Congestion Avoidance using Distributed Vehicular Traffic Re-Routing System

Dr. S. G. Santhi[1], **A. Visalatchi**[2]
[1, 2] Department of Computer Science and Engineering
[1, 2] Annamalai University, Chidambaram, India

Abstract- *Traffic safety is the main concern for many countries. Many accidents are caused by insufficient traffic information and by slow driver reaction to local visual and acoustic input.. Existing vehicular traffic re-routing schemes to alleviate congestion are centralized solutions and creates two intrinsic problems: First, the central server has to perform intensive computation and communication with the vehicles in real time. This can make centralized solutions infeasible for large regions with many vehicles. Second, in a centralized architecture, the server requires the real-time locations as well as the origins and destinations of the vehicles to estimate the traffic conditions and provide effective individual re-routing guidance. In this paper proposed system is DIstributed VEhicular Re-routing system (DIVERT) for congestion avoidance which leverages both cellular Internet and VANET communication. DIVERT offloads a large part of the re-routing computation at the vehicles, and thus, the re-routing process becomes practical in real-time. To take collaborative re-routing decisions, the vehicles exchange messages over vehicular ad hoc networks. DIVERT is a hybrid system because it still uses a server and Internet communication to determine an accurate global view of the traffic. In addition, DIVERT balances the user privacy with the re-routing effectiveness. The simulation result demonstrates that, compare with the centralized server. The proposed work increases the user privacy by 92% on average.*

Keywords- Proactive driver guidance, Vehicular congestion avoidance, VANET, Routing, Re-routing, GPRS protocol.

I. INTRODUCTION

In recent years, mobile computing and communication technology has become more widespread and affordable. A large amount of research has now emerged which aims to use these technologies to address a common problem: traffic. Throughout the world, millions (if not billions) of people move through traffic networks every day. If this traffic is not controlled efficiently and effectively, a wide range of economic, environment and social problems may arise. Intelligent, autonomous control of traffic, then, is an important research area which can help alleviate traffic congestion. Generally, proposed intelligent traffic control systems assume that specific information is available, such as traffic densities and average vehicle speeds[7]. Using current road based sensor technology (i.e., induction loop sensors), however, does not allow for most of this information to be accurately observed in real-time. By sharing information through the use of a Vehicular Ad Hoc Network (VANET), this information can be made available, enabling effective intelligent control to become a reality. To tackle all these problems, this paper proposes DIstributed VEhicular Re-routing system(DIVERT) for congestion avoidance, which leverages both cellular Internet and VANET communication [9]. DIVERT is a hybrid system because it still uses a server, reachable over the Internet, to determine an accurate global view of the traffic. The centralized server acts as a coordinator that collects location reports, detects traffic congestion and distributes re-routing notifications updated travel times in the road network to the vehicles [14]. However, the system offloads a large part of the re-routing computation at the vehicles and thus the re-routing process becomes practical in real-time. To take collaborative re-routing decisions, the vehicles situated in the same region exchange messages over VANETs. Also, DIVERT implements a privacy enhancement protocol to protect the user's privacy, where each vehicle detects the road density locally using VANET and anonymously reports data with a certain probability only from high traffic density roads. When signs of congestion are detected, the server sends the traffic map only to the vehicles that sent the latest updates. Subsequently, these vehicles disseminate the traffic data received from the server in their region. User privacy is greatly improved since this protocol reduces dramatically the number of vehicle location updates to the server and, thus, the driver exposure and identification risks [8]. Moreover, in this hybrid architecture, the server does not know the OD pairs of the users.

- To reduce the VANET overhead and to reduce vehicle-to-vehicle communication latency.
- To minimize the driver's privacy leakage by reducing the number of location reports uploaded at the server
- To maintain the traffic accuracy
- To significantly decrease sensitive location data exposure of the vehicles using privacy-aware re-routing system.

Hence, the main contribution of this article is the distributed system for re-routing.the rest of the paper organized as follows. Section III gives an overview of related works. Section IV describe the System architecture using DIVERT. Section V describe the modules of my paper. Section VI discusses about Results and discussion. Our proposed protocol can achieve better performance in terms of reducing the VANET overhead and to reduce the vehicle to vehicle communication latency and to maintains the traffic accuracy.

II. VEHICULAR AD-HOC NETWORKS

VANET are wireless networks which facilitate information exchange between mobile vehicles with no permanent network infrastructure required. VANETs become a cornerstone of the envisioned Intelligent Transportation Systems (ITS). There is an increasing interest in developing efficient vehicular ad-hoc routing protocols to expand the internet to vehicles on the road, thereby allowing point-to-point communication between vehicles as well as access to services available on the Internet in the proposed system is a novel vehicular communication system for detecting traffic jam through information gathered using inter-vehicles communication. This information is processed by the vehicles on-the-fly, allowing them to determine the congestion spots in urban areas, and thereby computing alternative and less congested itineraries.

