International Journal of Security and Its Applications
Vol. 11, No. 5 (2017), pp.69-78
http://dx.doi.org/10.14257/ijsia.2017.11.5.07

A Secure and Efficient Message Delivery Scheme for VANET

Huaijin Liu[1], Yonghong Chen[1] and Dharma P. Agrawal[2]

[1]Department of Computer Science and Technology, Huaqiao University,
Xiamen Fujian 361021, China
[2]University of Cincinnati, Cincinnati, OH45221-0030, USA
lhjhqdx@163.com; djandcyh@163.com; agrawadp@ucmail.uc.edu

Abstract

In order to meet the need of scalability of vehicular ad hoc network (VANET), when using the roadside unit (RSU) for message authentication and broadcast, many studies have paid little attention to the message transmission delay and the communication overhead caused by the signature. For the sake of guaranteeing the reliability of the message and improve the efficiency of message transmission, this paper proposes a secure and efficient message delivery scheme for VANET. The scheme firstly uses the opp-dir dissemination model to propagate the message to solve the problem of message transmission delay. Then, the message is signed by the aggregate MAC technique to ensure the reliability of the message. Extensive experiments validate that the proposed scheme can reduce the message transmission delay and communication overhead, improve the message delivery ratio.

Keywords: *Vehicular ad hoc network; Aggregate MAC; Opp-dir dissemination model; Message authentication*

1. Introduction

Vehicular ad hoc network (VANET) is the specific application of Mobile ad hoc Network (MANET) in the field of intelligent transportation. It has great significance in preventing traffic accidents, improving traffic efficiency and protection of people's life and property safety [1]. With the gradual development of VANET, VANET security issues have also been more attention.

In recent years, many studies have been reported on the security and privacy protection of VANET [2-4]. Although these studies address different levels of security and privacy issues, they do not consider the scalability of VANET. In order to meet the scalability of VANET, some research with the aid of RSU for message authentication and dissemination [5-7]. In [5], Zhang *et al.*, proposed a data aggregation and batch authentication scheme with the aid of RSU, which reduces the communication overhead and improves the efficiency of authentication, but each vehicle needs a large buffer space. Subsequently, Zhang *et al.*, [6] was extended on the basis of reference [5], require each vehicle to maintain a RSU key table, which solves the problem of message propagation authentication in different RSU range. However, this scheme does not take into account that RSU is not within the range of vehicle communication. Recently, Lim *et al.*, [7] proposed an efficient authentication and secure message delivery scheme that uses an onion routing scheme to sign and forward messages to nearby RSUs, preventing the forwarding vehicle to malicious tampering or forgery messages. However, the scheme greatly increases the communication overhead of message transmission.

To solve the above problems, this paper proposes a secure and efficient message delivery scheme for VANET, the main contributions are: 1) In order to satisfy the scalability of the network, we use RSU to authenticate and propagate messages. 2) When the vehicle sends a message to the RSU, RSU man not be within the communication

ISSN: 1738-9976 IJSIA

range of the vehicle. In order to improve the forwarding efficiency of messages when forwarding messages through nearby vehicles, we use the opp-dir dissemination model to forward the message. 3) In order to ensure the reliability of the message, RSU needs to authenticate all forwarding vehicles. To this end, we use the aggregate MAC technology to sign the message, which greatly reduces the additional communication overhead caused by RSU authentication message.

2. System Model

2.1. Network Model

In this subsection, we propose a general network model for VANET. As shown in Figure 1, the network model mainly includes three types of entities: trusted authentication center (TA), roadside unit (RSU) and vehicle unit (OBU). TA is responsible for generating public and private key pairs for RSU and OBU, and manages the privacy information of all registered vehicles, including the driver's identity information. OBU is loaded in the vehicle and responsible for sensing the road condition and transmitting the message to RSU. RSU is fixed on the roadside, responsible for verifying the authenticity and integrity of the message and broadcasting the message to all vehicles within the communication range. Compared to RSU, OBU has a short communication range and less computing power. In this network model, we assume that the communication range of OBU is 250m, and the communication range of RSU is 2500m.

