Seamless and Secured wide Fidelity enhancement in moving vehicles Using Eeack Technique

M Lavanya #,M Selvaraj^.
#Student, ME-Communication Systems, Valliammai Engineering College, Chennai. India
lavan21192@gmail.com
^Assistant Professor, Deptof ECE,Valliammai Engineering College, Chennai. India
selvaraj2k7@gmail.com

Abstract—*Packet transmission is the main important task in present days, because in wireless networks every time topology construction was changed dynamically then transmission is mostly important task in those situations. This process will be done unnecessary users or nodes enter into wireless networks based on their geo information and then they are accessing services of the other nodes. Traditionally propose simple yet effective scheme, which can identify misbehaving forwarders that drop or modify packets. Extensive analysis and simulations have been conducted to verify the effectiveness and efficiency of the scheme. This schema effectively detect dropped packets from misbehaving users but dynamic changes of the topology in wireless networks less communication process can be done wireless networks. In this paper we propose to develop Enhanced Adaptive Acknowledgement specially designed for wireless networks. EEACK demonstrates higher malicious- behavior-detection rates in certain circumstances while does not greatly affect the network performances*

Index Terms—*EAACK Detection, Internet Access, MANET, WiFi.*

I. Introduction

MANET is sensitive to malicious or dangerous attacks because of its open medium wide distribution of nodes. MANET is divided into two different types single hop network and multi-hope Network in single hope network all nodes are in a same radio range that directly communicate with one another. In multi hop network if the desired node is far away from its radio range area then nodes relay on other neighboring or intermediate nodes to transmit their data. At the time of transferring data some of the routing protocols in MANET assume that nodes in network will corporate to each other while forwarding data packets to another nodes. But in intermediate or neighboring nodes may occur several critical problems such as it can extract useful information packets, cannot forward packets or may modify the contents of packets during the data transmission session. These type of nodes are known as misbehavior nodes or misbehaving nodes.

MANET was used for mainly for Military application but in now a days mostly new usage like search and rescue mission , information collection, virtual classes and conference where computer, laptop, Personal Digital Assistant(PDA),some mobile devices which are wireless communication .MANET is unprotected based on the basic characteristics, like changing topology, open channel, absence of structure , compact power supply and measurability. Because of some open channel and some remote distribution area of MANET make it unprotected to different types of attacks. Using cryptography which are protected by provide authentication to all routing control packets, because of the outsider attacker does not participate
in this route discovery process. In that MANET nodes are very easy to get capture and hence, a malicious node holds the valid key can be prevented from participating in the route discovery process so this type of inside attackers can be blocked by using Intrusion Detection System (IDS).

There are two scenarios concerning topology in MANET. First, single-hop network where nodes within the radio communication range can directly communicate with each other; Second, Multi-hop network where nodes outside each the range must depend on some other nodes to relay messages. Thus acting like a Router to relay messages to other nodes outside each others range have to rely on some other nodes to relay messages.

Due to the transparency of wireless networks, they are especially vulnerable to spoofing attacks where an attacker falsifies its identity to masquerade as another device, or even creates multiple illegal identities. Spoofing attacks are a serious threat as they represent a form of identity compromise and can facilitate a variety of traffic injection attacks, such as DoS attacks. It is thus desirable to detect the presence of spoofing and remove them from the network [6] [7].

II. Architecture of The system

EAACK having three major components, these are ACK, secure ACK and Lease Report Authentication.

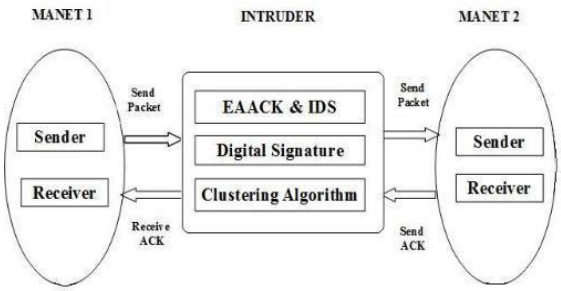

Fig.1. Two APs within the transmission range of the client.

