iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 3 **Issue:** VI **Month of publication:** June 2015

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)

A Survey of VANET Based Secure Message Communication in Cluster Formation by DSRC Protocol

Ravinder S[1], Preethi J[2], Nithiyananthan U[3]
[1]P.G. Student, Department of CSE, Anna University Regional Center, Coimbatore, Tamil Nadu, India
[2]Head Of The Department, Department of CSE, Anna University Regional Center, Coimbatore, Tamil Nadu, India
[3]P.G. Student, Department of CSE, Anna University Regional Center, Coimbatore, Tamil Nadu, India

Abstract: Vehicular Ad Hoc Networks (VANET) is kind of a special wireless ad hoc network, which has the characteristics of huge node mobility and fast topology changes. The Vehicle ad Hoc Networks may provide a large variety of services and range from safety-related warning systems to improved navigation schemes as well as information and entertainment applications. During the creation of VANET clusters, each vehicle chooses a cluster head vehicle to move. The average number of cluster head changes per vehicle measures the cluster stability in these simulations. This paper analyse how the vehicles are communicate with the other vehicles between the clusters.
Keywords - VANET, cluster, ITS, DSRC,OBU,TPD

I. INTRODUCTION

Tremendous investment from government, academia and industry under the big umbrella of intelligent transport systems (ITS), leading to the development of safety and traffic management technologies in vehicles and road infrastructure. Wireless vehicular communications and networking is a key enabling technology for future ITS services. The International Organization for Standardization (ISO) TC204 WG16 is developing a family of international standards and architecture on communications access for land mobiles (CALM). In 1999, the Federal Communication Commission (FCC) allocated a frequency spectrum for vehicle-vehicle and vehicle road-side wireless communication. Vehicular Ad-hoc Networks (VANETs) are receiving increasing attention in industry and academia, as they are considered by many to be the most challenging implementation of Mobile Ad-Hoc Networks (MANETs). The Commission then established Dedicated Short Range Communications (DSRC) Service in 2003. Recently, the promises of wireless communications to support vehicular applications have led to several research projects around world. In US, FCC allocated DSRC spectrum to "increase traveler safety, reduce fuel consumption and pollution, and continue to advance the nation's economy". The DSRC is licensed at 5.9 GHz with a 75-MHz spectrum, which is divided into seven 10-MHz channels and a 5-MHz guard band. The control channel (CCH) will be used for safety applications, whereas the other six channels, called service channels(SCHs),will be used for infotainment or commercial applications to make this technology more cost effective. The recently proposed WAVE standards on the dedicated short range communications (DSRC) frequency band. DSRC/WAVE is the only wireless technology that can potentially meet the extremely short latency requirement for road safety messaging and control. The unique feature of low latency secures the role of DSRC, as an essential communication technology.

The communication environment of DSRC is both vehicle-to-vehicle and vehicle-to/from-roadside. The VANET aims to provide a high data rate and at the same time minimize latency within a relatively small communication zone. Its primary purpose is to support critical safety applications which will reduce the number of accidents on the road and as a result will reduce the number of lives lost and its secondary purpose is to improve traffic flow although aside from these two, private services will also be permitted. The remaining section contains following:

II. VANET work performance and Attacks, III. Cluster Formation in VANET, IV. Simulation Results and
V. Conclusion and Future Work and References.

II. VANET WORK PERFORMANCE

A VANET is a form of Vehicular Mobile ad-hoc Networks to provide communication among nearby vehicles and between vehicles and nearby fixed equipment i.e. roadside equipment. Roads are saturated, safety distance

and reasonable speeds are hardly respected. VANETs allow vehicles to avoid problems, either by taking any desired action or by alerting the driver. Besides the road safety enhancements that VANETs will bring, they also open doors too many applications to enhance the driving and travelling comfort, like Internet access from a car. Each vehicle has OBU (on board unit), this unit connects the vehicle with RSU via DSRC radios, and another device is TPD (Tamper Proof Device), this device holding the vehicle secrets and placed in the vehicle.

