IOSR Journal of Electronics and Communication Engineering (IOSR-JECE)
e-ISSN: 2278-2834,p- ISSN: 2278-8735.Volume 9, Issue 2, Ver. III (Mar - Apr. 2014), PP 23-30
www.iosrjournals.org

A Novel Approach for Secured Data Transmission in VANET through Clustering

S.Bhuvaneshwari[1], G.Divya[2], K.B.Kirithika[3], S.Nithya[4]
[1, 2, 3]*(Student, Dept of ECE, KPR Institute of Engineering and Technology, Tamil Nadu, India)*
[4]*(Assistant Professor, Dept of ECE, KPR Institute of Engineering and Technology, Tamil Nadu, India)*

Abstract:*Vehicular Adhoc Network (VANET) is one of the emerging and promising technologies of our near future which provides Network on Wheels (NOW). It provides safety and other applications to the drivers as well as passengers. It has become a key component of the Intelligent Transport System (ITS). VANET is the special type of MANET (Mobile Ad Hoc Networks) where the mobile nodes are vehicles that move on roads at very high speed following traffic rules; they provide communication between vehicle and vehicle (V2V) and Vehicle and Road side infrastructural unit (V2I).An attempt has been made earlier to create a new cluster model for efficient communication among the VANET nodes.In this paper a new clustering model has been created along with security algorithms so that the communication among the VANET nodes can be made in more efficient manner.*

Keywords: *Clustering, Road Side Units (RSU), HARDY function, Cluster head, Registration, Session Management*

I. INTRODUCTION

Recently there has been increasing interest in exploring computations and communication capabilities in transportation system. Many automobiles manufacture started to equip GPS, digital map and communication interface with new vehicles. Exiting cars can easily upgrade with the rapid advance of information technology. The increasing demand of wireless communication and the need of new wireless devices have tend to research a self organizing, self healing network without the interference of centralized or pre established infrastructure. The networks with the absence of any centralized infrastructure are called ad hoc networks [1].

VANETs are special case of MANETs. It is composed of vehicles that are equipped with wireless communication devices, positioning systems, and digital maps. VANETs allow vehicles to connect to roadside units (RSUs), which may be interconnected witheach other through a high-capacity mesh network. The key differences as compared to MANET environment are following: 1) Restricted mobility constraints 2) Extremely high mobility and time-varying vehicle traffic density 3) Most of the vehicles provide sufficient computational and power resources, thus eliminating the need for introducing complicated energy-aware algorithms. 4) Vehicles will not be affected by the addition of extra weight for antennas and additional hardware. Due to high mobility of vehicle moving on the roads, protocols developed for general mobile ad-hocnetwork are unsuitable for such an environment [2]. In VANET network performance of routing protocol degrades with speed and size of network that posses research challenges to design efficient routing protocol for this high mobile environment.

Current research trends for VANETs focused on developingapplications that can be grouped into the following two classes:
1) Improving the safety level on the road and 2) Providing commercial and entertainment services. To enable such applications, vehicles and RSUs will be equipped with onboardprocessing and wireless communication modules. Then, vehicle-to-vehicle and vehicle-to-infrastructure (V2I) communications will directly be possible when in range or acrossmultiple hops. RSUs are usually connected to the Internet andallow users to download maps, traffic data, and multimedia files and check emails and news. These kinds of VANETs, referred to as *service oriented,* are expected to virtually provide alltypes of data to drivers and passengers.

However, due to the characteristics of VANETs highmobility and frequent link disconnection, they perform poorly in VANETs. Clustering is a method by which nodes are placed into groups, called clusters. This method helps in providing an exchange of information between vehicles without any RSU's.In this paper we are presenting cluster based routing approach for VANET and compare their performances with existing routing protocols.Section 2 presents the overview of clustering.The section 3 describes the security issues of VANET and their solutions, Section 4 presentsabout our proposed work, Performance metric and simulation setup is explained in section 5,theresult is presented in section 6. Finally we summarize the paper and outline future research in section 7.

