Chameleon Hashing Based Message Authentication, Private Communication and Revocation in Vehicular Ad Hoc Networks

Chih Hsueh Lin1, Alan Dahgwo Yein3, Wen-Shyong Hsieh1,2, Zhong-Ting Luo2
1Department of Computer and Communication, Shu-Te University
2Department of Computer Science and Engineering, National Sun Yat-sen University
3Department of Information Management, Shu-Te University,
josuslin@stu.edu.tw, alanyein@stu.edu.tw, wshsieh@stu.edu.tw, M013040085@student.nsysu.edu.tw

Abstract
Vehicular Ad Hoc Networks (VANET) is a mobile communication technology that involves the moving vehicles or transport facilities, uses wireless communication technology, and embeds the wireless device on vehicles to constitute a mobile network. In this paper, we proposed the Chameleon Hashing Based Message Authentication, Private Communication and Revocation in Vehicular Ad Hoc Networks. In the proposed scheme, TA and RSU keep secret values to be as the issuers that give neighbour RSUs or vehicles the public (anonymous) identity that are embedded a public chameleon hash value published by TA or RSU. Based on the chameleon hash function, the public identity can be verified. Associated the public identity, a personal value will be issued confidentially to represent they are owners of the public identity. All vehicles and RSUs register with TA to obtain public identities and personal values. Using the public identity, a vehicle can proposes anonymous request to RSU for anonymous identity and new personal value. Combined the techniques of chameleon hash function, HAMC and Diffie-Hellman key exchange, the vehicles under a RSU, can make message authentication, multicast or unicast communicating confidentially. When malicious attackers occur, TA and RSU can check the register table, which record public identity and anonymous identity, to revoke attacker’s identity in the revocation list. The proposed scheme satisfies the security requirements of VANET, such as message and identity authentication, non-repudiation, confidentiality, conditional anonymity and un-traceability.

Keywords : VANETs, Chameleon Hashing, Key Agreement, Anonymous Authentication, Revocation.

1. INTRODUCTION
VANET provides convenient wireless network services, which is involved by a trusted authorizer (TA), many road side units (RSU) and vehicles. In VANET, the vehicles can broadcast, exchange, or receive the message about road condition, traffic situation, vehicle position or vehicle speed to avoid accident or prevent the traffic jam to be even worse. For the privacy of vehicles, the message will be sent anonymously, so how to authenticate the validity of message is an important issue in VANET.

In VANET, then communication can be classified into two types: vehicle-to-vehicle communication and vehicle-to-RSU communication. In the first scenario, each vehicle can broadcast message to other vehicles or send message to the specific vehicles, in this scenario, the vehicles must take care the privacy, confidentiality and message authentication by themself. In the second scenario, RSU can help the vehicles under the coverage of this RSU to make privacy, confidentiality and message authentication.

In VANET, The message authentication is to make sure that the receiving message is valid and is sent by a legal vehicle. For the privacy, the real identity of vehicle can’t be explored and traced. In this paper, the chameleon hash function, HAMC and Diffie-Hellman key exchange are used to build an environment that the vehicles can get anonymous, communicate confidentially, make message authentication, and prevent the malicious attacking under the assistance of RSU.

2. RELATED WORKS
Many literatures have been proposed, with a variety of security and privacy mechanisms of VANETs.

In 2008, the researcher proposed literature of Efficient conditional privacy preservation (ECPP)(Rongxing & Xiaodong & Haojin & Han & Xuemin, 2008), it provides the anonymous authentication for secure message with authority traceability, and generation of short-time anonymous keys between RSUs and OBUs, the keys can provide anonymous authentication and privacy tracking. It overcome original of numerous anonymous certificate’s restriction.
In the efficient distributed-certificate-service (DCS) (Wasef & Jiang & Shen, 2010). The important concept of the system architecture is making generation of key from MA-CA-RSU-OBU, have the features of reliability, uniqueness and receiver can know the key who was sent. And offers flexible interoperability for certificate service efficiently, when OBUs want to update its certificate, whether OBUs was registered from RSU and moved out to another RSU, also can update certificate from other RSUs.

