

An Intelligent Secure Traffic Management System Based On Vanet

Abinaya.E¹, Sekar.R²

¹(PG Scholar in Communication Systems, Adhiyamaan College Of Engineering, Hosur,India)

²(AP in Electronics And Communication Engineering, Adhiyamaan College Of Engineering, Hosur,India)

Abstract : In this paper, vehicular ad hoc networks (VANETs) is used to collect and aggregate real-time speed and position information on individual vehicles to optimize signal control at traffic intersections. First formulate the vehicular traffic signal control problem as a job scheduling problem on processors, with jobs corresponding to platoons of vehicles. Under the assumption that all jobs are equal size, By using an online algorithm, which referred to as the oldest job first (OJF) algorithm, to minimize the delay across the intersection. The OJF algorithm is 2-competitive, implying that the delay is less than or equal to twice the delay of an optimal offline schedule with perfect knowledge of the arrivals. It show that, how a VANET is used to group vehicles into approximately equal-sized platoons, which can then be scheduled using OJF. The two-phase approach are used, where first approach is to group the vehicular traffic into platoons and then apply the OJF algorithm, i.e., the oldest arrival first (OAF) algorithm. Our simulation (NS2) results shows that, under light and medium traffic loads, the OAF algorithm reduce the delay experienced by vehicles as they pass through the intersection, as compared with vehicle-actuated methods, Webster's method, and pre-timed signal control methods. Under heavy vehicular traffic load, the OAF algorithm performs the same as the vehicle-actuated traffic method but still produces the lowest delay, as when compared with Webster's method and the pre-timed signal control method.

Keywords: vehicular ad hoc network (VANET), Traffic signal control, vehicular ad hoc network (VANET) simulation, vehicle-actuated traffic signal control

I. Introduction

INTELLIGENT traffic signal control Current methods of implementing intelligent traffic signal control include roadside sensors, such as loop detectors and traffic monitoring cameras. Loop detectors can only detect the presence or absence of vehicles, which is a serious limitation. These loop detectors are physically connected to the traffic signal controller, and this connection is used to communicate the information gathered from the loop detectors to the traffic signal controller. The traffic signal controller then uses the data to schedule traffic through the intersection by cycling through preset phases and assigning appropriate amounts of GREEN time or skipping phases altogether. More recently, video-based traffic detection systems employing traffic monitoring cameras have been considered for traffic signal control. A prominent example of this is in Reno, NV, USA, where traffic data from video cameras is aggregated, and duration of red lights are adjusted based on current traffic volumes. While these have been effective, particularly to coordinate traffic conditions with known events, they require a high degree of human intervention.

In this paper, we examine the possibility of deploying an intelligent and real-time adaptive traffic signal controller, which receives information from vehicles, such as the vehicle's position and speed, and then utilizes this information to optimize the traffic signal scheduling at the intersection. This approach is enabled by onboard sensors in vehicles and standard wireless communication protocols specifically for vehicular applications. For example, all vehicles are already equipped with a speed sensor. In addition, new vehicles are increasingly being equipped with Global Positioning System (GPS) units that can provide location information with accuracy of a few meters. Furthermore, vehicles can use wireless communications for vehicle-to-vehicle (V2V) or vehicle-to-infrastructure (V2I) communications, as described in the dedicated short-range communications/wireless access in vehicular environments standards operating in the spectral range of 5.85–5.95 GHz. We refer to the transient mesh networks formed via V2V or V2I communication links as vehicular ad hoc networks (VANETs).

II. VANET

2.1 VANET DEFINITION

A Vehicular Ad-Hoc Network, or VANET, is a form of Mobile ad-hoc network, to provide communications among nearby vehicles and between vehicles and nearby fixed equipment, usually described as roadside equipment. The main goal of VANET is providing safety and comfort for passengers. To this end a special electronic device will be placed inside each vehicle which will provide Ad-Hoc Network connectivity

for the passengers. This network tends to operate without any infra-structure or legacy client and server communication. Each vehicle equipped with VANET device will be a node in the Ad-Hoc network and can receive and relay others messages through the wireless network. Collision warning, road sign alarms and in-place traffic view will give the driver essential tools to decide the best path along the way. Vehicular Ad Hoc Networks (VANET) are a form of MANETs used for communication among vehicles and between vehicles and roadside equipment shown below in Figure 2.1

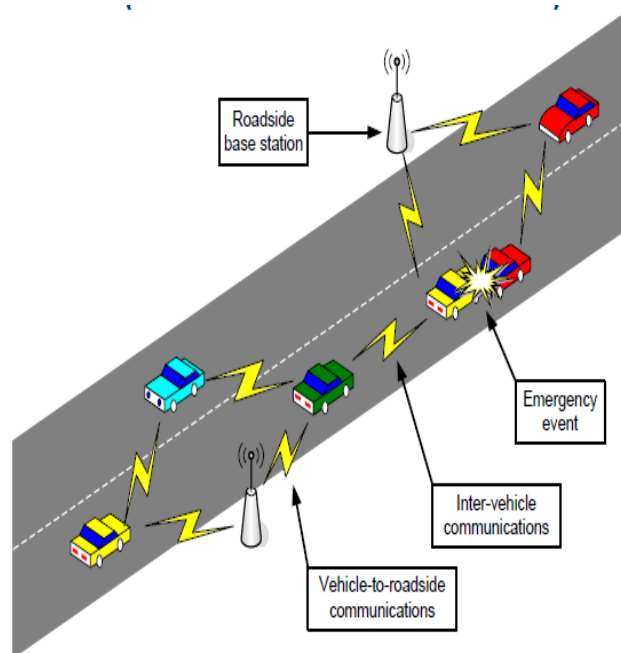


Fig 2.1 VANET Communications

2.2 BASICS OF VANET

Intelligent Vehicular ad-hoc Network

In VANET is an Intelligent Vehicular AdHoc Networking and uses WiFi IEEE 802.11 and WiMAX IEEE 802.16 for easy and effective communication between vehicles with dynamic mobility. Effective measures such as media communication between vehicles can be enabled as well methods to track automotive vehicles. InVANET is not foreseen to replace current mobile (cellular phone) communication standards. Automotive vehicular information can be viewed on electronic maps using the Internet or specialized software. The advantage of Wi-Fi based navigation system function is that it can effectively locate a vehicle which is inside big campuses like universities, airports, and tunnels.

