Wireless Networks

Liang Xiao
Weihua Zhuang
Sheng Zhou
Cailian Chen

Learning-based VANET Communication and Security Techniques

Springer

Wireless Networks

Series editor

Xuemin Sherman Shen
University of Waterloo, Waterloo, Ontario, Canada

More information about this series at http://www.springer.com/series/14180

Liang Xiao • Weihua Zhuang • Sheng Zhou
Cailian Chen

Learning-based VANET Communication and Security Techniques

Springer

Liang Xiao
Department of Communication Engineering
Xiamen University
Xiamen
Fujian, China

Weihua Zhuang
Department of Electrical & Computer
Engineering
University of Waterloo
Waterloo
ON, Canada

Sheng Zhou
Department of Electronic Engineering
Tsinghua University
Beijing, China

Cailian Chen
Department of Automation
Shanghai Jiao Tong University
Shanghai, China

ISSN 2366-1186 ISSN 2366-1445 (electronic)
Wireless Networks
ISBN 978-3-030-01730-9 ISBN 978-3-030-01731-6 (eBook)
https://doi.org/10.1007/978-3-030-01731-6

Library of Congress Control Number: 2018958477

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Preface

This book provides a broad coverage of the vehicular ad hoc networks (VANETs) to support vehicle-to-vehicle communications and vehicle-to-infrastructure communications and focuses on the vehicular edge computing, vehicular network selection, VANET authentication, and jamming resistance. Machine learning-based methods are applied to solve these issues. This book includes 6 rigorously refereed chapters from prominent international researchers working in this subject area. Professionals and researchers will find *Learning-Based VANET Communication and Security Techniques* a useful reference. Graduate students seeking solutions to VANET communication and security-related issues will also find this book a useful study guide.

In Chap. 1, we briefly introduce the vehicular communication and VANET security and review the machine learning techniques that can be applied in VANETs.

In Chap. 2, we discuss the VANET authentication and focus on the reinforcement learning-based rogue edge detection with ambient radio signals.

In Chap. 3, we review a multi-armed bandit-based offloading scheme for vehicular edge computing.

In Chap. 4, we present an intelligent network selection scheme to provide real-time services for vehicular systems.

In Chap. 5, we review the UAV-aided vehicular transmissions against jamming and formulate a stochastic game between the UAV and the jammer. A reinforcement learning-based UAV relay scheme is presented, and its performance is evaluated.

In Chap. 6, we conclude this book with a summary and point out several promising research topics in the learning-based VANET communication and security techniques.

This book could not have been made possible without the contributions by the following people: Xiaozhen Lu, Geyi Sheng, Minghui Min, Dongjin Xu, Xiaoyue Wan, Xingyu Xiao, Yuliang Tang, Yuxuan Sun, Xueying Guo, Jinhui Song, Zhiyuan

Jiang, Zhisheng Niu, Xin Liu, Shumin Bi, Yuying Hu, and Tom H. Luan. We would also like to thank all the colleagues whose work enlightened our thoughts and research made this book possible.

Xiamen, China	Liang Xiao
Waterloo, ON, Canada	Weihua Zhuang
Beijing, China	Sheng Zhou
Shanghai, China	Cailian Chen
August 2018	

Contents

Chapter 1
Introduction

Vehicular Ad Hoc Networks (VANETs) provides the efficient dissemination of information among the vehicles and roadside infrastructure. However, due to the high mobility of onboard units (OBUs) and the large-scale network topology, VANETs are vulnerable to attacks. In this chapter, we first review the fundamentals of VANETs in Sect. 1.1. Next, the type of attacks in VANETs is presented in Sect. 1.2, including the scope of the attack, and the impact to VANETs. We review the VANETs security solutions based on machine learning techniques including supervised learning, unsupervised learning and reinforcement learning in Sect. 1.3. Finally, we conclude in Sect. 1.4.

In this book, we briefly introduce communication and security in VANETs and investigate the techniques based on machine learning to improve communication efficiency and anti-jamming performance in Chap. 1. We propose a physical-layer rogue edge detection scheme based on reinforcement learning for VANET in Chap. 2. In Chap. 3, we establish a learning-based task offloading framework based on the multi-armed bandit. In Chap. 4, we apply a fuzzy-based method to make network selection on the heterogeneous vehicle network. We investigate anti-jamming solutions with the aid of UAV in VANETs and propose the UAV relay against smart jamming with reinforcement learning in Chap. 5. In Chap. 6, we conclude this book with a summary and point out several promising research topics in communication and security in VANETs.

