OBU has no \(t_i\) value and rsk\(_{RSU}\) to generate the OBU side ptk\(_i\) for decryption. So, the RSU-side \(pre-pGTK_b\) is created as shown in (2) to encrypt data, \(t_i\), and rsk\(_{RSU}\) for sending back to the OBU.

Step A.8. The RSU generates the key rsk\(_{RSU}\) to be a component of the key ptk\(_i\). In this step, the RSU already has both the keys rsk\(_{OBU}\) and rsk\(_{RSU}\). The RSU sends an authenticated WSM back to the OBU. This WSM consists of the src (MAC\(_{RSU}\)), the dst (MAC\(_{OBU}\)), ID\(_{UC}\), and the data field. The data is encrypted by the \(pre-pGTK_b\) including the reply message (i.e., type “200 OK”), ID\(_{RSU}\), rsk\(_{RSU}\), and \(t_i\).

Step A.9 and Step A.10. The OBU side \(pre-pGTK_b\) is then generated to decrypt the authenticated WSM data received from Step A.8. The OBU then obtains the key rsk\(_{RSU}\) to generate the OBU side ptk\(_i\). Hence, there are the ptk\(_i\) keys in both the OBU and the RSU for securing ITS WSMs for the service ID\(_{UC}\). When the key ptk\(_i\) expires at the RSU, the OBU cannot use this key to communicate with the RSU. So, it is obsoleted at the OBU. The OBU then has to complete the procedures in Figure 2 for a new Pairwise Transient Key.

3.2. Security Procedures between OBSUs and RSUs. To secure communication between the OBU and the RSU, the key ptk\(_i\), generated from Steps A.6 and A.10, is used to encrypt/decrypt ITS WSM data for service ID\(_{UC}\). The OBU has to update a current connected RSU to an Address Mapping (AM) service by completing Steps B.4–B.6 (Figure 3). These steps are activated, when the authentication process (as defined in Figure 2) is done or the OBU moves to a new RSU in the same LA. Steps B.7–B.9 are used to send an ITS message of service ID\(_{UC}\) to the OBU.

Step B.1 and Step B.2. The OBU has to perform Steps B.1 and B.2 to subscribe the AM service. This service is used to map the MAC\(_{OBU}\) and the connecting ID\(_{RSU}\). It is necessary to track the OBU’s location.

Step B.3. The key ptk\(_j\), generated in Step A.10 in Figure 2, is used to encrypt ITS WSM data from the OBU side (Steps B.4 and B.9).

Step B.4. The OBU sends an ITS WSM to the RSU for updating its address. The data payload contains the request message (i.e., “UPDATE”), ID\(_{OBU}\), and ID\(_{RSU}\). The RSU forwards these data to the ITS server. In AM service at the ITS server, the MAC\(_{OBU}\) and the ID\(_{RSU}\) pair is mapped and stored in AM cache. When the OBU enters a new RSU, it has to perform this step again to update the MAC\(_{OBU}\) and the new ID\(_{RSU}\) pair in AM cache.

Step B.5. The ptk\(_j\) key, created in Step A.6, is used to encrypt the ITS WSM data, generated by the RSU side (Steps B.6 and B.8).
Step B.6. The RSU generates a WSM and sends it back to the OBU. The WSM data message (i.e., “200 OK”) and ID_{RSU} are encrypted by the ptk_i key.

Step B.7. When the ITS server needs to send an ITS message (e.g., traffic jam warning message) to the OBU, the MAC_{OBU} and ID_{RSU} pair is obtained from the AM cache. The ITS message with the MAC_{OBU} and ID_{RSU} pair is sent to the RSU. After that, the RSU converts the received data into a WSM format to forward to the OBU accordingly.

Step B.8. The RSU forwards the ITS message as the WSM format under unicast communication to the OBU by using MAC_{OBU}, obtained from Step B.7 as the destination. The WSM data payload contains the ITS message and ID_{RSU}, which are encrypted by ptk_i.

Step B.9. When the OBU receives the ITS WSM, it uses the OBU side ptk_j to decrypt the message. The OBUs then send a WSM reply back to the RSU. The WSM data payload is encrypted by the ptk_j including the reply message (i.e., “200 OK”) and the ID_{OBU}. Conversely, the OBU can use the ptk_j to secure messages for reporting some road situations to the RSU.

