ENERGY EFFICIENT AND SECURED PRE EXISTING ROUTING IN MOBILE ADHOC NETWORK

[1] Madala Venkaiak Naidu, [2]Dr. R. Jegadeesan [3]Palakurthi Shashank, [4]Aileni Vinisha, [5]Thudi Ravali Reddy, [6]Balakishan Porika

[1,2,3,4] SB.Tech Sttudents, [2,6]Associate Professor-Dept of CSE

[1,2,3,4,5,6]Jyothishmathi Institute of Technology & Science, Karimnagar, India.

ABSTRACT:

A versatile specially appointed system (MANET) is a framework less system where the one cell phone interface with other gadget remotely. Every gadget in MANET changes its development and connections toward any path regularly. Directing in MANET is the way toward sending the data from source to goal hub. Amid directing procedure, vitality utilization and burden adjusting are the requesting issue to improve the system lifetime. Also, security has principle influence amid the information transmission from source hub to goal. Verified steering is procedure of saving the data from unapproved clients amid information transmission in MANET. In existing works, there are numerous strategies for vitality effective and verified directing in MANET. However, the vitality utilization and security level was not improved. Our primary goal of the paper is to think about the current issues for vitality productive and verified steering in MANET.

Keywords: Mobile ad hoc network (MANET), data transmission, secured routing, infrastructure-less network, energy consumption.

I. INTRODUCTION

Remote MANET is another system less correspondence development which is includes those conditions where organization of establishment costs high. Beside this authenticity it has awful checks in regards to verify correspondence. MANET is described by its features such as self-orchestrating, scattered application and multi center directing. Due to its dynamic nature keeping up the verified correspondence is dull when united organization does not exist. In such condition key organization plans is a troublesome endeavor to achieve an ensured correspondence [1].

The standard preliminary of "MANETs is to course with low expenses in spite of when the conditions were dynamic". An Overhead given here is depicted the degree that directing convention control messages which eat up both channel transmission limit and the battery essentialness of focus focuses for correspondence/dealing with. Existing controlling customs in remarkably assigned structures use the single course that is worked for source and target focus point facilitates. Because of focus point flexibility, focus point disappointments and the dynamic attributes of the radio channel, which is related in a course, may maybe finish up being rapidly far off, influencing the course to invalid. The overhead of discovering elective courses mounts close-by extra bundle development delay.

MANETs are rich, self-arranging, and structure less get-togethers of cell phones. They are normally made for a particular reason. Every gadget inside a MANET is known as a middle and should fill the job of a customer and a switch.

Correspondence over the system is master by sending packs to a target focus point; when a speedy reason target interface is closed off broadly engaging focuses are utilized as switches. MANET correspondence is usually remote. Remote correspondence can be superfluously gotten by whichever focus in the degree of transmitter. This may lead the MANETs open to a degree of strikes, for example, the Sybil trap and the course control assaults that can trade off the dependability of the system. A MANET "includes flexible stages (e.g., a change with different hosts and remote explicit gadgets) - in this essentially inferred as 'focus focuses'- which are allowed to go about abstractly". These inside focuses are masterminded in or on the planes, ships, trucks, vehicles, even on solitary gadgets, and possibly there is different hosts per switch. A Mobile uniquely designated Network is an autonomous arrangement of all-around focus focuses [2].

These structures may work in partition or section and interface with a settled system. In the previous arranged method, it is much of the time obvious to fill in as a "stub" deals with related with a settled web work. These Stub systems propose advancement beginning at or perhaps vault for inner focus focuses yet don't empower exogenous activity to "travel" totally through the stub deals with. MANET centers are outfitted with remote transmitters and recipients utilizing broadcasting (radio) wires which might be Omni directional (passed on), phenomenally directional (point-to-point), possibly steer capable, or some mix thereof. Consequently, "At a given point in time subordinate upon the middle focuses positions and their transmitter and gatherer scope plans, transmission control levels and co channel impedance levels, a remote openness as an optional, multi-jump diagram or 'interestingly administered' system exists between the middle focuses". This exceptionally appointed topology may change with time as the focuses move or alter their transmission and get-together parameters.

