ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 13, March 2017

A REAL TIME INTERFERENCIA CANFOD AND TRAIAL ROUTAGE IN VANET

[1] V.Vashu Reathaa [1],[2]G.Umamaheswari[2], [3]S.Gurubharathi[3], [4] J.Veeneswari(Asst Professor/CSE)
[1],[2],[3] (UG student)
E-Mail:umakirubha193@gmail.com
P.S.R.Rengasamy College Of Engineering For Women In Sivakasi.

***Abstract*—** A Jamming is one of the most important thread that disturb wireless network and communication. Many papers have been researching the jamming in wireless network. In vehicular-Ad hoc–network (VANet) we use jamming attack and building realistic jamming model and implement different jamming scenarios with respect to their mobility. we perform intensive experiment using NS2 simulation to study the threat of jamming attack in urban and highway roads. Then we propose a new jamming detection scheme to allow each node in vehicular network to detect jamming on its own. We can find out best path in mobilism.

Keywords: VANET; Detection system; ITS; Jamming problem; Vehicle Network; Android application; path planning

I. INTRODUCTION

Vehicular –ad-hoc Networks (VANETs) is road side communication network. It is wireless communication with self organizing system .VANET is a technology that were moving cars as a node in a network to create a mobile network. This can be achieved by utilizing cars to work as early warning devices against hazards while driving. Implementing intelligent transportation system (ITS) was provide innovate services relating to different nodes of transport and traffic management. ITS is an emerging transportation system which is comproised of an advanced information and telecommunication network for users, roads and vehicles. ITS is the integrated application of advanced technologies using electronics, mobile devices communication and advanced sensor.

Intelligent transportation systems (ITS) is advanced applications for providing innovative services which are related to transport and traffic management and allow users to be better informed and make safer, coordinated, and smarter use of transport networks. VANETs can provide enhanced Companies and Industries have acknowledged the importance and the capabilities of VANet. Thus started investing has improving all the aspects to increase the feasibility. In spite of the ongoing research efforts (academically and industrially), many security issues yet need to be addressed and resolved.

communication capabilities to collect real-time traffic related information delivery Both vehicle delivery Both vehicle-to-vehicle(V2V) and vehicle-to-roadside (V2R) communications are supported in VANETs to efficiently collect traffic updates to vehicles and roadside units. As a result, collected real-time traffic information can be utilized for freeway traffic flow management, path planning, and vehicle localization .However, most of the works assume that the incorporated techniques have small delivery delay for real-time collection of traffic information.

As VANETs is a short-range communication, the transmission delay cannot be neglected. Therefore, it is necessary to study how the transmission performance can affect the path planning Performance and how to design different transmission mechanisms to reduce delay when it cannot be neglected.

In this ,We propose a real-time algorithm that utilizes VANET communication facility to avoid vehicles from traffic congestion to a new system that utilizes beacons packets to alert nodes in the network at the presence of jamming attacks. when driving into an affected zone .The system work as a real-time jamming detection system to identify jammers and alert drivers to overcome the threat.

II. BACKGROUND & RELATED WORK

Traffic jam become a major problem in transportation which can result in late arrivals at additional cost for drivers. However, we can reduce this cost by navigation or path planning which will help to avoid traffic jam. For example, vehicles can be rerouted with the shortest path to their destination based on GPS navigation etc.

However, these approaches are not effective because update of the traffic information is not real-time. Thus, the real-time traffic information is important . Therefore, it is necessary to study how the transmission performance can be affect in path planning and how to design different transmission mechanisms to reduce delay when it cannot be changed .

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 13, March 2017

Since VANet provides promising potential to the safety of driving, hence it is essential to secure it against exploitation. At the same time, the Quality of Service (QoS) is very important to take in consideration when securing VANet against different security breaches. VANet provides promising potential to enhance the safety of driving, hence it is essential to secure it against exploitation. At the same time, the Quality of Service (QoS) is very important to take in consideration when securing VANet against different security breaches. [6] discussed about a system,the effective incentive scheme is proposed to stimulate the forwarding cooperation of nodes in VANETs. In a coalitional game model, every relevant node cooperates in forwarding messages as required by the routing protocol. This scheme is extended with constrained storage space. A lightweight approach is also proposed to stimulate the cooperation.