If the OBU cannot receive the ITS WSM (no reply back to the RSU), the following operations are activated. In Figure 1, when the message in path (3) cannot reach the OBU, the process of path (4) is activated. In this process, RSU_2 has to forward the message to its neighbors, and RSU_3 sends the message received from RSU_2 to the OBU. If the OBU has still not received the message, the current RSU (that received the message) must keep forwarding the message until arriving at the OBU or until the OBU enters a new LA. Hence, there is no extra operation for the ITS server, when this situation happens.

4. Security Analysis

The proposed scheme has been designed to secure V2I communication. By using the PTK procedures, the WSMs can be transmitted between OBUs and RSUs with minimum cryptographic overhead without introducing the management difficulties of public key certificates. So, this scheme is better than the traditional PKI-based schemes. The novel authentication scheme primarily satisfies the requirements of authentication, non-repudiation, integrity, and availability. The analysis of these security requirements is discussed as follows.

Authentication. The authentication procedures with two pairs of username/password have been proposed. To identify the permission of a legitimate user and an OBU, RSUs have to authenticate the OBU and the legitimate driver by using an OBU’s ID (as a username), its password, and an encrypted driver’s license plate number. To generate a ptk, the passwords of the driver’s license plate number and the OBU’s ID are used together with other components as described in the aforementioned procedures. Hence, we can authenticate both a vehicle (OBU) and its driver.

Nonrepudiation. Each unicast WSM data payload is encrypted by a Pairwise Transient Key. This key is generated by using the specific authentication data of an OBU and a legitimate driver by using an OBU’s ID (as a username), its password, and an encrypted driver’s license plate number. To generate a ptk, the passwords of the driver’s license plate number and the OBU’s ID are used together with other components as described in the aforementioned procedures. Hence, we can authenticate both a vehicle (OBU) and its driver.

Integrity. Message alteration and source modification can cause a serious damage to drivers, passengers, and vehicles.
To prevent the message alteration and the source modification, a unicast WSM is encrypted using a Pairwise Transient Key. When the WSM is modified, the specific Pairwise Transient Key for the original WSM cannot be used to decrypt the modified WSM.

**Availability.** Two pairs of username/password and random short keys are used to generate a \( ptk \) with a timestamp. By using these components, each key is changed in different LAs. Furthermore, each \( ptk \) key has a specific expired time. The RSU can check the expiration time by computing the period between the timestamp of a \( ptk \) and the current timestamp. So, it is tolerant to brute-force attack. The message encrypted with the expired \( ptk \) will be dropped at the destination. All RSUs in our scheme are partitioned into several LAs. The key \( ptk \) is designed to be used in the same LA, and it is renewed in a new LA. So, the OBU also has the keys to secure the unicast WSMs all over communication. Hence, scalability problems can be reduced. In addition, there is no extra operation at the authentication server, when the OBU travels in the same LA.

The possible potential attacks in vehicular networks have been presented in [10]. The most potential attacks can be eavesdropping, message alteration, privacy violation, and replay. By using these attacking techniques, an attacker can confuse victim drivers with fake information that can damage the drivers, passengers, and vehicles. Here, we analyze our security scheme to protect against the most potential attacks.

**Eavesdropping.** A driver authentication can be completed, when an authentication request message is successfully decrypted. By using this technique, attackers cannot eavesdrop to get the password. The passwords (of OBUs and drivers) have never been sent across the network. At the RSUs, the passwords of OBUs and the drivers are stored in location server’s database. Each OBU has also stored its own password and entered driver’s password. Furthermore, when an attacker eavesdrops a WSM, the information in the data payload cannot be decrypted at the attacker’s side because there is no valid victim’s \( ptk \) to decrypt.

**Message Alteration.** When a unicast WSM is altered by an attacker or encrypted by a fake key, the destination of the unicast WSM cannot decrypt to obtain the information due to the alteration of the WSM payload. If the decryption fails, this WSM may be illicitly altered. So, it will be dropped. In addition, the attacker cannot fake an RSU’s messages to a victim (OBU) because the attacker has no valid victim’s \( ptk \) to encrypt the messages.

**Privacy Violation.** We have proposed the new authentication procedures to improve the privacy concern in [11]. If we use a plaintext license plate number, privacy preservation could be failed. In this new scheme, the license plate number is encrypted before sending to authenticate at the Location Server. This license plate number is used to query its password to be used as a component of the \( ptk \). So, the driver can also be automatically authenticated, when the WSMs (exchanged between the OBU and the RSU) are successfully decrypted using the \( ptk \).

