IJRSET AUGUST 2016 Volume 3, Issue 8 Pages: 24-32

ISSN 2394-739X

International Journal for Research in Science Engineering and Technology

GSIDS: GROUP BASED SECURED INFORMATION DIFFUSION SCHEME FOR VANET

[1] Salva Mariya. k
[1] M. Tech Scholar
[1] Dept. of ECE
[1] MEA Engg. College Kerala, India

[2] Rajeev. N
[2] Assoc.Professor
[2] Dept. of ECE
[2] MEA Engg. College Kerala, India

ABSTRACT- In this paper, we propose a navigation scheme that utilizes the online road information collected by vehicular ad-hoc network to guide drivers to desired destination in a real-time and distributed manner in a large geographic area. The proposed scheme has the advantage that, which divides network to cluster or groups, where nodes are grouped using same search query like same direction or same destination routes. The clustering dissemination is a prominent solution to overcome limitation of available bandwidth of wireless medium and reduce communication burden. Simulation results shows that, the route returned by our scheme is very efficient in terms of processing delay and saving up to 80 percent of travelling time compared with tradition navigation system.

Keywords- [Navigation scheme, VANET, Secure vehicular sensor network, Anonymous credential, Pseudo identity, ITS, Proxy re-encryption.]

1. INTRODUCTION

Every driver has a common experience to find an actual route of certain destination. In old days, a user usually refers to a hard copy of atlas. Today for navigation service we mainly depends on GPS [6]. While receiving GPS signals, device capable to find its current location and it shows the geographically shortest route for certain destination based on a local map database. But, route searching procedure of these system is based on local map data base and real-time road conditions are not taken into consideration.

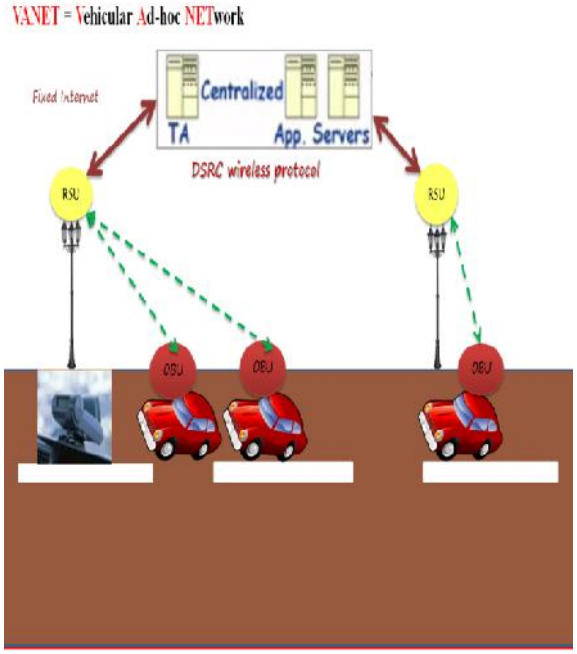

Figure 1- VANET overview

VANET [2] is an important element of the intelligent transportation system (ITS) [3]. VANET is part of Mobile Ad Hoc Networks (MANET) [4], this means that every node can move freely within the network coverage and stay connected, each node can communicate with other nodes in single hop or multi hop.In a VANET, each vehicle is supposed to have an on-board unit (OBU), there are road side units (RSU) fixed along the roads and a trusted authority (TA) and some other application servers are fixed at the back end. The OBUs and RSUs communicate using Dedicated Short Range Communication (DSRC) protocol [5] over the wireless channel within 1KM range area. The RSU, TA and application servers communicate using a secure fixed network such as internet. That means, VANET allow communications in between vehicles (denoted as vehicle-vehicle or V2V communications),in between vehicle and RSU (denoted as vehicle-infrastructure or V2I communications) and also allow in between RSUs or between RSU and other type of devices (inter road side communications).

