CHAPTER 1

INTRODUCTION

1.1 PREAMBLE

VANETs have emerged as a promising technology to meet the challenges of the next generation wireless communication networks for vehicle communication in recent years. VANET provided users with convenience by exchanging various information through communication among a Taxi, a driver and the external network. High node flexibility, dynamic topology transformations together with repeated link break and severe delay restrictions are observed in VANET Communication. Improving the overall performance obtained with the wireless communication having security issues are the important aspects in the vehicular communication.

1.2 THE GENESIS OF THE THESIS

VANETs are a subset of MANET and one of the highly hoped Intelligent Transportation System (ITS) technology which enables vehicles to share the information with other similar nodes present inside the network. It can assist in lane changing activities, collision avoidance, providing internet access and for sending emergency warning systems.

There are many challenges that need to be addressed when creating a VANET. One of the challenges is the topology of the network which changes more rapidly. While sharing some of the limitations, such as lack of
infrastructure and limited communications range, they have several dissimilarities that make VANETs a much different research area.

The main aim of this research work is to reduce delay, increasing packet delivery ratio and reducing waiting time using secure VANET schemes.

1.3 LITERATURE REVIEW OF PROBLEMS

In this brief study on various VANET secure communication protocols, different related research issues and challenges are investigated to narrow down the research problem.

1.3.1 Vehicular Ad Hoc Network (VANET)

Matsumoto & Mizui (2000) discussed about a prototype of a 2-way spread spectrum communication system as one part of a double boomerang transmission system. From experimental results, it is confirmed that this system is capable of communicating with each other in the situation with little interference.

Nagaosa & Hasegawa (2000) proposed a hierarchical vehicle position encoding scheme for inter-vehicle communication networks (IVCN) and describes the way to derive better performance using the newly introduced scheme under a specific condition.

Anchor-Based Street and Traffic Aware Routing (A-STAR) is a kind of position based routing protocol that is particularly designed for city environments for inter vehicle communication system was proposed by (Seet et al. 2004). It guarantees greater connectivity for packet delivery by making use of vehicular traffic city bus information in the case of an end-to-end connection.
Lochert et al. (2005) proposed a Geographic Source Routing (GSR) routing was proposed for the purpose of vehicular ad hoc networks in city environments that is the combination of position-based routing along with topological knowledge. GSR makes use of greedy forwarding through a pre-selected shortest path & this path is calculated by using Dijkstra algorithm. This protocol ignores the conditions such as sparse network where sufficient nodes are not available for forwarding the packets.

Kamat et al. (2006) presented a security framework for usage in VANETs, using Identity-Based Cryptography (IBC), to provide authentication, confidentiality, non-repudiation and message integrity.

Calandriello et al. (2007) are concerned with security problem; especially reliable pseudonym-based authentication, which reduces the security overhead involved in safety beaconing.

Zhang et al. (2008) introduced a novel Road Side Unit (RSU)-aided message authentication scheme, called RAISE which is responsible for verifying the authenticity related to the messages sent from the vehicles.

Li et al. (2008) introduced a lightweight authenticated key establishment scheme with privacy preservation to secure the communications between mobile vehicles and roadside infrastructure. Hartenstein et al. (2008) discussed many practical difficulties in VANET research, including lack of communication coordination, dynamic network topology due to mobility and radio propagation limitations, as well as balancing security and privacy.

Verma & Huang (2009) introduced a novel scheme to achieve safe, and effective vehicular communication, permits the vehicles to form group, which are also used for performing multi-hop Vehicle to Vehicle (V2V) communication without any assistance from a trusted authority and then
discussed a flexible, secure and decentralized attribute based secure key management framework for VANETs.

Kim et al. (2010) considered a scheme of identification and key exchange for secure VANETs that are based on group signature but they do not yield mutual identification and key exchange for imparting data confidentiality.

Mishra et al. (2011) proposed a reliable and competent protocol for vehicular ad hoc networks that ensures both message authentication and privacy preservation. As safety related message may contain life critical information, it is a necessity that the both the sender and the message is authentic. The proposed scheme is in accordance with a secure elliptic curve digital signature algorithm approach.

Shim (2012) presented a conditional privacy-preserving authentication scheme, called CPAS, using pseudo-identity-based signatures for secure vehicle-to-infrastructure communications in vehicular ad hoc networks. The scheme achieves conditional privacy preservation, in which each message launched by a vehicle is mapped to a distinct pseudo-identity, and a trust authority can always retrieve the real identity of a vehicle from any pseudo-identity.

Jia et al. (2013) presented an efficient identity based signature scheme EPAS, which satisfies conditional privacy requirements through software solution. In light of efficiency, lightweight signature as well as batch verification is used for providing effective authentication.

Mamun et al. (2014) used an application-friendly Group Signature (GS) model for VANET application demand.
1.3.2 Performance Analysis of Data in VANET Based on Clustering

This work develops an efficient routing protocol that is in accordance with the Long Range (LR) and Short Range (SR) unicasting and multicasting schemes. Clustering based routing schemes have been observed to produce significant QoS results.

Bononi & Di Felice (2007) illustrated the modeling of a cross-layered Medium Access Control (MAC) and clustering solution that is helpful in the rapid transmission of broadcast messages in a network like VANET. A distributed dynamic clustering algorithm is introduced to create a dynamic virtual backbone in the vehicular network which is responsible for implementing efficient messages propagation. A fast multi-hop MAC forwarding mechanism was defined to exploit the role of backbone vehicles, under a cross-layered approach.