The pseudonymous authentication scheme with strong privacy preservation (PASS) was proposed in 2010 (Sun & Lu & Lin & Shen & Su), unlike traditional pseudonymous authentication schemes, which is pseudonymous certificates are held by revoked vehicles. PASS is linear with the number of revoked vehicles, and supports the roadside unit RSU-aided distributed certificate service to update certificates on the road, and compared with DCS, it reduces the overhead of certificates updating. It provides strong privacy perservation to the vehicles, so the malicious attackers can not trace vehicles. However, PASS utilize bilinear pairing mechanism for generation and verification of signature, and it will increase the computation of authentication.

In Chen & Zhang & Susilo & Mu, 2007 Shamir and Tauman were designed an efficient on-line/off-line signature scheme, and used one-time trapdoor /hash key pair for each family based on the discrete logarithm, and utilize “hash-sign-switch” paradigm to propose more efficient generic on-line/off-line signature scheme, and it was proposed the special double-trapdoor hash family of chameleon hashing. In oder to solve problem, signature scheme endure the key exposure problem of chameleon hashing. In order to solve problem, thesis was proposed the special double-trapdoor hash family based on the discrete logarithm, and utilize “hash-sign-switch” paradigm. However, all on-line/off-line signature scheme endure the key exposure problem of chameleon hashing. In order to solve problem, thesis was proposed the special double-trapdoor hash family based on the discrete logarithm, and utilize “hash-sign-switch” paradigm to propose more efficient generic on-line/off-line signature scheme, and use one-time trapdoor/hash key pair for each message signing, and can prevent computing collisions.

3 BACKGROUND

In this section, we will introduce the proposed scheme used of technologies. Chameleon Hashing, Hash-Sign-Switch Paradigm, Elliptic Curve cryptosystem and Diffie-Hellman Key Exchange.

3.1 Chameleon Hashing

We introduce the basic notion of chameleon hash family (Chen & Zhang & Susilo & Mu, 2007).

A chameleon hash family consists of a pair $(f, H)$: $I$ is a probabilistic polynomial-time key generation algorithm that on input $1^k$, the outputs a pair $(HK, TK)$ such that the sizes of $HK, TK$ are polynomially related to $k$. $H$ is a family of randomized hash functions. Every hash function in $H$ is associated with a hash key $HK$, and is applied to a message from a space $M$ and a random element from a finite space $R$.

According to above described about chameleon hash family $(I, H)$, and has the following properties: Efficiency, collision resistance, trapdoor collision.

3.2 Elliptic Curve Cryptosystem

Elliptic curves was proposed for cryptography (Miller, 1986) and base upon the difficulty of elliptic curve discrete logarithm problem (ECDLP).

We use security of elliptic curve cryptosystem in our scheme. In the finite group $F_p^*$, given two different points $P$ and $Q$ on elliptic curve. The equation is $Q = s \cdot P$, it is hard to find a integer value $s$, where $P$ is larger than 160 bits.

3.3 Diffie-Hellman Key Exchange

Diffie-Hellman key exchange (D-H) is a specific method of exchanging cryptographic keys, and this security protocol method was proposed in 1976.

The security of D-H public key distribution scheme is based on discrete logarithm problem: Discrete Logarithm Problem (DLP): Given a large prime number $n$ and number of generation $g$. Calculate $1 \leq x \leq q - 1$ and satisfy $g^x \equiv b \pmod{n}$, where $b \in Z_q^*$ is well known, $Z_q^*$ is collection of all real numbers and base is $q$. Diffie-Hellman Problem (DHP): Given $g^a \pmod{n}$ and $g^b \pmod{n}$, demand to calculate $c = ab \pmod{q}$, where $a$, $b$, $c$ are unknown numbers.

4 THE PROPOSED SCHEME

We proposed the method which is using Elliptic Curve Cryptosystem as foundation. Introducing message authentication, private communication, revocation, and mutual authentication in Sparse RSU. Vehicles can utilize chameleon hash value to verify vehicle’s identity whether are legal, protect its privacy and utilize Diffie-Hellman to generate session key to communicate with other vehicles.

Table 4.1. Shows the notations used in this thesis.