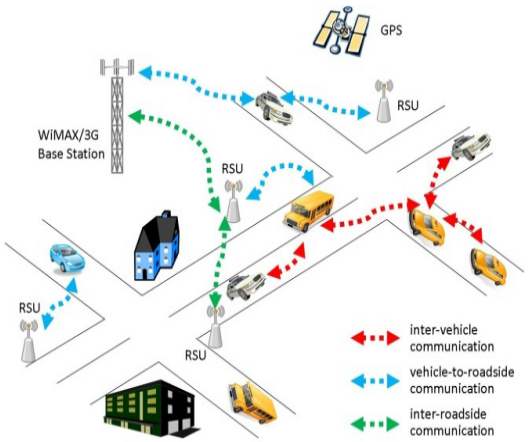


Fig. 1 VANET Architecture

VANET or Intelligent Vehicular Ad-Hoc Networking provides an intelligent way of using vehicular Networking. The main goal of VANET is providing safety and comfort for passengers helping drivers on the roads by anticipating hazardous. Each vehicle equipped with VANET device will be a node in the Ad-hoc network and can receive & relay other messages through the wireless network. Collision warning, Road signal arms and in place traffic view will give the driver essential tool to decide the best path along the way events or bad traffic areas. VANET has unique characteristics like high mobility with the constraint of road topology, initially low market penetration ratio, unbounded network size, infrastructure support that Differentiate it from MANET.

A. Attacks in VANET

VANET facing many attacks,

1) *Denial of Service attack*: This attack happens when the attacker takes control of a vehicle's resources or jams the communication channel used by the Vehicular Network, so it prevents critical information from arriving. It also increases the danger to the driver.
2) *Message Suppression Attack*: An attacker selectively dropping packets from the network, these packets may hold critical information for the receiver, the attacker suppress these packets and can use them again in other time.
3) *Fabrication Attack*: An attacker can make this attack by transmitting false information into the network, the information could be false or the transmitter could claim that it is somebody else.
4) *Alteration Attack:* This attack happens when attacker alters an existing data. It includes delaying the transmission of the information, replaying earlier transmission, or altering the actual entry of the data transmitted For instance, an attacker can alter a message telling other vehicles that the current road is clear while the road is congested.
5) *Replay Attack:* This attack happens when an attacker replay the transmission of an earlier information to take advantage of the situation of the message at time of sending Basic 802.11 security has no protection against replay. It does not contain sequence numbers or timestamps.

6) *Sybil Attack*: This attack happens when an attacker creates a large number of pseudonymous, and claims or acts like it is more than a hundred vehicles, to tell other vehicles that there is jam ahead, and force them to take alternate route.

III. CLUSTER FORMATION IN VANET

Cluster based Routing Formation combines the features of static and dynamic clustering together. Static clusters are formed around the static sources located at the road signals, street corners and congested places known as static cluster head. However buses are chosen as dynamic sources in our algorithm, having the predefined path and time chart to handle the high mobility situations known as dynamic cluster head. Hierarchical clustering creates a layering environment that poses some of the main challenges in such ad hoc networks. Top layer consists of static cluster head, middle layer consists of dynamic cluster head and lower layer consists of ordinary vehicles. Because of highly dynamic vehicles network topology also changes. This in turn affects the performance of the network and also invokes protocol mechanisms to react to such dynamics. Mobility awareness deals with sudden changes in topology by responding against malfunctions in routing. Some of mobility metrics are considered for cluster construction in order to form a stable cluster structure thereby decreasing its influence on cluster topology. Vehicles are grouped in two different ways either by those vehicles which are in the communication ranges of dynamic sources or by those vehicles which are in the ranges of static sources mounted at traffic signals and road junctions. By doing so, the re-affiliation and re-clustering rate can be naturally decreased.

A. Cluster creation algorithm

```
[Xi, Yi] = Get _Pos ( n);
Track the positions of nodes in cluster areas
[Ai,Bi]=Subset(Xi,Yi);
for(k=0;k<count(Ai);k++)

{
Find Movement Speed(N[k])
}
if(average movement of all node speed is slow)
{
Take the cluster size as smaller
}
else
Take the cluster as some larger
end if
function Get_Pos(int n)
for(i=0;i<n;i++)
{
Xi,Yi=FindGps_xy(i)
}
return X,Y
```

B. Number of Cluster nodes in a cluster

```
Note the border of the cluster
Procedure : Compute Node Count()
XiYi = fin Pos (n);
For(i=0;i<count(Xi);i++)
{
If ((Xi,Yi) within the cluster border)
{
```

Select that as cluster Node
}}

If this algorithm finds any roadside unit, it immediately elects that one as the cluster head, because normally the roadside units have greater processing power. Moreover they are fixed and unmoving. Hence it is not necessary to change the cluster head. Thus it provides a more reliable service than other mobile nodes. each nodes and chooses a particular node as the cluster head whose distance is very small due to low node velocity. It elects slow speed vehicle as cluster head because this node ensures that it will remain in its own cluster coverage area for a maximum period of time than the high speed vehicles.

IV. SIMULATION RESULTS

The simulation is performed using Network Simulator 2 (ns 2).Number of nodes are represented in NS2 and the data can be send within the range. The following simulations are explained for assumptions. Fig 2 represents nodes placed orderly and moving one by one, initial node represent as cluster head.

