International Journal of Science and Research (IJSR)
ISSN: 2319-7064
Impact Factor (2018): 7.426

Study of Vehicular AD-HOC Network in Cognitive Radio

Punitha A[1], Raghupathi S[2]

[1]Department of Electronics and Communication Engineering, M.N.M Jain Engineering College, Chennai, India

[2]Department of Electrical Engineering, IBRI College of technology, Oman

Abstract: ***Vehicular Ad-hoc Network (VANET) is a network in which vehicles can communicate with each other using the help of the road side equipment within the network. There are numerous applications using VANET and hence it has emerged as an important technology in the automobile industry. VANET is widely used in providing the real time traffic information to the vehicle users, offering notification related to the post-crash, street hassle handling, and traffic vigilance ability, and hence it is in good demand. But, VANETs are prone to several threats like reduced tolerance for error, very high mobility, etc. and high rate of attacks like eavesdropping, impersonating, session hijacking due to its security related challenges on the vehicular network. And also another great challenge is high road density where communication traffic is very high. To overcome this challenge especially we go for an emerging technology called cognitive radio. So, in this paper we discuss about cognitive radio channels and their bandwidth to overcome high density issue.***

Keywords: VANET, V-2-V & V-2-R communication, ITS, DSR, AODV, GPRS

1. Introduction

1.1 VANET

VANET is a promising technology that employs wireless communication networks to facilitate vehicles to communicate with one another, and with a fixed infrastructure such as *Road Side Units* (RSU) [1]. VANETs have attracted a lot of attentions due to their interesting and promising functionalities including vehicular safety, traffic congestion avoidance, and location based services [2]. Vehicle-to-vehicle and vehicle-to infrastructure communications improve vehicle's perception from the surrounding environment [4].

Intelligent vehicle is evolving with various types of services to provide convenience of life by integrating with home network, telemetric, and intelligent robot, thanks to development of convergence technology [3]. Smart vehicles have embedded computers, Global Positioning System (GPS), short-range wireless network interfaces, and potentially wireless access to the internet. With these equipments, vehicles can communicate with each other *(V2V: Vehicle-to-Vehicle)* or with RSU which are connected to the internet *(V2I: Vehicle-to-Infrastructure)* [6].

1.2 Characteristics Of VANET

- The nodes in the VANET have high mobility where their nodes move at very high speed to reach the destination node.
- The position of nodes changes frequently the network topology able to change their positions often.
- They have unbounded capacity so that they can connect many cities large in number.
- The VANET is specially designed for wireless communication so they connect with the other nodes so that they exchange information but one issue here is security can be handled by time limit.
- The VANET provides sufficient power that is another high advantage in VANET.

1.3 Issues in VANET

VANETs face a lot of issues due to its features like rapidly changing network topology, unbounded network size, High Mobility, etc. Some of the challenges faced are network management, congestion and collision control, environmental impact, MAC Design, security, data consistency liability, and key distribution. VANETs are also subjected to various attacks such as Impersonate, Session hijacking, Identity revealing, Location Tracking, Repudiation, Eavesdropping, Denial of Service, Routing attacks like Black Hole attack, Worm Hole attack and Gray Hole attack [8]. Hence, authentication is very important in VANET to maintain security and privacy.

1.4 Routing Protocols in VANET

The characteristic of highly dynamic topology has a challenge in order to make the design of efficient routing protocols for VANET. The VANET routing protocol is classified into two types such as Topology based routing protocols & Position based routing protocols. Topology based routing protocols use link's information in order to send the data packets from source to destination, whereas Position based routing protocols uses geographic position information in the network. Topology based routing protocols can be further categorized into proactive (table-driven) and reactive (on-demand) routing.

1.4.1 Proactive (Table-Driven) Routing

Proactive routing protocols are mostly based on shortest path algorithms in the network. They keep all the updated information of all connected nodes in the form of tables because these protocols are table based. Furthermore, these tables are also shared with their neighbors for its routing in the network. Every node updates its routing table according to the changes occurs in network topology. The one type of proactive routing protocol is discussed below.