Zhu et al. (2008) introduced a novel Aggregated Emergency Message Authentication (AEMA) scheme to validate an emergency event. It gives the information regarding the syntactic aggregation and cryptographic aggregation techniques to dramatically reduce the transmission cost, and adopt batch verification technique for efficient emergency messages verification. Compared with existing emergency message authentication approaches, this scheme shows the superiority on generality, enhanced security and efficiency.

Muraleedharan & Osadciw (2009) applied cognitive security protocol that disseminates information using distributed sensor technology while prioritizing prevention of data aging, efficient Quality-Of-Service (QoS) and robustness against Denial-of-Service (DoS) attack. In contrast, since the high precedence safety communications are extremely small in range, unmatched, and in nature it is available freely which is explained by
Shan et al. (2009) they have a firm delay condition and require a consistent broadcast service.

Shea et al. (2009) proposed a novel, mobility-based clustering scheme for Vehicle Ad hoc Networks, which utilizes the Affinity Propagation algorithm in a distributed fashion. The proposed algorithm considers typical vehicular mobility during cluster formation, which produces clusters with high stability. Clustering performance is measured through average cluster head duration, average rate of cluster head change, along with the average number of clusters.

Kim et al. (2009) explained about the Clustering-based Multi-channel MAC protocol adequate to VANET and then confirmed the appropriate channel conditions in a V2V communication on the basis of this protocol.

Maslekar et al. (2009) proposed a direction based clustering algorithm for data dissemination. The protocol is used to estimate the density of vehicles on a given road. As in any clustering algorithm, the formation of the cluster and the use of the bandwidth are important tasks. In the proposed solution the packet is forwarded to vehicles only if they are moving along the same direction which is not applicable in practical scenario as vehicles moving direction should also stay connected with the network.

Girinath & Selvan (2010) introduced an approach to evaluate the cluster based routing’s effect on mobility pattern and routing performance of vehicular ad hoc network systematically. It can be observed that combining clustering and routing pattern has an influence over the performance of VANET mobility. This new design of routing algorithm and Mobility model architecture for supporting traffic regulation minimizes the reclustering
process and generates more number of stable clusters in comparison to other models.

Chim et al. (2011) studied the problem related to finding and making reservation on charging stations via a vehicular ad hoc network. The author mainly focused on the privacy concern as drivers would not like to be traced by knowing which charging stations they have visited. An electric vehicle first generates a set of anonymous credentials on its own. A trusted authority then blindly signs on them after verifying the identity of the vehicle. Then the vehicle can make charging station searching queries and reservations by presenting those signed anonymous credentials.

Sadiq et al. (2011) presented the dynamic addressing scheme that tries to satisfy the requirement corresponding to the auto IP address configuration making use of the clustering approach, which actually gets over the challenge about unique IP address assignment.

Lu et al. (2012) achieved a vehicle user's privacy preservation while improving the key update efficiency of location-based services (LBSs) in VANETs.

Sahoo et al. (2012) introduced first algorithm an attempt to create clusters by considering direction, position and proportional speed of the vehicle for managing the scalability issue. A new algorithm for selecting the most appropriate Cluster Head (CH) taking into consideration the real time updated position and trust value of vehicles is used in this research. Ahizoune & Hafid (2012) focused on a new Stability-Based Clustering Algorithm (SBCA), specifically designed for VANETs, which takes mobility, number of neighbors, and leadership (i.e., cluster head) duration into consideration for the purpose of providing a more stable architecture.
Chai et al. (2013) proposed a clustering-based scheme applicable for propagation of data in VANET, which is a CH selection algorithm and a cluster switching algorithm for VANET. The proposed CH selection algorithm jointly considers node degree, the available resource of candidate CHs and the velocity difference between candidate CHs and other Cluster Members (CMs) in a cluster provided. The new optimal cluster switching scheme focuses on the QoS requirements of the delay-sensitive service as well as the throughput-sensitive service, by definition of the utility functions to provide access to different clusters, by means of which the optimal destination cluster can be achieved.

Rong et al (2013) proposed a CH selection algorithm and cluster switching algorithm. The CH selection algorithm considers node degree, resource available with the candidate CH and the velocity difference between the CH and other cluster members. In any point of time, the vehicular node may leave the present cluster and become a member of another cluster under assistance of some other CH. The cluster switching algorithm renders handover from one cluster to another by taking into account Quality of Service (QoS) requirements and various utility functions.

Souza et al. (2013) introduced the reliability of Multicast Ad hoc On Demand Distance Vector (MAODV) protocol is analyzed, a well known protocol that builds trees on demand to connect multicast group members. The protocol messages act as bio-inspired agents (Ants) depositing pheromone to evaluate the attractiveness of each route.

Wahab et al. (2013) addressed the problem of clustering in VANETs using Quality of Service Optimized Link State Routing (QoS-OLSR) protocol. The mobility-based algorithms ignore the QoS requirements that are important for VANET safety, emergency, and multimedia services.
Ding & Li (2013) presented a reputation management framework in order to decide if an incoming traffic message is important and can be trusted by the driver. Major number of people drive their vehicles daily for local commuting (to schools, workplaces, etc), and therefore, most of the vehicles have their predetermined stable daily trajectories. It is easy and practical to have the RSU take up the responsibility of controlling the long-term reputation scores for these commute vehicles, and also an event-centric reputation mechanism is also employed as a helpful support.

Wang et al. (2014) made use of model to address the (RSU) deployment problem by formulating it as a mobility clustering problem. They adopt Affinity Propagation (AP) algorithm to capture the spatial temporal mobility influence in different time period. The union set of the obtained clustering centers which have the maximum influence to its cluster members is then the solution to RSU deployment.

