Privacy Preserving Protocols in VANET: A Survey

G. Santhana Devi¹, M. Germanus Alex ²

¹Research & Development Center, Bharathiar University, Coimbatore-641 046, Tamilnadu
²Kamarajar Government Arts College, Surandai 627859, Tirunelveli District, Tamilnadu

Abstract

The vehicular ad-hoc networks (VANETs) are temporal networks which are self organized by vehicles and road side unit at the movement. In VANET each node to broadcast traffic associated message to other vehicles, which can be used to improve the traffic efficiency and safety. That message privacy and security are the major requirements in VANET. In this paper, we discuss the research challenges of security requirements in VANET and survey the recent privacy preserving protocols for VANET and finally compare the protocols with those utilize cryptographic primitives.

Keyword

Vehicular Ad-hoc Network (VANET), Trusted Authorities (TA), Road Side Unit (RSU), On-Board Unit(OBU), Tamper Proof Device (TPD), Security, Privacy, Message Authentication Code (MAC).

1. Introduction

Vehicular ad hoc networks (VANETs) are distributed, self-organized networks construct by many high-speed vehicles. All vehicles in the network would set up on board units (OBU), which would combine the vehicles’ wireless communications, sensors, embedded systems, and Global Positioning System (GPS) [1]. These smart vehicles could then communicate with each other as well as with roadside units (RSU), such as traffic lights or traffic signs, which would then improve the driving efficiency and make driving safer [2]–[4].

A VANET consists of three main types of entities, i.e., trusted authority (TA), roadside units (RSUs) and a vehicle with embedded on-board units (OBUs). The TA is responsible for the maintenance of the whole system. RSUs are deployed beside the roadside. They work as broadcast traffic related information to vehicle within the communication range. And also it performs some authentication between vehicles. OBUs help vehicles to collect and save the credentials, and it to communicate traffic and emergency associated information with other entities. There are three types of communication in VANETs as shown in Figure 1: vehicle-to-vehicle (V2V), vehicle-to-roadside (V2R) and roadside-to-vehicle (R2V).

![Figure 1 VANET Architecture](image-url)
Privacy is a main problem in VANETs as the wireless communication channel is a shared medium. Exchanging messages without any security guard over the air can simply leak the information that users may want to keep secret.

The organisation of the paper is presented as follows: Section 2 discuss VANETs characteristics. Section 3 discusses VANETs applications. Next, security Attacks for VANETs are described in Section 4. Section 5 discusses requirements. Section 6 describes popular privacy preserving scheme used for VANETs and the last section 7 presents the concluding remarks.

2. Characteristics of VANET

VANET has its own different characteristics, which are summarised as follows [6]:

**High Mobility**

Nodes in VANETs generally are moving at high speed. This makes difficult to calculate a node’s position and making security of node privacy.

**Dynamic Topology**

Due to high node mobility and vehicles random speed, the node position changes frequently. Thus, network topology in VANETs regularly changes. The link connection between the vehicles in VANET has frequent disconnections because of the high movement of the nodes and frequent change in the environment.

**Unbounded network size**

Network size of VANET is geographically unbounded. It means, VANET can be implemented for one city, several cities or for countries.

**Frequent exchange of information**

In VANETs encourages the nodes to gather information from the other vehicles and RSUs. Therefore, the information exchange among node becomes frequent.

**Wireless Communication**

VANET is designed for the wireless environment; nodes are connected and exchange their information via wireless. Consequently, security measure must be considered during communication.

Time Critical

The delivery of information to the nodes in VANET must be done within time limit so that it can perform the action accordingly, e.g. critical medical emergency messages must be delivered on time in order to save human lives.

Use of Other Technology

Most of the vehicles in VANET are capable of integrating their own system with other available technologies such as Global Positioning System (GPS).

No Power limitation

In VANET, nodes do not have concern energy and computation resources unlike other MANET devices. This can be utilised for efficient processing of complex and computational hungry routing/security mechanisms.

Predictable Mobility Patterns

Most of the vehicles move on pre-defined roads and highways in VANET environment. This allows the use of predictable mobility patterns in network design.

Geographic position available

Accurate positioning systems like GPS with integrated electronic maps are quite popular in cars, as vehicles equipped with these tools, provide location information for routing purposes.

3. VANET Application

There are many significant applications of VANET. These applications can be broadly categorized into two categories (i) safety applications and (ii) non safety applications [5].

A. Safety Related Application

These applications are used to increase the safety on the roads.

Road Traffic Safety: This applications work on reducing the number of fatalities/injuries on the roads by alerting the driver about dangers in advance.

Cooperative Driving: The drivers take part in very important role in this application. Such as violation warning, turn conflict warning, curve warning, lane merging warning etc. and considerably decrease the life-endangering accidents. In fact, many of the
accidents come from the lack of cooperation between drivers.  Traffic optimisation: Traffic can be optimized by the use of sending signals like traffic jam, accidents etc. to the vehicles, accordingly, they can choose their alternate path and also save time.

B. Non safety Application

Following are the services for the user.
Peer to peer application: These applications are very much useful to provide services like sharing multimedia files, movies, songs etc. among the vehicles in the network.  Internet Connectivity: People can connect with the Internet all the time. Thereby, VANET provides the constant connectivity of the Internet to the users.  Location Tracking Service: This type of application helps to drivers to track the location of service stations. That show the nearest fuel station, restaurant etc. These services also provide by GPS system. Location tracking system also used to track attackers.  Comfort Road Travel: These applications provide comfort for travellers like ‘advanced traveller information systems’, ‘electronic payment systems’, ‘electronic toll collection’ etc.

4. Security Attacks

The VANET use wireless open transmission medium for communication. So, there are possibilities to many types of attacks. These different types of attacks can be classified based on their nature, target and impact. Possible attacks are listed here [7][8][9].

A. Sybil Attack
A vehicle continuously sends messages to other vehicles in VANET from different source identities. The attacker wants to create an illusion by sending wrong message; such that there are so many vehicles those are sending different messages. For example it makes illusion for traffic jam so other vehicle takes alternative path for attacker’s benefit [8].

B. Denial of Service Attack
In this attack the communication medium is evicted by channel jam and has problem to access network services. The reason is that a vehicle broadcasts large number of unwanted messages continuously in a very short time period like as Sybil attack.

Bandwidth of channel is highly used so there occur channel jam condition [9].

C. Replay Attack
In this type, the attacker listens to other node broadcast or communication between nodes and RSUs. This information is replayed by attackers to take the advantages of situations and to confuse the authorities.

D. Privacy Attack
An attacker wants to obtain illegally sensitive and crucial information about the vehicle user. An attacker can build vehicle’s profile by using own personal identity information and location tracking of vehicle. Mostly driver is the vehicle owner. So attacker can unauthorized disclose the information that is harmful for vehicle user.

5. Security Requirements

Following security requirements must be satisfied in order to avoid various security attacks [10].

Vehicle authentication
The fundamental requirement of our approach is the privacy preserving authentication of a VANET user. This requirement assures the receiver of a beacon message about the legitimacy of the sender vehicle.

Message Integrity
The proposed approach should also guarantee the message integrity, i.e., the content of the message should be delivered to a receiver unaltered.

Privacy preservation
The content of a beacon should not reveal any information about the sending vehicle.

Non-repudiation
The sender vehicle must not be able to deny the transmission of the beacon.

Traceability
The approach must be able to track insider attackers.

Low overhead
The security overhead should be kept to a minimum in terms of computation and communication.

6. Privacy preserving scheme

A. EIAS-CP

In this paper [11], the author proposed efficient identity-based authentication scheme with conditional privacy preserving for VANETs by
using Elliptic Curve Cryptography (ECC). In this paper, the author uses single message verification and batch message verification. The advantage of the scheme is batch message verification and ECC are decreasing the computation cost.

**B. VSPN**

In this paper [12], the author proposed VANET based secure and privacy preserving navigation scheme (VSPN), which can be used to provide the real time road condition and route discovery to drivers. In this scheme the road information collected by RSU and it give the guidance to the drivers to reach the target in real time and distributed manner. This scheme provides the privacy to drivers, the queries and query results from eavesdroppers. The advantage of the scheme is providing the best route to authenticated vehicle based on RSU collected real time road information. The demerit of the scheme, the route searching process is done by a central server, which collect and verify the speed data and road information from RSU. But the centralized approach is not scalable for all time.

**C. Location based CPPA**

In this paper [13], the author introduced location based CPPA scheme for VANETs without the bilinear pairing and tamper-proof device. In this scheme, vehicle receives short term pseudonyms based on location from a new RSU. Such as, if it enters the new RSU communication range, it will receive new pseudonyms from new RSU.

**D. APPAS**

In this paper [14], the author proposed an autonomous privacy preserving authentication scheme. In this scheme, the vehicles create number of pseudonym self from a simple credential based on Elliptic Curve Cryptography (ECC). The advantage of the scheme is its autonomy, while the vehicles only need to communicate the TA once; after that they can renew their pseudonyms by themselves without knowledge of TA. The self-generation of pseudonyms is controlled by TA with the time restriction key. The TA provides the key periodically; therefore no need point-to-point connection between vehicles and TA. In addition the time restriction key is distributed in advance so it is used to lack of network infrastructure.

**E. 2FLIP**

In this paper, the author proposed [15] a TWO-Factor lightweight privacy preserving authentication scheme for VANET (2Flip) which utilize decentralized certificate and biological password based authentication. In this scheme use authentication code and one way hash operation for to improve the privacy preserving authentication. In addition tamper-proof device (TPD) is fixed in vehicle’s OBU to store system key and verify message. The demerit of the scheme is the system key receive from the centralized authority, it is not applicable for all time.

**F. HPPPA**

In this paper, the author proposed [16] a Hierarchical Privacy Preserving Pseudonym Authentication Protocol for VANET. In this protocol hierarchy of pseudonyms based on the time period of their usage and does not require and maintaining a CRL. In this paper the primary pseudonyms are used to communicate with the CA and RSU and it is used longer time period. The secondary pseudonyms are short lived, it is used to authenticate beacon broadcast. This protocol uses two separate cryptosystems such as Elliptic curve cryptography and paillier encryption. Moreover this protocol provides conditional anonymity to the users of the network and reveals the malicious vehicle real identity.

**G. CACPPA**

In this paper [17], the author proposed a cloud-assisted conditional privacy preserving authentication protocol for VANET. This protocol is hybrid approach that utilizes both the concept of pseudonyms based approaches and group signature based approaches. This protocol provide conditional anonymity that is vehicle anonymity is preserved only until it honesty follow the protocol. In this protocol uses elliptic curve cryptography as the cryptography tool. In this paper neighbouring vehicle communicate with other vehicle efficiently as well as anonymously.
7. Conclusion

VANET is an emerging new technology; security and privacy of vehicles message communications are main problem in vehicular network. In this paper, we have discussed about VANET architecture, characteristics, safety and non-safety application, possible attacks and required features for ideal communication in VANET. After that, we have classified different type of protocols those are proposed to achieve better privacy on the basis of protocol working principle and also discuss their merit as well as demerits in comparison with other protocols.

References


[8] Blum, J; Eskandarian, A “The threat of intelligent collisions”, IT Professional (vol. 6, 1); (2004); (pp. 24-29);