II. OVERVIEW OF CLUSTERING

Cluster based Routing in VANET is Particularly useful for applications that require better routing and scalability to hundreds or thousands of vehicles . Vehicles Mobility behavior determines the architecture of the cluster. In cluster based routing a group of nodes identifies themselves to be a part of cluster and a node is designated as cluster head will broadcast the packet to cluster. Cluster based Routing combines the features of static and dynamic clustering together [3]. Static clusters are formed around the static sources located at the road signals, street corners and congested places known as static clusterhead. However buses are chosen as dynamic sources since they have the predefined path and time chart to handle the high mobility situations known as dynamic clusterhead. Hierarchical clustering creates a layering environment that poses some of the main challenges in such ad hoc networks. Top layer consists of static clusterhead, middle layer consists of dynamic clusterhead and lower layer consists of ordinary vehicles.Because of highly dynamic vehicles network topology also changes. This in turn 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. Some of mobility metrics are considered for cluster construction in order to form a stable cluster structure thereby decreasing its influence on cluster topology.Vehicles Mobility behavior determines the architectureof the cluster. Vehicles are grouped in two different ways either by those vehicles which are in the communication ranges of dynamic sources or by those vehicles which are in the ranges of static sources mounted at traffic signals and road junctions. By doing so, the re-affiliation and re-clustering rate can be naturally decreased.

2.1) Cluster Creation:

Generally two approaches can be found in cluster formation. They are Identifier based and connectivity based. In that the identifier-based clustering is a better choicethan connectivity-based clustering, according to node movement. When usingidentifier-based clustering a node elects itself as the clusterhead if it has thelowest/highest ID in its neighborhood, or a neighbor node if one has a lowerID. Connectivity-based clustering elects the node, which has the most neighbor nodes, as the clusterhead. So, whenever a clusterhead losses a neighbor nodeits connectivity decreases and it is most likely that another node has to beelected to act as clusterhead. While in the identifier-based approach, a newclusterhead has to be chosen only when nodes with lower/higher ID appear [4].

2.2) Data transmission phase:

If a node in a cluster is in need of a service then it initially contacts its local Cluster head. The local cluster head searches it in the local database and ensures the specified service is available or not. If the specified service is present then it gives the necessary details about the service provider to the needed node to get the service. If the service is not present then the algorithm synchronizes all cluster heads in the VANET immediately. After synchronizing the procedure again it searches the cluster head for the availability of the required service. Thus this overview about the clustering gives us a general idea about the cluster formation and data transmission between the clusters.

III. OVERVIEW OF SECURITY

One of the challenges is security; limited attention has been devoted so far to the security of vehicular networks. Yet, security is crucial. VANET security should satisfy four goals, it should ensure that the information received is correct, the source is who he claims to be, the node sending the message cannot be identified and tracked and the system is robust. There are many types of attack such as Denial of Service attack, Message Suppression Attack, Fabrication Attack, Alteration Attack, Replay Attack, and Sybil Attack. VANET security should satisfy the following requirements [5].

3.1) Message Authentication and Integrity: Message must be protected from any alteration and the receiver of a message must corroborate the sender of the message. But integrity does not necessarily imply identification of the sender of the message.

3.2) Message Non-Repudiation: The sender of a message cannot deny having sent a message.

3.3) Entity Authentication: The receiver is not only ensured that the sender generated a message, but in addition has evidence of the livens of the sender.

3.4) Access Control: Access to specific services provided by the infrastructure nodes, or other nodes, is determined locally by policies. As part of access control, authorization establishes what each node is allowed to do in VANET.

3.5) Message Confidentiality: The content of a message is kept secret from those nodes that are not authorized to access it.

3.6) Availability: The network and applications should remain operational even in the presence of faults or malicious conditions. This implies not only secure but also fault-tolerant designs, resilience to resource depletion attacks, as well as survivable protocols, which resume their normal operations after the removal of the faulty participants.

3.7) Privacy and Anonymity: Conditional privacy must be achieved in the sense that the user related information, including the driver's name, the license plate, speed, position, and traveling routes along with their relationships, has to be protected; while the authorities should be able to reveal the identities of message senders in the case of a dispute such as a crime/car accident scene investigation, which can be used to look for witnesses.