<table>
<thead>
<tr>
<th>Notation</th>
<th>Descriptions</th>
</tr>
</thead>
<tbody>
<tr>
<td>$f(.)$</td>
<td>A cryptographic secure hash function: $f : Z_q \times G \rightarrow Z_q$</td>
</tr>
<tr>
<td>$P$</td>
<td>The generator of the cyclic group $G$</td>
</tr>
<tr>
<td>$Y_{TA}, Y_{B_i}$</td>
<td>$Y$ equal to $x$ multiplied by $P$</td>
</tr>
<tr>
<td>$CH_{TA}, CH_{B_i}$</td>
<td>Chameleon hash value of TA and RSU</td>
</tr>
<tr>
<td>$\alpha, x$</td>
<td>The secret value of RSU</td>
</tr>
<tr>
<td>RID</td>
<td>The identity of RSU</td>
</tr>
</tbody>
</table>
4.1 Initialization and Registration

4.1.1 System Initialization

The TA initializes the system by following steps:
1. TA chooses random numbers $a_{xTA}, x_{xTA} \in Z_q$.
2. TA selects a hash function $H: \{0, 1\} \rightarrow Z_q^*$.
3. TA sets $f: Z_q \times G \rightarrow Z_q$.
4. TA sets $Y_{TA} = x_{xTA}P$, and $C_{HTA} = a_{xTA}Y_{TA}$.
5. TA publishes $(C_{HTA}, H, Y_{TA}), P, f$, and keeps $(a_{xTA}, x_{xTA})$ as its own secret values.

The Ri initializes the system by following steps:
1. Ri chooses random numbers $a_{xRi}, x_{xRi} \in Z_q$.
2. Ri sets $Y_{Ri} = x_{xRi}P$, and $C_{HRi} = a_{xRi}Y_{Ri}$.
3. TA publishes $(C_{HRi}, Y_{Ri})$, and keeps $(a_{xRi}, x_{xRi})$ as its own secret values.

4.1.2 Registration

Supposed the RSU $R_i$ registers with TA and steps are described as following processes:
1. TA sets $CH: Z_q \times Z_q \rightarrow G$, $CH = f(m, K) \cdot K + rY$.
2. $R_i$ sends public identity, $RID_{Rik}$ to $R_k$, where $RID_{Rik}$ is $R_i$’s authorized identity.
3. $R_k$ chooses a random number $k_{Rk} \in Z_q$, computes $K_{Rk} = k_{Rk}P$ to $R_k$. $R_k$ sets $m_{Rk} = RID_{Rik} \parallel K_{Rk}$, and utilizes the chameleon hash function to calculate secret value $r_{Rk}$ as its secret value and $n$ sets of $(ID_{TA}, VID_{Vij}, K_{Vij}, r_{Vij})_{j=1 \rightarrow n}$ to $V_i$.
4. $V_i$ has $(VID_{Vij}, K_{Vij}, r_{Vij})_{j=1 \rightarrow n}$ holds $r_{Vij}$ as its secret value and $n$ sets of $(ID_{TA}, VID_{Vij}, K_{Vij}, r_{Vij})_{j=1 \rightarrow n}$ as its public identity.

TA maintains table to record registered parameters, in order to prevent the malicious attacks, TA can trace and revoke the malicious attacker’s identity in the revocation list.

4.2 RSU Acquires Neighbor RSU’s Authorized Identity

Supposed the RSU $R_i$ requests neighbor RSU $R_x$’s authorized identity, the steps are described as following process:
1. $R_i$ sends $CH: Z_q \times Z_q \rightarrow G$, $CH = f(m, K) \cdot K + rY$.
2. $R_x$ sends public identity, $RID_{Rix}$ to $R_k$, where $RID_{Rix}$ is $R_x$’s authorized identity.
3. $R_k$ utilizes $f(m_{Rk}, K_{Rk}) \cdot K_{Rk} + r_{Rk}Y_{TA}$ to verify whether is equal to $CH_{TA}$, if $CH_{TA}$ is equal, $R_x$ trusts these public identity are legal.
4. $R_k$ chooses a random number $k_{Rk} \in Z_q$, computes $K_{Rk} = k_{Rk}P$ to $R_k$. $R_k$ sets $m_{Rk} = RID_{Rik} \parallel K_{Rk}$, and utilizes the chameleon hash function to calculate secret value $r_{Rk}$ as its secret value and $n$ sets of $(ID_{TA}, VID_{Vij}, K_{Vij}, r_{Vij})_{j=1 \rightarrow n}$ as its public identity.
5. $R_x$ sends public identity, and encryption authorized parameters by key $S_{RxRk}$ to $R_k$, where $S_{RxRk} = (CH_{TA}(r_{Rk}Y_{TA}))^e$.
6. When $R_k$ received public identity, encryption authorized parameters, $R_k$ utilizes key $S_{RxRk} = (CH_{TA}R_{RxRk})$ to decrypt. If key equal, $R_k$ can obtain $(RID_{Rx}, RID_{RxRk}, K_{Rx}, K_{RxRk})$.
7. $R_k$ calculates $r_{Rk}Y_{Rx} \cdot Y_{Rx} = (r_{Rk}Y_{Rx})$ as authorized identity from $R_x$. 

