Efficient communication approach in Vehicular PKI

Ms. Nayana P Vaity[#1], Ms.Surekha Janrao[#2] ,Ms.Randeep Kaur
Asst Professor & Department of Computer Engineering[#1,] Asst Professor & Department of Computer Engineering[#2] , Asst Professor & Department of Computer Engineering[#2] ,Terna Engineering college,Nerul Navi Mumbai,INDIA

***Abstract*- In recent era, we know transport industry tend to incorporates many facilities to the vehicle users which not only helps people to have *safe journey* but also *smooth in nature*. *Intelligent transportation system* (ITS) is the need for today's luxurious life. In this paper, it is proposed that communication among vehicles is performed using efficient routing where as secure environment is established using PKI(public key environment). It can be said that proposed Routing approach have better capabilities than other existing routing protocols it means communication where emergency messages will be disseminated *efficiently* and *as early as possible.* When VANET is to be protected from malicious access or to avoid the problem of vehicle tracking, one of the security features is called as location privacy is not mainly offered by typical PKI. Here efficient routing approach will be blended with security feature such as vehicles 's location privacy feature. which is definitely will be used to enhance typical PKI security.**

Keywords- *ITS, Typical PKI .*

I.INTRODUCTION

Vehicular Network is new kind of network in which moving vehicles forms ad hoc type network for communication. This technology is as called VANET. Vehicles move on road with different speed, acceleration Vehicular ad hoc networks are expected to implement wireless technologies such as dedicated short-range communications (DSRC) which is a type of Wi-Fi [1]. Vehicular traffic consists of vehicles and road topology. Road is path connected by two or more nodes could be created by traffic generator[1,2]. Vehicles are having movement on this path can have dynamic (in flow) changes when roads are of different types. Performance evaluation[2] of distance vector protocols by considering road topology may give more accurate result. By Practical perspective routing protocols such as distance vectors and link state type which are already available in simulator and also used over decade to establish routing in vehicular network .

More over road topology[1,2,3] can be created manually and vehicles are added using mobility generator or directly taken from online service viz. www.openstreetmap.com. Both routing protocols and road topology affects VANET communication. Routing may also be affected by number of nodes/vehicles. Apart from this, here routing strategy[4,5] for opposite direction vehicles communication was invented for delivery of emergency messages when accident occurs . This opposite direction communication strategy is efficient as well as fast in nature. As we know ,In most of routing process flooding is used as fundamental step to forward messages to the destination node but it may give rise broadcast storm problem[4] due to redundant messages .When VANET is to be protected from malicious access or to avoid the problem of vehicle tracking, one of the security feature is called as location privacy is not mainly offered by typical PKI. There is always need of comparing and analyzing of new routing approaches with existing Protocols in order to obtain better routing strategy. In other words , This approach can be *blended with security features* such as *vehicles 's privacy*. Furthermore this approach can be tested against popular AODV Protocol.

In this work, section II discusses typical AODV and routing approach where as section III discusses about typical PKI and location privacy feature in which routing approach will work. In Section IV Cryptographic mechanism for AODV is discussed stepwise. Further Section V viz. Simulation environment explains workflow and performance metrics used for measuring performance whereas section VI includes implementation of scenarios with programming tools and graphs analysis. Section VI contains conclusion with comparative analysis of proposed routing approach and typical AODV in secure environment.

II. AODV AND ROUTING APPROACH

A. AODV[6]

The Ad Hoc On-Demand Distance Vector Routing Protocol is a reactive routing protocol based on DSDV. It was introduced in 1997. AODV is popular routing protocol used in adhoc networks wired or wireless networks. One feature of AODV is the use of a destination sequence number for each routing table entry. The sequence number is generated by the destination node. The sequence number included in a route request or route reply is sent to requesting nodes. Sequence number are very important because they ensures loop freedom and is simple to program. Sequence numbers are used by other nodes to determine the freshness of routing information

B. Routing Approach

Communication of vehicles on road can be in single direction[5,7] (all vehicles move in same direction) or Opposite-direction which usually happen on highway or Expressway. This routing approach [5,8] is helps when emergency such as accident occurrence should be informed as fast as possible in order to avoid traffic congestion. Following sections will describe this approach in brief.