The proposed a new model based on the measure of the correlation among the error and the correct reception times in order to detect jamming attack when present Another research paper studied the beacon frequency in VANET and proposed a new scheme called Distributed Beacon Frequency Control (DBFC) algorithm to reduce the beacon load and improve the channel condition by adjusting the transmit parameters according to the network condition

Our work is based on utilizing beacon packets to real time detect jammers or denial of Service (dos) attacks hence we look into understand the contents and requirements of beacon packets We focus the light in next section on explaining the different type of communication that VANet uses to grasp the network behaviors.

III. COMMUNICATION OVERVIEW

When the dealing with Vehicular Network communications we need to make distinction between different terms that we see Hence we present in this section the most widely spread acronyms that any reader will come across when dealing with VANet research.

A.WAVE

(Wireless Access in Vehicular Environment) is one of the IEEE1609 family of standards for Wireless Access in Vehicular Environment The family of theIEEE1609 standards describe the architecture communications model protocols security mechanisms network services multichannel operation use of Provider Service Identifiers and how they work with the physical layer and media access layer for high speed of the (up to 27 Mb/s) short range (up to 1000m) the low latency wireless communications in the vehicular environment of The main architectural components defined by these standards are the on Board Unit (OBU) Road Side Unit (RSU) and WAVE interface.

These standards also describe the functionality of applications that utilize WAVE in the WAVE environment .

VII (Vehicle Infrastructure Integration) has a main objective to deploy communications infrastructure that will support both vehicle to infrastructure as well as vehicle to vehicle communications, for a variety of applications. Principal applications are under development such as noticing drivers for unsafe conditions and collision which can be avoided .

VSC (Vehicle Safety Communication) has run many experiments with National Highway Traffic and Safety Administration (NHTSA). Its objective is to improve safety with the use of Dedicated Short Range Communication (DSRC), with requirements and parameters for safety applications, traveler information and fuel efficiency .

IVI (Intelligent Vehicle Initiative) has a goal to decrease severity of crashes by avoiding driver mistakes. It is based on vehicle to vehicle communication .

C2C (Car-to-Car Communication) was started in 2001 and has a main objectives of development and release of an open European standard with driver assistance and safety applications. It is also based on vehicle to vehicle communication .

Some of the recent techniques includes: Realization of bus transportation system, which uses Radio Frequency Identification (RFID) and wireless sensor technology to enhance public transportation system .Intelligent transportation system with wireless sensor network monitors online travel buses in real-time, to achieve the purpose of intelligent management and traffic measurement.

B. Behaviors classification

Besides categorizing jammers based on their mobility, jammers can adopt different behaviors. Here we present the different behavior that jammers may adopt when launching attacks.

I. Constant

A constant jammer sends out random radio signals all the time at the wireless medium. This type of jammers does not follow any underlying MAC protocol. The objective of this type of behavior is to prevent legitimate user from accessing communication channels or corrupt the sent out data by creating interference.

II. Random

Jamming requires high power to emit signals to the wireless medium hence; jammers lifetimes are restricted due to energy failure problem. Thus, random jamming helps adversaries to launch jamming attacks for longer period. The attacker can alternate between going to sleep mode for t_S seconds then wake up and jam for t_J seconds. This allows jammers to have more control over energy consumption by altering t_S & t_J as needed. This type of jammers can follow any jamming mobility model when launchingtheattack.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 13, March 2017

IV. Jamming models, threats & challenges

Jamming is a attack that intentionally attempts to interfere, disrupt, or block wireless communications. There are different jammers devices with different size . In this work, we focus exclusively on Jamming attacks communications – particularly transmitted and received packets. In order to evaluate jamming affect accurately we need to understand how they work.

Next we introduce different aspects that we considered when modeling jammers in a vehicular network.

