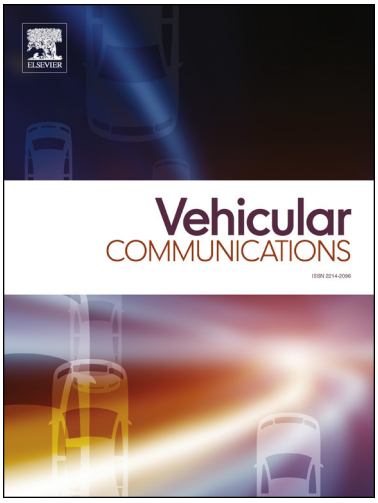
Accepted Manuscript



An efficient protocol for authenticated and secure message delivery in vehicular ad hoc networks

Kiho Lim, D. Manivannan

PII: S2214-2096(16)00011-5
DOI: http://dx.doi.org/10.1016/j.vehcom.2016.03.001
Reference: VEHCOM 46

To appear in: *Vehicular Communications*

Received date: 22 January 2015
Revised date: 20 October 2015
Accepted date: 2 March 2016

Please cite this article in press as: K. Lim, D. Manivannan, An efficient protocol for authenticated and secure message delivery in vehicular ad hoc networks, *Veh. Commun.* (2016), http://dx.doi.org/10.1016/j.vehcom.2016.03.001

An Efficient Protocol for Authenticated and Secure Message Delivery in Vehicular Ad Hoc Networks

Kiho Lim and D.Manivannan *

Department of Computer Science, University of Kentucky, Lexington, KY 40506, USA

Abstract

In Vehicular Ad Hoc Networks (VANETs), anonymity of the nodes sending messages should be preserved, while at the same time the law enforcement agencies should be able to trace the messages to the senders when necessary. It is also necessary that the messages sent are authenticated and delivered to the vehicles in the relevant areas quickly. In this paper, we present an efficient protocol for fast dissemination of authenticated messages in VANETs. It ensures the anonymity of the senders and also provides mechanism for law enforcement agencies to trace the messages to their senders, when necessary.

Key words: Vehicular Ad Hoc Networks, VANETs, Dissemination, Anonymity, Authentication, Security

1. Introduction

Vehicular Ad hoc NETworks (VANETs) are special type of Mobile Ad Hoc Networks (MANETs) that would allow vehicles on roads to form a self-organized network. VANETs are likely to be promising technology of the future because of the benefits it provides such as the following: Accident avoidance warnings could quickly notify drivers of conditions that could cause a collision. In case an accident, the velocity information exchanged between vehicles prior to collision may allow the accident to be reconstructed more easily by law-enforcement agency; it can also help the law-enforcement agency to reach the scene quickly. When VANETs are in widespread use, information about traffic and road hazards could be acquired in real-time and fed into vehicle navigation systems to provide alternate driving routes. In such situations, reliability and authenticity of the information disseminated need to be ensured. VANETs are likely to provide support for cooperative driving applications, which would allow vehicles to navigate without driver intervention. The IEEE 802.11 working group continues to actively develop 802.11p [1] for supporting Intelligent Transportation System (ITS) applications. The 802.11p standard will provide wireless devices with the ability to perform the short-duration exchanges necessary to communicate between a high-velocity vehicle and a stationary roadside unit. This mode of operation, called WAVE (wireless access in vehicle environments) will operate in a 5.9 GHz band and support the Dedicated Short Range Communications (DSRC) standard [2] sponsored by the U.S. Department of Transportation. These standards will support systems that communicate from vehicle-to-roadside, vehicle-to-vehicle, or both. For supporting such wide range of applications, messages exchanged should be authenticated while at the same time the anonymity of the senders should be preserved [3–8].

In the past, several researchers addressed the security issues. Raya et al. [9] proposed a protocol in which each vehicle needs to be preloaded with a large number of private keys, as well as their corresponding anonymous certificates. However, with limited storage space of On-Boars-Units (OBUs) of the vehicles and the nature of highly dynamic network, this is not suitable for VANETs. In [10], a security protocol based on group signature and identity-based signature scheme was proposed to meet the unique requirements of vehicular communication networks. This protocol addressed privacy issues with traceability, so real identity of vehicles are traceable for resolving a dispute. However, the verification of each group signature may cause high computation overhead when the density of the traffic increases. In [11], a spontaneous privacy-preserving protocol based on revocable ring signature with a feature for

* Corresponding author.
Email addresses: kiho.lim@uky.edu (Kiho Lim), mani@cs.uky.edu (D.Manivannan).
URL: http://www.cs.uky.edu/∼manivann (D.Manivannan).

authenticating safety messages locally; but this scheme is not scalable because every vehicle needs to participate in message verification process. Lu et al. [12] proposed an ID-based authentication framework for privacy preservation for VANETs using adaptive self-generated pseudonyms as identifiers. Hao et al. [13] proposed a cooperative message authentication protocol for VANETs to alleviate vehicles' computation burden by allowing vehicles to share verification tasks. Hsiao et al. [14] proposed a broadcast authentication scheme to reduce communication and computation overhead using fast authentication and selective authentication.

In a more recent work [15], Lin et al. proposed a cooperative authentication scheme for VANETs using an evidence-token approach to distribute the authentication workload, without direct involvement of a trusted authority (TA). The vehicles obtain an evidence token as they make contribution to the network and benefits are given to nodes based on the tokens. Wang et al. [16] proposed an accelerated secure in-network aggregation strategy to accelerate message verification and reduce computational overhead using the aggregation structure and TESLA scheme.