Communication capabilities in vehicles are the basis of an envisioned Intelligent Vehicular Ad-Hoc Network (InVANET) or Intelligent Transportation Systems (ITS). Vehicles are enabled to communicate among themselves (vehicle-to-vehicle, V2V) and via roadside access points (vehicle-to-roadside, V2R). Vehicular communication is expected to contribute to safer and more efficient roads by providing timely information to drivers, and also to make travel more convenient. The integration of V2V and V2R communication is beneficial due to the fact that V2R provides better service sparse networks and long distance communication, whereas V2V enables direct communication for small to medium distances/areas and at locations where roadside access points are not available.

Providing vehicle-to-vehicle and vehicle-to-roadside communication can considerably improve traffic safety and comfort of driving and traveling. For communication in vehicular ad hoc networks, position-based routing has emerged as a promising candidate. For Internet access, Mobile IPv6 is a widely accepted solution to provide session continuity and reachability to the Internet for mobile nodes. While integrated solutions for usage of Mobile IPv6 in (non-vehicular) mobile ad hoc networks exist, a solution has been proposed that, built upon on a Mobile IPv6 proxy-based architecture, selects the optimal communication mode (direct in-vehicle, vehicle-to-vehicle, and vehicle-to-roadside communication) and Figure2.2 shows that provides dynamic switching between vehicle-to-vehicle and vehicle-to-roadside communication mode during a communication session in case that more than one communication mode is simultaneously available.

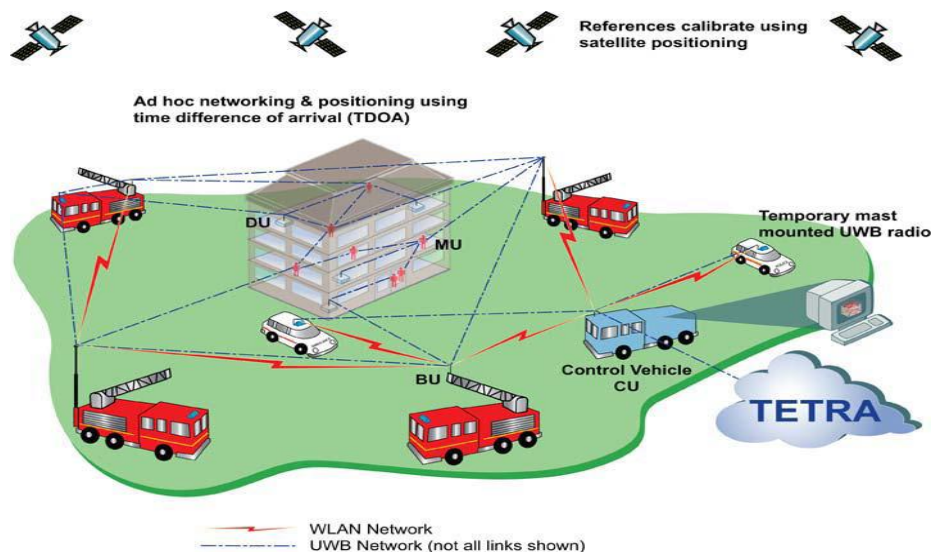


Fig 2.2 VANET Overview

InVANET is an Intelligent Vehicular Ad Hoc Networking and uses WiFi IEEE 802.11 and WiMAX IEEE 802.16 for easy and effective communication between vehicles with dynamic mobility. Effective measures such as media communication between vehicles can be enabled as well methods to track automotive vehicles. InVANET is not foreseen to replace current mobile (cellular phone) communication standards .

2.3 IMPORTANCE OF VANET

- To minimize and eliminate congestion based traffic path during transit by mapping the vehicle to traffic in multiple paths.
- To provide a safe and intelligent solution of identifying optimal paths to the vehicle driver.
- To provide traffic video information this is useful for driver to know particular junction during Traffic congestion.
- To identify the landmark to the vehicle driver or to a new entrant in the city.
- To enable continuous communication (conference) with other vehicle through wire-free networks in non line-of-sight.
-

2.4 CHARACTERISTICS OF VANET

Self-organized networks that do not require a central base station or a fixed network infrastructure

- Robust, scalable and flexible
- Efficient transmission energy
- Able to generate and use location information

Intelligent Vehicular AdHoc Network (InVANET) is a kind of Intelligence in Vehicle(s) which provide multiple autonomic intelligent solutions to make automotive vehicles to behave in intelligent manner during vehicle-to-vehicle collisions, accidents, drunken driving etc. InVANET uses WiFi IEEE 802.11 b/802.11g/802.11p and WiMAX IEEE 802.16 for providing easy, accurate, effective communication between multiple vehicles on dynamic mobility. Effective measures to track the automotive vehicles, media download /upload, conference between vehicles are also preferred. InVANET can also be applied for artillery vehicles during warfare / Battlefield / Peace operations.