2. EXISTING VANET BASED SECURE AND PRIVACY PRESERVING NAVIGATION

VSPN (VANET based secure and privacy preserving navigation) scheme [1] makes use of collected data to provide navigation service to drivers. Here, based on the destination and the current location of driver, the system can automatically search for a route that yields minimum travelling delay in a distributed manner using the online information of the road conditions. To provide security for drivers, the destination and the driver who issues the navigation request are guaranteed to be unlinkable from any third party including the trusted authority [8], [9], [10]. In addition to authentication and privacy preserving, this scheme full fills all other necessary security requirements [7], [11], [12].

STEPS IN NAVIGATION SYSTEM

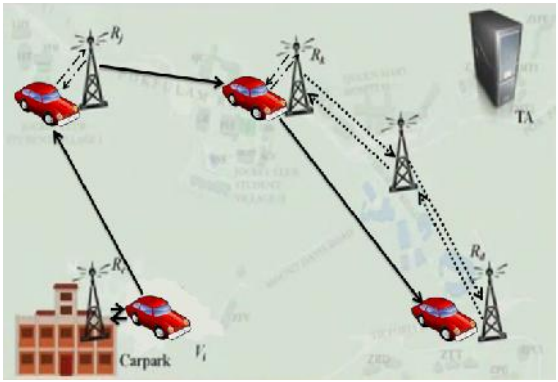

Figure 2- Basic steps in VSPN

VSPN scheme can summarize into some basic steps [1]. First, TA sets up parameters and generates anonymous credentials. Second vehicle V_i's tamper-proof device starts up and requests for the master secret s from RSU R_c. Third, vehicle V_i's tamper-proof device requests for a navigation credential from RSU R_j. Fourth, RSU R_j verifies V_i's identity and sends its tamperproof device an anonymous credential. Fifth, after a random delay or after travelling for a random distance, V_i's tamper-proof device sends out its navigation request to RSU R_k. Sixth, RSU R_k forwards the navigation request to its neighbours. This procedure iterates until the request reaches RSU R_d is covering the destination. Seventh, RSU R_d constructs the navigation reply message and sends it along the reverse route. Each hop along the path attaches the corresponding hop information (with signature). Eighth RSU R_k forwards the navigation reply message to V_i's tamper-proof device which then verifies the messages from all RSUs along the route in a batch. Ninth by presenting the navigation session number, each RSU along the route guides V_i to reach the next RSU closer to the destination. Based on V_i's pseudo identity received from RSU R_j, At last, TA find out V_i's real identity for billing purpose.

GAPS IN VSPN SCHEME

First, this scheme is not scalable especially for large areas due to the limited bandwidth of wireless medium. That means,

in case of high vehicle density many cars compete for the wireless medium, thus exceeding the available bandwidth. Second, communication burden at RSU is very high in urban environment. Hence, clustering [14] is only one possible solution to overcome the limitation of available bandwidth. The idea behind clustering is that many applications do not need atomic information, such as exact location and speed values from each vehicle. Instead, they only want to know average speed on the road, and where a possible traffic jam is exactly located to be able to react accordingly.

3. PROPOSED GROUP BASED SECURED INFORMATION DIFFUSION SCHEME FOR VANET

SYSTEM ASSUMPTIONS

The Proposed method is based on Group Based Receiver Driven Protocol (GACVO), which divides network to

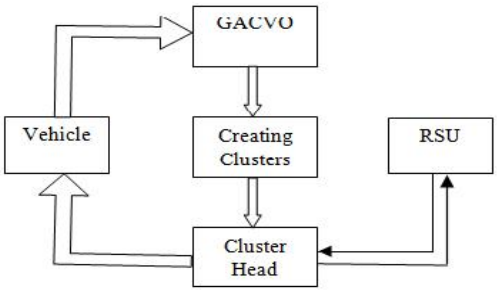

Figure 3- Block diagram of GSIDS

clusters or groups, where nodes are grouped using same search request like same direction or same destination routes. Each cluster has a cluster head. Cluster head manage communication process inside and outside the cluster. The cluster is managed by the number of members, consists of one cluster head (Group leader) and two or more cluster members. Node ID of cluster head becomes cluster ID of the cluster. Cluster head and cluster members (CM) connect each other with same cluster ID. Nodes inside the cluster communicate by direct paths, but their communication with other nodes outside the cluster is achieved by their cluster head hence create virtual infrastructure for the network [13].

