Journal of Information Hiding and Multimedia Signal Processing ©2015 ISSN 2073-4212
Ubiquitous International Volume **6**, Number **1**, January **2015**

Message Authentication Scheme for Vehicular Ad-Hoc Wireless Networks without RSU

Yu-Hsiu Huang[1,3], Kai-Hsun Fan[1], Wen-Shyong Hsieh[1,2]

[1]Department of Computer Science and Engineering
National Sun Yat-sen University
70 Lienhai Road, Kaohsiung, 804, Taiwan
yhhuang@cse.nsysu.edu.tw; potti12227@gmail.com; wshsieh@stu.edu.tw

[2]Department of Computer and Communication
Shu-Te University
59 Hengshan Road, Kaohsiung, 824, Taiwan
wshsieh@stu.edu.tw

[3]Department of Computer Science and Information Engineering
Cheng Hsiu University
840 Cheng-Qing Road, Kaohsiung, 833, Taiwan
yhhuang@cse.nsysu.edu.tw

Received July, 2014; revised August, 2014

Abstract. *Studies were conducted on vehicular ad-hoc network (VANET) in recent years. VANET is a network that combines on-board wireless equipment (On-Board Unit, OBU) and roadside fixed wireless equipment (Road Side Unit, RSU) through wireless communication technology. When vehicles broadcast messages, the traditional systems usually use RSU to do message authentication that we can ensure messages are integrity (message authentication) and broadcasted by legitimate vehicles (identity verification). But the cover range of RSU is limit and the cost is expensive, so these systems cannot work without RSU. In this paper, we propose the mechanism based on chameleon hashing and HMAC to do identity verification and message authentication under the environment without RSU. In the proposed scheme, two secret values are retained by TA, and TA will use these secret values to create and pre-load a public identity and a secret value to every registered vehicle. Based on the public identity and the secret value, a vehicle can broadcast message and make secure communication with other vehicles. The other vehicles can also make the message authentication and identity verification based on the techniques of chameleon hash, HMAC and Diffie-Hellman key exchange. The security and performance analysis show that the proposed scheme is secure and its performance is more superior than the related works.*
Keywords: VANETs, Chameleon hashing, Diffie-hellman key exchange, Message authentication, Identity verification, OBU, RSU

1. **Introduction and Related Works.** A vehicular ad hoc wireless network (VANET) provides convenient wireless network services. In VANET, vehicles can broadcast and receive the traffic information such as traffic accidents or jams. As a result, the accidents can be avoided and even the traffic jam can be reduced. In order to reach the demand of vehicle security, vehicles often broadcast traffic related message (vehicle position, speed, traffic accidents and so on) and other services, which could reduce traffic jams bypass the dangerous road sections and improve the driving security.

In VANET, we always assume that the malicious attacker can collect messages sent by other vehicles and monitors the vehicle's movement as well. It also enables to speculate the information and trace the vehicle's real identity, travelling routes and position. Many research topics had been issued to overcome the problems. Message authentication is used to make sure that the received message is integrity. Identity verification is used to verify the message which is sent by a legitimate vehicle. Anonymous authentication is used to protect the vehicle from exposing the real identity. The key agreement negotiates the session key for privacy communication. In this paper we propose the schemes for message authentication, identity verification and privacy communication under the environment without RSU.

In the field of security and privacy of VANETs, many related studies not only have focused on how to enhance the performance but also carry the security of VANETs.

In (Wasef & Jiang & Shen, 2010), the important concept of the system was set up by making the generation of key from top to bottom, such as TA to vehicles. When vehicles broadcast the messages with certificates, the message must be validated among vehicles by certificates. It provides reliability, uniqueness, and originality where the message came from. In addition, each vehicle can update its certificate from any RSU, whether or not the RSU is located in the domain where the vehicle was originally registered. Each message must be enclosed with certificates which will increase burden on packets, and additional computation of certificates which based on bilinear encryption method will increase the burden of message calculation. Furthermore, when vehicles constantly change certificates would also the burden on RSU.