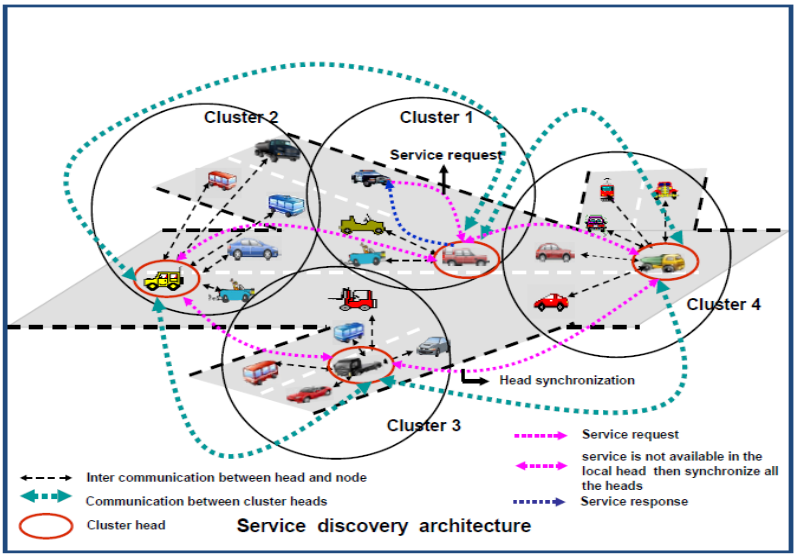

Cluster 2
Cluster 1
Service request
Cluster 4
Head synchronization
Cluster 3
Inter communication between head and node
Communication between cluster heads
Cluster head
Service discovery architecture
Service request
service is not available in the local head then synchronize all the heads
Service response

Fig 1: VANET service architecture scenario

IV. PROPOSED WORK

The above furnished concepts of clustering and security concerns will be optimized in our proposed work.

Clustering in vehicular ad hoc networks (VANET) is one of the control schemes used to make VANET global topology less dynamic. Our technique takes the speed difference as a parameter to create relatively stable cluster structure. The degree of the speed difference among neighboring vehicles is the key criterion for constructing relatively stable clustering structure. In general, vehicles build their neighborhood relationship using the position data embedded in the periodic messages. Usually, vehicles broadcast their current state to all other nodes within their transmission range (r). Therefore, two vehicles are considered neighbors if the distance between them is less than r. The total number of r-neighbors of a given vehicle is called the nodal degree of the vehicle. In our system, if we start with the slowest vehicle, then all the neighboring vehicles of this slowest vehicle that satisfy the speed threshold will be in the first cluster. The remaining vehicles will then go through the same cluster formation process to create other clusters. By extracting the velocity data embedded in the periodic messages, any vehicle can determine whether it has the slowest velocity among all its neighbors within R communication range. The slowest vehicle, in our method, is supposed to initiate the cluster formation process by sending a cluster formation request and only its stable neighbors participate in this process. Similarly the remaining vehicles do form the clusters depending upon the speed and direction.

In order to execute the cluster algorithm, each vehicle is assumed to maintain and update the two sets of database that contain the IDs of the stable neighbors. At any time, there should be a vehicle whose speed is the slowest among its stable neighbors, and as a result, the other list maintained by this vehicle is empty. The algorithm basically requires that the slowest vehicle or the vehicle whose members belong to other clusters originates the cluster formation process. This vehicle is called the cluster originating vehicle (COV).Even though clustering makes efficient management in message transmission there is an issue regarding security of messages, transmitted. In order to maintain confidentiality of the message we propose security algorithm along with clustering approach.

In this paper, we argue that the security of users should be accounted for, starting from the initial contact between a user and a RSU. Hence, we describe a web-based secure registration process that allows a user to create an account with RSUs. During the registration, users provide all required information that enables them to have the benefit of secure connectivity starting from the first packet that they send to the RSUs. Hence we derive a set of encryption keys that are used to encrypt the next packet from part of the data in the current packet.

In our algorithm, users register once with theRSUs online (through the Internet) before they start connecting to the RSUs from their vehicle. After registration, the RSUs obtain from a trusted authority (TA) a master key (K*m*) for the user. The users get their K*m* the first time they connect to an RSU from their vehicle.

Registration and Session Management:

As vehicles might be occupied by several users, where each user might have his/her own interests, it is better to consider each user as a distinct member and give him/her a unique account with the RSUs. Hence, we require users to register with the RSU‘s at the beginning through the web before they start connecting from their vehicles. The registration is done by the user only once to create an account with the RSUs and to benefit from security measures that exist in Internet protocols. These measures will enable users and RSUs to exchange credentials and keys that will help them start their connection in the VANET in a secure way [6].

