International Journal of Engineering Innovation & Research
Volume 2, Issue 6, ISSN: 2277 – 5668

An Implementation Analysis and Evaluation Study of DSR with Inactive DoS Attack in Mobile Ad hoc Networks

E. Suresh Babu
Associate Professor,
PACE Institute of Technology & Sciences Ongole.
Email: suresh_esb551@yahoo.co.in

C. Nagaraju
Associate Professor
YSR College of Engineering of YV University, Kadapa.
Email: cnrcse@yahoo.com

MHM Krishna Prasad
Associate Professor
JNTU College of Engineering, Kakinada
Email: mhmkrishnaprasad@gmail.com

***Abstract* – The idea of connecting anytime, anywhere as led to the development of Ad hoc Network, in which mobiles nodes and link connectivity might change all the time. In this kind of networks, security, quality of service, routing are important and complex problems. Secure routing in ad hoc network is a daunting task because of some contradictions between sustained benevolent behavior by all nodes participating in the network and the associated applications. In this paper tries to identify the benevolent behavior against the standard pre-existing routing protocol, Dynamic Source Routing (DSR) protocol. The selection of DSR is because it seemed that it would be the one that could more easily accommodate the needed modifications. The proposed solution will analyze routes in an ad-hoc network while discovering and maintaining in the presence of selfish node. With the simulations results obtained , we emphasize the efficiency that affects the Throughput, Packet delivery Ratio, End-to-End-Delay of our scheme and highlight that it outperforms the DSR protocol when as many as 3% of the nodes are acting selfishly and 5% nodes are maliciously.**

***Keywords* – DSR, Ad hoc Networks, Attacks.**

I. INTRODUCTION

Today modern civilization is bestowed with enormous advancement of Artificial Intelligence, Information Technology and Mobile Communication. Internet technology has added much ease and speed in all spheres of our life, from office job to personal entertainment. Recently mobile computing has enjoyed a tremendous improvement and enhancement. Excellent rise of processing power and computing power of mobile devices deserves the credit of such proliferation. There are situations where networking applications are badly needed even in absence of Internet connection, for example, in military applications and rescue operation in natural disaster. Furthermore, people using laptop computers may wish to initiate a conference without using the Internet access. Such scenarios depict the necessity of instant networking without any infrastructure more formally an *ad hoc* network. Such network is highly flexible and based on wireless transmission. In contrast of the applications of ad hoc network, it is evident to realize that secure service delivery in such network has become a major concern of the related researchers. Particularly secure routing has become an excellent topic of open research because of the extraordinary gap between the nature of ad hoc network and the security required by its applications.

II. AD-HOC NETWORKING – AN OVERVIEW, GOALS, CHARACTERISTICS AND ITS APPLICATIONS

Ad hoc networking is a group of nodes or computers without any fixed infrastructure and connected by wireless communication. A node communicates with another distant node (i.e. out of radio range) by hop-by-hop basis. There are some unique and attractive features of mobile ad hoc network (MANET) as such *No fixed infrastructure, Automatic self-configuration and maintenance, Quick deployment, No centralized administration, reduced administrative cost* To achieve the attractive features mentioned above ad hoc network often contains the following network properties[1]: *Peer-to-peer, Multi-hop, Dynamic, Zero administration, Low power, Autonomous, Self-configured.*

The concept of ad hoc network was founded to satisfy the following initial goals: *Scalability, To enable larger network, Quick convergence, Bi-directional communication, Loop freedom, Unicast* etc. But with the rapid proliferation of ad hoc network in different applications for the last few years, the applications deserve some other properties for ad hoc networking: *Security, Multicast, Quality of Service, Smooth handovers, Internet gateway operation, and Service discovery*.

Possible applications of MANET include: *soldiers relaying information* for situational awareness on the battlefield, business associates sharing information during a meeting, attendees using laptop computers to participate in an interactive conference, and *emergency disaster relief* personnel coordinating efforts after a fire, hurricane or earthquake. Other possible applications [5] include *personal area and home networking, location-based services*

3. VULNERABILITIES AND CHALLENGES IN AD HOC NETWORKS

Ad hoc network has some attractive features which are the major causes for rapid popularity in various applications. But at the same time, these features make it harder to achieve security. They can be summed up in the following way [3][4]:

Ad hoc network uses wireless media for transmission. It is beneficial from the point of view that it can be deployed at anytime and anywhere. But obviously it suffers from security flaws from wireless communication. Both active and passive attacks such as impersonation, eavesdropping, message redirection, traffic analysis can be performed by an adversary.

