Contents lists available at ScienceDirect

Signal Processing

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

An efficient message access quality model in vehicular communication networks

Xuejiao Liu [a], Zhenyu Shan [a,*], Wei Ye [a], Ruoyu Yan [b], Zhengliang Wang [c]

[a] Institute of Service Engineering, Hangzhou Normal University, Hangzhou, China
[b] College of Computer and Information Engineering, Henan University of Economics and Law, Zhengzhou, China
[c] Institute of Scientific and Technical Information of Zhejiang Province, Hangzhou, China

ARTICLE INFO

Article history:
Received 5 September 2014
Received in revised form
18 November 2014
Accepted 20 November 2014

Keywords:
VANET security
Attribute-based encryption
Attribute-based signature
Message authentication

ABSTRACT

In vehicular ad hoc network (VANET), vehicles equipped with computing, sensing, and communication capabilities can exchange information within a geographical area to distribute emergency messages and achieve safety system. Then how to enforce fine grained control of these messages and ensure the receiving messages coming from the claimed source in such a highly dynamic environments remains a key challenge that affects the quality of service. In this paper, we propose a hierarchical access control with authentication scheme for transmitted messages with security assurance over VANET. By extending ciphertext-policy attribute-based encryption (CP-ABE) with a hierarchical structure of multiple authorities, the scheme not only achieves scalability due to its hierarchical structure, but also inherits fine-grained access control on the transmitted messages. Also by exploiting attribute-based signature (ABS), the scheme can authorize the vehicles that can most appropriately deal with the message efficiently. The results of efficiency analysis and comparison with the related works show that the proposed scheme is efficient and scalable in dealing with access control and message authentication for data dissemination in VANET.

1. Introduction

Vehicular ad hoc network (VANET) is regarded as a promising approach for future intelligent transportation system, which enables communication between vehicles to vehicles and vehicles to roadside units. Although various parallelized fusion [1] and domain decomposition [2] are applied in intelligent transport system to understand the transport data, in VANET network vehicles can exchange information (e.g., detour, traffic accident, congestion information, and life-critical emergence messages) and provide early warnings to nearby vehicles in order to reduce traffic jams near the affected areas, and the traditional methods are not suitable in vehicular communication network. VANET will greatly enhance driving safety and experience, improve roadway system efficiency. Further, widespread deployment of VANET is heavily based on a secure and reliable infrastructure for providing accurate traffic and road system data. However, providing security in a vehicular network is more difficult than in other networks such as WSN due to the high mobility and wide range of vehicles [3]. Nowadays, the security issues, such as confidentiality, authentication, non-repudiation, localization and verification of data [4], are still the most important problem to be solved that affect the quality of service (QoS) in vehicular network.

Vehicular ad hoc networks are usually operated among vehicles moving at high speeds, thus their communication

[*] Corresponding author.
E-mail address: shanzhenyu@zju.edu.cn (Z. Shan).

http://dx.doi.org/10.1016/j.sigpro.2014.11.012
0165-1684/© 2014 Published by Elsevier B.V.

relations can be changed frequently. In such a highly dynamic environment, traditional security solutions face many challenges in VANET caused by the complex vehicular communications system, dynamic user groups, real-time constraints, etc. The privacy and confidentiality of the transmitted messages should be protected in VANET communications. Also the messages must be authenticated to prevent attackers from injecting, altering and replaying messages, as well as to prevent eavesdropping. Intuitively, it is extremely dangerous that if the messages are controlled by the attackers. This could easily cause confusions or unexpected situations especially in some emergency applications. In many cases, it is also desirable to provide a fine-grained access control mechanism to guarantee that messages transmitted to corresponding users.

Specially speaking, let us see the following scenario. In case of an emergency (e.g., a traffic accident, a fire or a bomb threat) in a certain area of a city, police headquarters will immediately transmit emergency messages. On one aspect, they intend to notice policemen to deal with the emergency at the time of accidents. On the other aspect, they want to broadcast an alert message to the vehicles which are in this district or will in this district, to avoid this emergency. Then, traffic jams or serious accidents can possibly be prevented if these emergency messages can be shared among vehicles. Also they want to define a policy that allow someone (e.g., police car) in selected locations near the scene of the accident to take over the control of traffic lights in order to facilitate rescue and carry out orderly vehicle evacuation.