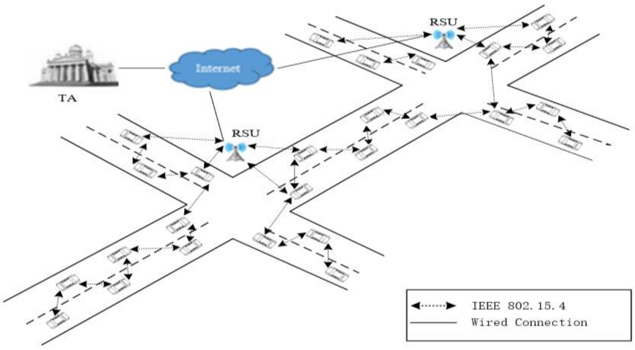


Figure 1. The Network Model

2.2. Dissemination Model

When the vehicle sends a message to RSU, RSU may not be within the communication range of the vehicle. In order to improve the efficiency of message transmission, we forward the message through the opp-dir dissemination model [8]. The model divides the broadcast data into generated data and forwarded data. When a vehicle V_1 broadcasts a packet, the vehicle V_2 can only receive and forward the packet if it satisfies the following conditions:

1) If V_1 is traveling west (or east), V_2 is traveling east (or west), and V_2 is within the transmission range of V_1, V_2 will receive and forward the packet. This is the case when V_1 broadcasts its generated data.

2) If V_1 and V_2 are traveling east (or west), V_2 is within the communication range of V_1 and is located in front of V_1, V_2 will receive and forward the packet. This is the case when V_1

forwards a packet.

Figure 2 shows an example of how information is propagated from vehicle V_{1W} to RSU using the opp-dir dissemination model.

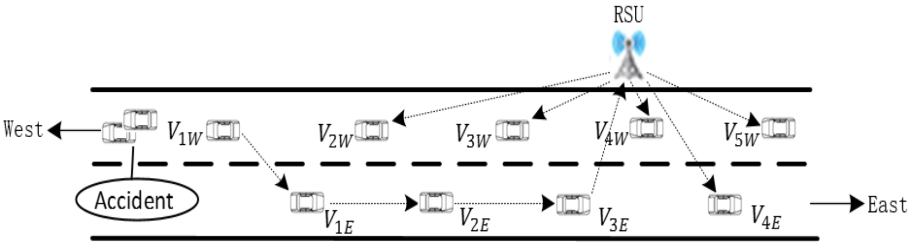


Figure 2. The Opp-dir Dissemination Model

3. Preliminaries

The scheme involves Diffie-Hellman public key cryptography [9] and aggregate message authentication codes [10] two kinds of basic technology.

3.1. Diffie-Hellman Public Key Cryptography

Diffie-Hellman public key cryptography divides the key k of symmetric cryptography into two parts, a public key (PK) and a private key (SK), in which PK can be known by anyone to encrypt the message or verify the signature, and SK can only be known by the recipient or signer of the message, and is used to decrypt or sign the message. The following is a public key cryptosystem definition.

Definition 1. A public key cryptosystem consists of the following three algorithms:

1) KeyGen (λ): randomly select a security parameter λ as the input value, output public key PK and private key SK, denoted as (PK, SK) ⟵keyGen (λ).

2) Encrypt (PK, m): input the public key PK and plaintext m, output ciphertext C, denoted as C⟵encrypt (PK, m).

3) Decrypt (SK, C): input the private key SK and ciphertext C, output plaintext m, denoted as m⟵decrypt (SK, C).

3.2. Aggregate MAC

Aggregate message authentication codes (aggregate MAC) allows aggregation of multiple MACs generated by different senders for multiple messages into a short authentication tag that the recipient can still verify the integrity of the message. The definition of aggregate MAC is given below.