Although the studies mentioned above solved the security and privacy issues to different extent, scalability issue has not been addressed well. Also, authenticated messages are not disseminated efficiently under the above protocols. RAISE [17], also tried to address these issues with the help of RSUs, but under their approach, RSUs must notify all other vehicles whether a message from a particular vehicle is valid or not which results in message overhead. Wu et al. [18] proposed a message authentication scheme for intra and inter RSU range using RID key table with all RSUs' ID and session keys. Priya et al. [19] proposed a group authentication protocol to address group authentication and conditional privacy. These scheme reduced communication overhead significantly with the aid of the RSU, but efficient dissemination of messages still remains an issue. We propose an efficient message authentication protocol which overcomes these problems. In our protocol, RSUs not only authenticate messages sent by vehicles fast, but also disseminate messages through the other RSUs to the vehicles in the appropriate areas quickly. Also, in order to efficiently secure messages when forwarded, our approach uses the basic idea behind the onion routing scheme [20] for signing and forwarding messages to the nearby RSUs.

The rest of the paper is organized as follows. Section 2 introduces the system model, assumptions, problem statement and solution objectives. Section 3 presents our proposed protocol in detail. In Section 4 we present analysis of our protocol. Finally, we conclude in Section 5.

2. System Model

In this section, we introduce the system model, assumptions, problem statement and solution objectives.

2.1. *System Model*

We assume that the following three types of entities exist in the network: a Trusted Authority (TA), Road Side Units (RSUs), and On Board Units (OBUs).

- **Trusted Authority (TA):** The TA issues certificates for vehicles. It also manages all private information about vehicles including certificates and shares them securely with RSUs upon request. The TA and the RSUs are able to communicate with each other securely via wired or wireless network, so the RSUs can verify vehicles' certificate with the TA and also can obtain identities of vehicles from the TA when legal authorities need to trace messages to their source.
- **Road Side Units (RSUs):** The RSUs are located along the roads and play an important role in verifying the authenticity and integrity of messages sent by vehicles and forwarding them to other RSUs as well as vehicles within its transmission range. Each RSU stores private information about vehicles such as identity (ID), pseudo ID, public key, shared key and timestamp in a tamper proof device. In addition, each RSU creates a group key and shares it with all vehicles within its transmission range, so the RSU can encrypt messages using the group key and broadcast them to the vehicles within its transmission range. The group key is updated periodically. All the RSUs in the system are assumed to be connected by a network so an RSU can disseminate a message to vehicles in any region quickly with the help of the RSUs in those regions. For simplicity, we assume that all RSUs have same transmission range.
- **On Board Units (OBUs):** An OBU, installed on the vehicles, is assumed to have significantly shorter communication range and less computation power than RSUs.

2.2. *Assumptions*

We assume that any vehicle that is within a target RSU's transmission range is capable of sending/forwarding messages to the RSU through other vehicles using a routing protocol suitable for VANETs [21–24]. RSUs have larger storage space and computation power than OBUs. Also, RSUs are connected to each other through wired or wireless network. Hence, our protocol utilizes RSUs not only to verify the authenticity and integrity of the messages received from vehicles, but also to disseminate those messages to the vehicles in appropriate regions through other RSUs, when necessary. A scenario of how a message is forwarded to an RSU by a vehicle for authentication and further dissemination is illustrated in Figure 1. Figure 2 illustrates how an RSU disseminates an authenticated message to vehicles in appropriate regions through other RSUs.

We also make the following assumptions.

(i) The TA and RSUs are totally trusted and are assumed to be not compromised.
(ii) When a vehicle is registered, the locations of RSUs

and their public keys are stored in the OBU installed in the vehicle and they are updated during renewal of vehicle registration. So, at any given time, an OBU knows the nearest RSU.

2.3. *Problem Statement and Solution Objectives*

When a vehicle senses an incident such as accident, bad road condition due to weather, traffic jam, etc., it needs to send that information to vehicles in appropriate regions so their drivers (or vehicles themselves, if they are self driving) can take appropriate action. When such messages are sent, the integrity and authenticity of the messages sent by the vehicles should be verified while at the same time the anonymity of the senders of these messages should be preserved. i.e, the identities of the vehicles (or drivers) should not be revealed to any other vehicle (driver). The proposed method should be scalable. The protocol should take into consideration the limited computation power of the OBUs. Also, ensuring security is essential due to the nature of messages in VANET. So protocol designed should prevent all possible attacks, which are discussed in Section 4. If an RSU is not within the transmission range of vehicles sending messages, messages are forwarded to the nearby RSU through other vehicles using a routing protocol. Hence the protocol should be robust against malicious relay cars in the network. In this paper, we present a protocol which addresses and solves the above problems.

To preserve the anonymity of the vehicles, our protocol uses pseudo IDs of the vehicles for message transmission. Since RSUs have more computation power, authentication of messages and dissemination of messages are carried out by the RSUs. Since message dissemination is carried out by RSUs, the protocol is scalable and messages are not unnecessarily broadcasted to vehicles in regions that do not require the message.

Our goal is to design a protocol which achieves the following objectives.

- **Privacy preservation:** During the transmission of a message, identities of the vehicles transmitting the message should be protected. However, when the authorities need to obtain user information for legal investigation, they should be able to do so.
- **Message integrity:** Integrity of messages should be ensured during the transmission of messages.
- **Source authentication:** The source of messages should be efficiently authenticated to prevent impersonation attack.
- **Low storage space usage:** OBUs have limited storage space, so its usage should be minimized during the transmission and the verification process.
- **Low communication overhead:** All communication should be done with minimum overhead.
- **Fast verification and efficient dissemination:** Messages should be verified and disseminated quickly and efficiently to all relevant users in regions covered by various RSUs.

Next, we describe our protocol in detail.

3. Proposed Protocol

In this section, we first present the basic idea behind our protocol and then describe the protocol in detail. The notations used in this paper are listed in Table 1.