When we considerate about (Zhang & Lin & Lu & Ho & Shen, 2008), it will do the identity verification between vehicle and RSUs that make sure both identity are legal. After that, they will establish the common key, the vehicle make a HMAC by using the common key which enclosed with the message and broadcasts to other vehicles in the communication range. However, two problems arise: long-term exposure of certificates and efficiency concerns regarding source authentication during message hand-off between different RSUs, and the inability of vehicles to authenticate with each other across different communication ranges.

For most current signature schemes are concerned online/offline signature schemes are based on Shamir-Tauman's paradigm. These in fact touch to the problem of key exposure. In order to solve the problem, it proposed a new double-trapdoor chameleon hash schemes (Chen & Zhang & Susilo & Mu, 2007) based on the discrete logarithm and being applied the "hash-sigh-switch" paradigm to enhance much more efficient the performance of online/offline signature scheme.

In (Sun & Zhang & Zhang & Fang, 2010), if vehicles want to broadcast a message, a common key will be established with them to receive the message, and to guarantee the security of communicating messages. But here comes the problem, this also brings some negative effects that we have to considerate about it. The establishment of common keys is got through pairing computation of Identity- based Cryptography, and we can realize the computation of bilinear pairing much more complicated than normal computation, and the calculation burden can't be ignored.

2. **Preliminaries.**

Here we will introduce the technologies used by the proposed scheme. Some preliminaries, such as using chameleon hashing and HMAC to do message authentication, elliptic curve cryptosystem, and Diffie-Hellman Key Exchange which is used to make a session key, are introduced in this session.

2.1. **Background.** In system environment, we assume that there is only one Trust Authority (TA) which is an institution with juristic authority and in charge of controlling the whole network's security. It must be taken into consideration that is the behavior of malicious attack. TA can trace the attacker's real identity and revoke the attacker's right. RSU is likely a smaller TA which has relevant coefficients set by TA, and RSU is set up on some critical points, such as intersection or traffic lights. As a result, it needs to set up many RSUs to cover wide range so that the cost must be raise a lot. Therefore, we figure out a way that use chameleon hashing and HMAC to do message authentication under the environment without RSUs. Furthermore, we are not only retain the advantages of the original properties but also achieve more faster message authentication and lower cost.

2.2. **Chameleon Hashing.** In this section, we will introduce the basic concept of chameleon hash family (Chen & Zhang & Susilo & Mu, 2007) which was the foundation of our proposed scheme.

A chameleon hash family consists of a pair (I, H):

1. I is a probabilistic polynomial-time key generation algorithm that on input 1^k , and the outputs a pair (HK, TK) such that the sizes of HK, TK are polynomial related to k.
2. H is a family of randomized hash functions. Every hash function in H is associated with a hash key HK, and it is used to map a message in a space M to a random element in a finite space R. However, the output of the hash function H_{HK} does not depend on TK.

Chameleon hash family (I, H) has the following properties:

1. Efficiency:
   Given a hash key HK and pair $(m, r) \in M \times R$, $H_{Hk}(m, r)$ is computable in polynomial time.
2. Collision resistance:
   There is no probabilistic polynomial time algorithm A in HK, to find two pairs $(m_1, r_1), (m_2, r_2) \in M \times R$ that satisfy $m_1 \neq m_2$ and $H_{HK}(m_1, r_1) = H_{HK}(m_2, r_2)$.
3. Trapdoor collisions:
   There exist a probabilistic polynomial time algorithm that given a pair $(HK, TK) \leftarrow I(1^k)$, a pair $(m_1, r_1) \in M \times R$, and an additional message $m_2 \in M$, outputs a value $r_2 \in R$ as follows: $H_{HK}(m_1, r_1) = H_{HK}(m_2, r_2)$.
   If r_1 is uniformly distributed in R then the distribution of r_2 is computationally indistinguishable from uniform in R.

2.3. **Elliptic Curve Cryptosystem.** Elliptic curves was proposed for cryptography (Miller, 1986) based on the difficulty of elliptic curve discrete logarithm problem (ECDLP). An elliptic curve equation is defined as the form of $E_p(a, b) : y^2 = x^3 + ax + b \ (mod\ p)$ over a prime finite field F_p, where $a, b \in F_p$, $p > 3$, and $4a^3 + 27b^2 \neq 0 \ (mod\ p)$. Given an integer $s \in {F_p}^*$ and a point $\in E_p(a, b)$, the point multiplication $s \cdot P$ over $E_p(a, b)$ can be defined as P plus s times.