Wang et al. (2015) proposed a model for cluster design on the basis of the impacts of MAC layer operation, Physical layer condition and mobility. The model assumes that a stable cluster with nodes moving at same speed which makes it difficult to be applicable in practical scenario.

Aswed & Abdala (2015) generalized the novel clustering method, referred to as Relatively Stable Clustering for Unbiased Environments (ReSCUE). The aim of ReSCUE is essentially assuring the cluster stability in an unprejudiced manner. ReSCUE keeps track of the spatio-temporal changes in VANET node characteristics, and uses these characteristics along with local information to avoid biased clustering that is in accordance with common and general node characteristics.
1.3.3 Enhanced Multicast Algorithm for Mobile Ad Hoc Using Cooperative Ad Hoc MAC in VANET

This work employs an enhanced multicast algorithm to reduce the delay shown by the vehicles as they pass through the intersection Road Side Unit (RSU). A Cooperation approach for supporting a VANET, primarily concentrating on the MAC layer known as Cooperative ADHOC MAC (CAH-MAC) is presented in this work. The proposed approach consists of helper detection and transmission algorithm using DSRC Protocol. The main aim of this protocol is to reduce the computational time for retransmitting packets when it is failed by poor channel conditions.

Bianchi (2000) developed a mathematical model to compute the throughput performance corresponding to IEEE 802.11 assuming some finite number of nodes along with ideal channel conditions. The performance of Discrete Coordination Function (DCF) is evaluated using a Markov model where each station is modeled by a pair of integers \((i, k)\). The back off stage, \(i\), starts at 0 and increased by 1 for every transmission that results in collision till the maximum value of \(m\). The counter \(k\) is selected to lie in the range of \([0, W_r-1]\) where \(W_r = 2^i W_0\) and \(W_0\) depends on Contention Window minimum value (CWmin) parameter of 802.11. On comparing the results of two access mechanisms, the Request to Send / Clear to Send (RTS/CTS) are superior in performance and efficient to cope with hidden terminals. Since the real traffic scenario does not have ideal channel condition with finite number of vehicles, the model based on saturated traffic assumption could not be applicable for practical applications in real world scenario.

Borgonovo et al. (2004) studied the performance of Ad-hoc networking, although a promising solution for several applications yet has several unsolved problems, like the hidden terminal problem, flexible and prompt access, QoS provisioning and effective broadcast service. MAC
architecture is capable of solving the above problems in environments with no limitations on power consumption, like the networks for inter-vehicle communications. This novel architecture is completely based on distributed access technique, RR-ALOHA, which is able to dynamically establish a robust single-hop broadcast channel on a slotted structure, for every active terminal in the network. Even though the proposed architecture makes use of a slotted channel it can be adjusted in order to work on the physical layer of various standards, such as the Universal Mobile Telephone Services (UMTS), Terrestrial Radio Access (TRA), Time Division Duplex (TDD) and IEEE 802.11.

Qiong et al (2014) proposed an analytical model for analyzing DCF based fair channel access. In VANET, there are conditions when more than one vehicular node accesses a single access point. During which the node moving at higher speed does not have same opportunity as vehicle moving with lower speed to communicate with the road side access point. The process of changing the transmission probability by changing contention window size is called fair channel effect. They have done the analysis in non-saturated environment.

Sabari et al. (2009) have discussed a design on Ant-Colony Based Multicast Routing (AMR) algorithm for MANETs, to solve the Traffic Engineering Multicast problem that optimizes several objectives simultaneously. The algorithm calculates one more additional constraint in the cost metric, which is the product of average-delay and the maximum depth of the multicast tree and try to minimize this combined cost metric event.

Li et al. (2009) explained the interference and power constrained broadcast/multicast and the delay-bounded interference and power constrained broadcast/multicast routing problems in wireless Ad Hoc Networks using directional antennas. Approximation and a Heuristic
Algorithm motivated the study of above optimization problems, and approximation schemes for two multi-constrained directed Steiner tree problems. Broadcast/Multicast message by using the trees found by the algorithms tend to have less channel collisions and higher network throughput.

Xin et al. (2009) proposed a fully distributed deterministic algorithm for such a Mobile to Mobile (M2M) multicasting problem and analyze its time complexity. The model could not be applicable for scenario when the maximum hop distance between nodes is not known in advance.

Shan et al. (2009) investigates the design of a distributed cooperative medium access control protocol for the effective functioning of multi hop wireless networks. Single-antenna mobile terminals in an environment containing multi-user share the antennas from other mobiles to create a virtual multiple antenna system which attains more robust communication with a larger diversity gain.

Zhang et al. (2009) introduced a novel protocol called Vehicular Cooperative Media Access Control (VC-MAC), which uses the idea of cooperative communication for vehicular networks, particularly for gateway downloading scenarios. VC-MAC uses the broadcast nature of the wireless medium to maximize the system throughput. Spatial diversity and user diversity are exploited by concurrent cooperative relaying to overcome the unreliability of the wireless channel in vehicular networks.

Liu et al. (2009) have proposed a 3-D Markov chain model that integrates the queuing process and contention resolution into one model. This is a finite buffer model and is capable of accurately measuring the important QoS measures, throughput and queue length. The 3-D Markov chain models the station using 3-tuple \((h, i, k)\) in contrast to 2-D model which uses only
(i, k). The index $h$ in 3-D model models the queue occupancy and it is in the range of $0 \leq h \leq L$, where $L$ is the maximum queue length. It does not consider imperfect wireless channel conditions which has major impact on network performance in practical application.