Most of the concerns of interest to MANets are of interest in VANets, but the details differ. Rather than moving at random, vehicles tend to move in an organized fashion. The interactions with roadside equipment can likewise be characterized fairly accurately. And finally, most vehicles are restricted in their range of motion, for example by being constrained to follow a paved highway.

2.5 APPLICATIONS

(i) Safety Alerts

- Requirement: Bounded latency
- Primary Issue: Broadcast storm

(ii) Congestion Warning

- Requirement: Message persistence
- Primary Issue: Disconnected network

(iii) Infotainment

- Requirement: End-to-end connectivity
- Primary Issue: Disconnection due to high mobility

(iv) Vehicle-to-Vehicle Communication

(v) Vehicle-to-Roadside Communication

- Traffic Signal
- Stop Sign
- Rail Crossing Violation Warning

III. Impulse Radio Technology

3.1 NEED FOR IMPULSE RADIO TECHNOLOGY

Impulse Radio Technology is a radio transmission scheme that uses extremely low power and it can transmit data at very high rates.

3.2 IMPULSE RADIO DEFINITION

Impulse Radio (IR) emission: is radio frequency energy that is intentionally generated and transmitted by radiation or induction that spreads over very large frequency range that meets the following criteria:

$$(f_H - f_L) / f_C > yy$$

[and/or]

$$(f_H - f_L) \geq zz$$

Where:

yy – fractional bandwidth is greater than [0.20],

zz – minimum limit of bandwidth is [500 MHz],

f_H – upper frequency of the –10 dB emission point,

f_L – lower frequency of the –10 dB emission point,

f_C – centre frequency of the emission.

NOTE – IR is typically generated by direct impulse excitation of the transmit antenna or by using a spectrally filtered approach.

IR transmitter : An intentional radiator that has a bandwidth equal to or greater than [500 MHz] [and/or] a fractional bandwidth greater than [0.2].

IR bandwidth : is the band bounded by the frequency points that are –10 dB below the highest radiated emission, as based on the complete transmission system including the transmit antenna. The upper and lower – 10 dB frequency points are referred to as f_H and f_L , respectively.

IR centre frequency: The centre frequency, f_C , of an IR emission is given by, $f_C = (f_H + f_L) / 2$.

IR fractional bandwidth: The fractional bandwidth of an IR emission is defined as:

$$FBW(\%) = 2(f_H - f_L) * 100 / (f_H + f_L)$$

Pulse transmitter duty cycle: for pulse generated IR, during the period in which the IR transmitter is active, this is the ratio of the impulse duration to the time between the start of two adjacent impulses.

IR radar imaging system: A IR system that is used to obtain images of obstructed objects. This includes in-wall/through-wall detection, ground penetrating radar, medical imaging, construction and home repair imaging, mining, and surveillance systems.

IR ground penetrating radar (GPR) system: A IR radar system that operates only when in contact with or within close proximity to the ground for the purpose of detecting or obtaining images of underground objects.

IR vehicular radar (VR) system: A IR directional radar system mounted on terrestrial transportation vehicles to detect the location and movement of persons or objects near a vehicle to avoid collision and enable other features.

3.3 IMPULSE RADIO CHARACTERISTICS

The high spectral content of the Figure 3.1 shows IR waveform gives rise to one of the primary advantages IR operation for communications where a IR system is robust against multipath fading and narrowband interference. In multipath fading, where the transmitted radio frequency (rf) signal can reflect off objects in its transmission path and can cause destructive interferences at the receiver, a loss of reception can occur. This effect is particularly problematic indoors where there are many reflecting surfaces. In the frequency domain, multipath is shown as frequency selective fading. Because IR communications systems spreads the

transmitted data over a broad frequency band if destructive interference occurs at a specific frequency, whether due to multipath or narrowband interference, the information can still be recovered over the good frequencies.

▪ FCC ruling permits IR spectrum overlay

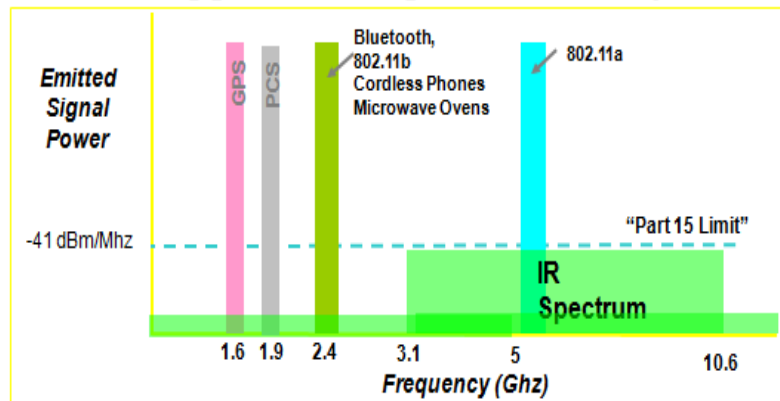


Fig 3.1 Impulse Radio Spectrum permits by FCC

IR implementations can provide low complexity, low cost solutions, thus enabling vast deployments of the technology. A critical component that reaffirms a low cost solution is noting that IR signals, being carrierless, have greater simplicity over narrowband transceivers and require smaller silicon die sizes. IR can be designed to achieve very high bit rates while still achieving low power consumption, a feature set which will be exploited by the consumer electronics industry. IR schemes can further be designed to be very scalable in terms of complexity, bit rate, power consumption, and range. IR technology can support many applications. Different IR modulation schemes offer different advantages for communication, radar, and precision geo-location applications. IR technology, which operates between 3.1 and 10.6 GHz, intrinsically offers an efficient reuse of precious spectrum by operating stealthily at the noise floor. This IR system operates at low power, to be compliant with operating under FCC Part 15 emissions, across a wide range of frequencies.

