Journal of Information Hiding and Multimedia Signal Processing ©2016 ISSN 2073-4212
Ubiquitous International Volume **7**, Number **5**, September **2016**

A Fast-Handover-Supported Authentication Protocol for Vehicular Ad Hoc Networks

Wei-Liang Tai

Department of Information Communications
Chinese Culture University
55, Hwa-Kang Road, Yang-Ming-Shan, Taipei, Taiwan
dwl@ulive.pccu.edu.tw

Ya-Fen Chang* and Yung-Chi Chen

Department of Computer Science and Information Engineering
National Taichung University of Science and Technology
No. 129, Sec. 3, Sanmin Rd., North Dist., Taichung, Taiwan
cyf@nutc.edu.tw; tina414099@gmail.com
*Corresponding author

Received January, 2016; revised June, 2016

Abstract. *Recently, Li and Liu proposed an identity authentication protocol for vehicular ad hoc networks (VANETs). They claimed their protocol ensured both efficiency and security and achieved fast handover with privacy protection. Later, Jia et al. show that their protocol is vulnerable to three drawbacks, protocol bottleneck, location detection, and parallel session attack. In this paper, we propose a fast-handover-supported authentication protocol for VANETs that ensures (1) location privacy, (2) fast handover, (3) security, and (4) the light computation load of AAA server.*
Keywords: Vehicular ad-hoc network, Fast handover, Authentication.

1. **Introduction.** Vehicular ad-hoc networks (VANETs) provide applications such as information exchange among vehicles, monitoring, and collision warning [1, 2]. In VANETs, each vehicle is configured with an on-board unit (OBU) to facilitate communication with a road-side unit (RSU). Some properties of mobile ad-hoc networks (MANETs) are familiar to VANETs. The greatest difference between VANETs and MANETs is that vehicles in VANETs possess high mobility. This results in long transmission delay and poor transmission reliability. Some unique communication standards [3, 4] are proposed to solve these problems. There exist two communication modes in VANETs: (1) vehicle-to-vehicle (V2V) and (2) vehicle-to-infrastructure (V2I). In the V2I mode, a vehicle connects to an RSU to access services, and a vehicle has to connect to a new RSU when it is about to leave the original RSU. The V2I mode is illustrated with FIGURE 1. In FIGURE 1, a vehicle first connects to RSU_1 through an authentication server's assistance to access services. When this vehicle is going to leave the service range of RSU_1, this vehicle will attempt to establish connection with RSU_2. After being authenticated, the vehicle can access services via RSU_2.

When a VANET is used to provide fee-based services such as network access, information download, and data search, how to ensure information exchanged securely becomes an important issue. Because data is transmitted through radio waves in VANETs, malicious users can easily eavesdrop and even counterfeit a registered vehicle to acquire services provided by the road-side units. When a VANET provides fee-based services, there are two important security considerations: (1) identity authentication and (2) confidentiality. Identity authentication denotes that road-side units and vehicles should be capable of authenticating the communication parties. Confidentiality denotes that an unauthorized third party cannot obtain the sensitive information transmitted by vehicles and road-side units.

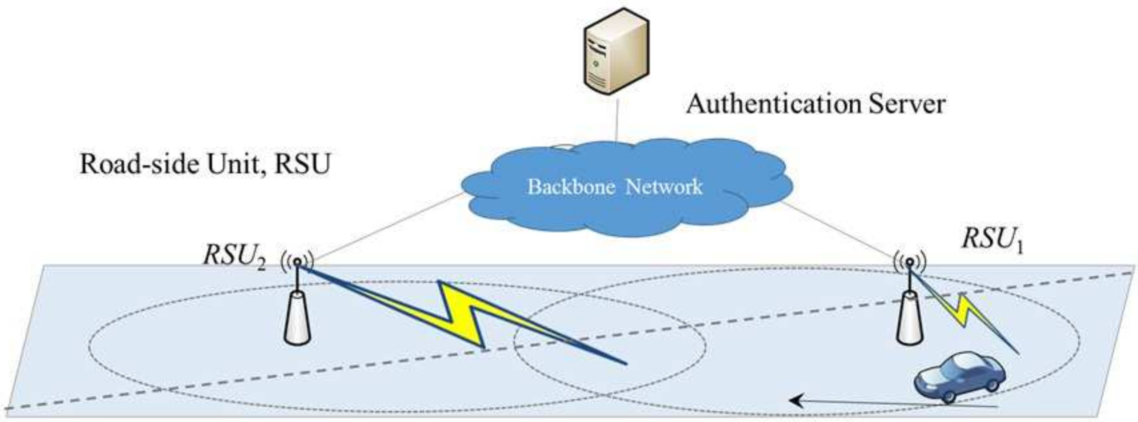

FIGURE 1. A vehicle and the road-side units in the V2I communication model

Because vehicles in VANETs are supposed to have high mobility, frequent handover operations are required. When a handover operation is executed, authentication is required. Authentication may place burdens on the whole system and may interrupt the service. As a result, how to authenticate a vehicle for fast handover while ensuring the security of sensitive information at the same time becomes the key to successful VANET applications. Information exchanged in VANETs is under the threat of active and passive attacks due to the characteristics of the transmission media. Active attack means that an attacker counterfeits a legitimate device to cheat a legal vehicle or a road-side unit, and passive attack means that an attacker can intercept the transmitted but not protected data to obtain sensitive information.