2.4. **Diffie-Hellman Key Exchange.** It allows both sides without each other any preconditions messages for establishing a session key over an insecure channel. This session key can be used as a symmetric key to encrypt the content of messages in subsequent communications.

We will introduce D-H properties in the following.

1. Using a public key distribution mechanism of encrypted messages content.
   1.1 It can establish a common session key to communicate with each other.

1.2 Only both sides can share the common session key.
1.3 The key content is determined by both sides.
1.4 It is based on the exponential operation in of finite group(Galois).

2. This key exchange system security is generally considered to be planted on discrete logarithm problem (DLP).
   2.1 Discrete Logarithm Problem is well known, for given a large prime number n and generation number g. Calculate $1 \leq x \leq q-1$ to satisfy $g^x \equiv b \ mod \ n$, is computation infusibility.
3. $g^x \ mod \ n$ and $g^y \ mod \ n$ are computed by both nodes with their secret random number x, y respectively. The two nodes exchange $g^x \ mod \ n$ and $g^y \ mod \ n$, then calculate the session key $(g^y)^x \ mod \ n$ or $(g^x)^y \ mod \ n$ by their secret random number.

3. The Proposed Scheme.

In traditional VANETs, there is a TA (Trust Authority). TA is a management station which accepts both vehicles registration and secret implant. Almost VANETs have RSU. RSUs on traffic lights or lights along roadside are used to accomplish local support functions in VANET. RSU also help vehicles to do message authentication with each other. In the proposed scheme, there are only two tiers, TA and vehicles.

3.1. Use of Chameleon Hash Value as the Message Authentication.

The main study of this paper is how vehicles to do message authentication, identify verification, and private communication, in the environment without RSU.

Our scheme is based on the technique of Chameleon Hashing which uses Elliptic Curve Cryptosystem as foundation. Besides, each vehicle can make its chameleon hash value to protect its privacy and authentication. Most of important, our scheme can also let vehicles communicate with each other without the help of RSU.

Table 1. Notation of the parameter generation

Notation	Descriptions
f(.)	a cryptographic secure hash function $f : Z_q \times G \to Z_q$
H(.)	$H : \{0,1\}^* \to \{0,1\}^*$
P	Denote G the subgroup generated by P
N_i	ID of vehicle i
k_i	a random number $k_i \in Z_p$
K_i	$K_i = k_i \cdot P$ of vehicle's public parameter
m_i	$N_i \| \| {K_i}^x$, where x of ${K_i}^x$ represents the value of x-axis
α, x	the secret value of TA
$r_i Y$	$r_i Y = r_i \cdot Y$ of vehicle's public parameters
M_i	the message which announced by vehicle i
r_i	the secret value of vehicle i which given by TA
CH_{TA}	the chameleon hash value of TA
Y	Y equal to x multiplied by P
$HMAC_{s_j}(.)$	A keyed-hash message authentication code with key s_j
s_j	the key of HMAC; $j = 1 \sim n$
T_i	the valid time of vehicle parameter

3.1.1. *System Setup and Registration.* To set up the system by the following steps:

1. TA chooses $\alpha, x \in Z_p$ as its secret.
2. It selects a hash function: $H : \{0,1\}^* \to \{0,1\}^*$
3. TA sets $CH_{TA} = f(m,K)K + rY = \alpha Y$ as its chameleon hash value, $Y = xP$

After that, TA will publish (CH_{TA}, *Y, P, H, f*), and keep (α, x) secretly. We let each one of vehicles be a node to register with TA in the following process:

1. For vehicle i as N_i, TA chooses a random number $k_i \in Z_p$, and compute $K_i = k_i P$.
2. TA sets N_i, $m_i = N_i || {K_i}^x$, and TA not only use the chameleon hash value to calculates the secret $r_i = \alpha - f(m_i, K_i) k_i x^{-1} \; mod \; q$ for V_i , but also pre-loads (N_i, K_i, r_i, T_i) and CH_{TA} to N_i
3. After vehicles receive the parameters from TA, each vehicle, as V_i has its own (N_i, K_i, r_i, T_i) as the ID, public key, secret value, and valid time, then V_i calculates $r_i \cdot Y = r_i Y$. V_i holds r_i as its secret value and use $(N_i, K_i, r_i Y, T_i)$ as the public identify.