Confirmed Routing for Ad hoc Networks (ARAN) convention utilizes open key cryptography to get indistinguishable outcome from SRP. Security-Aware Ad-hoc Routing is a far reaching convention to recognize the courses that experience a specific wellbeing foundation. The security criteria are met when the basic Secret Key (SK) is shared to all hubs [3]. A specific security level is met when the SAR finds the way.

After the distinguishing proof of the way, the ARAN and SRP are set up. In these conventions, imparting hubs are effectively found by the control messages and these control messages are taken care of by the middle hubs. Securing the Anonymity of the conveying hubs is a test that should be tended to. The Onion Routing convention tends to the issues of giving mysterious and secure correspondence [4]. A roundabout specialized strategy is given among the applications by organized Computing hubs, these hubs are called as onion routers. There are a few imperatives present in the current techniques, for example, directing overhead, throughput, vitality and security issues. To tackle these issues, this paper has presented AODV-DRSA-QC technique. This AODV-DRSAQC gives a higher verified strategy in MANET correspondence. In the typical security strategies, Cryptography technique is utilized for security reason in the middle of the source (Alice) and goal (Bob) by method for Key qualities. In our AODV-DRSA-QC framework, QC technique is utilized for same encryption reason and the cryptographic key is moreover scrambled by the method for double RSA strategy. AES is additionally utilized for security reason for MANET and the encoded type of a message (Cipher text) [5] is transmitted by utilizing the AODV Routing. In the wake of achieving the goal, the message (Cipher content) is changed over into plain content. The AODV-DRSA-QC strategy gives better outcomes as far as throughput, number of alive hubs, number of dead hubs, and vitality contrasted with the AODV-QC technique.

II. RELATED WORK

Another cryptographic system called Joint Cipher Mode (JCM) is presented. JCM furnishes a verified encryption with related information (AEAD) cryptographic administration in parcel based correspondence conventions. Portable impromptu systems (MANETs) need implementation of arrangement based access control instrument to limit unapproved gets to on the system assets. Arrangement based security framework in MANET is more unpredictable than conventional system because of uncontrolled media access and nonattendance of system borders. The expanding self-governance of Mobile Ad Hoc Networks (MANETs) has empowered a considerable number of huge scale unguided missions, for example, agrarian arranging, protection and comparable reviewing undertakings. As access control should be connected in a disseminated way, thinking about the versatility of hubs, customary security innovations like firewall, IDS and so forth can't fit for MANET. In this way, to guarantee security, appropriation and authorization of the approach governs over various hubs in MANET are the real research difficulties [6].

This work proposes an appropriated approach based access control system for MANET[7] MANETs have extraordinary qualities like powerful topology, remote radio medium, constrained assets and absence of incorporated organization; accordingly, they are defenseless against various kinds of assaults in various layers of convention stack. Every hub in a MANET is equipped for going about as a switch. Directing is one of the perspectives having different security concerns. In this paper, we will display review of regular Denial-of-Service (DoS) assaults on system layer to be specific Wormhole assault, Black gap assault and Gray opening assault which are not kidding dangers for MANETs. We will likewise talk about some proposed answers for identify and keep these assaults. As MANETs are broadly utilized in numerous imperative applications, loads of research work must be done to discover productive arrangements against these DoS assaults that can work for various steering conventions. [8] Mobile gadgets go about as hosts and switches in Mobile Ad-hoc Networks with no planned framework. The colossal increment in MANETs gives the advancement of different arrangements from wired to remote to Mobile Ad-hoc Networks. The security has been the key in any correspondence execution. The security usage in MANET is a testing and not thought about much for research. In this work we endeavor to construct a novel stage for the security answers for MANET design. We propose the structural reference show for MANET, which gives extension to scientists to upgrade and add to this examination work. We talk about the conventional IPsec and propose changed IPsec in MANET situations. [9] The expanding self-governance of Mobile Ad Hoc Networks (MANETs) has empowered a considerable number of huge scale unguided missions, for example, agrarian arranging, protection and comparable studying assignments. Business and military organizations have communicated extraordinary enthusiasm for such endeavors; bringing up the issue of security as the utilization of such frameworks in possibly unfriendly conditions turns into an ideal capacity of such systems. Counteracting burglary, disturbance or pulverization of such MANETs through digital assaults has turned into a concentration for some scientists therefore. Virtual Private Networks (VPNs) have been appeared to improve the security of Mobile Ad hoc Networks (MANETs), at a mind-boggling expense in system assets amid the setup of secure passages. VPNs don't ordinarily bolster communicate correspondence, diminishing their viability in high-traffic MANETs, which have many communicated correspondence necessities. To help steering, communicate refreshes and proficient MANET correspondence, Virtual Closed Network (VCN) design is proposed. By supporting private, secure correspondence in uncast, multicast and communicate modes, VCNs give an effective option to VPNs while verifying MANETs.