Radio propagation model: We build our jamming model based on free-space and shadowing model which were used to model the received signal power. The difference between the two models is that shadowing model captures both path loss versus distance and attenuation due to object blockage (building, trees, hills, etc) while free-space can only be considered where buildings and natural obstacles are very limited. In this work, we research both models to ensure the feasibility of our work when considering either one.

Several variables in jamming characteristics impact the communication differently. In order to evaluate jammers affect accurately, we propose two classifications of jammers based on their mobility and behaviors.

A. Mobility classification

Jammers can be divided into 3 different categories based on their mobility. Classifying jammers based on their mobility is crucial due to different types of nodes in VANET- stationary nodes (RSUs) and mobile nodes (vehicles). In order to solve the detection problem, we need to study the mobility of jammers. Hence, all jammers can be categorized under one of three following types –with respect to their mobility

1) Stationary

A Jammer who is not moving when launching the attack is considered stationary. A jammer can be standing on feet, sitting in a car (while the car is parked), or just sitting in a building. The effect of this type of jamming can only be in the same jammer's area at that time rather than jamming different areas. A stationary jammer has full control over their jamming location and distance between nodes N.

2) Targeting mobility

This is the same as the stationary jammer except that jammer is mobile (moving) while launching jamming attack. Jammer of this type might be in a car driving or walking in feet while the jammer device is on. The unique property of this type of jamming is that jammer is targeting a specific node (vehicle). The motive can be due to grudge, anger, envy, or just for sheer joy. Targeting-mobile jammers drive and stay in close range to one car to ensure the jamming affect.

3) Random mobility

Jammers in this category type is similar to the previous one (targeting mobility). The only difference is that jammer on roads -compatible with the standards- to make the best use of nodes and their communication.

3) Reactive

Most of jamming models target packets at the sender and prevent them from being transmitted. Reactive jammers behave a little differently by targeting packets that being transmitted to prevent the delivery at receiver nodes. Reactive jammers constantly listen to channel, and when jammer sense packets to be sent, he/she starts transmitting radio signals to cause collision and corrupt data that packet transfers.

V. Proposed detection-system

In order to detect jamming attacks reliably in VANet, nodes need to have the ability to estimate the channel condition and adjust their transmitting frequency (beacons) accordingly. We adopt Geographical Routing Algorithm proposed in to update the transmitting beacon Frequency (*bf*) in the nodes. Our contribution is that we build a detection system based on utilizing the bf to detect jamming attacks quickly and reliably by nodes (OBUs & RSUs). We also propose a unique placement strategy to deploy RSUs on the roads to improve the delivery of warning messages around the network and enable RSUs to detect jamming attacks.
Another technique has vehicles equipped with onboard unit to enable V2V communication for delivering the vehicle information (for e.g., vehicle location, density, and velocity) . When any vehicle senses accident related congestion, warning message will get generated and shared among all vehicles as well as with nearest roadside unit via V2R communication.

Signal Monitoring and Control

Signal monitor and control is becoming more complicated in today's life, as nobody is ready to wait on signal until it turns into green, which leads to a large number of accidents and traffic congestion. This problem can be overcome by controlling the traffic signal on real time using Vehicular Ad-Hoc Network protocol, so nobody has to wait unnecessarily on signal, and it will be helpful to minimize accidents at signal.

Path Planning

Traffic congestion problems have become a very crucial problem, because of rapid growth of car ownership. These cause great inconvenience to people in their daily life and also bring environmental pollution, waste of energy, traffic jams. This automatically affects the improvement of people's living standard, social and economic development. Path planning for urban traffic can solve the problem of road congestion and travel inconvenience.

RSU PLACEMENT & DEPLOYMENT

IEEE 802.11p Standards allows up to 27 Mbps data exchange rate and 1000 meter in radius apart between nodes.We propose a new placement technique to be used when deploying RSUs on roads -compatible with the standards- to make the best use of nodes and their communication.
When placing RSUs in urban or highway areas we propose placing RSU every 900 meter along the road to ensure the availability of communication. Doing so, allows every RSU to communicate constantly and consistently with two neighborsat least- along the road all the time.

