Simulating VANET Scenario in Nctuns-6.0

Shivani Singh[1], Dr B.V.R Reddy[2]

[1]Department of Computer Engineering,Jss Academy of Technical Education,Noida, India
[2] University School of Information Technology, G.G.S. Indraprastha University, Kashmere Gate, Delhi,India

ABSTRACT

A Vehicular Ad-Hoc Network (VANET) is a form of Mobile Ad-Hoc Network (MANET) which provides safety to vehicle drivers by communicating with nearby vehicles. A vehicle in VANET is considered to be an intelligent mobile node capable of communicating with its neighbours in the network. VANET is different from MANET due to high mobility of nodes and the large scale of networks. In this paper, we implement a VANET scenario in NCTUns-6.0 simulator. We implement two types of communication in VANET: (1) Vehicle to Vehicle (V2V) and (2) Vehicle to Road Side Unit (V2R) communication. The preliminary efforts were focused on the potential applications and the literature review. Our present work in progress is to model and implement various misbehaviours in VANET.

Keywords

VANET, Security, attacks

1. INTRODUCTION

VANET is a form of mobile ad hoc network providing communications among nearby vehicles as well as between vehicles and nearby fixed equipment, usually described as roadside equipment. VANETs are highly mobile wireless ad hoc networks and play an important role in public safety communications and commercial applications. Routing of data in VANET is a challenging task due to rapidly changing topology and high mobility of vehicles. Position based routing protocols are becoming popular due to advancement and availability of GPS devices. One of the critical issues of VANET are frequent path disruptions caused by high mobility of vehicle that leads to broken links which results in low throughput and high overhead .

Each node in VANET periodically broadcasts beacon packets to announce its presence to neighbouring nodes. Each beacon packet contains sender identity, position, time-stamp and speed etc.

2. ONTOLOGY OF VANET

Inter networking over VANET has been gaining a great deal of momentum over the past few years. Vehicles are becoming "computer networks on wheels" and acts as mobile nodes of the network. VANET technology integrates ad hoc network, wireless LAN (WLAN) and cellular technology to achieve intelligent Inter-Vehicle Communications (IVC) and Roadside-to-Vehicle Communications (RVC). VANETs are a special case of MANETs and both are characterized by the movement and self-organization of the nodes. However, unlike MANETs, the mobility of vehicles in VANETs is, in general, constrained by predefined roads. Vehicle velocities are also restricted according to speed limits, level of congestion in roads, and traffic control mechanisms. In addition, given the fact that future vehicles can be equipped with devices with potentially longer transmission ranges, rechargeable source of energy, and extensive onboard storage capacities, processing power and storage efficiency are not an issue in VANETs as they are in MANETs. From these features, VANETs are considered as an extremely flexible and relatively " easy-to-manage" network pattern of MANETs. Due to recent developments in the VANET field, a number of attractive applications, which are unique for the vehicular setting, have emerged. It is beneficial in providing intelligent transportation system (ITS) as well as drivers and passenger' s assistant services. Safety systems may intelligently disseminate road information, such as incidents, real-time traffic congestion, high-speed tolling, or surface condition to vehicles in the vicinity of the subjected sites. This helps to avoid platoon vehicles and to accordingly improve road capacity.

With such active safety systems, the number of car accidents and associated damage are expected to be largely reduced. In addition to the aforementioned safety applications, IVC communications can also be used to provide comfort applications. The latter may include weather information, gas station or restaurant locations, mobile e-commerce, infotainment applications, and interactive communications such as Internet access, music downloads, and content delivery. Here, we define some terminologies used in VANET.

1) RSU : These are the trusted entity standing on the road side.

2) OBU: These are the vehicles having GPS, processing unit, radar, transmitting and receiving antenna.

3. NCTUNS-6.0

NCTUns is a software tool that integrates user-level processes, operating system kernel, and the user-level simulation engine into a cooperative network simulation system. The NCTUns network simulator is a high-fidelity and extensible network simulator capable of simulating various devices and protocols used in both wired and wireless networks. NCTUns provides many unique advantages that cannot be easily achieved by traditional network simulator such as OPNET Modeler and ns-2. NCTUns is mainly composed of six components:

1) Graphical User Interface (GUI);

2) Dispatcher;

3) Coordinator;

4) simulation engine;

5) Application programs; and

6) patches to the kernel TCP/UDP/IP protocol stacks.

