International Journal of Information Security and Privacy
Volume 12 • Issue 1 • January-March 2018

CIAS:
A Comprehensive Identity Authentication Scheme for Providing Security in VANET

Arun Malik, Lovely Professional University, Punjab, India
Babita Pandey, Lovely Professional University, Punjab, India

ABSTRACT

Vehicular Ad hoc Network (VANET) is considered as an essential component of Intelligent Transport system. VANET has gained an ample amount of attention from the researchers and automobile industry. Security and privacy are the primary requirements in the successful deployment of vehicular communication in VANET. Lack of security and confidentiality in VANETs is the primary barricade in the successful deployment of VANET. To establish trust within the entities participating in VANET operations is the primary aim of VANET security and play a vital role in prevention of attack in VANET. This paper describes a comprehensive identity authentication scheme (CIAS) based on asymmetric encryption that facilitates the authentication for Vehicle-to-Infrastructure (V2I) and inter RSUs. The proposed scheme is validated by extensive simulations and compared with the related works on the basis of communication overhead (CO), Latency and packet delivery ratio (PDR). The result of simulations shows that proposed authentication scheme outperforms.

KEYWORDS

Communication Overhead, Intelligent Transport, Road Side Units, Vehicular Ad hoc Network

INTRODUCTION

In recent years, VANET gains a high attention from the government, researchers and automobile industry. VANET is a talented approach to increase transportation safety and effectiveness. VANET can increase traffic safety and improve traffic performance by sending messages containing information related to traffic and road conditions (Toor, Muhlethaler & Laouiti, 2008; Hartenstein & Laberteaux, 2008). VANET is considered as a solution for intelligent transport system (ITS) (Wang, Zeng & Yang, 2006). VANET provides variety of smart applications which includes traffic monitoring, exchange of information among vehicles and RSU, collision warning and so on (Zeadally, Hunt, Irwin, & Hassan, 2010). Every vehicle in VANET is outfitted with an OBU to communicate with other vehicles or with RSUs. Primarily, two types of communication exist in VANET vehicle-to-vehicle (V2V) and V2I. The primary concern of VANET is to ensure the protection of the information transmitted amongst the vehicles or between the vehicles and the RSUs. For example, VANET provides various types of safety and non-safety related services like Post and combined accident warning, dynamic traffic, road risk control warning, internet access, multimedia downloads, online video transfer etc., where all of the processes related to data exchange between vehicles and RSUs must be protected. On the other hand, since the exchange of information occurs over a wireless medium due to which there exist a risk of eavesdropping on the exchanged data by malicious user. The malicious user may

DOI: 10.4018/IJISP.2018010103

even counterfeit a registered vehicle to get access to the services offered by the RSU. The malicious user analyzes the habit of drivers and theft or other crimes may be executed by exploiting VANET communications. If VANET is affected by the malicious user, it may result in traffic jams or even severe accidents. Without providing essential security in VANET, use of VANET could cause danger to vehicles. To provide various types of safety and non-safety related services in an efficient manner, VANET required two types of vital security requirements, namely (a) identity authentication (i.e., RSU must have ability to confirm the to confirm the uniqueness of the vehicle and vice versa); and (b) confidentiality (i.e.; exchange of sensitive data between vehicles and RSU must remain hidden from the malicious user).

To sustain access to the RSU services without any interruption, a vehicle must set up a link with a new RSU at the time of departing the range of previous RSU in V2I environment. Due to high mobility of VANET the process of "establishing a link with a new RSU" is done frequently as the vehicle moves through the network. This handover procedure involves the uniqueness of the vehicle to be confirmed as a result of which the service time for the vehicle is decreased. In rigorous cases, the authentication operating cost may possibly effects the performance of the network or even causes network failure. Therefore, to design the efficient authentication algorithm by keeping the privacy of the vehicle's uniqueness and exchange of data between vehicles and RSU is a very challenging task in a successful deployment of VANET. This paper describes a comprehensive identity authentication scheme (CIAS) based on asymmetric encryption that facilitates the authentication for V2I and inter RSUs. This algorithm not only reduces the complexity of authentication process but also advances the privacy of data exchange in V2I and inter RSU environment.

The primary contribution of this paper can be recapitulated as follows:

- The various types of attacks in VANET are examined.
- The requirements and challenges related to security and privacy faced by the VANET are discussed.
- The existing authentication solutions for VANET are discussed
- A new authentication scheme based on asymmetric encryption that facilitates the authentication for V2I and inter RSUs is proposed and implemented by conduction extensive simulations.

The rest of the paper is categorized as follows. Section 2 describes the various types of attacks in VANET. Section 3 discusses the requirements associated to security faced by the VANET. Comprehensive surveys of related works for different authentication schemes are described in section 4. Section 5 describes the proposed authentication scheme based on asymmetric encryption. Intensive performance evaluation of our proposed scheme is presented in section 6 and section 7 concludes the paper.

ATTACKS IN VANET

VANET is vulnerable to various types of security threats and attacks due to its open wireless nature. An overview of attacks is presented in this section that may arise in VANET environment. Some basic and noteworthy attacks that are commonly available in literature are as follow:

- **Denial of Service (DoS) Attacks**: The primary aim of this attack is to block the principal means of communications and to interrupt the services provided by the VANET to the genuine user (Dhamgaye, Chavhan, & Communication, 2013). DoS can be executed by internal or external malicious vehicles to the VANET (Zeadally, Hunt, Irwin, & Hassan, 2012).