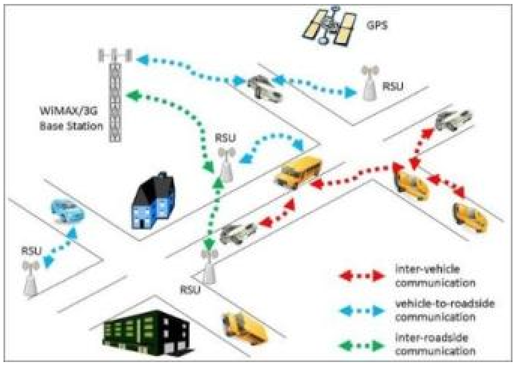


Figure2: Proposed Road-Side Units (RSUs) Placement technique

Implementing the proposed placement technique will allow each R to maintain a table for its both RN_i IDs and track changes in RN_i tables. Such a scenario can be easily implemented by periodically broadcasting beacons (beacons probing). We use the above suggested technique

in placing as many R_X as desired at the deployment phase to propose a jamming detection system. More details regarding system detection design is giving in the following section.

B. Beacon packet format

Since, there is no standards or restrictions regarding the contents of the beacons packets, many researchers suggested different models to describe the contents and sizes of the beacons packets. In this paper we propose a simple model - with crucial yet small dataset- to form our beacons packets. We adopt the beacon format that was suggested by Humeng in their work [11]. Based on the proposed format, each beacon has to include essential data such as (Source Address, beacon Frequency, Sequence Number, etc) figure 3.

Source Address	Beacons Freq.	Sequence Num.	Time Stamp	Position, Speed, Direction, Acceleration

Figure3: Vehicle OBU's Beacon Packet Content

We implemented the previous beacon format to be generated and transmitted by all OBUs (O_i) . We also implemented a simpler format to be generated by R_i to reduce network.

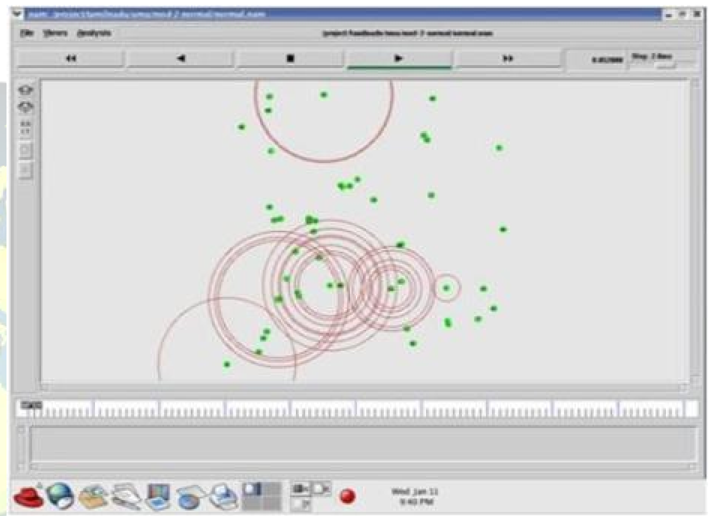
C. Detection system

Our detection system consists of two different schemes in which one will be implemented and adopted by OBUs and the other is solely for RSUs. two detection systems as OBU-DS and RSU-DS for distinction purposes.