To ensure security in VANETs, information privacy, location privacy, and identity authentication become essential security requirement [5, 6]. In order to achieve the security requirements mentioned above, the asymmetric or symmetric cryptosystem is commonly used to design the protection and authentication mechanisms. In VANETs, vehicles possess high mobility such that the connection time of a vehicle and an RSU is short. If authentication between vehicles and RSUs adopts the asymmetric or symmetric cryptosystem, this may interrupt the service because these systems are more complex and the required computations are more time-consuming. As a result, specific approaches are employed for authentication in VANETs. Up to present, these approaches can be divided into five categories:

(1) Pre-authentication approach: Vehicles are allowed to establish connection with several RSUs at the same time [7].

(2) Identity-based cryptographic approach: Via this approach, the user's identity is his public key. This can remove the burden to verify the certificate before the corresponding public key is used [8-12].

(3) Pre-key distribution approach: Via this approach, the key or information needed for authentication will first be sent to an RSU nearby [13-16], or it will be sent in advance to RSUs that are predicted in the path[17, 18].

(4) Symmetric cryptographic approach: Via this approach, all RSUs share a secret key. This makes key distribution unneeded [19].

(5) Asymmetric cryptographic approach: Mechanisms adopting this approach use public-key cryptosystems for key distribution and authentication [20].

In the above methods [7-20], authentication between vehicles and RSUs still requires complex computations, which will likely result in failed handover. In 2013, Li and Liu proposed an identity authentication protocol for VANETs [21]. They claimed that their protocol ensured both efficiency and security and achieved fast handover authentication with privacy protection. In 2015, Jia et al. showed that Li and Liu's protocol is vulnerable to three drawbacks, protocol bottleneck, location detection, and parallel session attack [22]. How to overcome these drawbacks and preserve the advantages becomes an urgent issue. In this paper, we propose a fast-handover-supported authentication protocol for VANETs that ensures (1) location privacy, (2) fast handover, (3) security, and (4) the light computation load of AAA server.

The rest of this paper is organized as follows. The proposed protocol is shown in Section 2 followed by property and security analyses in Section 3. At last, some conclusions are drawn in Section 4.

Table 1. The notations

Symbol	Definition
V_i	the ith vehicle
OBU_i	V_i's on-board unit
RSU_j	the jth road-side unit
AS	AAA server for authentication, authorization and accounting
UID_i	the identity of the user who applies for the service with V_i
PWD_i	the password of the user who applies for the service with V_i
RID_j	RSU_j's identity
x	the secret shared between AS and all vehicles
y	the secret shared between AS and all road-side units
K_i	the secret shared between AS and V_i
A_j	the secret shared between AS and RSU_j
$F()$	a function used to compute K_i
$h(.)$	a secure one-way hash function
TS_O	a timestamp generated by an entity O
w	a periodically updated secret for authentication
LT	w's lifetime
z	the secret seed that AS uses to generate w
$\|$	a concatenation operator
$\oplus$	a bitwise exclusive-or operator

2. **The Proposed Protocol.** To overcome the drawbacks that Li and Liu's protocol suffers from, we propose a fast-handover-supported authentication protocol for VANETs. The notations used in our protocol are listed in TABLE 1. Before this protocol proceeds, the Internet Service Provider (ISP) first needs to initialize the environment by the following. The ISP loads x into all on-board units, y into all road-side units, and A_j into RSU_j. V_i's user needs to apply to the ISP for services. After successful registration, V_i's user will get a dedicated identity UID_i and the corresponding password PWD_i. When

V_i's user enters UID_i and PWD_i into OBU_i, the smart card embedded in OBU_i computes $K_i = F(UID_i \parallel PWD_i)$ and saves it. The ISP initializes AS by storing x, y, z, (UID_i, K_i)'s and (RID_j, A_j)'s. Note that AS also maintains a register table to store the current connection of each joined vehicle. The proposed protocol consists of four phases: (1) RSU initialization phase, (2) vehicle initialization phase, (3) fast handover authentication phase, and (4) renewal phase. The details are as follows.

2.1. **RSU initialization phase.** When a new road-side unit RSU_j is added to the VANETs, the following steps will be performed. RSU initialization phase is illustrated in FIGURE 2, and the details are as follows:

Step 1: RSU_j computes $m_1 = h(TS_j \parallel RID_j \parallel y \parallel A_j)$ and sends an initialization request $\{TS_j, RID_j, m_1\}$ to AS.

Step 2: After getting RSU_j's request, AS uses RID_j to find A_j and checks TS_j with the current time. If this request is fresh, AS computes $h(TS_j \parallel RID_j \parallel y \parallel A_j)$ and checks if m_1 and the computation result are equal. If they are not equal, AS terminates this phase immediately; otherwise, AS computes $m_2 = h(TS_{AS} \parallel m_1 \parallel y \parallel A_j)$, $m_3 = m_2 \oplus w$, $m_4 = m_2 \oplus LT$, and $m_5 = h(TS_{AS} \parallel m_1 \parallel RID_j \parallel w \parallel LT \parallel y \parallel A_j)$. Then AS sends $\{TS_{AS}, m_3, m_4, m_5\}$ to RSU_j.

Step 3: After getting AS's reply, RSU_j checks whether TS_{AS} is valid. If TS_{AS} is valid, RSU_j computes $m_6 = h(TS_{AS} \parallel m_1 \parallel y \parallel A_j)$, $w = m_3 \oplus m_6$, and $LT = m_4 \oplus m_6$ and checks if $m_5 = h(TS_{AS} \parallel m_1 \parallel RID_j \parallel w \parallel LT \parallel y \parallel A_j)$. If it holds, RSU_j stores (LT, w); otherwise, RSU_j resends an initialization request.

