Volume 7, Issue 2, February 2017 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

A Novel Region Based Multipath Routing Algorithm for Vehicular Ad-hoc Networks

Bhanupriya

Department of Computer Science Engineering, DAV University,
Jalandhar, Punjab, India

DOI: 10.23956/ijarcsse/V7I2/0136

Abstract: Multimedia communication is a desirable medium to provide traffic information, news, advertisements, etc. to people on-the-road. Due to the high mobility and dynamic topology of Vehicular Ad-hoc Network (VANET) an open question is whether it is feasible to support video streaming services using license-free wireless communications between vehicles and road-side-units. In VANET, safety application and user Internet accessing related application are expected to be supported. VANET is an enhanced form of Mobile Ad-hoc Network (MANET), where communicating nodes are replaced by moving vehicles. VANETs promise many improvements in terms of accident avoidance and in better utilization of roads and resources such as fuel and time. In this paper, propose Region based Multipath using clustering routing algorithm (RMCRA) for inter cluster communications that is clustering-based scheme is applied for data transmission in VANET in which a cluster head (CH) selection and static cluster server taking density of road-network and traffic as the parameter. In this paper RMCRA proposed technique compare with existing technique Locations based Multipath Flooding (LMF) using four parameters i.e traffic sent and received, throughput, packet delay variation and packet dropped. Nodes of vehicular ad hoc network do not pose power challenges as posed by nodes of mobile ad hoc network. Hence, new clustering algorithms are developed for vehicular ad hoc network which aim for stable and effective clusters in the network.

Keywords- VANET, RMCRA, LMF, Clustering, throughput, packet delay variation and packet dropped.

I. INTRODUCTION

Many people lose their life and/or are injured due to accidents or unexpected events taking place on road networks. Besides traffic jams, these accidents generate a tremendous waste of time and fuel. Undoubtedly, if the vehicles are provided with timely and dynamic information related to road traffic conditions, any unexpected events or accidents, the safety and efficiency of the transportation system with respect to time, distance, fuel consumption and environmentally destructive emissions can be improved. VANETs are self-organizing networks established among vehicles equipped with communication facilities. The equipped vehicles are network nodes so that each node can act as the source of data, destination for data and a network router[1].

Vehicular Ad Hoc Networks have recently emerged as an effective tool for improving road safety through propagation of warning messages among the vehicles in the network about potential obstacles on the road ahead. VANETs and MANETs have some similar characteristics such as short range of transmission low bandwidth, omni-directional broadcast and low storage capacity. Fast changing network topology and varying communication conditions pose a great challenge for routing protocols being used in VANETs. For using routing protocols in VANET they should be robust, reliable, minimize latency and network load. For achieving more realistic results, we developed mobility models that reflect the movement of vehicles in city scenarios and evaluated topology based protocols performance. A Vehicular Ad-hoc Network (VANET) [1] facilitates communication between vehicle to vehicle, vehicle to infrastructure and infrastructure to infrastructure. Vehicular network is a specific type of mobile ad hoc network (MANET) where the mobile nodes are replaced with vehicles equipped with on board unit (OBU) communication devices. Now-a-days, road traffic activities are one of the most important daily routines worldwide. So VANET is one of application to solve this problem. In VANET, vehicles act as nodes which can exchange data between each other without any infrastructure network establishment.

In a Vehicular Ad-Hoc Network [2], the vehicles communicate with each other using Short Radio Signals e.g. DSRC, with a range of 1 km. Routers used known as roadside unit works as a router between vehicles and other units on the network ensuring communication. Each vehicle consists of an OBU (On Board Unit), which links the vehicle with RSU via DSRC radios signals. Roadside unit is a computing device located on the roadside that provides connectivity support to passing vehicles.