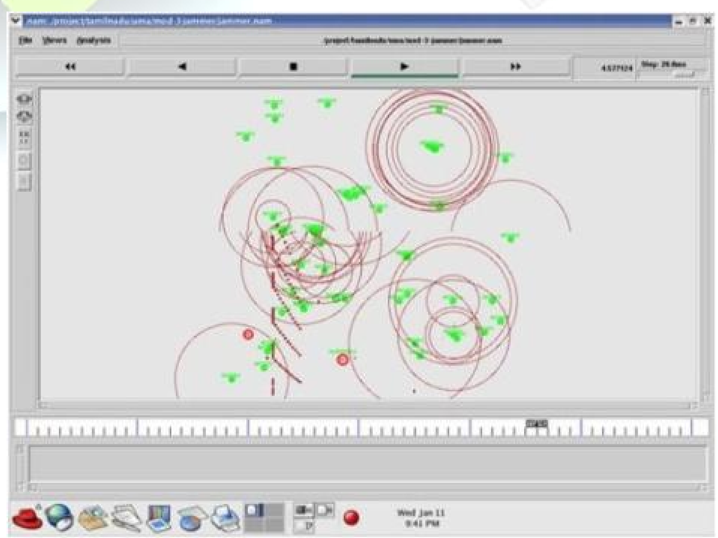
1) RSU-DS design overview

Based on the proposed RSU placement technique, each RSU node will have two neigh bore -highway- or more urban- to communicate with constantly. Our system design depends on utilizing the RSUs placement and the periodic probing technique in exchanging messages to detect jammers. there are two possibilities of jammers affect when launching an attack. Jammer can block all type of communications and entirely isolate nodes from the network. This can be achieved by jamming all the network frequencies. Jammers can also create noise to increase the packet drop rate and disrupts communication depending on the SNR.

Full Jamming: Depending on jammer transmission power, frequency and distance from the node, jammers can block all communications coming in to a node causing Denial of Service (DoS). When jammers intention is to drop all packets and take a node out of the network, they transmit useless data on the network frequency at close distance to overload the node and block communications.



Our detection method allows each node to detect if it is under jamming attack. Each node acts as an individual detection system and it is the node's responsibility to detect when it is under attack. Hence, we avoid the communication overhead to detect jamming attacks by allowing nodes to participate and be part of the detection system.

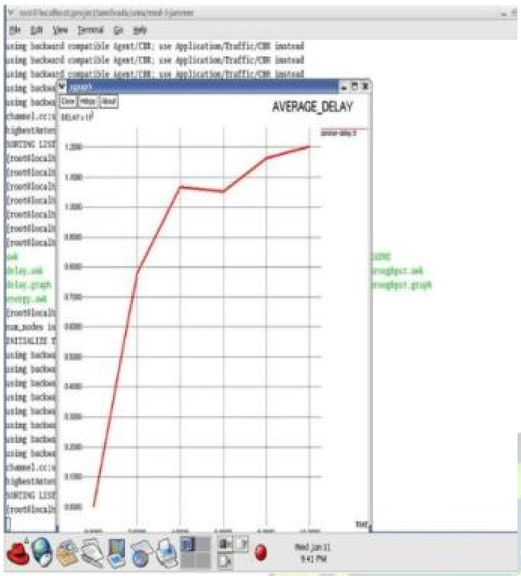


After running experiments we collected data from the Packet

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 13, March 2017

Trace File (PTR). Chart 1 shows the relation between the number of nodes and the number of

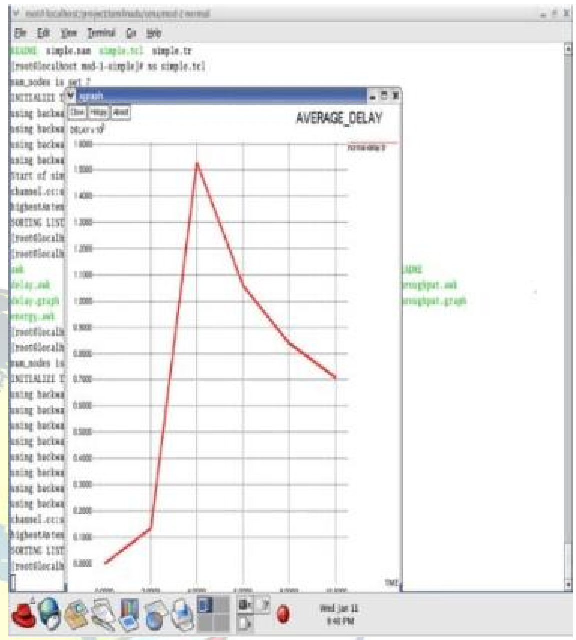


delivered beacons.