As a spread spectrum technology, IR offers a low probability of intercept and a low probability of detection. Thus, it is particularly well suited for covert military or sensitive usage scenarios. Because IR signals have extremely short bursts in time (e.g., durations of 1 ns or less) they are suited for precision geo-location applications. Though IR intrinsically offers the above-mentioned features, application optimization and improvements on these characteristics are left to specific designs and implementations, most notably by careful consideration of modulation schemes.

IV. Vehicular Ad Hoc Network-Based Traffic Intersection Control

Here, we show how we implemented the platooning phase (phase one) of the OAF algorithm and how we implemented the other traffic light control schemes, such as the vehicle-actuated logic and Webster’s method using VANETs. We first explain some of the terms used in describing our adaptive traffic control algorithms that may differ slightly from their conventional definitions.

- MAX-OUT: The maximum amount of GREEN time that can be allocated to the current phase.
- GAP-OUT: If a vehicle is more than the GAP-OUT units of time away from the stop line, then the signal goes to the next phase.
- EXTENSION: If a vehicle is detected less than GAP-OUT units of time away from the stop line, then the GREEN time is extended by EXTENSION units of time.

System Description

In this paper, we only study an isolated intersection. Fig 4.1 shows the single traffic intersection under consideration. It is a typical four-leg intersection with eight traffic movement groups represented by the arrows. Each of the legs of the intersection is *L* meters long, and each of the left turning bays is *B* meters long. The numbered arrows show the directions of the various traffic movements. For this type of traffic intersection, we now describe the system architecture of the VANET-based traffic signal controller. In the single traffic intersection scenario, the traffic signal controller is connected to a wireless receiver that is placed at the intersection. The wireless receiver listens to information being broadcast from the vehicles. The broadcast medium is the 5.9–5.95-GHz radio spectrum, and the communication standards are defined in the IEEE 802.11p standards. The information consists of speed and position data collected from vehicles. Speed data can be

gathered from the vehicle speedometers, and position data can be gathered using GPS receivers fitted to the vehicles. In our implementation, the following data are gathered and encapsulated in data packets that are broadcast over the wireless medium. This is what we call the data dissemination phase.

- **Vehicle ID:** Every vehicle is uniquely identified by its Vehicle ID#. In our traffic simulator, every vehicle is identified by a unique unsigned integer. In practice, the medium access control (MAC) address of the network interface card in the wireless receiver would serve the same purpose.
- **Location:** The location of each vehicle is specified by the LINK NUMBER#, Lane#, and position from a point of reference. The position from a point of reference is a subfield containing (x, y), which are floating point quantities. We chose to use the stop line as a point of reference; therefore, the stop line has position (0, 0) for each Link Number# and Lane#. Thus, collectively, these three fields describe vehicle location. In practice, it is assumed that each vehicle is equipped with a GPS receiver; therefore, vehicles always know their locations.
- **Speed:** Speed of a vehicle is a floating point quantity expressed in meters per second and is obtained from the in-vehicle speedometer sensor.
- **Current Time:** The time at which the packet was created. The format is (hh:mm:ss). Because of the nature of the traffic control application, there is no need for a finer grain time. However, we need to assume that all clocks are synchronized. The current time is required to distinguish between old packets and new packets.

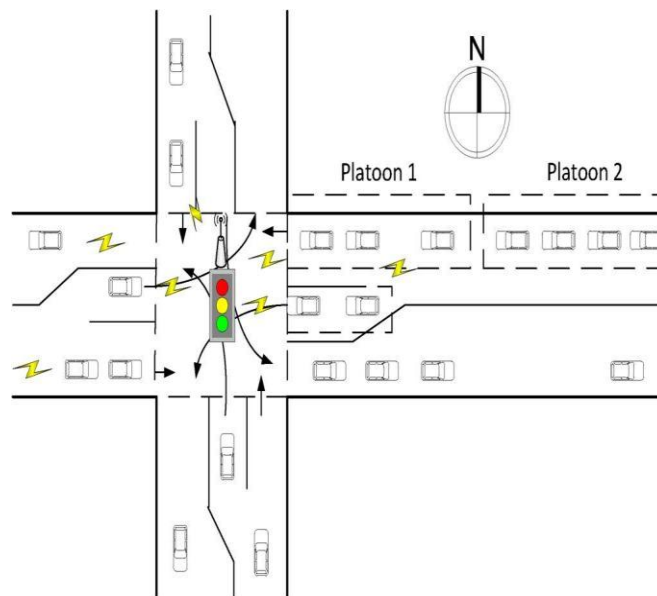


Fig 4.1 VANET-based traffic signal control architecture.

A. Vehicle route construction

In this module, Route has many numbers of vehicles and their details. It maintains the vehicle connection details also. Vehicles are connecting with other vehicles in all the route ways. Centralized server will maintain the vehicle details and status each and every vehicle movement required. Here generates the protection for each vehicle fixed and it secures on both condition OBU (On-Board Unit's) and RSU (Road Side Unit's). Vehicles will give the request to centralize server and get the needed response from centralized server while moving one network to another one.

B. Centralized Server

A server is a collecting the vehicle details list i.e., running to serve the requests of every vehicles. Thus, the "Network/ Server" performs some computational task or connect through the different network. Here the Centralized Server acts as the main resource for the vehicles. Each vehicles information will be stored in the Server. Also the Server will maintain the route traffic information, So that the Vehicle/User can retrieve the information of the current area into wherever, where the traffic is occurred.