1.1 Architecture of VANET

According to this architecture each vehicle composed of two types of units: (i) an on-board unit (OBU) and (ii) one or more application unit(s) (AUs). An OBU is a device in the vehicle having communication capabilities, including at least a short range wireless communication device dedicated for road safety while an AU is a device executing a single or a set of applications while making use of the OBU's communication capabilities. AU can be a portable device such as a laptop or PDA that can dynamically attach to (and detach from) an OBU. OBUs of different vehicles form a mobile ad hoc network (MANET) [3]. OBUs and road side units together will form ad-hoc network domain, road side units are stationary infrastructures fixed alongside road. An RSU can be attached to an infrastructure network, which in turn can be connected to the Internet. RSUs [4] can also communicate to each other directly or via multi-hop. RSUs allow OBUs to access infrastructure and internet. VANET can be implemented through integration between operators, providers and governmental authority. Architecture of network must allow communication among vehicles [5] and fixed road side infrastructures. One of such architecture is proposed within C2C-CC [6] [7]. Figure 1. illustrates this reference architecture [7]. In a Vehicular Ad-Hoc Network, the vehicles communicate with each other using Short Radio Signals e.g. DSRC (5.9), with a range of 1 km [8]. This is an Ad-Hoc communication which makes sure free movement of wireless vehicles in free road environment.

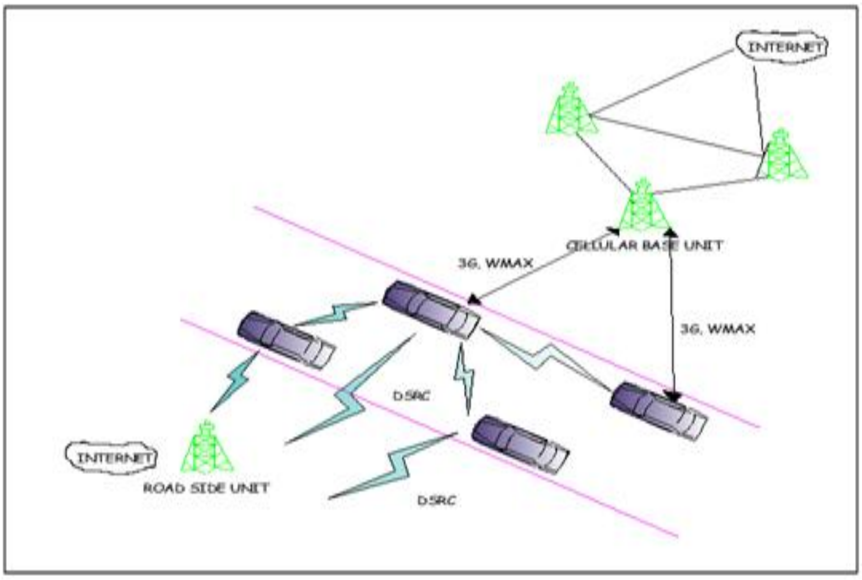

Figure 1: VANETs Architecture

1.2 Routing Protocols

Routing is a mechanism to establish and to select a specific path in order to send data from source to destination. There are various routing algorithm designed for ad-hoc networks.

1.2.1 Topology Based

Topology based routing protocols use link's information within the network to send the data packets from source to destination.

Proactive Routing

These types of protocols [9] are table based because they maintain table of connected nodes to transmit data from one node to another and each node share its table with another node. Different types of proactive routing protocols are Destination Sequence Distance Vector Routing (DSDV), Optimized link state routing (OLSR), Fisheye State Routing (FSR).

Destination Sequence Distance Vector Routing [10] is a table driven routing protocol for MANET based on Bellman-Ford algorithm. Every node in the network share packet with its entire neighbour. Packet contain information such as node's IP address, last known sequence number, hop count.

Optimized link state routing (OLSR) [12] protocol is an optimization of the classical link state algorithm. In OLSR every node use "HELLO" message to know about their neighbours. Flooding of message to sense the neighbour node is very expensive process therefore to reduce the cost of flooding to sense neighbours OLSR use multipoint relay (MPR) technique.

Fisheye State Routing (FSR) [13] uses the fisheye technique proposed by Kleinrock and Stevens. In FSR link state packets are not flooded but it allows sharing link state message at different intervals for nodes within different fisheye scope distance and thus reducing the size of link state message size.

Reactive Routing

It is also called On Demand routing because it establish a route to destination whenever a node has something to send thus reducing burden on network. Reactive routing have route discovery phase where network is flooded in search of destination. Different types of Reactive routing protocols are AODV, DSR, and TORA.

Ad Hoc On Demand Distance Vector (AODV) [14] is an reactive routing protocol which capable of both unicast and multicast. In AODV, like all reactive protocols, topology information is only transmitted by nodes on-demand. When source has something to send then initially it propagates RREQ message which is forwarded by intermediate node until destination is reached. A route reply message is unicasted back to the source if the receiver is either the node using the requested address, or it has a valid route to the requested address.