Fig 4.1.2.1 Vehicle registers with TA
4.3 Vehicles Proposed Anonymous Request to RSU

V_i proposes anonymous request to RSU R_k, steps are described as following and flow chart in Fig 4.3.1:
1. R_k sets CH_TA \times Z_k \rightarrow G, CH = f(m, K) \cdot K + rY.
2. V_i chooses one set of the public identity and broadcast selected public identity, PID_{V_i,R_k} to R_k, where PID_{V_i,R_k} is V_i’s anonymous identity.
3. R_k utilizes public identity, f(m_{V_i,1}, K_{V_i,1}) \cdot K_{V_i,1} + r_{V_i,1} Y_{TA} to verify whether is equal to CH_{TA}, if CH_{TA} is equal, R_k trusts public identity are legal.
4. R_k chooses a random number k_{V_i,R_k} \in Z_q, computes K_{V_i,R_k} = k_{V_i,R_k} P, sets m_{R_k} = PID_{V_i,R_k}||K^2_{V_i,R_k}, utilizes chameleon hash function to calculate secret value r_{V_i,R_k}.
5. R_k sends public identity, encrypts anonymous parameters by key S_{R_k,V_i}, value N as challenge to V_i, where key S_{R_k,V_i} = (P(R_k V_i Y_{TA}))^x.
6. V_i received message from R_k, utilizes key S_{V_i,R_k} = (V_i Y_{TA})^x to decrypt message. V_i can acquire (RID_{R_k}, PID_{V_i,R_k}, K_{V_i,R_k}, r_{V_i,R_k}), value N, and responses E_{SV_{R_k,N}}(N+1) to R_k.
7. R_k utilizes key S_{R_k,V_i} to calculate E_{SV_{R_k,N}}(N+1) whether is equal N+1. If equal, R_k records V_i’s anonymous parameters in the table and broadcast V_i’s anonymous identity to other vehicles.
8. V_i holds (RID_{R_k}, PID_{V_i,R_k}, K_{V_i,R_k}, r_{V_i,R_k}, Y_{R_k}) as anonymous identity.

RSU maintains table and record registered parameters in the table. When vehicle proposed anonymous to RSU and obtained anonymous identity, the RSU broadcasts current table of recorded vehicle anonymous identity to vehicles in the same domain, and vehicles will maintain a table to record all of vehicle anonymous identity.

4.4 Intra-RSU Message Authentication

The V_b can authenticate with other vehicles(ie.V_c) in the R_k, we described as following processes:

1. V_b broadcasts anonymous identity, \( (M_{V_b}, \text{List of } HMAC_{SV_b,V_c}(M_{V_b} || T_{V_b}) ) \) to V_c, where key \( S_{V_b,V_c} = (V_b Y_{R_k})^x \).
2. V_c receives the anonymous identity, utilizes \( f(m_{R_k}, K_{V_b,R_k}) \cdot K_{V_b,R_k} + r_{V_b,R_k} Y_{R_k} \) to verify whether is equal to CH_{R_k}. If CH_{R_k} is equal, V_c trusts anonymous identity are legal.
3. V_c utilizes key \( S_{V_c,V_b} = (V_c Y_{R_k})^x \) to calculate the \( HMAC_{SV_b,V_c}(M_{V_b} || T_{V_b}) \) and examines list of broadcast message whether is equal to \( HMAC_{SV_b,V_c}(M_{V_b} || T_{V_b}) \).
4. If key and message are equal, V_c believes this message issued by V_b.