PROPOSED CLUSTERING ALGORITHM

The proposed GACVO clustering algorithm consists of mainly four steps [15].

A. Network Construction

All vehicles and RSUs should be properly authenticated by trusted authority before entering in to navigation services. Thus if any dispute happens in the network TA is responsible for that. Because TA is a centralize server.

B. Verification of vehicles by RSU

To start navigation each vehicle sends out its navigation query to neighboring RSU. Up on receive

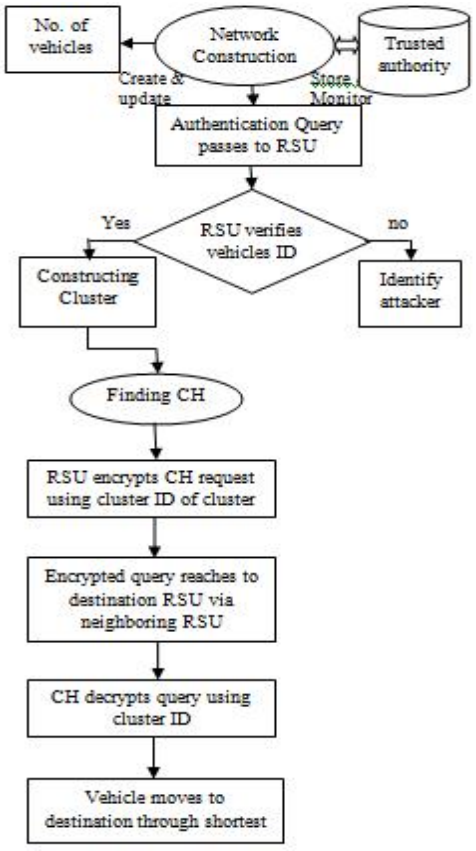

Figure 4- GSIDSs Data Flow Assignment

navigation query neighboring RSU first check validity of vehicle. If vehicle ID is invalid

then, RSU initiate procedure for identify attacker else cluster formation takes place.

C. Cluster Formation

From the navigation query from each vehicle RSU identifies vehicle's destination. Thus by considering a set of parameters like current location of vehicle, speed of vehicle, relative destination and final destination RSU helps

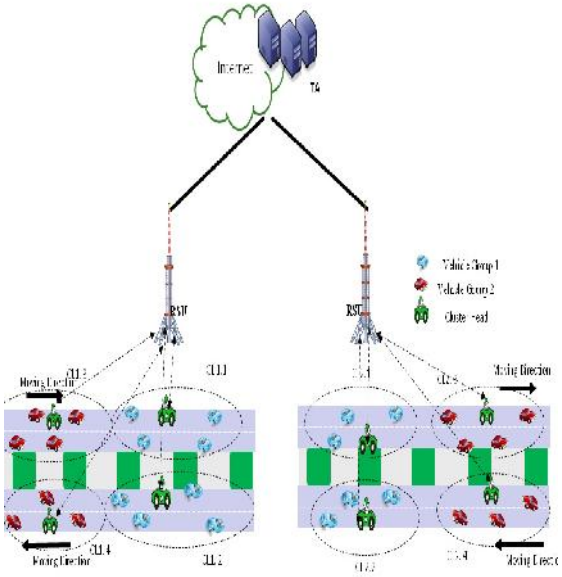

Figure 5- System architecture of GSIDS

vehicle for constructing a cluster. This vehicle is called the cluster originating vehicle (COV). COV sends the Initiate Cluster with its ID as a temporary cluster ID to all neighbours. Then, all non-clustered members react upon receiving this message by setting their cluster ID temporarily to be the ID of the COV. Each vehicles start calculating their suitability to become a CH.

D. Cluster Head Selection

Nodes having higher number of stable neighbours, maintaining closer distances to their stable neighbours, and having closer speed to the average speed of their stable neighbours should have higher suitability value, thus they are more qualified to be elected as cluster-heads.