Main objective of this approach to forward packets fast without increasing congestion or duplicate packets in network. Most often Hop by hop transmission is used to

forward the packets but in this multi hop is used with predefined counter. In this communication , only opposite direction vehicles are used to relay packets[4,5,8] which shows much better performance in terms of connectivity and network efficiency compared to same direction same direction and both-direction communication[2,4,7]. Thus, in this work, the sender as the static node (refer fig 3), is set to transmit packets to nodes coming from the opposite direction.GPS[5,8] receivers could provide accurate vehicle positions. Each packet has counter which calculates the number of relay node the packet has been sent to.

As a packet reaches to the relay node(the vehicle which travel in opposite direction), the relay node will check the counter of its own. If the counter is less than n - 1, it will relay the packet to a relay node at the back. As the counter reaches n = n - 1 which is 4,(see fig 3) the particular relay node will transmit the packet to vehicles on the opposite direction. This routing protocol approach combines distance and time based technique

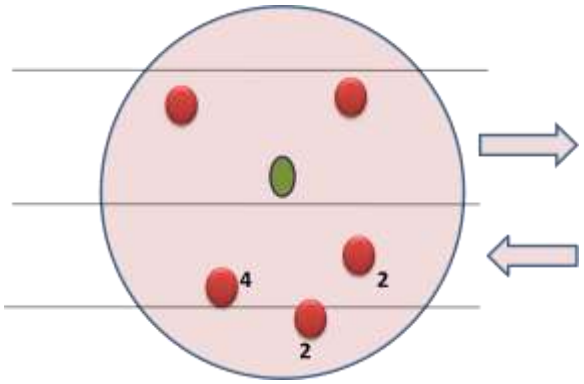

Fig 1: Time based technique

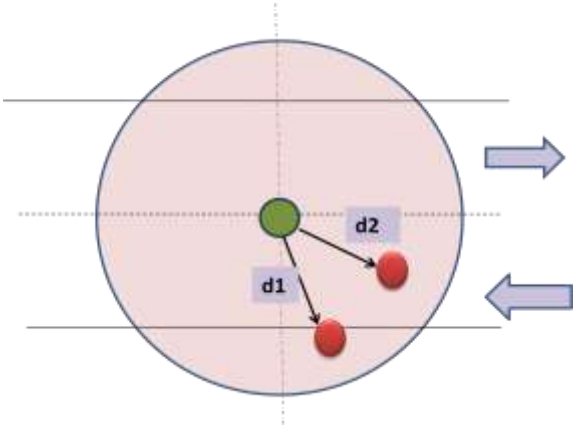

Fig 2: Distance based technique

In more density network, nodes share a limited wireless medium which causes problems such as choking of the shared medium with an excessive number of the same broadcast message by several consecutive cars. Packets that are broadcasted blindly may result in broadcast storm problem[4]. Combination of location based method and time based method(see fig 1 and 2) leads to less utilization bandwidth which is limited, the excessive number of packet transmissions only results in packet collisions[4,5,7] and message drops in the network.

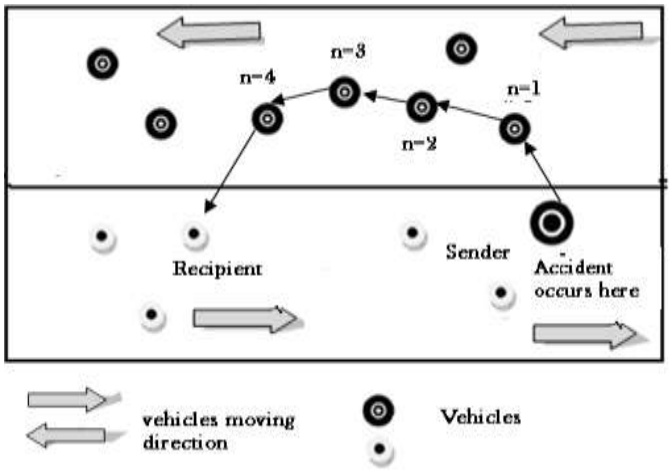

Fig3: Opposite direction communication routing approach.