Definition 2. An aggregate MAC is composed of a set of probabilistic polynomial time algorithms (Mac, Agg, Vrfy), which are constructed as follows:

1) Authentication algorithm Mac: input a key k and a message m, output message authentication code, denoted as $Mac_k(m)$.

2) Aggregation algorithm Agg: input l message authentication codes $Mac_{k_1}, \cdots, Mac_{k_l}$, through XOR operation for all message authentication codes aggregation, output the authentication tag, denoted as $\text{tag} = Mac_{k_1} \oplus Mac_{k_1} \oplus \cdots \oplus Mac_{k_l}$.

3) Validation algorithm Vrfy: input l message/key pairs $\{(m_1, k_1), \cdots, (m_l, k_l)\}$, and the authentication tag tag, calculate $tag' = \oplus_{i=1}^{l} Mac_{k_i}(m_i)$, and verify that $tag' = tag$ is equal, if equal, output 1; otherwise, output 0.

4. The Proposed Scheme

In this section, we will give a detailed introduction of the proposed scheme. This scheme involves three phases: symmetric key establishment, MAC aggregation, message authentication and dissemination.

4.1. Symmetric Key Establishment

When vehicle V_i enters an RSU R_j coverage area, it begins the mutual authentication process with R_j and establishes a shared key. This process is implemented using Diffie-Hellman public key cryptosystem. The mutual authentication and key establishment process is as follows:

$$V_i \longrightarrow R_j: \{ID_{V_i}, g^a, Ts\}_{PK_{R_j}}, \{g^a, Ts\}_{SK_{V_i}}$$
$$R_j \longrightarrow V_i: \{PID_{V_i}, g^b, Ts\}_{PK_{V_i}}, \{g^a, g^b, Ts\}_{SK_{R_j}}$$
$$V_i \longrightarrow R_j: \{g^b, Ts\}_{SK_{V_i}}$$

Where g^a and g^b are two elements of Diffie-Hellman public-key cryptosystem, and the shared key $K_{ij} \leftarrow g^{ab}$ of V_i and R_j can be calculated by these two elements. When R_j receives the first message of V_i, it first decrypts the message using its own private key SK_{R_j} to obtain g^a and then uses the public key PK_{V_i} of V_i to authenticate the identity of V_i . If the authentication is successful, R_j sets a pseudo identity PID_{V_i} to V_i and encrypts $\{PID_i, g^b, \text{Ts}\}$ using the public key PK_{V_i} of V_i and using its own private key SK_{R_j} signature $\{g^a, g^b, Ts\}$, where Ts represents the timestamp . In a similar manner, V_i decrypts and authenticates the received message. If the authentication succeeds, V_i signs $\{g^b, Ts\}$ with its own private key SK_{V_i} and sends it to R_j to inform that g^b has been obtained.

4.2. MAC Aggregation

When the shared key K_{ij} is established, V_i first encrypts M with K_{ij} to obtain $M_i = \{M, Ts, Sq\}_{K_{ij}}$, Where Sq denotes the message sequence number and M denotes the message to be sent, and then generates a MAC $Mac_{K_{ij}}(M_i)$ for M_i using the authentication algorithm Mac and sends it to R_j with $\{ID_{R_j}, PID_{V_i}, M_i\}$, where ID_{R_j} represents R_j's identity and PID_{V_i} represents V_i's pseudo identity.

$$V_i \longrightarrow R_j: ID_{R_j}, PID_{V_i}, M_i, Mac_{K_{ij}}(M_i)$$

In the process of transmission, R_j may not be within the communication range of V_i, and the message M_i needs to be forwarded to R_j through nearby vehicles. In order to improve the efficiency of message transmission, we use the opp-dir dissemination model [9] to forward M_i. At the same time, in order to prevent the forwarding vehicle from maliciously tampering or forgery M_i during the forwarding process, we adopt the aggregate message authentication code scheme [11]. In the process, each forwarding vehicle will generate a new aggregate MAC and forwards it along with M_i to the next hop forwarding vehicle. This operation is repeated until M_i is forwarded to R_j. Algorithm 1 gives the detailed forwarding steps. Note that no matter how many times a message is forwarded, the final result will always be an encrypted message M_i and an aggregate MAC.