Similar investigation of the set-up overheads of VCN and VPN approaches is given between Open VPN, IPsec, Virtual Private LAN Service (VPLS), and the proposed VCN arrangement: Security Using Pre-Existing Routing for MANETs (SUPERMAN).This paper displays a novel expansion to the Consensus-Based Bundle Algorithm (CBBA), which we have named Cluster-Formed Consensus-Based Bundle Algorithm (CFCBBA). CF-CBBA is intended to decrease the measure of correspondence required to finish a disseminated undertaking distribution process, by dividing the issue and preparing it in parallel groups. CF-CBBA has been appeared, in examination with pattern CBBA, to require less correspondence while apportioning assignments. Three key parts of assignment allotment have been examined, (a) the time taken to designate undertakings, (b) the measure of correspondence important to fulfill the prerequisites of circulated errand portion calculations, for example, CBBA, and (c) the productivity with which a gathering of undertakings (a mission) is finished by a gathering of robots (a system). [9] Resource allotment is a basic issue that decides the nature of administration of GSM voice calls and GPRS information bundle transmissions in an incorporated GSM/GPRS organize. In this paper, we examine dynamic asset designation plans utilizing channel de-distribution (DAS) and re-portion (RAS) conspires in such a system. An expository model with general GPRS information channel prerequisite is created to assess the execution of the plans as far as the GSM voice call blocking likelihood, GPRS information bundle dropping likelihood, normal GPRS information parcel transmission time, channel use and framework grant. Our outcomes show that RAS can impressively improve the framework execution by brushing diverse DAS techniques. It is likewise demonstrated that the choice to pick the most proper unique asset distribution plot must be made dependent on the QoS prerequisite of the framework. [10].

III. PROPOSED SYSTEM

SUPERMAN is a uniquely named framework controlling tradition which has been changed in order to give an approval instrument which just empowers affirmed centers to course development in the framework. Controlling traditions act like an essential viewpoint to execution in convenient remote frameworks and it is important that the changes improved the circumstance security purposes does not impact the coordinating execution by and large. The goal of this future was to extend the framework lifetime to help both the first and changed variation of the SUPERMAN convention.[13] At that point the test framework was used to contemplate and survey the traditions' diagram, interchanges, and considerable scale execution issues. The proposed framework engineering is given in the figure 1.