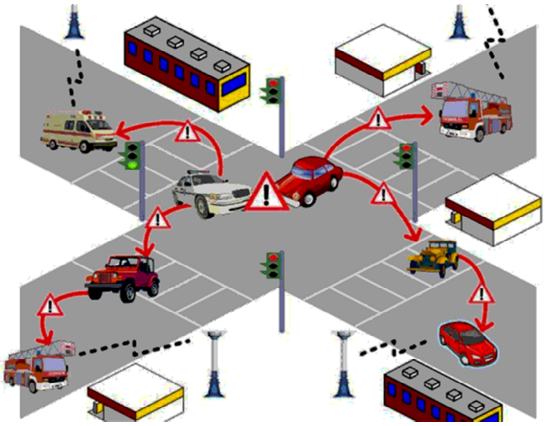


Figure 1. VANETs architecture

Traffic safety is the main concern for many countries. Many accidents are caused by insufficient traffic information and by slow driver reaction to local visual and acoustic inputs. VANETs (Vehicular Ad hoc Networks) overcome these problems by enhancing both the accuracy of traffic information and the delivery of alarms, thus helping prevent collisions as shown in Fig.1.In a VANET, cars communicate with each other over a wireless channel. They can send packets directly to neighbors within radio range[2]. Alternatively, intermediary cars route and forward packets to intended destinations. Communication is peer-to-peer, without centralized coordination. In VANETs[4], cars can exchange routine information such as current speeds, locations, directions, as well as emergency alarms like notifications of emergency braking, etc. With VANETs, cars can collect more accurate traffic information electronically than drivers can visually. Direct activation of commands (brakes, accelerator, steering wheel, etc.) by an alarm will ensure a car's prompt reaction without depending on the driver's alertness.

III. RELATED WORKS

In this section, the paper is related to DIVERT. We discuss the aspects related to server notification and privacy re-routing system.

Ruilin Liu, et al.., [1], have described the Themis: A participatory navigation system for balanced traffic routing. Navigators based on real-time traffic achieve suboptimal results since, in face of congestion, they greedily shift drivers to currently light-traffic roads and because of new traffic jams. Themis, a participatory system navigating drivers in a balanced way. By analyzing time-stamped position reports and route decisions collected from the Themis application, the Themis server estimates both the current traffic rhythm and future traffic distributions. According to the estimated travel time and a popularity score computed using the learned information, Themis coordinates traffic between alternatives and proactively alleviates congestions. Themis has been implemented and its performance has been evaluated at different penetration rates based on real data.

Juan Pan, et al.., .have describe the proactive vehicular traffic rerouting for lower travel time [3] Traffic congestion causes driver frustration and costs billions of dollars annually in lost time and fuel consumption. The five traffic rerouting strategies designed to be incorporated in a cost-effective and easily deployable vehicular traffic guidance system that reduces travel time. The proposed strategies proactively calculate individually tailored rerouting guidance to be pushed to vehicles when signs of congestion are observed on their route. The five proposed strategies are the Dynamic Shortest Path (DSP), the shortest path with repulsion (AR$*$), the random k shortest path (RkSP), the Entropy-Balanced kSP (EBkSP), and the Flow-Balanced kSP (FBkSP). The proposed strategies are capable of reducing the travel time as much as a state-of-the-art Dynamic Traffic Assignment (DTA) algorithm while avoiding the issues that make DTA impractical, such as the lack of scalability and robustness, and high computation time. Furthermore, the variety of proposed strategies allows tuning the system to different levels of tradeoffs between rerouting effectiveness and computational efficiency. Nicholas Loulloudes, et al.., describes [4] V-Radar: A vehicular traffic query protocol for urban environments Automobile congestions have an adverse effect on modern societies, causing the loss of billions of dollars and man hours every year throughout the world. In this era of global economic recession, drivers will require the necessary solutions and driving aids that facilitate the improvement of daily road transport and minimize unnecessary expenditure. The groundwork for V-Radar, a query protocol for retrieving vehicular traffic information using V2V communications[2]. The advantage of V-Radar over related works is its ability to monitor using location-dependent queries the prevailing traffic conditions in a number of road paths from a vehicle's current location towards its final destination: Raluca Ada Popa, et al.., have described the Privacy and Accountability for Location-based Aggregate Statistics [5]. The proposed system is a new location-based rewarding system, called LocaWard, where mobile users can collect location-based tokens from token distributors, and then redeem their gathered tokens at token collectors for beneficial rewards. Tokens act as virtual currency. It develops a security and privacy aware location-based rewarding protocol for the LocaWard system and proves the completeness and soundness of the protocol. Moreover, that the system is resilient to various attacks and mobile users' privacy can be well protected in the meantime. The system conducts extensive experiments to validate the system efficiency in terms of computation, communication, energy consumption, and storage costs. It provides an aggregate statistics protocol with strong location privacy guarantees, including protection against any general side information attack and to provides client accountability without a trusted party but in this protocol users do not share their location with other users. Baik Hoh, et al.., describes virtual trip lines for distributed privacy-preserving traffic monitoring [11]. Automotive traffic monitoring using probe vehicles with Global Positioning System receivers promises significant improvements in cost, coverage, and accuracy. Current approaches, however, raise privacy concerns because they require participants to reveal their positions to an external traffic monitoring server. To address this challenge, propose a system based on virtual trip lines and an associated cloaking technique. Virtual trip lines are geographic markers that indicate where vehicles should provide location updates. These markers can be placed to avoid particularly privacy sensitive locations[9]. They also allow aggregating and cloaking several location updates based on trip line identifiers, without knowing the actual geographic locations of these trip lines. Thus they facilitate the design of a distributed architecture, where no single entity has a complete knowledge of probe identities and fine-grained location information. It achieves the high-quality traffic information and strong privacy protection in this traffic monitoring system. However, the privacy of reporting users is one of the biggest challenges for such systems.