**Replay.** An attacker eavesdrops and replays a unicast WSM encrypted by the current \( ptk \) of a legitimate driver to a victim. The victim then replies another encrypted unicast WSM back to the attacker. Although the victim can decrypt the encrypted message, the reply message cannot be decrypted at the attacker’s side due to having no correct \( ptk \). Furthermore, the victim does not consider the messages, encrypted by the expired \( ptk \).

### 5. Evaluation

In this section, our scheme has been experimented on the Network Simulator (NS-2) (release 2.35) [17]. In [11], we have focused on a city environment only. However, our scheme is actually designed to support in both highway environments (where vehicles move very fast) and city environments (where vehicles move slowly). In this paper, we have extended the performance evaluation of our scheme to cover the highway environment scenario. The NS-2 based IEEE 802.11p is modified to simulate our scheme. To create vehicles movement, an NS-2 traffic generator has been developed using JAVA. This generator creates movement scripts and other parameters as discussed in what follows. The goal is to test whether or not our new scheme can be flexible to use in both highway and city scenarios.

#### City Scenario.

The traffic generator deploys a Manhattan model [18] to simulate the city environment. The probability of remaining on the same street is 0.5, and the probability of turning left or right is 0.25. Each node is randomly assigned the path of routes for traveling. The vehicle velocities are randomly generated between 3.5 and 20 m/s (12.6–72 km/h) to typically simulate a traffic behavior in the city scenario. Furthermore, the density of the vehicles on the road is a main factor to impact the vehicular network performance. So, there are different numbers of nodes (OBUs) introduced (as shown in Figure 4). The city scenario simulation parameters are shown in Table 2.

#### Highway Scenario.

In the traffic generator, we assume a three-lane highway of 20 kilometers length in one direction. The vehicles (simulation nodes) move to the end of the highway. The velocity of the vehicles is a main factor to evaluate the performance in highway environments. We have measured

| Parameters                      | Configuration value |
|---------------------------------|---------------------|
| Simulation scenario             | City                |
|                                 | Highway             |
| Simulation area                 | 5,500 m × 5,500 m   |
|                                 | 100 m × 20,000 m    |
| Number of RSUs                  | 16 nodes            |
|                                 | 10 nodes            |
| Number of OBUs                  | 20–350 nodes        |
|                                 | 10, 20, 30 nodes/km|
| Vehicle velocities              | 3.5–20 m/s          |
|                                 | 16–30 m/s           |
| Radio range                     | 1,000 m             |
| Pause time                      | 0 s                 |
| WSM packet size                 | 512 bytes           |
| Location Area (LA) size         | 1–4 nodes           |

---

*Table 2: Simulation configuration.*
the performance with different vehicle velocities. The average velocities are faster than the city scenario. In addition, the different numbers of nodes can cause the different results of the evaluation. In the normal behavior of a highway environment, the density of nodes is smaller than a city environment. However, the nodes density is still an important factor to affect the vehicular network performance. So, we consider different average numbers of nodes/km (including 10, 20, and 30 nodes/km). Table 2 presents the simulation parameters of the highway scenario.

According to Emmelmann et al. [19], packet size of 100 bytes is long enough to distribute the WSM safety related message. Yet, due to security overhead, the packet size is likely longer. An average packet size of 500 bytes has been used in [20] to evaluate the IEEE 802.11p performance, since it is a reasonable average packet size including data and security information. So, we choose a packet size of 512 bytes for covering our security overhead in each unicast WSM.

In order to evaluate the performance of our scheme, we focus on the authentication WSM delay and the ITS WSM delay. The WSM delay is the most important factor for the evaluation. It can indicate whether or not our scheme can provide a reliable service. The goal is also to test whether or not the authentication WSM and the ITS WSM in our scheme causes too high delay. The performance evaluation metrics and results are discussed as follows.

5.1. Authentication Delay. The authentication delay in different densities of the OBU nodes is a main factor to evaluate the efficiency of an authentication scheme. In our evaluation, we have measured the delay of the authentication WSM (from the OBU beginning to send an authentication request to the RSU until replying back the authenticated WSM to the OBU).

We consider the number of nodes separately between the city and highway.