E. Cluster maintenance

After formation of cluster only CH communicate with RSU. Thus, CH always has a parameter table contains cluster ID of cluster, node ID of cluster member, current location in terms of X,Y coordinates, relative destination and final destination information. Also CHs and CMs have a list of nearby CHs, for switching from one CH to another in case of current CH is no longer a good option. When cluster size is too large or CM violate speed limit within the cluster then, CM want to move from one cluster to another cluster.

The events that trigger the maintenance procedure can be summarized as follows:

Leaving a cluster: when a cluster member moves out of the cluster radius, it loses the contact with the cluster-head over the service channel. As a result, this vehicle is removed from the cluster members list maintained by the cluster-head. The vehicle changes its state to a standalone if there is no nearby cluster to join or there is no other nearby standalone vehicle to form a new cluster according to GACVO cluster formation algorithm.

Cluster merging: when two cluster heads come within each other's transmission ranges and their relative speed is within the predefined threshold Δv_{th}, the cluster merging process takes place. The cluster-head vehicle that has less number of members gives up its cluster-head role and becomes a cluster-member in the new cluster. The other cluster members join that neighbouring cluster if they are within the cluster head's transmission range and the speed is within the threshold. Finally, vehicles that cannot merge with the cluster nor can join a nearby cluster, start clustering process to form a new cluster according to GACVO algorithm.

F. Finding Shortest Path to Destination

After the formation on cluster only CH communicate with RSU. Thus communication burden at RSU can significantly reduce. Thus RSU encrypts CH requests by using cluster ID of cluster for security. The encrypted navigation query reaches destination RSU

with the help of neighboring RSUs. Hence destination RSU compute route reply message and send it along the reverse path. Upon receiving navigation reply message neighboring RSU will not forward it immediately into vehicle immediately. Instead it waits for a threshold amount of time for more replies. Among the replies neighboring RSU picks a travelling route that has highest average speed send it to CH. CH decrypts this navigation reply by using cluster ID of cluster. That is, here symmetric encryption is takes place. Thus all vehicles within the cluster move to destination through that path.

PROPOSED SYSTEM MODEL

An overview of our proposed work is shown in figure.5. All vehicles in the navigation systems are authenticated with a TA before they are assigned to a network. Then, each vehicle pre-request a number of navigation credentials before starts journey. Also all vehicles employ GPS or navigation system. After authentication by TA each vehicle sends its navigation query to neighboring RSU. Upon receiving navigation

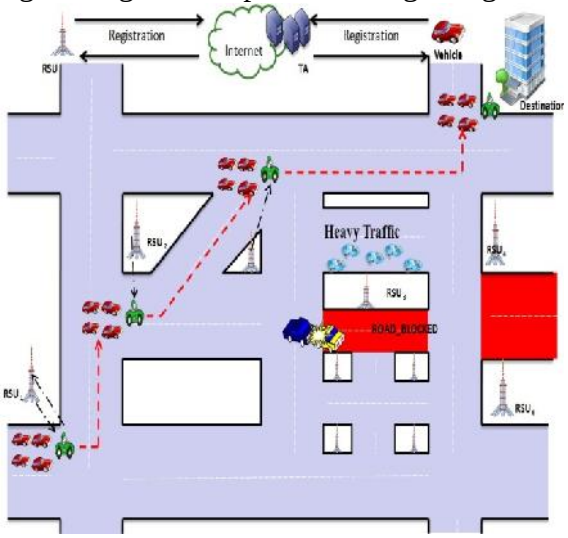

Figure 6- GACVO Overview

query to neighboring RSU, it first checks validity of vehicle. If vehicle ID is invalid then, RSU initiate procedure for identify attacker else cluster formation takes place by considering a set of parameters like current location of vehicle, speed of vehicle, relative destination and final destination RSU helps vehicle for constructing a cluster. In figure.5. near RSU1 a cluster is formed. Hence CH request navigation query to RSU1. Upon receiving navigation query RSU1 compute route request message, M_1={RT-REQ, nsn, $RRID_1$, DEST} and broadcast it to all neighbors that are closer to destination than itself. Receiving RSU RSU_2 first store nsn. RRID and DEST in to its navigation routing table to build up reverse path. Then check whether destination is within its range or not. Here destination is not within the range of RSU_2. Hence it simply rebroadcast message to its neighbor that are closer to destination than itself. This process repeats until request reaches RSU_4 covering destination. Destination RSU computes route reply message, M={RT_RPY, nsn, RRID, RL ,AvgSpd, RoadCond} and send it along the reverse path. While receiving route reply message RSU_1 will not forward it immediately into vehicle, instead it waits for a threshold amount of time for more replies. Among that RSU_1 select a route that has highest average speed and send it to CH. Thus a vehicles within a cluster moves to destination through that path.

