Ad Hoc Networks 10 (2012) 1445–1456

Contents lists available at SciVerse ScienceDirect

Ad Hoc Networks

journal homepage: www.elsevier.com/locate/adhoc

MLAS: Multiple level authentication scheme for VANETs

T.W. Chim [a,*], S.M. Yiu [a], Lucas C.K. Hui [a], Victor O.K. Li [b]

[a] Department of Computer Science, The University of Hong Kong, Hong Kong
[b] Department of Electrical and Electronic Engineering, The University of Hong Kong, Hong Kong

ARTICLE INFO

Article history:
Received 10 February 2011
Accepted 29 March 2012
Available online 25 April 2012

Keywords:
Secure vehicular sensor network
Message classification
Authentication
Batch verification
Proxy re-encryption

ABSTRACT

The vehicular ad hoc network (VANET) is an emerging type of network which enables vehicles on roads to inter-communicate for driving safety. The basic idea is to allow arbitrary vehicles to broadcast ad hoc messages (e.g. traffic accidents) to other vehicles. However, this raises the concern of security and privacy. Messages should be signed and verified before they are trusted while the real identity of vehicles should not be revealed, but traceable by authorized party. Existing solutions either rely too heavily on a tamper-proof hardware device, or do not have an effective message verification scheme. In this paper, we propose a multiple level authentication scheme which still makes use of tamper-proof devices but the strong assumption that a long-term system master secret is preloaded into all tamper-proof devices is removed. Instead the master secret can be updated if needed to increase the security level. On the other hand, messages sent by vehicles are classified into two types – regular messages and urgent messages. Regular messages can be verified by neighboring vehicles by means of Hash-based Message Authentication Code (HMAC) while urgent messages can only be verified with the aid of RSUs nearby by means of a conditional privacy-preserving authentication scheme. Through extensive simulation, we show that our multiple level authentication scheme is much more efficient that those RSU-aided authentication scheme as long as the proportion of urgent messages is less than 100%. The verification delay required can be up to 110 times smaller than other protocols. Our implementation shows that batch verification may not be as efficient as expected. In case without batch verification, the verification delay required by our scheme can even be up to 173 times smaller.

1. Introduction

The vehicular ad hoc network (VANET) is an emerging type of network by which driving safety can be enhanced through inter-vehicle communications or communications with roadside infrastructure. It is an important element of the Intelligent Transportation Systems (ITSs) [1]. In a typical VANET, each vehicle is assumed to have an on-board unit (OBU) and there are road-side units (RSUs) installed along the roads. A trusted authority (TA) and maybe some other application servers are installed in the backend. The OBUs and RSUs communicate using the Dedicated Short Range Communication (DSRC) protocol [2] over the wireless channel while the RSUs, TA, and the application servers communicate using a secure fixed network (e.g. the Internet). The basic application of a VANET is to allow arbitrary vehicles to broadcast safety messages (e.g. road condition, traffic accident information) to other nearby vehicles and RSU such that other vehicles may adjust their travelling routes and RSU may inform the traffic control center to adjust traffic lights for avoiding possible traffic congestion. This paper focuses on inter-vehicle communications.

Like other communication networks, security issues have to be well-addressed. For example, the message from an OBU has to be integrity-checked and authenticated

* Corresponding author.
E-mail addresses: twchim@cs.hku.hk (T.W. Chim), smyiu@cs.hku.hk (S.M. Yiu), hui@cs.hku.hk (L.C.K. Hui), vli@eee.hku.hk (V.O.K. Li).

1570-8705/$ - see front matter © 2012 Elsevier B.V. All rights reserved.
http://dx.doi.org/10.1016/j.adhoc.2012.03.020

before it can be relied on. Otherwise, an attacker can modify a vehicle's safety message or even impersonate a vehicle to transmit a fake safety message. For example, a boy may impersonate an ambulance to request other vehicles to give way to him or request nearby RSUs to change traffic lights to green so that he can catch up an appointment with his girl friend. Besides, privacy is another issue that raises a lot of concern in recent years. A driver may not want others to know its travelling routes by tracing messages sent by its OBU. Someone may argue that in current road system, a vehicle can already be traced by means of its license plate number. However, most parts of VANET are automatic (e.g. the status of a vehicle will be broadcasted by its OBU periodically and automatically) and such an automatic messaging system should not leak a driver's privacy any easier than the current situation. Thus an anonymous communications protocol is needed. While being anonymous, a vehicle's real identity should be able to be revealed by a trusted party when necessary. For example, the driver who sent out fake messages causing an accident should not be able to escape by using an anonymous identity. Thus we call this kind of privacy conditional privacy.