Due to the limitations of most of MANET routing rules, nodes MANET are reluctant on other nodes cooperation to relay data. This dependency facilitates an attacker opportunity to have its impact on network by compromising one or more nodes tackle this problem, it arises the need of enhancing the security level of MANETs.

A. WATCHDOG SCHEME

Watchdog was designed to improve the throughput of network with the existence of malicious node. It works for detecting malicious node by constantly listening to its next hop transmission. If the next hop fails to relay the packet ahead within certain period of time, it results in increment of failure counter.
Furthermore, if failure counter exceeds a specific threshold value, it reports network as misbehaving.

Watchdog scheme fails in the following:
a. ambiguous collisions
b. receivers collisions
c. limited transmission power
d. false misbehaviour report
e. partial dropping[3]

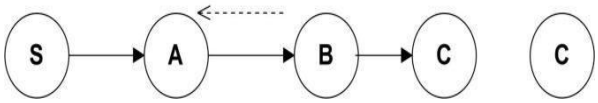

Fig.2. Watchdog Scheme

B. Two ACK Scheme

TWOACK [4]is neither an enhancement nor a Watch-dog based scheme. Aiming to resolve the receiver collision and limited transmission power problems of Watch-dog, TWOACK detects misbehaving links by acknowledging every data packets transmitted over each three consecutive nodes along the path from the source to the destination. Upon retrieval of a packet, each node along the route is required to send back an acknowledgement packet to the node that is two hops away from it down the route. TWOACK is required to work on routing protocols such as Dynamic Source Routing (DSR). The working process of TWOACK is

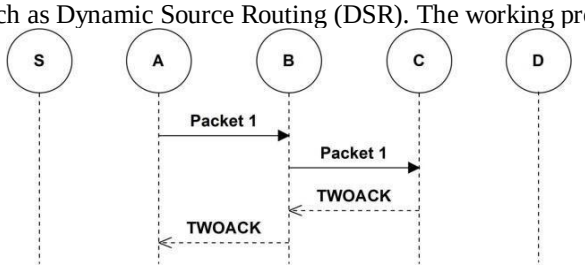

Fig.3. TWOACK scheme

Demonstrated in the figure.3 , node a first forwards packet 1 to node B, and then node B forwards Packet 1 to nodeC. When node C receives Packet 1, as it is two hops away from node A, node C is obliged to generate a TWOACK packet, which contains reverse route from node A to node C, and sends it back to node A. The retrieval of this TWOACK packet at node A indicates the transmission of Packet 1 from node A to node C is successful. Other-wise, if this TWOACK packet is not received in a prede-fined time period, both nodes B and C are reported as mali-cious. TWOACK scheme successfully solves the receiver collision and limited

transmission power problems posed by Watchdog. However, the acknowledgement process required in every packet transmission process added a
significant amount of unwanted network overhead. Due to the limited battery power nature of MANETs, such redundant transmission process can easily degrade the life span of the entire network.

C. ACK SCHEME

It is a hybrid scheme which uses TWOACK for ac- knowledgement. AACK is acknowledgement based net-work layer scheme which consists a combination of schemes called TACK (similar to TWOAACK) and end-to-end acknowledgement scheme called Acknowledgement. Compared to TWOACK, AACK significantly reduces net-work overhead, while still able to maintain or even out- shine the same network throughput[5]. In AACK, first the data transmit from source to destination.

When the destination receives a packet it is required to send back an acknowledgement packet to source in the reverse route of the data packet.

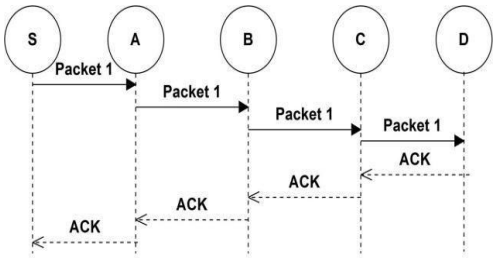

Fig.4. ACK scheme

Within the specified time period if the source receives the acknowledgement packet, then the packet transmission is successfully. Otherwise, the source will switch to TACK scheme by sending a TACK packet. This hybrid scheme greatly reduces network traffic but is still unable to cope up with false misbehavior report and forged acknowledgement.

