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

Contents lists available at ScienceDirect

Vehicular Communications

www.elsevier.com/locate/vehcom

EPA-CPPA: An efficient, provably-secure and anonymous conditional privacy-preserving authentication scheme for vehicular ad hoc networks

JiLiang Li [a], Kim-Kwang Raymond Choo [b], WeiGuo Zhang [c], Saru Kumari [d], Joel J.P.C. Rodrigues [e,f,g,h], Muhammad Khurram Khan [i], Dieter Hogrefe [a]

[a] Institute of Computer Science, University of Goettingen, Goettingen 37077, Germany
[b] Department of Information Systems and Cyber Security, University of Texas at San Antonio, San Antonio, TX 78249, USA
[c] State Key Laboratory of Integrated Services Networks, Xidian University, Xi'an 710071, China
[d] Department of Mathematics, Ch. Charan Singh University, Meerut, Uttar Pradesh, India
[e] National Institute of Telecommunications (Inatel), Brazil
[f] Instituto de Telecomunicações, Portugal
[g] ITMO University, St. Petersburg, Russia
[h] University of Fortaleza (UNIFOR), Brazil
[i] Center of Excellence in Information Assurance (CoEIA), King Saud University, Saudi Arabia

ARTICLE INFO

Article history:
Received 5 April 2018
Received in revised form 15 May 2018
Accepted 8 July 2018
Available online xxxx

Keywords:
Authentication
Privacy-preserving
Provably-secure
Vehicular ad hoc networks

ABSTRACT

Unlike wired networks, vehicular ad hoc networks (VANETs) are subject to a broader range of attacks due to its wireless broadcast nature. One of the potential cryptographic solutions to ensure authentication and privacy preservation is conditional privacy-preserving authentication (CPPA) schemes. Although a number of CPPA schemes have been proposed in the literature, existing approaches generally suffer from limitations such as the security problem of system private keys, high computation requirement during certificate generation and message verification phases. To resolve these issues, in this paper, it presents a provably-secure CPPA scheme for VANETs and demonstrates that the proposed solution provides both security and privacy required in a VANET application. It also demonstrates its utility in terms of computation and communication overheads and owns an optimal performance compared with rather related schemes.

1. Introduction

Due to constant and rapid advancements in the development of wireless communication and network technologies, vehicular ad hoc networks (VANETs) have regained renewed interest due to their capability to support vehicles with wireless devices to communicate with other vehicles and roadside units (RSUs) and ensure traffic safety and enhance driving efficiency [1–5]. Other benefits associated with VANETs include collision avoidance, lane merging, traffic optimization, toll collection, location-based services, infotainment, etc. [6]. In the literature, such settings have also been considered Internet of Vehicles and smart cities [7,8].

One can think of VANETs as a combination of mobile ad hoc networks (MANETs) with vehicles (e.g. cars, buses, trucks and motorcycles) and RSUs [3,9,10]. Unlike nodes in a MANET, vehicles are not usually resource constrained in terms of power, storage space and computing capability. A typical VANET includes trusted authorities (TAs), RSUs (e.g. placed on road sides or other installations), and onboard units (OBUs) equipped on vehicles [3,11,12] – see Fig. 1.

Communications in VANETs, such as vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I), use dedicated short range communication (DSRC), which is a short medium range communications protocol [11]. Every vehicle could communicate with adjacent vehicles and the nearby RSUs located at the roadside through the OBU installed in the vehicle and DSRC protocol. For example, on-vehicle OBUs periodically broadcast traffic-related information covering factors such as position, weather conditions, direction, speed, and traffic situation. Such information allow participating vehicles in the vicinity to take the required actions, for example take an alternate route to avoid a traffic accident, traffic congestion, etc. [13,14]. RSUs and other vehicles can also transmit traffic-related information (e.g. an accident that has just taken place) to the traffic administration department or other relevant department (e.g.

E-mail address: wgzhang@foxmail.com (W.G. Zhang).

https://doi.org/10.1016/j.vehcom.2018.07.001
2214-2096/

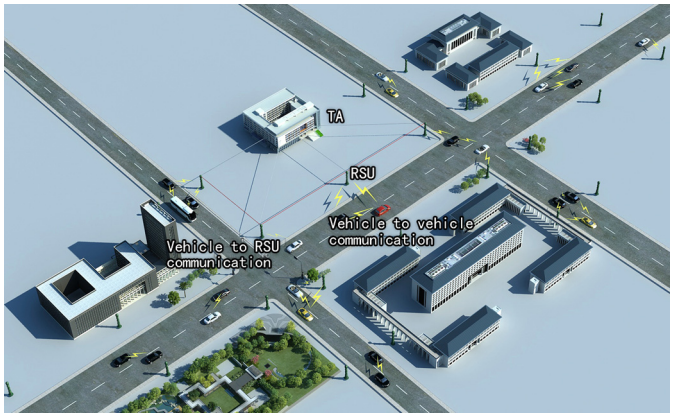

Fig. 1. An example of VANETs.

law enforcement or fire department), so that the necessary actions can be undertaken [15]. Hence, it is not surprising that VANETS and the many variants (e.g. Internet of Vehicles, intelligent transport systems, and smart cities) have received recent attention [6].

