International Journal of Emerging Technology and Innovative Engineering
Volume I, Issue 3, March 2015
ISSN: 2394 - 6598
www.ijetie.org

DESIGN AND ANALYSIS OF A ROBUST BROADCAST SCHEME TO VANET

Prof. Harish Barapatre[1] *Miss.* Siddhi Sawant [2] Miss. Rupali Patil [3]
Mr. Aditya Matlani [4] Miss. Smita Kamble[5]
B.E COMPUTER ENGINEERING

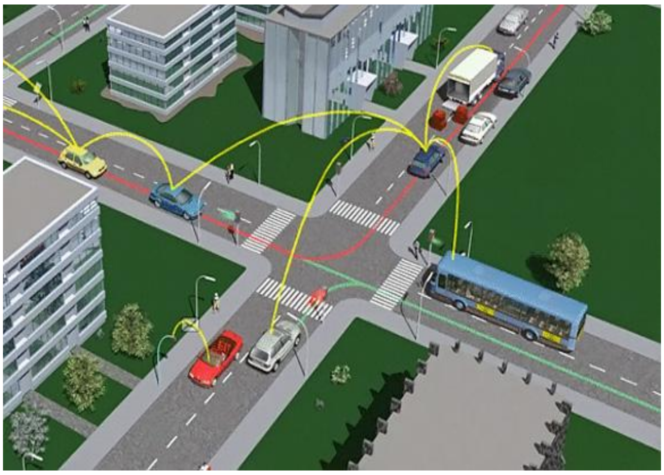
Yadavrao Tasgaonkar Institute Of Engineering And Technology, Bhivpuri Road, Karjat.[1 2 3 4 5]

***Abstract*—Establishment of vehicular ad-hoc network is most demanding in smart traffic management system. By sharing the information between traffic system, road side unit and vehicles research can create vehicular network. Automatic detection of road signs has recently received attention from the computer vision research community. The main objective of this system is to detect signs from a moving vehicle. Road Traffic Sign Detection is a technology by which a vehicle is able to recognize the traffic signs put on the .we are proposing the system which will use one signal transmitter in each and every symbol or message board at road side and whenever any vehicle passes from that symbol the receiver situated inside the vehicle will receive the signals and display proper message or the symbol details on display connected in car. Now driver can concentrate on driving Position information is a fundamental requirement for many vehicular applications such as navigation, intelligent transportation systems (ITSs), collision avoidance, and location based services**

***Keywords*—Ad hoc network, Road Traffic Sign, Symbols, VANET.**

Introduction

Inter vehicular communication is an integral part of intelligent transportation systems(ITSs),which have been growing attention in recent years. The concept of ITS has been originated to advance transportation safety and efficiency through dissemination of road and traffic information, e.g., real time updates regarding collisions, incidents, congestion, surface and whether condition etc. The most prominent feature of VANETs is the high mobility of the nodes, which is the underlying cause of a series of VANET-specific attributes requiring the development of applicable solutions. With the increase of road traffic volume in major cities and towns of most of the countries experiencing traffic congestions, accidents and greenhouse emissions leading to poor quality of city life. The most trusting features of VANETs are the high mobility of the nodes, which is the underlying cause of a series of VANET-specific attributes requiring the development of applicable solutions. Transient connectivity due to node mobility is an inherent attribute of all mobile networks, which becomes even more evident in the case of vehicular communications. This causes significant problems as communication is disrupted very often, resulting in poor performance. The constantly changing topology has numerous adverse effects on the efficiency of the operations of higher layers on the Protocol stack. The resulting disruption of information flow causes considerable delays, and route reconstruction depletes a significant amount of network resources.



I. DESIGN CHALLENGES

A. *Technical challenges*

The technical challenges deals with the technical obstacles which should be resolved before the deployment of VANET.
Network management, congestion and collision control.

B. *Social and economic challenges*

Apart from the technical challenges to deploy the VANET, social and economical challenges should be considered. It is difficult to convince manufacturers to build a system that conveys the traffic signal violation because a consumer may reject such type of monitoring. Conversely, consumer appreciates the warning message of police trap. So to motivate the manufacturer to deploy VANET will get little incentive.

C. *Security challenges*

The challenges of security must be considered during the design of VANET architecture, security protocols, cryptographic algorithm etc.