Yang et al. (2010) explained the concept of the throughput of Time Division Multiple Access (TDMA) with C-TDMA systems in Rayleigh fading channels. The maximum throughput of TDMA is only about 0.45 without using cooperative diversity in a Rayleigh fading channel. For a C-TDMA system, when $qc$ value increases from 0.2 to 1, there are several number of terminals in the cooperation terminal set. When $qc$ is 0, there is no cooperative transmission and the system becomes a TDMA system without cooperative diversity. It is seen that the maximum throughput of the C-TDMA system has 44% increase compared to the TDMA system due to the cooperation transmissions when $qc$ equals to 1.

Hassan (2011) analyzed regarding the improvement in the performance of the MAC for the case of safety applications in a Dedicated Short-Range Communication (DSRC) environment.

Sutariya & Pradhan (2012) proposed a routing protocol IAODV (Improved AODV) that ensures giving timely and accurate information to drivers in V2V communication compare to AODV protocols in city scenarios of vehicular ad hoc networks. Proposed IAODV is defined as limited source routing up to two hops with backup route between source node and destination node.

Annapurna et al. (2013) described about the network modeling of a wireless multicast network by approach of optimized joint MAC scheduling and network coding. A heuristic method of designing a network is achieved by scheduling algorithm which is based on network parameters such as
interference free transmissions and optimization of avoidable scheduling sets. They derive a joint linear optimization problem which is used in the designing of the wireless network. Further when the scheduling is done, the network coding is adapted. The code construction algorithms are used and the unequal timeshare is incorporated in designing network codes.

DasGupta et al. (2013) emphasized the Trusted Vehicle Authentication scheme for secured communication in VANET. The use of a layered structure for assigning trust values to a vehicle helps in detecting a node taking part in malicious activity. Finally the performance and effectiveness of vehicle authentication logic for the case of vehicular ad hoc networks are achieved.

Leanna & Rahmat (2013) presented about investigation result of AODV, Dynamic Source Routing (DSR) and Destination-Sequenced Distance-Vector (DSDV) that applied an Ant-algorithm which are AODV-Ant, DSR-Ant, and DSDV-Ant. DSDV represents about the proactive routing type protocol based on table driven, while AODV and DSR represents of reactive routing protocol type based on demand.

Yoo et al. (2013) proposed a method to utilize the information on vehicle’s moment and map information to calculate link duration. The links established between two nodes in wireless environment suffer from fading, shadowing, dynamic topology and high speed movement of vehicles. It provides stable link by preventing link-breakage before it happens.

Bhoi & Khilar (2014) introduced Intelligent Junction Selection based routing protocol (IJS) for transmitting the data in a path that is quicker, where the vehicles are connected mostly and have less link connectivity issue. In this protocol, a helping vehicle is fixed at each junction to regulate the communication through prediction of link failures or network gaps present in
a route. Rendering help to vehicles at the junction generates a score for every neighboring junction for the purpose of forwarding the data to the destination by taking the current traffic information into account and chooses that junction having minimum score. IJS protocol is realized and it is compared with Greedy Traffic Aware Routing protocol (GyTAR), Anchor-Based Street and Traffic Aware Routing (A-STAR) and Geographic Source Routing (GSR) routing protocols.

Hadded et al. (2015) introduced an RSU supported TDMA protocol to reduce the channel allocation time and management overhead involved. The problems pertaining to this are the restricted bandwidth, shared wireless medium, greater mobility of vehicles etc. For this purpose, the RSU separates the limited bandwidth that is assigned to its region into overlapping spatial clusters that is prefixed and the channel in every cluster is then divided into time slots. A time slot is allocated to a vehicle based on the priority of the request and the channel availability. Finally the allocation scheme is capable of delivering packets within the specified time with huge reliability for diverse vehicle speeds and density for channel allocation on the basis of the three overlapping clusters. TDMA based MAC along with contention based request maximizes the packet reception ratio in addition to the low channel acquisition delay.

A unified algorithm is presented for wireless MAC protocols - a pioneer trial of this vision that benefits future wireless networks. This unified algorithm is in accordance with the thought of MULCAR, a generalized model for MAC protocols proposed by Teng & Chen (2002).

Choi & Lee (2004) considered the dynamic use of the RTS and CTS frame exchange, a real-time algorithm updating the RTS-CTS threshold dynamically according to the number of transmission attempts and the number of STAs in the BSS is proposed to give the maximum MAC
throughput of IEEE 802.11e wireless LANs supporting the EDCA MAC
protocol.

Zheng et al. (2006) presented a mathematical model for evaluating
the performance of DCF in imperfect wireless channel condition. The various
factors such as binary exponential back off mechanism in DCF, various traffic
load given to the network, and queuing system at the MAC layer and
imperfect wireless channels has impact on the overall network performance.

Malone et al. (2007) extended the work of Bianchi to be applicable
for non-saturated environment. The internet applications such as web-browser
and e-mail produces bursty data whereas voice information is not so. This
varying range of data rate requires a non-saturated operation. The saturated
data flow may reduce the bandwidth available for low-rate voice over IP
(VoIP). The 2-dimensional Markov model \((i,k)\) used is a finite buffer model
and modified to be operating in post-backoff in contrast to that. The usage of
2-D Markov chain model does not give the Quality of service (QoS)
performance and queuing behavior.

Kim et al. (2009) presented a multi-channel MAC protocol based
on clustering process. It reduces the congestion and packet collision in the
network. Based on clustering process the selection of cluster head and making
a good cluster design has major impact on the network performance.