III System Description

ACK is nothing but an end to end acknowledgment scheme. It acts as a crossbreed scheme in EEAACK. When there are no misbehaving nodes the transmission from source to destination is successful. Then destination sends an acknowledgement packet to source within predefined time constraint, otherwise source will switch to S-ACK mode [12].

B. Secured Acknowledgement Process

Source sends S-ACK packet in the intention of detecting misbehaving nodes in the route. S-ACK sends acknowledgment back to source after the packet reaches consecutive three nodes ahead the route. The third node Required to send a S-ACK acknowledgement to first node. S-ACK mode facilitates easy detection of misbehaving nodes in the presence of receiver collision and limited power for transmission [12]. N1, N2, N3 are three consecutive nodes. N1 sends S-ACK data packet to N2 which is next in the route and N2 relays it to N3 When N3 receives the S-ACK data packet it acknowledges N2 with S-ACK acknowledgement packet and N2 acknowledge back to N1.

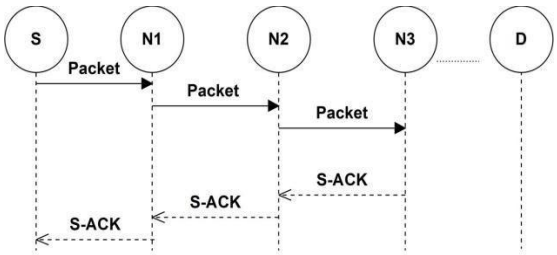

Fig.5. S-ACK scheme

If N1 doesn't receive the acknowledgement within a particular time it will report N2, N3 as malicious nodes by generating a misbehavior report. This misbehavior report is sent back to the Source. To validate this report the source switches itself to MRA mode.

C. MRA

Misbehavior Report Analysis (MRA)[12] is a scheme to confirm misbehavior report generated in S-ACK mode. This report may be a false one as attacker may interfere in S-ACK scheme generating a false misbehavior report. As a result, this may cause destruction of network by compromising guiltless nodes.

In MRA the source will check with the destination whether the destination node have received the missing packet through a different route. MRA mode is initiated by checking local knowledge base of sender for getting al-tentative route to destination; otherwise source uses Dynamic Source Routing method for alternative route. Once the destination gets the MRA packet, it compares the MRA packet with the local knowledge base to verify if the re-ported packet was received by it. If received, then it in-forms the source that the misbehavior report is false else it is considered as a legitimate report.

D. Digital Signature

All the above schemes are based on acknowledgement. These acknowledgements could be doubtful and must be checked for their rightfulness. We use digital signature in order to maintain integrity of the system. If we don't use digital signature the above discussed 3 schemes will be de-fenceless. We can use DSA or RSA algorithms to implement digital signature schemes is shown in the below figure.