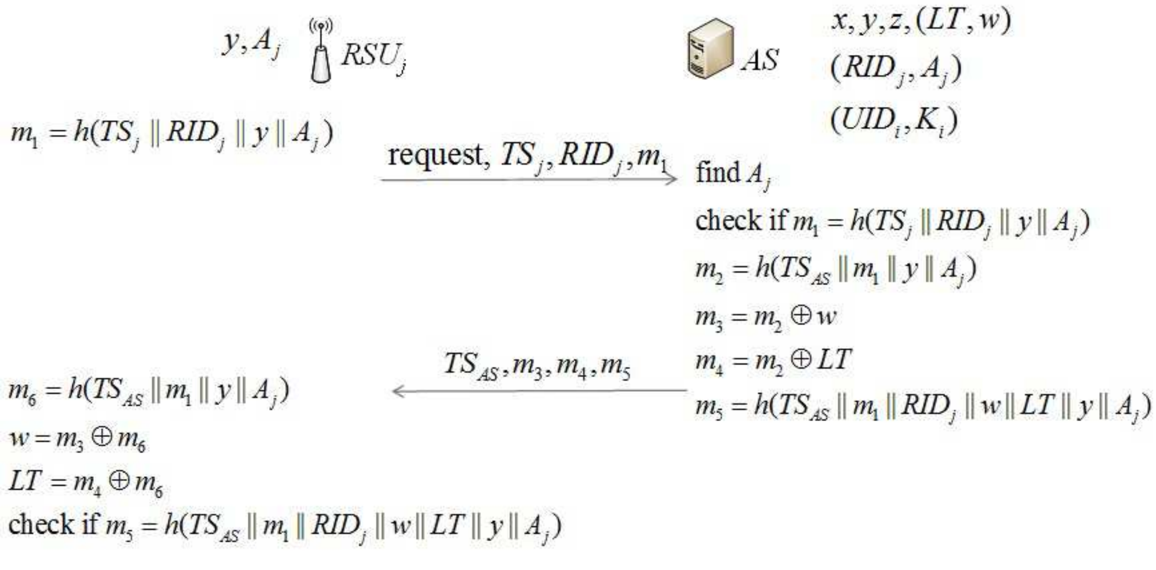

FIGURE 2. RSU initialization phase

2.2. **Vehicle initialization phase.** When a new vehicle V_i joins the network, the following steps will be performed. Vehicle initialization phase is illustrated in FIGURE 3, and the details are as follows:

Step 1: V_i sends an initialization request to the nearest road-side unit, RSU_j.

Step 2: After getting V_i's request, RSU_j computes $m_1 = h(TS_j \parallel RID_j \parallel y \parallel A_j)$ and sends $\{RID_j, TS_j, m_1\}$ to V_i.

Step 3: After getting RSU_j's reply, V_i checks whether TS_j is valid. If TS_j is valid, V_i computes $m_2 = h(TS_j \parallel RID_j \parallel x) \oplus UID_i$ and $m_3 = h(m_1 \parallel m_2 \parallel K_i)$. Then V_i sends $\{m_2, m_3\}$ to RSU_j.

Step 4: After getting $\{m_2, m_3\}$, RSU_j sends $\{RID_j, TS_j, m_1, m_2, m_3\}$ to AS.

Step 5: Upon receiving $\{RID_j, TS_j, m_1, m_2, m_3\}$ from RSU_j, AS checks whether TS_j is valid. If it is valid, AS uses RID_j to find the corresponding A_j and checks if m_1 and $h(TS_j \parallel RID_j \parallel y \parallel A_j)$ are equal. If they are not equal, AS rejects this request immediately; otherwise, AS computes $UID_i = m_2 \oplus h(TS_j \parallel RID_j \parallel x)$, uses the obtained UID_i to find K_i, and checks if $m_3 = h(m_1 \parallel m_2 \parallel K_i)$. If it does not hold, AS rejects this request immediately; otherwise, AS makes sure that RSU_j and V_i are legitimate. Then AS computes $w = h(LT \parallel z)$, $m_4 = h(TS_{AS} \parallel m_1 \parallel m_3 \parallel UID_i \parallel K_i)$, $m_5 = m_4 \oplus w$, $m_6 = m_4 \oplus LT$, $m_7 = h(TS_{AS} \parallel w \parallel LT \parallel RID_j \parallel K_i \parallel x)$, and $m_8 = h(TS_{AS} \parallel m_1 \parallel m_3 \parallel m_5 \parallel m_6 \parallel m_7 \parallel RID_j \parallel LT \parallel w \parallel y)$ and updates V_i's present connection to RSU_j in the register table. AS sends $\{TS_{AS}, m_5, m_6, m_7, m_8\}$ to RSU_j. Because w generated by AS for all vehicles and LT are the same, AS only needs to compute and store (LT, w) in its database once before w expires. That is, when w does not expire, AS does not need to recompute w even if a new road-side unit or a new vehicle sends a request.

Step 6: After getting $\{TS_{AS}, m_5, m_6, m_7, m_8\}$, RSU_j checks if TS_{AS} is fresh. If it is fresh, RSU_j checks if $m_8 = h(TS_{AS} \parallel m_1 \parallel m_3 \parallel m_5 \parallel m_6 \parallel m_7 \parallel RID_j \parallel LT \parallel w \parallel y)$. If it does not hold, RSU_j aborts the protocol; otherwise, V_i's legitimacy is ensured and RSU_j sends $\{TS_{AS}, m_5, m_6, m_7\}$ to V_i.

