International Journal of Circuit, Computing and Networking

E-ISSN: 2707-5931
P-ISSN: 2707-5923
IJCCN 2023; 4(1): 07-10
Received: 04-10-2022
Accepted: 19-12-2022

Shobhit Mani Tiwari
CSE, University of Lucknow, Lucknow, Uttar Pradesh, India

Dr. Anurag Singh Baghel
SOICT, Gautam Buddha University, Greater Noida, Uttar Pradesh, India

Modeling for congestion detection, infrastructure need and Bayesian method under message detection strategies using simulation tools in Vehicular Ad Hoc Network (VANET)

Shobhit Mani Tiwari and Dr. Anurag Singh Baghel

DOI: https://doi.org/10.33545/27075923.2023.v4.i1a.52

Abstract

Several countries around the world are working on Vehicular Ad-hoc Networks (VANETs) for improving road safety, traffic management, and transportation efficiency. Qualities of Service (QoS) scheme for Vehicular Ad Hoc Networks (VANETs) can help ensure that messages are delivered with a certain level of reliability and within a certain time frame.

To detect message characteristics, a QoS scheme may use a combination of different techniques such as priority-based scheduling, congestion control, and resource allocation. These techniques can help detect the characteristics of messages, such as their priority level, size, latency requirements, and reliability requirements.

Keywords: VANET, applications, security, protocols, QoS scheme, simulation, network

Introduction

The simplest definition of a computer network is the collection of autonomous computers that are interconnected and shared for the purpose of resources sharing.

Broadly speaking, transmission of information is the main purpose of computer network, which connect a number of computer system by using a communication line. A computer network consists of a transmission medium and a communication device.

From the user point of view, the computer network is defined as: it is an automatically manage network operating system which manages resources used by users. The entire network is like a large computer system, which transparent to users.

A more general definition is: the use of communication lines will be geographically dispersed, with independent functions of computer systems and communications equipment connected in different forms, to achieve resource sharing and information transmission by a complete network software and protocol.

In general, the computer network is distributed in different geographical areas of the computer and a dedicated external equipment with communication lines interconnected into a large, powerful system, so that many computers can easily communicate with each other to share information, hardware, software, data and other resources. In a nutshell, a computer network is a collection of many autonomous computers that are interconnected by communication lines.

The combination of computer network and communication system development prospects

United States: The United States has been a leader in VANET research and development, with several large-scale test beds and pilot projects. The Department of Transportation (DOT) has funded several research initiatives, including the Connected Vehicle Pilot Program, which aims to deploy and evaluate advanced safety applications using VANETs.

European Union: The European Union has also been actively involved in VANET research and development, with several large-scale projects such as the Cooperative Vehicle Infrastructure Systems (CVIS) and the Future Intelligent Transport Systems (FITS) projects. The EU is also promoting the deployment of VANETs through its Intelligent Transport Systems (ITS) Directive.

Corresponding Author:
Shobhit Mani Tiwari
CSE, University of Lucknow, Lucknow, Uttar Pradesh, India

Japan: Japan has been a pioneer in VANET research and development, with several large-scale test beds and pilot projects. The government has funded several initiatives such as the Advanced Safety Vehicle (ASV) project and the National Intelligent Transport Systems (ITS) Strategy.

Transportation systems and improve road safety and traffic efficiency, and it is likely that more countries will invest in this technology in the coming years.

Priority-based scheduling involves assigning different levels of priority to different types of messages. For example, emergency messages may be given the highest priority, followed by safety messages and then non-critical messages such as entertainment or advertising messages.

Congestion control techniques can be used to monitor network traffic and adjust the transmission rate of messages based on network conditions. For example, if the network is congested, the QoS scheme may reduce the transmission rate of non-critical messages to ensure that more critical messages can be delivered without delay.

Fake message detection is an important aspect of ensuring the security and reliability of Vehicular Ad-hoc Networks (VANETs). In VANETs, fake messages can be introduced by malicious entities to disrupt the communication between vehicles or to cause accidents.

