International Journal On Engineering Technology and Sciences – IJETS™
ISSN(P): 2349-3968, ISSN (O): 2349-3976
Volume IV, Issue II, February - 2017

Hybrid Data Transmission Framework with Prediction based Channel Assignment under Cognitive Radio based Vehicular Ad-Hoc Network

Ms. S. Jeevitha, M.Phil (Research Scholar),
Mr. S.SAMPATH, M.C.A., M.Phil., Associate Professor,
Department of Computer Science & Applications,
P.K.R. Arts College for Women,
Gobichettipalayam, Tamilnadu, India

Abstract

The Cognitive Radio based Vehicular Ad-Hoc Network (CR-VANET) is constructed to support the data communication over the vehicles. The data transmission and receive operations are managed with cognitive radio devices. The Road Side Infrastructure (RSI) or Access Points (AP) is deployed to transmit the data values. Data provider manages the shred data values. Unicast, multicast and broadcast data communication operations are supported by the CR-VANET environment.

Routing protocols are building to derive the rules for the data communication operations. The broadcast data transmission operations are carried out with the Robust and Fast Forwarding (ROFF) protocol. The Trajectory based Multicast (TMC) protocol is adapted to support the multicast data communication among the vehicles. The forwarder nodes are selected with Empty Space Distribution (ESD) bitmaps and Message Forwarding Metrics (MFM) measures. The bandwidth ranges are refereed as spectrum. The data communication tasks are carried out with allocated bandwidth levels.

The hybrid data communication framework is build to perform the multicast and broadcast data transmission tasks. The Secure Hybrid Routing Protocol (SHRP) integrates the ROFF and TMC protocol features with security solutions. Data replication methods are also integrated with the data communication model. The historical spectrum sensing data values are analyzed with data mining methods to perform channel assignment operations. The Dirichlet Process (DP) and Hidden Markov Model (HMM) methods are employed for the spatio temporal correlation based channel allocation process. Service channels are assigned with unlicensed frequencies and licensed frequencies are allocated for the emergency conditions. The transmission delay is controlled with high throughput and detection probability rate levels.

Index Terms : Cognitive Radio, Vehicular Ad-Hoc Networks, Channel Assignment, Secure Hybrid Routing Protocol and Data Security

1. Introduction

The topology of VANET changes because of the movement of vehicles at high speed. Suppose two vehicles are moving at the speed of 20m/sec and the radio range between them is 160 m. Then the link between the two vehicles will last 160/20 = 8 sec. From the highly dynamic topology results frequent disconnection occur between two vehicles when they are exchanging information. This disconnection will occur most in sparse network. The mobility pattern of vehicles depends on traffic environment, roads structure, the speed of vehicles, driver's driving behavior and so on**.** The communication environment between vehicles is different in sparse network & dense network. In dense network building, trees & other objects behave as obstacles and in sparse network like high-way this things are absent. So the routing approach of sparse & dense network will be different.

VANETs can improve traffic safety only if the messages sent by vehicles are trustworthy. Dealing with fraudulent messages is a thorny issue for safety engineers due to the self-organized operation of VANETs. The situation is further deteriorated by the privacy requirements of vehicles since, in a privacy preserving setting, the message generators, i.e. the vehicles, is anonymous and cannot be identified when performing maliciously. A number of schemes have been applied to reduce fraudulent messages; such proposals fall into two classes, namely a posteriori and a priori.

2. Related Work

VANETs enable traffic information sharing for intelligent transportation systems. To improve dissemination efficiency, Gao et al. proposed an adaptive query evaluation plan by taking into account the road topology. Also, Loulloudes et al. presented in [2] V-Radar, an efficient protocol for traffic information retrieval using V2V communications. Several works have sought inspiration in Biology and Internet protocols communication [3]. Since they employ vehicle ad hoc networking, the above approaches have only a partial view of the traffic conditions, which may lead to less accurate re-routing. Simply treating

vehicles as packets which always listen to the guidance ignores the nature of human behavior. Furthermore, these systems react to real-time data without insight into future conditions, thus introducing greater vulnerability to switching congestion from one spot to another.