Table 1
Notations

Notation	Description
R_i	an RSU
V_i	a vehicle
M_i	a message sent by V_i
Ts	timestamp
Sq	Sequence number of a message
h	number of hops the message needs to be forwarded
C_{p_i}	p_i's certificate, where p_i is a vehicle or an RSU
ID_{p_i}	p_i's identity
PID_{p_i}	p_i's pseudo identity
SK_{p_i}	p_i's private key
PK_{p_i}	p_i's public key
K_{G_i}	group key assigned by RSU R_i to vehicles within its transmission range
GID_i	group identity of the vehicles within the transmission range of R_i
K_{A_B}	shared key between A and B
$H()$	cryptographic one-way hash function
dgt_i	a message digest obtained by V_i using hash function $H()$

3.1. *Basic Idea Behind our Protocol*

The proposed protocol has the following phases:

- **Phase 1: Group Key and Symmetric key Establishment.** When a vehicle leaves the area covered by an RSU and enters an area covered by another RSU, it initiates communication with the new RSU and establishes a shared symmetric key with the new RSU so it can send encrypted messages using the symmetric key to the RSU. It also gets its pseudo ID and the group key from the RSU. The group key is used by the RSU to encrypt messages and send them to the vehicles in the area covered

by the RSU. The vehicle uses its pseudo ID in all communications. Here, by the area covered by an RSU, we mean the area that lies within its transmission range of the RSU.

– **Phase 2: Vehicles Sending Messages to RSU for Dissemination:** After completing Phase 1, a vehicle can send messages to the nearby RSU. It uses the shared symmetric key established in Phase 1 to encrypt the message as well as compute the digest of the messages it sends. This message digest helps the RSU in verifying the authenticity and the integrity of the messages. Note that the RSU to which the message is sent may not be within the transmission range of the vehicle sending a message and hence a routing protocol is used for routing the messages to the nearby RSU through intermediate nodes.
– **Phase 3: Verification and Dissemination of Messages by RSUs:**. When an RSU receives the messages sent by the vehicles, it verifies the authenticity and integrity of the messages and forwards the messages to the vehicles in appropriate regions either directly or through other RSUs.

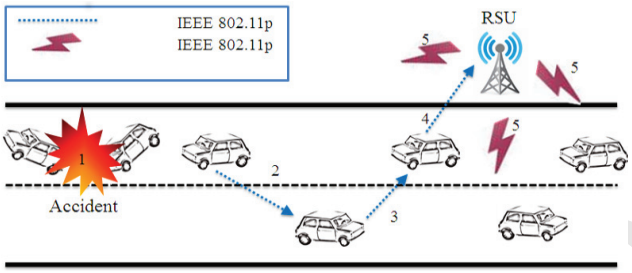


Fig. 1. Message forwarding with onion protocol for verification

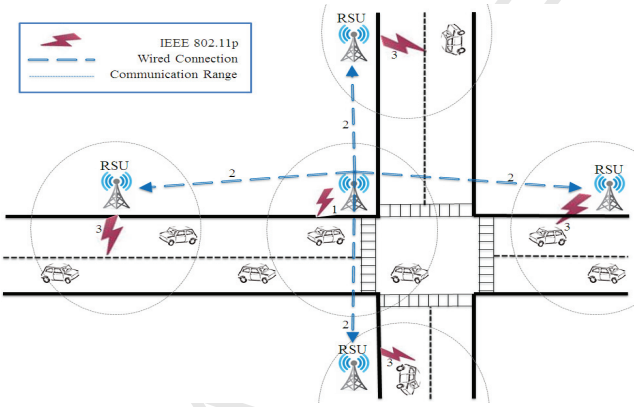


Fig. 2. Disseminating Messages through neighbor RSUs

3.2. *Group key and Symmetric key Establishment*

When a vehicle V_i leaves the region covered by an RSU and enters a region covered by a different RSU, say R_j, it initiates the key establishment process (illustrated in Figure 3). The key establishment process is based on the Diffie-Hellman key agreement protocol [25]. V_i initiates mutual authentication and key establishment by sending the message $g, p, A, \{g, p, A\}SK_{V_i}, C_{V_i}$. In this message, $\{A, B, g, p\}$ are elements of the Diffie-Hellman key agreement protocol: p is a prime number, g is primitive root $mod\ p$, $A = g^a\ mod p$, a is the secret integer kept by V_i, C_{V_i} is the certificate of V_i, $\{g, p, A\}$ is encrypted with the private key SK_{V_i} of V_i so that the RSU can authenticate V_i by decrypting it using the public key PK_{V_i} of V_i. Upon receiving this message, the RSU R_j concatenates the pseudo ID PID_{V_i} of V_i, the number $B = g^b \mod p$ (b kept secret by R_j), the group ID GID_j and the group key K_{G_j} and encrypts all this with the public key PK_{V_i} of V_i and sends it to V_i along with its certificate C_{R_j}. Note that $A\|B\|T_s$ are encrypted using RSU's private key, which means that only authentic RSU can generate this message, hence a fake RSU attack is prevented. We assume all RSUs are trustworthy and not compromised. Finally, V_i sends an acknowledgment for having received B. Thereafter g^{ab} serves as the secret key $K_{V_i\text{-}R_j}$ between V_i and R_j and K_{G_j} is the group key used by R_j for encrypting and sending messages to all vehicles in its region. This completes the mutual authentication and key establishment phase and R_j updates its group table which contains pseudo IDs, original IDs, certificates, shared secret keys. Note that we assume that a routing protocol is used for forwarding messages from V_i to R_j because R_j may not be within the transmission range of V_i. Note that T_s is attached to every message to prevent the replay attack.

$$V_i \rightarrow R_j : g, p, A, \{g, p, A\|T_s\}SK_{V_i}, C_{V_i}$$
$$R_j \rightarrow V_i : \{PID_{V_i}\|B\|GID_j\|K_{G_j}\}PK_{V_i}, \{A\|B\|T_s\}SK_{R_j}, C_{R_j}$$
$$V_i \rightarrow R_j : \{B\|T_s\}SK_{V_i}$$

Fig. 3. Key Establishment Process

3.3. *Vehicles Sending Messages to RSU for Dissemination*

After the key establishment phase between a vehicle V_i and an RSU R_j, V_i can send messages to R_j securely and without revealing its identity as follows. When V_i wants to send a message M about a sensed event, it computes M_i from M as follows and sends it to R_j.