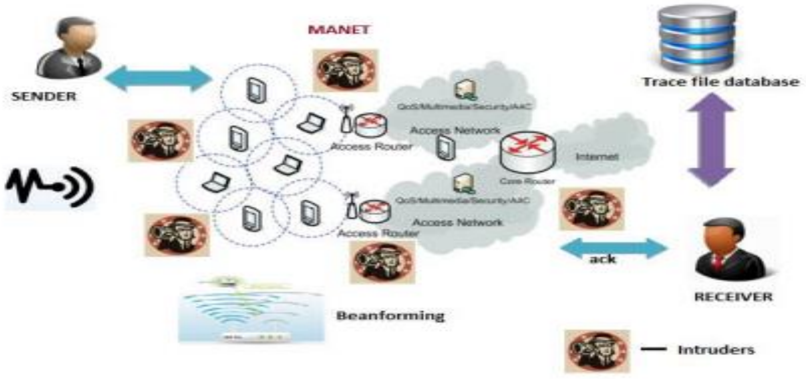

Figure1. Proposed Architecture

Three Phase Algorithms

One or various phantom assailants. Rather than bona fide center points, the attackers have no power or memory prerequisites. We acknowledge a three-arrange ambush show (a) pre-strike organize in which the attacker gets some answers concerning the framework by subtly listening stealthily the messages (b) Attack arrange in which the aggressor utilizes the insightful information to execute the ghost attack; and (c) post-ambush/fatigue organize. "Pre-Attack Phase: the attacker can pick up from the got messages the information of sender-beneficiary sets". The "proposed ambush does not require the data of the keys or the development information, the attacker can utilize information learned in the pre-strike stage to redesign its impact on the framework". Attack Phase: "The security suites depend upon the scramble or to make a novel key stream for each message to give semantic security". This errand is capable by using 16-bytes stand-out counter created from the fields in the message. [12]

The counter contains a "2-bytes static standards field, a 13-bytes nonce field.1-byte piece counter that numbers the 16-bytes discourages inside the message". The attacker sends different phony messages to quickly debilitate the imperativeness of the loss center point and thusly, suspend the availability of the organizations. For no good reason if the framework has some development oddity area plots set up, sending such different messages in a nutshell time allotment can be easily gotten. "To escape from the area, for instance, apparition attacker(s) can send messages either at different conditions or at different conveys to a subset of setback center points in its range". DoS in view of MAC inconvenience making: Due to the channel distinguishing and question based access CSMA/CA tradition, if a ghost attacker industriously sends the movement to the loss center point, all centers inside the obstacle area will be precluded from securing channel access and organizations [15].

IV. SIMULATION RESULTS AND ANALYSIS

In this paper, we will endeavor to look at the aftereffects of two Routing Protocols, one is Proactive Protocol and another is Reactive Routing Protocol. Responsive incorporates AODV (Ad-Hoc on Demand Distance Vector) Routing Protocol and Proactive incorporates DSDV (Destination Sequences Distance vector) Routing Protocol based on Average End to End Delay, Network Load, Throughput and Packet Delivery Ratio (PDR) quantitative measurements utilizing Riverbed Simulator. The AODV and DSDV Routing Protocols will chip away at TCP traffic design by making the situation with fixed number of hubs at consistent 3600 sec recreation time. Transmission Control Protocol (TCP) is one of the center Protocols of the Internet Protocol suite alluded to as TCP/IP. The reenactment setup has been contains 50 fixed hubs at a speed of 10 m/sec with substantial FTP traffic. The reenactment has been performed in Office Network Environment with 1 x 1 kilometers squared space.

A. RIVERBED Modeler

There are an assortment of programming are broadly accessible, for example, NS2 [9-12], RIVERBED (OPNET) [11], OMNeT++, QualNet [12], GloMoSim to perform reproductions of MANET Routing Protocols, in which we use RIVERBED Modeler variant 17.5. Our purpose behind choosing RIVERBED is because of its key highlights; giving answers for building systems and applications and it more often than not gives flawless outcomes. Riverbed Modeler is once in the past known as OPNET Modeler Suite. OPNET represents Optimized Network Engineering Tools. The utilization of RIVERBED is separated in four noteworthy advances displaying (making system hubs), at that point pick measurements, run reproductions lastly see and break down outcomes. The Results of our Simulation are: Throughput: Throughput is the quantity of parcels that are going through the direct in a specific unit of time and it tends to be improved with expanding hub thickness. It is generally estimated in byte/sec or bits/sec [3]. A few components influences the Throughput as though there are numerous topology changes in the system, untrustworthy correspondence between hubs, constrained data transfer capacity accessible and restricted vitality. High Throughput is constantly expected for any Routing Protocol.

