Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 4, April 2014, pg.21 – 27

RESEARCH ARTICLE

Vehicle to Vehicle Communication using RFID along with GPS and WAP

A.Vanitha Katherine*
Dept. of computer applications
PSNACET, dindigul
avanitha@yahoo.com

R.Muthumeenakshi
Dept. of computer applications
PSNACET, dindigul
muthumeenakshi83@gmail.com

N.Vallilekha
Dept. of computer applications
PSNACET, dindigul
vallilekhapsna@gmail.com

Abstract— ***This paper studies the vehicle to vehicle communication to share safety messages The communication is one-to-many, local, and geo-significant. The vehicular communication network is ad-hoc, highly mobile, and with large numbers of contending nodes. We design several random access protocols for medium access control. The protocols fit in the facility of RFID, GPS and WAP. This can be done using DSRC.***

Keywords— ***DSRC, RFID, GPS, Protocol, geocast***

I. INTRODUCTION

A Vehicular Ad-Hoc Network or VANET is a technology that uses moving vehicles as nodes in a network to create a mobile network. The main objective of this is to turn every participating vehicle into a wireless router or node, allowing vehicles approximately 100 to 300 meters of each other to connect and, in turn, create a network with a wide range. To provide road safety measures where information about vehicle's current speed, location coordinates are passed with or without the deployment of Infrastructure. To incorporate intelligence into a VANET to improve safety. To make intelligent inferences about traffic incidents, like identifying the speed and distance covered one can predict the chances of accident. To facilitate easy and effective communication between vehicles with dynamic mobility. To provide value added services like email, audio/video sharing etc., Various communications types are Vehicle to Vehicle (V2V), Vehicle to Infrastructure (V2I), Vehicle to Roadside (V2R), Hybrid Models such as Vehicle to Vehicle (V2V) & Vehicle to Infrastructure (V2I) and Vehicle to Vehicle (V2V) & Vehicle to Roadside (V2R) . Vehicle to Vehicle communication approach is most suited for short range vehicular networks. It is Fast and Reliable and provides real time safety it does not need any roadside Infrastructure. V2V does not have the problem of Vehicle Shadowing in which a smaller vehicle is shadowed by a larger vehicle preventing it to communicate with the Roadside infrastructure. Vehicle to Infrastructure provides solution to longer-range vehicular networks. It makes use of preexisting network infrastructure such as wireless access points (Road-Side Units, RSUs). Communications between vehicles and RSUs are supported by Vehicle-to-Infrastructure (V2I) protocol and Vehicle-to-Roadside (V2R) protocol. The Roadside infrastructure involves additional installation costs. The V2I infrastructure needs to leverage on its large area coverage and needs more feature enhancements for Vehicle Applications. Thus when RFID is combined along with GPS and WAP we no need to have a separate infrastructure which is achieved with DSRC.

The rest of the paper is structured as follows. Section II provides the technological background of VANET, Section III reviews the relevant literature. Section IV is the problem formulation, V discusses the communication design and VI summarizes and concludes.