Dynamic Source Routing (DSR) [15] is also a reactive routing protocol it uses source routing. When a node has something to send it broadcast a rout request message to its 1-hop neighbourhood if receiver is not a valid destination then it forward the updated RREQ message in which they add their address in this way all the intermediate node update RREQ message with their address and thus message along with updated route reach to destination. When RREQ reach to destination it returns a route reply message to source.

Temporally Ordered Routing Algorithm (TORA) [16] it belongs to a class of algorithm called the link reversal algorithm. TORA attempt to build DAG (Directed Acyclic Graph) towards destination is based on the height of the tree rooted at the source. TORA performs three tasks.

- Creation of a route from a source to destination
- Maintenance of rout
- Removing route if it is no longer valid.
- Hybrid Routing Protocol

To make routing more scalable and efficient Hybrid routing combines the characteristics of both reactive and proactive routing protocols. Mostly Hybrid Routing protocols are zone based i.e. whole network is divided into number of zones.

Zone Routing Protocol (ZRP) [17] is based on the concept of zone. Each routing zone has radius ‘p’ which mean a zone include all the nodes whose distance from node is at most ‘p’ hops. Nodes inside the zone whose minimal distance from centre node is ‘p’ hops are known as peripheral nodes and rest are known as interior nodes. Proactive routing protocols is used to route packet within a zone which is known as Intra-Zone routing protocol whereas reactive routing protocol is used to route packet outside zone which is termed as Inter-Zone routing protocol.

1.2.2 Vehicle Based Clustering Schemes

Protocols using the direction of vehicles for selection of clusters and cluster heads are classified under vehicle based clustering schemes.

Location based Multipath Flooding (LMF) algorithm

This is an approach for cluster based routing algorithm [10] for hybrid mobility model in regulating the vehicular traffic. This approach uses a new hybrid mobility model combining random waypoint and group mobility model using static and dynamic sources and a novel cluster based routing algorithm. It transmit the real time updated information and maintain long link duration to improve the data delivery ratio, and also suitable for vehicles with variable mobility [4].

Working of LMF

In this model, a fixed number of dynamic and static sources are known to every vehicle of the system, and a static source is always available for processing large amount of data. In this integrated approach the information pertaining to traffic is maintained in both sources, lesser time in dynamic source and longer duration in static sources for future purpose. If the distance between two cluster head nodes is found to be less than the threshold, the cluster with fewer members is dismissed to reduce communication overheads and its members join other clusters. During high mobility conditions the process of re-clustering increases the communication cost. Locating the position of nodes, relative speed predictions and effective communication distance between nodes according to mobility are dealt in our approach.

Cluster based routing

Basically static and dynamic clustering combines the features of together. Static clusters are formed around the static sources located at the road signals, street corners and congested places known as static cluster-head [22]. However buses are chosen as dynamic sources in our algorithm, having the predefined path and time chart to handle the high mobility situations known as dynamic cluster-head. Hierarchical clustering creates a layering environment that poses some of the main challenges in such ad hoc networks. Top layer consists of static cluster-head, middle layer consists of dynamic cluster-head and lower layer consists of ordinary vehicles. Because of highly dynamic vehicles network topology also changes which affects the performance of the network and also invokes protocol mechanisms to react to such dynamics. Mobility awareness deals with sudden changes in topology by responding against malfunctions in routing and mobility metrics are considered for cluster construction in order to form a stable cluster structure thereby decreasing its influence on cluster topology.

II. RELATED WORK

In this section, we give a brief discussion of work related to Vehicular Ad-hoc Network. The detailed literature surveys is done, to get preliminary knowledge and search scope of investigation, to design secure and reliable AAGS is explained in this paper. There are numerous work carried in the field of VANET using clustering. Many models, schemes and techniques are proposed for VANET in clustering.

Zhang et al. [12] Vehicular Sensor Networks (VSNs) have emerged as a new application to revolutionize the human driving experiences and traffic flow control systems. With the proposed scheme, since identity-based cryptography is employed in generating private keys for pseudo identities, certificates are not needed and thus transmission overhead can be significantly reduced. Proposed IBV scheme can improve the system performance by verifying multiple message signatures at once. Their scheme has also addressed the identity privacy and traceability issues in vehicular networks. IBV scheme’s performance was better than ECDSA and BLS in terms of signature verification delay and communication overhead.