Privacy-preserving authentication schemes have been discussed in the research community for a while. Examples include [3–5]. However, all of them propose having the same treatment to all messages. This is obviously improper. Some messages are more urgent than others. In fact, in daily operation of a VANET, more than 90% of messages are regular (non-urgent) messages such as those about change of travelling speed and turning direction. Urgent messages only appear when there are accidents or unexpected road conditions. Therefore, adopting the same authentication scheme (and with the same security level) to both regular and urgent messages usually yields a waste of power. In this paper, we propose to first classify messages sent by a vehicle into regular messages and urgent messages. Regular messages refer to those that are sent periodically (every 500 ms according to the DSRC [2] standard). They are usually about the current status of a vehicle including its travelling speed, turning direction and brake application. Urgent messages, on the other hand, refer to those that are sent when there are critical road situations such as accidents and road blocking. Messages sent by a fire engine or an ambulance are also considered as urgent since slowing down their travelling speed can cause loss of human life or property. We then propose different treatments on the two kinds of messages. For regular messages, the receiving vehicle only needs to show that they were generated and sent by a trusted tamper-proof device while for urgent messages, we provide a mechanism for a trusted party to reveal the real identity of the sender. That is, attacks caused by a vehicle are accountable.

Talking about tamper-proof devices, some existing schemes also assume the existence of them. However, their security assumption is too strong to be accepted. They assume that a long-term master secret key is preloaded into all tamper-proof devices and all security functions rely on it. In this sense, once one of the temper-proof devices is cracked and the system master secret is leaked to an attacker, the whole system will be compromised. In this paper, we use tamper-proof devices with a weaker security assumption. We still need a system master secret for security functions. However, instead of preloading them into tamper-proof devices permanently, we propose to transmit them to vehicles in a secure way. Also the system master secret can be updated when any tamper-proof device is proved to be compromised. This can help to raise the security level of the system.

Through security analysis and extensive simulation, we show that our schemes achieve the goals of authenticity, conditional privacy preserving and traceability. At the same time, the verification time is much shorter than previous schemes. The verification delay required by our scheme can be up to 110 times smaller than other protocols. On the other hand, our implementation shows that batch verification may not be as efficient as expected. In case without batch verification, the verification delay required can even be up to 173 times smaller. Hence our scheme is both effective and efficient.

The remainder of this paper is organized as follows. Related works are presented in Section 2. The system model and the problem statement are described in Section 3. Some preliminaries about bilinear maps are given in Section 4. Our schemes are presented in details in Section 5. The analysis and evaluation of our schemes are given in Sections 6 and 7. Finally, Section 8 concludes the paper.

2. Related work

In terms of integrity-checking and authentication, digital signature in conventional public key infrastructure (PKI) [6] is a well accepted choice. However, requiring a vehicle to verify the PKI signatures of other vehicles by itself as in works like [7] induces two problems as mentioned in [4]. First, the computation power of an OBU is not strong enough to handle all verifications in a short time, especially in places where the traffic density is high. Second, to verify a message from an unknown vehicle involves the transmission of a public key certificate which causes heavy message overhead. Therefore, one possible approach is to let the nearby RSU to help a vehicle to verify the message of another.

Related problems have been addressed in some recent works [4,3,8–15]. In [3], the IBV protocol was proposed for vehicle-to-RSU communications. The RSU can verify a large number of signatures as a batch using three *pairing* operations (see the Section 4 for what a pairing operation is). However, their work relies heavily on a tamper-proof hardware device, installed in each vehicle, which preloads the system-wide secret key. Once one of these devices is cracked, the whole system will be compromised. On the other hand, by actual implementation, we found that batch verification is not as efficient as they argue. Finally, the IBV protocol is not designed for vehicle-to-vehicle communications.

In a more recent work [4], the RAISE protocol was proposed for vehicle-to-vehicle communications. The protocol is software-based. It allows a vehicle to verify the signature of another with the aid of a nearby RSU. To notify other vehicles whether a message from a certain vehicle is valid, a hash value of 128 bytes needs to be broadcasted. There