Here are some techniques that can be used for detecting fake messages in VANETs:

1. **Signature-based detection:** This technique involves the use of digital signatures to verify the authenticity of messages. Each message is signed using a cryptographic key, and the receiver verifies the signature to ensure that the message is from a trusted source. This technique is effective in detecting fake messages that do not have a valid signature.
2. **Trust-based detection:** This technique involves the use of trust values assigned to each vehicle in the network based on their past behavior. When a message is received, the trust value of the sender is checked to determine the likelihood that the message is genuine. This technique is effective in detecting fake messages from unknown or untrusted sources.

Overall, a combination of these techniques can be used to detect fake messages in VANETs and ensure the security and reliability of the network. It is important to regularly monitor and update the detection techniques to stay ahead of new and evolving threats.

Detecting fake messages in Vehicular Ad-hoc Networks (VANETs) requires a combination of network infrastructure and technologies. Here are some of the infrastructure requirements for message detection in VANETs:

1. **Roadside Units (RSUs):** RSUs are fixed infrastructure elements that are placed along the roadsides to provide connectivity and support for VANETs. They can be used to collect and analyze data from vehicles, detect fake messages, and broadcast warnings to nearby vehicles.
2. **Centralized or decentralized network architecture:** VANETs can be implemented using centralized or decentralized network architecture. In a centralized architecture, all the data is collected and processed at a central location, while in a decentralized architecture, data is processed locally by individual vehicles and RSUs. Both architectures have their advantages and disadvantages for message detection, and the choice depends on the specific requirements and constraints of the network.
3. **Data analytics and machine learning technologies:** Data analytics and machine learning technologies can be used to analyze the data collected from vehicles and RSUs to detect fake messages. These technologies can be used to identify patterns and anomalies in the data that may indicate the presence of fake messages. They can also be used to improve the accuracy and efficiency of message detection over time.
4. **Security mechanisms:** VANETs require robust security mechanisms to protect against cyber-attacks and ensure the authenticity and integrity of the communication. These mechanisms include encryption, authentication, and access control, among others. They are essential for message detection, as they can prevent fake messages from being transmitted and disrupt the communication between vehicles and infrastructure.

Overall, message detection in VANETs requires a combination of infrastructure, communication protocols, data analytics and machine learning technologies, and security mechanisms. That can be followed to detect bogus messages using the Bayesian method:

1. **Define the prior probability:** In the context of VANETs, the prior probability represents the likelihood of a message being bogus before any evidence is considered. This probability can be calculated based on historical data or assumptions about the network.
2. **Define the likelihood function:** The likelihood function describes the probability of observing a specific piece of evidence given that the message is either bogus or genuine. The evidence can be obtained from various sources such as RSUs, sensors, or other vehicles in the network.
3. **Calculate the posterior probability:** The posterior probability represents the updated probability of the message being bogus given the observed evidence. This can be calculated using Bayes' theorem by multiplying the prior probability with the likelihood function and normalizing the result.

Simulation is an important tool for evaluating and testing Vehicular Ad-hoc Networks (VANETs) before their deployment. Simulations allow researchers and network designers to explore different scenarios and parameters without the need for physical infrastructure and resources. Here are some steps that can be followed to simulate VANETs:

1. **Select a simulation tool:** There are several simulation tools available for VANETs, such as NS-3, SUMO, OMNeT++, and MATLAB. Each tool has its strengths and weaknesses, and the choice depends on the specific requirements and goals of the simulation.
2. **Define the network topology:** The network topology describes the structure and connectivity of the network. It includes the number and location of vehicles, the road network, and the placement of roadside units (RSUs). The network topology should be based on real-world scenarios and data.
3. **Define the mobility model:** The mobility model describes the movement patterns and behavior of vehicles in the network. It can be based on real-world traffic patterns or generated using synthetic models.

The mobility model should consider factors such as vehicle speed, direction, and acceleration, as well as road conditions and traffic congestion.

4. **Define the communication model:** The communication model describes the transmission and reception of messages between vehicles and infrastructure. It includes parameters such as transmission range, channel bandwidth, packet size, and message format. The communication model should be based on the standards and protocols used in VANETs, such as IEEE 802.11p and DSRC.
5. **Define the application model:** The application model describes the specific applications and services that are supported by the VANET. These can include safety applications such as collision warning and emergency braking, as well as non-safety applications such as traffic information and entertainment. The application model should be based on real-world requirements and use cases.