Zhang et al. [13] the emerging requirement of today's world and advanced technology has given rise in the field of location privacy of the mobile users. To the best of our knowledge, this is the first developed anonymous mutual authentication scheme that can achieve provable link-layer, forward-secure location privacy. To improve efficiency, a Preset in Idle technique is exercised in the proposed scheme, which is further compared with a number of previously reported counterparts through extensive performance analysis.

Sun et al. [14] they propose a security system for VANETs to achieve privacy desired by vehicles and traceability required by law enforcement authorities, in addition to satisfying fundamental security requirements including authentication, non repudiation, message integrity, and confidentiality. Moreover, they propose a privacy-preserving defense technique for network authorities to handle misbehavior in VANET access, considering the challenge that privacy provides avenue for misbehavior. The proposed system employs an identity-based cryptosystem where certificates are not needed for authentication. They show the fulfillment and feasibility of their system with respect to the security goals and efficiency. Long Huang et al. [15] they introduce an anonymous batch authenticated and key agreement (ABAKA) scheme to authenticate multiple requests sent from different vehicles and establish different session keys for different vehicles at the same time. In vehicular ad hoc networks (VANETs), the speed of a vehicle is changed from 10 to 40 m/s (36–144 km/h); therefore, the need for efficient authentication is inevitable. Compared with the current key agreement scheme, ABAKA can efficiently authenticate multiple requests by one verification operation and negotiate a session key with each vehicle by one broadcast message. Elliptic curve cryptography is adopted to reduce the verification delay and transmission overhead. In the analytical analysis, they have elaborately evaluated ABAKA with current standard ECDSA schemes and other batch-based schemes in terms of verification delay and transmission overhead, as well as the verification cost for rebatch verifications. Chim et al [16] they proposed two secure and privacy enhancing communications schemes for VANETs to handle ad hoc messages and group messages for inter-vehicle communications. They are also the first to propose a group communications protocol to allow known vehicles to form a group for secure communications. Jinn Horng et al [17] SPECS provided a software-based solution to satisfy the privacy requirement and gave lower message overhead and higher successful rate than previous solutions in the message verification phase. SPECS also presented the first group communication protocol to allow vehicles to authenticate and securely communicate with others in a group of known vehicles. They show that SPECS is vulnerable to the impersonation attacks for ad hoc messages and group messages. To handle ad hoc messages, we describe how a vehicle as an attacker can act arbitrary vehicle to generate valid signatures for arbitrary message. To deal with group messages, they show how a malicious vehicle in a group can counterfeit another group member to send fake messages in the group communication. After that they have improved scheme to remedy the above weaknesses of SPECS. Their scheme not only satisfies the privacy preserving but also considers the related security issues such as message integrity and authentication, and collision resistance. Moreover, their scheme enables the trust authority to retrieve and revoke the real identity of arbitrary vehicle from any message signature, such that conditional privacy can be achieved.

Chi Lee et al. [18] they proposed an improved authentication of the batch scheme based on bilinear pairing to make VANET more secure, efficient. A malicious driver can broadcast wrong information to mislead other drivers and repudiate the behavior when the traffic manager traces him/her by his/her signature. Zhu et al. [19] they present an efficient privacy preserving authentication scheme based on group signature for vehicular ad hoc networks (VANETs). Group signature is widely used in VANETs to realize anonymous authentication, the existing schemes based on group signatures suffer from long computation delay in the certificate revocation list (CRL) checking and in the signature verification process, leading to high message loss. As a result, they cannot meet the requirement of verifying hundreds of messages per second in VANETs. In their scheme, they first divide the area into several domains, in which roadside units (RSUs) are responsible for distributing group private keys and managing vehicles in a localized manner. Then, they use a hash message authentication code (HMAC) to avoid time consuming CRL checking and to ensure the integrity of messages before batch group authentication. At last, they adopt cooperative message authentication among entities, in which each vehicle only needs to verify a small number of messages, thus greatly alleviating the authentication burden. Their scheme is more efficient in terms of authentication speed, while keeping conditional privacy in VANETs.