In ad hoc network there is no central authority. Again, this feature is highly attractive but poses a major barrier to ensure security. Different security mechanisms such as Key Management, Node Authentication, and Determination of Node Behavior etc without any central administration are really very difficult to achieve.

Ad hoc network is highly dynamic in nature. Node joins and departures are performed without any prediction. Moreover, network topology is always changed in such network. Therefore any static security mechanism will not be applicable in MANETs. In other words, security primitives must be dynamically adjusted to cope with the network which is, of course, a daunting task.

In MANETs most of the nodes are considered to be constrained by power and computational capability. For example, hand held PDAs, Laptops are the best feasible nodes to form an ad hoc network.

Security is an essential service for wired and wireless network communications. The success of MANET strongly depends on whether its security can be trusted. However, the characteristics of MANET pose both challenges and opportunities in achieving the security goals, such as *Confidentiality, Authentication, Integrity, Availability, Access Control, and Non-Repudiation.* In order to ensure high degree of security robust encryption with large key (i.e. such as RSA) may be applied but in MANETs it becomes very expensive

IV. Various Attacks in MANETS

There are a wide variety of attacks [14] that target the weakness of MANET. Some attacks apply to general network, some apply to wireless network and some are specific to MANETs. These security attacks can be classified according to different criteria, such as the domain of the attackers, or the techniques used in attacks.

Passive vs. Active Attacks: The attacks in MANET can roughly be classified into two major categories, namely passive attacks and active attacks [14, 17]. A passive attack obtains data exchanged in the network without disrupting the operation of the communications, Examples of passive attacks are eavesdropping, traffic analysis, and traffic monitoring while an active attack involves information interruption, modification, or fabrication, jamming, impersonating, denial of service (DoS), and message replay thereby disrupting the normal functionality of a MANET.

V. Overview of DSR Routing Protocol

The Dynamic Source Routing (DSR) protocol[6] is a reactive routing protocol. As the name suggests it makes use of the strict source routing feature of the Internet Protocol. This protocol is designed to restrict the bandwidth consumption by control packets as it eliminates the periodic table-update by the control packets. As compared with other on-demand routing protocols, it is a *beacon-less* and therefore does not require periodic *hello* packet (*beacon)* transmission, usually used by a node to inform its presence to the neighbors. The basic approach of this protocol is briefly described as under: The sender of a packet determines the complete sequence of nodes through which the node has travel. The sender of the packet explicitly mentions the list of all nodes in the packet's header, identifying each forwarding 'hop' by the address of the next node to which to transmit the packet on its way to destination host. In this protocol the nodes don't need to exchange the Routing table information periodically and thus reduces the bandwidth overhead in the network. Each Mobile node participating in the protocol maintains a *routing cache*, which contains the list of routes that the node has learnt. Whenever the node finds a new route it adds the new route in its routing cache. Each mobile node also maintains a sequence counter *'request-id'* to uniquely identify the requests generated by a mobile host. The pair <*source address, request-id*> uniquely identifies any request in the ad hoc network. The protocol does not need transmissions between hosts to work in bi-direction. The main phases in the protocol are – Route Discovery Phase and Route Maintenance Phase

5.1 Route Discovery Phase: Router discovery allows any host to dynamically discover the route to any destination in the Ad Hoc network. In DSR, a source initiates a route discovery process when the source wants to send a packet to a destination to which it doesn't have a valid route. The Source, if it has the valid route in its routing cache then it uses it otherwise it sends a ROUTE REQUEST packet by broadcasting it to the neighbors. The ROUTE REQUEST packet contains the *source address, request- id* (Unique Identification Number) and a route record in which the sequence of hops traversed by the request packet before reaching the destination are noted down.

5.2 Route Maintenance Phase: Route maintenance is a procedure of monitoring the correct operation of route in use. The host that uses the route does this maintenance. Since the nodes do not exchange any routing information in this protocol the route maintenance procedure monitors the operation of the route and informs the source of any errors. Any host if it detects that its neighboring node, which is the next hop for a route, is not working then the node sends an *error packet* containing its address and the address of the hop not working. A node upon receiving the route error packet removes the hop in error from its routing cache. Acknowledgements are used to verify the correct operation of the route. The route maintenance can be provided by using either hop-to-hop or by using end-to-

end acknowledgements. In case of hop-to-hop acknowledgements the hop in error is indicated in the route error packet. But in case of end-to-end acknowledgements the source node assumes that the last hop of the route to the destination is error.