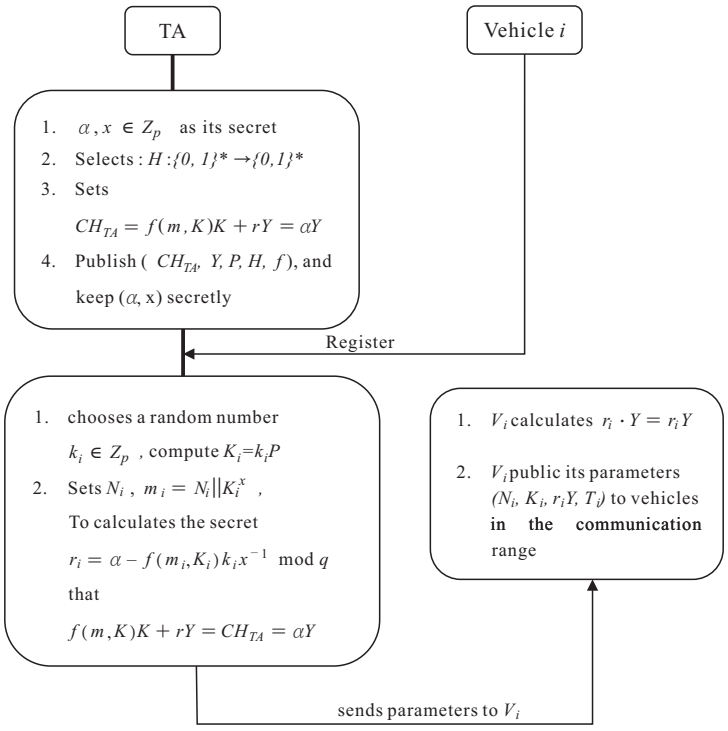

FIGURE 1. System Setup and Registration

3.2. **Announcement of Neighbor's Vehicles.** After registering with the TA, the vehicle V_i will get the secret value r_i that was sent from TA. After that, vehicle V_i will use the secret value r_i and the public identity to do message authentication as follows:

1. Each vehicle will publish their public identity, such as V_i public its identity $(N_i, K_i, r_i Y, T_i)$ to vehicles in the communication range.
2. Once vehicles (V_j)get the parameters from V_i, V_j will record V_i's parameters, and V_j also receive the other vehicles parameters at the same time so that V_j will maintain a table to record all these parameters. After that, V_j can use the parameters in the table to do message authentication with vehicles.

3.3. **Message Broadcasting and Authentication.** We use chameleon hash value to achieve message authentication and use HMAC to broadcast message in VANET without RSUs.

After that, we still can ensure message integrity and verify who sent the message. The steps show as follow:

1. Suppose vehicle V_i with public identity (N_i, K_i, r_iY, T_i) and V_i keep the secret value, and it will broadcast the message $(N_i, K_i, r_iY, M_i, T_1)$, list of $HMAC_{s_j}(M_i||T_1)$ to others vehicles in communication range, where $s_j = (r_i(r_jY))^x$ is a HMAC key, r_jY is announced by the neighbor vehicle V_j.
2. We assume there have a vehicle V_j, V_j receives the message and computes the Chameleon hash value $f(m_i, K_i)K_i + r_iY$. If $f(m_i, K_i)K_i + r_iY = CH_{TA}$, V_j will use the HMAC's key $s_j = (r_j(r_iY))^x$ to calculate the $HMAC_{s_j}(M_i||T_1)$ and check if it is in the list of broadcast message. If $HMAC_{s_j}(M_i||T_1)$ exists, V_j believes the message is sent by V_i , because V_i had used the secret value r_i which is associated with r_iY to create HMAC's key.