FSR

Fisheye State Routing (FSR) is an efficient link state routing that maintains a topology map at each node and propagates link state updates with only immediate neighbors not the entire network. Furthermore, the link state information is broadcast in different frequencies for different entries depending on their hop distance to the current node. Entries that are further away broadcast with lower frequency than ones that are closer. The reduction in broadcast overhead in the network is traded for the imprecision in routing. However, the imprecision gets corrected automatically as packets approach progressively closer to the destination.

1.4.2 Reactive (On Demand) Routing

Reactive routing protocol is also called as on demand routing protocol because it starts route discovery when a node needs to communicate with another node and hence it reduces network traffic. The different types of reactive routing protocols are given below.

a) AODV

In *Ad Hoc On Demand Distance Vector* (AODV) routing, upon receipt of a broadcast query (RREQ), nodes record the address of the node sending the query in their routing table. This procedure of recording its previous hop is called backward learning. Upon arriving at the destination, a reply packet (RREP) is then sent through the complete path obtained from backward learning to the source.

b) DSR

Dynamic Source Routing (DSR) uses source routing, that is, the source indicates in a data packet's the sequence of intermediate nodes on the routing path. In DSR, the query packet copies in its header the IDs of the intermediate nodes that it has traversed. The Destination then retrieves the entire path from the query packet and uses it to respond to the source. As a result, the source can establish a path to the destination.

c) TORA

Temporally Ordered Routing Algorithm (TORA) (Park, 2007) routing belongs to a family of link reversal routing algorithms in the network where a *Directed Acyclic Graph* (DAG) toward the destination is built based on the height of the tree rooted at the source. The DAG directs the flow of packets and ensures reach ability to all nodes.

2. Related Works

K. Priya [1] et al has proposed a Secure Privacy and Distributed Group Authentication Protocol (GAP) for VANET. This GAP protocol is designed for VANET to endow with security services such as authentication, traceability and anonymity preservation. Group signature and batch verification of the protocol significantly reduce the message delay when compared with its counterparts. Multiple RSUs in the case of a high node density help for successful delivery of certificates. The proposed protocol also scales well when the number of messages have increased and improves the service rate. For future work, the protocol can be tested with different batch verification time slots and can also be tested using a roadway traffic simulation such as MOBISIM tool.

Yong Hao [2] et al has proposed a distributed key management framework with cooperative message authentication in VANETs. In this paper, a novel distributed key management scheme based on the short group signature to provision privacy in the VANETs is proposed. The distributed key management is further enhanced with a cooperative message authentication protocol to alleviate the heavy computation overhead. The challenging issue that semi-trust RSUs may be compromised, and compromised RSUs may even collude with malicious vehicles is investigated. A security protocol to prevent compromised RSUs and malicious vehicles from attacking is designed. The proposed method guarantees that RSUs distribute keys fairly to the neighbors and provide some mechanisms in order to detect compromised RSUs and malicious vehicles.

Xiaoling Zhu [4] et al has proposed a Distributed Pseudonym Management Scheme in VANETs. In this paper, a secure and efficient pseudonym management scheme for vehicular ad hoc networks is proposed. The scheme not only maintains the property of conditional privacy preservation but also provides the advantages in security against authority forge attacks and better robustness. In the scheme, a pseudonym is coproduced by *V* and PCA to avoid the deception of either party. A blind signature method is used to achieve the separation of issuance and tracking. Based on the improved share generation scheme of the RSA keys, the distributed tracking protocol is proposed to avoid a single point of failure. By searching for the optimal number of messages with a pseudonym certificate, the efficient pseudonym authentication mechanism is given to reduce communication overhead. By uniting the pseudonym issuance protocol and the tracking protocol, malicious vehicles are revoked easily. The communication cost and computation cost in our scheme are lower. As a result, our proposed scheme is suitable for anonymous communication with tracking requirements in VANETs, since it provides security, robustness, and efficiency.