The Reactive protocols in ad-hoc networks typically assume that all nodes are cooperative in the coordination process. This assumption is unfortunately not true in a hostile environment. Because cooperation is assumed but not enforced in MANETs, malicious attackers can easily disrupt network operations by violating protocol specifications. The main network layer operations in MANETs are ad-hoc routing and data packet forwarding, which interact with each other and fulfill the functionality of delivering packets from the source to the destination. The ad-hoc routing protocols exchange routing messages between nodes and maintain routing states at each node accordingly. Based on the routing states, data packets are forwarded by intermediate nodes along an established route to the destination. Nevertheless, both routing and packet forwarding operations are vulnerable to malicious attacks, leading to various types of malfunctions in the network layer. Network layer vulnerabilities generally fall into one of two categories: routing attacks and packet forwarding attacks, based on the target operation of the attacks. For example, in the context of DSR, the attacker may modify the source route listed in the RREQ or RREP packets by deleting a node from the list, switching the order of nodes in the list, or appending a new node into the list. By attacking the routing protocols, the attackers can attract traffic toward certain destinations in the nodes under their control, and cause the packets to be forwarded along a route that is not optimal or even non-existent. The attackers can create routing loops in the network, and introduce severe network congestion and channel contention in certain areas. Multiple colluding attackers may even prevent a source node from finding any route to the destination, and partition the network in the worst case. In addition to routing attacks, the adversary may launch attacks against packet forwarding operations as well. Such attacks do not disrupt the routing protocol and poison the routing states at each node. Instead, they cause the data packets to be delivered in a way that is intentionally inconsistent with the routing states. For example, the attacker along an established route may drop the packets, modify the content of the packets, or duplicate the packets it has already forwarded. Another type of packet forwarding attack is the denial-of-service (DoS) attack via network layer packet blasting, in which the attacker injects a large amount of junk packets into the network. These packets waste a significant portion of the network resources, and introduce severe wireless channel contention and network congestion in the MANET.

VI. MALICIOUS ATTACK, SELFISH NODE AND FAULTY NODE FOR EXISTING DSR PROTOCOL

The main focus of this paper to generate Byzantine faults- *malicious packet-dropping, Selfish Node and Faulty Node* where a node intentionally drops packets that are destined for other nodes. The methodology and the algorithm used for creating malicious packet dropping is discussed with an example scenario in the following sections.

Some of the reasons might be genuine while others indicate malicious or selfish

- *Malicious Intent:* A node might want to disrupt the communication by misrouting, dropping or corrupting data packets. This scenario is very likely to occur in battlefield operations where the enemy nodes are always trying to disrupt the ongoing communication.
- *Selfish Behavior:* Every node in an ad-hoc network must forward packets on behalf of others even if they are not of interest to it. So, a node might not be willing to expend its battery power on behalf of others.

In any case, it is imperative to detect such behavior and take appropriate action to avoid any unnecessary wastage of scarce network resources like bandwidth, battery power, etc to retransmit the packets and to exchange control information. In other words, such behavior impedes the efficient functioning of the ad-hoc network.

The main assumptions being made to generate Byzantine faults include:

- The ad-hoc network has DSR as the underlying routing protocol and TCP is the underlying transport layer protocol
- A node chosen to behave maliciously does so starting at some random time and from that time onwards it drops all the packets it receives
- A malicious node only drops packets that belong to the higher layers (for eg. tcp) in the TCP/IP stack but not the control messages sent out by the DSR agents for route discovery, maintenance etc
- Malicious nodes do not collude with one another
- All the packet drops are either due to malicious packet dropping or due to broken link(s) at some intermediate node in the source route

6.1 Scenario of Malicious Attack in DSR Protocol

In the DSR routing protocol, a node sends a DSR route error message back to the source if it is unable to deliver the packet to its next hop neighbor as indicated in the source route. This could be due to node movement which could result in a new network topology and the old route no longer exists or this could be due to a temporary broken link between the node and its next hop and the node is unable to find an alternate route to that destination using the routes it had already discovered. A TCP timeout normally occurs when sender does not receive an acknowledgement within a specific interval. This may happen because the packet was dropped at an intermediate node due to congestion at that node or the packet's Time To Live (TTL) value has expired or by some malicious node trying to disrupt the network or due a broken link at some intermediate node in the source route or the packet got corrupted during transmission and was dropped by an intermediate node. But it should be pointed out that the current research assumes that there is no congestion in the

network and hence there will not be any packet drops due to congestion.