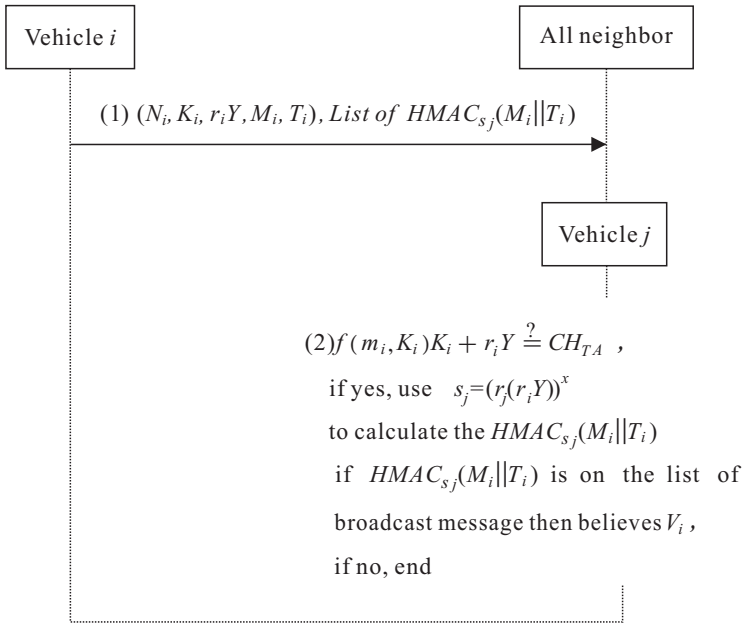

FIGURE 2. Message broadcasting and Authentication

3.3.1. *Message sent to specific vehicles.* In addition to make message authentication, we assume that V_i want to communicate with specific V_j, and V_i has the public identity of V_{js}, (N_j, K_j, r_jY, T_j).

V_i wants to send a message M to V_{js}

1. V_i sets $M = M_1 \oplus M_2$, $M_2 = M \oplus M_1$.
2. V_i sends message $< N_i, K_i, r_iY, M_1, T_1$, list of $HMAC_{s_j}(M_1||T_1)$, list of $M_2 \oplus s_j >$ to V_{js}, where $s_j = (r_i(r_jY))^x$.
3. V_j receives the above message, and V_j will use parameters which get from V_i to check if $f(m_i, K_i)K_i + r_iY$ is equal to CH_{TA}. If yes, V_j verify the legality of the message which may be sent by V_i. V_j will use the HMAC's key $s_j = (r_j(r_iY))^x$ to calculate the $HMAC_{s_j}(M_1||T_1)$ and check if it is in the list of broadcast message. If $HMAC_{s_j}(M_1||T_1)$ is in the list, V_j make sure that the message was send by V_i, then V_j will acquire corresponding values with list of $M_2 \oplus s_j$.