4.4.1 Transmitted Message to Specific Vehicles

V_b transmits message to specific vehicles V_c.s. Steps are described as following, flow chart in Fig 4.4.1.1:

1. V_b sets \( M = M_1 \oplus M_2, M_2 = M \oplus M_1 \).
2. V_b broadcasts anonymous identity, \( (M_1, \text{List of } HMAC_{SV_b,V_c}(M_1 || T_{V_b} ), \text{List of } M_2 \oplus SV_b,V_c ) \) to vehicle V_s, where \( S_{V_b,V_c}=(V_b Y_{R_k}(V_c Y_{R_k} Y_{R_b}))^x \).
3. V_c receives anonymous identity, V_c computes \( f(m_{R_k}, K_{V_b,R_k}) \cdot K_{V_b,R_k} + r_{V_b,R_k} Y_{R_k} \) to verify whether is equal to CH_{R_k}. If CH_{R_k} is equal, V_c trusts these anonymous identity are legal.
4. V_c utilizes key \( S_{V_c,V_b} = (V_c Y_{R_k})^x \) to calculate the \( HMAC_{SV_b,V_c}(M_1 || T_{V_b}) \) and examines list of broadcast message whether is equal to \( HMAC_{SV_b,V_c}(M_1 || T_{V_b}) \).
5. If key and message are equal, V_c believes message issued by V_b.
6. V_c utilizes \( S_{V_c,V_b} \) to calculate List of M_2 \oplus SV_b,V_c.
7. V_c computes M_1 \oplus SV_b,V_c \oplus S_{V_c,V_b} = M_2, M_1 \oplus M \oplus M_1 = M, V_c can obtain message M.
4.4.2 Establish Session Key to Communicate

Vehicle $V_b$ wants to establish session key with $V_c$ and flow chart in Fig 4.4.2.1:

1. $V_b$ chooses a random number $a \in \mathbb{Z}_q$, calculates $aP$. $V_b$ sends anonymous identity, $aP$, to $V_c$.
2. $V_c$ receives anonymous identity, computes $f(m_{V_b}, K_{V_b,R_b}) \cdot K_{V_c,R_c} + r_{V_b,R_b}Y_{R_b}$, and verify whether it is equal to $CH_{R_b}$. If the is $CH_{R_b}$ equal, $V_c$ trusts these anonymous identity are legal.
3. $V_c$ chooses a random number $b \in \mathbb{Z}_q$, calculates $bP$.
4. When $V_b$ receives message, $V_b$ computes $f((b(aP))^x) \parallel (V_{V_b,R_b} (V_{V_b,R_b} Y_{R_b}))^x$, sends anonymous identity, $bP$, $Csh_b$ back to $V_b$.
5. $V_b$ utilizes $V_{V_b,R_b}$, $a$ to compute challenge $Csh_b$. If $f((a(bP))^x) \parallel (V_{V_b,R_b} (V_{V_b,R_b} Y_{R_b}))^x$, $V_{V_b,R_b}$ is equal $Csh_b$, vehicles can utilize this method to establish session key.
6. The $V_b$ utilizes hash function to make session key $= H((a(bP))^x) \parallel (V_{V_b,R_b} (V_{V_b,R_b} Y_{R_b}))^x$.

4.5 Inter-RSU Authentication

After a period of time, $V_b$ moves to domain of $R_x$, $V_b$ proposes anonymous request to $R_x$ and get anonymous identity, we described as following and flow chart in Fig 4.5.1:

1. $V_b$ sends anonymous identity from $R_k$, PID$_{V_b,R_k}$ to $R_x$, where $PID_{V_b,R_k}$ is $V_b$ using as identity.
2. $R_x$ utilizes $f(m_{V_b}, K_{V_b,R_b}) \cdot K_{V_c,R_c} + r_{V_b,R_b}Y_{R_b}$ to verify whether is equal to $CH_{R_b}$. If $CH_{R_b}$ is equal, $R_x$ trusts anonymous identity are legal.
3. $R_x$ sends authorized identity from $R_k$, encryption anonymous parameters and value $N$ as challenge to $V_b$, where $key = (r_{V_b,R_b}, r_{V_c,R_c}, r_{V_b,R_b}Y_{R_b})$.
4. When $V_b$ received message, $V_b$ utilizes key $SV_{V_b,R_x} = (SV_{V_b,R_x} (SV_{V_b,R_x} Y_{R_b}))^x$ to decrypt. If key was equal, $V_b$ obtains (RID$_{V_b}$, PID$_{V_b,R_k}$, K$_{V_b,R_k}$, r$_{V_b,R_k}$), value N, responses $E_{SV_{V_b,R_x}}(N+1)$ to $R_x$. 
5. R_s utilizes S_{R_s,V_b} to calculate E_{S_{V_b,R_s}}(N+1), verify whether is equal N+1, if equal, records anonymous parameters in table and broadcasts anonymous identity to other vehicles.
6. R_s will inform to R_k, V_b was moved out and R_k will remove V_b’s anonymous identity in broadcasting list.