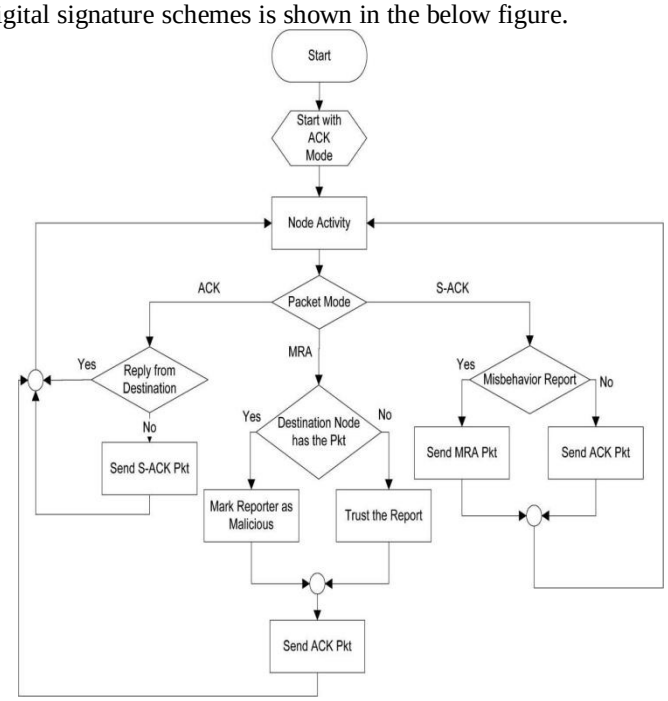

Fig.6. Detection Scheme

IV Simulation Tool

NS (version 2) is an object-oriented, discrete event driven network simulator developed at UC Berkely written in C++ and OTCL. NS is primarily useful for simulating local and wide area networks. Although NS is fairly easy to use once you get to know the simulator, it is quite difficult for a first time user, because there are few user-friendly manuals. Even though there is a lot of documentation written by the developers which has in depth explanation of the simulator, it is written with the depth of a skilled NS user. The purpose of this project is to give a new user some basic idea of how the simulator works, how to setup simulation networks, where to look for further information about network components in simulator codes, how to create new network components, etc., mainly by giving simple examples and brief explanations based on our experiences. Although all the usage of the simulator or possible network simulation setups may not be covered in this project, the project should help a new user to get started quickly NS is an event driven network simulator developed at UC Berkeley that simulates variety of IP networks.

It implements network protocols such as TCP and UPD, traffic source behavior such as FTP, Telnet, Web, CBR and VBR, router queue management mechanism such as Drop Tail, RED and CBQ, routing algorithms such as Dijkstra, and more. NS also implements multicasting and some of the MAC layer protocols for LAN simulations.

As shown in Figure in a simplified view, NS is Object-oriented Tcl (OTCL) script interpreter that has a simulation event scheduler and network component object libraries, and network setup (plumbing) module

libraries (actually, plumbing modules are implemented as member functions of the base simulator object). In other words, to use NS, you program in OTCL script language. To setup and run a simulation network, a user should write an OTCL script that initiates an event scheduler, sets up the network topology using the network objects and the plumbing functions in the library, and tells traffic sources when to start and stop transmitting packets through the event scheduler.

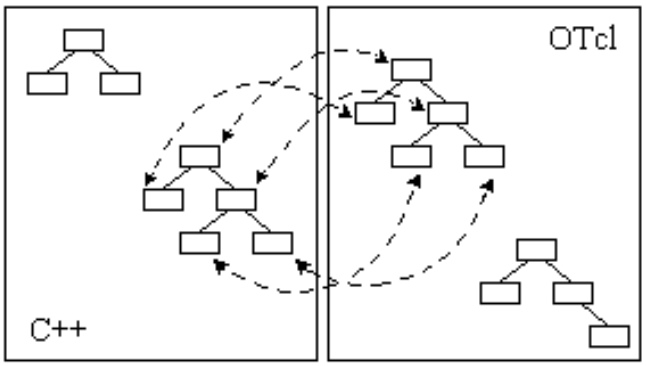

Fig.7. C++ and OTCL: The Duality

NS is written not only in OTCL but in C++ also. For efficiency reason, NS separates the data path implementation from control path implementations. In order to reduce packet and event processing time (not simulation time), the event scheduler and the basic network component objects in the data path are written and compiled using C++. These compiled objects are made available to the OTCL interpreter through an OTCL linkage that creates a matching OTCL object for each of the C++ objects and makes the control functions and the configurable variables specified by the C++ object act as member functions and member variables of the corresponding OTCL object. In this way, the controls of the C++ objects are given to OTCL. It is also possible to add member functions and variables to a C++ linked OTCL object. The objects in C++ that do not need to be controlled in a simulation or internally used by another object do not need to be linked to OTCL. Likewise, an object (not in the data path) can be entirely implemented in OTCL.
Figure 8 shows the general architecture of NS. In this figure a general user (not an NS developer) can be thought of standing at the left bottom corner, designing and running simulations in Tcl using the simulator objects in the OTcl
library. The event schedulers and most of the network components are implemented in C++ and available to OTcl through an OTcl linkage that is implemented using tclcl. The whole thing together makes NS, which is a OO extended Tcl interpreter with network simulator libraries. This section briefly examined the general structure and
architecture of NS. At this point, one might be wondering about how to obtain NS simulation results. As shown in Figure 7, when a simulation is finished, NS produces one or more text-based output files that contain detailed simulation data, if specified to do so in the input Tcl (or more specifically, OTcl) script. The data can be used for
simulation analysis (two simulation result analysis examples are presented in later sections) or as an input to a graphical simulation display tool called Network Animator (NAM) . NAM has a nice graphical user interface similar to that of a CD player (play, fast forward, rewind, pause and so on), and also has a display speed controller.
Furthermore, it can graphically present information such as throughput and number of packet drops at each link, although the graphical information cannot be used for accurate simulation analysis.