III PKI WITH LOCATION PRIVACY FEATURE

A. *TYPICAL PKI*

PKI [9]is nothing but public key infrastructure in which there is different types of entities such as TA ,RSU,RA, Vehicles etc. This infrastructure enables vehicular network to have more secure data dissemination. TA is main entity to issue certificates to each vehicle whereas Regional Authority where take care of CRL(Relocated certificates list). Apart from that every vehicle can use certificates to check authenticated and authorized communication with other vehicles . Each vehicle has OBU(on board unit) and Typical PKI is depicted as follows

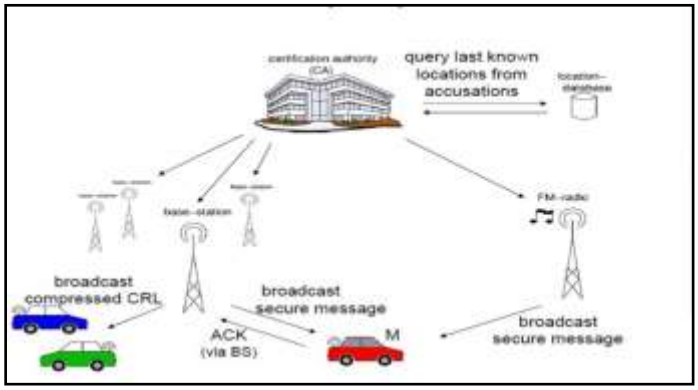

Fig 4: Vehicular PKI (Public key infrastructure)

B. *Vehicle tracking*

Although anonymous certificates[9,10] in PKI can guarantee *identity privacy*, they cannot support *location*

privacy. If a vehicle changes its certificate between two observation points controlled by an attacker while moving in the same lane and with the same speed on the road, an attacker can correlate the certificates used by that vehicle and hence track the vehicle position.

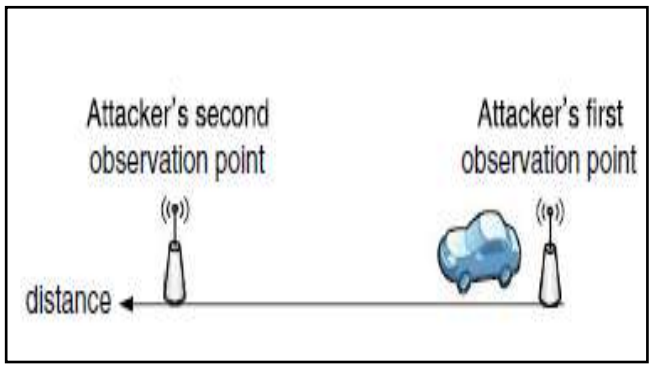

Fig 5 : Vehicle tracking

C. Cryptographic mechanism

To create encryption zone[9,10] following steps can be used

- OBU'S before changing certificate, sends msg to neighbors
  - msg ={ request REP || PID || TREP }
- Other OBU'S start encrypting their messages with kg (Initial group key)
- Other OBU's which are using group key forms group called as CMIX zone.
- OBU change its certificate and Monitors other OBU's (If(OBUs certificate validity time less than <=TREP)
  - =Force to change its certificate.
- TREP (time out) = stop encryption

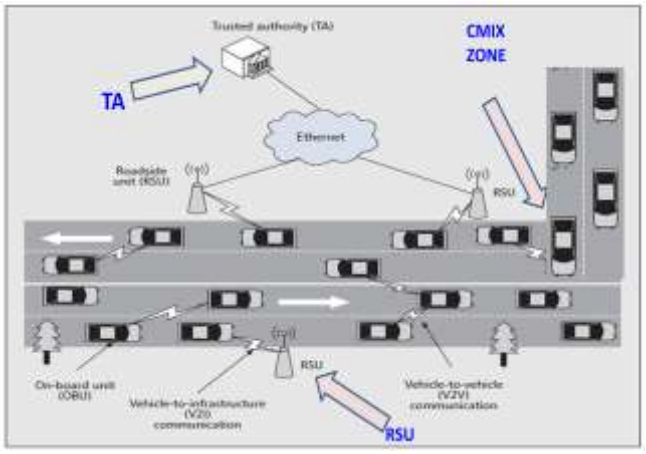

Fig 6 :CMIX ZONE Example

IV.CRYPTOGRAPHY FOR AODV

A. Route Request

In AODV Route is found by source node by broadcasting route request packets[11,12]. While sending Route request packet Creation of group session key is performed and it uses Sharing session key with immediate nodes. Encrypting route request packet with such session key. Broadcasting this encrypted packet with neighbors until packet reached to the destination