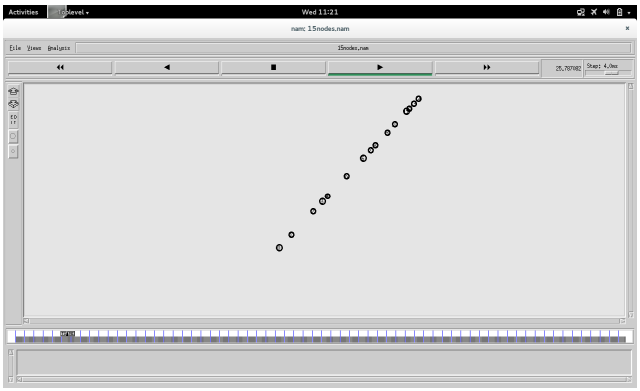
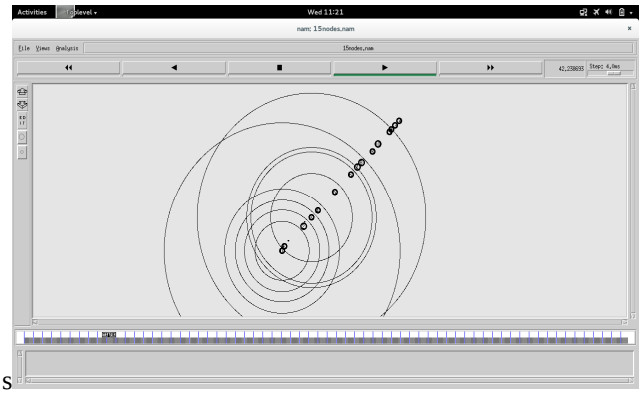


Fig 2. Node Placement

Fig 3 represents packet send between the node within the region and Fig 4 represents nodes are grouped and packet send into the nodes, any malicious node in the region packet not sent into that node.



S

Fig 3. Packets send within the ranges

Vehicles can form a group to communicate timely with each other. A group of VANET nodes within a radio range can form a cluster area. Cluster concept has successfully applied in MANET for a better delivery ratio and to reduce broadcast storms. In a Cluster environment, the Cluster Head gathers data from any node of that cluster and sends them to another cluster head. Cluster head can be select as dynamically in each group of cluster formation.

