Neurocomputing 181 (2016) 132–138

Contents lists available at ScienceDirect

Neurocomputing

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

Efficient authentication and access control of message dissemination over vehicular ad hoc network☆

Qian Kang [a], Xuejiao Liu [a,*], Yiyang Yao [b], Zhiqiang Wang [b], Yang Li [a]

[a] Institute of Service Engineering, Hangzhou Normal University, China
[b] State Grid Zhejiang Electric Power Company Information & Telecommunication Branch, Hangzhou, China

ARTICLE INFO

Article history:
Received 14 March 2015
Received in revised form
3 June 2015
Accepted 4 June 2015
Available online 27 November 2015

Keywords:
VANETs security
Attribute-based encryption
Identity based signature
Message authentication

ABSTRACT

Recently, security and privacy have been one of the main concerns that impedes the development of vehicular ad hoc networks (VANETs). In this paper, we put forward an access control with authentication scheme for disseminated messages in VANETs. In the scheme, we integrate pseudonym with identity based signature (IBS) which could not only authenticate the messages in vehicular communication, but also protect the privacy of message generators. When vehicles receive numerous messages that need to be authenticated in a short time, we also apply batch verification to improve the efficiency of message disseminating. Then we adopt ciphertext policy attribute based encryption (CP-ABE), which provides access control service to set expressive and flexible access structure for the specified vehicles in VANETs communication. The experimental results show that the proposed scheme is efficient in message authentication and access control for vehicular communication in VANETs.

1. Introduction

Vehicular ad hoc networks (VANETs) are regarded as a backbone for the development of intelligent transportation system (ITS) [1], which provides a platform for applications among vehicles to improve driving safety and transportation efficiency, provide driver assistance, etc. [2–6].

Therefore, considerable efforts from research institutes, industry and governments are undertaken to develop VANETs. The United States Department of Transportation [7] studies the connected vehicular communication with California PATH groups [8] and establishes some state testbeds in USA for simulating experiments. National ITS architecture, proposed by U.S. Department of Transportation, provides a definitive and consistent framework to guide the planning and deployment of VANETs. It is estimated that the market for vehicular communications will reach several billions of euros in the coming years [9].

Recently, security and privacy issues have been one of the main concerns that impede the development of VANETs. There are mainly two means of communication, they are vehicle to vehicle (V2V) and vehicle to infrastructure (V2I) in VANETs. By such communications, vehicles could send warning messages once an emergency event happens. If the nearby vehicles could receive these messages with little delay, the receiver can take advantage of the information to refrain from dangerous situation. In addition to the emergency messages, various information can be disseminated among vehicles through V2V or V2I communication, such as detour information, traffic accident, and congestion information. A problem is that any adversaries may eavesdrop on the communication, inject erroneous information in the network, or even jeopardize a transportation system to disseminate bogus messages. Therefore, it is critical to develop an applicable communication mechanism for achieving security and conditional privacy in VANETs.

For security reasons, these messages disseminated in VANETs should satisfy the following requirements: at first, message confidentiality and integrity is the most important. Otherwise if data confidentiality is compromised, it would easily cause confusions or unexpected situations, especially in some emergency applications. Also, in most of VANET applications, messages broadcasting may be necessary especially for emergency information and road congestion information. The selected locations or specific types of vehicles (such as ambulances, fire trunks nearby) are determined in the process of message broadcasting. All messages should be delivered unaltered, and the origin of the messages should be authenticated to guard against impersonation attack.

To solve the above-mentioned security issues, we figure out an access control scheme with authentication in VANETs. We adopt identity based signature (IBS) to authenticate the message in vehicular communication and exploit pseudonym as vehicles' identity to protect privacy. The explosive increase of messages in a

☆Fully documented templates are available in the elsarticle package on CTAN.
* Corresponding author.
E-mail address: liuxuejiao0406@163.com (X. Liu).

http://dx.doi.org/10.1016/j.neucom.2015.06.098
0925-2312/© 2015 Elsevier B.V. All rights reserved.

short time may make the recipient vehicles verify these messages, which would lead to authentication delay in VANETs. To improve the verification efficiency, we apply batch verification in the process of message dissemination. Then we adopt scheme with ciphertext policy attribute based encryption (CP-ABE), to ensure the confidentiality, which meanwhile allows us to set and enforce expressive and flexible access structure for the specified vehicles in vehicular communication. The contributions of this paper can be addressed as follows:

1. We propose a privacy-preserving message disseminating model with access control in VANETs, by ciphertext-policy attribute based encryption.
2. For data authentication's sake, we adopt identity based signature with pseudonym in message disseminating in scheme, as well as protect drivers' privacy.
3. To improve message authentication efficiency, we adopt batch verification with identity based signature when vehicles recover emergency message.