By John and B. Kenney describes Dedicated Short-Range Communications (DSRC) Standards in the United States [6]. Wireless vehicular communication has the potential to enable a host of new applications, the most important of which are a class of safety applications that can prevent collisions and save thousands of lives. The automotive industry is working to develop the (DSRC) technology, for use in vehicle-to-vehicle and vehicle-to-roadside communication. The effectiveness of this technology is highly dependent on cooperative standards for interoperability. It shows how these standards fit together to provide a comprehensive solution for DSRC. Most of the key standards are either recently published or expected to be completed in the coming year. A reader will gain a thorough understanding of DSRC technology for vehicular communication, including insights into why specific technical solutions are being adopted, and key challenges remaining for successful DSRC deployment. It is network acquisition, high reliability and priority Department of Transportation promoted the standards of interoperability, security and for privacy in transportation short-range communication, specifically WAVE system. Marco Gruteser and Dirk Grunwald describes The anonymous usage of location-based services through spatial and temporal cloaking[14]. The proposed system demonstrates that a practical, cost-effective, and efficient traffic re-routing system can be implemented and deployed in real-life settings. This system, DIVERT, offloads a large part of the re-routing computation at the vehicles, and thus, the re-routing process becomes scalable in real-time. To make collaborative re-routing decisions, the vehicles exchange messages over VANETs. It optimized VANET data dissemination to allow for efficient distributed re-routing computation. It reduces the communication overhead and scalable achieves the good level of location privacy protection. However, it assumes a system-wide static k value for all mobile clients, which affects the service quality for those mobile clients whose privacy requirements can be satisfied using smaller k values. Their approach fails to provide any quality of service guarantees with respect to the sizes of the cloaking boxes produced. This is because the quadtree-based algorithm anonymizes the messages by dividing the quadtree cells until the number of messages in each cell falls below k and by returning the previous quadrant for each cell as the spatial cloaking box of the messages under that cell.

IV. SYSTEM OVERVIEW

In this section discuss the DIVERT architecture and designing principle of the system.

A. DIVERT architecture

In this architecture is proposed to implement DIVERT is composed of a central server and a software stack running on an onboard device (e.g., a smartphone) in each participating vehicle as shown in Fig.2. DIVERT uses two types of communication. The vehicles communicate with the server over a 3G/4G network to report local traffic density data and receive the global traffic density in the road network (i.e., the pink line in Fig.2).

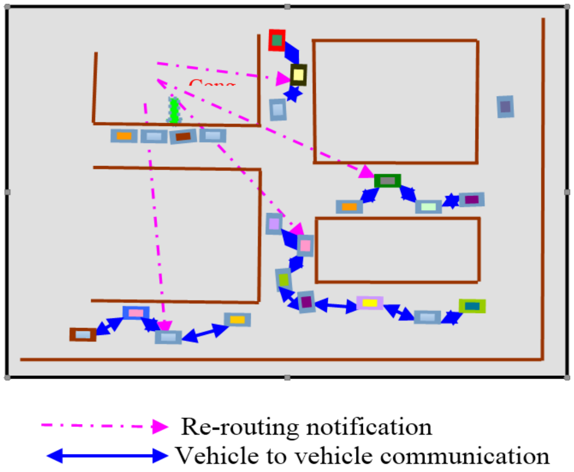


Figure 2. DIVERTs Architecture

The vehicles report data according to a privacy-aware algorithm also the vehicles that closely located communication with each other over VANETs to determine the local traffic density, to disseminate the traffic data received from the server, and to implement a distributed re-routing strategy (i.e., the blue line in Fig.2)

V. MODULES

A. Privacy-Aware Traffic Reporting

DIVERT strives to minimize the driver's privacy leakage by reducing the number of location reports uploaded at the server while maintaining good traffic accuracy. The vehicles communicate with the server to report local traffic density data and to receive the global traffic density in the road network. In Fig.4 vehicles report data according to a privacy-aware algorithm. A density-based traffic reporting mechanism is proposed wherein vehicles report to the server only if the road density is higher than a predefined threshold. The server computes the smoothed average of the traffic density on each road segment as it receives new traffic reports. The estimated density is computed locally by each vehicle, which obtains information about its neighbor vehicles by periodic exchange of beacons. Each vehicle counts the received beacons in a short time window and each vehicle emits beacons with the same frequency.

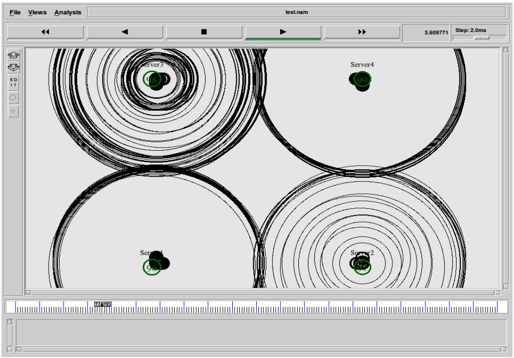
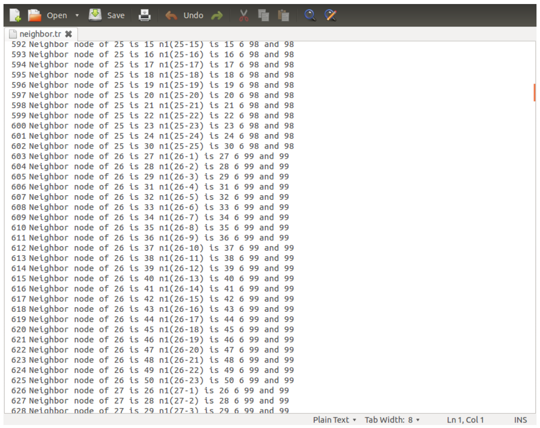