We contrast DSDV and AODV Routing Protocol and the assistance of Throughput factor. In this, it tends to be unmistakably observed that, DSDV Routing Protocol is demonstrating higher Throughput than AODV Routing Protocol of the system of 50 fixed hubs for TCP traffic. In the time interim of 1200 to 3600 sec., greatest measure of bundles have been conveyed from source to goal hub as far as DSDV in light of the fact that it is a Proactive kind Routing Protocols and favorable position of these sort of Protocols is there are no postponement to discover the course from source to goal hubs since way is promptly accessible when source need to send a parcel. For a similar time interim AODV does not performs well as a result of less dynamic course.

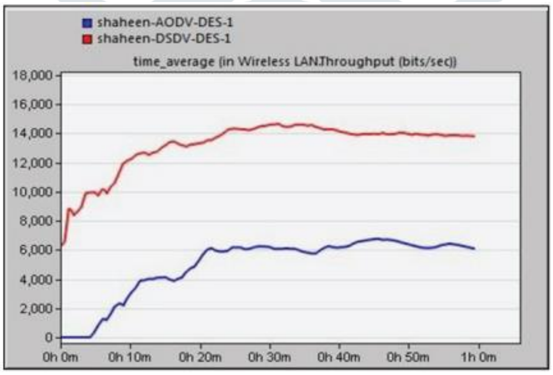

Fig. 2: Throughput

B. End to End Delay

The bundle End-to-End Delay (EED) is the normal deferral of information parcels from source to goal. It is likewise called Data Latency. It is communicated in seconds [4]. EED incorporates course disclosure, proliferation, lining, and exchange delays. In fig. 3, plots are appeared between AODV Routing Protocol in correlation with DSDV Routing Protocol for End to End Delay factor. The correlation is unmistakably demonstrating that DSDV Routing Protocol is indicating higher End-to-End Delay than AODV Routing Protocol with 50 fixed hubs setup in condition. The deferral in DSDV is high in light of the fact that in that specific time interim the separation between sending hub and getting hub is high because of traffic.

One purpose behind the corruption at last to-End Delay of DSDV is at higher number of hubs is credited to its course revelation process. In any case, the execution of AODV improves with the expansion in the quantity of sources. The responsive idea of AODV lessens the End-to-End Delay.

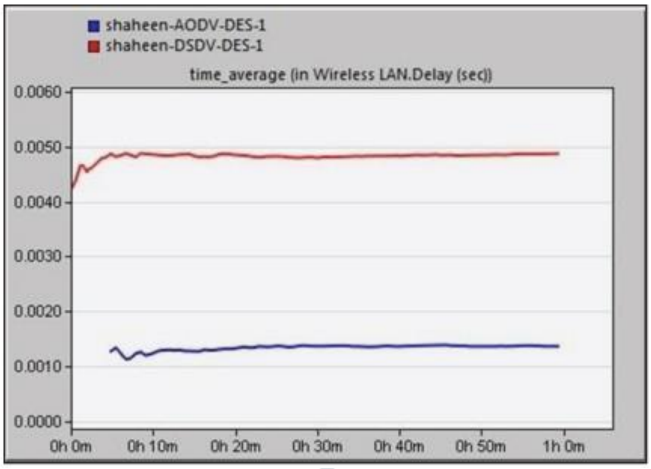

Fig. 3: End-to-End Delay

C. Packet Delivery Ratio (PDR):

Parcel Delivery Ratio (PDR) is the proportion between the quantity of got bundles by goal hub and the quantity of information bundles sent by source hub. It describes both the accuracy and proficiency of Ad-hoc Routing Protocols. A high Packet Delivery Ratio (PDR) is favored in a system [35]. In fig. 4, Packet Delivery Ratio (PDR) is being appeared among DSDV and AODV Routing Protocol, utilizing 50 hubs for FTP application. The DSDV Routing Protocol beats AODV directing convention as far as PDR with normal time interim. This is on the grounds that, as number of hubs builds, PDR will likewise increment in DSDV Routing Protocol as for time, accepting deferral as less vital factor. The significant reason for low PDR is the utilization of TCP traffic. TCP endures gigantic debasement in view of widespread retransmissions.

