Vehicular Communications 4 (2016) 30–37

Contents lists available at ScienceDirect

Vehicular Communications

www.elsevier.com/locate/vehcom

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

Kiho Lim, D. Manivannan*

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

ARTICLE INFO

Article history:
Received 22 January 2015
Received in revised form 20 October 2015
Accepted 2 March 2016
Available online 7 March 2016

Keywords:
Vehicular Ad hoc Networks
VANETs
Dissemination
Anonymity
Authentication
Security

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.

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 of 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 identities 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 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

* Corresponding author.
E-mail addresses: kiho.lim@uky.edu (K. Lim), mani@cs.uky.edu (D. Manivannan).
URL: http://www.cs.uky.edu/~manivann (D. Manivannan).

http://dx.doi.org/10.1016/j.vehcom.2016.03.001
2214-2096/© 2016 Elsevier Inc. All rights reserved.

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.

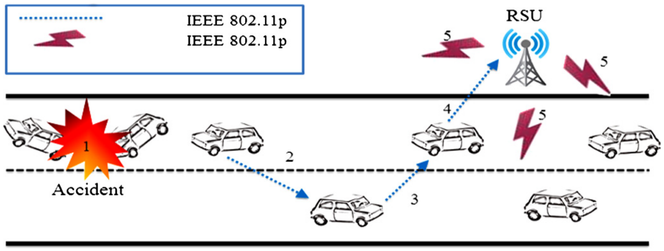

Fig. 1. Message forwarding with onion protocol for verification.

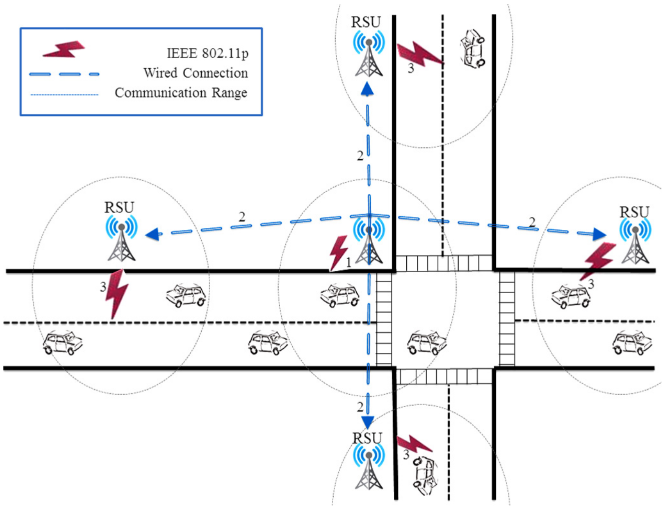

Fig. 2. Disseminating Messages through neighbor RSUs.

- **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 Fig. 1. Fig. 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.