C. Priorities Based Vehicle Movement

In this module, it uses both algorithms to identify the locations of the vehicles. For each route we can use OJF and OAF up to the destination. By showing the designed the network, we can identify that the Vehicle/User is traveling in a specified location based on speed and traffic signal controller. To view the traffic

and user's movement, we will use this waives the need for a traffic light schedule for movements while a high-density road traffic condition poses a challenge for authentication of vehicular messages since the required verification time is often much longer than the average inter arrival time.

D. Identify The Traffic And Accident

In this module, the server will identify the traffic or an accident is occurred by indicating the signal that was passed the anyone of the Vehicle ID. So that the user can know that the traffic has been occurred in the specific path. Then the user will take an alternative route to reach their destination. That intimation will flow the Server maintaining and monitoring for each and every vehicles in the entire network.

E. Alertnate and best path identification

In the Modification part, the user can give a request to the server regarding the source and destination information that they want to travel. The server will display the best path identification to reach the destination. By using this technique, the user can priory knows about the traffic in the specific location and takes alternate/best route to reach the destination.

Requirement Analysis

Requirement analysis determines the requirements of a new system. This project analyses on product and resource requirement, which is required for this successful system. The product requirement includes input and output requirements it gives the wants in term of input to produce the required output. The resource requirements give in brief about the software and hardware that are needed to achieve the required functionality.

i. Minimum Hardware Requirements

Operating system	: Windows XP/Ubuntu
Processor	: Intel Core 2 Duo processor (2.2 GHz)
Hard disk	: 160 GB
RAM	: 2 GB DDR

ii. Software Requirements:

Since the project is based on Ad-hoc networks it makes use of NS2 simulator for this purpose. The simulator is an open source product. Since NS2 is a Unix/Linux based application, Fedora 8 Linux is used as the platform for the development process. The details of the simulator and the software used are given below,

- Red Hat / Fedora core 8 / Linux / Windows XP
- Network Simulator 2
- Network Animator
- Trace graph

a) Network Simulator

Network simulator is an object-oriented discrete event simulator. It is also a package of tools that simulates behavior of networks. It is primarily UNIX based. It creates network topologies. It is written in C++ and OTCL formats (TCL scripting with object-oriented extensions). NS is primarily useful for simulating local and wide area networks. It can be used to simulate a variety of IP networks. It implements network protocols such as TCP and UPD, traffic source behavior such as FTP, Telnet, Web, CBR and VBR, router queue management mechanism such as Drop Tail, RED and CBQ, routing algorithms such as Djikstra, and more. NS also implements multicasting and some of the MAC layer protocols for LAN simulations. A simplified view of NS2 is shown below in figure 4.2

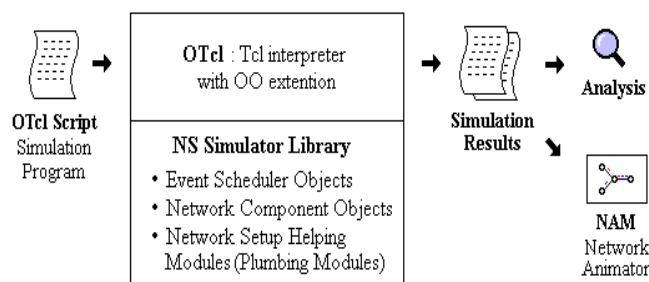


Figure 4.2 Simplified user view of NS2

NS is Object-oriented TCL (OTCL) script interpreter that has a simulation event scheduler and network component object libraries, and network setup (plumbing) module libraries (actually, plumbing modules are implemented as member functions of the base simulator object). In other words, to use NS, you program in OTCL script language. To setup and run a simulation network, a user should write an OTCL script that initiates an event scheduler, sets up the network topology using the network objects and the plumbing functions in the library, and tells traffic sources when to start and stop transmitting packets through the event scheduler. The C++ and OTCL duality is shown below in figure 5.2

NS is written not only in OTCL but in C++ also. For efficiency reason, NS separates the data path implementation from control path implementations. In order to reduce packet and event processing time (not simulation time), the event scheduler and the basic network component objects in the data path are written and compiled using C++. Likewise, an object (not in the data path) can be entirely implemented in OTCL. figure 4.2 shows an object hierarchy example in C++ and OTCL.

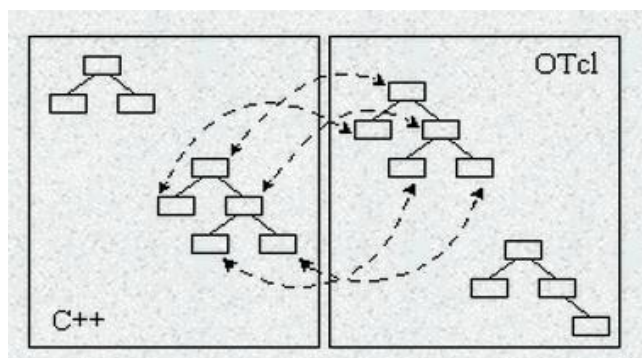


Figure 4.3 C++ and OTCL- The duality

The event schedulers and most of the network components are implemented in C++ and available to OTCL through an OTCL linkage that is implemented using Tcl. The whole thing together makes NS, which is a OO extended TCL interpreter with network simulator libraries. When a simulation is finished, NS produces one or more text-based output files that contain detailed simulation data, if specified to do so in the input TCL (or more specifically, OTCL) script. figure 4.3 gives a broad idea about the architecture of NS. The data can be used for simulation analysis (two simulation result analysis examples are presented in later sections) or as an input to a graphical simulation display tool called Network Animator (NAM).