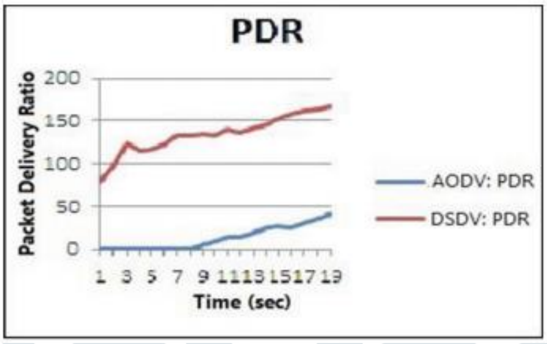

Fig. 4: Packet Delivery Ratio

D. Network Load

It speaks to the complete burden estimated in bits/sec, which is submitted to remote LAN layers by every single higher layer in all WLAN hubs of the system. It demonstrates the adequacy of Routing Protocols when the parcels are being gotten. The bigger this part is, the less effective the Protocol is.

Proactive Protocols are relied upon to have a higher burden than responsive ones. It very well may be found in Figure 2 of course; the Network Load in DSDV is higher than AODV. Despite the fact that, the receptive idea of AODV Routing Protocol causes more number of control overhead than DSDV and standardized steering load for AODV is high. Inspite of that, DSDV is Proactive in nature, keeps up directing table routinely consequently have substantial courses MAC overhead, which naturally builds by and large Network Load.

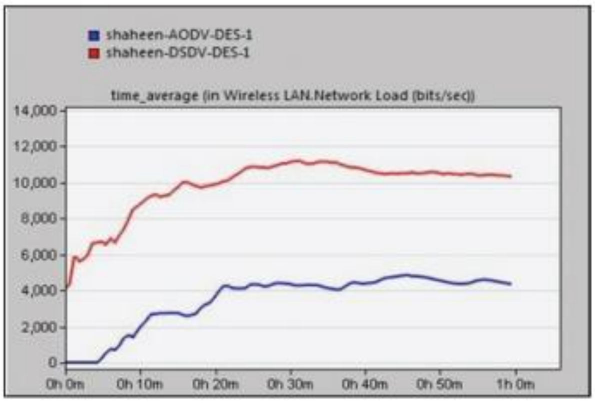

Fig. 5: Network Load

VI. CONCLUSION

Versatile Ad-hoc arranges is an exceptional sort of remote systems. It is a get-together of flexible focuses without having help to create framework. Amidst blueprint, security makes as a focal fundamental because of different ambushes that impacts the execution of the ad libbed structures. Especially Black opening trap is one such uncommon assault against extraordinarily named controlling customs which is an attempting one to verify against. The standard focus of the security tries acquainted with the SUPERMAN custom was to unite a sort of access control instrument in Mobile Ad hoc Networks (MANETs) which were to be utilized as a bit of for example crisis and extra conditions. The craving was to intertwine these security fragments. The proposed exhibit joins the SUPERMAN with CCMP-AES model to verify against diminish opening trap and it gives riddle and check of packs in both organizing and affiliation layers of MANETs. The crucial purpose of union of this work is to gives security instruments related in transmitting information plots in a middle point to focus point way through the security custom CCMP-AES working in information interface layer and it keeps information outline from tuning in, impedance, change, or dropping from unapproved party along the course from the source to the goal. The proposed show has shown better outcomes comparably as bundle transport degree, throughput, and End to End concede CCMP-AES Model with SUPERMAN guiding convention to verify Link layer and Network layer in Mobile Adhoc Networks. By differentiating SUPERMAN tradition and SUPERMAN tradition we show that SUPERMAN tradition is capable in all of the five parameters which reduces Delay and group incident and enlarge the throughput.