A large body of works considers the problem of preserving the user's privacy in the context of location based services (LBSs). For instance, the middle layer of DSRC defines the security services for application and message management [1]. Authentication schemes are designed to preserve the driver privacy in DSRC-based VANETs [4]. To prevent malicious tracking, a vehicle could change its anonymous key within an interval of a few minutes [8]. DIVERT has a different goal from all these works: it focuses on protecting the driver's location privacy from the central server, not from the other drivers in VANET. For driver-to-driver privacy, DIVERT can leverage the solutions.

SCMS [7] provides privacy protection from both outsiders and insiders. DIVERT is complementary to SCMS, as its goal is to minimize the amount of privacy sensitive information uploaded to the server, not to protect the information privacy once it has been uploaded. Furthermore, SCMS relies on the organizational separation assumption to protect against insider attacks. DIVERT, achieves a good level of location privacy protection even if this assumption does not hold.

Many works focus on spatial cloaking [6] to provide k-anonymity. The work argues that both spatial and temporal dimensions should be considered in the algorithm to achieve better k-anonymity. Fundamentally, k-anonymity reduces the quality of the user's localization, which is not applicable for continuous location based services realtime vehicle re-routing. A number of mechanisms provide solutions for highly accurate real-time location updates, while achieving good privacy protection. These mechanisms require a trusted centralized entity a proxy server for location reporting. Our privacy aware mechanism works in a distributed and probabilistic fashion without any help from trusted entities. The risk of location tracking is distributed over VANETs, and we argue that this is qualitatively better than trusting a single central entity.

3. Data Dissemination under VANET

A lot of safety applications over vehicular ad-hoc networks (VANET) rely on emergency message dissemination (EMD) through multi-hop broadcast. In EMD, a certain vehicle issues an emergency message when a dangerous situation such as vehicle collision has been detected. Since the emergency message includes time-sensitive life-critical information, it should be disseminated to all vehicles in the target region as quickly and reliably as possible. Commonly, the target region is a road segment that is up to several kilometers long in the opposite direction of the source. Since the one-hop communication range of a source cannot cover the target region fully, multi-hop broadcasting should be used to disseminate the emergency message.

Many broadcast schemes have been applied to meet the requirements on the timeliness and reliability of EMD. The reliability can be improved by retransmitting the original copy of the emergency message or removing interference from hidden nodes. Retransmissions and control messages exchanged for the interference avoidance increase the latency of the message dissemination. Apart from reliability issues, for fast message dissemination, the vehicle farthest from a forwarder in the message dissemination direction should be designated as a next forwarder. Since the farthest vehicle can fail to successfully receive the message due to an inherently lossy wireless channel, the explicit designation of the farthest vehicle as the next forwarder may cause the multi-hop forwarding to be suspended. In most forwarding mechanisms, vehicles have received the broadcast message and are farther away from the previous forwarder contend to become a new forwarder in a distributed manner. Eventually, the farthest forwarder candidate (FFC) from a forwarder is opportunistically selected. Since retransmissions can help to increase the reliability of dissemination, each of contentions for transmission completed as quickly as possible in order to minimize the latency of the overall dissemination process. Note that achieving conflicting both goals simultaneously.

The common idea behind forwarding mechanisms is to differentiate each waiting time (WT) of forwarder candidates. The waiting time ranges from 0 to the predefined upper bound (PUB). A forwarder candidate selects a point in the time range and uses it as the waiting time. In particular, in order to maximize the hop progress of the message each forwarder candidate uses its waiting time that is inversely proportional to the distance from itself to the previous forwarder. The farthest forwarder candidate uses the shortest waiting time and then forwards the message first.

