# Chapter 6
# Location Security in Vehicular Wireless Networks

**Gongjun Yan**
*University of Southern Indiana, USA*

**Danda B. Rawat**
*Georgia Southern University, USA*

**Bhed Bahadur Bista**
*Iwate Prefectural University, Japan*

**Lei Chen**
*Sam Houston State University, USA*

## ABSTRACT

*In Vehicular Ad-Hoc Networks (VANETs), applications are based on one fundamental piece of information: location. Therefore, attackers will exploit location information to launch attacks. The authors present an in-depth survey of location security methods that have been recently proposed in literature. They present the algorithms or protocols of different methods and compare them with each other in this chapter. The methods are mainly in three aspects: position integrity, position confidentiality, and position availability. The position integrity methods focus on validating a vehicle's position to ensure the position information is correct. Position confidentiality ensures not only the confidentiality of position information but also the authentication of location that a location related message can only decrypt by the receiver which is "physically" present inside a decryption region that is specified by location, time, and speed. The position availability methods create and maintain a reliable routing path to delivery position information. The selection and maintenance of routing paths in literature can be based on multiple resources, for example wireless signal strength, computation resources, and probability models. The three aspects, position integrity, position confidentiality, and position availability, are the three basic requirements of information security based on the standard 200 of NIST.*

DOI: 10.4018/978-1-4666-4691-9.ch006

## INTRODUCTION

In the past few years, VANETs, specializing Mobile Ad-hoc Networks (MANET) to Vehicle-to-Vehicle and Vehicle-to-Roadside wireless communications, have received a huge amount of well-deserved attention in the literature. Indeed, because of their unmistakable societal impact that promises to revolutionize the way we drive, various car manufacturers, government agencies and standardization bodies have spawned national and international consortia devoted exclusively to VANET. Examples include the Car-2-Car Communication Consortium (Car 2 Car Communication Consortium (2009)), the Vehicle Safety Communications Consortium (US Department of Transportation, National Highway Traffic Safety Administration (2006)), and Honda's Advanced Safety Vehicle Program (Takahashi & Asanuma (2000); Yan et al. (2008)), among others. In addition, third party providers have already started to offer Internet access, distributed gaming, as well as other features of mobile entertainment.

The original impetus for the interest in VANET was provided by the need to inform fellow drivers of actual or imminent road conditions, delays, congestion, hazardous driving conditions and other similar concerns. In time, however, it was recognized that the veracity of the traffic advisories is as important as the advisories themselves. A fabricated or doctored traffic advisory distributed by a malicious driver or bystander is apt to create slow-downs and even congestion. This simple fact of life has, in turn, spawned a substantial body of research in information security in VANET. Almost all advisories and other traffic-safety related messages depend in a critical way on positional information. For example, traffic status reports, collision avoidance, emergency alerts, cooperative driving, or resource availability are directly related to positional information. Online payment services, online shopping, and the like, mainly focus on network access. However, most of the time, these applications involve local services which need position information as well. Therefore accurate position information is of key importance. If position information is altered by malicious attackers, these applications will not work at all and will not be adopted by the public.

Therefore it is of importance to make sure location information is integrity. Location integrity means information is origin, correct, and not modified. There are two major methods which enhance or ensure the location integrity. One is encryption. The position information are encrypted. Only those who can decrypt the message can obtain the position information. The other way is validation. Validation can through checking the physical parameters, like the radio signal strength to locate the position. Validation can also be done by computational resources (vehicles failing to solve a puzzle are identified as fakes). Radar or camera can be enlisted to validate the position as well.

Moreover, we discuss the inter-cell position information availability as well because applications (for example, traffic notification, road view, etc.) often involve position information of remote vehicles or entities which are beyond a cell (ranging to miles). The location information of remote vehicles is often aggregated in one packet. Because of the high mobility of vehicles, the routing path which deliveries the aggregated location information packets is fragile. The position information that is not available when you need it, is almost as bad as none at all. It may be much worse for many applications like traffic view application because drivers may be used to these applications and rely on them. But these applications will not work when drivers need them most. The method to improve location availability, i.e., stable routing schemes are addressed.

On the other hand, it is vulnerable to use and store plaintext position information, especially aggregated position information because an attacker can easily modify the position information and harm the position integrity. Both encryption/decryption and access control mechanisms