Figure 3. Network Environment

Each vehicle periodically checks the number of vehicles on the current road. In Fig3 the network environment having four server and hundred nodes are placed[10]. To obtain accurate traffic information, each vehicle encapsulates in the beacon the current road identifier and direction of traffic (side). When a vehicle estimates the number of cars, it only counts the beacons on the same road and side as itself. The vehicle reports the detected density to the central server.



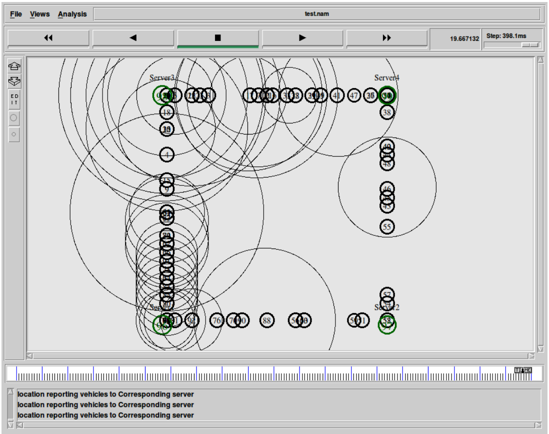
```
592 Neighbor node of 25 is 15 n1(25-15) is 15 6 98 and 98
593 Neighbor node of 25 is 16 n1(25-16) is 16 6 98 and 98
594 Neighbor node of 25 is 17 n1(25-17) is 17 6 98 and 98
595 Neighbor node of 25 is 18 n1(25-18) is 18 6 98 and 98
596 Neighbor node of 25 is 19 n1(25-19) is 19 6 98 and 98
597 Neighbor node of 25 is 20 n1(25-20) is 20 6 98 and 98
598 Neighbor node of 25 is 21 n1(25-21) is 21 6 98 and 98
599 Neighbor node of 25 is 22 n1(25-22) is 22 6 98 and 98
600 Neighbor node of 25 is 23 n1(25-23) is 23 6 98 and 98
601 Neighbor node of 25 is 24 n1(25-24) is 24 6 98 and 98
602 Neighbor node of 25 is 30 n1(25-25) is 30 6 98 and 98
603 Neighbor node of 26 is 27 n1(26-1) is 27 6 99 and 99
604 Neighbor node of 26 is 28 n1(26-2) is 28 6 99 and 99
605 Neighbor node of 26 is 29 n1(26-3) is 29 6 99 and 99
606 Neighbor node of 26 is 31 n1(26-4) is 31 6 99 and 99
607 Neighbor node of 26 is 32 n1(26-5) is 32 6 99 and 99
608 Neighbor node of 26 is 33 n1(26-6) is 33 6 99 and 99
609 Neighbor node of 26 is 34 n1(26-7) is 34 6 99 and 99
610 Neighbor node of 26 is 35 n1(26-8) is 35 6 99 and 99
611 Neighbor node of 26 is 36 n1(26-9) is 36 6 99 and 99
612 Neighbor node of 26 is 37 n1(26-10) is 37 6 99 and 99
613 Neighbor node of 26 is 38 n1(26-11) is 38 6 99 and 99
614 Neighbor node of 26 is 39 n1(26-12) is 39 6 99 and 99
615 Neighbor node of 26 is 40 n1(26-13) is 40 6 99 and 99
616 Neighbor node of 26 is 41 n1(26-14) is 41 6 99 and 99
617 Neighbor node of 26 is 42 n1(26-15) is 42 6 99 and 99
618 Neighbor node of 26 is 43 n1(26-16) is 43 6 99 and 99
619 Neighbor node of 26 is 44 n1(26-17) is 44 6 99 and 99
620 Neighbor node of 26 is 45 n1(26-18) is 45 6 99 and 99
621 Neighbor node of 26 is 46 n1(26-19) is 46 6 99 and 99
622 Neighbor node of 26 is 47 n1(26-20) is 47 6 99 and 99
623 Neighbor node of 26 is 48 n1(26-21) is 48 6 99 and 99
624 Neighbor node of 26 is 49 n1(26-22) is 49 6 99 and 99
625 Neighbor node of 26 is 50 n1(26-23) is 50 6 99 and 99
626 Neighbor node of 27 is 26 n1(27-1) is 26 6 99 and 99
627 Neighbor node of 27 is 28 n1(27-2) is 28 6 99 and 99
628 Neighbor node of 27 is 29 n1(27-3) is 29 6 99 and 99
```

Figure 4. Privacy-Aware Traffic Density

Each node maintains and updates the neighbor list and corresponding server periodically as shown in Fig.3

B. Server Notification

After car reports, it stops reporting for a time period to prevent frequent reporting that could lead to privacy leakage. The server receives reports from vehicles indicating the number of vehicles on a road segment and computes the traffic density on the roads. Every time the server receives a report concerning a road rc, it will smooth the computed average current density value and sends the notification to vehicles which are the nearer to congestion spot.



```
location reporting vehicles to Corresponding server
location reporting vehicles to Corresponding server
location reporting vehicles to Corresponding server
```

