Computer Networks 134 (2018) 78–92

Contents lists available at ScienceDirect

Computer Networks

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

NECPPA: A novel and efficient conditional privacy-preserving authentication scheme for VANET

Seyed Morteza Pournaghi[a], Behnam Zahednejad[b], Majid Bayat[c], Yaghoub Farjami[a,*]

[a] Department of Computer Engineering, University of Qom, Qom, Iran
[b] Department of Computer Engineering, University of Shiraz, Shiraz, Iran
[c] Department of Computer Engineering, Shahed University, Tehran, Iran

ARTICLE INFO

Article history:
Received 15 July 2017
Revised 7 December 2017
Accepted 15 January 2018
Available online 31 January 2018

Keywords:
VANETs
Authentication
Conditional privacy preserving
Security
Formal proof
ProVerif analysis

ABSTRACT

Vehicular Ad-hoc Networks (VANETs) are growing in recent decades providing real-time communication between vehicles for a safer and more comfortable driving. The main idea of VANET is the fact that vehicles can broadcast ad-hoc messages such as traffic incidents and emergency events. The security of such networks is quite critical. This paper firstly reviews and analyzes the main authentication schemes in VANET to compare their pros and cons. We then propose a new authentication scheme which provides secure communications in VANET. Our proposed scheme is a combination of Road Side Unit Based (RSUB) and Tamper Proof Device Based (TPDB) schemes. A novel idea in NECPPA is to let the keys and the main parameters of the system be stored in the Tamper Proof Device (TPD) of Road Side Units (RSUs). Since, there is always a secure and fast communicational link between TA and RSU, inserting TPD in RSUs is much more efficient than inserting them in OBUs. It also should be noted that due to the fact that in NECPPA scheme, the main key of TA (master secret key) is not stored in all OBUs, the compromise or hacking a single OBU does not threaten the whole network despite what happens in TPDB scheme which makes the whole vehicles re-register and change their secret keys. In addition, our proposed scheme is much more cost efficient compare to other on-line RSUB schemes, as it does not need the establishment of on-line RSUs in the whole roads. We also prove the security of our scheme with formal proof and ProVerif automatic analysis tool. The simulation results show that the efficiency and performance of our proposed scheme in VANETs have improved compare to other schemes.

1. Introduction

Due to the daily increase of vehicles in recent years and consequently the increase of accidents, vehicles manufacturers and urban traffic managers have a tendency to use smart vehicles. Establishment of security in such vehicles using smart processes independent of the abilities of the driver is an important concern. These vehicles form a special type of ad-hoc network in which the nodes of the network are the vehicles. This network is called VANET.

The main difference of VANETs with wireless networks which use IEEE 802.11p [1] standard is the fact that the connection between the nodes of the VANETs are established for a short interval without any central infrastructure or base station. The network consists of a set of vehicles (nodes) which are in movement having no fixed position. None of them play the role of a router or access point.

VANETs are a special type of MANETs in which vehicles are the nodes. Vehicles can identify other vehicles around them to form a network by connecting to them and do necessary communications.

High movement of nodes is the main property of such networks which enables them to change their pattern immediately. Considering the lack of security of VANET, designing a secure communication protocol is the main challenge of this field.

The idea of VANET was first posed in 1998 by an electronic engineering group named Delphi Delco Electronics Systems which was cooperating with IBM. VANETs make different kinds of communication including vehicle-to-vehicle communication (V2V), vehicle-to-infrastructure communication (V2I) or a combination of them, namely vehicle-to-vehicle-to infrastructure communication (V2V2I). Vehicles communicate with each other in an autonomous

* Corresponding author.
E-mail addresses: sm.Pournaghi@stu.qom.ac.ir (S.M. Pournaghi), farjami@qom.ac.ir (Y. Farjami).

https://doi.org/10.1016/j.comnet.2018.01.015
1389-1286/

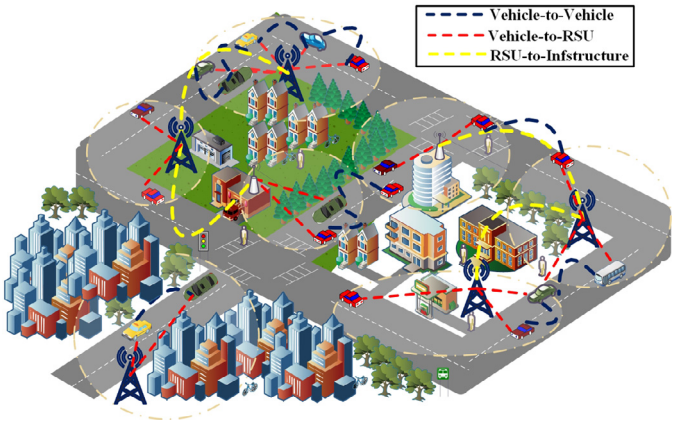

Fig. 1. Communications inside VANETs.

manner to make a wireless network operate without any infrastructure.