In this paper, we propose a hierarchical access control scheme with authentication in VANET. We develop ciphertext-policy attribute-based encryption algorithm into a hierarchical access control scheme, which is a flexible hierarchical structure to organize all of the trust authorities in VANET. Each vehicle has its capabilities and access rights according to the attributes it owns. Then only the vehicles that have certain attributes satisfying the access policy can decrypt the broadcasted messages. Also, we apply attribute-based signature to authenticate and authorize the appropriate vehicles to handle the messages that satisfy specific policy. Our contributions can be addressed in the following aspects:

(1) We propose a hierarchical message access quality model in VANET network, by encrypting the transmitted messages in ciphertext-policy attribute based encryption with multiple authorities. The model is scalable and efficient in dynamic vehicular communication environment.
(2) Our scheme achieves fine-grained access control among various types of vehicles using well defined attributes. When a message broadcasted in VANET, only those vehicles that possess the selected attributes can access the messages.
(3) Our scheme enforces message authentication by integrating attribute-based signature, in order to ensure message integrity checking and maintain anonymity and privacy of the vehicles.

The rest of the paper is organized as follows: Section 2 details previous work in the aspects of VANET security. In Section 3 we present the related technologies used in our scheme. Section 4 presents system model and algorithm definition. We give the specific construction and performance evaluation in Section 5. Finally, we conclude the paper in Section 7.

2. Related work

Proving a secure communication plays a vital role in establishing a more reliable driving environment in vehicular network. There are several security threats in vehicular communication, such as forging messages and transmitting bogus warnings by the malicious attackers, dropping or modifying messages by man-in-the-middle attackers, and privacy violations. To protect vehicular communication against these various attacks, the use of cryptographic algorithm is inevitable. ElGamal signature scheme [5] is a way to create a secure communication in which each vehicle has a specific public and private key (k_{pu}, k_{pr}). However, this scheme is not suitable for broadcasting messages in dynamic vehicular environment.

Verifying the authentication of users is also important in vehicular communication network, that is, determining whether someone or something is the one who or what it is claimed to be to receive the message or deal with the message. There are some studies on this aspect in vehicular network. Kim et al. [6] propose an auditable and privacy-preserving authentication in vehicular based on the MAC-chain method for privacy-preserving authentication. Several efforts [7–9] have been made to protect user privacy in the authentication process, but most of them use a policy that places full trust on the roadside units or the servers.

Access control is a challenging aspect in vehicular network in which an identification of the user is checked before gaining access to the resource. Huang et al. [10] are the first one to introduce ciphertext-policy attribute based encryption [11] in VANET in which vehicles are divided into several groups and two vehicles belonging to two different RSUs' communication ranges cannot communicate with each other directly. An improved scheme is proposed in [12], which addresses the abovementioned issues by employing the decentralized attribute based encryption scheme of Lewko et al. [13]. Gongjun et al. [14] proposed that various access control levels are predefined and each user belongs to a specific cluster based on its role in the network. Nevertheless, none of these schemes can provide mechanism for authenticating senders and authorizing receivers to handle the messages.

3. Building blocks

3.1. Bilinear maps

Let $\mathbb{G}$ and $\mathbb{G}_T$ be two multiplicative cyclic groups of prime order p. Let g be a generator of $\mathbb{G}$ and e be a bilinear map, $e: \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$ with the following properties:

1. *Bilinearity*: for all $u, v \in \mathbb{G}$ and $a, b \in \mathbb{Z}_p$, we have $e(u^a, v^b) = e(u, v)^{ab}$.

Please cite this article as: X. Liu, et al., An efficient message access quality model in vehicular communication networks, Signal Processing (2014), http://dx.doi.org/10.1016/j.sigpro.2014.11.012