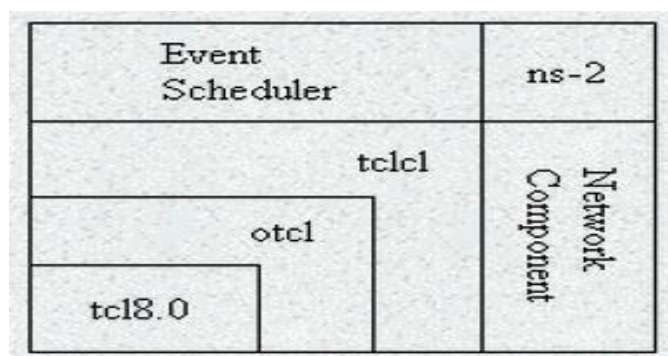


Figure 4.4 Architectural View of NS

b) Network Animator

NAM is a TCL based animation tool for viewing network simulation traces and real world packet trace data. The design theory behind NAM was to create an animator that is able to read large animation data sets and be extensible enough so that it could be used indifferent network visualization situations.

c) Trace Graph

Trace graph is a free network trace file analyser developed for network simulator NS2 trace processing which runs under UNIX systems. Trace graph can support any trace format if converted to its own or NS2 trace format. Trace graph supports wired as well wireless network tracing.

V. Methodologies And Simulator Result

5.1 METHODOLOGY USED

1. Security Algorithm(faster randomized algorithm)

Fast Randomized Algorithm:

This is an algorithm which gives excellent results when detect and verify on node location via RSU in the networks based random key. And it is much faster, if the attacker hack the secret key means it don't create any misbehavior activity because vehicle moves one network to another network means the random key changed for security purpose. In our concept Centralized server will maintain vehicle details and status each and every vehicle movement required. CRL generates the Secret key(random key) for each vehicle and it secures on OBU and RSU. Vehicles will give the request to centralize server and get the needed response from centralized server while moving one network to another one.

2. Block Forwarding Process

Block forwarding process is used to identify the best route when collision occurring. the CRL Server will maintain the route traffic information, So that the Vehicle/User can retrieve the information of the current area into anywhere where the traffic is occurred. the user can give a request to the server regarding the source and destination information that they want to travel. The server will display the best path identification to reach the destination.

3. Oldest Arrival First (OAF) algorithm

Oldest arrival first (OAF) algorithm, show that, under light and medium traffic loads, the OAF algorithm reduces the delays experienced by vehicles as they pass through the intersection, as compared with, pre timed signal control methods. Under heavy vehicular traffic load, the OAF algorithm performs the same as the vehicle-actuated traffic method but still produces lower delays.

5.2 SIMULATOR RESULTS

When we run the Network simulator ,first the VANET network initialize the current network ,RSU units,Vehicles position and other sub units i.e.,fig 5.1. All the information about the vehicle is collected and stored in the desired RoadSideUnit(RSU),the number of vehicles ,RSU and networks are allocated by their respective places ,the allotted numbers are default.Vehicles are connected with the other vehicles and network with the help of routes .