Algorithm 1. The message propagation algorithm

```
When a vehicle $V_i$ wants to send a message $M$ to the nearby RSU $R_j$, $V_i$ first encrypts $M$ to get $M_i = \{M, Ts, Sq\}_{K_{ij}}$, and then generates a message authentication code $Mac_{K_{ij}}(M_i)$ for $M_i$.
If $R_j$ is within the communication range of $V_i$ then
    $V_i$ sends the message $\{ID_{R_j}, PID_{V_i}, M_i, Mac_{K_{ij}}(M_i)\}$ to $R_j$.
else $V_i$ broadcast the message $\{ID_{R_j}, PID_{V_i}, M_i, Mac_{K_{ij}}(M_i)\}$ to all vehicles within the communication range.
If the vehicle $V_t$ is traveling in the same direction as $V_i$ then
    $V_t$ does not forward the message $\{ID_{R_j}, PID_{V_i}, M_i, Mac_{K_{ij}}(M_i)\}$.
else $V_t$ computes a message authentication code $Mac_{K_{tj}}(M_i)$ for $M_i$, and then XOR with $Mac_{K_{ij}}(M_i)$ of $V_i$ to get an aggregate MAC, denoted as $tag = Mac_{K_{ij}}(M_i) \oplus Mac_{K_{tj}}(M_i)$.
If $R_j$ is within the communication range of $V_t$ then
    $V_t$ sends the message $\{ID_{R_j}, PID_{V_i}, PID_{V_t}, M_i, tag)\}$ to $R_j$.
else $V_t$ sends the message $\{ID_{R_j}, PID_{V_i}, PID_{V_t}, M_i, tag\}$ to the next-hop forwarding vehicle.
Repeat the above steps until the message $M_i$ is forwarded to the nearby RSU $R_j$.
```

4.3. Message Authentication and Dissemination

When R_j receives the message sent by a vehicle V_k, it finds the shared key of the sender and all forwarding vehicles according to the pseudo identity of the sender and each forwarding vehicle, and then calculates $tag' = \oplus_{i=1}^{k} Mac_{K_{ij}}(M_i)$ and verifies it with tag, if $tag' = tag$ is equal, decrypt M_i to obtain the message M and broadcasts to all vehicles within the communication range; if not equal, it is discarded;

5. Performance Evaluation

In this section, the performance of the proposed scheme is studied by simulation experiments. In contrast, the simulation also implements the batch authentication scheme (called RAISE) in [5] and the onion signature authentication scheme (called EAMDP) in [6].

5.1. Simulation Settings

Our experimental equipment for the Intel i5-4200U 2.30GHz processor, 4G memory, 64-bit Windows 7 operating system. The experimental environment was built on Ubuntu 14.04.1 on Oracle VM VirtualBox 5.0.4, with 2GB of memory allocated. The experimental simulation software is NS-2.35, and the specific values of the parameters are shown in Table 1.

Table 1. Simulation Parameters

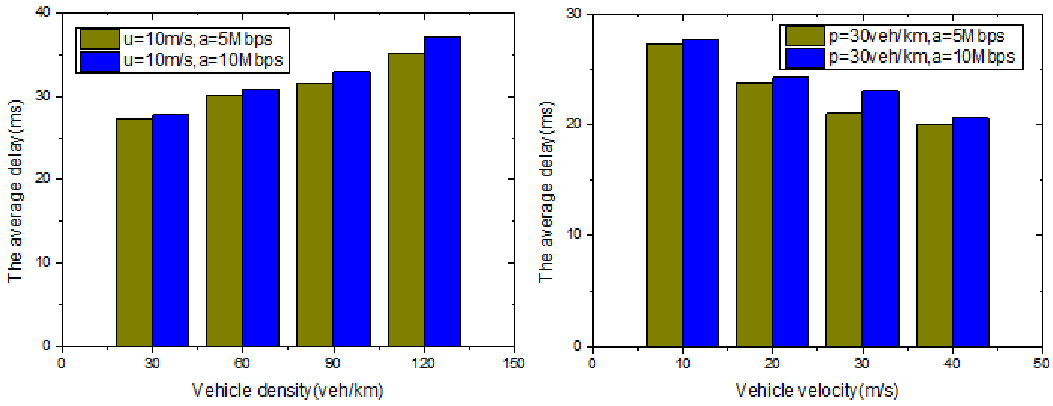
Parameters	Value
Simulation area	2500m × 30m
Traffic type	CBR
MAC protocol	IEEE 802.15.4
RSU communication range	2500m
Vehicle communication range	250m
Queue length	50
Packet size	512byte
Simulation time	100s