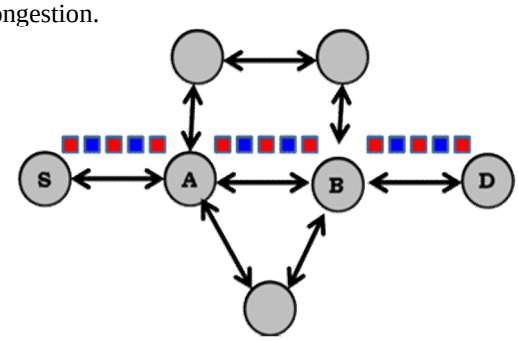

Fig.1. DSR Packet Delivery from Source Node to Destination Node

Figure-1 shows a snapshot of the current network topology at a particular instance of time. Node S is the source and D is the destination. Assume that the DSR routing agent in node S has found the source route S-A-B-D to the destination D for a request from the TCP agent at node S to establish a connection with node D and also assume that the source node S is equipped. Figure shows the scenario where there are no malicious nodes in the network and everything is normal. Since, there is no malicious activity in the network; it will only be silently monitoring the status of the network. While the communication between nodes S and D is in progress, at some random time, node B starts behaving maliciously by dropping the packets destined for D instead of forwarding them.

Figure-2 shows the scenario where there are no malicious nodes in the network and everything is normal initially. Since, there is no malicious activity in the network; it will only be silently monitoring the status of the network. While the communication between nodes S and D is in progress, at some random time, node B starts behaving maliciously by dropping the packets destined for D instead of forwarding them.

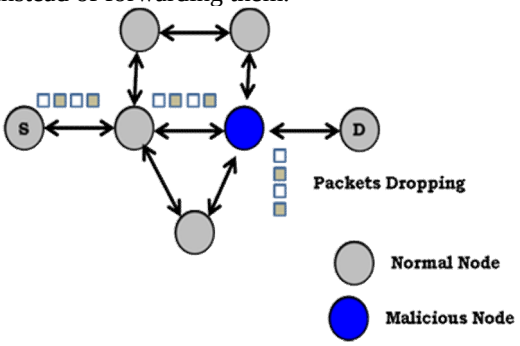

Fig.2. Malicious Packet Dropping

Figure- 3 shows such a scenario Selfish Node Dropping the Packet. In this case the Selfish node B sends out DSR route error messages to the source node S after dropping packets destined for node D. So, node S will think of them as genuine timeouts and will acts as a malicious behavior. Also, if a selfish node selectively drops the packets instead of dropping all of them. Currently selective packet dropping and colluding malicious nodes are not being taken into consideration and will be studied as part of future research.

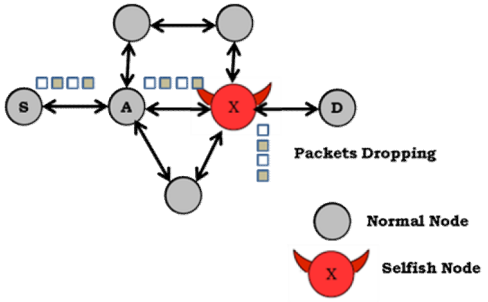

Fig.3. Selfish Node Dropping the Packet

VII. Simulation Environment

Our Simulation used for experiments and provides an analysis of the Dynamic Source Routing protocol with Malicious and Selfish Attack is implemented using NS-2. A mobile ad hoc network consisting of 50,150,100,200 nodes in a simulation area of 750m×750m is simulated. The link layer model of the IEEE 802.11 wireless LAN standard. The radio model uses the frequency hopping spread spectrum technology with 2 Mbps capacity. The radio propagation range for each node is 250 meters. In order to get realistic performance, the results are averaged for a number of scenarios. We tried to measure the protocols performance on real life scenario at a speed of 10 m/s. The simulation time was taken to be of 150 seconds for FTP traffic type with a packet size of 512 Byte. Also, we have considered nodes with Omni-Antenna and Two Ray Ground Radio Propagation method. Simulation parameters are appended in Table-1.