Network simulator (NS) is an object–oriented, discrete event simulator for networking research. NS provides substantial support for simulation of TCP, routing and multicast protocols over wired and wireless networks. The simulator is a result of an ongoing effort of research and developed. Even though there is a considerable confidence in NS, it is not a polished product yet and bugs are being discovered and corrected continuously. On the other hand, one disadvantage is that modifying and extending the simulator requires programming and debugging in both languages.

NS can simulate the following:
1) Topology: Wired, wireless
2) Sheduling Algorithms: RED, Drop Tail,
3) Transport Protocols: TCP, UDP
4) Routing: Static and dynamic routing

5) Application: FTP, HTTP, Telnet, Traffic generators.

Trace analysis. Running the TCL script generates a NAM trace file that is going to be used as an input to NAM and a trace file called "out.tr".

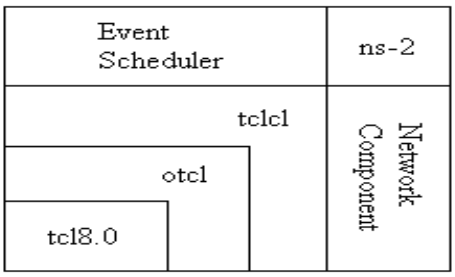

Fig.8. Architectural View of NS

that will be used for our simulation analysis. Figure shows the trace format and example trace DATA from";out.tr". Where each line in trace file represents an event associated to a packet.

V. Simulation Results

Now a day, WIFI hotspots are deployed widely and densely in many cities and the trend continues. Compared with cellular networks, WIFI has obvious advantages: lower cost and higher peak throughput. Thus, WIFI is considered as a suitable solution for cellular traffic offloading. However, it is still challenging to provide WIFI - based Internet access for users in moving vehicles. The above problems solve our proposed system concept. To support seamless and efficient WIFI-based Internet access for moving vehicles. It consists of innovative protocols in both uplink and downlink. Seamless roaming of clients was gracefully achieved, while channel utilization efficiency was dramatically improved.

Will prove high performance of compared to existing system.This work presents a coexistence study between DVB-T2 broadcasting services and IEEE 802.11p transmissions in the UHF TV channels in urban environments. A first measurement series allowed assessing the maximum transmission power level of an IEEE 802.11p signal while assuring the integrity of the DTT services for the typical MFN and

SFN operation modes of a real DVB-T2 broadcasting network. To assure the protection of the DTT systems the reception quality was quantified assuming the absence of a picture failure during a minimum observation time of 30 seconds.The results obtained for the investigated DVB-T2 transmission modes suggest that the effect of the 802.11p adjacent interference changes with its configuration. For the tested DVB-T2 receiver the worst operative case has been considered. The 802.11p interfering signal was initially set to a power level of -20 dB below the sensibility of the tested receiver and then adjusted at the output of the SDR board to achieve the required degradation (PF point) of the received and decoded TV signal.