Step 7: When V_i gets the reply from RSU_j, V_i computes $m_9 = h(TS_{AS} \parallel m_1 \parallel m_3 \parallel UID_i \parallel K_i)$, $w = m_5 \oplus m_9$, and $LT = m_6 \oplus m_9$. Then V_i checks if $m_7 = h(TS_{AS} \parallel w \parallel LT \parallel RID_j \parallel K_i \parallel x)$. If it does not hold, V_i aborts the protocol and searches others legitimate road-side units; otherwise, V_i makes sure that RSU_j and AS are both legitimate and records (LT, w).

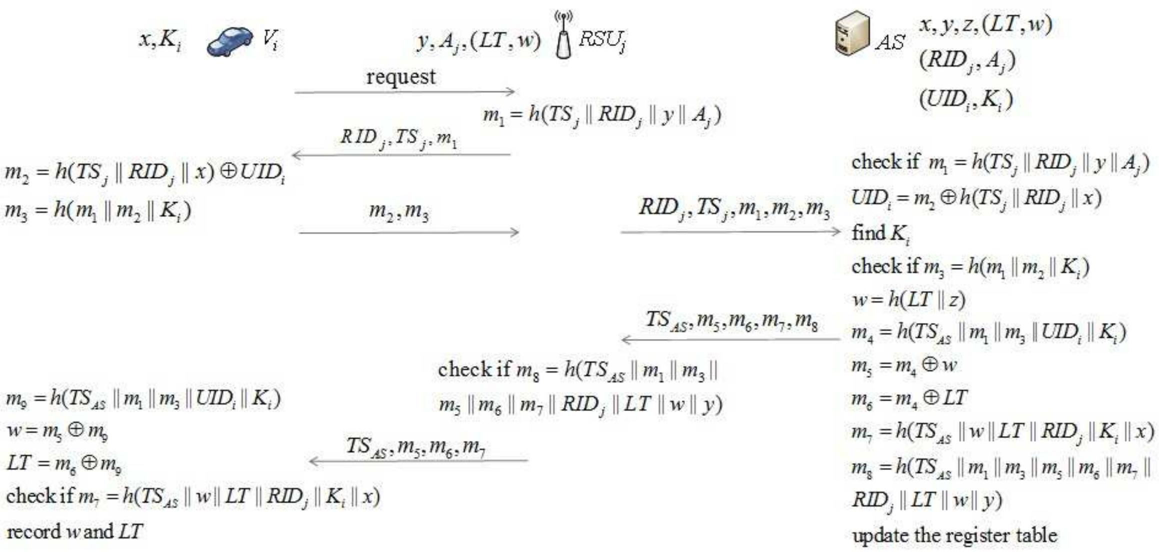

FIGURE 3. Vehicle initialization phase

2.3. **Fast handover authentication phase.** After vehicle initialization phase, V_i can access the Internet service via RSU_j. In VANETs, vehicles are supposed to possess high mobility so handover operations are required frequently. When V_i needs to access the Internet service via the new road-side unit RSU_{j+1} instead of the original road-side unit RSU_j, fast handover authentication phase is triggered. Fast handover authentication phase is illustrated in FIGURE 4, and the details are as follows:

Step 1: V_i sends a handover authentication request.

Step 2: After getting V_i's request, RSU_{j+1} computes $m_1 = h(TS_{j+1} \parallel RID_{j+1} \parallel LT \parallel w \parallel y)$ and sends $\{RID_{j+1}, TS_{j+1}, m_1\}$ to V_i.

Step 3: After getting RSU_{j+1}'s reply, V_i checks whether TS_{j+1} is valid. If it is valid, V_i computes $m_2 = h(TS_{j+1} \parallel RID_{j+1} \parallel LT \parallel w \parallel x) \oplus UID_i$ and $m_3 = h(TS_i \parallel RID_{j+1} \parallel m_1 \parallel m_2 \parallel LT \parallel w)$. V_i sends $\{TS_i, m_2, m_3\}$ to RSU_{j+1}.

Step 4: After receiving $\{TS_i, m_2, m_3\}$ from V_i, RSU_{j+1} checks if $m_3 = h(TS_i \parallel RID_{j+1} \parallel m_1 \parallel m_2 \parallel LT \parallel w)$. If it does not hold, RSU_{j+1} rejects this request immediately; otherwise, RSU_{j+1} makes sure that V_i is legitimate, provides V_i with services, and computes $m_4 = h(m_2 \parallel RID_{j+1} \parallel TS'_{j+1} \parallel LT \parallel w)$ and $m_5 = h(TS_{j+1} \parallel TS'_{j+1} \parallel RID_{j+1} \parallel m_2 \parallel LT \parallel w \parallel y \parallel A_{j+1})$, where TS'_{j+1} is a new timestamp generated by RSU_{j+1}. Then RSU_{j+1} sends $\{TS_{j+1}, TS'_{j+1}, RID_{j+1}, m_2, m_5\}$ and $\{TS'_{j+1}, RID_{j+1}, m_4\}$ to AS and V_i, respectively.

Step 5: When V_i gets the reply $\{TS'_{j+1}, RID_{j+1}, m_4\}$ from RSU_{j+1}, V_i checks if TS'_{j+1} is valid. If it is valid, V_i checks if $m_4 = h(m_2 \parallel RID_{j+1} \parallel TS'_{j+1} \parallel LT \parallel w)$. If it does not hold, V_i terminates this phase immediately; otherwise, V_i makes sure that RSU_{j+1} is legitimate.