Figure 5. vehicles to server communication

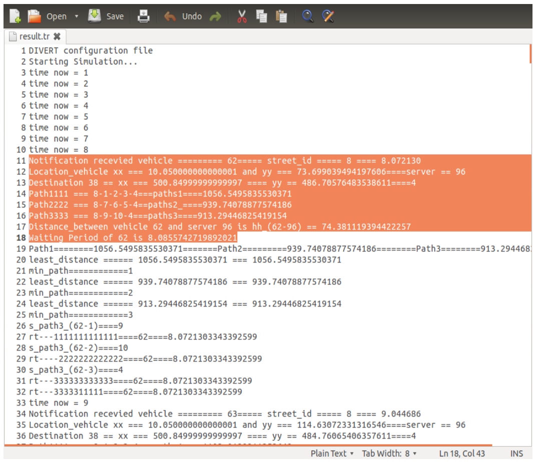
The network with nodes are placed like a vehicles and communicate between vehicle to vehicle as shown in Fig.4. Each vehicles reporting the Location and update the message from corresponding server

C. Distributed Re-routing Strategies

If the server detects signs of congestion in the road network, it will alert the vehicles by sending the updated map information, containing tuples such as road id, newly computed travel time for all the roads that have a current travel time different from the free flow travel time. The server sends messages only to the vehicles that reported most recently and that are located near a congestion spot. The server notification triggers the re-routing process that consists of a dissemination phase and a route computation phase. All the notified vehicles participate in the updated map data dissemination, but only the vehicles whose current paths traverse a congestion spot execute the computation phase. The route information depends on the re-routing strategy employed by DIVERT, i.e., either the k-shortest paths or the OD pair of the vehicle[13]. Two distributed re-routing strategies are presented there are, Entropy Based k Shortest Paths (distributed EBkSP), and A* with Repulsion (AR*) algorithm (distributed AR*). In the centralized version, the rank of each vehicle is assigned by the server. Here, each vehicle picks a random rank value between 0 and rank max which is the estimated total number of re-routed vehicles; rank max is calculated by each re-routed vehicle based on the traffic density of the incoming road segments. A vehicle of a certain rank computes a new route by considering the higher ranked vehicle paths. In dEBkSP, each vehicle affected by congestion calculates the k loop-less shortest paths based on its current OD pair and the updated travel times on the roads. Then, the vehicles disseminate their rank and k shortest paths in their region for a predefined time interval. In the final route computation phase, each vehicle iterates through the local sorted list of vehicles for which it has received information. in the case of dAR*, the notified vehicle chooses a random rank but it does not compute the k shortest paths. Instead, the notified vehicles only broadcast their OD pairs. In the event of a broadcast timeout, for each received OD pair in the buffer, the vehicle applies the original AR* algorithm to compute a virtual path. the current vehicle computes the best shortest path for itself based on other vehicles' paths.

D. Optimizations for Re-routing Information Sharing

The effectiveness of the distributed re-routing strategies mainly depends on the amplitude of the re-routing information dissemination among vehicles. Achieving the best level of dissemination in VANETs is challenging for two main reasons. First, the data dissemination has to be done in real-time and therefore the dissemination time interval is short. Second, regular data dissemination in VANETs exhibits poor performance in congested areas because of wireless contention. DIVERT uses a prioritized dissemination to avoid that all the notified vehicles in a region start broadcasting at the same time, and thus reduce the network contention. When receiving a congestion notification, vehicle waits some seconds before broadcasting its OD pair or its k-shortest paths.



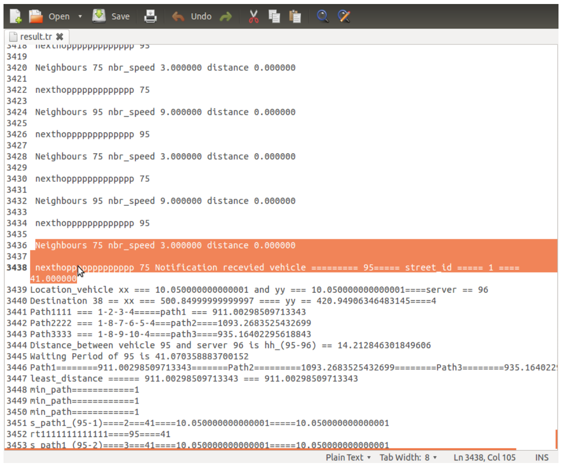
```
DIVERT configuration file
Starting Simulation...
time now = 1
time now = 2
time now = 3
time now = 4
time now = 5
time now = 6
time now = 7
time now = 8
Notification recevied vehicle ========= 62===== street_id ===== 8 ==== 8.072130
Location_vehicle xx === 10.050000000000001 and yy === 73.699039494197606====server == 96
Destination 38 == xx === 500.84999999999997 ==== yy == 486.70576483538611====4
Path1111 === 8-1-2-3-4===paths1====1056.5495835530371
Path2222 === 8-7-6-5-4==paths2_====939.74078877574186
Path3333 === 8-9-10-4===paths3====913.29446825419154
Distance_between vehicle 62 and server 96 is hh_(62-96) == 74.381119394422257
Waiting Period of 62 is 8.0855742719892021
Path1=======1056.5495835530371======Path2========939.74078877574186=======Path3=======913.294468
least_distance ====== 1056.5495835530371 === 1056.5495835530371
min_path===========1
least_distance ====== 939.74078877574186 === 939.74078877574186
min_path===========2
least_distance ====== 913.29446825419154 === 913.29446825419154
min_path===========3
s_path3_(62-1)====9
rt---1111111111111====62====8.0721303343392599
s_path3_(62-2)====10
rt----2222222222222====62====8.0721303343392599
s_path3_(62-3)====4
rt---333333333333====62====8.0721303343392599
rt---3333311111====62====8.0721303343392599
time now = 9
Notification recevied vehicle ========= 63===== street_id ===== 8 ==== 9.044686
Location_vehicle xx === 10.050000000000001 and yy === 114.63072331316546====server == 96
Destination 38 == xx === 500.84999999999997 ==== yy == 484.76065406357611====4
```

