Available online at www.sciencedirect.com

ScienceDirect

Computer Communications 31 (2008) 2803–2814

computer communications

www.elsevier.com/locate/comcom

A secure and efficient communication scheme with authenticated key establishment and privacy preserving for vehicular ad hoc networks ☆

Chun-Ta Li [a], Min-Shiang Hwang [b,*], Yen-Ping Chu [c]

[a] *Department of Computer Science and Engineering, National Chung Hsing University, 250 Kuo Kuang Road, Taichung, Taiwan 402, ROC*
[b] *Department of Management Information Systems, National Chung Hsing University, 250 Kuo Kuang Road, Taichung, Taiwan 402, ROC*
[c] *Department of Computer Science and Information Engineering, Tunghai University, 181 Section 3, Taichung Harbor Road, Taichung, Taiwan 407, ROC*

Available online 23 December 2007

Abstract

Privacy and security should be paid much more attention in secure vehicular ad hoc networks (VANETs). However, as far as we know, few researches on secure VANET protocols have addressed both the privacy issues and authenticated key establishment. Therefore, in this work, a lightweight authenticated key establishment scheme with privacy preservation to secure the communications between mobile vehicles and roadside infrastructure in a VANET is proposed, which is called SECSPP. Our proposed scheme not only accomplishes vehicle-to-vehicle and vehicle-to-roadside infrastructure authentication and key establishment for communication between members, but also integrates blind signature techniques into the scheme in allowing mobile vehicles to anonymously interact with the services of roadside infrastructure. We also show that our scheme is efficient in its implementation on mobile vehicles in comparison with other related proposals.

Keywords: Key establishment; Mutual authentication; Privacy; Security; Vehicular ad hoc networks

1. Introduction

Vehicular ad hoc networks (VANETs) with interconnected vehicles and numerous services promise superb integration of digital infrastructure into many aspects of our lives, from vehicle-to-vehicle, roadside devices, base stations, traffic lights, and so forth. A network of a huge number of mobile and high-speed vehicles through wireless communication connections has become electronically and technically feasible and been developed for extending traditional traffic controls to brand new traffic services that offer large traffic-related applications. Applications of vehicular ad hoc networks range from rapid transportation development to civil life-support operations such as electronic toll systems, vehicle-collision avoidance, collection of traffic information, vehicle diagnostics, cooperative driving, and entertainment-related applications. In VANETs, the vehicles act as mobile nodes, and self-organized, wireless communications occur with each other directly, by multi-hop communications, and do not rely on a predefined or centralized infrastructure to keep the network connected such as with MANETs (Mobile Ad Hoc Networks) [1,3,22,25,28,30]. Some important characteristics need to be considered for VANETs and are quite different from MANETs shown in Table 1. Jungels et al. [21] simply classify the VANET applications into two types, namely: vehicle-to-vehicle communication and vehicle-to-roadside infrastructure communication, respectively. For the former type, vehicles are able to communicate with others in order to receive some valuable traffic information from them,

☆ This work was supported in part by Taiwan Information Security Center (TWISC), National Science Council under the Grants NSC95-2218-E-001-001, NSC95-2218-E-011-015, and NSC96-3114-P-001-002-Y.

* Corresponding author. Tel.: +886 4 22855401; fax: +886 4 22857173. *E-mail address:* mshwang@nchu.edu.tw (M.-S. Hwang).