$$M_i = ID_{R_j}, PID_{V_i}, \{M, T_s, S_q\}K_{V_i\text{-}R_j}$$

To compute M_i, the secret key $K_{V_i\text{-}R_j}$, established between V_i and R_j is used to encrypt the message M, the sequence number of the message S_q and the timestamp T_s; the pseudo ID PID_{V_i} of V_i is also appended. Note that when R_j receives the message, it will be able to verify the authenticity of the sender and the integrity of the message based on the pseudo ID and the secret key used for encryption. However, since R_j may not be within the transmission range of V_i, the message may have to be routed through other intermediate

nodes using the available routing protocol. We must make sure that the destination RSU R_j is able to authenticate all the intermediate nodes forwarding this message. For that purpose, we adopt the onion signature scheme [26]. With onion signature, every vehicle forwarding message simply appends its signature and forwards it towards the destination RSU. When an intermediate vehicle V_j receives the message M_i from V_i, it computes M_j, by attaching its signature as follows and forwards it to the next hop on the route using a pre-established routing protocol.

$$M_j = ID_{RSU}, PID_{V_j}, M_i, dgt_j$$

where the digital signature $dgt_j = E\big(H(M_i), K_{V_j\text{-}RSU}\big)$ is obtained by computing the hash of the received message M_i and encrypting it using the shared key $K_{V_j\text{-}RSU}$ between V_j and the destination RSU. This process is repeated until the message reaches the destination RSU.

3.4. *Verification and Dissemination of Messages by RSUs*

When an RSU receives a message sent by a vehicle V_i, since it has a shared key with each vehicle which forwarded the message, it can decrypt the signatures attached by all nodes on the route one by one and verify the authenticity of each node and the integrity of the message received. After it verifies the authenticity and integrity of the message, it disseminates the message to the vehicles in appropriate regions. Since the RSUs have higher computation power than the OBUs, RSUs can verify messages more quickly than OBUs. After checking the integrity and authenticity of a message received from a vehicle, the RSU, say R_i, determines the areas to which the message needs to be propagated. If it needs to be propagated to only vehicles within its transmission range, then it computes the digest $dgt_i = E\big(H(M), SK_{R_i}\big)$ of the message M by encrypting the hash of M. Then it encrypts the message, sequence number and the digest using the group key K_{G_i} as
$M_{type1} = GID_i, \{M, Ts, Sq, dgt_i\}K_{G_i}$
and broadcasts to all vehicles within its transmission range. If the message needs to be propagated to vehicles that are not within its transmission range, then it computes M_{type2} as

$$M_{type2} = ID_{receiver\_RSU}, ID_{sender\_RSU}, \{M, Ts, Sq, h, dgt_i\}PK_{receiver\_RSU}$$

where $dgt_i = E\big(H(M), SK_{R_i}\big)$ and sends the message to the respective neighboring RSUs by setting the number of hops h (i.e., the number of RSUs, through which the message needs to propagate) to the appropriate value. When an RSU receives this message, it decrements the value of h by 1 and forwards it to its neighbors if $h > 1$. Based on the nature of the message, an intermediate RSU can decide whether or not to disseminate the message to the vehicles within its transmission range. The detailed protocol is given in Figure 4.

When a vehicle V_i wants to send a message M to the nearby RSU
Let $M_i = ID_{RSU}, PID_{V_i}, \{M, T_s, S_q\}K_{V_i\text{-}RSU}$
Send M_i (i.e., to the next hop towards the RSU)

When a vehicle V_j receives the message M_i from V_i
Let $M_j = ID_{RSU}, PID_{V_j}, M_i, dgt_j$,
  where $dgt_j = E\big(H(M_i), K_{V_j\text{-}RSU}\big)$
Send M_j (i.e., to the next hop towards the RSU)

When an RSU with id ID_{RSU_i} receives a message M_k from vehicle V_k
It peels of the onion M_k, and retrieves the message M
Sets h based on nature of message
Let $M_{type1} = GID_i, \{M, Ts, Sq, dgt_i\}K_{G_i}$,
  where $dgt_i = E\big(H(M), SK_{R_i}\big)$
Disseminate M_{type1} to all vehicles in the table if needed
if $h > 0$ **then**
  $h = h - 1$
  Let $M_{type2} = ID_{receiver\_RSU}, ID_{RSU_i}$,
  $\{M, Ts, Sq, h, dgt_i\}PK_{receiver\_RSU}$,
    where $dgt_i = E\big(H(M), SK_{RSU_i}\big)$
  Forward M_{type2} to relevant neighboring RSUs
end if

When an RSU with id ID_{RSU_j} receives a message M_{type2} from a neighboring RSU with ID ID_{RSU_i}
Decrypt M_{type2} and retrieve M
Let $M_{type1} = GID_j, \{M, Ts, Sq, dgt_j\}K_{G_j}$,
  where $dgt_j = E\big(H(M), SK_{RSU_j}\big)$
Disseminate M_{type1} to all vehicles in the table
if $h > 0$ **then**
  $h = h - 1$
  Let $M_{type2} = ID_{receiver\_RSU}, ID_{RSU_j}$,
  $\{M, Ts, Sq, h, dgt_j\}PK_{receiver\_RSU}$,
    where $dgt_j = E\big(H(M), SK_{R_j}\big)$
  Forward M_{type2} to relevant RSUs
end if

When a vehicle V receives a message M_{type1} from an *RSU*
Decrypts the message M_{type1} using group key
and consumes it

Fig. 4. The Protocol

3.5. *Discussion*

Under our protocol, when a vehicle enters a region covered by an RSU (i.e., the area that lies within the transmission range of the RSU), it initiates key establishment with the RSU and establishes a symmetric key with the RSU so that it can encrypt all the messages it needs to send to the RSU while in its region. It also obtains a pseudo ID and the group ID and group key. The vehicle uses only its pseudo ID in all communications and hence the anonymity of the vehicle is preserved. The RSU uses the group key to encrypt messages it sends to the vehicles in its region. So

all messages are encrypted and no intruder can decrypt the messages. Vehicles do not broadcast messages. When a vehicle senses an event and wants to disseminate it to other vehicles in specific regions, it simply sends it to the nearby RSU (through the intermediate vehicles, if the RSU is not within the vehicle's transmission range). The nearby RSU authenticates the vehicles sending the message and also checks the integrity of the message and then disseminates the message to the vehicles in the relevant regions through other RSUs. When a message sent by a vehicle needs to be traced to the vehicles sending the message, it can be done with the help of the RSUs because the RSUs maintain the table binding the pseudo IDs of the vehicles to their real IDs.