Figure 6. Broadcast

After notification received by vehicle it calculates waiting period for broadcasting (Fig. 6). If waiting period is greater than threshold means it broadcast the k shortest path other wise it does not broadcast (Fig.6). The waiting time is determined based on the rank of the vehicles. The rationale is that the higher rank vehicle information is more important since each vehicle computes its own path based on the higher ranked vehicle paths. Data compression is the another option to optimize the information dissemination between vehicle. A large packet size increases the communication overhead and decreases the dissemination effectiveness. The dAR* re-routing strategy is very efficient from the communication point of view since vehicles only disseminate their OD pair. However, this is not the case in the dEBkSP algorithm that requires vehicles to transmit their k-shortest paths. Hence, depending on the k value and the distance between the origin and destination, the size of the messages can be large. Data dissemination in VANETs can be significantly affected by packet losses. To allow vehicles to recover lost packets, a supplementary XOR coding field is appended to each transmitted packet. When receiving a packet, a vehicle may recover one of the lost packets from the XOR field. This technique helps to reduce the number of transmissions and also improves vehicles' knowledge coverage. In this way, each vehicle can build up a neighbor table containing the knowledge of its neighbors. This table is essential for finding the best coding. In DIVERT, a distance-based timer approach is used to reduce excessive broadcasting when multiple vehicles are within communication range. After receiving a broadcast message, the vehicle waits for a certain time period until rebroadcasting the message. The waiting time period is inversely proportional to the distance between the receiving vehicle and the source vehicle. Therefore, a vehicle that is farther from the message source should re-broadcast the message earlier.

E. Data Forwarding through Stable Neighbor

If the vehicle involved in the forwarding path vehicle moves in opposite direction the source then there is the situation of link failure which leads to packet loss. Hence, it is required to select the vehicles with mobility relative to source vehicle which means selection of stable vehicle as forwarder based on its mobility. Source vehicle predicts the distance of each neighbor from itself at the particular time (t) using the current location of neighbor and speed of the neighbor.



```
 nexthoppppppppppppp 95

 Neighbours 75 nbr_speed 3.000000 distance 0.000000

 nexthoppppppppppppp 75

 Neighbours 95 nbr_speed 9.000000 distance 0.000000

 nexthoppppppppppppp 95

 Neighbours 75 nbr_speed 3.000000 distance 0.000000

 nexthoppppppppppppp 75

 Neighbours 95 nbr_speed 9.000000 distance 0.000000

 nexthoppppppppppppp 95

 Neighbours 75 nbr_speed 3.000000 distance 0.000000

 nexthoppppppppppppp 75 Notification recevied vehicle ========= 95===== street_id ===== 1 ====
41.000000
Location_vehicle xx === 10.050000000000001 and yy === 10.050000000000001====server == 96
Destination 38 == xx === 500.84999999999997 ==== yy == 420.94906346483145====4
Path1111 === 1-2-3-4=====path1 === 911.00298509713343
Path2222 === 1-8-7-6-5-4===path2====1093.2683525432699
Path3333 === 1-8-9-10-4====path3====935.16402295618843
Distance_between vehicle 95 and server 96 is hh_(95-96) == 14.212846301849606
Waiting Period of 95 is 41.070358883700152
Path1=======911.00298509713343======Path2=========1093.2683525432699========Path3========935.164022
least_distance ====== 911.00298509713343 === 911.00298509713343
min_path===========1
min_path===========1
min_path===========1
s_path1_(95-1)====2===41====10.050000000000001=====10.050000000000001
rt1111111111111====95====41
s_path1_(95-2)====3===41====10.050000000000001=====10.050000000000001
```

Figure 7. Stable Neighbor

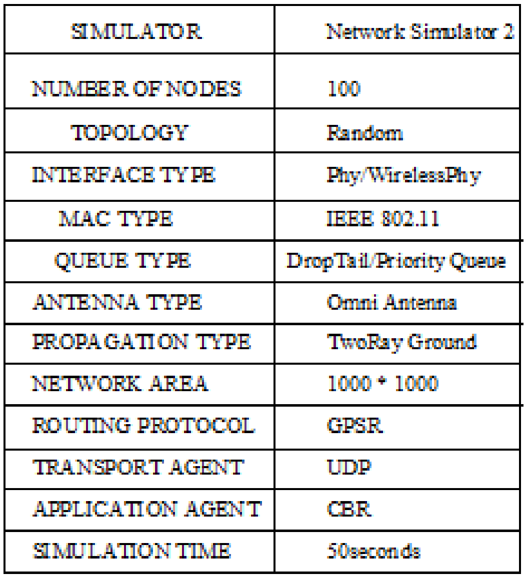
If the vehicle comes under neighbor status then it is highly stable neighbor (Fig.7). The neighbor which is having the minimum distance is selected as forwarder. After a certain time (t+T) it predicts the distance again using the current location and speed of the neighbor vehicle (in Fig. 7). In both times if the vehicle comes under neighbor status then it is a highly stable neighbor. The neighbor which is having the minimum distance is selected as the forwarder.