The other forwarder candidates detect the transmission from the newly selected forwarder and suppress their scheduled transmissions.

Two fast forwarding schemes are considered for the data dissemination process. First, schemes tacitly assume the perfect suppression of redundant transmissions, means that all forwarder candidates can successfully receive the message from FFC within their waiting times. Due to the short difference between waiting times of forwarder candidates, some forwarder candidates may start their transmissions before detecting the transmission from FFC and such redundant transmissions can collide with the transmission from FFC. The waiting time difference between two forwarder candidates is affected by PUB and the difference between distances from the previous forwarder to the forwarder candidates. The distance difference depends on the spatial vehicle distribution. In addition, under a given distribution of vehicles, a smaller PUB allows the next forwarder to be selected earlier, but results in a higher probability of collisions caused by the short waiting time difference. The schemes simply regard PUB as a system parameter without considering the relationship between the selected PUB and collision probability (CP) under dynamically changing vehicle distributions. Second, the vehicle distribution is not uniform and continuously changing due to dynamic VANET traffic conditions. Various scales of empty space with no vehicle can be present between vehicles. Two vehicles separated by a large empty space, one closer to the previous forwarder should delay its forwarding necessarily for a long time even though there exists no vehicles farther than itself when it becomes FFC.

RObust and Fast Forwarding scheme (ROFF) is applied as a solution to collision and latency-related problems mentioned above. Given two adjacent forwarder candidates A and B where A is farther from the previous forwarder than B, A's forwarding priority will be always higher than B's one, regardless of the size of the empty space between A and B. ROFF allows forwarder candidates to use waiting times which are inversely proportional to the forwarding priority in order to avoid unnecessary delay caused by the large empty space. In addition, ROFF finds out the minimum difference between waiting times of two adjacent vehicles required for the successful suppression. minDiff is affected by the latency in MAC and PHY layers. Based on minDiff, ROFF sophisticatedly adjusts the waiting times of forwarder candidates for guaranteeing that the waiting time difference between any two vehicles is larger than minDiff. The main contributions are twofold. First, the collision and latency problems in forwarding schemes analyzed. Second, ROFF is constructed to handle the data dissemination tasks.

4. Problem Statement

Multi hop broadcasting schemes are used to disseminate safety messages. Forwarder node manages the data transmission process in multi-hop broadcasting protocols. Forwarder node selection process is carried out with reference to the waiting time details. RObust and Fast Forwarding (ROFF) protocol solves the unnecessary delay and collusion issues in data dissemination process. A forwarder candidate is allowed to use the waiting time is inversely proportional to its forwarding priority. Empty Space Distribution (ESD) bitmap describes the distribution of empty spaces between vehicles. A forwarder candidate acquires its forwarding priority using the concept of ESD bitmap. Collisions are avoided by control the waiting time differences than the predefined lower bound. The following problems are identified from the current VANET data transmission methods.

- Multicast data delivery is not supported
- Data security is not provided
- Forwarder node selection is not optimized
- Sparse vehicular network conditions are not managed

5. Prediction based channel assignment in CR-VANET

Traffic congestion, road accident and air pollution become social problems and lead to poor quality of life. It was reported that half of traffic congestion events were caused by highway accidents rather than by rush hours in a common perception. Cooperative communications among vehicles is used to make the driving experience safer and more comfortable. VANET is a special ad-hoc network that equips vehicles with wireless communications devices. Hence, vehicles can "talk" with each other; infrastructure and road side units (RSU) and the traffic information can be shared among them. According to the report of America national highway traffic safety administration (NHTSA), New Federal Motor Vehicle Safety Standards will require all vehicles to be equipped with such wireless communications device in the future, in order to mitigate traffic accidents.