A vehicle never broadcasts any message to other vehicles. Dissemination of messages to other vehicles is the responsibility of the RSUs and hence this approach is scalable. Messages exchanged are generally small so OBUs can use symmetric key for encryption without incurring much computation overhead and RSUs can use the public key of receiving RSUs for encrypting and sending messages to them; however, the protocol can be easily modified so that the RSUs use symmetric key for encryption after establishing a shared symmetric key with the receiving RSUs.

4. Comparison with Related Work and Security Analysis

4.1. *Comparison with existing related works*

In this section, we compare our protocol with some existing related works. The protocol proposed in [9] ensures secure communication of messages. But, it is not scalable because each vehicle needs to be preloaded with private keys of all other vehicles and their corresponding anonymous certificates. As the number of vehicles grows in the network, not only maintaining those security data is difficult, but also storage issues may occur due to the large number of private keys and certificates that need to be stored in the limited space available in OBUs. In contrast, in our protocol, vehicles do not need to store other vehicles' private keys and their certificates to authenticate messages since RSUs authenticate messages on behalf of vehicles, thus the storage requirements is very low compared to aforementioned protocol.

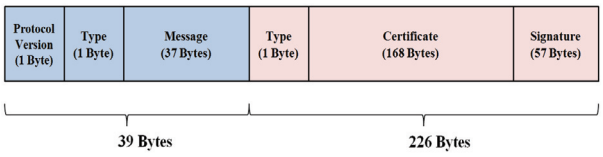


Fig. 5. The format of a signed message from IEEE Standard

When a vehicle sends a message, a certificate and a signature is attached to the message in order to authenticate the message and ensure the integrity of the message. Figure 5 shows the format of a signed message derived from IEEE 1609.2 Standard [27]; the size of a message is 265 bytes including 39-Bytes of unsigned message field, 169-Bytes of a certificate, and 57-Bytes of signature.

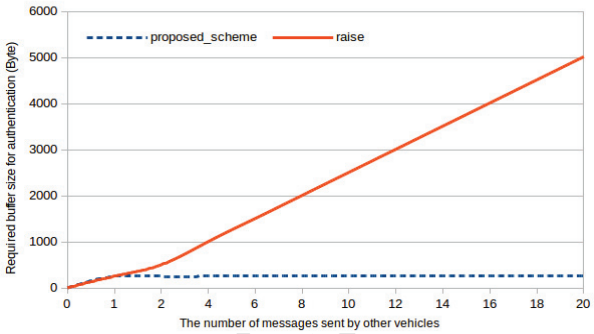


Fig. 6. Storage usage vs. Traffic load

Figure 6 shows the relationship between the storage usage and traffic load. The storage usage represents the buffer size required on OBUs for messages waiting to be authenticated and the traffic load represents the number of messages sent by other vehicles. Since each signed message is 265 Bytes long, the necessary buffer size for storing the unauthenticated messages increases under RAISE [17] as the traffic load increases whereas under our protocol the required buffer size for storing the received message is constant. RAISE performs better than the PKI based protocol [27] and group signature protocol [10] in terms of packet loss, packet delay, and communication overhead because the vehicles can simply authenticate messages once validation messages are received from the RSU; however, each vehicle has to buffer all messages received from other vehicles until validation messages arrive. Thus, the vehicles require more buffer space as message traffic increases. Hence, the required buffer space is proportional to traffic load. On the other hand, our protocol does not keep messages in the buffer of OBUs until they are authenticated as RSUs directly broadcast authenticated messages to vehicles within their transmission range. Thus, under our protocol, buffer required for storing messages at OBUs does not increase as the traffic load increases.

Under our protocol, messages sent by vehicles do not need to be authenticated and verified by other vehicles; authentication of messages is done by RSUs which have higher computation power as well as lager storage than OBUs in vehicles. Figures [7,8,9] compare RAISE [17] and our protocol with respect to the number of retransmissions and the number of original messages sent as the number of vehicles participating varies from 10 to 30 in the network. The number of message transmissions under our protocol is obtained using the following equation:

$$T_n^1 = (V_n * M_n) * 1B + (M_n + 1U), \quad (1)$$

where T_n^1 is the number of messages communicated, V_n is the number of vehicles in the network, $1B$ is 1 broadcast and

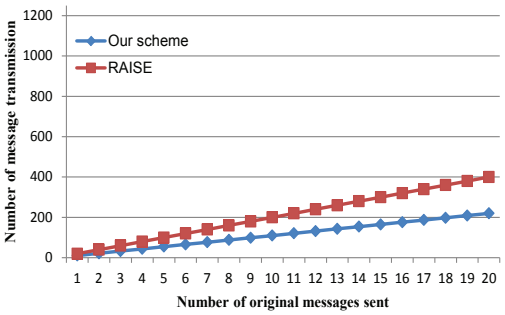


Fig. 7. Number of message transmission with 10 vehicles

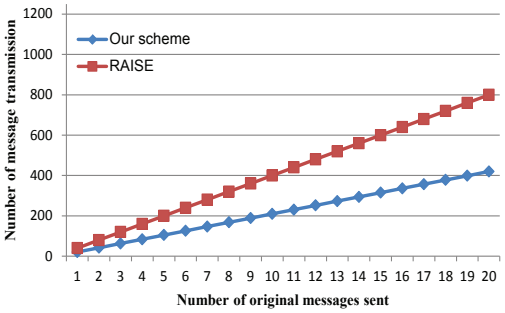


Fig. 8. Number of message transmission with 20 vehicles

$1U$ is 1 unicast. And the number of message transmission for RAISE is obtained by following equation:

