Chapter 6
Real-Time Traffic Simulation of Vehicular Ad hoc Networks

Pradeep Kumar T. S.
https://orcid.org/0000-0001-7071-4752
Vellore Institute of Technology, Chennai, India

Vetrivelan P.
Vellore Institute of Technology, Chennai, India

ABSTRACT

Vehicular ad hoc networks (VANETs) are a type of ad hoc networks where the node movements are high and there will be instant communication between the vehicles (nodes). In this chapter, the authors propose a real-time simulation of vehicular ad hoc networks using simulation of urban mobility (SUMO) in two cases: 1) user-defined road structure and 2) roads designed through open street maps. In both these cases, cars, buses, trucks, pedestrians, and bicycles will be running in the roads. Most of the vehicles will be following the Euro emission norms. Later these cars will be modelled as nodes in a network and analyse the various network performance metrics like throughput and packet delivery ratio were computed.

INTRODUCTION

Vehicular Adhoc networks or VANETs play a major role for various automotive companies for their infotainment systems, car to car connectivity, connecting to Roadside Units (RSU) in case of emergencies like accidents, forest fire, etc. In this chapter, a real world simulation is being carried out using the software Simulation of Urban Mobility (SUMO) for different road design. One of the design would be

DOI: 10.4018/978-1-6684-3610-3.ch006

Copyright © 2023, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

to design a road by any user based on conditions like type of driving (Right Hand or Left Hand), lanes in each road, etc. The other design would be select a Map in the globe through open street map and simulate the network. Many works have been carried out by the researchers and students across the globe in this area. Some of those works are listed here.

Wang, J., et al., (2020) proposed a context aware quantification method for VANETs using Markov Chain process. The simulation is carried out analytically with a creation of a state transition matrix through discrete Markov Chain and Poison process. The security strategies were imitated for the experimentation. Seliem, H et al., (2018) proposed a drone with vehicular communication to minimise the delay between the drones and the vehicles on road. The simulation is carried out in a two-way highway. This paper used a method called as the Drone active service which will identify the location of the vehicles on road. Their results prove that the packet delivery delay between the drones and the vehicles are minimum.

Liu, B et al., (2015) suggested a method for safety messages between the vehicles. In this paper, cloud provisioning is used to deliver the safety message initially to the gateways. Through the gateways, the messages will be delivered to the vehicles nearby. Later using V2V technology, all the vehicles in the networks can get the safety messages. Since its cloud assisted platform, there could some latency in delivering the messages. Alharthi, A., et al., (2021) proposed a blockchain based biometric framework for vehicular networks to store the biometric data secure in a block chain to prevent attacks like Sybil and replay attacks. The simulations were carried out in OMNet++ along with VEINS and calculated the PDR, PLR and the computational cost of such a network. Cheng, C. M., & Tsao, S. L. (2014) implemented a new protocol and simulated using SUMO and QualNet. This protocol deals with a bloom filter that improves the efficiency of the information retrieval system while using the two tier architecture namely VANET and P2P. This paper reduces the latency and overhead by 12 and 20% respectively.

Kumbhar, F. H., & Shin, S. Y. (2020) proposed a fog based node architecture that can predict the most suitable path based on the machine learning models adopted for the VANETs. This work is simulated using SUMO which also measures the packet delivery ratio and the connectivity of up to 4 hops. Haghighi, M. S., & Aziminejad, Z., (2019) have implemented an onion based routing protocol that can maintain anonymity for the source, destination and even the route. The simulation is carried out using SUMO and its compared against the naïve onion protocol that compares with delivery ratio, retransmission and end to end delay. Abuashour, A., & Kadoch, M., (2017) introduced three cluster based routing protocols that can improvise the parameters like delay, throughput, route stability and control overhead messages. The traffic generation is carried out in SUMO and compared it against MATLAB.

13 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/real-time-traffic-simulation-of-vehicular-ad-hoc-networks/313225

Related Content

Reliable Communication in WCF
(2017). *Developing Service-Oriented Applications Using the Windows Communication Foundation (WCF) Framework (pp. 302-334).*
www.irma-international.org/chapter/reliable-communication-in-wcf/175129

How Hiring Baby Boomers Can Assist with the Global Cybersecurity Employee Shortage
Darrell Norman Burrell (2019). *International Journal of Hyperconnectivity and the Internet of Things (pp. 1-10).*
www.irma-international.org/article/how-hiring-baby-boomers-can-assist-with-the-global-cybersecurity-employee-shortage/241801

From Ubiquitous Computing to the Internet of Things
Bozidar Radenkovicand Petar Kocovic (2017). *Emerging Trends and Applications of the Internet of Things (pp. 1-42).*
www.irma-international.org/chapter/from-ubiquitous-computing-to-the-internet-of-things/179784

Smart Ads for Better User Targeting
Albert Asmaryan, Alexey Levanovand Irina Borovik (2019). *Strategic Innovations and Interdisciplinary Perspectives in Telecommunications and Networking (pp. 47-55).*
www.irma-international.org/chapter/smart-ads-for-better-user-targeting/221942

A Strategic Approach to IoT Security by Working Towards a Secure IoT Future
M'Kaila J. Clarkand Lila Rajabion (2023). *International Journal of Hyperconnectivity and the Internet of Things (pp. 1-18).*
www.irma-international.org/article/a-strategic-approach-to-iot-security-by-working-towards-a-secure-iot-future/317088