5.1.1. Evaluation Results in the City Scenario. The simulation results are shown in Figure 4(a) with error bars that represent the 95% Confidence Interval. According to the figure, with the increase of traffic load (i.e., increasing the numbers of nodes in the simulation area), we can find that the authentication delay increases. However, when the traffic load becomes large, the WSM authentication delay increases negligibly (e.g., 350 nodes with around 4 ms) comparing to the light traffic (e.g., 20 nodes with around 3 ms). In case of the traffic load growing up, the results with ITS WSM background traffic are more volatile (the variation of the error bars) than the results without ITS WSM background traffic. This is due to the interruption by the background traffic in different road situations. However, the results are applicable, even if the traffic load becomes large.

The improvement of our new authentication scheme cannot significantly change the evaluation results in the city scenario because the concept of WSM transmission remains the same as proposed in [11]. However, this new authentication scheme has been improved to be the better solution in terms of security and privacy as discussed in Section 4.

5.1.2. Evaluation Results in the Highway Scenario. We have simulated a highway scenario with different vehicle velocities and numbers of nodes/km. The simulation results with error bars that represent the 95% Confidence Interval are shown in Figure 5(a). The results of the average authentication WSM delay are negligible. The maximum value with the peak error bar is around 4 ms. The results of the higher
velocity nodes (e.g., 24 and 30 m/s) in the larger traffic density (e.g., 30 nodes/km) are more volatile (the variation of the error bars) than the slower velocity nodes in the smaller traffic density. When the traffic density becomes large, the number of WSM packets then increases. So, it can increase the probability of the packets from a node interrupting each other and can make the variation of the error bars depending on the road situations. Even after increasing the velocity, the differences of the authentication delays are still negligible. The velocity may have little effect on the results due to the small number of authentications in the Location Area design.

5.2. Unicast ITS WSM Delay. Packet delay of the unicast ITS WSM is also important to evaluate the efficiency of our security procedures. In our simulation, RSUs periodically send ITS WSM traffic (e.g., traffic jam alerting) in unicast mode to OBUs. So, we simulate the unicast ITS WSMs and let the RSUs intermittently send the messages to the OBUs. The OBUs then reply the messages (“200 OK”) back to the RSUs as unicast WSMs. The ITS WSM delay in each communication (from the source address beginning to send an ITS WSM until receiving at the destination address) has been used to measure the efficiency of the security procedures.

5.2.1. Evaluation Results in the City Scenario. The experimental results with error bars that represent the 95% Confidence Interval are shown in Figure 4(b). It can be seen that the ITS WSM delay ratio and the error bars ratio grow up when the traffic load becomes large. This is reasonable because when the traffic load increases, there are more numbers of packet transmission. However, the ITS WSM delay does not vary a lot. This delay is still smaller than the maximum delay of 100 ms, discussed in [19] to be able to provide a reliable service.

5.2.2. Evaluation Results in the Highway Scenario. Figure 5(b) shows the results with error bars that represent the 95% Confidence Interval. A slower velocity node must take longer time to travel to the end of the highway than a faster velocity node. So, with the slower velocity node, the probability to receive the ITS WSMs is higher. When the average velocity is 16 m/s with the largest number of nodes/km (e.g., 30 nodes/km) in the simulated highway, the average ITS WSM delay is approximately 16 ms, and the error bar is more volatile than other node densities. The slower velocity node takes longer time to travel in the highway. So, it can increase a chance to receive WSMs. Also, the ITS WSM delay can be increased due to interrupting by several WSMs from many nodes in different road situations. However, in the same velocity of 16 m/s, the delays are still negligible in the smaller density (e.g., 10 and 20 nodes/km) due to fewer packets at the light traffic density.

For the high velocity (e.g., 24, and 30 m/s) nodes, the average ITS WSM delays are smaller than the slower velocity nodes. When the nodes move very fast, the chance to receive the ITS WSMs is low. So, the small number of packets can decrease the delays. However, the experimental results demonstrate that our scheme introduces very small delay in various road situations.

6. Conclusions

In this paper, a novel authentication scheme based on WAVE unicast services has been proposed for V2I.
Pairwise Transient Key (ptk) schemes, authentication, non-repudiation, integrity, and availability can be achieved without introducing the overhead of PKI. An improvement of authentication procedures has been proposed to increase security and privacy. By using the unicast communication, the WAVE messages can be effectively transmitted with small delay. To support unicast services, an address mapping with ptk security schemes has been designed to track the locations of the OBUs.

To test whether or not our new scheme can be flexible to use in both highway and city scenarios, the experimental results have been done using NS-2. The experimental results have demonstrated that the unicast WSM delay can be kept quiet low in both simulated scenarios.