4.6 Authentication in Sparse RSU

We described this situation as following process and flow chart in Fig 4.6.1:
1. V_b wants to communicate with other vehicles, V_b broadcasts its public identity to other vehicles in the communication range, V_c received V_b’s public identity, V_c will maintain a table to record V_b’s public identity and also record other vehicles broadcast their public identity.
2. When the V_b wants to authenticate with other vehicles, V_s selects one set of the public identity and broadcast selected public identity, M_{V_b}, List of HMAV_{V_b, V_c}((M_{V_b} || T_{V_b})) to other vehicles V_c, where S_{V_b,V_c} = (v_{p,1}, (v_{c,1}T_{V_b}))
3. When V_c received the message and utilizes f(\text{mv}_{b,1}, K_{V_b,1}) \cdot K_{V_b,1} + v_{p,1} T_{V_b} to verify whether is equal to CH_{TA}. If the CH_{TA} is equal, V_c trusts these public identity are legal.
4. V_c utilizes key S_{V_b,V_c} = (v_{p,1}, (v_{c,1}T_{V_b}))^t to calculate the HMAV_{V_b, V_c}((M_{V_b} || T_{V_b})), and examines list of broadcast message whether is equal to HMAV_{V_b, V_c}((M_{V_b} || T_{V_b})).
5. If key and message are equal, V_c believes message was issued by V_b.

4.7 Revocation

In VANETs, revocation is required to prevent malicious vehicles execute malicious attacks on other legitimate vehicles.

Supposed the vehicle V_b has registered with TA, moved to domain of R_k and proposed anonymous request. When V_b performed malicious attack (i.e. forge or tamper) on other legitimate vehicles, the legitimate vehicle would have observed the violation and will report the violator V_b to the domain of R_k. And R_k looks up table, which was record vehicle’s anonymous parameters and knows V_b’s public identity based on has registered issued by TA, and report malicious attacker’s public identity to TA, TA will look up vehicle registered parameters, issue V_b’s registered parameters to all RSUs and revoke registered parameters in revocation list. According to above process, since vehicle does the behavior of violation, the vehicle’s identity has record in the revocation list, so the V_b cannot register with TA and proposed anonymous request to RSU again, so V_b cannot communicate with other vehicles.

5 SECURITY AND PERFORMANCE ANALYSIS

We illustrate the proposed schemes achieve the security requirement.

5.1 Security Analysis

We analyze the security of our proposed scheme.

Authentication and Non-Repudiation: When vehicle registered with TA and proposed anonymous request to RSU, and vehicles can get their own secret value r. According to TA and RSU publish CH=\text{f}(m, KJK + rY), vehicles can verify vehicle’s parameters whether are legal. if malicious attacker forges vehicle’s parameters, and forge parameters will not equal CH. Besides, the proposed scheme was based on elliptic curve cryptosystem, when malicious attacker wants to forge rY, because of elliptic curve discrete logarithm problem, it is difficult to calculate secret value.

Confidentiality: According to our proposed scheme, vehicle can negotiate common session key with each other vehicle in communication range. Based on property of the elliptic curve discrete logarithm problem and Diffie-Hellman key exchange methods, the vehicle utilize its own secret value and communication of vehicle’s secret value to make session key. Assume the malicious attacker want to forge the message, it is hard to find out vehicle secret value between vehicles. Other vehicles can’t know the vehicle’s secret value, so it is unable to calculate session key.

Efficiency: We using property of elliptic curve cryptosystem to make key, one of the property of ECC is the computation of point multiplication, and compare with pairings-based authentication scheme, and the proposed scheme is less computation loads for vehicles than pairing-based scheme, then the efficiency is ensured.

Scalability: The scalability is based on valid time of vehicle’s parameters, we supposed the parameter’s valid time is a period of time, when over through a period of time, the vehicle’s parameters will be invalid, the vehicle must be register with TA and propose the anonymous request to RSU again, so that we can ensure the scalability about TA and RSU’s recording vehicle’s parameters and anonymous identity list.

Conditional Anonymity and Un-traceability: In order not to expose the identity of vehicle, every vehicle propose anonymous request to RSU, and vehicle obtain anonymous identity to prevent malicious attackers forge vehicle’s identity. TA has the ability to reveal the identity of vehicles. When vehicle sends the bogus message, RSU traces vehicle’s anonymous identity and know the vehicle’s identity, which has registered with TA, RSU sends message to TA. Finally, TA will look up the table and revoke this vehicle’s identity in the revocation list.