The vehicular Ad-hoc Network (VANET) and Cognitive Radio (CR) (CR-VANET) are combined to solve spectrum scarcity problem in VANET. The CR communication device equipped in vehicle can facilitate accessing DSRC channel and other detected idle channels. When transmission load over DSRC channel is heavy, the CR will detect and use other idle channels for broadcasting. The vehicles equipped with CR are unlicensed users in this case, also called as SUs. Hence, CR-VANET should first operate spectrum sensing and then access idle channels opportunistically. The Robust and Fast Forwarding (ROFF) protocol is integrated with Trajectory based MultiCast (TMC) protocol for data dissemination process. Message Forwarding Metric is applied to select the forwarder node with capability factors. Data dissemination process is improved with security and replica features. Network connectivity information is managed with vehicle trajectory information.

Multicast is a crucial routine operation for vehicular networks, which underpins important functions such as message dissemination and group coordination. As vehicles may distribute over a vast area, the number of vehicles in a given region can be limited which results in sparse node distribution in part of the vehicular network. This poses several great challenges for efficient multicast, such as network disconnection, scarce communication opportunities and mobility uncertainty. Multicast schemes are employed for vehicular networks typically maintain a forwarding structure assuming the vehicles have a high density and move at low speed while these assumptions are often invalid in a practical vehicular network. As more and more vehicles are equipped with GPS enabled navigation systems, the trajectories of vehicles are becoming increasingly available. The novelty of TMC includes a message forwarding metric that characterizes the capability of a vehicle to forward a given message to destination nodes and a method of predicting the chance of inter-vehicle encounter between two vehicles based only on their trajectories without accurate timing information. TMC is designed to be a distributed approach. Vehicles make message forwarding decisions based on vehicle trajectories shared through inter-vehicle exchanges without the need of central information management.

Vehicular Ad hoc networks (VANET) are constructed to manage communication between vehicles. Robust and Fast Forwarding (ROFF) protocol is used to handle data dissemination process. Trajectory based Multicast protocol is applied for multicast data delivery process. The Secure Hybrid Routing protocol (SHRP) is constructed to handle the data dissemination operations. The system integrates the ROFF and TMC protocols with security features. Data replication methods are adapted to improve the data delivery speed. Cognitive Radio based Vehicular Ad-hoc network (CR-VANET) has two additional advantages: (1) there are always licensed DSRC channels in spectrum pool, which can be easily used to form common control channel (CCC). The CCC is usually used for spectrum sensing information exchange among vehicles. Compared with CR-VANET, it is very challenging to form stable CCC in conventional CR networks; (2) Vehicles travel along pre-allocated road and different vehicles running on one road have the similar trajectory. Hence, they share one channel availability map in statistic.

Historical spectrum sensing data mining to reveal the spectrum state transition rules in VANET. Historical data mining results are applied to predict the channel availability profile on the next road segment. A Bayesian model is built up in the prediction algorithm, where the likelihood function and prior distribution are utilized, respectively. A Bayesian inference is build on the channel availability probability. The joint spatiotemporal correlations among historical spectrum sensing data are utilized in data mining algorithm. DP and non-parametric HMM models are used to exploit spatial and temporal correlations, respectively. The Secure Hybrid Routing protocol (SHRP) is improved with spectrum sensing data mining based channel allocation method.

6. Hybrid Data Transmission Framework under CR-VANET

The hybrid data communication framework with prediction based channel assignment scheme is constructed for the Cognitive Radio based Vehicular Ad-Hoc Network environment. The Robust and Fast Forwarding (ROFF) protocol is integrated with Trajectory based Multicast (TMC) protocol for data dissemination process. Message Forwarding Metric is applied to select the forwarder node with capability factors. Data dissemination process is improved with security features. Network connectivity information is managed with vehicle trajectory information. Trajectory based Multicast (TMC) protocol is used

to handle the multicast communications. The Secure Hybrid Routing Protocol (SHRP) is build to handle the multicast and broadcast data communication with security features. The spectrum sensing based channel assignment is carried out for emergency data communications.