II. SOLUTION FOR CHALLENGES

To overcome this issue proposed system is designed to have an infrastructure to vehicle communication to share infrastructure information. Whenever any vehicle passes away from any symbol its signal get detected by the signals detectors which are connected in car. This signal then converted in to proper symbol and displayed on the display panel connected in the car. This is how it show specific symbols to the driver which help driver in finding specific symbols and there meaning also. Similarly the next proposed method is Vehicle to Vehicle Communication. Suppose a vehicle having different information like vehicle location, vehicle statistics or vehicle health. This information need to be share with other vehicle in VANET in order to avoid traffic conjunction and to dealevery symbol or navigational boards has unique symbols and the unique meaning. In VANET many security solutions been proposed, and large number of papers were introduced to solve the above problems, the authors in [1] and in [4] suggested the use of VPKI (Vehicular Public Key Infrastructure) as a solution, where each node will have a public/private key. When a vehicle sends a safety message, it signs it with its own private key and adds the Certificate Authority (CA's) certificate as follows: V → r: M, SigPrKV [M|T], Certv [5] Where V is the sending vehicle, r represents the message receivers, M is the message, | is the concatenation operator, and T is the timestamp to ensure message freshness (it can be obtained from the security device).The receivers of the message will obtain the public key of V using the certificate and then verify V's signature using its certified public key. In order to do this, the receiver should have the public key of the CA [8]; this solution is cited in [2], [3], [6], and [4].

III. IMPLEMENTATION

The protocol stack depicted in Fig. 1describes how different protocols are involved in enabling include cooperative collision warning (CCW), electronic emergency brake light (EEBL), and slow/stopped vehicle alert (SVA). In general, these active safety applications require that a subject vehicle have a good estimate of the position and state of the cars in its proximity. The availability of such proximity awareness allows various safety applications to provide advisory services to the driver (via audio or visual human-machine interfaces) or perform emergency reactions to avoid hazardous situations. For this safety/tracking purpose, each vehicle is assumed to be equipped with a DSRC radio, a Global Positioning System (GPS) receiver, and onboard sensors.

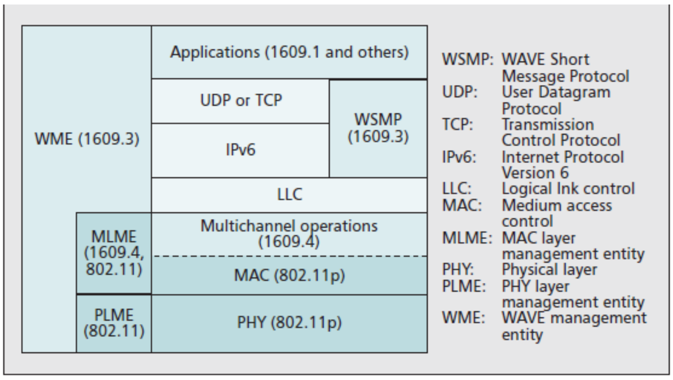

WME (1609.3)
Applications (1609.1 and others)
UDP or TCP
IPv6
WSMP (1609.3)
LLC
MLME (1609.4, 802.11)
Multichannel operations (1609.4)
MAC (802.11p)
PLME (802.11)
PHY (802.11p)
WSMP: WAVE Short Message Protocol
UDP: User Datagram Protocol
TCP: Transmission Control Protocol
IPv6: Internet Protocol Version 6
LLC: Logical lnk control
MAC: Medium access control
MLME: MAC layer management entity
PHY: Physical layer
PLME: PHY layer management entity
WME: WAVE management entity

Figure 1. *Protocol stack for WAVE, mainly composed of IEEE 802.11p [1] and IEEE 1609 family standard [2]: 1609.1 (resource manager), 1609.2 (security), 1609.3 (networking services), and 1609.4 (multichannel operations). Note that 1609.2 works jointly with 1609.3 and thus is not shown in the above architecture.*

As shown in Fig. 2, eachvehicle is designed to continuously report its own statu (e.g., position, speed, and direction) by broadcasting safety messagesin WSM format. At the same time, each vehicle alsotracks movements of neighboring vehicles based on information received from them over the shared channel. The question of how often and how far these messages should be broadcast is one that drives this research.

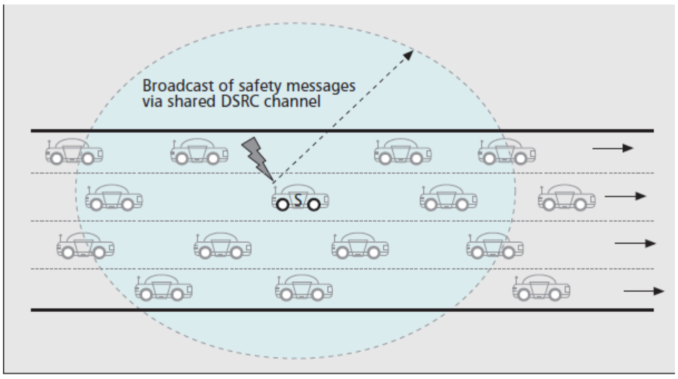


Figure 2. *To enable active safety applications, each vehicle broadcasts its own state information to neighboring vehicles via the DSRC channel.*

As shown in Fig.3, Each vehicle is designed to contain a communicationcontrol logic, a bank of estimators to track other vehicles, and a plant (producing vehicle state information). The estimated states of neighboring vehicles will be fed to active safety applications, which in turn will provide warnings to the driver or take emergency control of the vehicle in case of imminent danger. The proposed rate and power control scheme is implemented in the communication control logic.