Varshney et al. [20] an algorithm in order to overcome these network attacks via low message passing and try to reduce the bandwidth at the time of authentication. An algorithm which has been proposed is secured, cost effective, consuming sufficient bandwidth and give better performance. After analyze the research work done and they made a comparison with the existing work. The result of the comparison shows that the protocol was better in the basis of security, performance and cost. Fan I et al. [21] Vehicular ad hoc networks (VANETs) can enhance the safety and efficiency of road traffic. In this paper, they have presented a strong privacy preserving protocol with efficient tracing method based on the blind signature technique. Not only does their scheme satisfy all security requirements such as message integrity, authentication, non-repudiation, traceability, Safety message unforgeability, and safety message unlinkability, but also it preserves vehicle anonymity against roadside units (RSUs). In addition, considering the real environment, scheme was more practical and efficient and suitable to VANETs. Zhou et al. [22] If a new vehicle node wants to access the VANET, we need to validate the new vehicle node to improve the security of the VANET. They propose a security authentication method based on trust evaluation. Firstly, when a vehicle wants to access the Internet through the roadside base station, they evaluate the access node by employing the direct trust evaluation. Based on the historical security event record, the direct security degree of the new vehicle node is determined. When a group of vehicles form a wireless network to communicate information with each other, they adopt the indirect trust evaluation mechanism to evaluate the new vehicle node.

Liu and Khorashadi [23] discuss the flexibility of VGSim in adopting different mobility models and also present simulation results that empirically validate the modified mobility model that is implemented. They discussed how VANET applications can be easily modelled in VGSim, and demonstrate this by using two important applications like Accident Alert and Variable Speed limit. The application development process is also easy and suitable for building multiple distributed VANET applications that can execute concurrently. Additionally, since it executes as a standalone Java application using the efficient JiST/SWANS package, it is more resource efficient than approaches that integrates existing network and traffic simulators. Girinath and Selvan [24] the scenario and the network are modelled and investigated through extensive simulations using ns-2 simulator to study the performance in terms of cluster construction. The clustering schemes so proposed works well in a dynamic environment because it does not require frozen period of motion for initial cluster formation.

Hence, it is more suitable for urban environments where vehicle change their speed and direction frequently. They tried to group vehicle nodes with low relative mobility with respect to each other into the same cluster. Thus the impact of vehicle movements on cluster topology may be minimized.

III. SIMULATION ENVIROMENT

After going through all the techniques of clustering and having a need to have stable and efficient communication in VANET of lower packet delivery delay, load balancing between the nodes, reducing overhead in performing clustering, trusted communication links between the nodes through clusters and managing a database at the Centre Server (CS) for maintaining information for reference purposes. A city should be divided into specific areas forming static clusters. Cluster heads are static like stationary objects like any fixed infrastructure or any road side units in every cluster. This scheme reduces cluster forming overhead. Dynamic clustering and cluster head selection are avoided so as to avoid confusion and less lifespan of cluster heads in dynamic clustering hence, resulting in reduced load balancing among the nodes of a cluster network.

3.1 Performance Parameters

The right choice of performance evaluation criteria for the characterization of vehicular ad-hoc network represent one of the key issues for the effective design of high performance network. Some VANET performance evaluation metrics are as following:

Data Dropped-The total size of higher layer data packets (in bits/sec) dropped by all the WLAN MACs in the network due to:

a) full higher layer data buffer, or
b) the size of the higher layer packet, which is greater than the maximum allowed data size defined in the IEEE 802.11 standard.

Packet Delay Variation-Variance among end to end delays for voice packets. End to end delay for a voice packet is measured from the time it is created to the time it is received.

Throughput- Throughput is defined as; the ratio of the total data reaches a receiver from the sender. The time it takes by the receiver to receive the last message is called as throughput. Throughput is expressed as bytes or bits per second (bytes/sec or bits/sec). Throughput (bits/sec) is represented mathematically as

$$\boldsymbol{Throughput} \frac{= \boldsymbol{Number\ of\ delivered\ packet \times Packet\ size \times 8}}{\boldsymbol{Total\ duration\ of\ simulation}}$$

Routing Traffic Sent and Received- It refers to the total amount of packet sent and received in the entire network.

Traffic sent-Average number of packets per second submitted to the transport layers by all voice applications in the network.

Traffic received- Average number of packets per second forwarded to all Voice applications by the transport layers in the network.