The rest of paper is organized in the following way. In Section 2, we present related work in the aspects of VANET security. In Section 3, we describe several technical preliminaries used in our scheme. We discuss the system overview in Section 4 and give our construction in detail in Section 5. We analyze the performance of our scheme in Section 6. Finally, we summarize the paper in Section 7.

2. Related work

Over the past years, several security related works [10–12] have been suggested in VANETs. Most of the research on security issues in VANETs has been concentrated on authentication, confidentiality, access control, etc. The anonymity is an important issue of achieving privacy preserving [10,13,11] in VANETs communication. Chim et al. [13] introduced an anonymous credential scheme to protect the privacy of vehicle to guarantee that vehicles are unlinkable to any party. Pseudonym-based schemes are usually efficient and simple, and can be applied in a variety of scenarios in vehicular communication system [12].

Authentication is achieved by signatures in VANETs and has been studied by some researchers [14–16]. In some approaches, each vehicle needs to preload the public/private key pairs to sign or verify the messages, it could bring a heavy burden of authentication on storage, generation, verification. Therefore, those studies [17,18] regarded identity based scheme as a suitable scheme for vehicular communications authentication because it allows batch and quick verification in VANETs communication.

Confidentiality is achieved using encryption algorithm in VANETs communication, as Boyen [19] discussed, they adopted scheme called IBES which integrates the identity based signature algorithm and identity based encryption algorithm to ensure messages’ confidentiality. By sharing parameters and keys, IBES could improve the security and effectiveness in scheme implementation.

Attribute based encryption (ABE) has several applications of message access control in VANETs. ABE was firstly proposed by Bethencourt et al. [20] and could help to control the message dissemination. As far as we are concerned, Huang and Verma [21] firstly proposed the scheme based on ABE in VANETs which is a flexible, secure and decentralized key management framework. But all of the key and ciphertext are labeled with certain attributes to achieve access control. Liu et al. [11] extended CP-ABE algorithm with multiple authorities and authorized the vehicles by exploiting attribute-based signature.

3. Technological preliminaries

3.1. Bilinear maps

$\mathbb{G}_0$ and $\mathbb{G}_1$ are two multiplicative cyclic groups of prime order p, g is a generator of $\mathbb{G}_0$. e is a bilinear map, $e:\mathbb{G}_0\times\mathbb{G}_0\rightarrow\mathbb{G}_1$, if the bilinear map e has the following properties:

1. Bilinearity: for all $g_1, g_2 \in \mathbb{G}_0$ and $a, b \in \mathbb{Z}_p$, we have $e(g_1^a, g_2^b) = e(g_1, g_2)^{ab}$.
2. Non-degeneracy: $e(g, g) \neq 1$.

If the group operation in $\mathbb{G}_0$ and the bilinear map $e:\mathbb{G}_0\times\mathbb{G}_0\rightarrow\mathbb{G}_1$ are both efficiently computable, then we say that $\mathbb{G}_0$ is a bilinear group. Meanwhile, $e(g^a, g^b) = e(g, g)^{ab} = e(g^b, g^a)$, then the map e is symmetric.

3.2. Identity-based signature

IBS is a public key signature scheme. Combined with certain system-wide information, user within a system could use their online identifers as their public keys [22]. This greatly reduces the problems with key management that have tampered the mass uptake of public key cryptography on a per individual basis [23]. The user, as a prover, can then identify itself to a verifier in a protocol in which the verifier begins by knowing only the claimed identifers of the prover.

3.3. Attribute-based encryption

Ciphertext-policy attribute-based encryption (CP-ABE) is a public key cryptography primitive for one–many communications. It provides a mechanism to specify an access structure over attributes in the encryption process. Then the user can decrypt the ciphertext if and only if the attributes associate with the user satisfy the access structure.

4. System overview

In this section, we present an overview of our proposed scheme, and give a snapshot of the algorithms used in our proposed solutions.

4.1. System model

Fig. 1 illustrates the system model, which consists of three entities: the trusted center (TC), the roadside units (RSU) and onboard units (OBU) equipped with each of the running vehicles.

Trusted Center (TC): It can be viewed as trusted authority and traffic center. For trusted authority, it is responsible for setting up the whole system, including generating public parameters and issuing secret keys for immobile RSUs at the road side and mobile OBUs on the vehicles. Besides, it takes charge of verifying the emergency messages and transmitting the messages to the corresponding RSUs. We assume that TC is fully trusted by all parties in the system.

RSU: RSU is a subordinated facility in the system, which communicates with TC by wired channel. RSU plays the role of (1) issuing a short-time anonymous public key to the OBUs when it requests to register; (2) disseminating messages to the OBUs in a certain distance. RSU is considered to be honest but curious, which means that it is trusted to carry these computations, but it is still curious to learn any information about the messages.

OBU: Each vehicle is equipped with an OBU, which can communicate with neighboring RSUs for registering and transmitting messages using Dedicated Short Range Communication (DSRC)