Vehicular Communications ••• (••••) •••–•••

Contents lists available at ScienceDirect

Vehicular Communications

www.elsevier.com/locate/vehcom

HCPA-GKA: A hash function-based conditional privacy-preserving authentication and group-key agreement scheme for VANETs

Jie Cui [a,b,c], Xuefei Tao [a,b,c], Jing Zhang [a,b,c], Yan Xu [a,b,c], Hong Zhong [a,b,c,*]

[a] School of Computer Science and Technology, Anhui University, Hefei, 230039, China
[b] Institute of Physical Science and Information Technology, Anhui University, Hefei, 230039, China
[c] Anhui Engineering Laboratory of IoT Security Technologies, Anhui University, Hefei, 230039, China

ARTICLE INFO

Article history:
Received 15 April 2018
Received in revised form 14 August 2018
Accepted 7 September 2018
Available online xxxx

Keywords:
VANETs
Anonymous authentication
Conditional privacy
Hash function
Group key
Chinese remainder theorem

ABSTRACT

In recent years, the continuous economic development and the emergence of new technologies have made vehicles an indispensable travel tool in people's lives. However, the intelligent and efficient control and management of the increasing number of vehicles to improve traffic efficiency has become a problem. Vehicular ad hoc networks (VANETs) are one of the most important development trends that are used for communication between vehicles to provide information such as weather conditions, road conditions, and traffic jams and their status, which is significant in improving traffic safety and efficiency. In this scenario, authenticating the entity that is sending the message is a critical task to ensure secure communication in VANETs. In this paper, we propose a conditional privacy-preserving authentication scheme based on the hash function, which does not use complex bilinear mapping and elliptic curve encryption for identity authentication to prevent illegal vehicle interference and ensure the legitimacy of the source. Meanwhile, a group key agreement mechanism based on the Chinese remainder theorem (CRT) is proposed to distribute the group key for authenticated vehicles. The group key can be updated when the vehicle joins and leaves the group. In the process of anonymous message generation and verification, analysis of the results shows that our proposed scheme satisfies the security privacy requirements and has significant advantages in terms of computation cost and communication overhead compared with existing schemes.

1. Introduction

With the increasing number of vehicles in the city, Intelligent Transportation System (ITS) is one of the most promising directions for the efficient management of urban transport. Based on the concept of Mobile Ad-hoc Network (MANET), researchers and vehicle manufacturers have introduced the Vehicular Ad-hoc Networks (VANETs) to build the next-generation transportation systems. As a variant of MANET, VANET is a distributed, less infrastructure, self-organizing communication network, which is built among moving vehicles. VANET aims to provide attractive services such as security services, including curve speed warnings, emergency vehicle warnings, lane changing assistance, pedestrian crossing warnings, traffic violation warnings, road intersection warnings, and road condition warnings [1]. Moreover, it can also provide weather information, traffic information, gas station or restaurant location and other comfort and interactive services such as Internet access. In general, VANET is mainly composed of three parts: the trusted authority (TA), roadside unit (RSU) and vehicle. The TA provides the necessary network connection and stores information about the vehicle and the RSU. Each vehicle is equipped with an on-board unit (OBU), which is a tamper-proof device. Vehicles exchange traffic information through wireless communication.

A typical VANET structure is shown in Fig. 1. There are two types of communication in VANETs: vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I). In V2V communication, vehicles in the same RSU range are allowed to exchange secret information. Meanwhile, V2I communication is mainly between the vehicle and an RSU fixed on the side of the road. Both V2V and V2I communications are controlled by short-range wireless communication protocol called dedicated short-range communication (DSRC) protocol, which improves the overall security and efficiency of the transportation system. The DSRC protocol allows vehicles to broadcast information about road traffic and vehicle conditions periodically every 100–300 ms [2] in open wireless channels. If the information is not properly handled, communication in VANETs is vulnerable to various attacks, such as intercepting, modifying, replaying, and deleting messages [3].

The authentication mechanism is a universally accepted method to ensure communication security in VANETs, and all certified ve-

* Corresponding author.
E-mail address: zhongh@ahu.edu.cn (H. Zhong).