4.1) Registration: When user registers using the RSU website, they specify their personal details (i.e., name, address, and phone) plus a user name and password to use for authentication when they connect to the RSU network from their vehicle. Users also choose a default RSU, which will save their account in its database. Examples of users' interests are Web Pages, certain news, traffic information in certain areas, and email messages(possibly from different email accounts).When they later connect to the VANET, they send a Hello packet to the nearest RSU, which will notify their default RSU, which, in turn, retrieves their interests from its database and collects the required data for them. User can choose any RSU as their default one, but it is best to select the nearest to their starting point in the VANET.

4.2) Master Key: After the users have registered, their default RSU saves their account and contacts the TA to obtain a master key (Km) for them. The users obtain Km the first time (after registration) they connect from their vehicle to one of the RSUs. To achieve this, we propose a technique that depends on deriving a group of encryption keys from the user's password (of their account with the RSUs) and using these key to securely transfer Km to them. To generate these keys, we propose a new key derivation and encryption function. One of the inputs to this function is an initial iteration count (IC1), which an integer is kept as a secret between the user and the RSU. After registration, the RSU generates IC1 and sends it to the user (online during the Internet session in which the user registers), who saves it and uses it as an input to the hierarchal password-based key derivation (HARDY) function when he/she obtains and decrypts (Km).

4.3) Participating in a Session: Each time a user connects to an RSU, he/she starts a new session. To preserve users' location privacy, we make an RSU assign to a user a new pseudonym in each packet. A user starts a session by sending a Hello packet that contains his/her user name to the nearest RSU. Each packet will include a time stamp to be used for resisting replay attacks. When the RSU receives the Hello packet, it starts preparing the user's data that don't require authentication with other systems. Although the RSU prepares users' data, it assigns them a pseudonym and sends it to them in an ID packet. The user replies with an "Identify" packet that contains his/her user name, password, and Kc. Both packets will be encrypted using Km. Accordingly; we assume that only the RSU and the user will be able to encrypt/decrypt packets with the user's master key or packet keys. If an attacker stores a packet from the RSU to the user and tries to send it later to the user, pretending that he/she is the RSU, the user will detect the attack from the time stamp. Hence, using time stamps and securely transfer ring keys will assure the users that they are receiving packets from the RSU and not from an attacker. The sequence of connecting to the RSU is given in the Fig 2.

4.4) Hand Over: A vehicle observes its current location at constant intervals of time and calculates its distance from all nearby RSUs using the digital map. When it finds that it is much closer to another RSU (e.g. closer by a factor of 30%), it switches to it. Contrary to handover in traditional wireless networks (such as cellular networks), where the communication between the mobile user and the access point is always through a single-hop connection, the communication between a vehicle and an RSU could traverse several vehicles (i.e., multi hop). Hence, the packets exchanged between the vehicle and the RSU during a hand over could be sent in a multi hop manner. These packets are small in size and, hence, will take much less time to travel compare to data packets. In the next section we have shown our simulation results, in which we can find that the hand over delay is less compared to the other routing protocols. This is because we specifically designed to route packets by combining store-and-forward and location-based routing techniques.

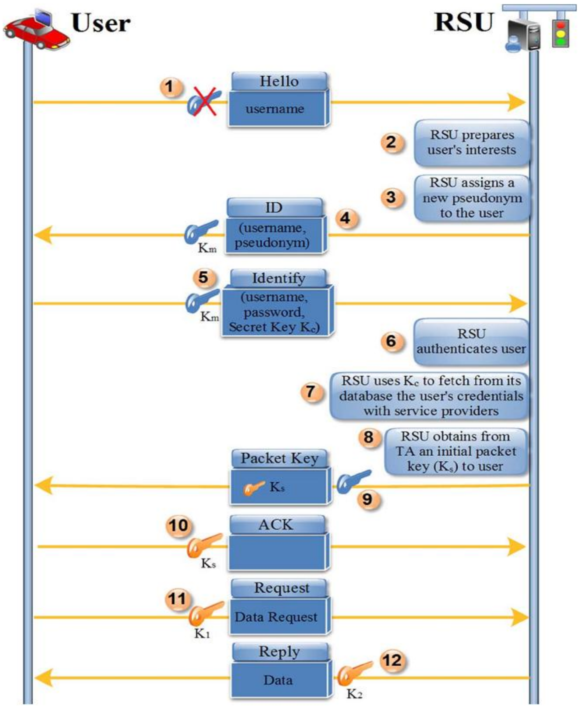

User
RSU
1
Hello
username
2
RSU prepares user's interests
3
RSU assigns a new pseudonym to the user
4
ID
(username, pseudonym)
K_m
5
Identify
(username, password, Secret Key K_c)
K_m
6
RSU authenticates user
7
RSU uses K_c to fetch from its database the user's credentials with service providers
8
RSU obtains from TA an initial packet key (K_s) to user
Packet Key
K_s
9
10
ACK
K_s
11
Request
Data Request
K_1
Reply
Data
12
K_2

Fig:2 Sequence diagram for participating in a session

Based on the above described parameters simulation has been carried out using the Network Simulator NS2 to evaluate the performance of our proposed system. Also we have compared our system with other system to differentiate the performance between the systems. The results are further described in coming section.