VI. RESULTS AND DISCUSSIONS

The performance of DIVERT (Distributed Vehicular traffic re-Routing system) is analyzed using network simulator2. The experimental model is built with 100 nodes distributed on a surface of 600 X 600 m2 [12] DIVERT implements a privacy enhancement protocol to protect the user's privacy, where each vehicle detects the road density locally using VANET and anonymously reports data with a certain probability only from high traffic density roads. When signs of congestion are detected, the server sends the traffic map only to the vehicles that sent the latest updates. Subsequently, these vehicles disseminate the traffic data received from the server in their region. User privacy is greatly improved since this protocol reduces dramatically the number of vehicle location updates to the server and, thus, the driver exposure and identification risks [8]. Moreover, in this hybrid architecture, the server does not know the OD pairs of the users. Hence, the main contribution of this article is the distributed system for re-routing.

VII. PERFORMANCES AND EVALUATION

A. Simulation Model



SIMULATOR	Network Simulator 2
NUMBER OF NODES	100
TOPOLOGY	Random
INTERFACE TYPE	Phy/WirelessPhy
MAC TYPE	IEEE 802.11
QUEUE TYPE	DropTail/Priority Queue
ANTENNA TYPE	Omni Antenna
PROPAGATION TYPE	TwoRay Ground
NETWORK AREA	1000 * 1000
ROUTING PROTOCOL	GPSR
TRANSPORT AGENT	UDP
APPLICATION AGENT	CBR
SIMULATION TIME	50seconds

Figure 8. Simulation Model

(i) Network overhead is reduced

Overhead is any combination of excess or indirect computation time, memory, bandwidth, or other resources that are required to attain a particular goal. Network overhead can be calculated by sending a fixed-size data transmission across the network and observing the number of extra bytes of data transmitted for the action to be completed.

(ii) Better scalability is achieved

Scalability can refer to the capability of a system to increase its total output under an increased load when resources are added. It is measured by packet delivery ratio or delay.

(iii) Efficient Re-routing is achieved

Rerouting is a technique that can be used in Packet Switching networks. When a link in a network fails, traffic that was using the failed link must change its path in order to reach its destination.It is measured by the total travel time of the vehicle.

(iv) Throughput

How much data can be transferred from one location to another in a given amount of time. It is used to measure the performance of sources to destination

(v) End to end delay

It refers to the time taken for a packet to be transmitted across a network from sources to destination

(vii) Packet Delivery Ratio

It is defined as the ratio between the received packets by the destination and the generated packets by the sources

Comparative Graph

Throughput

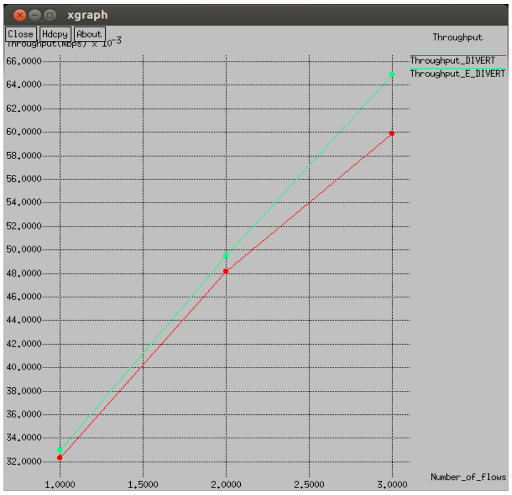


Figure 9. Throughput

Here the X axis represents the number of flows and Y axis represents the Throughput(Mbps). E_DIVERT achieves increased Throughput when compared to DIVERT method.

Delay

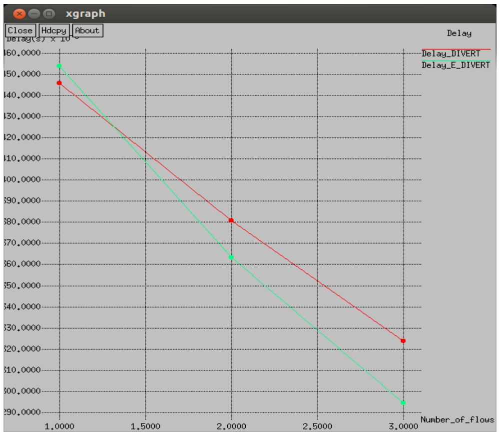


Figure 10. Delay

Here X-axis represents the number of flows and Y-axis represents time Delay(s) .E_DIVERT achieves reduced delay when compared to DIVERT method.