II. TECHNOLOGICAL BACKGROUND

Each vehicle in VANET equipped with WiFi/WiMax device acts as a node Unique ID and IP address for each vehicle. Each node can communicate with any other node. Any vehicle can register its identity to a roadway WAP Information provided by the vehicles directly to the WAPs. Collective information stored by the WAPs at a dynamic server database If there is a gridlock / high traffic density detected by a roadside infrastructure then the roadside system can broadcast the information to all its nodes/vehicles In turn using the DTN(Delay tolerant Network) capabilities of VANETs, the information can be transmitted to other vehicles heading towards this junction. Likewise, it can convey to the incoming vehicles other paths, depending on a centralized system co-ordination of finding non-traffic routes at that point of time. Sensor technologies (Infra-red sensing/Video and Camera Image Perception / RADAR /gyro sensor / inertial sensor), process data through mathematical algorithms to come up with a virtual understanding of the vehicle environment. In-vehicle digital maps and positioning technologies (GPS / WiFi / WiMax) as sensing systems to accurately identify the vehicle position and interpret the environment. RFID complements to the current GPS navigation system when GPS signals are not available (such as in tunnels) or if the GPS position is ambiguous to a vehicle (such as at cloverleaf intersections). But in practice, GPS does not provide sufficient information for navigation due to its low positioning accuracy (5 to 7 meters). Moreover, even combined with map-matching technologies, GPS still can not achieve lane level positioning and can not provide information regarding the traffic direction in the current lane. Nevertheless, this information is necessary to prevent vehicles from entering a wrong way when roads are under construction or lanes are temporarily borrowed by the traffic along a different direction. Radio frequency identification (RFID) is a radio based communication technique The RFID system consists of reader and tags. Both reader and tags are equipped with antenna. Data is transferred between a tag and a reader via low-power radio waves. In communication between reader and tags the most applied frequencies are the following: LF (low frequency): 125-134 kHz, HF (high frequency): 13.56 MHz, UHF (ultra high frequency): 868-956 MHz, Microwaves: 2.45 GHz. The system is capable of detecting ghost drivers even in high speed, motorway environment. The main causes of ghost-driving: suicide attempt, ignoring traffic signs, tiredness, bad weather conditions, poor visibility, intended entry, proving courage, Short cut to reduce travel time, The goal of a ghost driver system is to warn the road users as early as possible if there is a moving vehicle against them. Such rapid detection system can be supported by the RFID technology by deploying RFID readers on the roadside.

III. LITERATURE REVIEW

In ad hoc vehicular networks, TDMA, FDMA, or CDMA are difficult due the need to dynamically allocate slots, codes, or channels without centralized control. We base our designs on random access [17].

ALOHA [3] and CSMA [17] are the earliest studied random access protocols. MACA [11], MACAW [5], FAMA and its variants [9] all use the RTS/CTS scheme. Our communication is geocast. We do not use RTS/CTS.

HIPERLAN/1 [4], “Black Burst” [16], and the Enhanced Distributed Coordination Function (EDCF) of IEEE 802.11e [20] are all designed to support QoS. The HIPERLAN/1 and Black Burst approaches have no scheme to combat hidden terminals. In EDCF, when the number of contending packets of equal priority is large the probability of collision is still high. This is the case for vehicle safety communications. Reference [15] reviews the existing variants of the 802.11 DCF to support QoS. Its authors conclude that the design of a mechanism to provide predictable QoS in an 802.11 network is still an open problem. Reference [22] gives an overview of DSRC applications and assesses the characteristics of the IEEE 802.11 MAC and PHY layers in this context. It is anticipated that the current 802.11 specifications will need to be suitably altered to meet the QoS requirements of DSRC applications.

A RFID system is composed of RFID tags and RFID readers. A RFID tag stores data, and a RFID reader accesses the tag to collect the data through wireless communications. There exist two types of RFID tags: active tags, which contain power modules to support wireless communications, and passive tags, which power their transmissions through the energy absorbed from the radio waves of the RFID readers. Compared to active RFID tags, passive RFID tags are easier to maintain as they do not need power, and their cost can be as low as several cents. Therefore, passive RFID tags are more appropriate for applications that require a large number of tags. Traditionally RFID tags were designed for commercial applications to replace the bar codes for asset counting [1], [2] and identification [3]. One important challenge in such applications is how to handle the read collision problem that occurs when one or more RFID readers query multiple RFID tags roughly simultaneously in a small area. As a result, most existing research focuses on anti-collision protocol design to schedule the reader's read requests and the tag's responses [4]–[6]. In RFID-ANS, read collision is not possible as our design guarantees the one-to-one coupling of a RFID reader and a tag in a restricted area. RFID systems have been deployed for VANETs, in which RFID tags are installed on vehicles while RFID readers are deployed on stationary infrastructures. For example, in a typical Electronic Toll Collection (ETC) system [7], automatic toll RFID readers are installed at the gate. A RFID tag (attached to the E-ZPass on a vehicle) is read by the reader when a vehicle passes by the gateway. The toll system identifies the vehicle through the data obtained from the RFID tag, and automatically charges to the vehicle's or the driver's account. A similar system is established for parking fee collection in [8]. Compared to these systems, RFIDANS contains stationary tags on roads while readers move with vehicles at high speeds. The most related work to RFID-ANS are reported in [9]–[11]. Chon et al. [9] proposes the idea of using stationary RFID tags deployed on roads to localize vehicles when passing by. The feasibility of utilizing RFID tags for navigation when vehicles move at high speeds is investigated through an experiment in which a RFID reader reads the data in a tag when the tag is dropped down to the ground. Lee et al. [10] studies the relationship between the tag read latency and the vehicle's speed, and evaluates their results on a test road. These two works demonstrate the feasibility and practicality of applying commercial RFID tags and readers in the vehicular environment. But none of them considers critical issues such as tag deployment and read scheduling, which are important to the design of a practical RFID-ANS as they mainly focus on the concept and feasibility study. In the Road Beacon System proposed by [11], RFID tags serving as traffic signs are deployed in the pavement and vehicles get the road information through reading the tags. The technical details of this work are unavailable to our best knowledge.