Road conditions may vary abruptly. A road which is initially in good condition may become blocked in a second. After route request reply propagation when vehicle move to destination through shortest delay path road within the range of RSU_3 is blocked. Therefore it immediately composes the road blocking notification message that is defined as M_3={ROAD_BLOCKED} and broadcast it to all neighboring RSUs. The message is propagated along the reverse path until RSU_2 that is currently in contact with this cluster reached. The RSU_2 forwards message to CH. Hence select an alternative path to reach destination.

4. RESULTS AND DISCUSSION

In this section, we evaluate our GSIDS scheme in terms of processing delay and reduction in travelling time implemented in

Ubuntu Linux environment within NS2 simulator, which has been highly validated by the networking research community. Through simulation, we show that the processing delay is minimal, while the savings in the travelling time after using GSIDS scheme is significant.

Simulation Models

Here used different network parameters in the simulation. The data rate is set to 2-11 Mbps and the periodic messages are sent every 100 ms, the size of the message including the mobility information is 100 bytes. The RSUs are placed in such a way that there is at least one RSU covering the two ends of each road because V2I communication is more critical there. Other RSUs are then randomly placed to improve the coverage. The RSU-to-vehicle communication (V2I) and the inter vehicle communication (V2V) ranges are set to 600 and 300m, respectively. In the backbone, there is a TA server. RSUs communicate with each other and with TA via a fixed infrastructure. The bandwidth of DSRC channel and the fixed infrastructure are assumed to be 6 and 10 Mb/s, respectively. In our GSIDS scheme, an RSU need to look up its routing table for forwarding direction and such lookup can be accomplished in 0.6ms on average. When the simulation was run node generated data and start building clusters.

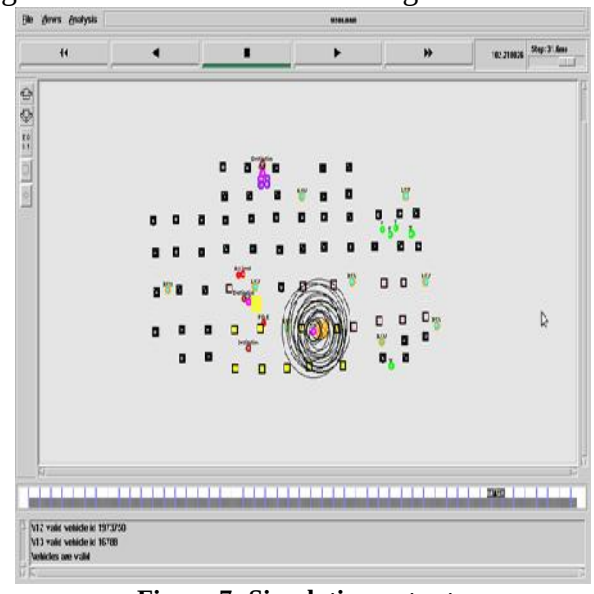

Figure 7- Simulation outputs

In our simulation as shown in figure.7 a fixed number of geographical distance ranges are defined. We randomly pick 3 set of sources and destinations. When the experiment starts, about 10 percent of all roads are blocked. We only consider sources and destinations that have roads connected and these roads are not blocked at this time. Without loss of generality, we assume that a vehicle requests for a navigation credential or sends out its navigation query once it enters an RSU's range (upon hearing its beacon broadcasts). Since a vehicle can wait for a random delay or travel for a random distance after obtaining a navigation credential before sending out its navigation query, we define the processing time as the period from when the vehicle sends out its navigation query to when it finishes verifying the information provided by all RSUs along the returned path. This processing time is then normalized by the duration that the vehicle is in the range of the RSU to which it sends its query. Here, we assume the vehicle concerned keeps on moving as cluster without being blocked by traffic jam or accident.