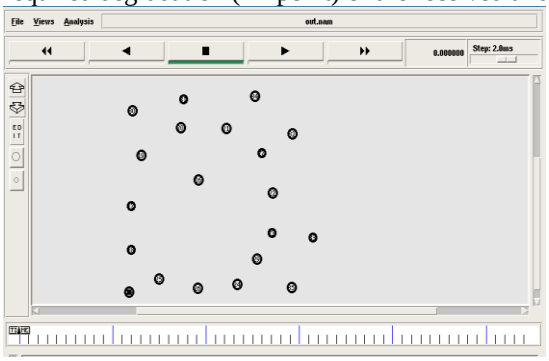

Fig.9. Nodes Deployed

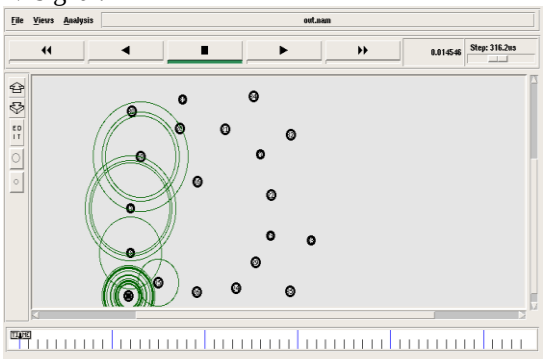

Fig.10. Coverage Area Analysis

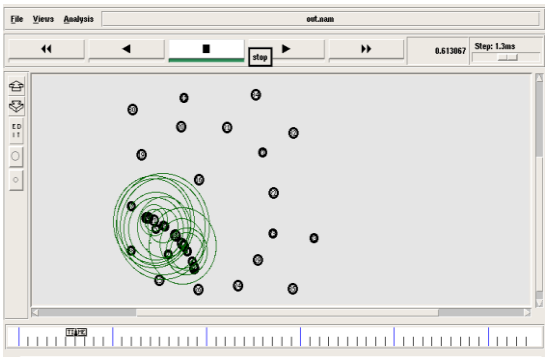

Fig Backhaul Implementation

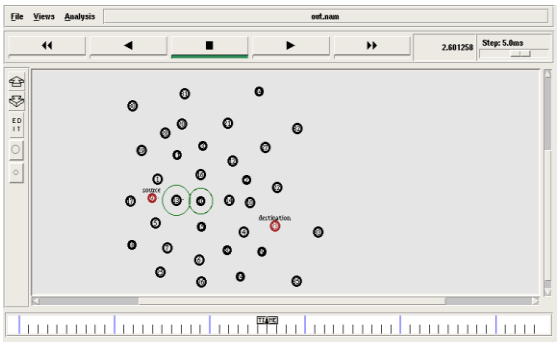

Fig.11. Acknowledgement Process

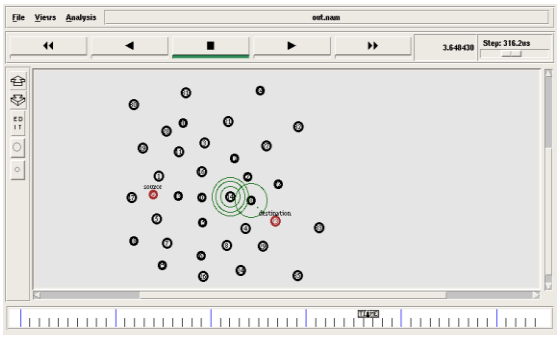

Fig.12. Secured Acknowledgement Process

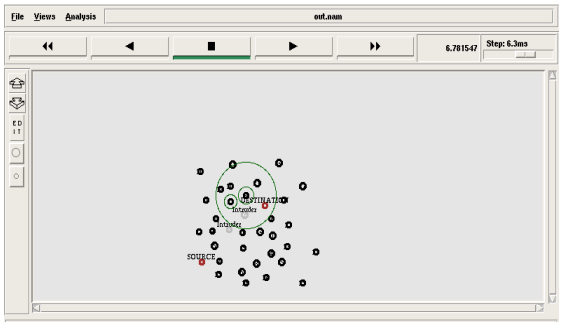

Fig.13. Misbehavior Report Authentication Process

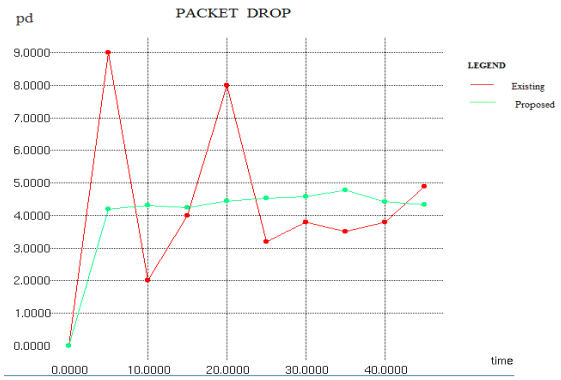

Fig .14. Packet Drop Comparison Graph

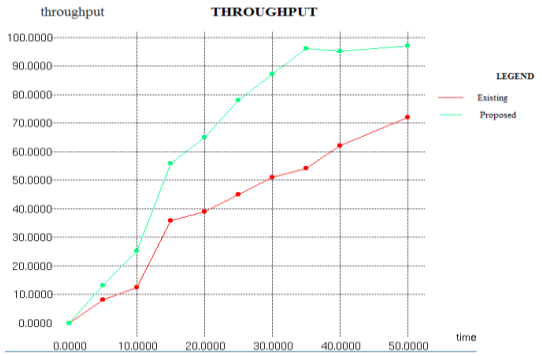

Fig.15. Throughput Comparison Graph

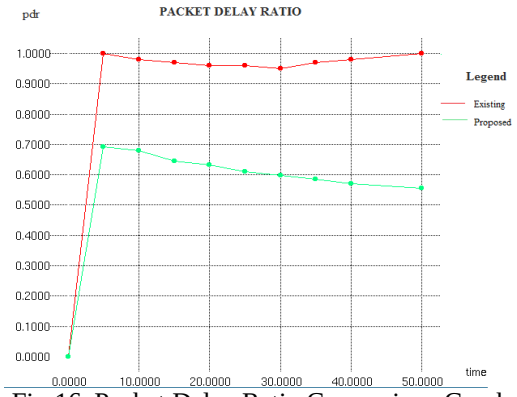

Fig.16. Packet Delay Ratio Comparison Graph

VI . Conclusion

Compared with cellular networks, WIFI has obvious advantages: lower cost and higher peak throughput.

Thus, WIFI is considered as a suitable solution for cellular traffic offloading. However, it is still challenging to provide WIFI -based Internet access for users in moving vehicles. The above problems solve our proposed system concept. To support seamless and efficient WIFI-based Internet access for moving vehicles. It consists of innovative protocols in both uplink and downlink. Seamless roaming of clients was gracefully achieved, while channel utilization efficiency was dramatically improved. Will prove Secure Seamless Wi-Fi Enhancement in Dynamic Vehicle is high performance of compared to existing system.