4. V_j computes $M_2 \oplus s_j \oplus s_j = M_2$. V_j gets the message $M = M_1 \oplus M_2$.

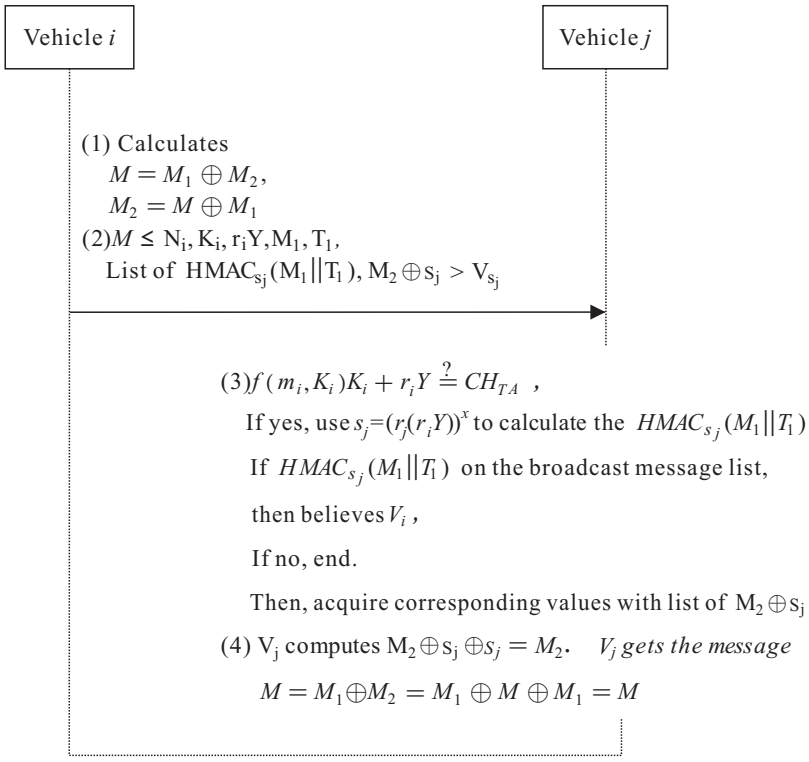

FIGURE 3. Message sent to Specific vehicles

3.3.2. *Session Key Exchange for Message Communication.* Vehicles want to private communicate with each other constantly that they need a session key.

We assume V_i want to communication with V_j confidentially.

1. V_i chooses a random number $a \in Z_q$ and calculates aP. Vi sends the message $(N_i, K_i, r_i Y, T_1, aP)$ to V_j .
2. After receiving the message from V_i, V_j checks if $f(m_i, K_i)K_i + r_i Y$ is equal to CH_{TA}. If yes, V_j believes the message may be sent by V_i and verifies the legality of the message, then V_j chooses a random number $b \in Z_q$ and calculates bP. V_j sets $(b(aP))^x$, makes a challenge $Mar_j = f((b(aP))^x || (r_j(r_i Y))^x, K_j)$ and sends Mar_j with V_j parameters $(N_j, K_j, r_j Y, T_2, Mar_j)$ back to V_i.
3. When V_i get the message from V_j, V_i checks if $f(m_j, K_j)K_j + r_j Y$ is equal to CH_{TA}. If yes, V_i believes the message may be sent by V_j and verifies the legality of the message. Due to V_i needs to response the V_j's challenge, V_i uses $(a(bP))^x$ and $(r_i(r_j Y))^x$ to check if $f((a(bP))^x || (r_j(r_j Y))^x, K_j)$ is equal to Mar_j.If it is successful, V_i makes sure the message that sent by V_j. In addition, V_i can privately communicate with V_j by using session key= $H(a(bP))^x || (r_j(r_j Y)^x)$.

4. **Security and Performance Analysis.** In this section, we mainly illustrates the method proposed in the paper could reach 1. Authentication: message authentication, identity verification, and non-repudiation; 2. Confidentiality and flexibility; 3. Efficiency; 4. Scalability; 5. Conditional anonymity and un-traceability; in terms of security analysis.