5.2 Performance Analysis

Table 1: Compared Property with References

<table>
<thead>
<tr>
<th>Functions</th>
<th>Security and Privacy</th>
<th>Scalability</th>
<th>Confidentiality</th>
<th>Not need the certificate</th>
<th>In sparse RSU</th>
<th>Revocation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scheme</td>
<td>[1]</td>
<td>[2]</td>
<td>[4]</td>
<td>[6]</td>
<td>[3]</td>
<td></td>
</tr>
<tr>
<td>Security and Privacy</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Scalability</td>
<td>✓</td>
<td>x</td>
<td>✓</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Confidentiality</td>
<td>✓</td>
<td>✓</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Not need the certificate</td>
<td>✓</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>In sparse RSU</td>
<td>✓</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Revocation</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
</tbody>
</table>

We compare the performance of our scheme with other previous related works. During the signing phase of authentication, we ignore length of transmitted message. \( V_i \) registered from TA and proposed anonymous request to RSU; \( V_i \) broadcasts message to \( V_j \), then vehicle calculate chameleon hash value utilize offline phase to calculate spending time, so spending time of signing phase can be save. Assume the event have \( n \) vehicles, we utilize HMAC to calculate spending time of verification phase, the total spending time is \( nT_m + HMAC \). When \( V_i \) receives message, verifies chameleon hash value, chameleon hashing time is \( 2T_m + f_r \) that we can ignore it. If \( V_i \) verifies chameleon hash value is legality, and check message by calculating HMAC whether is on the list of broadcast message, \( V_i \) utilizes HMAC to verify legality of msgag, believes message is sent by \( V_j \). The spending time of verification phase is \( 2T_m + HMAC \). (HMAC\( \approx 0.002ms \), Pairing operation \( T_p \approx 4.5ms \), Point Multiplication \( T_m \approx 0.6ms \))

Table 3: The Comparison of Total Spending Time (S:Signing, V:Verification)

<table>
<thead>
<tr>
<th>Property</th>
<th>Broadcast message</th>
<th>Total</th>
<th>Spending time</th>
</tr>
</thead>
<tbody>
<tr>
<td>[1]</td>
<td>S: ( 1T_m )</td>
<td>V: ( 11T_m + 3T_p )</td>
<td>( 37T_m + 12T_m )</td>
</tr>
<tr>
<td>[2]</td>
<td>S: ( 2T_m )</td>
<td>V: ( 3T_m + 5T_p )</td>
<td>( 5T_m + 5T_m )</td>
</tr>
<tr>
<td>[4]</td>
<td>S: ( 1T_m )</td>
<td>V: ( 4T_m + 3T_p )</td>
<td>( 37T_m + 5T_m )</td>
</tr>
<tr>
<td>[6]</td>
<td>S: ( 2T_m )</td>
<td>V: ( 2T_m )</td>
<td>( 4T_m )</td>
</tr>
<tr>
<td>Scheme</td>
<td>S: ( n \times HMAC )</td>
<td>V: ( 2T_m + HMAC )</td>
<td>( 2T_m + (n+1) HMAC )</td>
</tr>
</tbody>
</table>

6 CONCLUSIONS

In our proposed scheme, vehicle proposed anonymous request to RSU, then vehicle utilizes anonymous identity, technologies of chameleon hash value and HMAC methods to do message authentication, transmit message and make a session key anonymously, even though vehicle moved to domain without RSU, vehicle still can communicate with other vehicles. When malicious attack occurs, the RSU can trace malicious attacker’s identity and send identity to TA. TA will revoke identity in the revocation list and send malicious attacker’s identity to all RSUs. So, the malicious attacker cannot keep on forge other vehicle’s identity. We combined chameleon hash function on Elliptic curve cryptosystem and HMAC to do message authentication, by this method can guarantee message integrity, computation of authentication is efficiency than bilinear pairing based, establish session key to communicate with other vehicles can ensure security of confidential communication, and RSU provides vehicle’s anonymous identity to achieve conditional anonymity and un-traceability, also provide revocation mechanism to revoke malicious attacker’s identity in the revocation list. Furthermore, the computation performance of our scheme is better than other thesis.

REFERENCES