5.2. Experimental Results

In VANET, due to the vehicle has a certain energy supply capacity, so the experiment mainly pick the vehicle's average transmission delay (TD), average loss ratio (LR), and communication overhead are analyzed. Where the TD is defined as the average time between the source node generating a packet and its successful delivery to the destination node in a time period and the LR is defined as the ratio between the number of packets delivered to the destination node and the number of packets sent by the source node in a time period. Since the different parameters of the opp-dir dissemination model directly affects the transmission delay and loss ratio, so we first analyze the opp-dir dissemination model.

5.2.1. Opp-dir Dissimination Model

There are many factors that affect the opp-dir dissemination model, and we mainly perform the simulation with different vehicle densities p=30 veh/km, 60 veh/km, 90 veh/km, 120 veh/km, different vehicle velocity u=10 m/s, 20 m/s, 30 m/s, 40 m/s and different message transmission rate a=5 Mbps, 10 Mbps. Figure 3(a) shows the average delay of different vehicle densities. From Figure 3(a) we can see that with the increase of vehicle density, the average delay is increasing. Because as the vehicle density increases, the number of vehicles forwarding the message is increasing, thereby increasing the message transmission delay. Figure 3(b) shows the average delay of different vehicle velocity. From Figure 3(b) we can see that with the increase of vehicle velocity, the average delay is decreasing. This is because the vehicle velocity increases the transmission efficiency of the message.



(a) Vehicle Density vs. Average Delay (b) Vehicle Velocity vs. Average Delay

Figure 3. The Opp-bir Dissemination Model Delay

5.2.2. Transmission Delay and Loss Ratio

In order to study the effect of traffic load on transmission delay, we fixed the vehicle's message transmission rate a=5 Mbps and the vehicle's velocity u=10 m/s. Here the traffic load is represented by the number of vehicles within the RSU communication range. Figure 4 shows the relationship between traffic load and average delay. Obviously, from the figure we can see that EAMDP has a maximum transmission delay. The reason is due to the onion signature method is used to increase the transmission delay. On the other hand, our scheme has a minimum transmission delay. This is because our scheme reduces the computational overhead by aggregate MAC and improves the efficiency of message transmission by using the opp-dir dissemination model.