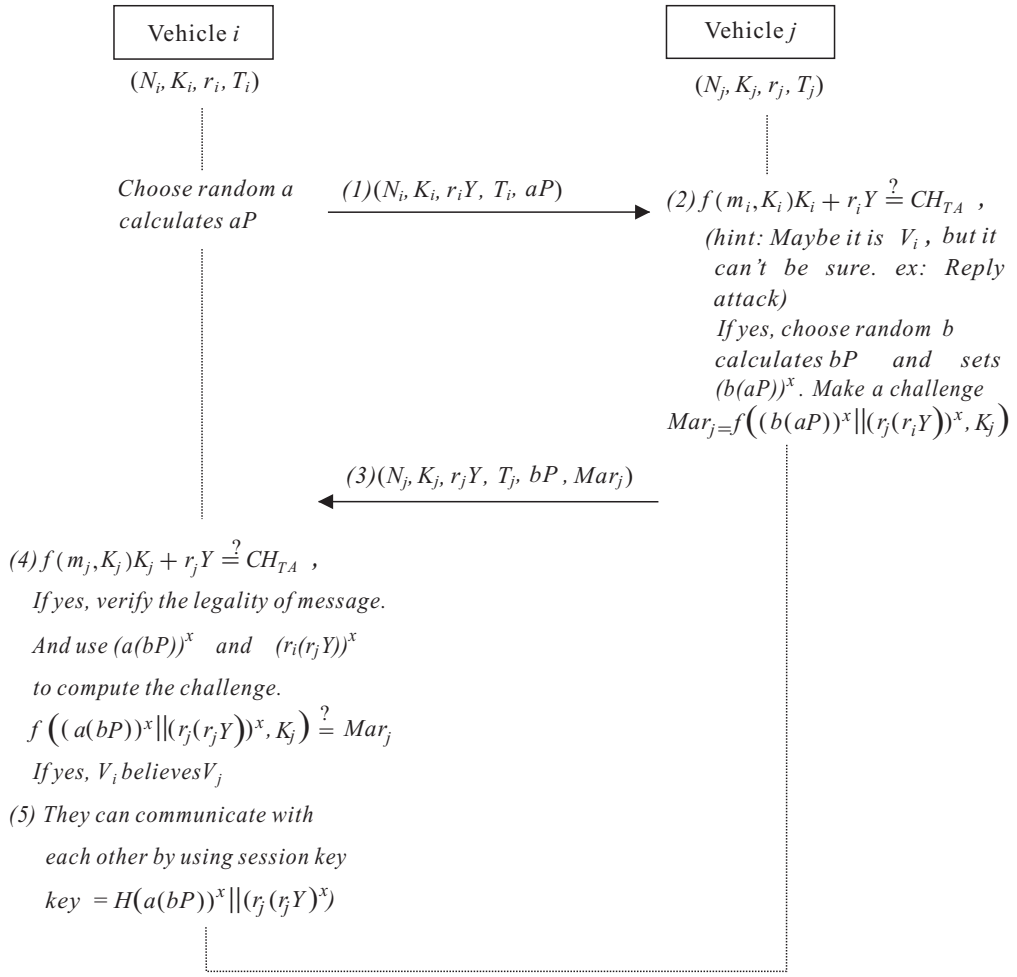

FIGURE 4. Session Key

4.1. **Security Analysis.** We analyse the security of our proposed scheme.

1. Authentication and Non-Repudiation:
   After vehicles registered with TA, Vehicles can get their own secret r_i from TA. If there have an attacker try to tamper with the message, the receiver can't make the result of $(f(m_i, K_i)K_i + r_iY = CH_{TA})$, and then the modified message will be ignored.
   We set up by using elliptic curve cryptosystem about Y and r_iY, it still hard to get the r_i based on the difficulty (ECDLP). Identity authentication can be achieve by the chameleon hashing and HMAC. Similarly, the message with a chameleon hash value can guarantee non-repudiation.
2. Confidentiality and Flexibility:
   According to Elliptic Curve Discrete Logarithm Problem (ECDLP) and Diffie-Hellman , the session keys are created by their own secrets. We assume there have a malicious node (V_k), it is hard for V_k to find out the secret values between V_i and V_j. Other vehicles are unable to calculate the common session keys because they still don't know the secret r_i of V_i. After that, the security of confidentially communicating is ensured.
3. Efficiency:
   Our scheme does not need to do additional computations to verify the certificates because we use chameleon hash value and HMAC to replace it. Without additional

computation for certificate, the computation loads and energy costs can efficiency reduce.

4. Scalability:
   The proposed scheme utilizes chameleon hash value with each vehicle's unique secrets to accomplish the message authentication. Thus, vehicles can do message authentication with each other without RSUs, and TA just need to maintain a small public-key table (i.e. store $K_i = k_i P$) while the number of vehicles become very large.
5. Conditional Anonymity and Un-traceability:
   We assume there have a vehicle (V_j) and use the new idea that V_j registers k sets of $N_{ia}, K_{ia}, r_{ia}, T_{ia}$ $(a = 1 \sim K)$ with TA at first. When V_j wants to send a message, V_j can use one of the sets $(N_{ia}, K_{ia}, r_{ia}, T_{ia})$ to do message authentication. V_j can change another set over period of time and all parameters of V_j given from TA has the valid time that is difficult to be tracked.

4.2. **Performance Analysis.** We compare the performance of our scheme with other previous related works. L.Rongxing 2008[1], A Wasef 2010[2], J.Y.Sun2010[3], and Xiaofeng Chen, 2007[4].