Burton & Hill (2009) made an analysis to derive an achievable
tradeoff between broadcast efficiency and reliability. Enhanced distributed
channel access (EDCA) is designed for contention based QoS support. The
working of EDCA is similar to that of DCF but with some additional
qualities. The EDCA mechanism defines four access categories that provide
data traffic with four different priorities. Each access category is equivalent to
a DCF station with its own EDCA parameters. Instead of DIFS as in DCF,
EDCA uses Arbitration Inter Frame Space (AIFS). Each access category had different AIFS, CWmin and CWmax value.

Gazdar et al. (2012) introduced an effective dynamic architecture of the PKI for VANET that is developed on the basis of a trust model and a new distributed clustering algorithm. Furthermore, the author introduced the concept of a VANET Dynamic Demilitarized Zone (VDDZ), comprising of the set of confident vehicles that are located within the immediate adjacency of every CH to assume the role of Registration Authorities (RA). The VDDZ targets at securing the elected CAs by protecting them from dangerous or malicious vehicles. A set of simulations making use of urban and highway scenarios are performed to have an investigation over the effects of the range of transmission, the speed of vehicles moving and the number of confident vehicles in the network that are on the security level, the stability and the effectiveness of this proposed architecture.

Shuqing & Jinye (2012) introduced a model for analysis of periodic broadcast messages in VANET. They have considered only a one dimensional Markov model since there is no packet retransmission in broadcast mode. The assumption of having unsaturated traffic and there is no packet waiting for transmission in the buffer of the node. These assumptions make it difficult to implement in real time scenario. It does not extend for dynamically changing Contention Window (CW) sizes.

Han et al. (2012) proposed an analytical model which is appropriate for both the basic access mode and RTS/CTS mode such that it is applicable all four access categories of IEEE 802.11p. Based on the analysis they have come to a conclusion that the IEEE 802.11p standard provides an effective service differentiation mechanism. Consideration of saturated traffic scenario makes analytical model tedious to implement in non-saturated real world environments. It could not support bandwidth consuming large applications as
it requires a challenging level of resource allocation which is not addressed here.

Chandrasekharan et al. (2012) illustrated a mathematical model to examine the connectivity features for VANETs with the channel randomness present, from the view of a queuing theory. They have considered different fading models like Rayleigh, Rican and Weibull for analysis. A distance-dependent power law model is employed for representing the path loss observed in the channel. They have analyzed the impacts of physical layer parameters namely path loss exponent, shadow fading standard deviation and fading factors.

Wang et al. (2012) studied the connectivity of information propagation in inter-vehicle communication, mainly focusing on packet loss rate, packet transmission distance and effective coverage range of road-side station. Such indicators are useful for the performance evaluation of inter-vehicle communication for different equipped rates, wireless communication ranges and typical distributions of vehicle space headway, which can be reference in practical deployment of VANET.

Luan et al. (2012) proposed a logical model for assessing the throughput of DCF in the large scale drive-thru Internet environment. The model integrates the high-node mobility along with the modeling of DCF and exposes the effects of mobility (featured by node velocity and directions of movement) on the resulting throughput. On the basis of the model, it is shown that the throughput of DCF will be minimized with increasing node velocity because of the mismatch arising between the MAC and the varying high-throughput connectivity of vehicles. They also proposed different enhancement schemes for adaptive adjustment of the MAC tuned with the node mobility.
Luo et al. (2013) introduced a Hybrid MAC protocol (H-MAC) which is a combination of the reservation and competition methods for solving the abrupt burst data flow at link layer of the VANET. On the basis of the whole network time synchronization, H-MAC protocol does the division of a frame cycle into two parts. The first part is the reservation period in which every node has got its own slot. Node can send constant data flow like beacon packets in the slot. The second part is the competition period having the transmission of the burst data. This way, beacon frames and burst data are separated.

Prabhakar et al. (2013) presented a protective mechanism for the VANET security using heuristic based ant colony optimization. The heuristic based ant model, operated with known adversaries and unknown ones on the basis of the density of pheromone that is collected in the road network path along with new road path findings by the help of the traversing ants. Afterwards, the Nash equilibrium is employed with the game theoretic framework for identifying the stability state of the players who are involved in it. Optimal usage of traffic organizers and security framework is studied in in the static (e.g., prefixed roadside units) as well as the active cases (e.g., moving law enforcement units).

Akhtar et al. (2013) analyzed VANET topology characteristics observed on a large highway section through the integration of non-abstract microscopic mobility traces that are generated exploiting practical-world road topology and real-data based traffic needs with the real channel simulations considering the impact of vehicles on the signal power received. The performance of this realistic kind of scenario is compared with that of the most generally utilized and more simplistic channel models making use of different metrics of interest. Obstacle based channel model and simplistic channel models that includes unit disc and log-normal shadowing models are
considered for analysis. The method proposed has been shown to be a good match to the computation-wise expensive and hard to realize obstacle-based model.

Dang et al. (2014) introduced an Efficient and Reliable MAC protocol for VANETs (VER-MAC) which allows nodes to broadcast safety packets twice during both the control channel interval and service channel interval to increase the safety broadcast reliability. By using the additional data structures, nodes can transmit service packets during the control channel interval to improve the service throughput.

Nguyen et al. (2014) proposed a novel TDMA-based MAC protocol, called the e-VeMAC protocol, is proposed for VANETs based on the VeMAC protocol. As simulation results, in the e-VeMAC protocol the number of nodes resent packet on the CCH is lower than the VeMAC protocol in parallel transmission.