We then simulated the same previous cases with additional node which was configured to behave as a jammer. When simulating jammer w e took in consideration the different mobility and behaviors that jammers may adopt.
We noticed a significant drop in the data packets including beacons packets. W e also noticed that when simulating a stationary jammer, the results were almost similar when jammer is adopting a reactive or constant jamming behavior. That's because jamming affect will only shows while the attack is being launched (active). Likewise, obile jamming will have the same affect when adopting constant or reactive jamming.
The only difference is that jamming affect will take a place only in the affected area. Chart 1 shows different jamming impact (stationary & mobile) on the number of received beacons packets.

In our simulation we use the following metrics to evaluate the feasibility and effectiveness of the proposed detection systems:

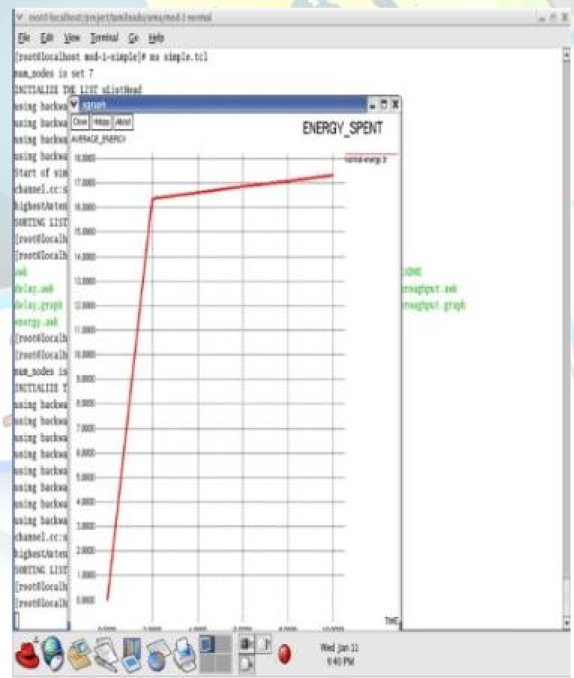
(TN): Jammer detected but no jammer exists.
(TP): Jammer detected while they exist.
(FN): No jammer detected when no jammer exists.
(FP): No jammer detected but jammer actually exists



This is fully compatible with 802.11p and safety-related applications requirements. When jammers exist, the communications get disrupted and the number of beacons drops to below the suggested value for safety-related applications .Table 3 shows the detection system accuracy –in percentage- when dealing with different jamming types and behaviors.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
***Available online at* www.ijartet.com**

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 13, March 2017

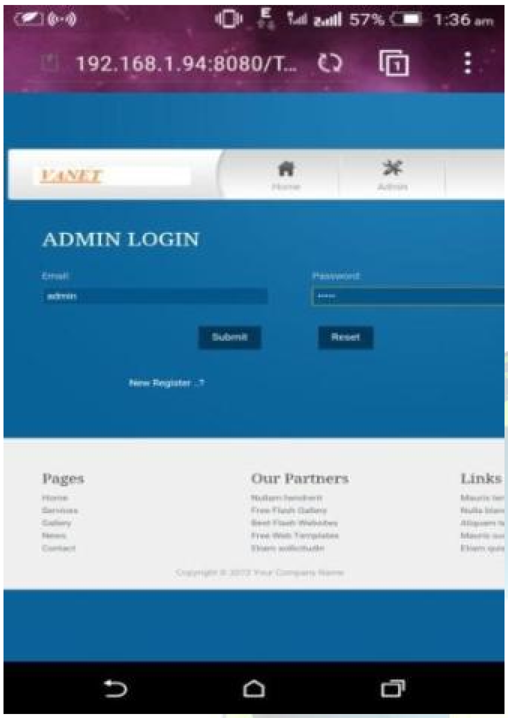


ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 13, March 2017

MOBILE APPLICATION

Then the application will ask for either admin login or user login. As shown in figure 4(b) if we select admin login then we have to provide email address and password of our main server from where we are providing the database.