B. Route reply

While sending Route reply, Route reply packets are again encrypted with backward session keys that are used by nodes to communicate with those immediate / neighbor nodes while sending route request packet**.** Route Reply[11,12] packet can be then decrypted using Same Group session key

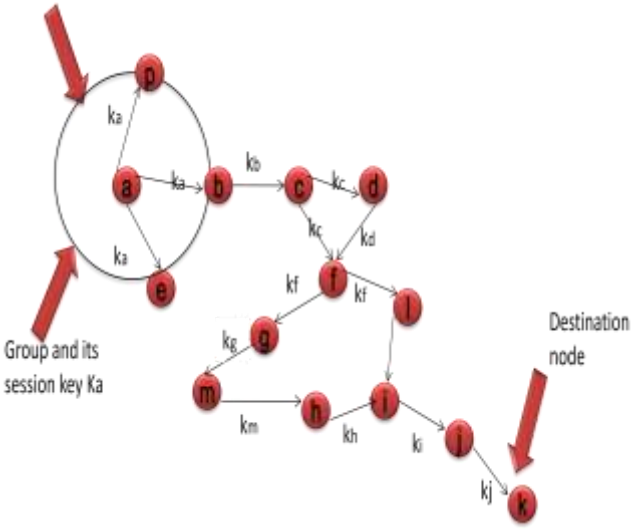

Fig 7: Secure AODV Example

V. SIMULATION ENVIRONMENT

To simulate network environment, It is required network simulator NS2.34 in which tcl code runs and also result can be observed by analyzing trace files after each scenario executed[13,14]. Here are steps for implementation

A. Steps to generate scenario in NS2.34

By using mobility generator [1,13,14] specifying position discrete time or by utilizing real time maps an vehicles movement.

- View the movement of vehicles using traffic simulator.
- Configuration file which run in traffic simulator converted in tcl language code.
- Tcl code can be executed in NS 2.34 and .tr file (trace file) will be generated.
- Using Network animator(NAM),scenario can be view

B. Performance metrics

Trace file(generated after execution) will be interpreted using awk script and giving command Awk -f file1.awk file.tr and following metrics can be used to calculate performance of the scenario.

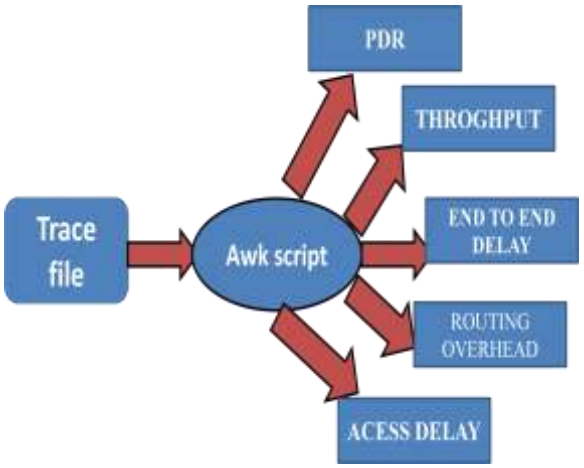

Fig 8: Different performance metrics

C. Workflow

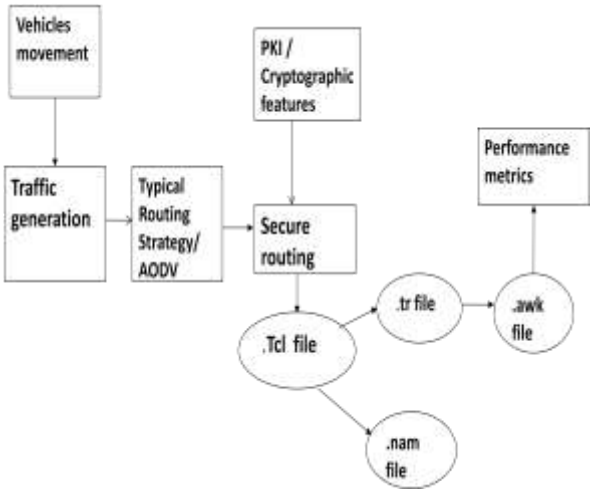

Fig 9 : Workflow for implementation

To evaluate efficiency of routing approach or AODV using NS 2.34 we have system flow(see fig 9) from which it can be said that routing approach or AODV has security element(which we add to make environment secure). After Adding security in routing approach and AODV further output is used to calculate performance metrics for each of them. Two files .tr and .nam (having extention) are used for such purpose of evaluation.