3.2 Proposed Scenario

Only cluster will keep the record of every vehicle that is entering and exiting the cluster. This all information is collected by each cluster head of every cluster that is entering and exiting the cluster. This information is immediately passed to Centre Server (CS) where database could be maintained of whole of the city. Database of daily local vehicles could also be maintained for a city like for city buses, private cars of families living in that particular city Buying and selling information is also updated at the center server from time-to-time. Therefore, permanent VID could also be assigned with a unique vehicle number and only checking-inn function could be performed for a vehicle entering and exiting the cluster. Therefore, record of foreign cars can be differentiated which could be efficiently maintained for future purposes. Simulation parameters table shown in table 1.

Table 1.1: Simulation Parameters

Statistic	Value
Propose Model	RMCRA
Traffic Type	TCP

Simulator	NS2
Transmission Range	200m
Routing Protocols and Cluster	AODV and Cluster Head
802.11 data rate	11 Mbps
Nodes	30
Simulation Time	300 s
Existing Model	LMF
Application Traffic	FTP and HTTP
Channel Type	Wireless channel
Performance Parameter	Data Dropped, Throughput, Packet Delay, Traffic

IV. RESULTS AND DISCUSSION

From the above mentioned simulation statistic value and according to all performance parameters, it can be concluded that the RMCRA technique is far better than existing technique LMF. The statistical results are mentioned in the table below as:

Table 1: Overall Result Analysis

Parameters	*No. of Nodes*	*Average Number of Hops Per Route*	*Average Route Discovery Time (in Second)*	*LMF (Existing Technique)*	*RMCRA (Proposed Technique)*
Data Dropped (Bits/Sec)	0	0	0.06	0	0
	40	1	0.22	4.25	2.4
Throughput (Kb/Sec)	0	0	0.05	0	0
	40	1.001	0.16	72.06	74.08
Packet Delay Variation (sec)	0	0	0.06	0	0
	40	1.001	0.129	8.4437	6.0234
Routing Traffic Sent and Received (Packets/sec)	0	0	0.09	0	0
	40	1	1	4.5	4.4

V. CONCLUSION

Recently, as an alternative to the IEEE 802.11p based VANET, the usage of cellular technologies has been investigated. In this paper a new advance algorithm for Region based Multipath using clustering routing algorithm (RMCRA) are developed for vehicular ad hoc network which aim for stable and effective clusters in the network. Vehicular ad hoc network protocols using static geographic clustering scheme is proposed which uses static cluster server, cluster head and clusters. Hence, they reduce the cluster formation overhead. AODV protocol is used to perform routing as maintaining table require resources, overhead which sometimes also create redundancy which creates problems while smooth functioning of the network. Throughput is maximum as connectivity is maximum; Packet drop is minimum because clustering enables dedicated communication Delay is reduced Packet drop is zero and traffic is less produced. On the basis of this techniques future work could be extended the proposed algorithm can be implemented to form a clustering protocol for routing purposes.

REFERENCES

[1] Sanjay Batish, Alka Jindal, Prateek Murli, Amardeep Dhiman, "Analysis Of Security Attacks In VANET", International Journal of Advances in Computer Science and Communication Engineering (IJACSCE) Vol 2 Issue I (March2014).

[2] Mohamed Salah Bouassida, Gilles Guette, Mohamed Shawky, and Bertrand Ducourthial, "Sybil Nodes Detection Based on Received Signal Strength Variations within VANET", International Journal of Network Security, Vol.9, No.1, pp.22-33, July 2009 .

[3] Mina Rahbari and Mohammad Ali Jabreil Jamali, "Efficient Detection Of Sybil Attack Based On Cryptography In VANET", International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.6, November 2011.

[4] [Online].Available:*http://techsoupforlibraries.org/planning-for-success/ networkin g-and-security/tools/wired-for-success -a-tool-for-understanding-your-w.*

[5] McCullagh Noel, Barreto S.L.M. Paulo, Libert Benoˆıt and Quisquater Jacques Jean, "Efficient and Provably-Secure Identity-Based Signatures and Signcryption from Bilinear Maps", International Association for Cryptologic Research, PP.515-532 2005.

[6] Cheon Hee Jung, Kim Yongdae and Yoon Jin Hyo, "A New Id-Based Signature With Batch Verification", Information Center for Mathematical Sciences Volume 8, Number 1, June, 2005, Pages 119-131 .

[7] Sun Jinyuan, Zhang Chi and Fang Yuguang, "An Id-Based Framework Achieving Privacy and Non-Repudiation In Vehicular Ad Hoc Networks", IEEE, PP.4244-1513 2007.