Figure(1)

The android application is developed to support best path planning strategy. Application will now ask for start and end address i.e. source and destination of user. For e.g. kkw and nashik road is start and end address respectively as shown in figure (2) .

Figure(2)

Then after submitting the request application will provide all the paths from particular source to destination with their respective traffic count as shown in figure (3).

Figure(3)

When the user will ask for best path with minimum traffic, application will provide required path along with googlemap as shown in figure(4).

Figure(4)

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 13, March 2017

CONCLUSION

In this work we have introduced a new strategy to be used when placing road-side-units on roads. We also proposed two new beacons formats to be generated by RSUs and OBs during communication. We then built two detection systems in which one is used strictly by OBUs and the other by RSUs. The two detection systems – when applied together- gave promising results to accurately detect jammers with very low failure detection rate. Several cases reported when the detection systems failed to give correct results. These cases were mostly when jammers first launch the attack or right before going into sleeping mode. Despite these cases, OBU-DS and RSU-DS have proven their feasibility and showed promising results to
warn drivers when jammers exist especially when combined together.

This paper gives an overview of past few techniques in the field of vehicular ad hoc networks and presents a real–time intelligent transportation system. Proposed system is based on RFID and ARM controller to minimize traffic congestion with proper signal control. And the android mobile application will help users to find a path with minimum traffic to their destination. This can greatly reduce the problems of road

VI FUTURE SCOPE

Our future work will be focusing in utilizing the proposed detection system to build a new protocol that enables nodes to communicate in the presence of jammers. Many people have proposed solutions to the jamming problem.

System can be made more effective and can be implemented at traffic signal in real life. The RFID reader can be replaced with digital cameras at roadside to increase the efficiency of system. By increasing the range and capability of the components used, the system can become deployable. It can possess more parameters for increasing the applications of system. Changes can be made as per the users requirement and ideas to make it more useful and beneficial for them. All the traffic logs and data can be maintained on cloud which can be helpful to analyze city traffic and beneficial to take various traffic control decisions. Cloud computing and storage solutions provide users and enterprises with various capabilities to store and process their data in third-party datacenters.

VII REFERENCES

[1] Miao Wang, Hangguan Shan, *Member, IEEE*, Rongxing Lu, *Member, IEEE*, Ran Zhang, Xuemin (Sherman) Shen, *Fellow, IEEE*, and Fan Bai, "Real-Time Path Planning Based on Hybrid-VANET-Enhanced Transportation System", IEEE Transactions on vehicular technology, Vol. 64, No. 5, May 2015.

[2] M. Papageorgiou, C. Diakaki, V. Dinopoulou, A. Kotsialos, and Y. Wang, "Review of road traffic control strategies," *Proc. IEEE*, vol. 91, no. 12, pp. 2043–2067, Dec. 2003.

[3] Texas Transp. Inst. (2007). Texas Transportation Institute: Urban mobility information annual urban mobility report, College Station, TX, USA. [Online]. Available: http://mobility.tamu.edu/ums.

[4] H. Hartenstein and K. Laberteaux, *VANET: Vehicular Applications and Inter-Networking Technologies*. Hoboken, NJ, USA: Wiley, 2010. [Online]. Available: http://www.nhtsa.gov/

[5] T. Hunter, R. Herring, P. Abbeel, and A. Bayen, "Path and travel time inference from GPS probe vehicle data," in *Proc. Neural Inf. Process. Syst. Found.*, Vancouver, BC, Canada, Dec. 2009, pp. 1–8.

[6] Christo Ananth, M.Muthamil Jothi, A.Nancy, V.Manjula, R.Muthu Veni, S.Kavya, "Efficient message forwarding in MANETs", International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE), Volume 1,Issue 1, August 2015,pp:6-9

[7] R. Lu, X. Lin, and X. Shen, "SPRING: A social-based privacy- preserving packet forwarding protocol for vehicular delay tolerant networks," in *Proc. IEEE INFOCOM*, San Diego, CA, USA, Mar. 2010, pp. 1–9.