IV. PROBLEM FORMULATION

This paper evaluates the feasibility of sending vehicle- vehicle and roadside-vehicle safety messages. These messages should be received reliably and with small delays. We define the Probability of Reception Failure (PRF) as the probability a targeted receiver fails to receive a safety message within a given time delay. The safety messages are to be sent on the control channel. The control channel also has to communicate other non-safety messages for the remaining channels to be used. Therefore the fraction of the control channel time occupied by safety messages is important as well. This is measured by channel busy time (CBT). Both PRF and CBT should be low. To evaluate feasibility we have had to make an assessment of the offered safety traffic. When the offered traffic is large, reliability, latency, and CBT deteriorate. In wired networks offered traffic is measured by the total bits/second produced by all the senders. In wireless networks the right measure of offered traffic is bit- meters/second [10], i.e., a network able to transmit a bit 100 meters, may not be able to transmit the same bit 200 meters.

Therefore the offered traffic de- pends on the safety message rate (messages/sec), size (bytes/message), message range (meters), and the density of vehicles producing these messages. Table II gives ranges for the parameters determining the offered traffic. Our evaluation is based on these ranges. A vehicle at high freeway speeds (90 mph) moves 2 meters within its lane in 50 msec. This is usually not a significant movement at high speed. Thus messages repeating faster than once every 50 msec are unlikely to provide significantly new information. On the other hand an update slower than once every 500 msec is probably too slow. Driver reaction time to stimuli like brake lights can be of the order of 0.7 seconds and higher. Thus if updates come in slower than every 500 msec, the driver may realize something is wrong before the safety system. Message sizes have been chosen to permit sender or receiver location as per the SAE J1746 standard, GPS, NTCIP hazard codes, and standard protocol headers to be included. Safety messages are usually short. Communication is more difficult at high vehicle densities. The 10 meters per vehicle represents the jammed highway. The 30 meters per vehicle represents the highway at capacity. Likewise, the 4 to 8 lane range spans the usual to large roads. Safety application designers would prefer large message ranges to smaller ones. On the other hand large message ranges make network design more difficult. The 300-meter message range corresponds to the comfortable stopping distance of a high speed car. When the road is jammed, neighbouring cars will be much closer. Therefore it should not be necessary to send safety messages over the same distance. We assume a top range of 100 meters for jammed roadways, or approximately 10 inter-vehicle distances. We have proposed a communication service able to execute at least the vehicle-vehicle communication without any roadside or base station infrastructure, i.e., an ad-hoc service. This would be good for deployment. Since 802.11a radios are designed to transmit over distances of 200 to 300 meters, i.e., the upper end of the message range in Table II, we propose a single hop, local area communications service. Reliable communication in networks has typically meant re-transmitting a message till it is acknowledged by the recipient(s). This is good for file transfers since even one missing byte may render the entire file un- usable. Thus reliable transmission protocols like TCP ensure each byte is received with certainty. For DSRC safety messages we have proposed a local area communication service that only delivers messages with high probability. This is for several reasons. We think most safety messages, like those in Table I, will be repeated by the source. For example, a broken down vehicle stopped or moving slowly in a high-speed arterial, would transmit its status, position, and speed repeatedly. This is because the set of vehicles approaching the stopped vehicle changes. If the message repeats every 100 msec and a message has still not been received 100 msec after it was created, the source will produce a new message obsolescing the old one. The communication service should also drop the old one and work on the new one. We think most safety messages have a useful lifetime. Therefore we have focused on the design of a single-hop local-area communication service delivering messages within their lifetime with high probability. The lifetime is the delay requirement. Therefore the PRF is a targeted receiver's probability of failing to receive a message within its lifetime. We think of the lifetime and probability of reception failure as the Quality of Ser- vice (QoS) requirement of the message. Our evaluation focuses on senders that generate periodic or Poisson distributed messages. If the active safety systems on the vehicle assist the driver rather than substitute for her, we think probability-ties of reception failure of 1/1000 to 1/100 per message may be adequate. In any case, most safety messages should be consumed by an estimator. For example, the warnings from the slowly moving or stopped vehicle should be consumed by an estimator of the position of the damaged vehicle relative to the receiver, conditioned on all received messages and possibly sensor information as well. Since an estimator leverages correlations in the time series of messages, it is usually robust to the loss of messages, unless the losses occur in bursts. Most safety messages produced by a vehicle are useful to many vehicles. For example, the stopped vehicle warning is useful to all approaching vehicles. Therefore we have focused on a broadcast service. In summary, we propose a service to broadcast mes- sages while meeting QoS requirements in vehicular ad- hoc local-area networks. Purpose of V2V communication enables safety and can be implemented at four roads joining areas to avoid and reduce accidents. It can be implemented at heavily traffic areas. To improve traffic safety and comfort of driving. To minimize accidents, traffic intensity, locating vehicles. To get Up-to-date traffic information. To get intersection collision warning, local danger warning, weather information and to detecting vehicles traveling against traffic direction.

V. COMMUNICATION DESIGN

In a wireless ad-hoc network there are two obstacles to the reliable reception of messages. If two transmitters within the interference range of a same receiver transmit concurrently, their transmissions collide at the receiver. The receiver does not receive either message. To combat this problem one designs a Medium Access Control (MAC) protocol, i.e., a set of rules by which a radio decides when to transmit its messages and when to keep silent. Secondly, even if there is no collision, the wireless channel may attenuate the transmitted power so much that it is swamped by thermal noise. This is combated by selecting the transmission energy to be high enough to reach all receivers within the message range with high probability, when there are no collisions. Transmission energy is determined by transmission power, modulation, and error coding. DSRC radios are to be based on the 802.11a radio. set the transmission energy control parameters to model the 802.11a radio transmitting over a 20 MHz channel at 5.4 GHz and focus on the MAC design problem, i.e., is there a MAC able to deliver safety messages with sufficiently high reliability and small delays? The stochastic modelling of the wireless vehicle-to-vehicle communication channel is an open problem. We use the deterministic Friis Free-space model for short distances and the Two-ray model for longer distances [13], i.e., if the distance between the transmitter and receiver antennas is d, then the power of the signal decreases as d2 when the distance is short and d4 when the distance is large. In unicast communication reliability is enhanced by policies based on receiver feedback, e.g. RTS/CTS, TCP, or WTP. These require the sender to learn the identity of its receiver(s). When there are many receivers or the network is highly mobile, meaning the set of receivers can change a lot, learning identities may itself require significant communication. Therefore we have chosen to evaluate ways to enhance reliability without receiver feedback. The following is the communication architecture of the safety applications

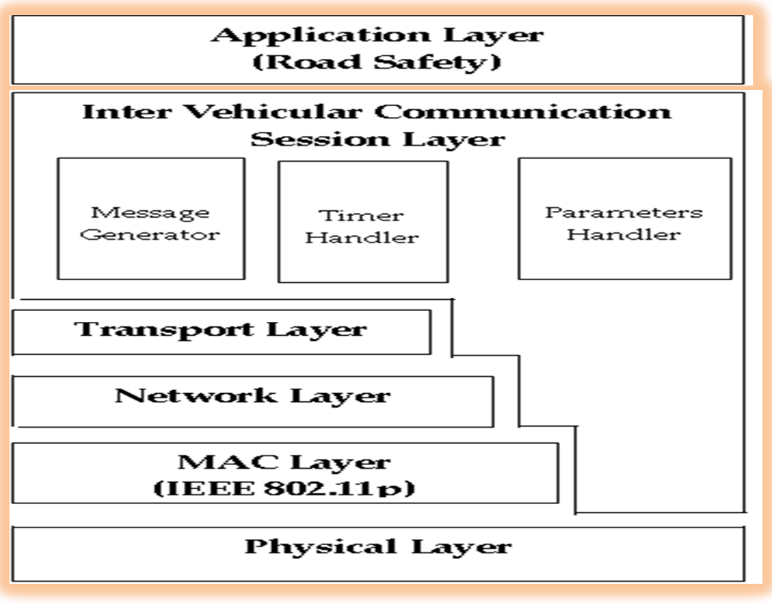

Fig 1: Communication Architecture

The Application characteristics are as follows

Table 1: Application Characteristics

S.No	Application Characteristics	Description
1	User benefit of Application	Safety
2	Participants of Application	Vehicle to Vehicle
3	Application region of Interest (ROI)	Medium region
4	Recipient Pattern of Application Message	One to zone
5	Application trigger condition	Periodic
6	Event Lifetime	Long
7	Event correlation	None
8	Event Detector	One

The network attribute characterization is also as follows.

Table 2: Network attributes

S.No	Network Attributes	Description
1	Channel Frequency	DSRC – CCH
2	Infrastructure	No
3	Message time-to-live	Multi hop
4	Packet format	WSMP
5	Routing protocol initiative mode	Geocast
6	Network Triggered	Event triggered
7	Transport Protocol	Connectionless
8	Security	V2V security

The following figure shows the DSRC radio implementation

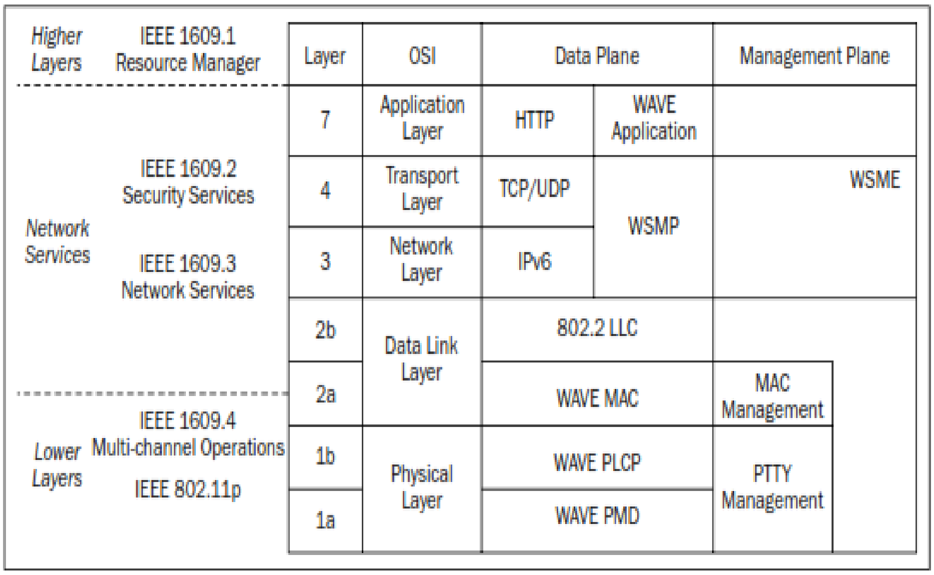

Fig 2: DSRC Radio implementation

DSRC / WAVE is used for communication which includes IEEE 802.11P+IEEE 1609.(1-4) IEEE 802.11P, IEEE 802.11a PHY: OFDM Modulation, IEEE 802.11 MAC: CSMA/CA, IEEE 802. MAC enhancement: message prioritization. Data rate: 3-27 Mbps Modulation: OFDM OFDM Symbol Duration: 8.0µs Guard period: 1.6 µs Occupied Bandwidth: 10MHz Frequency:

5.8 – 5.9 GHz. In the above specified standards IEEE 1609.1 – Defines the resource manager that should allow multipath applications run on the VANET devices. IEEE 1609.2 – Defines security service for V2X. IEEE 1609.3 – Specifies networking service for V2X. IEEE 1609.4 – For multi channel operations.