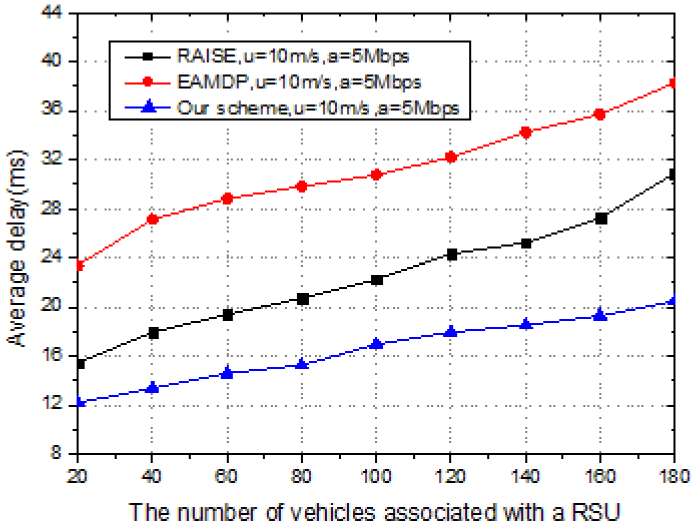


Figure 4. Traffic Load vs. Average Delay

Figure 5 shows the relationship between traffic load and average loss ratio. As can be seen from the figure, the average loss ratio of the three schemes increases with the increase of traffic load, the main reason is caused by channel congestion. On the other hand, our scheme has a lowest average loss ratio, because our scheme has a minimal communication overhead.

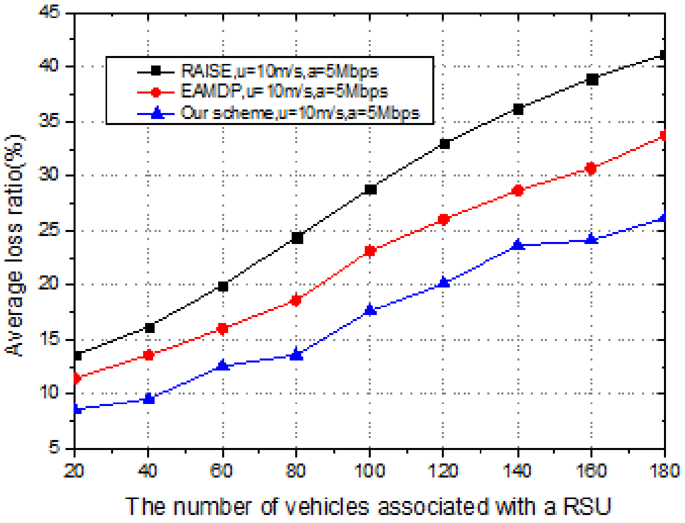
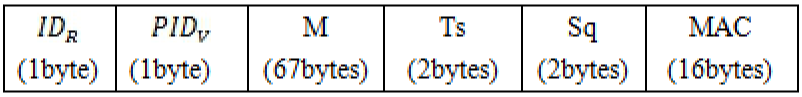


Figure 5. Traffic Load vs. Average Loss Ratio

5.2.3. Communication Overhead

First of all, we give a signed message format for our scheme, as shown in Figure 6. RAISE message format is listed in [5], and EAMDP message format is listed in [6]. According to [11], we can know that the size of a digital signature is 56 bytes, the size of a MAC is 16 bytes, and the size of a message is 67 bytes. At the same time, we set the vehicle pseudo-identity PID_V and RSU identity ID_R of the size of 1 byte, timestamp Ts and message sequence number Sq of the size of 2 bytes. Therefore, our scheme message size is 89 bytes, RAISE message size is 256 bytes and EAMDP message size is 129 bytes.



ID_R	PID_V	M	Ts	Sq	MAC
(1byte)	(1byte)	(67bytes)	(2bytes)	(2bytes)	(16bytes)

Figure 6. The Signed Message Format of our Scheme

Figure 7 shows the relationship between traffic load and communication overhead. As can be seen from the figure, our scheme has a small communication overhead compared to the other two schemes. To be specific, when the number of vehicles is 180, the communication overhead of our scheme is 65.23% and 31.01% less than that of RAISE and EAMDP respectively.