$$T_n^2 = (V_n * M_n) * 2B \quad (2)$$

,where T_n^2 is the number of message communication, V_n is the number of vehicles in the network, and $2B$ is 2 broadcasts. Under RAISE, every message is stored in each vehicle until a validation message from the RSU arrives, so a vehicle sending a message broadcasts it once and the RSU broadcasts it again after verifying the message. *However, under our protocol, in order to minimize the communication overhead, vehicles sending a message just unicasts it to the RSU and only the RSU broadcasts the verified message to the vehicles in relevant areas (through other RSUs, if necessary). so, under our protocol, the number of message retransmissions is minimized and this reduction clearly becomes prominent as the number of vehicles sending messages increases.*

There are other approaches [16,14,18,19] to address communication and computational overhead. Hsiao et al. [16] proposed a scheme addressing excessive signature verification requests by exploiting sender's ability to predict its own future beacons and quickly spread bogus signatures. Using fast authentication and selective authentication, they try to reduce consumption of the computational resources. However, receivers still need to verify messages received from other vehicles; this is still a overhead for OBUs with their limited computation power. In our scheme, vehicles

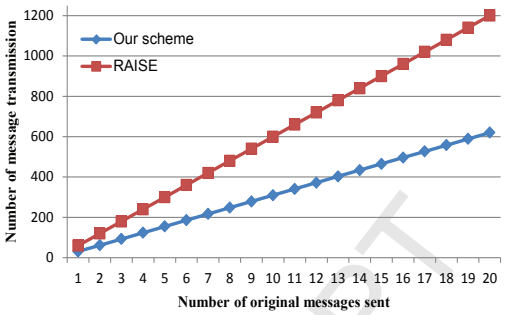


Fig. 9. Number of message transmission with 30 vehicles

do not need to verify all messages received. Messages are first authenticated and verified for integrity by an RSU, and then disseminated to the vehicles in relevant regions. Hence communication overhead is much less under our protocol because vehicles only need to verify messages received from RSU that are meant for them. Wang et al. [14] proposed an accelerated secure in-network aggregation strategy to expedite message verification and reduce communication overhead. This scheme uses the aggregation structure to detect potential misbehavior and TESLA-based broadcast authentication scheme to avoid expensive encryption algorithms. However, the TESLA is not suitable for dynamic and time critical environment of VANET as delay in verification process is unavoidable with it. So, receivers need to wait until they receive the key to read the received message earlier even if it's very time sensitive message. The situation may get worse if the sender vehicle and the receiver vehicle are traveling in opposite direction because it might cause delay of the message delivery or the key could be lost. In our scheme, when RSUs send messages to vehicles, they use symmetric group key, therefore, once a vehicle obtains a group key and symmetric key from RSU, computation overhead for verification is significantly reduced and vehicles can receive and read messages quickly.

Wu et al. [18] proposed a technique for message authentication with the aid of RSU; however, they assume that all vehicles maintain a RSU key table where all RSUs' IDs and session keys are stored, which makes this scheme not scalable. It is also assumed that all vehicles are reachable to RSU in one-hop communication; but due to significant difference in the transmission ranges of vehicles and RSUs, and sparsely deployed RSUs, one-hop communication between a vehicle and the nearest RSU may not become a reality in the near future. In addition, if a receiver is not within the transmission range of the same RSU, then the receiver needs to request another message for corresponding RSU's information to the sender and then needs to verify the message with a RSU in its region. This causes 4-way communication and it's not suitable for highly mobile nodes in VANETs because the receiver must stay within its RSU's region until it receives a requested message from the sender to verify the message with the RSU. In our scheme,

verified messages are quickly disseminated through neighboring RSUs and vehicles within the transmission range of other RSUs do not directly send a request to the sender and verify with another RSU within its transmission range. Messages sent by vehicles are verified by the first RSU once and then the messages are immediately disseminated to vehicles in relevant regions. Priya et al. [19] proposed a group authentication protocol for verifying large number of messages and improving message loss ratio. However, this scheme also does not address the situation when messages need to be forwarded to reach a destination RSU.

4.2. *Security Analysis*

4.2.1. *Preventing Propagation of Redundant Messages*

In many of the existing protocols, when a vehicle observes a phenomena it disseminates the observed phenomena to all the vehicles in relevant regions. This approach can result in the propagation of redundant messages; this is because several vehicles may observe the same phenomena and propagate the same message. *However, under our protocol, observed phenomena are only sent to the RSU for further dissemination. So, RSUs can determine and suppress propagation of redundant messages.*

4.2.2. *Message Integrity*

When a node senses an event, it sends a message to the nearby RSU about the event so that the RSU can forward the message to the respective regions. The message is encrypted with the shared key between the vehicle and the RSU. When an intermediate vehicle receives the message, it computes the digest of the received message, encrypts the digest using its shared key with the RSU and forwards it to the next hop towards the RSU. This facilitates the RSU receiving the message to verify the authenticity of each vehicle through which the message traveled as well as the integrity of the message; the RSU then forwards the message to the vehicles in its region and/or other regions through other RSUs, as is necessary. Messages forwarded by the RSUs to vehicles in their regions are encrypted using the group key. So, integrity of messages is ensured.

4.2.3. *Source Authentication and Privacy*

Every vehicle is assigned a pseudo ID and symmetric key by the RSU. Also, an RSU maintains a group table that contains pseudo IDs, original IDs, certificates, shared secret keys and timestamps of all vehicles within its transmission range. If a message sent from a pseudo ID can be decrypted by the RSU that receives the message using the corresponding shared secret key, then the RSU can find the identity of the sender from its table and authenticate the source. A vehicle never uses its real ID in any communication and hence the anonymity of the vehicles is preserved. Also, a pseudo ID is issued again if a vehicle enters another RSU's region and the issued pseudo ID is re-issued frequently if a vehicle stays in a RSU's region for a long time to prevent tracking of the pseudo identity.