V. PERFORMANCE METRICS AND SIMULATION SETUP

There are many network simulators available in the market but the most frequently used are OPNET, Qualnet, and NS2 but OPNET and Qualnet are not open source tools and costs more. Hence the best choice is to use the NS2 simulator which is completely free and open source tool for all kinds of network simulations and researches. We carried our simulation study with NS2 to have better performance evaluation.

Performance Metrics:

There are several performance metrics to be evaluated which are as follows:

5.1) Throughput: Represents the average rate of successful message delivery over a communication channel.

5.2) Success ratio:Represents the average ratio of the number of successfully received data packets at the destination node to the number of data packets supposed to be delivered.

5.3) Message delay: Refers to the time taken for a message to be transmitted across a network from source to destination.

5.4) Handover traffic:Ratio of data rate difference between first and second vehicle to that of total data rate.

5.5) Handover delay:Defined as ratio of switching time between two RSU to the total time taken to cross a unit.

Simulation Setup:

A highway model has been created using the Network Simulator2 (NS2). The screenshot of the highway model is shown in Fig 3 and Fig 4.

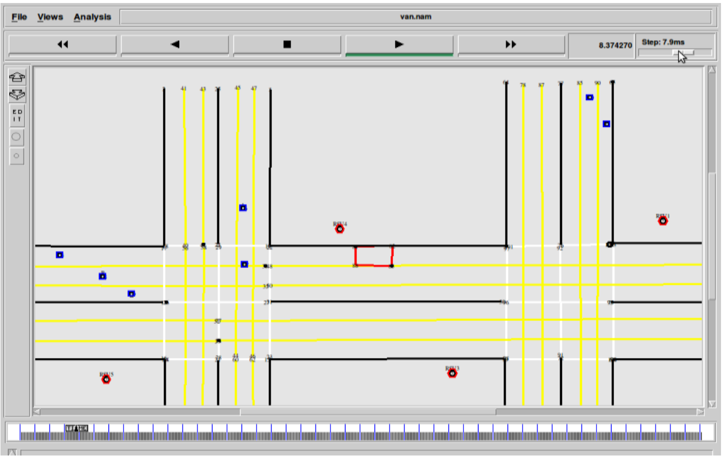
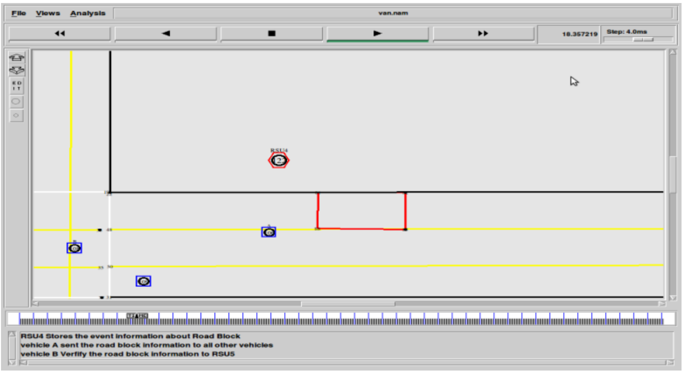


Fig: 3 Highway Model

From the above figure we can understand the clusters of vehicles being indicated in the blue circles and the RSU is being given in red color in the shape of hexagon. The small rectangle at the middle of the lane indicates the block in the lane and hence the vehicles must take other lane for further transportation.

The next shown highway model indicates a block in the lane. This information will be further passed to the vehicles through the RSU4. Hence the delay in travel time can be reduced.



RSU4 Stores the event information about Road Block
vehicle A sent the road block information to all other vehicles
vehicle B Verfify the road block information to RSU5

Fig: 4 Highway Model- Msg Transmission about the block in lane

VI. SIMULATION RESULTS

The above discussed performance metrics has been shown in the following simulation results.