VI. IMPLEMENTATION

A. Minimum Requirement

Hardware/software requirement is as follows

- Pentium IV Processor
- 512MB RAM
- 2 GB HDD
- Red hat Linux
- NS2.34

Following are screenshots of secure routing approach and secure AODV . from figure we can observe TA,RSU and normal nodes as well as malicious nodes.

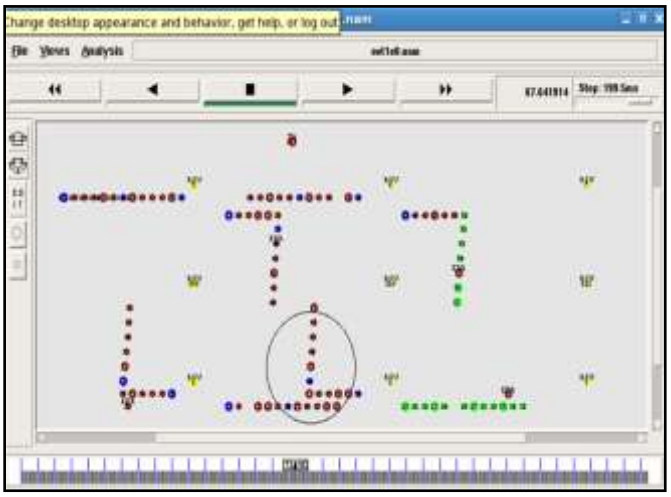

Fig 10 :Screen shot of secure routing strategy in NS2.34

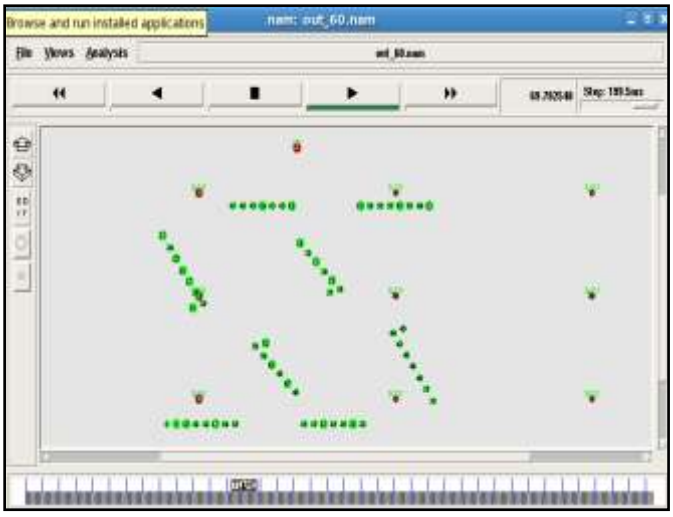

Fig 11: Screenshot of secure AODV in NS 2.34

B. Result Analysis

On running of scenario in Network simulator , following results have been achieved.