4.2.4. *Computation Overhead*

Vehicles simply forward messages to an RSU by attaching its signature for verification and only the RSU verifies authenticity of the messages. When vehicles receive messages from an RSU encrypted using the group key, they simply decrypt the message and consume the message; this reduces the computation overhead on the OBUs because there is no public key cryptography involved for encryption, unlike RAISE [17].

4.2.5. *Fast Verification and Efficient Dissemination*

In our protocol, the authenticity and integrity of the messages are verified by RSUs that have higher computation power than OBUs. Also, they can communicate with neighboring RSUs securely via wired or wireless connection. Thus, messages can be verified and disseminated quickly through other RSUs to vehicles in appropriate regions. Therefore, fast verification and efficient dissemination are achieved. Moreover, RSUs can suppress duplicate messages sent by vehicles in the same region (i.e., messages about the observation of the same event by different vehicles in the same region).

4.2.6. *Man in the Middle Attack*

The symmetric key establishment process in our protocol uses the Diffie-Hellman key agreement protocol. Even though Diffie-Hellman key agreement protocol is vulnerable to man-in-the-middle attack [28], our protocol does not suffer from this weakness because of the following reasons: When a vehicle V_i enters the region covered by an RSU, it encrypts g, p, A and the timestamp T_s using its private key PK_{V_i}. An intermediate vehicle can carry out the man-in-the-middle attack only if it is also an authentic vehicle which has a (public, private) key pair already established by the TA, in which case the RSU can trace the messages to the intruder.

4.2.7. *Other Attacks*

In VANETs, various other types of attacks exist [29] and their consequences may be detrimental to the users. In this section, we discuss how our protocol prevents such threats.

(i) **Sybil attack:** This is a type of security threat that exists when a malicious node can present multiple identities at once. In our protocol, each vehicle is assigned a pseudo ID by an RSU after its certificate is verified and vehicles encrypt outgoing messages using a symmetric key established with the RSU. Hence, a malicious node is not able to use multiple identities at once.

(ii) **Replay attack:** In this attack, an attacker keeps a message that was sent earlier and tries to use the same message later by rebroadcasting it. In order to prevent the replay attack, every message in our pro-

tocol uses a timestamp to guarantee the freshness of the message. This requires loose synchronization of the clocks. Given the widespread use of GPS devices, they can be used for synchronizing clocks loosely.

(iii) **Message fabrication/alteration attack:** In this attack, an attacker tries to modify, delete, or alter existing messages. In our protocol, when a vehicle sends a message, it attaches it digital signature that is obtained by computing the hash of the original message and encrypting it with its private key. Since only the sender can create its signature, an RSU (receiver) can verify the integrity of the message received. Hence, fabrication/alteration attack is prevented. However, if a vehicle is not willing to forward a message sent by another vehicle, it can deleted the message. Handling nodes that do not cooperate has been extensively studied in the context of ad hoc networks. Similar mechanisms can be used for handling such nodes.

(iv) **Malicious relay vehicles:** In our protocol, relay cars forward messages using onion signature. Every vehicle forwarding a message simply appends its signature to the message and forwards it to the destination RSU. So relay vehicles are not able to read or modify received message. Only option a malicious relay car would have is not to forward messages. We do not address this issue of a malicious node enroute dropping messages. Many solutions for handing malicious nodes during route establishment for Mobile ad hoc networks have been proposed in the literature.

(v) **Fake RSU attack:** An adversary may pretend to be a real RSU in this type of attack. In our protocol, however, a fake RSU attack is infeasible to succeed because a RSU appends its signature using its private key during symmetric key establishment process so the receiver knows who actually sent the signed message by decrypting it using the RSU's public key. Hence the fake RSU attack is prevented. We assume RSUs are reliable and not compromised.

Acknowledgment

We sincerely thank the anonymous reviewers for their constructive comments which helped us improve the quality of the paper both in content and presentation.

5. Conclusion

In this paper, we presented an efficient protocol for propagating the phenomena (such as accidents, road conditions, etc) observed by vehicles in VANETs to vehicles in appropriate regions so they can use them to make informed decision. Our protocol utilizes RSUs that have higher computation power than OBUs to disseminate authenticated messages about the observed phenomena by vehicles within an RSUs' transmission range. Since multiple vehicles within the transmission range of an RSU can observe the same phenomenon and inform the RSU about it, the RSU can suppress these messages about the observation of the same phenomenon from disseminating further. Moreover, in our approach, the RSUs have the ability to verify the authenticity of the sender and the integrity of the message before disseminating it to the other vehicles. Our approach preserves the anonymity of the senders while at the same time has the ability to trace a message to its sender, when required by legal authorities and law enforcement agents.

References

[1] L. Armstrong and W. Fisher, "Status of Project IEEE 802.11 Task Group p: Wireless Access in Vehicular Environments (WAVE)," http://grouper.ieee.org/groups/802/11/Reports/tgp_update.htm, May 2010, meeting Update.

[2] N. H. T. S. Administration, "Vehicle safety communications project, final report," U.S. Department of Transportation, Tech. Rep., Apr. 2006.

[3] K. M. Manvi S.S, "Message authentication in vehicular ad hoc networks: Ecdsa based approach," in *Proceedings of International Conference on Future Computer and Communication, 2009. ICFCC 2009.*, 2009, pp. 16 – 20.

[4] K. Chhoeun, S.A.; Ayutaya, "A novel message fabrication detection for beaconless routing in vanets," in *Proceedings of the International Communication Software and Networks, 2009. ICCSN '09. Conference*, 2009, pp. 453–457.

[5] P. P. C Harsch, A Festag, "Secure position-based routing for vanets," in *Proceedings of the IEEE Vehicular Technology Conference, 2007. IEEE VTC'07*, 2007.