Michael Feiri [5] et al has presented a technique that performs pre-distribution of certificates for pseudonymous broadcast authentication in VANET. In this paper, a new technique that combines certificate omission and certificate pre-distribution is proposed. This technique significantly reduces cryptographic packet loss caused by pseudonym changes while driving. Moreover, the introduction of certificate pre-distribution is possible without requiring deep changes to existing architectures for certificate management in vehicular communication.

3. CR-VANET

Currently, high-speed trendy vehicles and an outsized variety of cars go on the road on a daily basis. They aim to develop advanced applications for improving safety and efficiency of road infrastructure and transportation. This will modify users to utilize transport networks during a smarter and safer method. Presently, the first objective of car trade is to boost the traveling expertise of users by enhancing transport communication capabilities with higher safety and potency, additionally as web access and infotainment applications.

The number of vehicles on road is always increasing as well as the demand for inter-vehicle communications. However, ITS [11] and vehicle communications need to overcome several technical challenges. Protocols and applications designed for transport communications ought to contemplate varied vital factors like communication infrastructure, road infrastructure, vehicle density, user demands and types of vehicular networks, as well as available wireless spectrum. Many visualized applications can would like uninterrupted and reliable property and this will be difficult in high-speed transport eventualities. New protocols area unit required that may alter speedily dynamical surroundings and area unit fault tolerant particularly for applications associated with safety. Overall needs for such applications area unit QOS support, ability to quick dynamical surroundings, robustness, and additional bandwidth to deal with congestion and high bandwidth requirements of some applications such as video streaming.

We argue that the psychological feature radio technology will facilitate in respondent some needs, and also the motivations resulting in CR-VANETs area unit provided within the remaining a part of this section.

3.1 QOS Requirements

Quality Of Service (QOS) support is very important for applications like associated with safety. From the purpose of read of radio technology, satisfying QOS guarantees is easier when there is enough bandwidth, which can be traded with QOS guarantees such as low delay or high reliability. Additionally, there ought to be mechanisms to safeguard vital flows from lower priority flows. We discuss the problems associated with information measure and flow priority within the following text.

3.1.1Bandwidth Scarcity and Congestion

Wireless communication is well-liked as ever and also the demand for additional information measure and spectrum is ever increasing. In addition, applications like video streaming are getting well-liked, which, in turn, consume high bandwidth and can cause congestion. Similar issues of information measure insufficiency and congestion can impact transport communications with growing demands. Recently, several automotive manufactures have began to give property options in their cars facultative net property through cellular networks (that give mobile voice and information connections) and alternative wireless access technologies for accessing various applications. However, the performance of cellular networks suffers in urban areas (large cities) because of congestion of cellular spectrum whereas in rural areas, cellular coverage is either absent or low. Moreover, as mentioned previously, for dedicated communication, ITS are based on IEEE 802.11p, which is based on an old version of Wi-Fi, namely, IEEE 802.11a, and thus, it has limited capacity. Presently, there is a lack of applications for inter vehicle communications, which will change in the future. Car manufacturers look unlikely to buy spectrum. Additionally, note that spectrum could be a scarce natural resources and may be used expeditiously. Thus, opportunistic spectrum access is an attractive solution.

3.1.2 Offloading Lower Priority Flows

Many applications area unit visualized for VANETs like motion picture. Some of these video applications, as an example, Peer-to-Peer (P2P) video sharing and transmission advertisements will consume plenty of information measure and might cause collision with different flows. One idea is to use the main 802.11p spectrum for important flows and use additional bandwidth available with cognitive radio, opportunistic spectrum for lower priority video flows, and P2P traffic.

3.2Resiliency

The flexibility and gracefulness offered by psychological feature radio is extremely helpful for resilient communications in conveyance situations. In case of emergency things, CR can be reconfigured in real time to operate in emergency mode by focusing on minimizing Bit Error Rate (BER) and avoiding interference. This property is extremely helpful for ITS safety applications, and with CR functionalities, some objectives like bandwidth maximization or power minimization can be flexibly traded for more resiliency.