Step 6: After getting $\{TS_{j+1}, TS'_{j+1}, RID_{j+1}, m_2, m_5\}$, AS checks whether TS_{j+1} and TS'_{j+1} are valid. If they are both valid, AS computes $UID_i = m_2 \oplus h(TS_{j+1} \parallel RID_{j+1} \parallel LT \parallel w \parallel x)$ and checks if $m_5 = h(TS_{j+1} \parallel TS'_{j+1} \parallel RID_{j+1} \parallel m_2 \parallel LT \parallel w \parallel y \parallel A_{j+1})$. If it holds, AS uses UID_i as the index to update the register table by updating V_i's present connection RSU_j to RSU_{j+1}; otherwise, AS informs RSU_{j+1} to terminate V_i's service. Note that if there is no information of V_i's present connection, AS informs RSU_{j+1} to terminate V_i's service as well such that vehicle initialization phase is triggered.

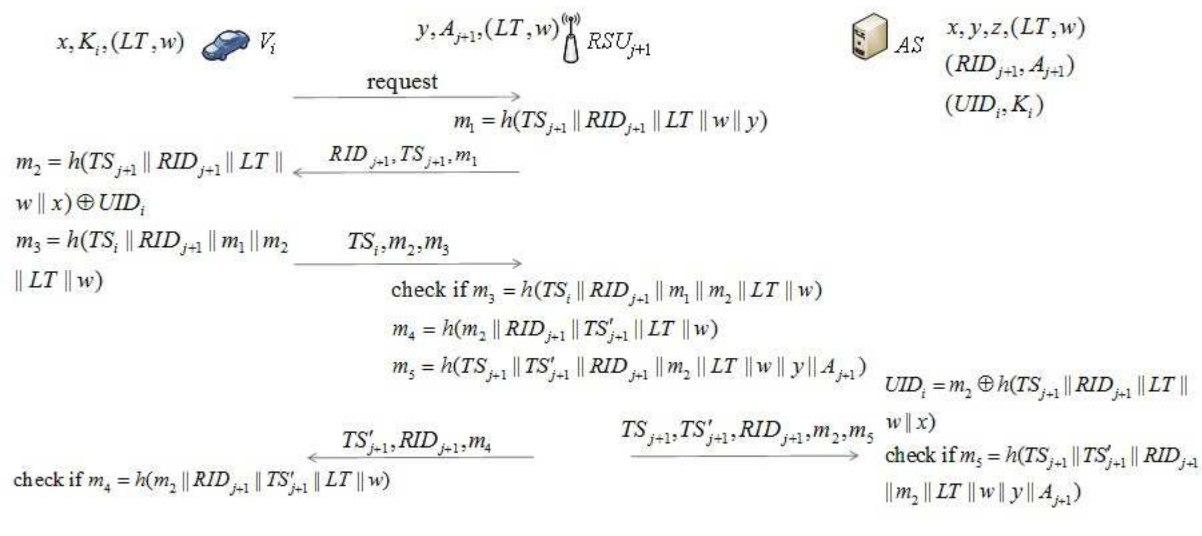

FIGURE 4. Fast handover authentication phase

2.4. **Renewal phase.** When w expires, V_i executes vehicle initialization phase, and AS broadcasts new (LT', w') to all road-side units. Renewal phase is illustrated in FIGURE 5, and the details are as follows:

Step 1: AS computes $w' = h(LT' \parallel z)$, $m_1 = h(TS_{AS} \parallel LT \parallel w \parallel y)$, $m_2 = m_1 \oplus LT'$, $m_3 = m_1 \oplus w'$, and $m_4 = h(TS_{AS} \parallel m_2 \parallel m_3 \parallel LT' \parallel w' \parallel y)$. AS sends $\{TS_{AS}, m_2, m_3, m_4\}$ to all road-side units.

Step 2: When RSU_j gets $\{TS_{AS}, m_2, m_3, m_4\}$ from AS, RSU_j checks whether TS_{AS} is valid. If it is valid, RSU_j computes $m_5 = h(TS_{AS} \parallel LT \parallel w \parallel y)$, $LT' = m_2 \oplus m_5$, and

$w' = m_3 \oplus m_5$. Then RSU_j checks if $m_4 = h(TS_{AS} \parallel m_2 \parallel m_3 \parallel LT' \parallel w' \parallel y)$. If it does not hold, RSU_j executes RSU initialization phase; otherwise, RSU_j updates (LT, w) to (LT', w').When RSU_j fails to get new (LT', w') because of the Internet failure or other factors, RSU_j executes RSU initialization phase as well.