Table 2. The Comparison of Functions

Method / Functions	The proposed scheme	[1]	[2]	[3]	[4]
Security and Privacy	Y	Y	Y	Y	Y
Scalability	Y	N	Y	Y	Y
Confidentiality	Y	N	N	N	N
Not need the certificate	Y	N	N	N	Y
Without RSU	Y	N	N	N	N

Table 3. Execution Time in Milliseconds

Executing	Descriptions	Execution Time(ms)
HMAC	HMAC	≈ 0.002
T_e	Field Exponentiation	≈ 0.54
T_m	Point Multiplication	≈ 0.6
T_p	Pairing operation	≈ 4.5

Here we try to calculate the operation time of message authentication, and we ignore the length of transmitted message, the execution time is in table 3, and the comparison of message authentication is in table 4, n is the number of neighbor's vehicles.

5. **Conclusions.** In this paper, we propose the mechanism based on the chameleon hash function and HMAC to provide the processes of message authentication, identity verification and privacy communication for VANET under the environment without the help of RSU. Based on the difficulty of ECDLP, the vehicles can keep the secret value for identity verification and key exchange. Broadcasting message is included in the chameleon hash function with the vehicle's public identify, it can prevent the broadcasting message from malicious attacking.

There are only the checking of chameleon hash value and HMAC involved in the processes, so the processes are very easy and efficient.

TABLE 4. The Comparison of Total Spending Time

Property method	Authentication message	Total	Spending time
[1]	Signing: $1T_m$ Verification: $11T_m + 3T_p$	$3T_p + 12T_m$	20.7ms
[2]	Signing: $2T_m$ Verification: $3T_m + 5T_p$	$5T_m + 5T_p$	25.5ms
[3]	Signing: $1T_m$ Verification: $4T_m + 3T_p$	$5T_m + 3T_p$	16.5ms
[4]	Signing: $2T_m$ Verification: $2T_m$	$2T_m + 2T_m$	2.4ms
The proposed Scheme	Signing: n^*HMAC Verification: $2T_m$ +HMAC	$2T_m$+HMAC(1+n)	1.2ms

The security and performance analysis show that the proposed scheme is secure and full of functionality, and gets more superior performance in message authentication than the related works.

REFERENCES

[1] R. X. Lu, X. D. Lin, H. J. Zhu, P. H. Ho, and X. M. Shen, ECPP: Efficient Conditional Privacy Preservation Protocol for Secure Vehicular Communications, *Proc. of the IEEE 27th Conference on Computer Communications*, pp. 1229-1237, 2008.

[2] w. Albert, Y. X. Jiang, and X. M. Shen, DCS: An Efficient Distributed-Certificate-Service Scheme for Vehicular Networks, *IEEE Trans. on Vehicular Technology*, vol. 59, no. 2, pp. 533-549, 2010.

[3] C. X. Zhang, X. D. Lin, R. X. Lu, P. H. Ho, and X. M. Shen, An Efficient Message Authentication Scheme for Vehicular Communications, *IEEE Trans. on Vehicular Technology*, vol. 57, no. 6, pp. 3357-3368, 2008.

[4] Y. P. Sun, R. X. Lu, X. D. Lin, X. M. Shen, and J. S. Su, An Efficient Pseudonymous Authentication Scheme With Strong Privacy Preservation for Vehicular Communications, *IEEE Trans. on Vehicular Technology*, vol. 59, no. 7, PP.3589-3603,2010.

[5] X. F. Chen, F. G. Zhang, W. Susilo, T. Mu, Efficient Generic On-Line/Off-Line Signatures Without Key Exposure, *Information Sciences*, vol. 178, PP.4192-4203, 2008.

[6] J. Y. Sun, C. Zhang, Y. C. Zhang, and Y. G. Fang, An Identity-Based Security System for User Privacy in Vehicular Ad Hoc Networks, *IEEE Trans. on Parallel and Distributed Systems*, vol. 21, no. 9, pp. 1227-1239, 2010.

[7] J. Y. Liu and W. S. Hsieh, An Anonymous Authentication and Key Agreement Scheme in VANETs, Department of Computer Science and Engineering, Master Thesis, National Sun Yat-sen University, Kaohsiung, Taiwan, 2012.

[8] H. Krawczyk and T. Rabin, Chameleon hashing and signatures, *Proc. of the 7th Annual Network and Distributed System Security Symposium*, pp. 143-154, 2000.

[9] V. S. Miller, Use of elliptic curves in cryptography, *Proc. of CRYPTO '85 on Advances in cryptology*, pp. 417-426, 1986.