1.1 Vehicular Communications

With mobile operating systems becoming increasingly common in vehicles, it is undoubted that vehicular demands for real-time Internet access would get a surge in the soon future [1–8]. The VANET offloading represents a promising solution to the overwhelming traffic problem engrossed to cellular networks. The wide

L. Xiao et al., *Learning-based VANET Communication and Security Techniques*, Wireless Networks, https://doi.org/10.1007/978-3-030-01731-6_1

deployment of different wireless technologies and the advanced vehicles with multiple network interfaces equipped, would allow in-vehicle users to access to different real-time services at anywhere anytime from any networks. Therefore, with a vehicular heterogeneous network formed by the cellular network and VANET, efficient network selection is crucial to ensuring vehicles' quality of service (QoS), avoiding network congestion and other performance degradation.

Researches for network selection in urban traffic environment are really few. In the context of future wireless networks, efficient network access system is required for vehicular users' real-time services provisioning [9–11]. We briefly introduce the hierarchical architecture of the heterogeneous vehicular networks as follows.

A hierarchical architecture is shown in Fig. 1.1. It consists of three layers: access network layer, data aggregation layer and application layer. In the access network layer, vehicles connect to cellular base station (eNB) through 3G/LTE or VANET base station (RSU) through DSRC technology. In the data aggregation layer, eNB and RSU are connected to the so-called central controller to access Internet. The aggregation center in the cloud aggregates data from vehicles and static sensors to estimate and predict the urban traffic. The cloud also connects with other service providers such that the traffic-related information can be fused out and provided in the application layer. Different services are then delivered to vehicles through the complementary resources of the cellular network and regional VANET.

In addition to the simple architecture, four components of the architecture are introduced to highlight the characteristics for real-time service provisioning.

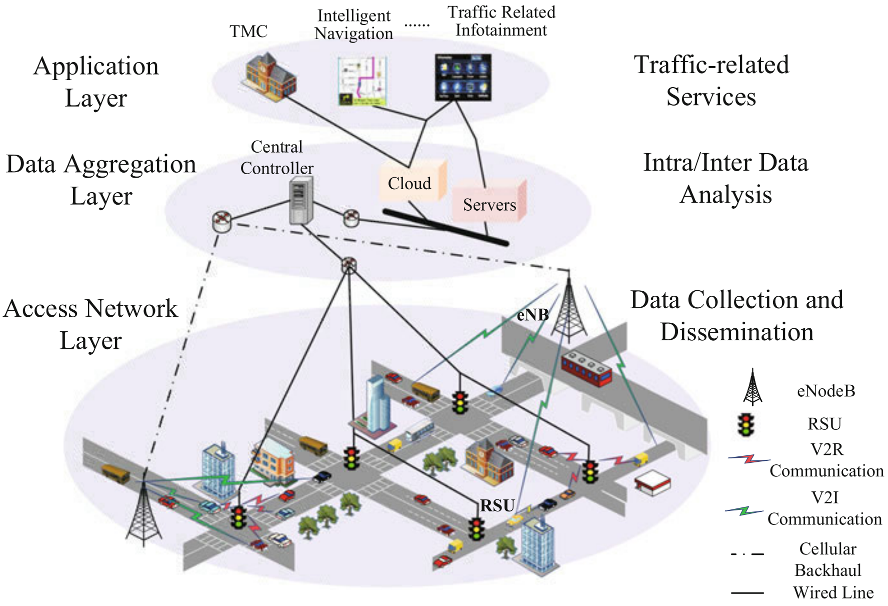

Fig. 1.1 Hierarchical architecture of vehicular networks for ITS

- **Infrastructure:** The infrastructures consist of eNBs and RSUs. The communication link between mobile devices and eNB is more stable than that between devices and RSU. Equipped with a wireless transceiver operating on DSRC, RSU has a smaller transmission range than eNB. But it provides higher rate and lower cost transmission for mobile devices.
- **Vehicle:** We do not discriminate what kind of mobile devices they are, but we care about which network they access to. Normally, smartphones can connect to cellular network through off-the-shelf 3G, while vehicles can connect to VANET and other vehicles through DSRC. We regard both smartphones and vehicles as vehicles.
- **Central controller:** Central controller connects with infrastructures and Internet. An access recommender console is applied in it to guide vehicles' network accessing based on the real-time traffic estimated through cloud calculation. It acts as an interface between physical network routers and network operators to specify network services.
- **Cloud:** As the computing center for traffic management center and other service providers, the cloud receives data from static traffic sensors and mobile sensors, and analyses them for traffic estimation and prediction. One key feature provided by cloud is the access guidance for vehicles in specific location according to traffic analysis and service requests.