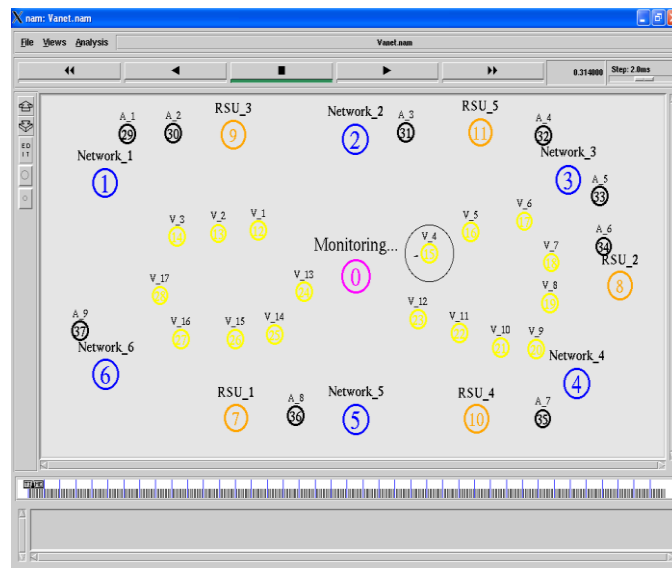


Fig 5.1- Initialization of VANET Monitoring the Vehicles

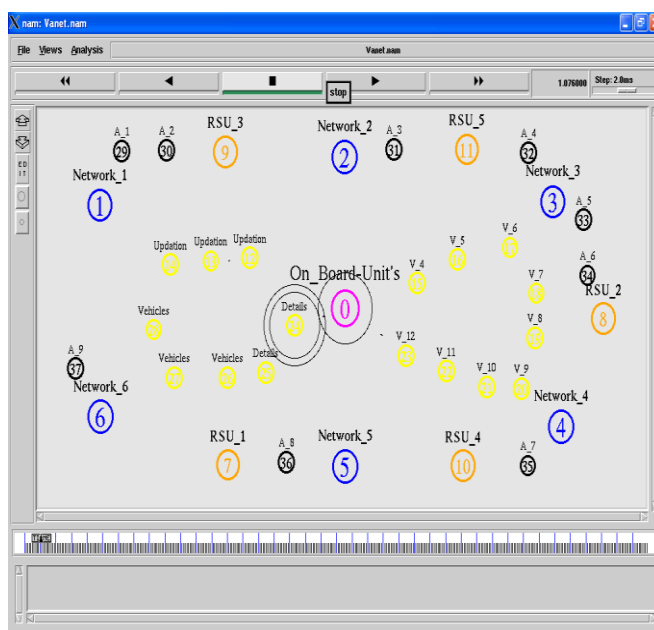


Fig 5.2 On-Board- units in the vehicle

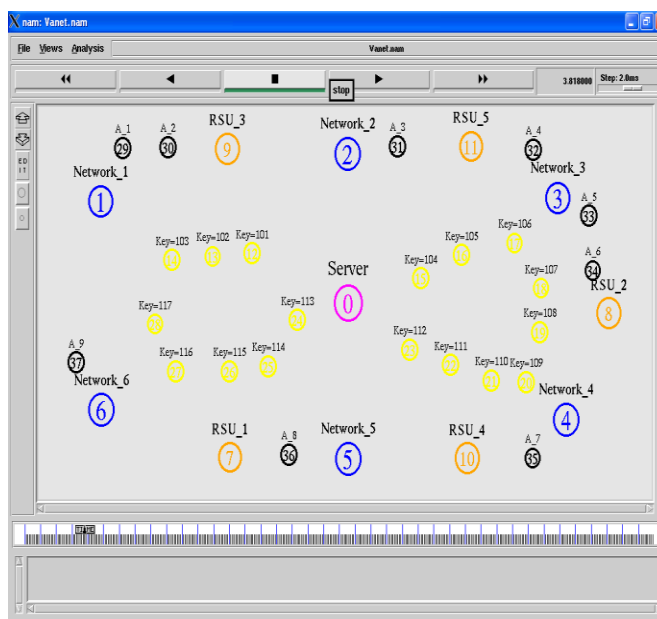


Fig 5.3-Server and key Allocation

In above fig 5.3, all vehicles around the server have their own ID and License Number for their identification. A server collect the Vehicle details with the help of the Certificate Revocation List(CRL) which contain current key and future key. When the vehicle moves from one network to other network, the desired network will monitor the vehicle and check for the new key fig 5.4. The advantages by applying the different keys are,

- a. By randomly changing the key, it avoid the hacker.
- b. During the traffic, if any vehicle blocked in center of road or any place in vehicle, suddenly the RSU unit inform to server and it send the information about the incident to all allocated vehicle.
- c. If no traffic in the road, the RSU monitor the road continuously and intimate the server, If any vehicle stopped in roadside, the RSU will turn off the sending and receiving the information of that particular vehicle, and set it as in SLEEP MODE. After this process that particular vehicle have to register and get the new ID or Key.

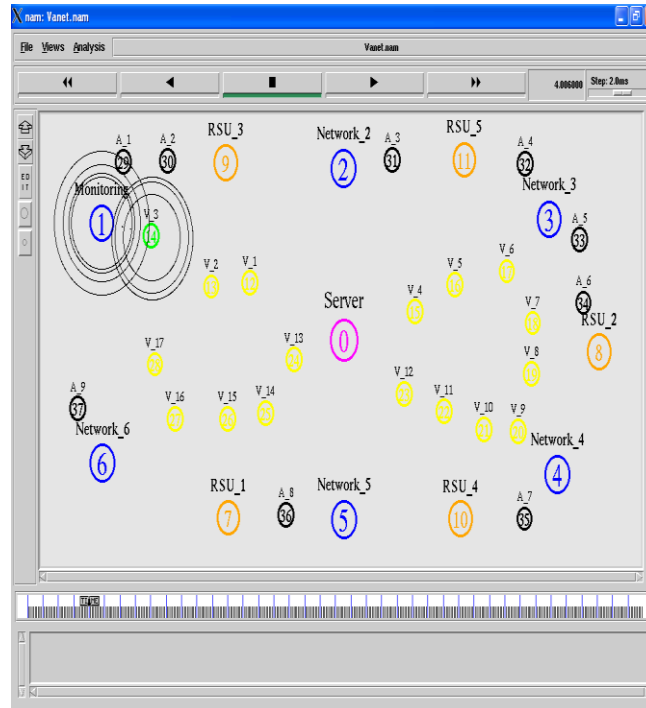


Fig 5.4 server,CRL Monitoring



Fig 5.5 Comparison between the ServerMonitoring Vs Networks

5.3 FEASIBILITY STUDY

The feasibility of the project is analyzed in this phase and business proposal is put forth with a very general plan for the project and some cost estimates. During system analysis the feasibility study of the proposed system is to be carried out. This is to ensure that the proposed system is not a burden to the company. For feasibility analysis, some understanding of the major requirements for the system is essential.