VI. CONCLUSIONS & DISCUSSION

VANET is the networking infrastructure for supporting vehicular applications. It is more suitable for delivering content in vehicular communications. The RFID system can be found a wide range of logistics applications. The system has the advantage of fast data collection and reporting, which obviously works only with vehicles equipped by RFID tags. Assumingly, in the near future all vehicles will carry such tags that can also replace the license plates or car registration cards. Since the RFID technology is standardized, it can be used all over the world. Deploying multiple readers in a carefully planned constellation in a traffic junction, the radio frequency identification is suitable for special task.

REFERENCES

1. Dedicated Short Range Communications (DSRC) home. http://www.leearmstrong.com/dsrc/dsrchomeset.htm
2. The network simulator: NS-2. http://www.isi.edu/nsnam/ns.
3. N. Abramson. The throughput of packet broadcasting channels. *IEEE Trans. Comm.*, COM-25:117–128, January 1977.
4. G. Anastasi, L. Lanzini, and E. Mingozzi. HIPERLAN/1 MAC protocol: stability and performance analysis. *IEEE Journal on Selected Areas in Communications*, 18(9):1787– 1798, September 2000.
5. V. Bharghavan, A. Demers, S. Shanker, and L. Zhang. MACAW: A media access protocol for wireless LANs. *ACM SIGCOMM'94*, pages 212–225, August 1994.
6. B. Cash. IEEE briefing on 5.9 GHz concepts and band plan. Presentation in DSRC standardization monthly meeting, 2002.
7. Federal Communications Commission. FCC 99-305. FCC Report and Order, October 1999.
8. Federal Communications Commission. FCC 03-024. FCC Report and Order, Feburary 2004.
9. J. Garcia-Luna-Aceves and C. Fullmer. Floor aquisition multi- ple access (FAM A) in single channel wireless networks. *ACM Mobile networks and applications*, 4:157–174, 1999.
10. P. Gupta and P. Kumar. The capacity of wireless networks. *IEEE Transactions on Information Theory*, IT-46(2):388– 04, March 2000.
11. P. Karn. MACA-a new channel access method for packet radio. *ARRL/CRRL Amateur Radio 9th Computer Networking Conference*, pages 134–140, 1990.
12. H. Krishnan and C. Kellum. Use of communication in vehicle safety application. Internal Report of General Motors Company, 2002.
13. W. C. Y. Lee. *Mobile Communications Design Fundamentals*.John Wiley & Sons, 2 edition, 1993.
14. California PATH. Shift: The hybrid system simulation programming language. http://www.path.berkeley.edu/shift/
15. W. Pattra-Atikom, P. Krishnamurthy, and S. Banerjee. Dis- tributed mechanisms for quality of service in wireless LAN. *IEEE Wireless Communications*, pages 26–34, June 2003.
16. J. Sobrinho and A. Krishnakumar. Quality-of-service in ad hoc carrier sense multiple access wireless networks. *IEEE Journal on Selected Areas in Communications*, 17(8):1353–1368, August 1999.
17. F. Tobagi and L. Kleinrock. Packet switching in radio chan- nels: Part I- carrier sense multiple-access modes and their throughput/delay characteristics. *IEEE Trans. Comm.*, COM-23(12):1400–1416, December 1975.
18. J. VanderWerf, N. Kourjanskaia, S. Shladover, H. Krishnan, and M. Miller. Modeling the effects of driver control assistance systems on traffic. *National Research Council Transportation Research Board 80th Annual Meeting*, January 2001.
19. J. Walrand and P. Varaiya. *High-performance Communications Networks*. Morgan Kaufmann, 2 edition, 2000.
20. Y. Xiao. Enhanced DCF of IEEE 802.11e to support Qos. *Proceedings of IEEE WCNC*, pages 1291–1296, 2003.
21. Q. Xu, T. Mak, J. Ko, R. Sengupta, and D. Jiang. Ad hoc medium access control protocol design and analysis for vehicle safety communications. In preparation, 2004.
22. J. Zhu and S. Roy. MAC for Dedicated Short Range Communications in Intelligent Transportation System. *IEEE Communications Magazine*, pages 60–67, December 2003.