Ad-hoc On- Demand Distance Vector (AODV) and Dynamic source Routing(DSR) which are works for less count of host. When the network is larger, then clustering of hosts and also using distinct algorithm like routing algorithms between and within cluster can be a better solution. The main aim behind this approach is location property. If topology within cluster is change, then only those nodes are get inform which are present in cluster.

This approach hides all the small details in cluster. From time to time basis each and every node within a cluster gets some information about the topology.To make sure the purity of the IDS, in EEACK needs all acknowledgement packets should be digitally signed ahead they are send out and documented tillthose are received. The requirement of the more resources which are needed in MANET for accomplishing the digital signature. To achieve this goal we have carried out both DSA, RSA digital signature strategy in this planned approach. The aim is to detect maximum appropriate clarification by applying digital signature in this MANETs system.

Acknowledgement

We thank SRM Valliammai Engineering College for providing research resource to complete the task successfully.

References

[1] Ahmed. N, Keshav. S, and Papagiannaki. K (2011),"Omnivoice: A mobile voice solution for small-scale enterprises," in Proc. 12th ACM Int. Symp. Mobile Ad Hoc Netw. Comput., pp. 1–11

[2] Aijaz. A, Aghvami. H, and Amani. M (April 2013), "Adaptive Frequency Hopping Algorithm for Mulitcast Rendezvous in DSA Network," IEEE Wireless Commun., vol. 20, no. 2,pp. 104–112.

[3] Bai. F, Stancil. D, and Krishnan. H (2010),"Toward understanding characteristics of Dedicated Short Range Communications (DSRC) from a perspective of vehicular network engineers," in Proc. 16th Annu. Int. Conf. Mobile Comput. Netw.,pp. 329–340.