Carpenter (2014) proposed a realistic model for shadowing and fading effects. VANET investigators often model propagation loss deterministically dependent upon transmitter-receiver distance, fading and shadowing effects are often modeled stochastically, leading to probabilistic results which are independent of the actual environment and thus fail to consider realistic road topologies and the presence of obstacles. They have implemented for the empirically-validated obstacle shadowing model by leveraging building data from Open Street Map to deterministically evaluate line of sight propagation effects using techniques from computational geometry.

Wu & Zheng (2015) outlined about an analytical model for analyzing DCF based fair channel access. The node moving at higher speed does not have same opportunity as vehicle moving with lower speed to
communicate with the roadside access point. The process of changing the transmission probability by changing contention window size is called fair channel effect. They have done the analysis in non-saturated environment.

1.3.4 A New Secure Message Transfer in Taxi Service for Vehicular Ad Hoc Network

A new security characteristic completely lessens the threat of taxi offences and helps to protect the privacy concern of taxi passengers. Authentication mechanisms consist of digital signatures which show the evidence of most appropriate scheme regardless of high overhead. The current network solutions cannot be openly implemented with VANETs, provided the drastically varying characteristic of this new category of networks. This work does not consider V2V communication.

Sampigethaya et al. (2005) studied the issue of issuing location privacy in VANET by permitting vehicles to avoid the tracking of their broadcast communications. A location privacy scheme which evaluates the privacy improvement accomplished under few standard constraints of existing VANET applications, under the very nose of a global opponent.

Sampigethaya et al. (2007) tried to resolve the problem of unauthorized tracking of vehicles on the basis of their broadcast communications and to improve the user location privacy in VANET. A scheme called AMOEBA that provides location privacy by utilizing the group navigation of vehicles. It is suited to the user privacy provided is considered under various attacks.

Harsch et al. (2007) introduced the problem of secure VANET communications and the author provided a scheme that secures geographic position-based routing, which has been widely accepted as the appropriate
one for vehicular communication. The author used defense mechanisms, relying both on cryptographic primitives and plausibility checks mitigating false position injection.

Qian et al. (2008) introduced a secure MAC protocol for VANETs with different message priorities for different types of applications to access DSRC channels. The secure communication protocol is designed to guarantee the freshness of the message, message authentication and integrity, message non-repudiation, and privacy and anonymity of the senders.

Lin et al. (2008) proposed a Time Efficient and Secure Vehicular Communication (TSVC) scheme with privacy preservation, which aims at minimizing the packet overhead in terms of signature overhead and signature verification latency without compromising the security and privacy requirements.

Wang et al. (2008) reviewed the safe and secure infrastructure of VANET, few significant applications and thought provoking security challenges. To cope with these security challenges, the author introduced a novel secure scheme for vehicular communication on VANETs. This scheme not only protects the privacy but also helps in maintaining the responsibility indulged in the secure communications by exploiting session keys. The author also analyzed the robustness of this scheme.

Yan et al. (2008) achieved local security by enlisting the help of on-board Radar to detect neighboring vehicles and to confirm their announced coordinates. Local security is extended to achieve global security by using preset position-based groups to create a communication network and by using a dynamic challenging mechanism to confirm remote position information. Chaurasia et al. (2008) introduced a group signature scheme for inter mobile vehicle communication in VANET. The threats occurred during vehicle
communication, dynamic nature of the VANET and mobility of the vehicles are discussed as an important issue in VANET. To overcome these issues, the authors introduced group signature schemes along with pseudonyms to enhance the effectiveness and efficiency of group signatures in VANETs.

Ibrahim & Weigle (2008) presented a technique for accurate grouping of highway traffic information in the case of VANETs. Highway congestion notification applications are required to distribute information about traffic situation to vehicles in a distance. In conditions of dense traffic, aggregation is necessary for allowing a single frame to conduct information about a huge number of vehicles. The method, CASCADE, employs compression for providing aggregation without any loss of accuracy. CASCADE efficiently uses the wireless channel while also providing every vehicle with highly accurate data, representing a large area in the front of the vehicle, and can be used in combination with data aggregated from other vehicles for the purpose of further extending the area covered.

Liu et al. (2009) introduced an autonomous road side infrastructure network approach. Road side infrastructures in the same autonomous network cache and forward certificates, which are invisible to other autonomous network. A distributed Intrusion Detection System (IDS) system integrated with the CA database provide further security protection from malicious vehicles with legal certificates.

Jung et al. (2009) make up for the limitations and presented a healthy conditional privacy-preserving authentication protocol without loss of efficiency as compared with Efficient Conditional Privacy Preservation (ECPP). Furthermore, in this protocol, RSUs can issue multiple anonymous certificates to an On Board Unit (OBU) to alleviate system overheads for validity check of RSUs. For the purpose of achieving these targets, the author considers a universal re-encryption scheme as building block.
Biswas & Misic (2010) introduced a framework for having a secure RSU-to-OBU message broadcasting for use in VANETs making use of proxy signatures. The author considered a VANET infrastructure, having similar network assumptions as similar to that of the current standards of VANET communications. The chief goal of this scheme is about providing message integrity, authentication of the broadcast messages, and authentication of the RSU to the OBUs. The author determined the suitable responsibilities to the network components, thereby facilitating the OBU pertaining to the verification of the message received for being valid and unbroken.

Wasef & Shen (2010) presented a novel location privacy preservation mechanism for VANETs using Random Encryption Periods (REP). REP is based on a privacy preserving group communication protocol, which has a conditional full statelessness property. In addition, REP ensures that the requirements to track a vehicle are always violated. By conducting detailed analysis and simulation, REP is demonstrated to be reliable, efficient and scalable.