Simulation Results

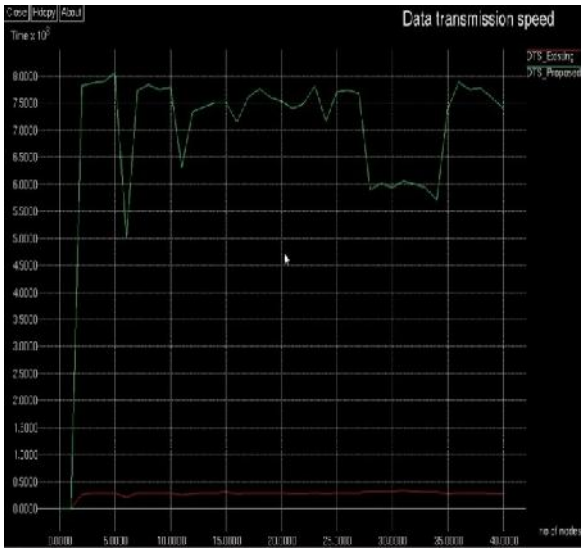

Figure 8- Graph of data transmission speed comparison

First we compare data transmission speed of our proposed work and VSPN scheme as shown in figure.8. For all geographical

distance ranges, the travelling route returned by GSIDS scheme offer better data transmission speed than the VSPN scheme. Because in GSIDS CH manage communication inside and outside the cluster. In VSPN scheme all vehicles broadcast safety messages and all vehicles communicate with RSU. Thus with increasing geographical distance communication burden to RSU also get increases.

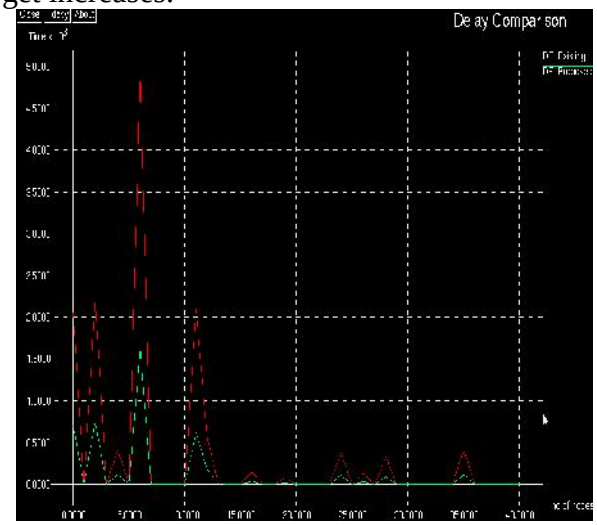

Figure 9- graph of delay comparison

Figure.9. shows delay comparison between GSIDS scheme and VSPN scheme. For all geographical distance ranges, travelling route returned by GSIDS scheme introduce lower delay than VSPN scheme.

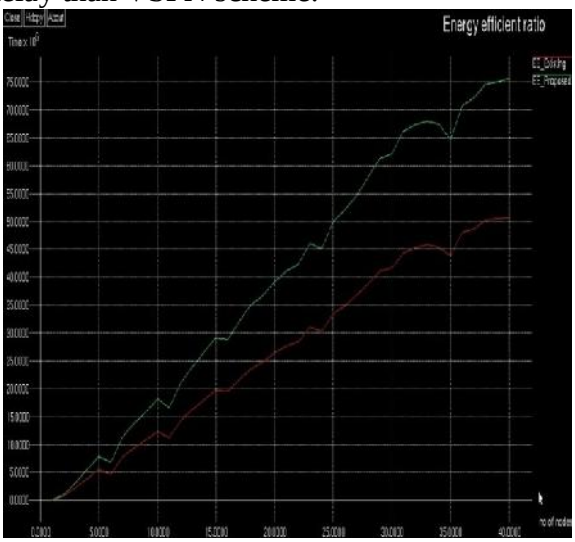

Figure 10- Graph of energy efficient ratio comparison

Next, compare the energy efficiency of proposed scheme with VSPN scheme in figure.10. With increase in the number of nodes, energy efficiency is also increases under both schemes. But, there is significant raise in the energy efficiency of proposed scheme.