3.3 More Spectrum Holes On Highway

In several cases, highways are open spaces and there is a high chance of finding a spectrum hole that can be accessed opportunistically. This is in contrast to downtown and concrete areas wherever probabilities of finding spectrum holes will be low because of high population. In fact, some experiments have been done which show free abundant spectrum available for opportunistic use on highways. Thus, psychological feature radio technology is extremely engaging because it will exploit such spectrum availableness mistreatment expedient spectrum access. This, in turn, will answer a number of the information measure and congestion issues mentioned on top of.

3.4 Sufficient Space and Power Supply in Vehicles

Some of the advanced psychological feature radio capabilities come back at a value in terms of larger size of aboard units. Some functionality can also consume energy. However, vehicles have comfortable house and power provide and aren't restricted by them in contrast to the case with good phones and alternative extremely moveable devices. Cost will still be an element, but performance vs. cost trade-off can be exploited. Cost may also be reduced with the assistance of production, by optimally designing an OBU with cognitive radio capabilities.

3.5 Reprogrammable Vehicular Telematics

Every 2 to 3 years, a new communication standard is being proposed, such as DVB-H, DVB-T2, WiMaX, 802.11p, LTE, and HSDPA. Some of these standards face the chance of turning into an advert failure like was the case with DVB-H. Moreover, totally different countries have different laws associated with spectrum usages, transmit power limits, etc. Thus, international makers of vehicles face a quandary on that technology to deploy and the way to deploy completely different versions of communication units for various

countries. A vehicle includes a life cycle of quite fifteen years, and onboard communicating devices should not become obsolete during that period. Moreover, the drivers as well as passengers would like to use the newer technologies that come out in the future.

Cognitive radio combined with SDR offers an answer to deal with evolving and diverse technologies. Reconfigurable and reprogrammable capabilities of atomic number 24 and SDR give the chances to style 'future proof' aboard units that ar upgradeable with software system updates. This permits flexibility in deploying completely different versions of units for various countries and allows upgradeability once new technologies commence in future.

3.6 Highly Mobile Environment

Deploying base stations to supply wireless services (e.g., Internet access) in vehicular networks is challenging due to the highly mobile environment. VANETs ar thought-about as a special case of Mobile unintentional Networks (MANETs) because of their specific characteristics like special quality pattern, variable vehicle density, and interference with other types of networks. Several applications of VANETs are projected that take under consideration the preceding constraints of conveyance communication. As represented before, different communication technologies have been standardized (WAVE, IEEE 802.11p, etc.) for vehicular communications. However, presently, the preparation and performance analysis of the projected standards, particularly in a very large-scale conveyance surroundings, are works in progress. Moreover, completely different standards and protocols projected for conveyance communication applications ought to be practical. Additionally, short-range communication protocols might not be able to give sensible net property for high-speed vehicles which would need developing new economical protocols appropriate for them.

4. Recent Advances in CR-VANET

Cognitive radio technology [11] presents a promising solution for addressing the problem of spectrum scarcity. Vehicle communication could have the benefit of psychological feature radio technologies like dynamic spectrum access, adaptive software-defined radios. CR-enabled VANETs will use extra spectrum opportunities in TV bands in line with the QOS requests of the applications.

Existing works on CR focus on various issues that include investigating techniques for spectrum sensing and spectrum access (dynamic spectrum access), cooperative communications, MAC protocols, routing protocols, QOS, and software-defined radios. While many studies exist in literature on applying atomic number 24 to wireless mesh networks, ad hoc networks, and cellular networks, the research on applying CR to VANETs is still in its early stage. The research solutions proposed for general-purpose CR networks cannot be directly applied to CR-VANETs as the unique features of vehicular environment, such as the role of mobility, and the cooperation opportunities got to be taken under consideration whereas coming up with the spectrum management functions for CR-VANETs. Thus, the present solutions got to be customized for CR-VANETs to account for prime quality, dynamic topologies, frequent disconnections, etc. Unlike static atomic number 24 eventualities, in CR-VANETs, multiple cooperating vehicles (during busy hours) can exchange spectrum information to get information on the spectrum availability. Moreover, this permits reconciling operations and proactive response possible for the vehicles that follow.