Similar to other wireless networks, there are a number of other features important to VANETS, such as the following:

Security: Once attackers have control over the communication channels, they could easily eavesdrop, tamper, replay or even drop messages sent within VANETs. In other words, designers of VANETs need to ensure the system is secure against a wide range of attacks such as masquerading, replaying, tunneling, message modification, key and certificate replication attacks [6,11,15]. For example, a malicious adversary may hijack and modify the initial messages or masquerade one legitimate vehicle to broadcast 'fake' messages, resulting in chaos or traffic incidents [15]. Hence, the capability to ensure the authenticity of messages from vehicles in VANETs is crucial.

Anonymity: In addition, if the vehicle user sends his/her identity to RSUs or other vehicles without masking, a malicious attacker may track the user's routes through capturing of the messages. The leakage of routes may have real-world consequences such as physical stalking, kidnapping, and assassination (e.g. a malicious adversary intercept and replace intercepted messages with fabricated messages in order to reroute the victim's vehicles). Therefore, anonymity is another key feature in VANETs [16].

Traceability (and *conditional privacy*): If a misbehaving vehicle transmits malicious or suspicious information to RSUs or nearby vehicles, then the system needs to have the capability to identify the vehicle (and the owner) so that the vehicle (and the owner) can be taken to task (e.g. monetary penalties to other criminal sanctions). Thus, both traceability and conditional privacy are important features [15]. Conditional privacy restricts to the TA being the only party who can extract the vehicle's real identity.

Conditional privacy-preserving authentication (CPPA) schemes such as those presented in [3,6,9,15–22] can be used to achieve both security and privacy related properties in VANETs. There are, however, limitations in these existing schemes as discussed in Section 2.

In this paper, it introduces an efficient, provably-secure and anonymous conditional privacy-preserving solution for VANETs in order to overcome limitations in existing CPPA schemes. To be specific, four main contributions of our work are described as follows.

- First, the vulnerabilities of existing schemes are retrospected and analyzed. Meantime, several security weaknesses of these schemes are pointed out. Then, it gives the vehicular system architecture consisting of network model and design goals.
- Second, this paper presents an efficient, provably-secure and anonymous CPPA protocol for VANETs. To improve efficiency further, the proposed CPPA scheme added the function of batch verification.
- Third, this paper proves the security of the proposed CPPA scheme deeply (e.g. taking the advantage of the random oracle model) in order to demonstrate the proposed efficient and anonymous CPPA scheme could satisfy security and privacy requirements within VANETs.
- Finally, we also conducted an analysis of the computation overhead and the communication overhead to prove that the proposed efficient and anonymous CPPA scheme processes more favorable performance compared with existing solutions for VANETs.

The rest of this paper is organized as follows. Section 2 provides an overview of some related works in this field. Some background knowledge is prepared in Section 3. Section 4 presents an efficient and anonymous conditional privacy-preserving scheme. Section 5 and Section 6 evaluate the security and performance of our proposed method respectively. At last, we conclude this paper in Section 7.

2. Related literature

This section briefly reviews existing literature on CCPA schemes designed for VANETs.

In 2006, Gamage et al. [18] introduced an identity-based ring signature solution to ensure privacy for VANETs applications. However, the presented approach does not provide traceability and this implies a lack of conditional privacy. A year later in 2007, Raya et al. [6] introduced a CPPA solution based on anonymous certificates. Specifically, to mask the vehicle's real identity, a large number of public/private key pairs and corresponding certificates based on Public Key Infrastructure (PKI) are preloaded into the memory space of vehicles' OBUs and the OBU randomly selects a pair of public/private key that can be used for authentication. This imposes storage requirements for each vehicle (e.g. to store its public/private key pairs and corresponding certificates), and the TA (e.g. to store all vehicles' certificates). For a large system with vehicles constantly joining and leaving, it is not a trivial task to search for and identify a misbehaving vehicle in practice. In 2008, a new CPPA solution using bilinear pairing is designed by Lu et al. [20]. In this solution, the RSU sends a temporary anonymous certificate to the vehicle which passes by the region of the RSU. The RSUs also provide the vehicles a new anonymous certificate periodically to enforce conditional privacy. However, this solution has a low efficiency. In the same year, Lin et al. [23] provided a privacy-preserving protocol utilizing group signature technique, which provides traceability. However, in Lin et al.'s solution, each vehicle has to store the revocation list to avoid communicating with the 'blacklisted' vehicles. Therefore, as the number of revoked vehicles increases, the vehicles will need to spend considerably amount of time on the verification phase alone. This is clearly not practical.

In 2008, Zhang et al. [22] constructed an identity (ID)-based batch authentication protocol based on pairing-based cryptography. In their approach, both vehicles and RSUs do not need to store any certificate. Moreover, their solution provides batch verification for multiple messages. In other words, this CPPA solution overcomes the limitation in the approaches of Raya et al. [6] and Lu et al. [20]. However, in the approach of Zhang et al. [22], a long-term system master secret s is embedded in the vehicle's tamper-proof devices, which could be extracted by an adversary (e.g. via side-channel attacks [24]), particularly when the adversary has physical access to the tamper-proof devices.

In 2009, Jiang et al. [19] presented an authentication scheme using the binary authentication tree (BAT), in which the RSU could