The main functions of these components are explained below.

1) **GUI:**

NCTUns provides a front-end GUI program (called "nctunsclient" in its package), which provides useful facilities for users to efficiently create simulation scenario. GUI has been further classified into four components.

a) The "Draw Topology" mode: In this mode, one can insert network nodes, create network links, and specify the locations and moving paths of mobile nodes. In addition, the GUI program provides a complete tool kit for users to construct road networks.

b) The "Edit Property" mode: In this mode, one can double-click the icon of a network node to configure its properties (e.g., the network protocol stack used in this node, the applications to be run on this node during simulation, and other parameters).

c) The "Run Simulation" mode: In this mode, the GUI program provides users with a complete set of commands to start/pause/stop a simulation. One can easily control the progress of a simulation by simply pressing a button on the GUI control panel.

d) The "Play Back" mode: After a simulation is finished, the GUI program will automatically switch itself into the "Play Back" mode and read the packet trace file generated during the simulation. In this mode, one can use the GUI program to replay a node's packet transmission/reception operations in an animated manner.

2) Dispatcher

NCTUns provides a flexibility by which the GUI program and the simulation engine program can be run on different machines. It sends the inquiry message to know which simulation server is currently available. The Dispatcher program is responsible for monitoring the status of the simulation servers to serve the simulation request issued from the GUI program.

3) **Coordinator**

The Coordinator program has the following four tasks:

1) processing the commands sent from Dispatcher;

2) forking (creating) a simulation engine process to perform a simulation;

3) reporting the status of the created simulation engine process to the Dispatcher program; and

4) collecting the simulation results produced by its created simulation engine process and sending them to the GUI program.

4) Simulation Engine

The simulation engine program is composed of a set of various protocol modules and an event scheduler. The former is responsible for simulating protocol behaviors while the latter is r esponsible for scheduling events. The simulation engine can be thought of as a small operating system kernel. It performs basic tasks such as event processing, timer management, packet manipulation, etc. Its API plays the same role as the system call interface provided by an UNIX operating system kernel.

5) Application Program

Application programs are responsible for generating network traffic in a simulated network.

6) Kernel Patches

NCTUns uses the real-life Linux network protocol stack to "simulate" transport-layer and network-layer protocols, such as TCP, UDP, IP, and ICMP.

4. EXPERIMENTAL SETUP

Requirement:

OS: Fedora 10
Platofrm: NCTUns-6.0
ram: 512 MB

The first thing is to construct a road having 2 or more number of lane. Deploy the OBUs and RSUs on the road. You can give the carAgent command and rtg command to all the OBUs and stg command to all the RSUs. Enable the function of provider, set PSID(Provider service Id), Application priority, Service channel Id in the edit mode.

5. CONCLUSION AND FUTURE WORK

In this paper, we present the implementation of VANET scenario in NCTUns-6.0 simulator. We implement two types of communication in VANET (V2V and V2R). Our simulation results show the effectiveness of VANET applications in realistic scenario. In our future work, we would like to enhance our experiments to provide aspects of VANET.

6. REFERENCES

[1] R.Parker and S.Valaee,"Vehicular node localization using received signal strength indicator"IEEE Transactions on Vehicular Technology, vol.56,no.6,part 1,pp 3371-3380,2007.

[2] C. Laurendeau and M. Barbeau,"Insider attack attribution using signal strength based hyperbolic location estimation,"IEEE Transactions on Vehicular Technology, vol.56,no.6,part 1,pp 3371- 3380,2007.

[3] B.-C. Liu, K.-H. Lin, and J.-C. Wu,"Analysis of hyperbolic and circular positioning algorithms using stationary 1. Leinmller T, Schoch E, Kargl F. Position signal-strength-difference measurements in wireless communications,"IEEE Transactions on Vehicular Technology, vol. 55, no.Acknowledgments 2, pp. 499509, 2006.

[4] Rizwanul Karim Sakib , Bisway Reza "Security issues in VANET" Department of Electronics and Communication Engineering April 16, 2010, BRAC University, Dhaka, Bangladesh

[5] NCTUns 6.0, Network Simulator and Emulator.http://NSL.csie.nctu.edu.tw/nctuns.html.