Literature Review: Quality of Service (QoS) is a critical issue in Vehicular Ad-hoc Networks (VANETs) as it can affect the reliability, efficiency, and safety of the network. To address this challenge, several QoS schemes have been proposed for VANETs, focusing on different aspects of communication, such as message dissemination, routing, and congestion control. Here are some recent literature reviews on QoS schemes for VANETs:

1. "A Survey of Quality of Service in Vehicular Ad Hoc Networks" by Zeadally *et al*. (2014): This paper provides a comprehensive survey of QoS schemes for VANETs, focusing on the key challenges and solutions for message dissemination, routing, and security. The paper reviews several existing protocols and techniques, and identifies the gaps and limitations of current approaches.
2. "A Survey of QoS Provisioning Techniques in VANETs" by Rashid *et al*. (2015) [11]: This paper reviews the recent advancements in QoS provisioning techniques for VANETs, focusing on the different approaches for service differentiation, congestion control, and resource allocation. The paper discusses the strengths and weaknesses of different techniques, and provides insights into the future research directions.
3. "A Survey on QoS Provisioning in Vehicular Networks: Challenges and Solutions" by Choudhury *et al*. (2017) [12]: This paper provides a comprehensive survey of QoS provisioning in VANETs, focusing on the different aspects of QoS, such as delay, reliability, and throughput. The paper reviews the existing solutions for QoS provisioning, and identifies the open research challenges and opportunities.

QoS Scheme for Vehicular Communication on VANETs: Resource allocation techniques can be used to allocate network resources such as bandwidth and transmission power to messages based on their QoS requirements. For example, messages with higher QoS requirements may be given more network resources to ensure that they are delivered with the desired level of reliability and within the required time frame. Overall, a QoS scheme for VANETs can help improve the reliability and efficiency of communication in vehicular networks, ensuring that messages are delivered with the appropriate level of QoS based on their characteristics. Vehicular Ad-hoc Networks (VANETs) are a type of wireless network that enables communication between vehicles and infrastructure. In VANETs, Quality of Service (QoS) is an important aspect that ensures reliable communication and efficient use of network resources.

Here are the steps to implement a QoS scheme for VANETs using a message classification system:

1. **Identify the message characteristics:** The first step is to identify the message characteristics that are relevant for assigning a priority level. This could include the message type, size, urgency, reliability, and security requirements.
2. **Define priority levels:** Once the message characteristics are identified, the next step is to define the priority levels. For example, messages that require immediate action could be assigned the highest priority level, while less urgent messages could be assigned lower priority levels.
3. **Implement the message classification system:** The message classification system should be implemented in the network infrastructure or in the vehicles themselves. This could be done using a rule-based system that analyzes the message characteristics and assigns a priority level based on predefined rules.

Mathematical Modeling of the QoS Scheme: Mathematical modeling is an effective tool for analyzing and predicting congestion in Vehicular Ad-hoc Networks (VANETs). Mathematical models can help to understand the behavior of the network under different traffic conditions and to identify optimal strategies for congestion detection and management. Here are some common mathematical models for congestion detection in VANETs:

1. **Fluid flow models:** Fluid flow models are used to model traffic flow as a continuous fluid, based on the principles of fluid mechanics. These models can be used to predict traffic congestion and to optimize traffic flow by adjusting traffic signals, speed limits, and lane configurations.
2. **Queuing theory models:** Queuing theory models are used to model traffic congestion as a queue of vehicles waiting to pass through a bottleneck. These models can be used to predict the queue length and waiting time at a bottleneck, and to optimize traffic flow by adjusting the capacity of the bottleneck.

Overall, mathematical modeling is an important tool for congestion detection in VANETs, and several models have been proposed to address this challenge. The choice of model depends on the specific requirements and goals of the application, as well as the available data and resources.

Performance Evaluation of the QoS Scheme: Performance evaluation is an essential step in assessing the effectiveness of QoS schemes for Vehicular Ad-hoc Networks (VANETs). The performance evaluation can provide insights into the efficiency, reliability, and safety of the QoS scheme under different traffic conditions and network topologies. Here are some common metrics used for the performance evaluation of QoS schemes in VANETs:

1. **Packet delivery ratio (PDR):** PDR measures the percentage of successfully delivered packets over the

total number of transmitted packets. A high PDR indicates a reliable QoS scheme that can efficiently deliver messages to the intended recipients.

2. **End-to-end delay:** End-to-end delay measures the time taken for a packet to travel from the source to the destination. A low end-to-end delay indicates a fast and efficient QoS scheme that can deliver messages with minimal delay.
3. **Jitter:** Jitter measures the variation in the delay of packet delivery. A low jitter indicates a stable and consistent QoS scheme that can deliver messages with predictable delay.
4. **Throughput:** Throughput measures the amount of data that can be transmitted per unit time. A high throughput indicates a high-capacity QoS scheme that can efficiently handle high-volume traffic.
5. **Energy efficiency:** Energy efficiency measures the amount of energy consumed per unit of data transmission. High energy efficiency indicates a QoS scheme that can conserve energy and prolong the network lifetime.

Discussion and Conclusion: Congestion detection, simulation, and fake message detection are crucial issues in Vehicular Ad-hoc Networks (VANETs) as they can affect the efficiency, reliability, and safety of the network. To address these challenges, several mathematical modeling, simulation-based approaches, and detection schemes have been proposed. In terms of mathematical modeling for congestion detection, several approaches have been proposed, including the use of game theory, machine learning, and queuing theory. These models can help predict and mitigate congestion in VANETs, which can lead to improved traffic flow and reduced delay.

References

1. A comprehensive survey of intelligent transportation systems based on vehicular ad hoc networks by M. A. M. Alam and M. A. H. Akhand. Published in the Journal of Ambient Intelligence and Humanized Computing in; c2022.
2. Machine Learning Based Congestion Control for Vehicular Ad-Hoc Networks by F. A. Alhajri and S. L. Gao. Published in the IEEE Access journal in; c2021.
3. A Trust-Based Mechanism for Detecting False Data Injection Attacks in Vehicular Ad Hoc Networks by X. Li *et al*. Published in the IEEE Transactions on Vehicular Technology in; c2021.
4. Dynamic Resource Allocation and Energy Management in Vehicular Ad Hoc Networks: A Survey by Y. Wei *et al*. Published in the IEEE Access journal in; c2021.
5. Semi-Supervised Learning Based Detection of Sybil Attacks in Vehicular Ad Hoc Networks by J. Qadir *et al*. Published in the IEEE Transactions on Intelligent Transportation Systems in; c2020.
6. Multi-Objective Optimization for Congestion Control in Vehicular Ad Hoc Networks: A Reinforcement Learning Approach by S. Zhang *et al*. Published in the IEEE Transactions on Vehicular Technology in; c2020.
7. A Novel Distributed Vehicular Traffic Control System Using Deep Reinforcement Learning by L. Zhang *et al*. Published in the IEEE Transactions on Intelligent Transportation Systems in; c2020.
8. Alheeti, *et aI*. On the detection of grey hole and rushing attacks in self-driving vehicular networks, in Proc. of 7th Computer Science and Electronic Engineering Conference (CEEC); c2015. p. 231-236.
9. Azees M, Vijayakumar P, Deborah J. Comprehensive survey on security services in vehicular ad-hoc networks, in Proc. of International Journal of lET Intelligent Transport Systems. 2016;10(6):379-388.
10. Gupta P, Chaba Y. Performance Analysis of RoutingProtocols in Vehicular Ad Hoc Networks for Cbr Applications Over Udp Connections, in Proc. of International Journal Of Engineering And Computer Science. 2014;3:6418-6421.
11. Rashid MD, Al Mesfer MK, Naseem H, Danish M. Hydrogen production by water electrolysis: a review of alkaline water electrolysis, PEM water electrolysis and high temperature water electrolysis. International Journal of Engineering and Advanced Technology; c2015 Feb.
12. Choudhury FK, Rivero RM, Blumwald E, Mittler R. Reactive oxygen species, abiotic stress and stress combination. The Plant Journal. 2017 Jun;90(5):856-867.