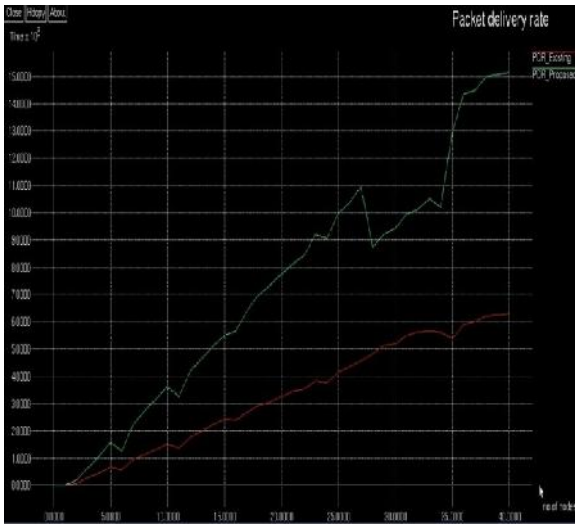

Figure 11- Graph of packet delivery rate comparison

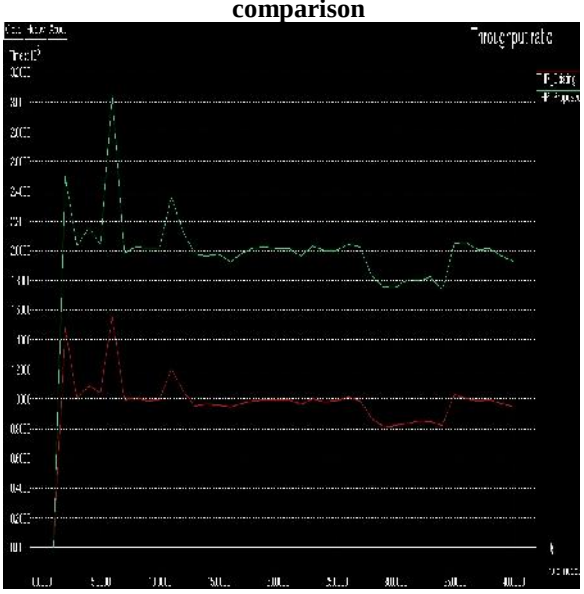

Figure 12- Graph of throughput ratio comparison

Besides processing delay, energy efficiency and travelling time, simulation outputs also include packet delivery rate comparison as shown in figure.11. Proposed scheme establishes a maximum packet delivery ratio, so it reduces the hop delay. In existing VSPN scheme the most packets get lost in transmission due to communication overhead

at RSU. GACVO algorithm makes network to clusters where nodes are grouped using same search query like vehicles that are moving in same direction or having same destination route. Therefore, it results no loss in transmission, and packets having high probability delivery rate. From figure.12 we can see a significant raise in the throughput of proposed work. For any number of nodes GSIDS scheme maintain better throughput result.

Through the above simulation results and comparison it is evident that the proposed Group based secured information diffusion scheme for VANET is superior over the traditional VANET based secure and privacy preserving navigation in the sense that vehicle can complete whole navigation querying process and receive urgent notification in a very short time. GSIDS takes into account the destination of the vehicles to arrange the clusters and implements an efficient message mechanism to respond in real time and avoid global re-clustering. The benefits of consider the current location, the speed and the vehicles destination in the CH selection are evident. The route returned by GSIDS scheme can lead to saving up to 80 percent of travelling time compared with offline map data searching approach.