Control Overhead

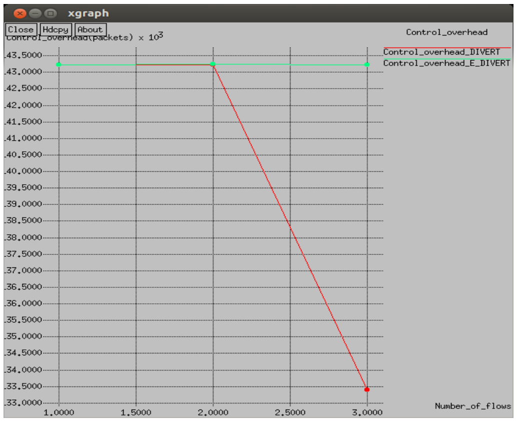


Figure 11. Control Overhead

Here the X-axis represents a number of flows and Y-axis represent Control Overhead(packets). Control overhead is similar for DIVERT and E-DIVERT.

Packet Delivery Ratio

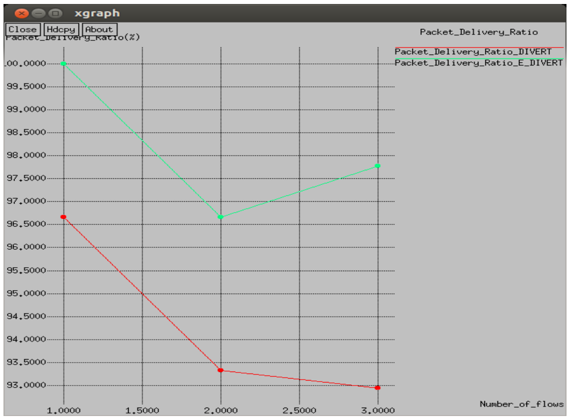


Figure 12. Packet Delivery Ratio

Here X axis is a number of flows and Y axis Packet Delivery Ratio (%). E_DIVERT achieves increased packet delivery ratio when compared to DIVERT method.

VII. CONCLUSION

The proposed system demonstrates that a practical, cost-effective, and efficient traffic re-routing system can be implemented and deployed in real-life settings. This system, DIVERT, offloads a large part of the re-routing computation at the vehicles, and thus, the re-routing process becomes scalable in real-time. To make collaborative re-routing decisions, the vehicles exchange messages over VANETs. It optimized VANET data dissemination to allow for efficient distributed re-routing computation. In addition, the system balances user privacy with the re-routing effectiveness. The simulation results demonstrate that, compared with a centralized system, DIVERT increases the user privacy substantially.

REFERENCES

[1] Ruilin Liu, Hongzhang Liu, Daehan Kwak, Yong Xiang, Cristian Borcea, Badri Nath and Liviu Iftode, “Themis: A Participatory Navigation System for Balanced Traffic Routing” In Proceedings of the IEEE Vehicular Networking Conference (VNC), pp. 159–166, 2014.

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

[3] Juan Pan, Iulian Sandu Popa, Karine Zeitouni, and Cristian Borcea, “Proactive Vehicular Traffic Rerouting for Lower Travel Time” IEEE Transactions on Vehicular Technology, Vol. 62, No. 8, 2013.

[4] Nicholas Loulloudes, George Pallis, and Marios D. Dikaiakos, "V-Radar: A Vehicular Traffic Query Protocol for Urban Environments" In Vehicular Traffic Management for Smart Cities (VTM), First International Workshop on, IEEE, pp. 1–6, 2012.

[5] Raluca Ada Popa, Andrew J. Blumberg, and Hari Balakrishnan, "Privacy and Accountability for Location-based Aggregate Statistics", In Proceedings of the 18th ACM conference on Computer and communications security, ACM, pp. 653–666, 2011.

[6] By John and B. Kenney, “Dedicated Short-Range Communications (DSRC) Standards in the United States” In Proceedings of the IEEE Transaction on, Vol. 99, No. 7, pp. 1162–1182, 2011.

[7] M. Behrisch, L. Bieker, J. Erdmann, and D. Krajzewicz. Sumo - simulation of urban mobility: An overview. In Proceedings of the 3rd International Conference on Advances in System Simulation(SIMUL 2011), pages 63–68, Barcelona, Spain, 2011.

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

[9] T. Xu and Y. Cai. Feeling-based location privacy protection for location based services. In Proceedings of

the 16th ACM conference on Computer and communications security, pages 348–357. ACM, 2009.

[10] TeerwatIssariyakul, EkramHossain, “Introduction to Network Simulator NS2” Springer,2009.

[11] Baik Hoh, Marco Gruteser, Ryan Herring, Jeff Bana, Dan Work, Juan-Carlos Herrera, Alexandre Bayen, Murali Annavaram and Quinn Jacobson, “Virtual Trip Lines for Distributed Privacy-Preserving Traffic Monitoring” In Proceedings of the 6th International Conference on Mobile Systems, Applications and Services, ACM, pp. 15–28, 2008.

[12] Broder and M. Mitzenmacher. Network applications of bloom filters: A survey.Internet Mathematics, 1(4):485–509, 2004.

[13] R. Dingledine, N. Mathewson, and P. Syverson. Tor: The second-generation onion router. Technical report, Naval Research Lab Washington DC, 2004.

[14] Marco Gruteser and Dirk Grunwald, “Anonymous Usage of Location-Based Services Through Spatial and Temporal Cloaking” In Proceedings of the 1st International Conference on Mobile Systems, Applications and Services, ACM, pp. 31-42. 2003.