Table 1: Simulation Parameters

Parameter	Value
Channel	Channel/Wireless Channel
Propagation model	Propagation/Two Ray Ground
Antenna	Antenna/Omni Antenna
Simulator	NS-2
No of Nodes	50,100,150,200
Routing Protocols	DSR
MAC Layer	802.11 IEEE
Simulation Time	150 Second
Simulation Area	750m X 750m
Transmission Range	250m
Node Movement	Model Random Waypoint
Traffic Type	FTP
Data Payload	512 Bytes/Packet

7.1 Misbehaving Nodes

The ns-2 simulator was modified to enable particular node(s) to be configured as malicious. The configuration also takes in a time parameter that specifies the time from which that node starts behaving maliciously. Beginning from that time, the node drops all the packets (non-control packets) that are received at that node till the end of the simulation. Each network is designed to contain 5 malicious nodes reflecting misbehavior of 30% of the

nodes. The number and placement of the malicious nodes ensures that they will be located along active paths in the network. To determine the effectiveness of our approach, the percentage of misbehaving nodes was varied from 0% to 30% in 5% increments.

VIII. PERFORMANCE EVALUATION

The performance evaluation is based on the comparison of following metrics

- *Packet Delivery Fraction (PDF):* The ratio of the data packets delivered to the destination and the total number of data packets generated by the sources. Mathematically, it can be expressed as:

$$P = \frac{1}{C}\sum_{k=0}^{s}\frac{R_k}{N_k}$$

Where, P is the fraction of successfully delivered packets, C is the total number of flow or connections, k is the unique flow id serving as index, R_k is the count of packets received from flow k and N_k is the count of packets transmitted to k.

- *Average End to End Delay (AEED)*: It is an aggregated average of the time taken by a packet for the successful delivery at the destination. The time for the successful delivery is the interval between between the packet is generated at the source and the time when it is delivered to the application at the destination. It includes all the delays that can occur due to waiting in the data buffer, in the network interface queue and the time taken in propagation. Where N is the number of successfully received packets, i is unique packet identifier, R_i is time at which a packet with unique id i is received, S_i is time at which a packet with unique id i is sent and D is measured in ms.

$$D = \frac{1}{N}\sum_{i=1}^{s} R_i - S_i$$

- *Routing Load (RL)*: It is the ratio of the routing packets generated to the data packets delivered at the destination. Sometime it also renamed as throughput.

$$\text{Throughput } (T) = \frac{r_a}{g_a}$$

Table 2: Performance Metrics for Original DSR Routing Protocol

Nodes	Throughput	End2End Delay	PDF
25	390.06	612.049	0.9958
50	406.06	333.293	0.9967
100	321.48	605.303	0.9921
150	351.33	659.157	0.9915
200	430.21	628.573	0.9958

r_a: total no. of received packets at application layer;
g_a: total no. of generated packets at application layer

Table 3: Performance Metrics for DSR Routing Protocol with Internal Attacks

Nodes	Throughput	End2End Delay	PDF
25	255.88	672.422	0.9845
50	182.19	448.455	0.9834
100	263.26	665.452	0.9802
150	192.96	715.956	0.9819
200	292.53	680.284	0.9812

8.1 Performance Analysis

It is observed that from Figure-4 shows End-2-End delay for DSR with internal attack such as Selfish node and Malicious node provides extra time than Original DSR which affects the performance when the numbers of malicious nodes in the network are more. It also be seen from Figure-5 PDF is the ratio of the number of data packets received by the destination to the number of data packets sent by the source between DSR and MDSR have almost similar performance expect slight difference when the number of malicious nodes in the network is relatively small which falls short when compared to those by DSR, by about 1%. This performance shown in the graph confirms this result.