DELAY	30	60	100
SEC-STRATEGY	0.017	0.017	0.016
SEC-AODV	0.218	0.606	6.44

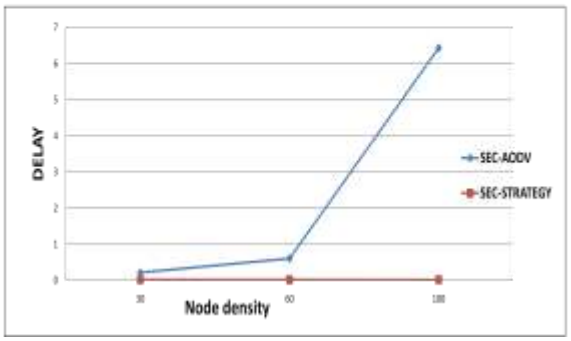

Fig 12: End to End Delay

THROUGHPUT	30	60	100
SEC-STRATEGY	36894	363294	1697444
SEC-AODV	7680	99520	368320

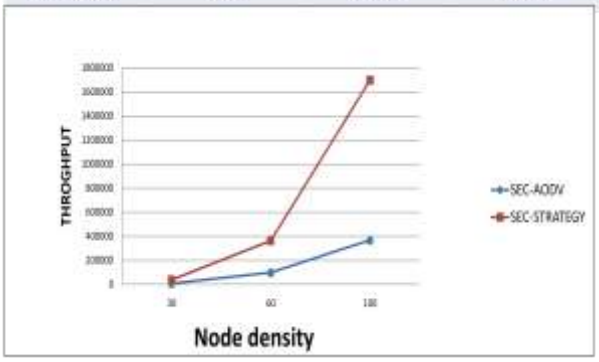

Fig 13: Throughput

PDR	30	60	100
SEC-STRATEGY	12.63	12.44	29.08
SEC-AODV	2.7	35.1	130.3

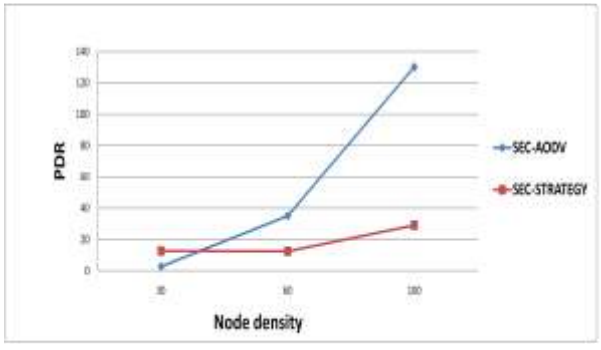

Fig 14:Packet Delivery Ratio(PDR)

Node density	30	60	100
SEC-STRATEGY	4.48	8.2	2.85
SEC-AODV	5.7	6.4	3.4

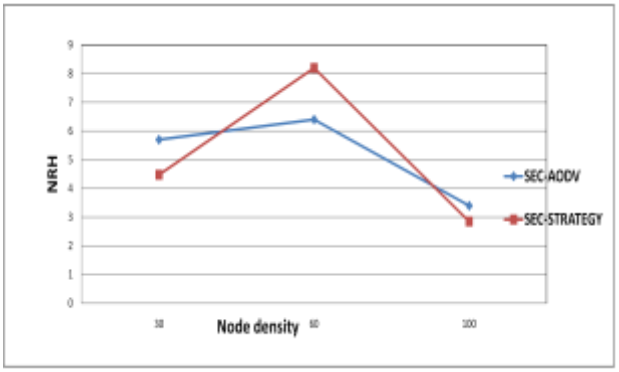

Fig 15: Normalized Control overhead

ACCESS_DELAY	30	60	100
SEC-STRATEGY	0.8267	0.3579	0.3666
SEC-AODV	0.6671	1.00878	1.46798

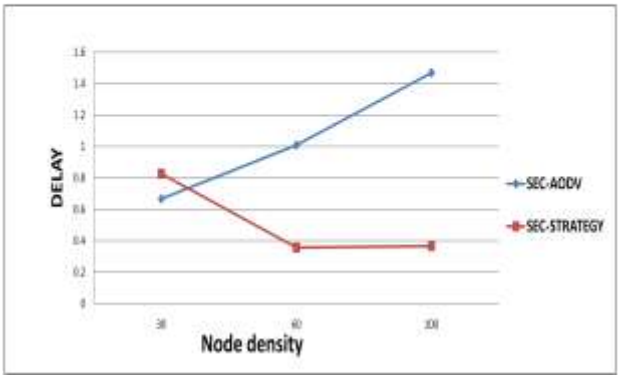

Fig 16: Access delay

VII. CONCLUSIONS

Initially we made run routing approach in secure PKI(has security features such as TA,CMIX Zone etc) and then added security element in AODV Protocol. This is done because we need to compare AODV with routing approach and decide better one for secure environment as well as accident scenarios.

The evaluation work of routing approach is essentially done by calculating Performance metrics for various node densities. We observe that for our secure routing approach metric end to end delay is almost low when run for all node densities. Where as in secure AODV delay increases as node density increases. Routing overhead for both approaches increase till node density is 60 but as node density increases further, routing overhead decreases.