REFERENCES

[1] Darren Hurley-Smith, Jodie Wetherall, Andrew Adekunle, “SUPERMAN: Security Using Pre-Existing Routing for Mobile Ad hoc Networks”, IEEE Transactions on Mobile Computing (Volume: 16, Issue: 10, Oct. 1 2017), DOI: 10.1109/TMC.2017.2649527.
[2] Johnson D, Maltz D. Dynamic source routing in ad hoc wireless networks. In Mobile Computing, chapter 5, Imielinski T, Korth H (eds). Kluwer Academic: Hingham, MA, USA, 1996.
[3] Johnson DB, Maltz DA, Hu Y. The dynamic source routing protocol for mobile ad hoc networks.
[4] Park VD, Corson MS. A highly adaptive distributed routing algorithm for mobile wireless networks. In Proceedings of IEEE Infocom, 1997.
[5] Perkins CE, Royer EM. Ad hoc on-demand distance vector routing. In Proceedings of IEEE Workshop on Mobile Computing Systems and Applications (WMCSA), 1999.
[6] Perkins CE, Belding-Royer E, Das SR. Ad hoc on-demand distance vector (AODV) routing. http://www.ietf.org/rfc/rfc3561.txt, July 2003. RFC 3561.
[7] Perkins CE, Bhagwat P. Highly dynamic destination-sequenced distance-vector routing (DSDV) for mobile computers. In Proceedings of ACM Sigcomm, 1994.
[8] P. Sathishkumar , S. Balakrishnan , A. Vivek , “HOP Optimal Algorithm With Greedy Link Scheduler, To Avoiding Link Failure For Multihop Wireless Networks”, International Journal of Innovative Research & Development Vol 2, Issue 4, April 2013.
[9] P.Arivazhagan, S.Balakrishnan, Dr.K.L.Shunmuganathan, “An Agent Based Centralized Router with Dynamic Connection Management Scheme Using JADE”, International Journal of Applied Engineering Research, ISSN 0973-4562, Volume 11, Number 3 (2016) pp 2036-2041.
[10] Nadjib Badache, Djamel Djenouri and Abdelouahid Derhab “ Mobility Impact on Mobile Ad hoc Routing Protocols” In ACS/IEEE International Conf. on AICCSA’03, July 2003.
[11] Ian D.Chakeres and Elizabeth M.Belding-Royer “AODV Routing Protocol Implementation Design” International Conf. on Distributed Computing Sysmtes(ICDCSW’04) IEEE, vol.7 2004

[12] Ravi Prakash, Andre Schiper and Mansoor Mohsin “Reliable Multicast in Mobile Networks” Proc. of IEEE 2003(WCNC) [13] Weiliang Li and Jianjun Hao “Research on the Improvement of Multicast Ad Hoc On-demand Distance Vector in MANETS” IEEE Vol.1 2010 [14] M.Gerla et al., “On-demand multicast routing protocol (ODMRP) for ad hoc networks”. Internet draft,,(2000)

[15] Shapour Joudi Begdillo, Mehdi Asadi and Haghighat.A.T. “Improving Packet Delivery Ratio in ODMRP with Route Discovery”, International Jour. Of Computer Science and Network Security, Vol.7 No.12, Dec2007.