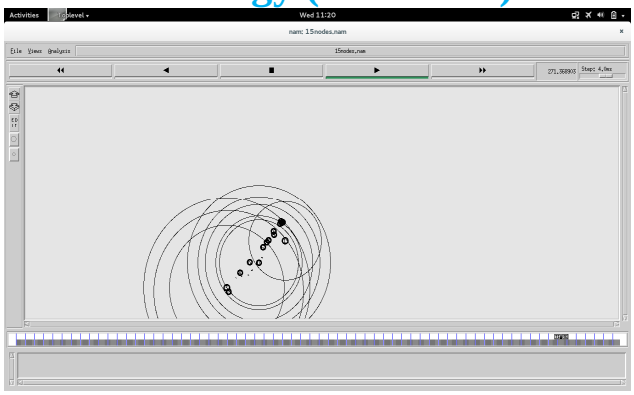


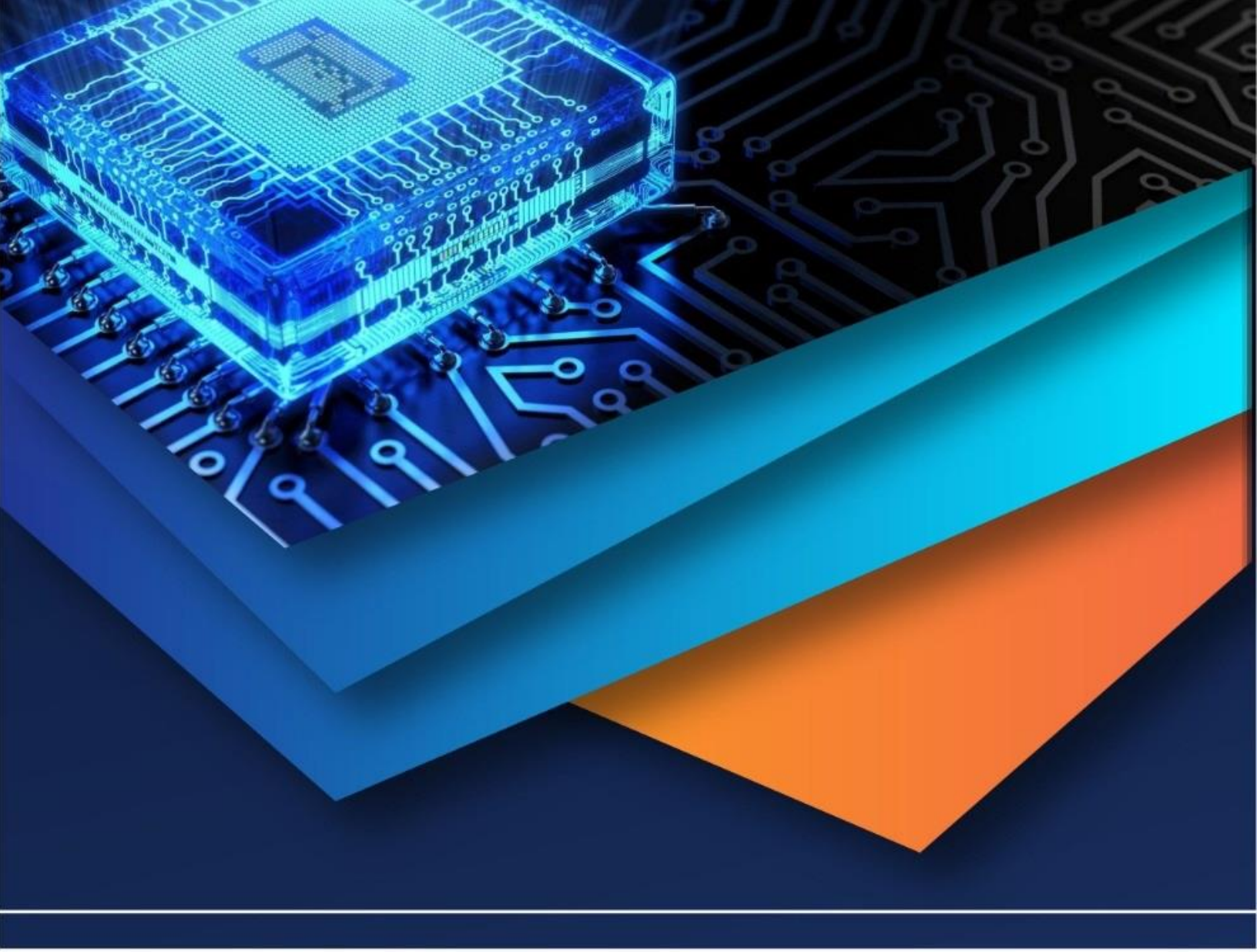
Fig 4. Nodes grouped within a range

V. CONCLUSION AND FUTURE WORK

Safety is the important concern to many road users. VANET application has the opportunity to provide such a safety requirements. However, life critical messages must be transmitted from node to node in the VANET network in reliable and timely manner. To achieve this, secure communication and network availability must be obtained in the VANET set up. This paper discusses a new cluster based model with central authority to ensure authentication. It also focuses the different types of attacks that may be applicable to VANET.In the Future Modification Process, convert Android based Mobile Application instead of system based implementation.

REFERENCES

[1] T.W. Chim, S.M. Yiu, Lucas C.K. Hui," VSPN: VANET-Based Secure and Privacy-Preserving Navigation" IEETRANSACTIONS ON COMPUTERS, VOL. 63, NO. 2, FEBRUARY 2014.
[2] Mrunmayi S Sahasrabudhe et al." Survey of Applications based on Vehicular Ad-Hoc Network (VANET) Framework" Vol. 5 (3) , 2014.
[3] Ghassan Samara, Wafaa A.H.Al-Salihy, R.Suresh," Security Issues and Challenges of Vehicular Ad Hoc Networks (VANET)"
[4] B.Ramakrishnan,Dr.R.S.Rajesh,R.S.Shaji, "CBVANET: A Cluster Based Vehicular Adhoc Network Model for Simple Highway Communication" Volume: 02,2011.
[5] Long Chen,1 Xuedan Jia (2013),'Expedite Privacy-Preserving Emergency Communication Scheme for VANETs', Volume 2013, Article ID 693930.
[6] R.Lakshmi Devi, C. Maheswari (2012),' A Cluster Based Authentic Vehicular Environment for Simple Highway Communication' IPCSIT vol. 37
[7] Yunxin (Jeff) Li 'An Overview of the DSRC/WAVE Technology'
[8] Hervé Boeglen, Benoît Hilt (2011) 'A survey of V2V channel modeling for VANET simulations'
[9] Monika Khatri, Sona Malhotra," AN INSIGHT OVERVIEW OF ISSUES AND CHALLENGES IN VEHICULAR ADHOC NETWORK", Volume 2, No. 12, December 2011.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY