Location Based Security and Message Authentication Services in Vehicular Ad Hoc Network (VANET)

P.Chandrasekar¹, Arul Lawrence Selvakumar²

¹Assistant Professor, Dept. of Computer Applications, S. A. Engineering College, Chennai, India.
²Professor & Head, Dept. of CSE, Rajiv Gandhi Institute of Technology, Bangalore-32, India.
¹mail2chandruu@yahoo.co.in; ²aarul72@hotmail.com

Received 28 December 2013; Accepted 15 January 2014; Published 15 May 2014
© 2014 Science and Engineering Publishing Company

Abstract

The most recent years have observed an unmistakable convergence of Vehicular Ad hoc Networks (VANETs) that promise to modernize the way we drive. Information about the location is fundamental objective in Vehicular Ad-hoc Networks. Nearly, all VANETs rely on location based information, addressing security and privacy issues as the requirement of VANETs development; it’s difficult to avoid any possible malicious attacks and resources abuse. Employing a digital signature scheme is widely recognized as the most effective approach for VANETs to achieve authentication, integrity, and validity. The proposed system exposes the location based security and message authentication services in vehicular ad hoc networks.

Keywords

VANETs; Security and Privacy Issues; Message Authentication

Introduction

According to Traffic Safety Facts Annual Report from the National Highway Traffic Safety Administration, nearly 6 million police-reported motor vehicle crashes occurred in the United States alone in 2006, leading to 1.75 million injuries and 38,588 deaths. According to the 2006 Annual Report on Traffic Congestion in the Denver Region, each resident on average faces about 32 hours of congestion delay per year. Travel during rush hours is 27% longer than non-rush hours. $1.7 billion per year is lost due to the traffic delays. The above numbers indicate that the traditional traffic crash alert and traffic control systems should be meliorated in order to improve the quality of the public transportation. Fortunately, various manufacturers, government units and standardized bodies have generated national and international association committed exclusively to VANETs.

Vehicular Ad-hoc Networks (VANETs) have appeared as a new appliance that is envisioned to modernize the human driving experiences, optimize traffic flow control systems, etc. Location is fundamental information in Vehicular Ad-hoc Networks (VANETs) and Addressing security and privacy issues as the prerequisite of VANETs’ development must be emphasized. Almost all VANET applications rely on location information. Therefore it is very important to make sure location information integrity, meaning that location information is original, secure, correct (Not false or fabricated) and unmodified (value not changed). According to the security and privacy it is difficult to avoid any possible malicious attacks and resources sharing abuses and employing various digital strategy scheme is widely recognized, whereas, this is the most effective approach for VANETs to achieve message authentication, integrity and secure validity.

The number of information received by a vehicle becomes large; a scalability problem emerges immediately, where a vehicle could be difficult to sequentially verify each time received data within 100-300 ms interval in accordance with the current Dedicated Short Range Communications (DSRC) Protocol. Nowadays we have a vehicle tracking system using GPS is available but due to some natural obstacles we couldn’t track it on the hills and valley sides. Vehicles and roadside infrastructures are equipped with wireless communication devices and
constitute a vehicular ad hoc network (VANET). VANET aims at improving the road safety and avoid potential traffic accidents. This technology mostly helps us to improve not only the country growth, but also saves the human value from the timing incidents.

**Smart and Sophisticated Vehicles’ in VANETs**

In vehicular network the new technology brings not only updated design but also new devices to vehicles. These new devices can extend vehicle’s capabilities in computing, communication and sensing. The provision of on-board Global Positioning System (GPS) devices has modernized driving. Similarly, the recent introduction of short-range radar in some top-of-the-line models promises to reduce the number of fender-benders, quick-struck and other accidents. In fact, on-board radar has already been used in advanced cruise control systems. We base our vehicle model on the smart vehicle proposed by Hubaux et al. Hubaux includes an Event Data Recorder (EDR), a GPS receiver, and radar in his smart vehicle model. It is equipped with various features such as wireless transceiver, Digital Map, Common Service Centre, GPS receiver, radar communication, a location key identification and etc.

**Location Information**

VANET is composed of vehicles and road side units (RSUs). Vehicles are equipped with wireless communication devices, which are called on-board units (OBUs). The wireless communication devices enable vehicles to exchange traffic related messages with each other and with RSUs. The location in a message can be part of the message as shown in Figure 1a. E-Business applications for VANETs (online shopping, toll payment collection, etc.) can use this type message to enhance the security of messages. The whole content of a message can be composed of location information in OBUs, shown in Figure 1b. Military vehicle movement on the arena can use this type of message. The location information of all vehicles is aggregated and it can be strictly encrypted and decrypted in a specified decryption region to enhance the security of the location information. We also expect the decryption region can move along with the receiver vehicle.

<table>
<thead>
<tr>
<th>Address</th>
<th>Location-1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Location-2</td>
<td></td>
</tr>
<tr>
<td>......</td>
<td></td>
</tr>
<tr>
<td>Location-n</td>
<td></td>
</tr>
</tbody>
</table>

**FIG. 1: TWO TYPES OF LOCATION MESSAGES:** (a) LOCATION IS PART OF THE MESSAGE AND (b) LOCATION IS THE WHOLE CONTENT OF THE MESSAGE

Location information can be obtained from several devices, including GPS receiver, infrared scanner, etc. Since GPS imposes some constraints such as lack of other positioning techniques have been proposed for the vehicular field, including cellular or WiFi localization, dead reckoning (by using last known last location information and velocity), ultrasound range sensors and image/video localization.

**Message security and privacy issues in VANETs**

Addressing the security and privacy issues in VANETs includes message verification and conditional privacy preservation. Nowadays, Vehicles have been equipped with more and more high-technology devices. For example: GPS System, Radars and OBUs. This type of wireless enabled devices makes vehicle intelligent and be able to “talk” with each other, and thereby form a self-organized VANET. With the assistance of Vehicle to Vehicle communications, potentially fatal road accidents can be avoided; dangerous driving behaviors can be alerted; city traffic flows can be optimized; traffic jams can be alleviated. However, even though VANETs bring tremendous benefits to us, VANETs raise many research challenges as well. One of these challenges is security concerns. In VANETs, malicious vehicles may modify or insert fake information in the network, which could incur life-endangering accidents. In a word, if the security mechanism in VANETs is not carefully designed, misbehavior and malicious attacks may ruin the original intention of VANETs. Therefore, prior to putting VANETs into the practice, it is important to have a robust and efficient security mechanism on board.

**Security Threats in Location Based Privacy VA-Network**

Since security and privacy are basically important in VANETs, recently more and more research efforts have been put on designing security and privacy preservation protocols for location based privacy. In
VANETs, there are several possible security threats are available in location based privacy VA-network. Such that False information attack, DoS attack, Replay attack, Impersonation attack, Message modification attack, Privacy attack and Trajectory disclosure attack in a particular location. Generally, to escape from these attacks in the location based VANET that the following five requirements are directly associated with the security threads. Such are authentication, confidentiality, integrity, conditional privacy, and scalability. The implication of message authentication and security related schemes are motivated by this fact that, the proposed system introduces an efficient RSU-Aided Message Authentication scheme named RAIMA, for VANETs.

RAIMA explores an important feature of VANETs by employing RSUs to assist vehicles in authenticating messages. With RAIMA, vehicles first perform mutual authentication and key agreement with an RSU. Vehicles that received safety messages do not need to verify the message through a conventional PKI-based scheme. Instead, each safety message will be attached with a short Message Authentication Code (MAC) that is generated by a sender under the secret key shared between the sender and an RSU. The major contribution of RAIMA improves the authentication efficiency and reduces the communication overhead.

Design Objectives

The importance to ensure the security of location information has not been seriously addressed until recently. PKI is an important way to ensure information confidentiality. We assume there is a trusted authority. The trusted authority will generate keys for PKI. PKI has two keys, one is a public key which will be known by everyone and the other is a private key which is known only by the owner. The PKI algorithm is known to all parties. If a public key is used by the PKI algorithm to encrypt information, a cipher text will be generated. PKI is naturally adopted in VANET.

RSU-aided Message Authentication Scheme Using PKI Algm.

Towards a better understanding of RAIMA, it is important to understand the following four steps as in Figure 2. Which are Registration, Key Establishment, Hash Aggregation, and Verification. When vehicles enter the communication range of an RSU, vehicles initiate a mutual authentication process with an RSU. An RSU authenticates vehicles by verifying their signatures. Vehicles compute message signatures with their private keys, and RSUs verify the signatures and their corresponding public key certificates. A valid signature means that the signer of the signature is a legitimate user in VANETs. In a similar way, vehicles can also authenticate an RSU. Meanwhile, the messages that have been signed by vehicles and RSUs include secret credentials which can be used to compute a PKI used shared key. Here, Diffie-Hellman key agreement could be adopted to establish the shared symmetric key. It is worth noticing that different vehicles share different keys with an RSU. Vehicles do not know the key shared between an RSU and other vehicles.

PKI brings new challenges to VANETs. PKI includes both the public key and the private key. The public key needs to be known by other vehicles and the private key needs to be secretly stored. Therefore, key management is one of the challenges because of the large scale of the vehicle population. Some vehicles may have expired keys. To update the public and private keys, pervasive infrastructure will be required. Another challenge is that RSU message authentication scheme using PKI that requires homogenous configuration to achieve communication among vehicles. Some old vehicles may not have PKI installed. In addition, the overhead of PKI in terms of processing time will add significant processing time overhead to VANETs as well.

RAIMA Key Establishment

When a vehicle \( V_i \) detects the existence of an RSU \( R \) (e.g., through a Hello message from the \( R \)), the \( V_i \) initiates anonymous mutual authentication and establishes a shared secret key with the \( R \). This can be achieved by adopting the Diffie-Hellman key establishment protocol secured with signature scheme. The mutual authentication and key establishment
processes are shown as follows:

\[
V_i \rightarrow R : aP | CertV_i|PKR.
\]

\[
R \rightarrow Vi : IDi \| bP | (IDi \| aP \| bP)SKR.
\]

\[
V_i \rightarrow R : (IDR \| bP \| aP)SKV_i
\]

If the above three steps are completed correctly, the mutual authentication succeeds. Note that the mutual authentication in the protocol is provably secure (refer to for more details).

**Validating Locations and Message Communication**

We simulated a bidirectional 3 km highway with two lanes in each direction. The cell radius was 100 meters, traffic arrival rate was 1600 vehicles/hour, mean velocity was 33.3 m/s, and transmission radius initially was 100 meters. Each simulation has some number of compromised, or malicious, vehicles and a single observer vehicle. When the observer enters the simulated highway, it initiates a request to find all of the compromised vehicles. The simulation terminates when the observer reaches the end of the 3 km highway. To determine how transmission range affects the time needed to detect malicious vehicles, we ran a set of experiments with a 100 m transmission range and a set with a 500 m transmission range. The vehicle density was about 30 vehicles per kilometer per lane on the highway. The compromised vehicles were 5% of the total vehicles and were randomly deployed along the highway. In each set of simulations, we varied the length of the highway to investigate the effect of transmission range.

Finally, TABLE 1: General Integrity Case: Parameters and Values shows and to investigate how many compromised vehicles could remain undetected in our system. We randomly distributed compromised vehicles along the highway. The vehicle density was about 30 vehicles per km on the highway.

**TABLE 1: GENERAL INTEGRITY CASE: PARAMETERS AND VALUES**

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initial traffic density</td>
<td>30 vehicles/Km/lane</td>
</tr>
<tr>
<td>The length of the road L</td>
<td>3 Km</td>
</tr>
<tr>
<td>Average speed</td>
<td>60 km/h</td>
</tr>
<tr>
<td>The number of lanes</td>
<td>4/direction</td>
</tr>
<tr>
<td>The mean error μ</td>
<td>1 m</td>
</tr>
<tr>
<td>The deviation of error σ</td>
<td>1 m</td>
</tr>
<tr>
<td>Error ε</td>
<td>3 m</td>
</tr>
<tr>
<td># of neighbor outliers m_n</td>
<td>4</td>
</tr>
<tr>
<td># of opposite outliers m_o</td>
<td>1</td>
</tr>
<tr>
<td>The weight for rular w_1</td>
<td>0.5</td>
</tr>
<tr>
<td>The weight for opposite w_2</td>
<td>0.3</td>
</tr>
<tr>
<td>The weight for neighbors w_3</td>
<td>0.2</td>
</tr>
</tbody>
</table>

The transmission radius was 100 meters. We varied the percentage of all vehicles that were compromised from 0% to 30% because our assumption is that the majority of vehicles are honest. Compared with previous compromised vehicle percentage (5%), we increased this number to 30% to investigate a larger scope. We measured the number of compromised vehicles detected in 30 seconds.

**Conclusion and future work**

Vehicles installed with advanced devices can communicate with each other and create wireless networks, called VANETs. The applications of VANETs include safety and entertainment applications. Most, if not all, of these applications are location-aware and strongly depend on location information. Compared with other networks, such as MANETs, the Internet, and cellular networks, VANETs have unique and distinctive features. We are protecting a tuple, correct time, correct identity, and correct location. Based on information security requirements, we have to ensure location information confidentiality, integrity and availability. The research in this dissertation addresses location information security by providing location information confidentiality, integrity, and availability.

To ensure inter-cell location integrity, the aggregated position information of several vehicles is transmitted over the wireless medium which is open to the public. If the aggregated message is in plaintext, it is vulnerable to an assortment of attacks. One simple solution is to encrypt the plaintext message by using conventional cryptography. However, key management is a very challenging task given the huge number of participating vehicles. This is my future work to follow along with a geographic location-based security mechanism for the provision of physical security on top of conventional methods. The security and privacy message transfer needs to encrypt messages with a secret key which is converted from geographic location information.

**REFERENCES**


94
in Proceedings of IEEE Global Communications Conference (GLOBECOM '09), Nov, 2009.

G.Calandriello, P.Papadimitratos, A.Lioy, and J.P.Hubaux,