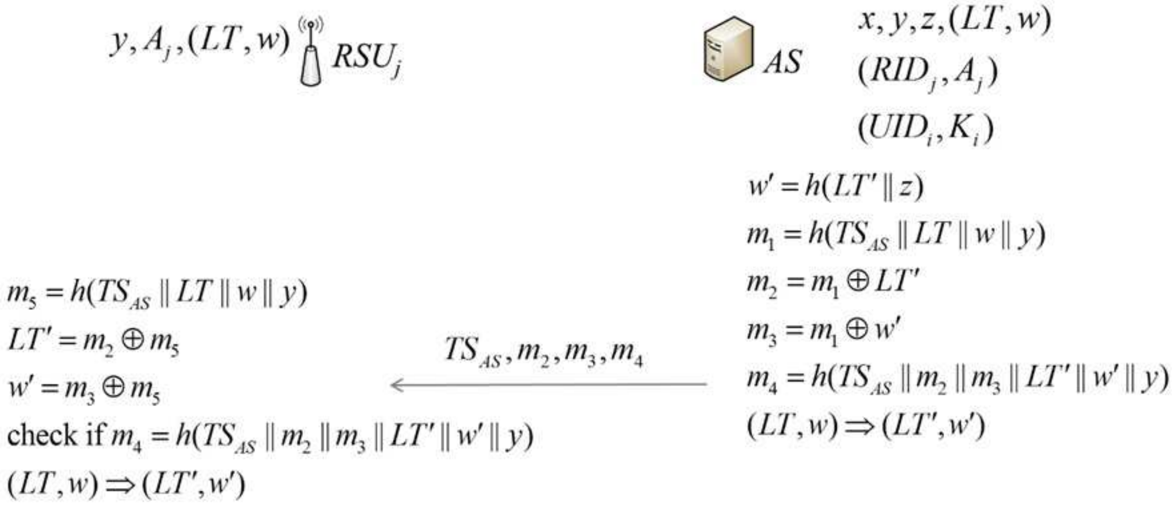

FIGURE 5. Renewal phase

3. **Property and security analyses.** This section first demonstrates that the proposed scheme can provide location privacy, fast handover, and the light computation load of AAA server. Then why the proposed scheme can resist common attacks such as offline attack, collaborative attack, and masquerade attack is given to show the proposed scheme ensures security as well. The details are as follows.

3.1. **Location privacy.** In fast handover authentication phase, an attacker may attempt to trace V_i's location. However, V_i does not transmit fixed parameters such that the attacker is incapable of tracing V_i's location. On the other hand, AS records $\{x, y, z, (LT, w), (RID_j, A_j), (UID_i, K_i)\}$ and RSU_j stores only $\{x, A_j, (LT, w)\}$ such that only the trusted AAA server AS knows V_i's location. That is, even if an RSU is compromised, no one can get V_i's location except AS.

3.2. **Fast handover.** Before this protocol proceeds, the ISP initializes the environment by the following. The ISP loads x into all on-board units, y into all road-side units, and A_j into RSU_j. When V_i needs to access the Internet service via the new road-side unit RSU_{j+1} instead of the original road-side unit RSU_j, fast handover authentication phase is triggered. In fast handover authentication phase, V_i sends $\{TS_i, m_2, m_3\}$ to RSU_{j+1}, where $m_2 = h(TS_{j+1} \parallel RID_{j+1} \parallel LT \parallel w \parallel x) \oplus UID_i$ and $m_3 = h(TS_i \parallel RID_{j+1} \parallel m_1 \parallel m_2 \parallel LT \parallel w)$. After receiving $\{TS_i, m_2, m_3\}$ from V_i, RSU_{j+1} checks if $m_3 = h(TS_i \parallel RID_{j+1} \parallel m_1 \parallel m_2 \parallel LT \parallel w)$. If it holds, RSU_{j+1} makes sure that V_i is legitimate and provides V_i with services. Then, RSU_{j+1} computes $m_4 = h(m_2 \parallel RID_{j+1} \parallel TS'_{j+1} \parallel LT \parallel w)$ and $m_5 = h(TS_{j+1} \parallel TS'_{j+1} \parallel RID_{j+1} \parallel m_2 \parallel LT \parallel w \parallel y \parallel A_{j+1})$ and sends $\{TS_{j+1}, TS'_{j+1}, RID_{j+1}, m_2, m_5\}$ and $\{TS'_{j+1}, RID_{j+1}, m_4\}$ to AS and V_i, respectively. Then AS computes $UID_i = m_2 \oplus h(TS_{j+1} \parallel RID_{j+1} \parallel LT \parallel w \parallel x)$ and checks if $m_5 = h(TS_{j+1} \parallel TS'_{j+1} \parallel RID_{j+1} \parallel m_2 \parallel LT \parallel w \parallel y \parallel A_{j+1})$. If it holds, AS uses UID_i as the index to update the register table by updating V_i's present connection RSU_j to RSU_{j+1}, and makes sure that RSU_{j+1} is legitimate; otherwise, AS informs RSU_{j+1} to terminate V_i's service. If there is no information of V_i's present connection, AS informs RSU_{j+1} to terminate V_i's service as well such that vehicle initialization phase is triggered. This approach makes handover can be proceeded as soon as possible because RSU_{j+1} first uses w to authenticate V_i. If V_i is authenticated successfully, RSU_{j+1} provides V_i with services immediately. Later, AS uses w to authenticate RSU_{j+1} and UID_i as an index to update V_i's present connection. The process that AS executes does not delay handover. On the other hand, after getting RSU_{j+1}'s reply $\{TS'_{j+1}, RID_{j+1}, m_4\}$, V_i checks if $m_4 = h(m_2 \parallel RID_{j+1} \parallel TS'_{j+1} \parallel LT \parallel w)$ to determine if RSU_{j+1} is legitimate. The process is for mutual authentication and does not delay handover as well. Consequently, our scheme ensures fast handover.

3.3. **The light computation load of AAA server.** In our proposed scheme, AS executes simple computational operations such as exclusive-or operation and one-way hash function. This approach makes the computation load of AS light and greatly removes the burden on AS. Consequently, AS will not be the bottleneck in the proposed scheme.

3.4. **Security.** Security is an important issue in all applications. We have shown that our scheme ensures location privacy, fast handover, and the light computation load of AAA server in the above. In the following, we show that the proposed scheme can resist common attacks such as offline attack, collaborative attack, and masquerade attack to demonstrate that it can provide security.