https://doi.org/10.1016/j.vehcom.2018.09.003
2214-2096/

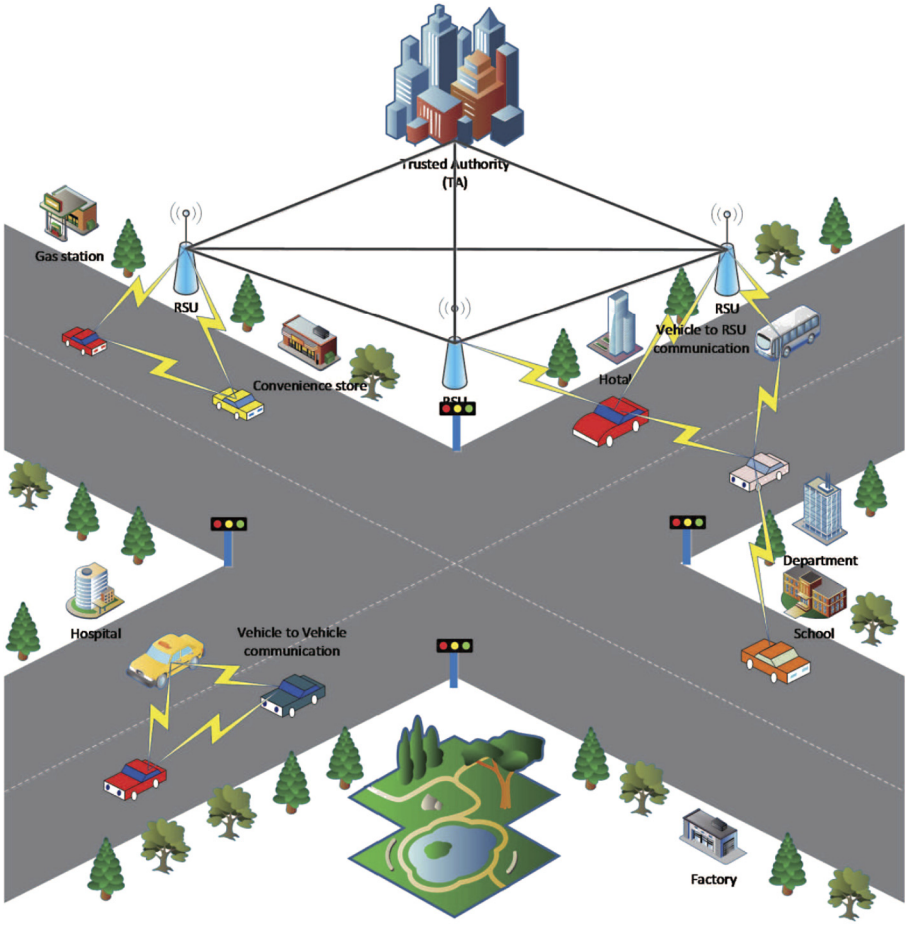

Fig. 1. System model.

hicles can be easily identified. Authentication is the process of verifying the identity of a vehicle before authorizing access to the network. The authentication process ensures that only effective vehicles can become part of VANETs [4]. Most of the existing conditional privacy-preserving authentication (CPA) protocols use either bilinear pairing techniques or elliptic curve cryptography. Bilinear pairings and elliptic curves are very expensive to compute compared to the general hash function. These protocols suffer from heavy computational burdens and some security weaknesses. In this paper, we propose a hash function-based conditional privacy-preserving authentication and group-key agreement (HCPA-GKA) scheme. The vehicle sends a login message to the RSU. If the sign in is accepted by the RSU, it is forwarded to the TA, which then verifies the identity of the vehicle and allows the certified vehicle to communicate with other vehicles and corresponding RSU. The TA is responsible for authenticating all vehicles in the network.

Authentication is the first barrier to restrict vehicles from entering VANET. However, for authenticated vehicles, message confidentiality is also a concern when they communicate with each other. Therefore, we introduce a group-key agreement mechanism based on the Chinese Remainder Theorem (CRT). Under this mechanism, the TA distributes group key for vehicles that have been authenticated in the vicinity of the same RSU. The communication among vehicles in the group is encrypted with the group key to ensure privacy and security. We used a simple method to replace the complex and time-consuming encryption and decryption operations to accomplish the group key distribution. The group key can be dynamically updated when the vehicle joins or leaves the group. A leaving group member cannot access the current communication process (forward security), and the newly added group member cannot access the previous communication process (backward security). The main contributions of this paper are briefly described as follows.

- A novel conditional privacy authentication scheme is proposed, which is implemented using a generalized hash function and does not rely on the bilinear pairing and elliptic curve technique with high computational cost.
- We propose a simple group key distribution mechanism to complete the group key distribution task securely.
- An in-depth comparative analysis of existing schemes in computing and communication overhead shows that our proposed scheme performs better than existing CPA schemes.

The rest of this paper is organized as follows. Section 2 reviews the existing CPA protocol in VANETs. Section 3 describes the relevant preliminary knowledge and background. Section 4 describes our proposed HCPA-GKA scheme in detail. Section 5 analyzes the safety of the proposed HCPA-GKA scheme. Section 6 analyzes the performance of the HCPA-GKA scheme in comparison with existing schemes. Finally, a summary of the scheme is provided in Section 7.

2. Related works

To solve the security and privacy issues in VANETs, the authentication mechanism has been extensively investigated by researchers. Raya and Hubaux [5] used anonymous certificates to design conditional privacy-preserving model by modifying the public

Please cite this article in press as: J. Cui et al., HCPA-GKA: A hash function-based conditional privacy-preserving authentication and group-key agreement scheme for VANETs, Veh. Commun. (2018), https://doi.org/10.1016/j.vehcom.2018.09.003