With the development of autonomous driving, future vehicles will be equipped with various resources, including computing power, data storage and sensors. It is predicted that about 10^6 dhrystone million instructions executed per second (DMIPS) computing power is required by each vehicle to enable self-driving. These computing resources have huge potential to enhance the intelligence at the edge of the network, and can be integrated as Vehicular Edge Computing (VEC) systems for better utilization [12–14].

In VEC systems, vehicles and infrastructures like RSUs can contribute their computing resources to the network, while computation tasks are generated from various kinds of applications by the vehicular driving systems, on-board mobile devices and pedestrians. To be specific, in safety driving applications such as collective environmental perception and cooperative collision avoidance, the sensing data needs to be processed within tens of milliseconds [15]. By analyzing video recordings in real-time, vehicular crowd-sensing can help to monitor the road conditions and optimize traffic flows [16]. Computation tasks from other applications of mobile edge computing (MEC) [17], such as video stream analysis, augmented and virtual reality, IoT and tactile Internet, can also be offloaded to and processed by the VEC systems.

Compared with the MEC system, task offloading in the VEC faces more uncertainties due to the dynamic vehicular environment. First, the network topologies and the wireless channel states are time varying. Second, the density of vehicles is much higher than that of the static MEC servers, and the computing resources owned by vehicles are heterogeneous. How to allocate computing and communication resources of vehicles, in order to satisfy the delay requirements of tasks, is the key problem of task offloading in VEC systems.

In the VEC system, tasks can be either scheduled by a centralized controller, or offloaded in a distributed manner by each task generator. Some recent efforts are summarized as follows.

- **Centralized approaches:** A centralized VEC architecture is proposed in [14], inspired by the software-defined network. A centralized controller collects the state information of vehicles periodically, including location, velocity, moving direction, and computing resource occupation. Upon user requests, the controller predicts the instantaneous states of vehicles, and allocates the radio and computing resources to process the tasks. In [18], the task assignment problem is formulated based on the semi-Markov decision process. The objective is to minimize the average system cost, which is composed of the delay of tasks and the energy consumption saved at mobile devices. To further improve the reliability of computing services, task replication is introduced in [19], where task replicas are offloaded to multiple vehicles and processed at the same time.

  However, a major drawback of centralized task scheduling is that, the controller needs to govern the accurate state information of vehicles through frequent state updates, which brings high signaling overhead to the VEC systems. To reduce the signaling overhead, distributed approaches are investigated.
- **Distributed approaches:** In distributed approaches, task offloading decisions are made by each task generator individually. An autonomous offloading framework is proposed in [20], and then a task scheduling algorithm is designed based on ant colony optimization. Based on multi-armed bandit theory, a learning-based task offloading algorithm is proposed in [21], which enables task generators to learn the delay performance of other vehicles. The major challenge of distributed control is that vehicles may lack the global state information to make the optimal decision. The state information can be learnt by the task generators using online learning techniques, which will be discussed in detail in Chap. 3.

1.2 VANET Security

Due to time constraints, network scale, node mobility and volatility of the VANET, it's vulnerable to various attacks such as DoS, jamming, eavesdropping and spoofing attacks [22, 23], as shown in Fig. 1.2. For instance, the high mobility of OBUs and the large-scale network with infrastructures such as RSUs make the VANET vulnerable to jamming [24]. Smart jammers send faked or replayed signals with the goal to block the ongoing transmissions between the OBUs and the serving RSUs with flexible jamming strategies and strong radio sensing capabilities.

The global number of the connected vehicles increases rapidly, and vehicles are equipped with increasing amount of computing and storage resources. In order to improve the utilization of vehicle resources, the concept of vehicular cloud