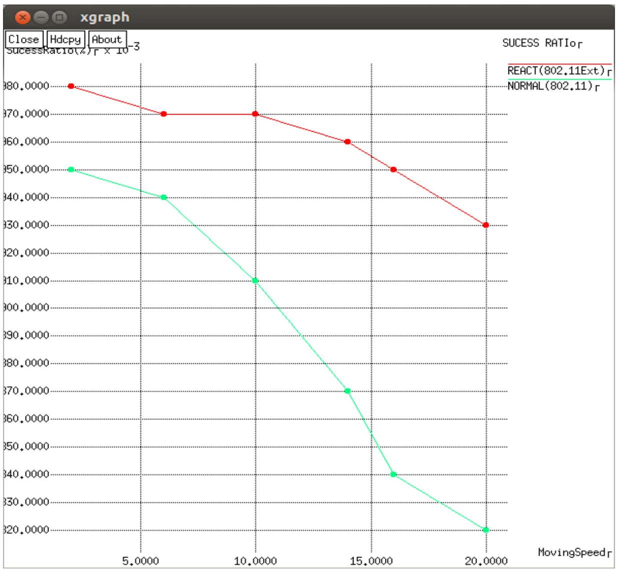


Fig: 5 Success Ratios

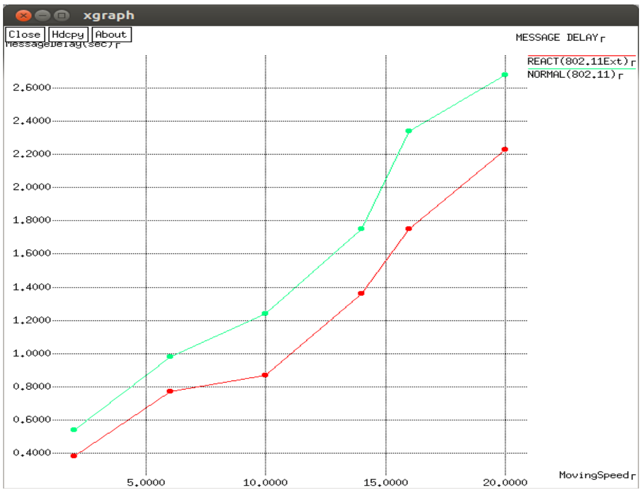


Fig: 6 Message Delay

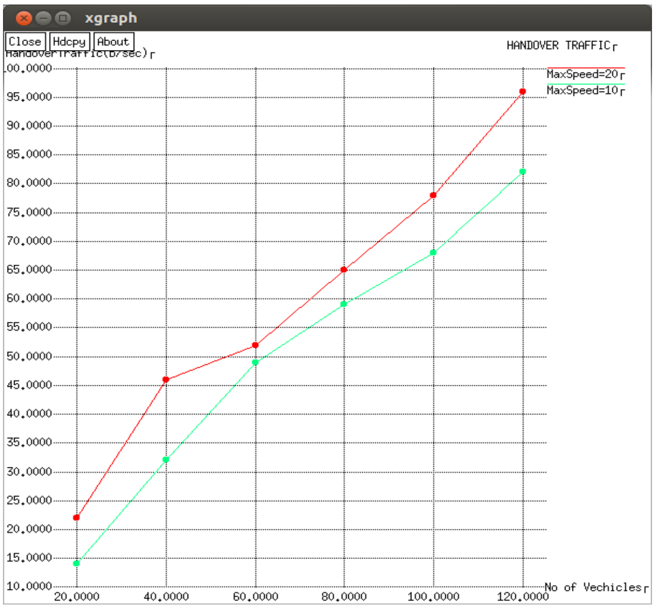


Fig: 7 Handover Traffic

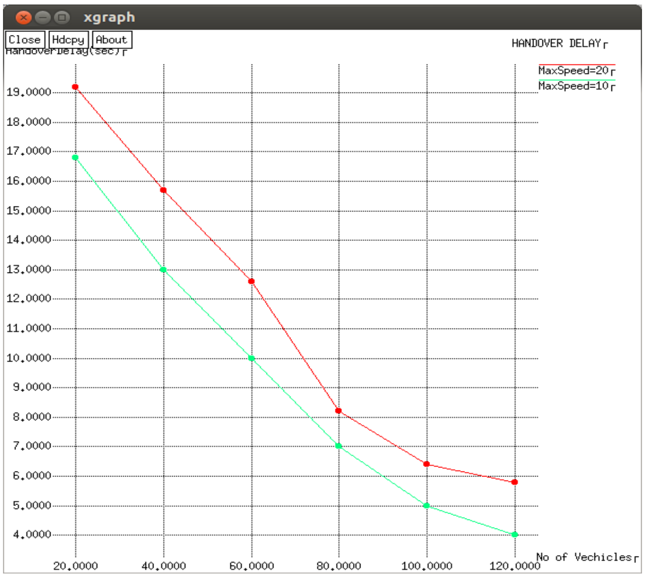


Fig:8 Handover Delay

The above shown simulation results depict that our proposed algorithm has better performance than the normal routing algorithm.

VII. CONCLUSION

The unanswered questions about the privacy and security in the service-oriented VANET have been given solutions in our proposed system. We have also created a cluster based model which helps in providing the services among the vehicles even in the absence of RSU's. By the concepts of clustering the message transmitted is either in single hop or multi hops. There again comes a question about the security. So as to enhance the security of the messages transmitted we have introduced a novel and provable cryptographic algorithm for key generation and powerful encryption. Thus security concerns are achieved. Also, the evaluation of our proposed scheme has confirmed its effectiveness among the other security mechanisms for VANET. The future work focuses on making our proposed more scalable in terms of numberofusersthatcanconnecttoanRSU. By this method, we can priorities the Time Slots for each user and hence the load in the RSU can be distributed equally.

REFERENCES

[1]. Zaydoun Y Rawashdeh and Syed Masud Mahmud, "A novel algorithm to form stable clusters in vehicular ad hoc networks on highways", *EURASIP Journal on Wireless Communications and Networking 2012, 2012:15.*

[2]. Bhuvaneshwari.S,Divya.G, Kirithika.K.B and Nithya.S , "A Survey On Vehicular Ad-Hoc Network", *International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering ,Vol. 2, Issue 10, October 2013.*

[3]. B. Ramakrishnan, "Performance Analysis of AODV Routing Protocol In Vehicular Ad-hoc Network Service Discovery Architecture",*ARPN Journal of Systems and Software,vol. 2, no. 2, February 2012.*

[4]. KapilBhagchandani, Yatendra Mohan Sharma, "Exploration of VANET Mobility Models with New Cluster Based Routing Protocol", *International Journal of Soft Computing and Engineering (IJSCE), Volume-2, Issue-6, January 2013.*

