# Chapter 22
# Security Attacks of Vehicular Networks

**Jen-Chun Chang**
*National Taipei University, Taiwan, R.O.C.*

**Chun-I Fan**
*National Sun Yat-sen University, Taiwan, R.O.C.*

**Ruei-Hau Hsu**
*National Sun Yat-sen University, Taiwan, R.O.C.*

## ABSTRACT

*The application of vehicular ad hoc network (VANET) improves driving safety and traffic management. Due to the above applications, security attacks on VANET can be serious threats all the time. VANET is a special form of mobile ad hoc network (MANET). Hence any attacks exist on MANET also can be arisen on VANET. Moreover, some special attacks can be raised on VANET, which do not exist on MANET. Nevertheless, some characteristics of VANET can be positive effects and some can be negative effects on security issues. Before designing the security mechanism to defend attacks, the authors should take the positive effects and avoid the negative effects on the security of VANET. Furthermore, the authors class all possible attacks of VANET from every network layer. They also introduce the reason of forming every attack and the possible effect on VANET in detail. Therefore this chapter helps understanding the latent threats and the useful resources of security issues on VANET.*

## INTRODUCTION

In recent years, people have fixed their eyes upon traffic-safety topic, because current traffic accident statistics are notoriously horrific. According to the European Red Cross Road Safety Campaign report, approximately 43,000 people die every year on the roads of the European Union (EU), with around 1.8 million people injured, and the costs associated with traffic accidents estimated 160 billion euros. The annual costs associated with crashes (like hospital bills and damaged property) total nearly 3 percent of the world's gross domestic product (GDP) in 2000, or roughly US $1 trillion. In order to reduce the traffic accidents, governments and researchers around the world try to find out effective solutions, and Vehicular Communication (VC) system, or we can also call it Vehicular ac hoc network (VANET),

DOI: 10.4018/978-1-60566-840-6.ch022

Copyright © 2010, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

seems to be one of the answers and will be ubiquitous everywhere in the not-too-distant future.

Vehicular ac hoc network (VANET) is likely to become the most universal and relevant form of ad hoc networks due to the urgent need of driving safety. Another reason about the fast development of VANET is the impact to the market. There are more than 50 applications have been submitted by major car manufactures like BMW, Daimler-Chrysler, Ford, and GM which are based on Dedicated Short Range Communication (DSRC) technology. DSRC is a short range wireless protocol specifically for automotive use. It offers communication between vehicles and Road Side Units (RSUs). This technology for VANET applications is working in the 5.9 GHz band (U.S) or 5.8 GHz band (Japan, Europe).

VC system includes two types of communications:

Inter-vehicle communication (IVC) (or someone call it Vehicle-to-vehicle (V2V) communication) and Roadside-to-vehicle communication (RVC) (or someone call it Vehicle-to-infrastructure (V2I) communication). All two types are based on wireless multi-hop communication.

## Inter-Vehicle Communication

IVC systems have some properties that support security and others that are negative effect.

Properties that have positive effects.

- **No energy constraints:** unlike the sensor node in ad hoc network and/or sensor network and some mobile device, such as cellular phone and personal digital assistant (PDA), cars usually provide enough energy to operate communication system and related computation of security.
- **Known position and time:** This information is required for most safety application on VANET. This information can also be used to security application.
- **Limited physical access:** The operator of IVC usually limited to the owner of car or authorized personnel.
- **Periodic maintenance:** Cars always need to be maintained in a period of time. Therefore, the IVC also can check and update regularly.
- **Secure computing platform:** Automotive environment it seems inevitable that some kind of secure computing platform must be available in the future.

Properties that have a negative effect:

- **High mobility:** High degree of mobility is one of properties of vehicles. It means that the average speed of the node of VANET will be very high and the average connection time will be very short. Therefore, when we design the security mechanism, the communication time and computation time should be considered.
- **Large number of nodes:** IVC network can be a huge ad hoc network. Scalable solutions for adequate and sufficient performance should be considered.
- **No centralized infrastructure:** When we deal with a distributed ad hoc network, the centralized infrastructure is only available at specific situations. The design of some security building block should be adapted to such kind of infrastructure, such as trust management and key distribution and requires new concepts.
- **Privacy concerns:** Privacy is a serious problem in IVC system because cars are highly personal devices and the owners will keep it for a long duration. The system design should reflect the need for flexible identifiers.
- **No user interaction:** The scenario of IVC system is that no user interaction possible since it could distract drivers and reduce the popularity and usability of IVC system.

9 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:
www.igi-global.com/chapter/security-attacks-vehicular-networks/39537

## Related Content

Implicit Cognitive Vulnerability Through Nudges, Boosts, and Bounces
Caroline M. Crawford, Sharon Andrewsand Jennifer K. Young Wallace (2022). *International Journal of Hyperconnectivity and the Internet of Things (pp. 1-14).*
www.irma-international.org/article/implicit-cognitive-vulnerability-through-nudges-boosts-and-bounces/285588

Mobile Peer-to-Peer Collaborative Framework and Applications
Alf Inge Wang (2009). *Mobile Peer-to-Peer Computing for Next Generation Distributed Environments: Advancing Conceptual and Algorithmic Applications (pp. 415-436).*
www.irma-international.org/chapter/mobile-peer-peer-collaborative-framework/26809

Review of Advanced Mobility Solutions for Multimedia Networking in IPv6
József Kovács, László Bokor, Zoltán Kanizsaiand Sándor Imre (2013). *Intelligent Multimedia Technologies for Networking Applications: Techniques and Tools (pp. 25-47).*
www.irma-international.org/chapter/review-advanced-mobility-solutions-multimedia/73983

Alternative Generation in Complex Decision Modelling Using a Firefly Algorithm Metaheuristic Approach
Julian Scott Yeomans (2020). *International Journal of Hyperconnectivity and the Internet of Things (pp. 68-79).*
www.irma-international.org/article/alternative-generation-in-complex-decision-modelling-using-a-firefly-algorithm-metaheuristic-approach/258105

The Effect of the Use of Social Media on Organizational Commitment
Pavithra Salanke, Osibanjo A. Omotayoand Deepak K. V. (2022). *International Journal of Hyperconnectivity and the Internet of Things (pp. 1-13).*
www.irma-international.org/article/the-effect-of-the-use-of-social-media-on-organizational-commitment/294896