[4] Balasubramanian. A, Mahajan. R, and Venkataramani. R (2010), "Channel Hopping based Communication Rendezvous in Cognitive Radio System," in Proc. ACM 8th Int. Conf. Mobile Syst, Appl. Services, pp. 209–222.

[5] Balasubramanian.A,Mahajan. R, Venkataramani. R,Levine. B, and Zahorjan. J (2008), "Interactive wifi connectivity for moving vehicles," in Proc. ACM SIGCOMM,pp. 427–438.

[6] Balasubramanian. A , Zhou. Y, Croft. W, Levine. B, and Venkataramani. A(2007),"Web search from a bus," in Proc. ACM 2nd ACM Workshop Challenged Netw., pp. 59–66.

[7] Bychkovsky. V, Hull. B, Miu. A, Balakrishnan. H, and Madden. S (2006), "A measurement study of vehicular internet access using in situ wi-fi networks," in Proc. ACM 12th Annu. Int. Conf. Mobile Comput. Netw.,pp. 50–61.

[8] Cheung. M, Hou. F, Wong. V, and Huang. J (May 2012)," Dynamic optimal random access for vehicle-to- roadside communications," IEEE J. Sel.Areas Commun., vol. 30, no. 4, pp. 792–803.

[9] Chen. B and Chan. M (2009),"Mobtorrent: A framework for mobile internet access from vehicles," in Proc. IEEE INFOCOM, pp. 1404–1412.

[10] Eriksson. J, Balakrishnan. H, and Madden. S (May 2012),"Cabernet: Vehicular content delivery using wifi," in Proc. ACM 14th ACM Int. Conf. Mobile Comput. Netw., pp. 199–210.

[11] Gozalvez. J, Sepulcre. M, and Bauza. R (May 2012),"IEEE 802.11p vehicle to infrastructure communications in urban environments," IEEE Commun. Mag., vol. 50, no. 5,pp. 176–183.

[12] Lv. P, Wang. X, Xu. M, and Chen. Y (2011),"Network-leading association scheme in ieee802.11 wireless mesh networks," in Proc. IEEE Int. Cnf. Commun.

[13] Mahajan. R, Zahorjan. J, and Zill. B (2007),"Understanding wifi-based connectivity from moving vehicles," in Proc. 7th ACM SIGCOMM Conf. Internet Meas., pp.321–326.

[14] Miu. A, Balakrishnan. H, and Koksal. C (2005), "Improving loss resilience with multi-radio diversity in wireless networks," in Proc. ACM 11th Annu. Int. Conf. Mobile Comput. Netw.,pp. 16–30.

[15] Ott. J and Kutscher. D (2004),"Drive-thru internet: IEEE 802.11b for 'automobile' users," in Proc. IEEE INFOCOM, pp. 362–373.

[16] Pin Lv, Xudong Wang, Xiuhui Xue and Ming Xu (May 2015),"Seamless and Efficient Wi-Fi based Internet Access from Moving Vehicles,"IEEE Transactions on Mobile Computing., vol. 14,no. 5.

[17] Ramani.I and Savage. S (2005),"Syncscan: Practical fast handoff for 802.11 infrastructure networks," in Proc. IEEE INFOCOM, vol. 1, pp.675–684.

[18] Rodriguez. P, Chakravorty. R, Chesterfield. J, Pratt. I, and Banerjee. S (2004), "Interference Issues for VANETs Communication in the TVWS in Urban Environments,"in Proc. ACM2nd Int. Conf.Mobile Syst., Appl. Services, pp. 217–230.

[19] Wu. H, Tan. K, Zhang. Y, and Zhang. Q (2007), "Proactive scan: Fast handoff with smart triggers for 802.11 wireless lan," in Proc. IEEE INFOCOM, pp. 749–757.

[20] Wong. S,Yang. H, Lu. S, and Bharghavan. V (2006), "Robust rate adaptation for 802.11 wireless networks," in Proc. ACM MobiCom,pp. 146–157