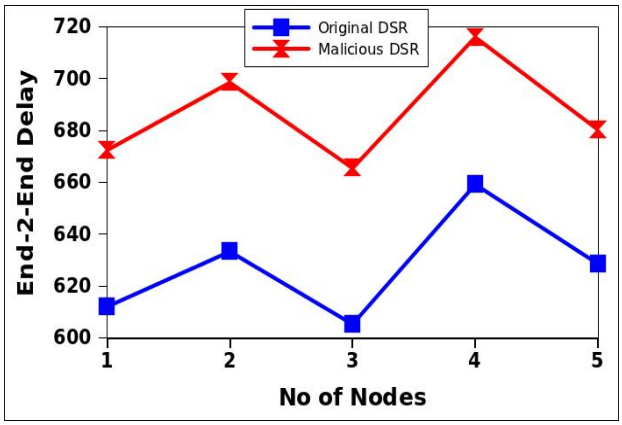

Fig.4. End-To-End Delay with Varying No of Nodes with DSR vs. MDSR

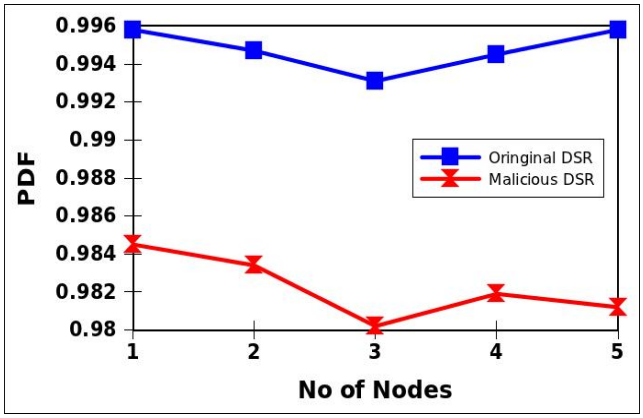

Fig.5. Packet Delivery Fraction with varying number of Nodes with DSR Vs MDSR.

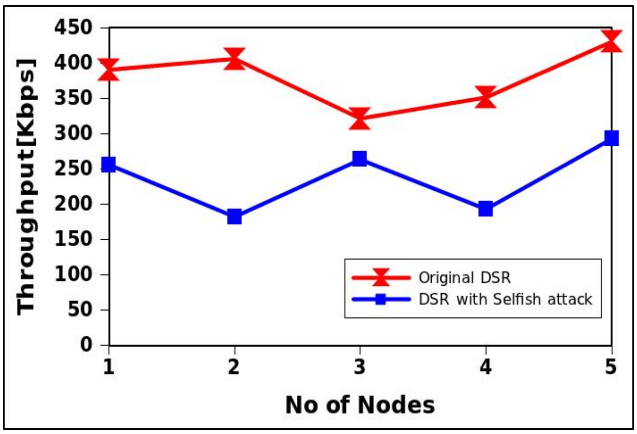

Fig.6. Throughput with varying number of Nodes with DSR Vs MDSR

It may be seen from Figure-6 that the data packets received in case of MDSR falls drastically with increase in the number of malicious nodes, those packets received in case of DSR increases. It clearly indicates that MDSR is badly affected by malicious nodes.

IX. Conclusion and Future Work

Mobile ad-hoc networks have several advantages over traditional wireless networks including simplicity of deployment, speed of deployment, and decreased dependence on a fixed infrastructure. Mobile ad-hoc networks constitute an emerging wireless networking technology for future mobile communications. In this paper, we presented a scheme to analyze insider attacks against mobile ad-hoc routing protocols, and reported a systematic analysis of the DSR protocol. We classified the possible insider attacks into atomic misuses and compound misuses, and identified a number of atomic misuses as well as compound misuses. We also performed a series of experiments (based on simulation) to validate these misuses. Our results showed that an inside attacker can effectively invade into routes, consume the nodes' resources, isolate victim nodes from the rest of the network, disrupt existing route, or prevent certain nodes from establishing routes in DSR networks. The results are potentially useful for protocol developers to evaluate their designs, and for intrusion detection researchers to validate their detection algorithms and systems.

We performed simulation of the DSR protocol. Our study results indicate that DSR may be considered as one of the best routing protocol for providing secure routing using DNA cryptography algorithm because there are no periodic beacons, thus resulting in a lesser overhead during communication. In the presented work, the selfish nodes are dealt with; it would be interesting to note the behavior of a routing protocol capable of handling both selfish and malicious nodes using DNA cryptography.

References

[1] M. Frodigh, P. Johansson, and P. Larsson. "Wireless ad hoc networking: the art of networking without a network," *Ericsson Review*, No.4, 2000, pp. 248-263.

[2] IETF Working Group: Mobile Adhoc Networks (manet).http://www.ietf.org/html.charters/manet-charter.html.

[3] Ad Hoc Networking Extended Research Project. Online Project. http://triton.cc.gatech.edu/ubicomp/505.