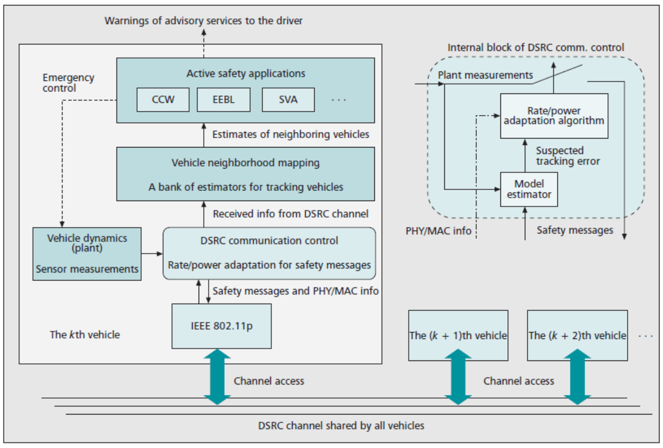

Warnings of advisory services to the driver
Emergency control
Active safety applications
CCW
EEBL
SVA
. . .
Estimates of neighboring vehicles
Vehicle neighborhood mapping
A bank of estimators for tracking vehicles
Received info from DSRC channel
Vehicle dynamics (plant)
Sensor measurements
DSRC communication control
Rate/power adaptation for safety messages
Safety messages and PHY/MAC info
IEEE 802.11p
The kth vehicle
Internal block of DSRC comm. control
Plant measurements
Rate/power adaptation algorithm
Suspected tracking error
Model estimator
PHY/MAC info
Safety messages
The (k + 1)th vehicle
The (k + 2)th vehicle
. . .
Channel access
Channel access
DSRC channel shared by all vehicles

Figure 3. *Functional blocks of the in-vehicle unit, including the DSRC communication control modoule.*

The internal architecture of the communication control logic is shown in the upper right corner of Fig. 3. Note that the produced safety messages are in WSM format, which allows specifying permessage power level for 802.11p radio.

Channel access in DSRC, especially for safety applications, is performed in a random manner, following carrier sense multiple access with collision avoidance (CSMA/CA) rules [6]with no centralized coordination. Therefore, the vehicle tracking problem is essentially a remote estimation problem over a random access channel. In this section we first state the VANET tracking problem at an abstract level.

IV. CONCLUSION

Cooperative active safety applications are among the most important services provided by ITSs. Such cooperative safety systems require that each vehicle track its neighboring vehicles in real time and detect hazardous situations. The uncontrolled transmission of state information by each vehicle is shown to produce excessive data traffic that could choke the vehicular wireless network and fail all applications. In this article we propose a joint rate-power control algorithm for broadcast of self-information that enables neighbor tracking in VANETs. We evaluated the presented solution through realistic network and microscopic traffic simulations. We also defined a statistical performance measure for tracking accuracy. To verify the robustness of the algorithm, we observed the tracking performance of the proposed algorithm that adapts transmission power and rate in different traffic scenarios. Simulation results confirm that the proposed design is robust and can considerably reduce the tracking error compared to that of the de-facto solution (beaconing at 100 ms or 500 ms intervals). Our future work includes further performance analysis, implementation of the proposed design on a DSRC radio testbed, and conducting hardware-in-the-loop evaluation.

V. REFERENCES

[1] M Raya, P Papadimitratos, JP Hubaux, "Securing Vehicular Communications", IEEE Wireless Communications, Vol 13, October 2006 .

[2] GMT Abdalla, SM Senouci "Current Trends in Vehicular Ad Hoc Networks", Proceedings of UBIROADS workshop, 2007.

[3] B. Parno and A. Perrig, "Challenges in Securing Vehicular Networks", Proc. of HotNets-IV, 2005.

[4] M Raya, J Pierre Hubaux," The security of VANETs", Proceedings of the 2nd ACM international workshop on Vehicular ad hoc networks, 2005.

[5] X Lin, R Lu, C Zhang, H Zhu, P Ho,and X Shen. "Security in Vehicular Ad Hoc Networks ", IEEE Communications Magazine, vol. 4, April 2008.

[6] Wireless Access in Vehicular Environments (WAVE) in Standard 802.11, Specific Requirements: IEEE 802.11p/D2.01, Mar. 2007.