The VANET data transmission scheme is adapted to handle multicast and broadcast operations. Replicas are deployed to improve the data transmission process. Data transmission process is improved with security features. The Secure Hybrid Routing Protocol (SHRP) is constructed to support multicast and broadcast data communication with security features. The spectrum sensing based channel allocation model is applied in the system. The system is divided into six major modules. They are ESD Bitmap Construction, Forwarder Node Selection, Trajectory Analysis, Channel assignment, Multicast and Broadcast Communication and Security Enhancement for data delivery.

Empty Space Distribution (ESD) bitmap is constructed to indicate the distance between the vehicles. Forwarder node selection is carried out to identify the nodes for retransmission process. Complete network information are observed from the trajectory analysis. The historical spectrum sensing based channel assignment is performed to assign bandwidth for the nodes. Group based data delivery is carried out under multicast data transmission. Broadcast operations are handled under the data dissemination process. Multicast and broad cast data transmission operations are protected with security enhancement.

6.1. ESD Bitmap Construction

Vehicles identify the topology of neighbors by collecting periodic beacons of neighbor vehicles. Neighborhood topology is referred as local view. Each vehicle manages a neighbor table (NBT) for monitoring its local view. Update and delete operations on Neighbor Table is carried out to maintain the freshness of the local view. Space between the vehicles is represented in the Empty Space Distribution (ESD) bitmap. The ESD bitmap is constructed through two phases. A forwarder measures its distances towards each of all the PFCs using the Potential Forwarder Candidate (PFC) topology. The ESD bitmap is constructed with the distance information of the vehicles.

6.2. Forwarder Node Selection

RObust and Fast Forwarding (ROFF) protocol is used to select forwarder nodes. Each vehicle within Naive Forwarding Area (NFA) is called as a Potential Forwarder Candidate (PFC). Waiting time and collusion factors are considered in the forwarder node selection process. A PFC can be assigned as a forwarder candidate when it is allowed to participate in the new forwarder selection process. Forwarding priority is used to assign the waiting time limits for the forwarder nodes. Forwarding priority is estimated using the Empty Space Distribution (ESD) bitmaps and the location of the previous forwarder. Each forwarder candidate is assigned with different waiting time limits. The waiting time is used to initiate the data forwarding process

6.3. Trajectory Analysis

Trajectory of vehicles is identified using Global Positioning Services (GPS) enabled navigation systems. Trajectory based Multicast (TMC) exploits vehicle trajectories for efficient multicast in vehicular networks. Message forwarding metric is estimated to identify the capability of a vehicle to forward a message to destination nodes. TMC scheme uses the distributed approach for the message communication process.

6.4. Channel Assignment Process

The historical spectrum sensing data collection process is carried out to estimate the channel usage levels. The Cognitive Radio (CR) communications are carried out with the 70 MHz spectrum levels. The model uses 6 channels with each 10MHz frequency level for service communication. The six channels are referred as service channels. One channel is allocated for the control communication. It is referred as control channel. The seven channels are categorized as unlicensed channels. The emergency communications can be performed through the licensed channels. The prediction models are used to analyze the history records. The Dirichlet Process and Hidden Markov Model are used to handle the channel assignment process.

6.5. Multicast and Broadcast Communication

Message dissemination and group coordination operations are carried out under the multicast transmission. Network disconnection, sparse communication and mobility uncertainty factors are handled in the data transmission process. Trajectory information is used to make the message forwarding decisions. Message forwarding metric is also used to predict the entry of intermediate vehicle. Data dissemination operations are carried out using the forwarder nodes. Empty Space Distribution (ESD) bitmap and trajectory information are used to handle the data

transmission process. The Secure Hybrid Routing Protocol (SHRP) is employed to manage the multicast and broadcast data communication with confidentiality and integrity verification features. Replica nodes are used to maintain the frequently transferred messages. Forwarder nodes collect the messages from the replica nodes.