CONCLUSIONS

Our GSIDS scheme is very efficient in the sense that a vehicle can complete the whole navigation querying process and receive urgent notification in a very short time. This approach is scalable for large areas and urban environments. Main advantage of our proposed algorithm is that during cluster formation vehicular movements are taken in to consideration. In dynamic environments such as VANETs, the cluster reconfiguration and changing CH may affect stability. To overcome this problem clusters are created by considering parameters such as relative destination, final destination, speed etc. Hence GSIDS scheme is very efficient for constructing stable clusters. On the other hand, the route returned by our System output can lead to savings of up to 80 percent of traveling time compared with the offline map data searching approach. To make it practical in real world, coordinated effort from all parties like vehicle manufacturers, transportation authorities, law enforcement agencies, insurance companies, and academic researchers are involved.

REFERENCES

[1]. T.W. Chim, S.M. Yiu, Lucas C.K. Hui , and Victor O.K. Li, “VSPN: VANET-Based Secure and Privacy-Preserving Navigation,” IEEE transactions on computers, VOL. 63, NO. 2, FEBRUARY 2014.

[2]. Zeadally, Sherali, ‘Vehicular Ad-hoc Networks (VANETS): Status, Results and Challenges,’ Telecommunication Systems, pp 217-241, 2012.

[3]. Vivek Kathiyar, PrashantvKumar, niarottam Chand, ‘An Intelligent Transportation System Architecture Using Wireless Sensor Networks,’ International journal of computer applications, volume 14,No 2, januvary 2011.

[4]. Gurpinder Singh, Jaswinder Singh, MANET: Issues and Behavior Analysis of Routing Protocols,’ International journal of advanced research in compute scienece and software engineering, Volume 2, April 2012.

[5]. H. Oh, C. Yae, D. Ahn, and H. Cho, “5.8 GHz DSRC Packet Communication System for ITS Services,” Proc. IEEE VTS 50th Vehicular Technology Conf. (VTC ’99), pp. 2223-2227, Sept. 1999.

[6]. Global Positioning System Standard Positioning Service Signal Specification. Navtech GPS Supply, 1995.

[7]. J.P.H.M. Raya, P. Papadimitratos, “Securing Vehicular Communications,” IEEE Wireless Comm., vol. 13, no. 5, pp. 8-15, Oct. 2006.

[8].K. Sampigethaya, M. Li, L. Huang, and R. Poovendran, “AMOEBA: Robust Location Privacy Scheme for VANET,” IEEE J. Selected Areas in Comm., vol. 25, no. 8, pp. 1569-1589, Oct. 2007.

[9]. A. Wasef and X. Shen, "PPGCV: Privacy Preserving Group Communications Protocol for Vehicular Ad Hoc Networks," Proc. IEEE Int'l Conf. Comm. (ICC '08), pp. 1458-1463, May 2008.
[10]. C. Zhang, X. Lin, R. Lu, and P.H. Ho, "RAISE: An Efficient RSU Aided Message Authentication Scheme in Vehicular Communication Networks," Proc. IEEE Int'l Conf. Comm. (ICC '08), pp. 1451- 1457, May 2008.
[11]. C. Zhang, R. Lu, X. Lin, P.H. Ho, and X. Shen, "An Efficient Identity-Based Batch Verification Scheme for Vehicular Sensor Networks," Proc. IEEE INFOCOM '08, pp. 816-824, Apr. 2008.
[12]. R. Hwang, Y. Hsiao, and Y. Liu, "Secure Communication Scheme of VANET with Privacy Preserving," Proc. IEEE 17th Int'l Conf. Parallel and Distributed Systems (ICPADS '11), pp. 654-659, Dec. 2011.
[13]. B. Ramakrishnan, Dr. R. S. Rajesh and R. S. Shaji, **"**CBVANET: A Cluster Based Vehicular Adhoc Network Model for Simple Highway," Communication Int. J. Advanced Networking and Applications 755 Volume: 02, Issue: 04, Pages: 755-761, 2011.
[14]. P. Basu, "A Mobility Based Metric for Clustering in Mobile Ad Hoc Networks," International Conference on Distributed Computing Systems Workshop April 2011.
[15]. You Lu, Biao Zhou, Fei Jia and Mario Gerla, "Group-based Secure Source Authentication Protocol for VANETs," IEEE Globecom 2010 Workshop on Heterogeneous, Multi-hop Wireless and Mobile Networks.