[5]. Ram Shringar Raw, Manish Kumar, Nanhay Singh, "Security challenges, issues and their Solutions for VANET", *International Journal of Network Security & Its Applications (IJNSA), Vol.5, No.5, September 2013.*

[6]. Khaleel Mershad and Hassan Artail, "A Framework for Secure and Efficient Data Acquisition in Vehicular Ad Hoc Networks", *IEEE Transactions on Vehicular Technology,Vol.62, No.2, February 2013.*

BIOGRAPHY

BHUVANESHWARI currently purses Bachelor's Degree in the field of Electronics and Communication engineering at KPR Institute of Engineering and Technology, Coimbatore, Tamil Nadu. Having interest in the field of Networks she has presented papers in 3 National Conferences and 8 papers in National and State level technical symposiums. She has published 1 paper in an International Journal.

DIVYA is doing BE Electronics & Communication Engineering at KPR Institute of Engineering & Technology, Coimbatore. Her research interests include Wireless Networks and Nano Technology. She has presented 2 paper in National conference and 10 papers in National level Technical Symposiums and published 1 paper in International Journal.

KIRITHIKA is doing BE Electronics & Communication Engineering at KPR Institute of Engineering & Technology, Coimbatore. Her research interests include Wireless Networks. She has presented 2 paper in National conference and 7 papers in National level Technical Symposiums and published 1 paper in International Journal.

NITHYA is with ECE department in KPR Institute of engineering & Technology, Coimbatore as Assistant professor. She has done her B.E in Electronics & Communication Engineering from Sengunthar Engineering College, Tamil Nadu, and M.E. in Communication Systems from Sri Shakthi Institute of Engineering & Technology, Tamil Nadu. Her research interests include Mobile ad hoc Networks, Network Security & Cryptography. She has presented 7 papers in national conference and 4 papers in International conferences. She has published 5 papers in international journals.