5. Conclusion

VANET is used for intellectual transport system for the drivers the ad-hoc network is used to transmit various types of message over the network. For safety message to be transmitted for the security reasons on the vehicle and road transportation various routing protocols. The VANET is used for mainly V2V and V2R purposes. V2V is vehicle to vehicle communications and V2R is vehicle to roadside communication. In varied eventualities message transmission is finished in line with vehicle density on the market on the road. The main issue of road density is due to high load on road message communication get overhead due to less amount of network bandwidth to overcome this issue cognitive radio bandwidth can be utilize for data transmission by channel.

References

[1] Brijesh Kumar Chaurasia and ShekharVerma, "Infrastructure based Authentication in VANETs", International Journal of Multimedia and Ubiquitous Engineering Vol. 6, No. 2, April 2011.
[2] Huaqun Wang and Yuqing Zhang, "On the Security of an Anonymous Batch Authenticated and Key Agreement Scheme for Value-Added Services in VANETs", International Workshop on Information and Electronics Engineering (IWIEE), 2012.
[3] Kamal Deep Singh, PriyankaRawat and Jean-Marie Bonnin" Cognitive radio for vehicular ad hoc networks (CR-VANETs) approaches and challenges", EURASIP Journal on Wireless Communications and Networking,Vol.15,No.4, June 2014.
[4] Khalid Haseeb, Dr.Muhammad Arshad, Dr.ShaziaYasin, and Naveed Abbas, "A Survey of VANET's Authentication", ISBN: 978-1-902560-24-3 © 2010 PGNet.
[5] Michael Feiri, Rolf Pielagey, Jonathan Petitx, Nicola Zannoney, and Frank Karglz, "Pre-distribution of certificates for pseudonymous broadcast authentication in VANET", IEEE Vehichular Technology Conference,2015.
[6] Network Simulator: http:///www.isi.edu/nsnam/ns.
[7] Priya K and KomathyKaruppanan, "Secure Privacy and Distributed Group Authentication for VANET", IEEE-International Conference on Recent Trends in Information Technology,
[8] Ram Shringar Raw, Manish Kumar, and Nanhay Singh, "Security Challenges, issues and their solutions for VANET", International Journal of Network Security & Its Applications (IJNSA), Vol.5, No.5, September 2013.
[9] Xiaoling Zhu, Yang Lu, Benhong Zhang, and ZhengfengHou, "A Distributed Pseudonym Management Scheme in VANETs", International

Journal of Distributed Sensor Networks, Vol.7,No.1, July 2013.
[10] You-Boo Jeon, Keun-Ho Lee, Doo-Soon Park, and Chang-Sung Jeong, "An Efficient Cluster Authentication Scheme Based on VANET Environment in M2M Application", International Journal of Distributed Sensor Networks, Vol.6, No.3, Nov 2016.
[11] Yong Hao, Yu Cheng, Chi Zhou and Wei Song,"A Distributed Key Management Framework with Cooperative Message Authentication in VANETs", IEEE Journal on selected areas in Communications, Vol. 29, No. 3, March 2011.

Author Profile

Punitha A working as ***Associate Professor*** in the *Department of Electronics and Communication Engineering* at *M.N.M Jain Engineering College, Chennai.* She acquired B.E. Degree in Electronics and Communication Engineering from Trichy Engineering College, Trichy in 2002. She obtained M.E. Degree in Communication Systems from Hindustan College of Engineering, Chennai, in 2009 and Ph.D degree from Anna University, Chennai. She has over 15 years of experience in teaching and guiding projects. Her areas of interest include Mobile Ad hoc Networks, Wireless Sensor Networks, Digital Communication, Optical Communication and Network Security.

Raghupathi S working as ***Lecturer*** in the *Department of Electrical Engineering* at *IBRI College of technology*, Oman. He acquired B.E. Degree in Electronics and Communication Engineering from Trichy Engineering College, Trichy in 2002. He obtained M.E. Degree in VLSI Design from SASTRA University in 2006. He has over 15 years of experience in teaching and guiding projects. His areas of interest include Mobile Ad hoc Networks, Wireless Sensor Networks, VLSI Design and Network Security.