Throughput is comparatively higher for secure strategy but when node density is increases to 100 secure approach shows high throughput. PDR increases for both approaches as node density increases but for secure AODV it increases to the highest. Access delay is more for secure AODV where as it is low for routing approach of all node densities. Our secure routing approach is better when minimum delay is to be incurred. Efficiency of routing approach is compared with secure AODV and result we have achieved is routing approach is much more efficient even though accident scenario occurs. Also Adding security features in routing approach makes it powerful mechanism rather than adding security in existing Protocol.

ACKNOWLEGEMENT

It is great opportunity for us to write this research paper. At the time of preparing this paper, we have gone through different books and websites(including references) which helped us to get acquainted with papers topics. We are focusing on those topics which are important for us to understand this VANET security subject more easily and precisely.

We acknowledge with gratitude to Professor Lata Ragha who is always been helpful and inspiring for our work and research in this field.

Apart from us, this paper will certainly be immense importance for those who are interested to know about this subject. We hope they will find it comprehensible.

REFERENCES

[1]Hannes hartenssen , Kenneth laborteux "VANET Vehicular Applications and internetworking technologies" Book by A John Wiley and Sons Ltd, Publication. Pp1-112.

[2] Zijie Zhangy, Guoqiang Maoyx and Brian D.O. Anderson "On the Information Propagation Process in Multi-lane Vehicular Ad Hoc Networks", National ICT Australia (NICTA), Australia.

[3]Mushtak Y. Gadkari AND Nitin B. Sambr, "VANET: Routing Protocols, Security Issues and Simulation Tools" OSR Journal of Computer Engineering (IOSRJCE) ISSN: 2278-0661 Volume 3, Issue 3 (July-Aug. 2012), PP 28-38.

[4] Y. Tseng, S. Ni, Y. Chen, J. Sheu "The broadcast storm problem" a Wireless Networks 8, 153–167, 2002, Kluwer Academic Publishers. Manufactured in The Netherlands

[5] Nur Diana Mohd. Nuri, Halabi Hasbullah "Strategy for Efficient Routing in VANET", Computer and Information Sciences Department University Teknology PETRONAS Tronoh Perak, Malaysia. 978-1-4244-6716-711-0 ©20 10 IEEE

[6]Perkins, C.; Belding-Royer, E.; Das, S. "Ad hoc On-Demand Distance Vector (AODV) Routing protocol" jointly developed at Nokia Research Center, University of California, Santa Barbara and University of Cincinnati in year July 2003

[7]Fozolo A. and Zanella A "An Effective Broadcast Scheme for Alert Message Propagation in Vehicular Ad hoc Networks" University of Padova ,A Department of Information Engineering, Via Gradenigo 6/B, 35131 Padova, Italy,IEEE, E-ISBN :1-4244-0355-3.0.2006.

[8]Amit R. Welekar and Dr. S.S. Dorle "Efficient use of Bidirectional Communication to Increase Communication Capabilities in Distributed VANET" in Int.J.Computer Technology & Applications,Vol 3 (3), 1034-1039 , ISSN:2229-6093 .

[9] Albert Wasef And Rongxing Lu "Complementing public key infrastructure to Secure vehicular ad hoc networks" University Of Waterloo,1536-1284/10/2010-IEEE, Wireless Communications , October 2010.

[10]Albert Wasef and Xuemin (Sherman) Shen "REP: Location Privacy for VANETs Using Random Encryption Periods" Published online: 27 May 2010 © Springer Science and Business Media, LLC 2009.

[11]Asad Amir Pirzada and Chris McDonald, "Secure Routing with the AODV Protocol ", Asia-Pacific Conference on Communications, Perth, Western Australia, October 2005.

[12] Akshai Aggarwal1, Dr. Savita Gandhi "A Novel Approach To Secure Ad Hoc On-Demand Distance Vector (AODV) Routing Protocol From Insider Attacks In Manets"in International Journal of Computer Networks & Communications (IJCNC) Vol.4, No.4, July 2012.

[13] Prof Bilal Mustafa, Umar Waqas Raja, "Issues of Routing in VANET", Computer science thesis ,no MCS-2010-20, School of Computing, Blekinge Institute of Technology Box 520 SE – 372 25 Ronneby, Sweden.

[14] Jaya Jacob, V.Seethalakshmi, "Performance Analysis and Enhancement of Routing Protocol in Manet", International Journal of Modern Engineering Research (IJMER) www.ijmer.com Vol.2, Issue.2, Mar-Apr 2012 pp-323-328 ISSN: 2249-6644.