Improving the performance of mobile nodes in VANET

Rohit Singh Rajput1 and Dr. Rachana Dubey2*
1M. Tech Scholar, Department of CSE, LNCTE, Bhopal (India).
2Professor & Head, Department of CSE, LNCTE, Bhopal (India).
email: 1rajpoot.rohit2010@gmail.com; 2rachananikishra812@gmail.com
*Corresponding author

Abstract — In the recent years, car manufacturing industries, academia and government agencies have started putting much joint efforts together towards realizing the concept of vehicular communications in a wide scale. Some frameworks are already worked out with the first landmark of standardization processes made by US Federal Communications Communication (FCC) through the allocation of 75 MHz of dedicated short range communication (DSRC) spectrum basically to accommodate V2V and V2I communications for safety-related applications [26]. In this paper, we present the new modified MAC layer protocol for the vehicular ad-hoc network and improve the results for the vehicular ad-hoc network.

Keywords – Vehicular Ad-hoc Network, Data Link Layer, V2V, IEEE.

I. INTRODUCTION

During the last few years, we have all witnessed steadily increasing growth in the deployment of wireless and mobile communication networks [1]. Mobile ad-hoc network is basically a collection of mobile nodes and further is divided into some class such as wireless sensor networks, wireless mesh networks, vehicle ad-hoc network etc. There are various routing techniques used to send the packets information from the source to destination. In order to maintain connectivity in a mobile ad-hoc network all participating nodes have to perform routing of network traffic [5].

MANETs are also capable of handling topology changes and malfunctions in nodes through network reconfigurations. Examples include on-the-fly conferencing applications, networking intelligent devices or sensors etc. Interest in such dynamic wireless networks is not new. It dates back to the seventies, when the U.S. Defense Research Agency, DARPA worked on PRNET and SURAN projects. They supported automatic route set up and maintenance in a packet radio network with moderate mobility. Interest in such networks has recently grown due to the common availability of wireless communication devices that can connect laptops and palmtops and operate in license free radio frequency bands (such as the Industrial-Scientific-Military or ISM band in the U.S.). In an interest to run internetworking protocols on ad hoc networks, a new working group for Mobile, Ad hoc Networking (MANET) has been formed within the Internet Engineering Task Force (IETF), whose charter includes developing a framework for running IP based protocols in ad-hoc networks. Interest has also been partly fueled by the recent IEEE standard 802.11 that include the MAC and physical layer specifications for wireless LANs without any fixed infrastructure.

Routing protocols in packet-switched networks traditionally use either link-state or distance-vector routing algorithm. Both algorithms allow a host to find the next hop neighbor to reach the destination via the “shortest path.” The shortest path is usually in terms of the number of hops; however, other suitable cost measures such as link utilization or queuing delay can also be used. Such shortest path protocols have been successfully used in many dynamic packet switched networks.

The sender of the messages must be authenticated. Nodes should react to the information received from the legitimate users only. As an unauthorized node may transmit false information and mislead others. Therefore we need to authenticate the senders of these messages. It is a challenging task within the vehicular network to ensure authentication because of unattended nature of the network and wireless nature of the transmission media.

II. SECURITY SERVICES OF VANET

* Authentication:

The correctness and timely receipt of information is a major vulnerability. This service deals with the consistency of a stream of messages throughout communication. In the vehicular network, data Integrity is needed to ascertain the reliability of the data. It assures that messages are received as sent without insertion, modification, replays or reordering [7]. As a vehicle can act malicious and tamper the information sent, though it may be a legitimate user [10]
Non-repudiation:
Non-repudiation service refers that either sender or receiver cannot deny the transmission of a message. It is possible that a node may transmit false traffic alerts, however later it refuses that the messages were sent by it [14]. This service may be crucial for investigation to determine the correct sequence and content of messages exchanged before the accident [19] [27].

Confidentiality:
This service ensures that the classified information in the network can never be disclosed to the illegitimate users. Confidentiality protects the privacy of the confidential communication content like name, location, plate number etc. It guarantees the privacy of drivers against unauthorized observers [17]. Pseudonyms technique is used in order to preserve the privacy of the drivers in VANETs.

Availability:
There can be attacks that can lead to loss or reduction in the availability of VANET services such as bandwidth and connectivity. Even a robust communication channel can still suffer some attacks (such as denial of service) which can bring down the network [7]. Therefore, availability of VANETs resources should be also supported by alternative means [27] so that's communication is not hampered.

Access Control:
In VANET, it is essential to define the access privileges for different users. The authorized party needs to define the network policies for the vehicles to access the network [12]. This will help to control the access of different users to various services provided by the VANETs. Access control can be implemented through communication channels, to limit a user's access other vehicles, applications and RSUs.

III. EXPERIMENTAL RESULT ANALYSIS

In this section we present the experimental result analysis and their comparative study with the existing approach and research paper, all the experimental results are simulated with the network simulator ns 2.34.

This chapter provides an overview of network simulation and different VANET simulators that can be used to simulate different VANET algorithms to analyze the performance of the network without the need of real systems. This not only saves cost but also provides opportunity to test new protocols and algorithms in a controlled environment which otherwise would have not been possible.
IV. CONCLUSIONS

The time-based scheme is another approach to control the media access. In this approach, the time is divided into frames, which are divided into time slots. This approach is called Time Division Multiple Access (TDMA). The TDMA mechanism is a contention free method that relies on a slotted frame structure that allows high communication reliability, avoids the hidden terminal problem, and ensures, with high probability, the QoS of real-time applications. In this paper we improve the quality of services parameters for the vehicular ad-hoc network using dedicated short range communication protocol.

REFERENCES