Chong et al (2012) proposed an analytical model that is suitable for both the basic access mode and RTS/CTS mode in such a way that it is applicable all four access categories of IEEE 802.11p. Based on the analysis they have concluded that the IEEE 802.11p standard provides an effective service differentiation mechanism. Consideration of saturated traffic scenario makes analytical model tedious to implement in non-saturated real world scenario. It could not support bandwidth 8 consuming large applications as it requires a challenging level of resource allocation which is not addressed here.

Hwang et al. (2011) reviewed a safe and secure communication and privacy maintained scheme of VANET. The VANET enhances road safety and traffic situations via exchange of the traffic information by the vehicle
with other vehicles and few other infrastructures with steadfastness. Guaranteeing secure exchange messages and being trustworthy and protective of user privacy are critical issues. The transmission message must be well guarded in order to assure the integrity, confidentiality, anonymity and unlinking ability.

Sun et al. (2011) introduced RescueMe, location-based VANETs, to assist in secure and reliable rescue planning for the effective assignment of rescue resources. RescueMe makes the best use of the location information saved during normal network conditions for enabling post-disaster rescue planning, while ensuring that the sensitive user location information is not manipulated to trace a user's locations in the absence of disasters, and the presence of the most harmful collusion attack. The author provided a new location update message construct and several enhancements are used to attain the functional and security targets of RescueMe. Yeh et al. (2011) introduced a novel Portable Privacy-Preserving Authentication and Access Control Protocol (PAACCP), for non-safety applications in VANETs.

Lee et al. (2012) presented Signature-Seeking Drive (SSD), a secure incentive framework for commercial dissemination in VANETs. Unlike currently proposed incentive systems, SSD does not rely on tamper-proof hardware or game theoretic approaches, but leverages a PKI to provide secure incentives for cooperative nodes.

Mershad et al. (2012) focused on routing; namely the author exploited RSUs to route packets between any source and destination in the VANET. The author compared this scheme to existing solutions and proves the feasibility and efficiency of the scheme in terms of query delay, packet success delivery ratio, and total generated traffic.
Xiong et al. (2012) introduced an efficient and trustworthy conditional privacy-preserving communication protocol for VANETs based on proxy re-signature. The protocol is characterized by the Trusted Authority (TA) designating the RSUs to translate signatures computed by the OBUs into one that are valid with respect to TA’s public key.

Salem et al. (2012) presented an efficient non-interactive secure protocol preserving the privacy of drivers in vehicle-to-roadside (V2R) communication networks with the ability of tracing malicious drivers only by a Third Trusted Party (TTP), who was considered to be fully reliable and yield these complex needs based on symmetric cryptographic algorithms. A powerful key revocation scheme was also described here.

Chen et al. (2013) concentrates on security solutions for the VANETs in the cases of emergency communication, where the communication infrastructures are not existent always. Expedite Privacy-preserving Emergency Communication (EPEC) scheme was proposed for the vehicles to be able to securely connect with others in the neighborhood area even during the times of destruction of the trusted infrastructures by the disaster.

Wu et al. (2013) had set up an evolutionary game model to formulate the competition among vehicles in the same community and different communities with bounded rationality in VANET for RSU access problem. Zhu et al. (2013) introduced a traceable distributed pseudonym management technique in VANETs. In this scheme, a blind signature method is employed to accomplish strict isolation of issuance and tracking. The distributed tracking protocol is introduced in order to improve the tracking robustness that is based on the enhanced scheme for shared RSA keys generation. An effective pseudonymous authentication technique is presented in order to minimize the communication overhead.
Galaviz-Mosqueda et al. (2014) introduced a Reliable Low-overhead Multihop Broadcast (RLMB) protocol is proposed to address the well-known broadcast storm problem. The proposed RLMB uses a point-to-zone link evaluation approach to reduce the redundant broadcast and the hello messages rate dependency.

Wang et al. (2014) proposed a new Location-based Distributed Group Key Agreement (LDGKA) scheme for VANETs. Here a hybrid approaches in which members in the vehicular ad hoc network from various logic groups in the same region. Within each group, virtual key tree model is employed so that the rekeying operation can be efficiently carried out when members leave or join.

Lee et al. (2014) analyzed the characteristics of vehicles’ mobility and analyze them. With the navigation information, the author discussed mobility management scheme based on route prediction in VANET. Handoffs with intra highway mobility were managed locally and transparency was provided to CHs, while global mobility is managed with Mobile IPv6.

Chim et al. (2014) studied about a navigation scheme which makes use of the online road information gathered by a VANET in order to lead the drivers to needful destinations in a real-time and distributed way. This scheme has the benefit of making us of realistic road conditions in order to calculate a better route and simultaneously, the information source can also be authenticated properly. In order to defend the privacy of the drivers, the query (destination) and the driver who inputs the query are assured to be non-connectable to any party inclusive of the trusted authority.

Chi et al. (2014) introduced a new practical and secure architecture for vehicular black-box image communication in a VANET environment.
Since black-box images show more detailed descriptions of the vehicle and the ambient conditions, more reliable traffic information and analysis can be provided. This model minimizes the communicational and computation overheads by GPS based-key frame extraction and communication technique.

1.4 MOTIVATION OF THE RESEARCH

Vehicular transportation is the prominent mode of transportation which accounts for about 60% of overall transportation modes. Advancements in technology led to the development of automated vehicles and increased safety related applications. Vehicular Ad Hoc Networks (VANETs) are a special type of Mobile Ad hoc Networks (MANET), in which vehicles are simulated as mobile nodes to provide the protection, comfort and efficient driving.