[8] Lin Xiaodong, Sun Xiaoting, Ho Pin-Han and Shen Xuemin, "GSIS: A Secure and Privacy-Preserving Protocol for Vehicular Communications", IEEE Transactions On Vehicular Technology, Vol. 56, No. 6, November 2007.

[9] Raya Maxim and Pierre Hubaux Jean, "Securing vehicular ad hoc networks", Journal of Computer Security Vol.15 PP.39–68 2007.

[10] Zhang Chenxi, Lin Xiaodong, Lu Rongxing, Ho Pin-Han and Shen Xuemin (Sherman), "An Efficient Message Authentication Scheme for Vehicular Communications", IEEE Transactions On Vehicular Technology, Vol. 57, No. 6, November 2008.

[11] Zhu Haojin, Lin Xiaodong, Lu Rongxing, Ho Han Pin, Shen (Sherman) Xuemin , "AEMA: An Aggregated Emergency Message Authentication Scheme for Enhancing the Security of Vehicular Ad Hoc Networks", IEEE Communications Society subject matter experts for publication in the ICC 2008 proceedings.

[12] Zhang Chenxi, Lu Rongxing, Lin Xiaodong, Ho Pin-Han, and Shen Xuemin (Sherman), "An Efficient Identity-based Batch Verification Scheme for Vehicular Sensor Networks", IEEE Communications Society subject matter experts for publication in the IEEE INFOCOM 2008 proceedings.

[13] Zhang Chenxi, Lu Rongxing, Lin Xiaodong, Ho Pin-Han, and Shen Xuemin (Sherman), "A Novel Anonymous Mutual Authentication Protocol With Provable Link-Layer Location Privacy", IEEE Transactions On Vehicular Technology, Vol. 58, No. 3, March 2009.

[14] Sun Jinyuan, Zhang Chi, Zhang Yanchao, and Fang Yuguang, "An Identity-Based Security System for User Privacy in Vehicular Ad Hoc Networks", IEEE transactions on parallel and distributed systems, vol. 21, no. 9, september 2010.

[15] Long Huang Jiun, Yao Yeh Lo, and Yu Chien Hung, "ABAKA: An Anonymous Batch Authenticated and Key Agreement Scheme for Value-Added Services in Vehicular Ad Hoc Networks", IEEE Transactions On Vehicular Technology, Vol. 60, No. 1, January 2011.

[16] Chim, TW; Yiu, SM; Hui, LCK; Li, VOK, "SPECS: Secure and privacy enhancing communications schemes for VANETs", Attribution 3.0 Hong Kong License Vol. 9, No. 2, PP. 189-203 2011.

[17] Jinn Horng Shi, Feng Tzeng Shiang, Pan Yi, Fan Pingzhi, Wang Xian, Li Tianrui, and Khan Khurram Muhammad, "b-SPECS+: Batch Verification for Secure Pseudonymous Authentication in VANET", IEEE 2013.

[18] Chi Lee Cheng, Ming Lai Yan, "Toward a secure batch verification with group testing for VANET", Springer 20 January 2013.

[19] Zhu Xiaoyan, Jiang Shunrong, Wang Liangmin, and Li Hui, "Efficient Privacy-Preserving Authentication for Vehicular Ad Hoc Networks", IEEE transactions on vehicular technology, vol. 63, no. 2, february 2014.

[20] Varshney Neeraj, Roy Tumpa, Chaudhary Niharika, "Security Protocol for VANET by Using Digital Certification to Provide Security with Low Bandwidth", International Conference on Communication and Signal Processing, April 3-5, 2014, India .

[21] Fan I Chun, Sun Zhe Wei, Huang Wei Shih, Juang Shenq Wen and Huang Jia Jheng, "Strongly Privacy-Preserving Communication Protocol for VANETs", Ninth Asia Joint Conference on Information Security 2014.

[22] Zhou Ao , Li Jinglin, Sun Qibo, Fan Cunqun, Lei Tao and Yang Fangchun, "A security authentication method based on trust evaluation in VANETs", Springer 2015.

[23] Shiang-Feng Tzeng, et.al, "Enhancing Security and Privacy for Identity-based Batch Verification Scheme in VANET", IEEE Transaction on Vehicular Technology 2015.

[24] https://engineering.purdue.edu