0140-3664/$ - see front matter © 2008 Elsevier B.V. All rights reserved.
doi:10.1016/j.comcom.2007.12.005

Table 1
Comparisons of VANETs and MANETs

Characteristics	MANET	VANET
Network topology	Random deployment	Deployment stands on the direction of the roadway route
Mobility	Normal speed (less than 20 km/h)	High speed (more than 40 km/h)
Route direction	From any direction	Driving directions (or reverse of driving direction)
Communication models	Peer-to-peer	Vehicle-to-vehicle and vehicle-to-roadside device
Resource constraints	Limited computation ability and power	Unlimited computation ability and power
Connected range and nodes	Small scale and few nodes (10–100 communication nodes)	Large scale and many nodes (more than 100 nodes)
Application areas	Military, calamity, emergency, and civil environments	Traffic safety, traffic control, and electronic toll systems, etc.

such as roadway conditions, accidents on the road, etc. For the latter type, Dotzer et al. [4] further classify it into two communication modes, namely: (1) transmitting messages from fixed roadside nodes to mobile vehicular nodes (i.e. transmission of traffic signals and entertainment services), (2) transmitting messages from mobile vehicular nodes to fixed roadside nodes (i.e. an ambulance can transmit emergency signals to control the destined traffic lights). In this issue, we would like to propose a new secure communication scheme and apply it to above-mentioned two situations for VANETs.

Unlike traditionally wired networks are protected by several lines of defense such as firewalls and gateways, security attacks on such wireless networks may come from any direction and target all nodes. Therefore, VANETs are susceptible to intruders ranging from passive eavesdropping to active spamming, tampering, and interfering due to the absence of basic infrastructure and centralized administration. Moreover, the main challenge facing vehicular ad hoc networks is user privacy. Whenever vehicular nodes attempt to access some services from roadside infrastructure nodes, they want to maintain the necessary privacy without being tracked down for whoever they are, wherever they are and whatever they are doing. It is considered as one of the important security requirements that should be paid more attention for secure VANET schemes, especially in privacy-vital environment. A number of security threats to vehicular ad hoc networks have been addressed [5,13,14,18]. In [19,20], Raya et al. introduced three kinds of security threats in VANETs, including attacks on safety-related applications, attacks on payment-based applications, and attacks on privacy. They further proposed certain recommended mechanisms to achieve security issues in VANETs. For example, establishing vehicular public key infrastructure, setting up an Event Data Recording (EDR) machine and tamper-proof hardware in vehicles, etc. In [15], Leinm*ü*ller et al. proposed some security requirements and two solutions including reactive and proactive security concepts for securing VANETs. In [17], Moustafa et al. developed an AAA (Authentication, Authorization, and Accounting) scheme for vehicular environments by employing EAP-Kerberos and EAP-TLS authentication protocols, however, an online centralized authority (CA) is not suitable for VANETs due to the CA being a single point and it is susceptible to damage the security of the entire network whenever it fails or is compromised.

According to the security threats and privacy issues into consideration, our proposed scheme must maintain the following essential requirements:

- Providing mutual authentication between the two communicating parties such as vehicle-to-vehicle and vehicle-to-roadside device.
- Allowing mobile vehicles to anonymously interact with the roadside devices to access the service.
- The system must have light overheads in terms of computational costs and high efficiency.
- Generating dynamic session key to secure the communications between nodes in VANETs.
- Providing data confidentiality and integrity in applications of vehicle-to-vehicle and vehicle-to-roadside device communications;
- Preventing impersonation attacks, that is, no one can impersonate another authorized member to cause service abuse problems and to damage the security of VANETs.
- Preventing eavesdropping, in other words, an intruder cannot discover some valuable information from communications between members in VANETs.

In summary, our proposed scheme has two main advantages that compared with other related schemes: one is that it allows anonymity of the communications between vehicles and roadside infrastructure, and the other one is that it combines the authenticated key establishment into the scheme by using the following cryptographic techniques including non-interactive key agreement, blind signature, one-way hash function, and nonces. To the best of our knowledge, this work is the first attempt to provide a secure communications model with mutual authentication, key establishment protocol, and privacy preservation in vehicular ad hoc networks.

The rest of this article is organized as follows. In Section 2, we describe some basic preliminaries of our scheme. In Section 3, we present our secure communication scheme for VANETs, followed by the security analysis and performance evaluation in Section 4. Finally, we conclude this article in Section 5.

2. Preliminaries

As a preliminary, we used some cryptographic techniques and basic tools in our scheme. The security of our