[6] C. Aslam, B. Zou, "Distributed certificate and application architecture for vanets," in *Proceedings of IEEE Military Communications Conference, 2009. MILCOM 2009.*, 2009, pp. 1–7.

[7] S. Biswas, "Proxy signature-based rsu message broadcasting in vanets," in *Proceedings of 25th Biennial Symposium Communications (QBSC), 2010*, 2010, pp. 5–9.

[8] J. Kim and J. Song, "A pre-authentication method for secure communications in vehicular ad hoc networks," in *Proceedings of 8th International Conference on Wireless Communications, Networking and Mobile Computing (WiCOM), 2012*, Shanghai, China, Sept. 2012, pp. 1 – 6.

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

[10] X. Lin, X. Sun, P. H. Ho, and X. Shen, "Gsis: A secure and privacy-preserving protocol for vehicular communications," *IEEE Transactions on Vehicular Technology*, vol. 56, no. 6, pp. 3442–3456, 2007.

[11] H. Xiong, K. Beznosov, Z. Qin, and M. Ripeanu, "Efficient and spontaneous privacy-preserving protocol for secure vehicular communication," in *Proceedings of 2010 IEEE International Conference on Communications (ICC)*, May 2010, pp. 1–6.

[12] H. Lu, J. Li, and M. Guizani, "A novel id-based authentication framework with adaptive privacy preservation for vanets," in *Proceedings of Computing, Communications and Applications Conference (ComComAp), 2012*, Hong Kong, Jan. 2012, pp. 345 – 350.

[13] Y. Hao, T. Han, and Y. Cheng, "A cooperative message authentication protocol in vanets," in *Proceedings of Global Communications Conference (GLOBECOM), 2012 IEEE*, Anaheim, CA, Dec. 2012, pp. 5562 – 5566.

[14] X. Wang and P. Tague, "Asia: Accelerated secure in-network aggregation in vehicular sensing networks," in *Proceedings of the 10th Annual IEEE Communications Society Conference*

on Sensor, Mesh and Ad Hoc Communications and Networks (SECON). IEEE, 2013, pp. 514–522.

[15] X. Lin and S. Li, "Achieving efficient cooperative message authentication in vehicular ad hoc networks," *Vehicular Technology, IEEE Transactions on*, vol. 62, no. 7, pp. 3339–3348, 2013.

[16] H.-C. Hsiao, A. Studer, C. Chen, A. Perrig, F. Bai, B. Bellur, and A. Iyer, "Flooding-resilient broadcast authentication for vanets," in *Proceedings of the 17th annual international conference on Mobile computing and networking*. ACM, 2011, pp. 193–204.

[17] C. Zhang, X. Lin, R. Lu, and P. H. Ho, "`raise`: An efficient rsu-aided message authentication scheme in vehicular communication networks," in *Proceedings of IEEE International Conference Communications, 2008. ICC '08.*, Beijing, May 2008, pp. 1451 – 1457.

[18] H.-T. Wu, W.-S. Li, T.-S. Su, and W.-S. Hsieh, "A novel rsu-based message authentication scheme for vanet," in *Proceedings of the fifth International Conference on Systems and Networks Communications (ICSNC)*. IEEE, 2010, pp. 111–116.

[19] K. Priya and K. Karuppanan, "Secure privacy and distributed group authentication for vanet," in *Proceedings of 2011 International Conference on Recent Trends in Information Technology (ICRTIT)*. IEEE, 2011, pp. 301–306.

[20] D. Goldschlag, M. Reed, and P. Syverson, "Onion routing for anonymous and private internet connections," *Communications of the ACM*, vol. 42, no. 2, pp. 39–41, 1999.

[21] C. Lochert, H. Hartenstein, J. Tian, H. Füßler, D. Hermann, and M. Mauve, "A Routing Strategy for Vehicular Ad Hoc Networks in City Environments," in *Proceedings of the IEEE Intelligent Vehicles Symposium*, Jun 2003, pp. 156–161.

[22] J. Tian, L. Han, K. Rothermel, and C. Cseh, "Spatially Aware Packet Routing for Mobile Ad Hoc Inter-Vehicle Radio Networks," in *Proceeding of the IEEE Intelligent Transportation Systems, 2003.* , vol. 2. IEEE, 2003, pp. 1546–1551.

[23] B.-C. Seet, G. Liu, B.-S. Lee, C.-H. Foh, K.-J. Wong, and K.-K. Lee, "A-STAR: A Mobile Ad Hoc Routing Strategy for Metropolis Vehicular Communications," in *Proceedings of the third International IFIP-TC6 Networking Conference, Networking Technologies, Services, and Protocols; Performance of Computer and Communication Networks; Mobile and Wireless Communications (NETWORKING 2004)*, ser. Lecture Notes in Computer Science. Springer Berlin / Heidelberg, 2004, vol. 3042/2004, pp. 989–999.

[24] J. Bernsen and D. Manivannan, "`river`: A reliable inter-vehicular routing protocol for vehicular ad hoc networks," *Computer Networks*, vol. 56, no. 17, pp. 3795–3807, 2012.

[25] W. Diffie and M. E. Hellman, "New directions in cryptography," *IEEE Transactions on Information Theory*, vol. 22, no. 6, pp. 644–654, 1976.

[26] M. Raya, A. Aziz, and J.-P. Hubaux, "Efficient secure aggregation in vanets," in *Proceedings of the 3rd international workshop on Vehicular ad hoc networks. VANET '06*, Sept. 2006, pp. 67–75.

[27] `IEEE Standard` 1609.2, "Ieee standard for wireless access in vehicular environments - security services for applications and management messages," *IEEE Standard*, Aug 2013.

[28] R. L. Rivest and A. Shamir, "How to expose an eavesdropper," *Communications of the ACM*, vol. 27, no. 4, pp. 393–394, 1984.

[29] M. N. Mejri, J. Ben-Othman, and M. Hamdi, "Survey on vanet security challenges and possible cryptographic solutions," *Vehicular Communications*, 2014.