[16].Jegadeesan,R.,Sankar Ram M.Naveen Kumar JAN 2013 “Less Cost Any Routing With Energy Cost Optimization” International Journal of Advanced Research in Computer Networking,Wireless and Mobile Communications.Volume-No.1: Page no: Issue-No.1 Impact Factor = 1.5

[17]. Jegadeesan,R.,Sankar Ram, R.Janakiraman September-October 2013 “A Recent Approach to Organise Structured Data in Mobile Environment” R.Jegadeesan et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 4 (6) ,Page No. 848-852 ISSN: 0975-9646 Impact Factor:2.93

[18]. Jegadeesan,R., Sankar Ram October -2013 “ENROUTING TECHNICS USING DYNAMIC WIRELESS NETWORKS” International Journal of Asia Pacific Journal of Research Ph.D Research Scholar 1, Supervisor2, VOL -3 Page No: Print-ISSN-2320-5504 impact factor 0.433

[19]. Jegadeesan,R., Sankar Ram, M.S.Tharani (September-October, 2013) ”Enhancing File Security by Integrating Steganography Technique in Linux Kernel” Global journal of Engineering,Design & Technology G.J. E.D.T., Vol. 2(5): Page No:9-14 ISSN: 2319 – 7293

[20]. Ramesh,R., Vinoth Kumar,R., and Jegadeesan,R., January 2014 “NTH THIRD PARTY AUDITING FOR DATA INTEGRITY IN CLOUD” Asia Pacific Journal of Research Vol: I Issue XIII, ISSN: 2320-5504, E-ISSN-2347-4793 Vol: I Issue XIII, Page No: Impact Factor:0.433

[21]. Vijayalakshmi, Balika J Chelliah and Jegadeesan,R., February-2014 “SUODY-Preserving Privacy in Sharing Data with Multi-Vendor for Dynamic Groups“ Global journal of Engineering,Design & Technology. G.J. E.D.T.,Vol.3(1):43-47 (January-February, 2014) ISSN: 2319 –7293

[22]. Jegadeesan,R.,SankarRam,T.Karpagam March-2014 “Defending wireless network using Randomized Routing process” International Journal of Emerging Research in management and Technology

[23].Jegadeesan,R.,T.Karpagam, Dr.N.Sankar Ram , “Defending Wireless Network using Randomized Routing Process“ International journal of Emerging Research in management and Technology ISSN: 2278-9359 (Volume-3, Issue-3) . March 2014

[24]. Jegadeesan,R., Sankar Ram “Defending Wireless Sensor Network using Randomized Routing ”International Journal of Advanced Research in Computer Science and Software Engineering Volume 5, Issue 9, September 2015 ISSN: 2277 128X Page | 934-938

[25]. Jegadeesan,R., Sankar Ram,N. “Energy-Efficient Wireless Network Communication with Priority Packet Based QoS Scheduling”, Asian Journal of Information Technology(AJIT) 15(8): 1396-1404,2016 ISSN: 1682-3915,Medwell Journal,2016 (Annexure-I updated Journal 2016)

[26]. Jegadeesan,R.,Sankar Ram,N. “Energy Consumption Power Aware Data Delivery in Wireless Network”, Circuits and Systems, Scientific Research Publisher,2016 (Annexure-I updated Journal 2016)

[27]. Jegadeesan,R., Sankar Ram , and J.Abirmi “Implementing Online Driving License Renewal by Integration of Web Orchestration and Web Choreogrphy“ International journal of Advanced Research trends in Engineering and Technology (IJARTET) ISSN:2394-3785 (Volume-5, Issue-1, January 2018

[28]. Pooja,S., Jegadeesan,R., Pavithra,S., and Mounikasri,A., “Identification of Fake Channel Characteristics using Auxiliary Receiver in Wireless Trnsmission“ International journal for Scientific Research and Development (IJSRD) ISSN (Online):2321-0613 (Volume-6, Issue-1, Page No. 607-613, April 2018

[29]. Sangeetha,R., Jegadeesan,R., Ramya,P., and Vennila.,G “Health Monitoring System Using Internet of Things“ International journal of Engineering Research and Advanced Technology (IJERAT) ISSN :2454-6135 (Volume-4, Issue-3, Page No. 607-613, March 2018.