[4] Mobile Ad Hoc Networking: An Essential Technology for Pervasive Computing Jun-Zhao Sun MediaTeam, Machine Vision and Media Processing Unit, Infotech Oulu P.O.Box 4500, FIN-90014 University of Oulu, Finland

[5] Mobile ad hoc networking: imperatives and challenges Imrich Chlamtac ,Marco Conti b, Jennifer J.-N. Liu

[6] David B. Johnson, David A. Maltz, Yih-Chun Hu. The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks (DSR). *Internet Draft,draft-ietf-manet-dsr- 09.txt*, 15 April 2003.

[7] Ram Ramanathan and Jason Redi *A Brief of Overview of Ad Hoc Networks: Challenges and Directions*.. BBN Technologies.

[8] Charles.E.Perkins. *AdHoc Networking*.. Addison- Wesley, 2001.

[9] Pekka Savola. *DSR: Dynamic Source Routing*.CSC/FUNET, Helsinki University of Technology.

[10] Charles.E.Perkins, Elizabeth M Royer, Samir.R.Das and Mahesh.K.Marina. Performance Comparison of Two On-Demand Routing Protocols for Ad Hoc Networks *IEEE Personal Communications*,, Feb 2001.

[11] ElizabethMRoyer, Chai-Keong Toh A Review of Current Routing Protocols for Ad Hoc Mobile Wireless Networks. *RFC 2409, IEE Personal Communications* , 1999

[12] A Survey of Attacks and Countermeasures in Mobile Ad Hoc Networks Bing Wu, Jianmin Chen, Jie Wu, Mihaela Cardei

[13] Yih-Chun Hu, David B.Johnson Caching Strategies in On-Demand Routing Protocols for Wireless Ad HocNetworks *Carnegie Mellon University, Pittsburgh*

[14] ElizabethMRoyer, Chai-Keong Toh A Review of Current Routing Protocols for Ad Hoc Mobile Wireless Networks. *RFC 2409, IEE Personal Communications* , 1999

[15] Yih-Chun Hu, David B.Johnson Caching Strategies in On-Demand Routing Protocols for Wireless Ad Hoc Networks *Carnegie Mellon University, Pittsburgh*

[16] Maltz.D , Broch. J, Jetsceva. J, Johnson.D The effects of On-Demand Behavior in Routing Protocols for Multi-Hop Wireless Ad Hoc Networks *IEEE Journal on Selected Areas in Communications special issue on mobile and wireless networks. August 1999.*

[17] E.Suresh Babu , C.Nagaraju, MHM Krishna Prasad " An Implementation and Performance Evaluation Study of AODV ,MAODV ,RAODV in Mobile Adhoc Networks in JSER-2013

[18] E.Suresh Babu ,C.Nagaraju, MHM Krishna Prasad " An Implementation and Performance Evaluation of Passive DoS Attack on AODV in Mobile Adhoc Networks in IJETTCS-2013.

Author's Profile

E. Suresh Babu

received his B.Tech degree in Computer Science from RGM College of Engineering, Nandyal, M.Tech degree in Computer Science from V.T.University Belgaum and pursuing PhD in Computer Science & Engineering from J.N.T.University Kakinada. Currently, he is working as an Associate Professor in the Department of CSE in PACE Institute of Technology & Sciences; Ongole He has got 11 years of teaching experience. He has published 6 research papers in various International Journal and 7 research papers in various National and International Conferences. He has attended 20 seminars and workshops. His areas of interests are wireless communication and Mobile Computing.

Dr. C. Naga Raju
received his B.Tech degree in Computer Science from J.N.T. University Anantapur, M.Tech degree in Computer Science from J.N.T. University Hyderabad and PhD in digital Image processing from J.N.T. University Hyderabad. Currently, he is working as a Associate professor in YSR College of Engineering of YV University, Poddutur. He has got 16 years of teaching experience. He has published thirty Five research papers in various National and International Journals and about twenty eight research papers in various National and International Conferences. He has attended twenty seminars and workshops. He is member of various professional societies like IEEE, ISTE and CSI.

Dr. MHM. Krishna Prasad
received his B.Tech from CBIT Hyderabad, M.Tech degree in Computer Science from J.N.T. University Hyderabad and PhD in Computer Science & Engineering from J.N.T. University Hyderabad. Currently, he is working as a Associate professor in the Dept of Information Technology JNTUK University College of Engineering Vizianagaram. . He has got 19+ years of teaching experience. He has published Twenty research papers in various National and International Journals and various research papers in National and International Conferences. He has attended twenty seminars and workshops. He is member of various professional societies like IEEE, ISTE and CSI.