Direct efforts could be exerted on the safety and life of users in a case of emergency telegraph message such as the surrounding road conditions or Taxi accidents differently from general multi-media information.

The main research areas in VANET are routing, broadcasting, traffic control, congestion control, security, etc. Security is also a major issue in the routing protocols to check the malicious attacks from the malicious drivers.

Many routing protocols have designed to implement MANET and in VANET. Topology based routing protocols are useful for implementing VANET but it undergoes several problems like frequent topology change and link disruption. The best method for routing in VANET is to be proposed to maximize the network performance and data packet transmission. However the most of the available routing algorithms does not satisfy the security
requirements such as authentication, authorization, and Data consistency, Data Consistency, Confidentiality, Integrity, Availability, Non Repudiation, Privacy and Anonymity. There should be a kind of routing available that can be approached and in case there is low network density. Behavior of the driver also considered to design the delay-bounded routing protocols.

1.5 OBJECTIVES OF THE RESEARCH

- The goal of this work is to design novel routing approaches for secure communication between V2V which significantly focuses on the issues such as Message Transferring, Delay, Network Performance, Throughput and Security.

- To develop a novel approach to improve the probability of successful packet data communication employing relative mobility. Moreover, the unicasting and multicasting routing schemes using long and short range communications have to be developed in VANET for both Cooperative and non-Cooperative schemes.

- To improve the packet delivery ratio by means of making use of the free time slots for the purpose of retransmission of packet when it is unsuccessful because of poor channel condition.

- To develop a VANET based approach to transfer messages for the purpose of providing a safe, secure and privacy based Taxi service.
1.6 RESEARCH CONTRIBUTION AND METHODOLOGY

The overall architecture is illustrated in Figure 1.1. It has been observed that major limitations of the existing techniques are due to the conventional approaches. Thus to overcome the existing shortcomings, new approaches are proposed in the present research work.

Routing protocols are assumed as a critical dilemma that needs to be tackled in VANET, particularly in a sparse environment, by designing an efficient routing mechanism that impacts on enhancing network performance. In terms of disseminating messages to a desired destination, balancing the generated packet (overhead) on the network and increasing the ratio of packet delivery within the limited time delay. MAC protocols are employed to assist in the performance improvement of routing. Many schemes are exploited as parameters for enhancing the performance of the protocols.

![Figure 1.1 Stages in performance optimization](image)

**Figure 1.1 Stages in performance optimization**
The proposed Cooperative scheme with MAC is referred as Cooperative Ad Hoc-Medium Access Control (CAH-MAC), where the neighbouring nodes are assisted by means of utilizing free time slots, for the purpose of retransmission of a packets when it is unsuccessful by poor channel conditions. Network life time is achieved by discovering multicast path that attempts to reduce the variation energy of all the nodes. Hence this scheme increases the probability of packet transmission utilizing relative mobility and thereby improves the network throughput. Hence VANET, used to provide communication among vehicles and between vehicles to RSU, MAC is designed to send information from source to destination.

The MAC protocols implemented in taxi services are used for reducing the routing issues such as reducing delay and improving the PDR. The security issues are also considered during the real time implementation of protocols. The VANET will be supported by some fixed infrastructure that assists with certain services for feasible assumption due to restricted node movement. The fixed infrastructure will be deployed at critical locations like slip roads, service stations, dangerous intersections or places well-known for hazardous weather conditions. To handle this problem, a clustering based Cooperative scheme manages channel access and schedule transmission within the cluster for ensuring reliable long range communication. The simulation results indicate that the performance of the algorithm proposed is better in comparison with the existing algorithm and provides a satisfactory trade-off between computational complexity and detection performance.

1.7 ORGANIZATION OF THESIS

The Research is carried out and its findings are presented in six chapters and are delineated in the Approach Flow Diagram as in Figure 1.2.
INVESTIGATIONS ON IMPROVING THE PERFORMANCE OF THE VEHICULAR ADHOC NETWORK

- Analysis of Existing Hash Message Authentication Code (HMAC)
- Analysis of Existing Dijkstra’s Architecture of AODV & IEEE 802.11 P for VANET
- Analysis of Existing Intelligent VANET using Wi-Fi IEEE 802.11 and Wi-MAX IEEE 802.16 wireless

- Development of HCA with long term evolution Resource Block Scheme
- Development of Enhanced Multicast Algorithm with CAH-MAC
- Development of Cluster based New Secure Message Transferring in Taxi Service for VANET

- Validation of Simulation Results of the Clustering Schemes
- Performance Comparison of Proposed and Existing Approaches using various parameters like
- Validation of Simulation Results
- Enhancing Privacy and security

VANET Performance Optimization

Figure 1.2 Approach flow diagram
Chapter 1 briefly focuses the review of literature which necessitated the scope of the present research. The main objectives and research contribution are also presented in this chapter. The performance analysis of VANET based on clustering schemes, the details about the long range and short range communication with HCA are presented in Chapter 2.

Chapter 3 discussed about the Enhanced Multicast Algorithm for Mobile ADHOC Using Cooperative ADHOC MAC in VANET. Simulation results showed that, how the proposed MAC protocol reducing the energy consumption, delay, improves the network lifetime, increasing throughput is also explained.

Chapter 4 discussed about new security features for the purpose of reducing the possibility pertaining to taxi crimes and also to protect the privacy of taxi passengers. Authentication mechanisms consist of digital signatures which showed the evidence of most appropriate scheme regardless of high overhead.

A Comprehensive summary obtained from this research along with future scope of the work is presented in Chapter 5 which functions as a suitable conclusion.