Acknowledgments

This research has been funded by Thailand Research Fund (RSA5080013), National Research Council of Thailand, and Mahasarakham University.

References

[1] "IEEE Standard for Information technology—telecommunications and information exchange between systems—Local and metropolitan area networks— Specific requirements— Part II: wireless LAN medium access control (MAC) and physical layer (PHY) specifications amendment 6: wireless access in vehicular environments," 2010.
[2] "IEEE draft standard for wireless access in vehicular environments (WAVE)—networking services," IEEE P1609. 3/D9, pp. 1–133, 2010.
[3] X. Lin, X. Sun, P.-H. Ho, and X. Shen, "GSIS: a secure and privacy-preserving protocol for vehicular communications;" IEEE Transactions on Vehicular Technology, vol. 56, no. 6, pp. 3442–3456, 2007.
[4] H. Hartenstein and K. P. Laberteaux, "A tutorial survey on vehicular ad hoc networks;" IEEE Communications Magazine, vol. 46, no. 6, pp. 164–171, 2008.
[5] X. Lin, R. Lu, C. Zhang, H. Zhu, P.-H. Ho, and X. Shen, "Security in vehicular ad hoc networks [security in mobile ad hoc];" IEEE Communications Magazine, vol. 46, no. 4, pp. 88–95, 2008.
[6] C. Zhang, R. Lu, X. Lin, P.-H. Ho, and X. Shen, "An efficient identity-based batch verification scheme for vehicular sensor networks;" in Proceedings of the 27th IEEE Communications Society Conference on Computer Communications INFOCOM, pp. 816–824, April 2008.
[7] M. Boban, O. Tonguz, and J. Barros, "Unicast communication in vehicular ad hoc networks: a reality check;" IEEE Communications Letters, vol. 13, no. 12, pp. 995–997, 2009.
[8] C.-C. Huang-Fu, Y.-B. Lin, and N. Alrajeh, "Mobility management of unicast services for wireless access in vehicular environments;" IEEE Wireless Communications, vol. 19, no. 2, pp. 88–95, 2012.
[9] "IEEE Trial-use standard for wireless access in vehicular environments—security services for applications and management messages;" IEEE Std 1609. 2-2006, pp. 1–105, 2006.
[10] M. Raya, P. Papadimitratos, and J.-P. Hubaux, "Securing vehicular communications;" IEEE Wireless Communications, vol. 13, no. 5, pp. 8–15, 2006.
[11] A. Suwannasa and S. Puangprupmit, "A fast and efficient authentication scheme for WAVE unicast services in vehicular networks;" in In Proceedings of The IEEE International Conference on Ubiquitous and Future Networks, pp. 240–245, Da Nang, Vietnam, July 2013.
[12] "IEEE draft standard for wireless access in vehicular environments (WAVE)— multi-channel operation;" IEEE P1609. 4/D9, 2010.
[13] C.-C. Huang-Fu, C.-L. Chen, and Y.-B. Lin, "Location tracking for WAVE unicast service;" in Proceedings of the IEEE 71st Vehicular Technology Conference (VTC ’10), May 2010.
[14] Y. B. Lin and A. C. Pang, Wireless and Mobile All-IP Networks, John Wiley & Sons, New York, NY, USA, 2005.
[15] A. Shamir, "Identity-based cryptosystems and signature schemes;" in Proceedings of Advances in Cryptology, vol. 196, pp. 47–53, New York, NY, USA, 1985.
[16] Z. Zhang, A. Boukerche, and H. Ramadan, "Design of a lightweight authentication scheme for IEEE 802.11p vehicular networks;" Ad Hoc Networks, vol. 10, no. 2, pp. 243–252, 2012.
[17] "The Network Simulator-ns-2;" http://www.isi.edu/nsnam/ns/.
[18] F. Bai, N. Sadagopan, and A. Helmy, "Important: a framework to systematically analyze the impact of mobility on performance of routing protocols for ad hoc networks;" in Proceedings of the 22nd Annual Joint Conference on the IEEE Computer and Communications Societies, pp. 825–835, April 2003.
[19] M. Emmelmann, B. Bochow, and C. C. Kellum, Vehicular Networking Automotive Applications and Beyond, Wiley, 1st edition, 2010.
[20] S. Eichler, "Performance evaluation of the IEEE 802.11p WAVE communication standard;" in Proceedings of the IEEE 66th Vehicular Technology Conference (VTC ’07), pp. 2199–2203, October 2007.