In the V2V communication, the vehicles such as cars, trucks, buses, etc. exchange the information (direction, speed, acceleration, vehicle size, etc.) to predict and warn safety threats and potential accidents (e.g., collisions) without direct intervention of RSUs [2,3]. In some schemes, secure communications of vehicles (V2V) is based on reputation and trust methods, in which vehicles share encryption keys to send and receive files with each other [4,5].

Considering the fact that such networks have no trouble in consuming energy and using computational resources, they can change their topology immediately to provide flexibility for the whole network. For instance, a vehicle can connect to two different VANETs simultaneously to receive necessary information. The coverage area of VANETs may be a circle with radius of several kilometers. Every vehicle can communicate with other vehicles which are 2–3 km away by using IEEE 802.11p and DSRC [6] standards. Short range communications is provided in these networks as well. DSRC is the communication protocol between OBUs that operates in 5.9 GHz.

VANETs are safe, convenient and may be commercialized. One can connect to central stations or Internet via VANETs to exchange data with them. Vehicle-to-vehicle communication is the most useful type of VANET communication. VANETs are one of the main components of intelligent transportation systems. Many researches have been done in recent years. The main importance of direct communications in such networks is the safety of vehicles and traffic reduction. Fig. 1 shows the communications inside VANETs [7–9].

1.0.1. Applications of VANET

Network properties and capabilities are important for future vehicles. In such networks, they can exchange a wide variety of information such as weather conditions, traffic information, multimedia data, alarm signals and any other kind of information.

Today, VANETs have important advantages compare to cellular and dedicated networks. Such advantages have motivated manufacturers to invest on them to make them developed separately. The most important part of VANET is the sensors that should be implemented in different parts of the vehicle to report the circumstance of the vehicle and the external environment to the driver. It can listen to the commands of the driver or receive information of other vehicles.

The inherent properties of ad-hoc networks make them useful for the safety of vehicles and traffic. These properties include being short-range, forming a network immediately, changing the topology and transferring signals from the origin to the destination. Vehicles can get informed of any incident happening in hundreds of meters away in less than a second. They can recognize the traffic, ask questions or receive responses from other vehicles to become aware of the traffic of the street or the cross-road and the side alleys. Fig. 1 shows a schematic of this condition.

When a sudden incident happens in the street or the road, the vehicles on the front or the back communicate with each other with the aid of a central station or the urban traffic manager. Drivers can experience a safe and comfortable driving. They can get definite and better decisions with the aid of a central station to inform the police or the urban traffic manager. VANETs are useful specially in adverse weather conditions such as snow, dust, rain and etc. Vehicles can guide each other in foggy and such adverse weather conditions to avoid incidents.

1.1. Related work

So far, many authentication schemes have been proposed to secure VANETs. In general, four types of schemes have been suggested:

1. Schemes based on a huge number of anonymous keys (denoted as HAB) [10,11]
2. Group signature based schemes [12–14] and ring signature based schemes [15–18] (denoted as GSB)
3. The RSU based schemes [19–22] (denoted as RSUB)
4. The tamper-proof device based schemes [23–25] (denoted as TPDB)

- HAB schemes

The main idea of HAB (Huge Anonymous Based) protocols is that vehicles need to pre-load a huge pool of anonymous certificates (about 43,800) and their corresponding private keys based on the anonymity level they require. These certificates are signed by TA.

Note that there is not any information about the real identity of users in these certificates. Thus these certificates are thoroughly anonymous. The number of pre-loaded certificates in each vehicle should be large enough to provide security and privacy preservation for a long time, e.g. one year. Each vehicle can update its certificates during the annual inspection. Firstly vehicles select randomly an anonymous certificate and the corresponding private key to sign the messages that they want to broadcast. The verifying vehicles obtain the public key of the signer to verify the signature using the anonymous certificate.

In these schemes, TA stores the credential information of certificates which have been delivered to all vehicles. Thus TA is able to obtain the real identity of users if needed. Revocation process is the greatest weakness of HAB schemes. The requirement to load a large number of certificates in each vehicle makes the management of certificates inefficient, as revoking one vehicle requires the revocation of a large number of certificates loaded in Certificate Revocation List (CRL). This problem becomes essentially fatal when the CRL becomes large. The CRL maintains all the revoked anonymous public keys. Note that when a signature has been verified, the public key should also be authenticated. However, verifying the authenticity of public keys in vehicular network is not as easy as that of wired networks. Thus increasing the number of revoked users causes extreme increase of the CRL volume which increases the verification time of the signatures. The reason is that before verifying the signature, vehicles should verify a large CRL to make sure that the signer was not revoked.

- GSB schemes

The idea of group signatures was first proposed by Chaum and van Heyst [26]. It allows the group members to sign messages anonymously on behalf of the whole group. However, in