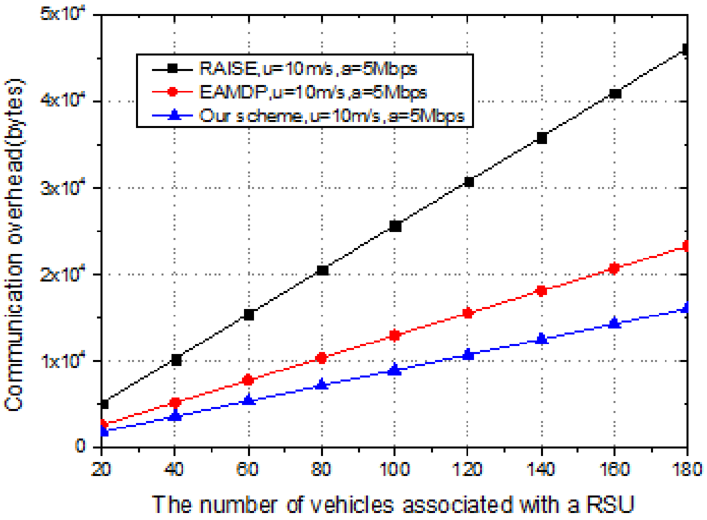


Figure 7. Communication Overhead vs. Average Hop

6. Conclusion

In this paper, we propose a secure and efficient message delivery scheme for VANET. The scheme forwards messages to RSU through the opp-dir dissemination model, which improves the efficiency of message transmission. In the message forwarding process, in order to prevent the forward vehicle tampering or forgery from the message, we use the aggregate MAC technology to sign the message. The experimental results show that our scheme has lower transmission delay, smaller loss ratio and less communication overhead.

Acknowledgments

Above work is supported by National Natural Science Foundation (NSF) of China under grant Nos. 61370007, 61572206, U1405254, Huaqiao University graduate research innovation ability cultivation project of China under grant No. 1511314006, Fujian

Provincial Natural Science Foundation of China under grant No. 2013J01241, and Program for New Century Excellent Talents of Fujian Provincial under grant No. 2014FJ-NCET-ZR06.

References

[1] F. Kargl, P. Papadimitratos, L. Buttyan, M. Müter, E. Schoch, B. Wiedersheim, J. P. Hubaux, "Secure vehicular communication systems: implementation, performance, and research challenges", IEEE Communications Magazine, vol. 46, no. 11, **(2008)**, pp. 110-118.

[2] 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, **(2007)**, pp. 3442-3456.

[3] P. Papadimitratos, L. Buttyan, T. Holczer, E. Schoch, J. Freudiger, M. Raya and J. P. Hubaux, "Secure vehicular communication systems: design and architecture", IEEE Communications Magazine, vol. 46, no. 11, **(2008)**, pp. 100-109.

[4] S. Guo, D. Zeng, Y. Xiang, "Chameleon hashing for secure and privacy-preserving vehicular communications", IEEE Transactions on Parallel and Distributed Systems, vol. 25, no. 11, **(2014)**, pp. 2794-2803.

[5] C. Zhang, X. Lin, R. Lu, P. H. Ho, "RAISE: an efficient RSU-aided message authentication scheme in vehicular communication networks", Proceedings of IEEE International Conference on Communications, Beijing, China, **(2008)**, pp. 1451-1457.

[6] C. Zhang, X. Lin, R. Lu, P. H. Ho, X. Shen, "An efficient message authentication scheme for vehicular communications", IEEE Transactions on Vehicular Technology, vol. 57, no. 6, **(2008)**, pp. 3357-3368.

[7] K. Lim, D. Manivannan, "An efficient protocol for authenticated and secure message delivery in vehicular ad hoc networks", Vehicular Communications, vol. 50, no. 4, **(2016)**, pp. 30-37.

[8] T. Nadeem, P. Shankar, L. Iftode, "A comparative study of data dissemination models for VANETs", Proceedings of the 3rd Annual International Conference on Mobile and Ubiquitous Systems-Workshops, **(2006)**, pp. 1-10.

[9] W. Diffie, M. Hellman, "New directions in cryptography", IEEE transactions on Information Theory, vol. 22, no. 6, **(1976)**, pp. 644-654.

[10] J. Katz, A. Y. Lindell, "Aggregate message authentication codes", Topics in Cryptology–CT-RSA, Springer Berlin Heidelberg, **(2008)**, pp. 155-169.

[11] Intelligent Transportation Systems Committee, "IEEE trial-use standard for wireless access in vehicular environments-security services for applications and management messages", IEEE Vehicular Technology Society Standard, **(2006)**.