6.6. Security Enhancement for data delivery

Group keys are used for the data encryption/decryption operations in the multicast data transmission process. Data security is provided with Advanced Encryption Standard (AES) algorithm. Secure Hash Algorithm (SHA) is used for the data integrity verification in VANET communication. Message forwarder nodes are verified with trust levels.

7. Conclusion and Future Enhancement

Cognitive Radio based Vehicular Ad hoc networks (CR-VANET) are constructed to manage communication between vehicles. Robust and Fast Forwarding (ROFF) protocol is used to handle data dissemination process. Trajectory based MultiCast (TMC) protocol is applied for multicast data delivery process. The system integrates the ROFF and TMC protocols with security features. The historical spectrum sensing data values are processed with data mining methods to carry out the channel allocation operations. The Dirichlet Process and Hidden Markov Model techniques are applied to manage the channel assignment operations. The channel assignment operations are integrated with the Robust and Fast Forwarding (ROFF), Trajectory based MultiCast (TMC) and Secure Hybrid Routing Protocol (SHRP) models. The system supports faster and reliable data delivery scheme with security. The vehicular ad-hoc network communication system controls the collision and latency in data dissemination process. Data transmission is handled without the central information management authority. Multicast and broadcast operations are integrated in the VANET data communication process. The system can be improved to handle anonymous and malicious attacks. Clustering techniques can be integrated to improve the bandwidth scheduling process.

REFERENCES

[1] J.B Kenney. Dedicated short-range communications (dsrc) standards in the united states. Proceedings of the IEEE, 99(7):1162–1182, 2011.

[2] N. Loulloudes, G. Pallis, and M.D. Dikaiakos. V-radar: A vehicular traffic query protocol for urban environments. In Vehicular Traffic Management for Smart Cities (VTM), First International Workshop on, pages 1–6. IEEE, 2012.

[3] H. Prothmann, H. Schmeck, S. Tomforde, J. Lyda, J. Hahner C. Muller-Schloer and J. Branke. Decentralized route guidance in organic traffic control. In Proceedings of the 5th IEEE International Conference on Self-Adaptive and Self-Organizing Systems, pages 219–220. IEEE, 2011.

[4] C. Sommer, R. German and F. Dressler. Bidirectionally Coupled Network and Road Traffic Simulation for Improved IVC Analysis. IEEE Transactions on Mobile Computing, 10(1):3–15, January 2011.

[5] Hassan Artail and Noor Abbani, "A Pseudonym Management System to Achieve Anonymity in Vehicular Ad Hoc Networks", IEEE Transactions On Journal Name, Manuscript Id Jan-Feb2016.

[6] T. Xu and Y. Cai. Feeling-based location privacy protection for location based services. In Proceedings of the 16th ACM conference on Computer and communications security, pages 348–357. ACM, 2009.

[7] W. Whyte, A. Weimerskirch, V. Kumar and T. Hehn. A Security Credential Management System for V2V Communications. In Proceedings of the 2013 IEEE Vehicular Networking Conference, pages 1–8, 2013.

[8] B. Wiedersheim, Z. Ma, F. Kargl and P. Papadimitratos. Privacy in inter-vehicular networks: Why simple pseudonym change is not enough. In Wireless On-demand Network Systems and Services (WONS), 2010 Seventh International Conference on, pages 176–183. IEEE, 2010.

[9] Jie Li, Huang Lu and Mohsen Guizani, "ACPN: A Novel Authentication Framework with Conditional Privacy-Preservation and Non-Repudiation for VANETs", IEEE Transactions On Parallel And Distributed Systems, Vol. 26, No. 4, April 2015.

[10] Joon Ahn, Maheswaran Sathiamoorthy and Lin Zhang, "Optimizing Content Dissemination in Vehicular Networks with Radio Heterogeneity", IEEE Transactions On Mobile Computing, Vol. 13, No. 6, June 2014.