Three key considerations involved in the feasibility analysis are

- ECONOMICAL FEASIBILITY
- TECHNICAL FEASIBILITY
- OPERATIONAL FEASIBILITY

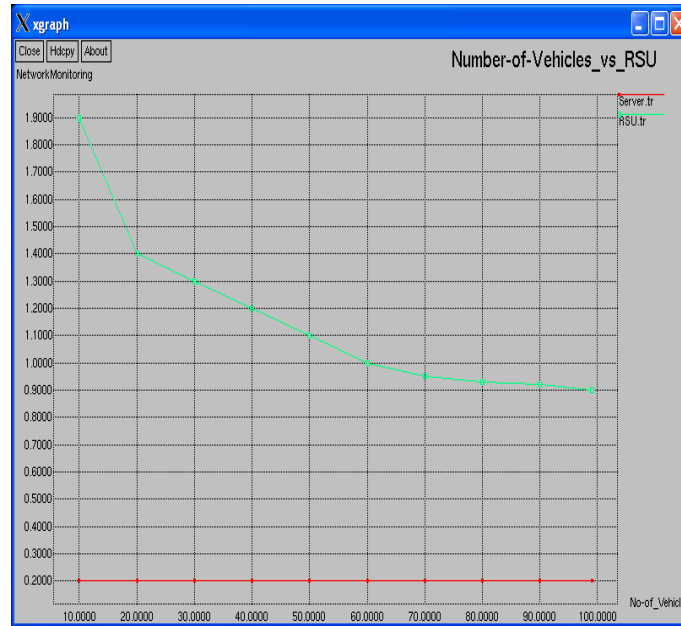


Fig 5.6 Comparison between the Number-Of-Vehicles Vs RSU

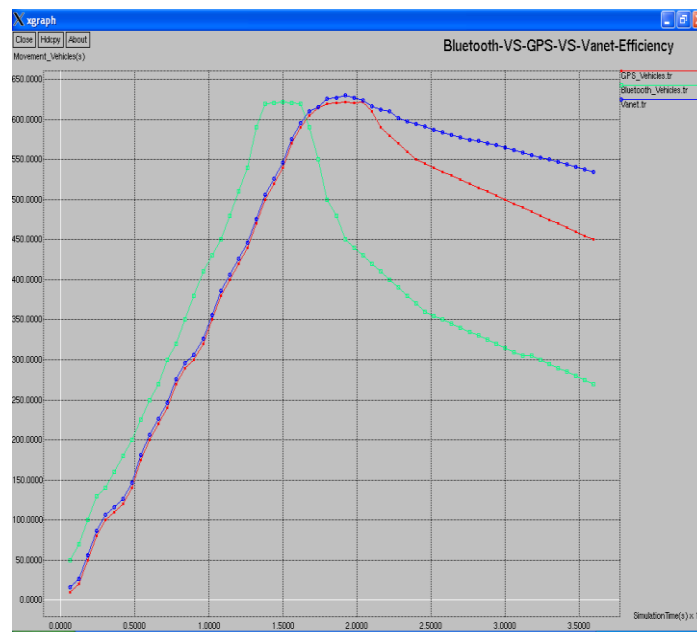


Fig 5.7 Comparison between the Bluetooth Vs GPS Vs Vanet Efficiency

VI. CONCLUSION

In this paper, we have shown how a VANET can be used to aid in traffic signal control, including a new job-scheduling based online algorithm, i.e., the OAF algorithm. We implemented several adaptive traffic signal control algorithms that use the fine grain information broadcasts by the vehicles. In this paper, we designed an ID-based anonymous user authentication scheme and a cross-layer verification approach to WAVE enabled VANET's safety messages. A variation of the conventional ECDSA approach is used with the ID-based signature approach, where the common geographical area information on signing vehicles is taken as the signer's identity. This exempts a vehicle from the mandatory inclusion of a trusted third-party certificate with each broadcast message in a VANET, whereas a user is still identifiable by the trusted third party upon a dispute. A cross-layer message verification scheme verifies the received messages based on their MAC traffic class and traffic intensity. This ensures that under rush-hour congestions or after a traffic accident, most important messages will not be missed by the Verifier. Security analysis and performance evaluation justify our authentication and verification approach to WAVE-enabled vehicular communications.

Under heavy vehicular traffic load, the performance of the OAF algorithm degenerates to that of the vehicle-actuated traffic method but still produces lower delays, compared with Webster's method and the pre timed signal control method. This is because, under lighter traffic, the OAF algorithm can dynamically skip through phases and minimize the delay of vehicles whenever there is a gap in the traffic. In Future work, the research can make in an optimal method of key distribution is needed. It is still clear as to the best method of key distribution. However, special times to update keys would be convenience for most owners, so the updates and distributions should perhaps be done during regular maintenance or license renewal.

REFERENCES

- [1] Vanet Based Traffic Management System Development And Testing Using Aodv Routing Protocol, PATIL V.P.Smt. Indira Gandhi college of Engineering, New Mumbai, INDIA, IJCER, sep2012
- [2] Velocity Measurement and Traffic monitoring Using GSM Passive Radar Demonstrator, P. Krysik, P. Samczynski, M. Malanowski, L. Maslikowski, K. S. Kulpa, Warsaw University of Technology, IEEE oct 2012
- [3] Adaptive Traffic Lights Using Car-to-Car Communication, Victor Gradinescu, Cristian Gorgorin, Raluca Diaconescu, Valentin Cristea "Politehnica" University Bucharest Computer Science Department, IEEE
- [4] Vanet Based Traffic Management System Development And Testing Using Aodv Routing Protocol. PATIL V.P.Smt. Indira Gandhi college of Engineering, New Mumbai, INDIA, International Journal Of Computational Engineering Research (ijceronline.com) ,sep 2012
- [5] Intelligent Traffic System for VANET: A Survey Ganesh S. Khekare¹, Apeksha V. Sakhare² Department of Computer Science and Engineering, G. H. Raisoni College of Engineering, Nagpur, India, International Journal Of Computational Engineering Research (ijceronline.com) ,dec 2012
- [6] A VANET-based Emergency Vehicle Warning System Andreas Buchenscheit, Florian Schaub, Frank Kargl, and Michael Weber Institute of Media Informatics, Ulm University, Germany, IEEE2009
- [7] An Ultra-Wide Band Based Ad Hoc Networking Scheme for Personnel Tracking in Emergencies, Liang Xia, Anthony Lo, Ignas Niemegeers Department of Telecommunications Delft University of Technology Delft, the Netherlands, EUROPCOM project.
- [8] An Intelligent Secure and Privacy-Preserving Parking Scheme Through Vehicular Communications ,Rongxing Lu, Student Member, IEEE, Xiaodong Lin, Member, IEEE, Haojin Zhu, Member, IEEE, and Xuemin (Sherman) Shen, Fellow, IEEE, july2010
- [9] Performance Modeling of Safety Messages Broadcast in Vehicular Ad Hoc Networks, Mehdi Khabazian, Member, IEEE, Sonia Aïssa, Senior Member, IEEE, and Mustafa Mehmet-Ali, Member, IEEE, march2013