3.4.1. *Offline attack.* In RSU initialization phase, vehicle initialization phase, fast handover authentication phase, and renewal phase, messages are transmitted via the public but insecure channel. A malicious user can intercept the transmitted messages and try to analyze them to get sensitive data. In RSU initialization phase, an attacker can get $\{m_3, m_4, m_5\}$, where $m_2 = h(TS_{AS} \parallel m_1 \parallel y \parallel A_j)$, $m_3 = m_2 \oplus w$, $m_4 = m_2 \oplus LT$, and $m_5 = h(TS_{AS} \parallel m_1 \parallel RID_j \parallel w \parallel LT \parallel y \parallel A_j)$. In vehicle initialization phase, an attacker can get $\{m_1, m_2, m_3, m_5, m_6, m_7, m_8\}$, where $m_1 = h(TS_j \parallel RID_j \parallel y \parallel A_j)$, $m_2 = h(TS_j \parallel RID_j \parallel x) \oplus UID_i$, $m_3 = h(m_1 \parallel m_2 \parallel K_i)$, $m_4 = h(TS_{AS} \parallel m_1 \parallel m_3 \parallel UID_i \parallel K_i)$, $m_5 = m_4 \oplus w$, $m_6 = m_4 \oplus LT$, $m_7 = h(TS_{AS} \parallel w \parallel LT \parallel RID_j \parallel K_i \parallel x)$, and $m_8 = h(TS_{AS} \parallel m_1 \parallel m_3 \parallel m_5 \parallel m_6 \parallel m_7 \parallel RID_j \parallel LT \parallel w \parallel y)$. In fast handover authentication phase, an attacker can get $\{m_1, m_2, m_3, m_4, m_5\}$, where $m_1 = h(TS_{j+1} \parallel RID_{j+1} \parallel LT \parallel w \parallel y)$, $m_2 = h(TS_{j+1} \parallel RID_{j+1} \parallel LT \parallel w \parallel x) \oplus UID_i$, $m_3 = h(TS_i \parallel RID_{j+1} \parallel m_1 \parallel m_2 \parallel LT \parallel w)$, $m_4 = h(m_2 \parallel RID_{j+1} \parallel TS'_{j+1} \parallel LT \parallel w)$ and $m_5 = h(TS_{j+1} \parallel TS'_{j+1} \parallel RID_{j+1} \parallel m_2 \parallel LT \parallel w \parallel y \parallel A_{j+1})$. In renewal phase, an attacker can get $\{m_2, m_3, m_4\}$, where $m_1 = h(TS_{AS} \parallel LT \parallel w \parallel y)$, $m_2 = m_1 \oplus LT'$, $m_3 = m_1 \oplus w'$, and $m_4 = h(TS_{AS} \parallel m_2 \parallel m_3 \parallel LT' \parallel w' \parallel y)$. Although the attacker can eavesdrop to get the above information, he still cannot get any sensitive data such as w, y, x, K_i and A_j because they are all protected by the one-way hash function.

3.4.2. *Collaborative attack.* Collaborative attack is mounted on the proposed scheme when several legal users collaborate to get system secrets z, y, and A_j. Unfortunately, these malicious users will never succeed because they only know $\{w, x, K_i\}$ and z, y, and A_j are protected by the one-way hash function. That is, our scheme can defend against collaborative attack.

3.4.3. *Masquerade attack.* In vehicle initialization phase, the attacker may masquerade as a new vehicle V_i to join the network. However, the attacker has no way to get x and K_i to compute m_2 and m_3, where $m_2 = h(TS_j \parallel RID_j \parallel x) \oplus UID_i$ and $m_3 = h(m_1 \parallel m_2 \parallel K_i)$. When AS computes $UID_i = m_2 \oplus h(TS_j \parallel RID_j \parallel x)$, uses the obtained UID_i to find K_i, and checks if $m_3 = h(m_1 \parallel m_2 \parallel K_i)$ to authenticate V_i, only

V_i can be authenticated successfully. It is because only V_i knows K_i. That is, even if the attacker is a legal but malicious user and knows x, masquerade attack still cannot be mounted successfully because K_i is unknown. On the other hand, if the attacker wants to impersonate RSU_j to cheat a new vehicle, he will never succeed as well. It is because RSU_j sends $\{RID_j, TS_j, m_1, m_2, m_3\}$ to AS. AS records $\{(RID_j, A_j), (UID_i, K_i)\}$, uses RID_j to find the corresponding A_j, and checks if m_1 and $h(TS_j \parallel RID_j \parallel y \parallel A_j)$ are equal. If they are not equal, AS rejects this request immediately. Because only RSU_j knows A_j, only RSU_j can compute m_1. That is, only RSU_j can be authenticated by AS.

In fast handover authentication phase, an attacker may impersonate a road-side unit to cheat V_i. But, masquerade attack will not be mounted successfully because of the following. When V_i gets the reply $\{TS'_{j+1}, RID_{j+1}, m_4\}$ from RSU_{j+1}, V_i checks if TS'_{j+1} is valid. If it is valid, V_i checks if $m_4 = h(m_2 \parallel RID_{j+1} \parallel TS'_{j+1} \parallel LT \parallel w)$. If it does not hold, V_i terminates this phase immediately; otherwise, V_i makes sure that RSU_{j+1} is legitimate. Only legal road-side units know w so only legal road-side units can be authenticated successfully.

4. **Conclusions.** In this paper, we propose a fast-handover-supported authentication protocol for VANETs to overcome the drawbacks that Li and Liu's scheme suffers from. We have shown that the proposed scheme ensures (1) location privacy, (2) fast handover, (3) security, and (4) the light computation load of AAA server. Via these possessed properties, our scheme indeed suits VANETs possessing specific requirements.

Acknowledgment. This work was supported in part by Ministry of Science and Technology under the Grants MOST 103-2221-E-025-011, MOST 104-2221-E-034-004-, and MOST 104-2221-E-025-006-.

REFERENCES

[1] D. Jiang, V. Taliwal, A. Meier, W. Holfelder, and R. Herrtwich, Design of 5.9 GHZ DSRC-based vehicular safety communication, *IEEE Wireless Communications*, vol. 13, no. 5, pp. 36–43, 2006.

[2] S. Zeadally, R. Hunt, Y. S. Chen, A. Irwin, and A. Hassan, Vehicular ad hoc networks (VANETS): status, results, and challenges, *Telecommunication Systems*, vol. 50, no. 4, pp. 217–241, 2012.

[3] ASTM E2213-03, Standard Specification for Telecommunications and Information Exchange Between Roadside and Vehicle Systems - 5 GHz Band Dedicated Short Range Communications (DSRC) Medium Access Control (MAC) and Physical Layer (PHY) Specifications, *ASTM International*, West Conshohocken, PA, 2010.

[4] D. Jiang and L. Delgrossi, IEEE 802.11p: towards an international standard for wireless access in vehicular environments, *Proc. of the 67th IEEE Vehicular Technology Conference (VTC2008)*, Singapore, pp. 2036–2040, 2008.

[5] Y. M. Chen and Y. C. Wei, SafeAnon: a safe location privacy scheme for vehicular networks, *Telecommunication Systems*, vol. 50, no. 4, pp. 339–354, 2012.

[6] M. Raya and J. P. Hubaux, Securing vehicular ad hoc networks, *Journal of Computer Security*, vol. 15, no. 1, pp. 39–68, 2007.

[7] M. Gast, *802.11 wireless networks: the definitive guide*, O'Reilly Media, 2005.

[8] R. Lu, X. Lin, H. Zhu, P. H. Ho, and X. Shen, ECPP: efficient conditional privacy preservation protocol for secure vehicular communications, *Proc. of the 27th IEEE International Conference on Computer Communications (INFOCOM 2008)*, USA, pp. 1229–1237, 2008.

[9] C. Zhang, R. Liu, P. H. Ho, and A. Chen, A location privacy preserving authentication scheme in vehicular networks, *Proc. of the 2008 IEEE Wireless Communications and Networking Conference (WCNC 2008)*, USA, pp. 2543–2548, 2008.

[10] Y. Kim, W. Ren, J. Y. Jo, M. Yang, Y. Jiang, and J. Zheng, SFRIC: a secure fast roaming scheme in wireless LAN using ID-based cryptography, *Proc. of the 2007 IEEE International Conference on Communications (ICC 2007)*, Scotland, pp. 1570–1575, 2007.

[11] K. Masmoudi and H. Afifi, Building identity-based security associations for provider-provisioned virtual private networks, *Telecommunication Systems*, vol. 39, no. 3-4, pp. 215–222, 2008.

[12] D. Boneh and M. K. Franklin, Identity-based encryption from the Weil pairing, *Proc. of the 21st Annual International Cryptology Conference on Advances in Cryptology (CRYPTO 2001)*, USA, pp. 213–229, 2001.

[13] H. Wang and A. R. Prasad, Fast authentication for inter-domain handover, *Proc. of the 11th International Conference on Telecommunications (ICT 2004)*, Brazil, pp. 973–982, 2004.

[14] K. Hong, S. Jung, and S. F. Wu, A hash-chain based authentication scheme for fast handover in wireless network, *Proc. of the 6th International Workshop on Information Security Applications (WISA 2005)*, Korea, pp.96–107, 2005.

[15] J. H. Park and Q. Jin, Effective session key distribution for secure fast handover in mobile networks, *Telecommunication Systems*, vol. 44, no. 1-2, pp. 97–107, 2010.

[16] C. T. Lin and S. P. Shieh, Chain authentication in mobile communication systems, *Telecommunication Systems*, vol. 13, no. 2-4, pp. 213–240, 2000.

[17] A. Mishra, M. H. Shin, N. L. Jr. Petroni, T. C. Clancy, and W. A. Arbaugh, Proactive key distribution using neighbor graphs, *IEEE Wireless Communication Magazine*, vol. 11, no. 1, pp. 26–36, 2004.

[18] S. Pack and Y. Choi, Fast handoff scheme based on mobility prediction in public wireless LAN systems, *IEE Proceedings-Communications*, vol. 151, no. 5, pp. 489–495, 2004.

[19] J. Choi, S. Jung, Y. Kim, and M. Yoo, A fast and efficient handover authentication achieving conditional privacy in V2Inetworks, *Proc. of the 9th International Conference on Next Generation Wired/Wireless Networking (NEW2AN 2009)*, Russia, pp. 291–300, 2009.

[20] S. Ohzahata, S. Kimura, and Y. Ebihara, A fast authentication method for secure and seamless handoff, *Proc. of the 2002 International Conference on Information Networking, Wireless Communications Technologies and Network Applications (ICOIN 2002)*, Korea, pp. 243–252, 2002.

[21] J. S. Li and K. H. Liu, A lightweight identity authentication protocol for vehicular networks, *Telecommunication Systems*, vol. 53, no. 4, pp. 425–438, 2013.

[22] X. D. Jia, Y. F. Chang, C. C. Chang, and L. M. Wang, A critique of a lightweight identity authentication protocol for vehicular networks, *Journal of Information Hiding and Multimedia Signal Processing*, vol. 6, pp. 2073–4212, 2015.