Volume 5, Issue 5, MAY 2015 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Comparison of QoS metrics with AODV and DSDV in simulator NS-2.35

Mattareddy S
M.Tech, Jntu Kakinada
Andhra Pradesh, India

Kanthi Rekha
M.Tech, Jntu Kakinada
Andhra Pradesh, India

B. A. S. Roopa Devi
Associate Professor
Andhra Pradesh, India

Abstract— Mobile Ad-hoc Networks (MANETs) are future wireless networks consisting entirely of mobile nodes that communicate on-the-move without base stations. Nodes in these networks will both generate user and application traffic
and carry out network control and routing protocols. Rapidly changing connectivity, network partitions, higher error rates, collision interference, and bandwidth and power constraints together pose new problems in network control—particularly in the design of higher level protocols such as routing and in implementing applications with Quality of Service requirements. This paper provides an overview of comparision of AODV and DSDV QoS metrics i.e packet delivery ratio, delay ,throughput ,jitter overall residual energy, and control overhead .And give the total information about for which metric which protocol is better it give the exact idea of main metrics of MANETs.

Keywords— MANETS , AODV , DSDV , Q o S metrics , Network Simulator.

I. INTRODUCTION

The remarkable technology of wireless networks started in late 1970s and the interest has been growing ever since. Earlier, information sharing between various communication devices was difficult, as the users need to set up static, bi-directional links between the devices to perform various administrative tasks. In order to prevent the difficulty in maintaining these infrastructure based networks, various techniques have been determined leading to ad hoc networks. In Adhoc Networks, there is no infrastructure, which makes it easily deployable and connects the communication devices (nodes) within no time. Such interconnection between mobile nodes is called a Mobile Ad hoc Network (MANET). Mobile ad hoc network is an autonomous and decentralized network in which any mobile node can freely move in and out of the network. These mobile nodes must act as both host and router in which both route discovery mechanism and data transmission between nodes is handled by the mobile nodes itself. These nodes have the ability to configure themselves and because of their self-configuring capability, they can form an arbitrary network when needed without the basis of any fixed infrastructure. Due to these characteristics, the network topology gets varied more frequently and hence a routing protocol must be efficient enough in delivering an ameliorated network performance. Traditional routing protocols used for wired networks cannot be employed for mobile ad hoc networks because the basic idea of such ad hoc networks is mobility with dynamic topology [Janne Lundberg et al, 2014]. Routing protocols plays a major role in such type of networks whose function is to transfer data packets between the mobile nodes efficiently tackling all the varying situations. Due to their inherent characteristics and lack of any centralized administration, mobile ad hoc networks are vulnerable to different types of security attacks. These attacks include active interfering, passive eavesdropping, impersonation and denial of service [Ketan et al, 2014]. Since the communication among the nodes is purely based on mutual trust between nodes, malicious nodes in the network must be identified carefully and must be restricted in their behavior. Hence securing a mobile ad hoc network is necessary for basic functionality of the network. Black hole attack is one among these various attacks. In the black hole attack, a malicious node drops all the packets coming in its way without transferring them to its neighborhood node, thus degrading the network performance. Black hole attack may occur due to a malicious node which is deliberately misbehaving, as well as a damaged node interface. Such type of attacks must be prevented in order to obtain better performance of the network. In this paper, the performance of the AODV routing protocol is examined under black hole attack.

II. ROUTING PROTOCOLS IN MANETS

In MANETs, nodes are not familiar with the network topology in priori. Routing protocols are responsible in establishing the paths between the mobile nodes in order to transmit data between source and destination in that path. Hence a routing protocol must be efficient enough in handling various network phenomenon's and must tolerate against different security attacks. These routing protocols are broadly classified into three types based on the phenomenon in which they broadcast information.

1. Proactive or Table-Driven routing protocols
2. Reactive or On-Demand routing protocols
3. Hybrid routing protocols

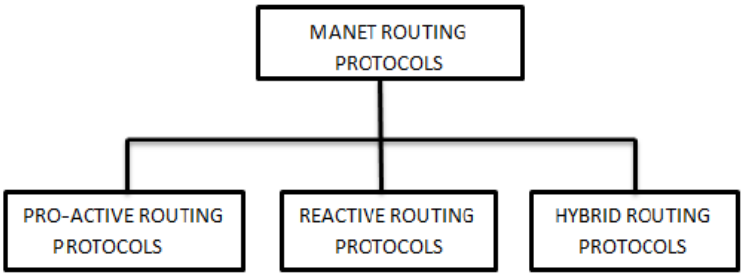

Figure 1: Routing Protocols in MANETs

2.1 Proactive routing protocols

Proactive routing protocols designed for MANETs are adopted from various traditional routing protocols available for wired networks. Proactive routing protocols attempt to maintain an up-to-date routing information from each node to every other node in the network prior to the need of data transmission. The routing information is kept in a number of different routing tables and the routing information is updated regularly responding to the changes in the network topology. Primary advantage of proactive routing protocols is the availability of routes to concern nodes at any moment. Control overhead generated by these protocols is significantly more in large networks. Examples of such networks include DSDV, OLSR, WRP etc.

2.2 Reactive routing protocols

In this type of routing protocols, routes between the mobile nodes are not continuously maintained without any need such as in proactive routing protocols. Routes are established between the mobile nodes only when needed i.e., On-Demand. Here in reactive routing protocols, if a source node needs to send data packets to some destination, it checks whether it already has a route towards the destination to transmit data packets. If it does not find any route, then it initiates the route discovery phase to establish a new path towards the destination, through which the data packets are sent. The drawback of the reactive routing protocol is the introduction of route acquisition latency. The time taken by the data packets to reach the destination is more compared to proactive routing protocols. Reactive routing protocols include AODV, DSR, and AOMDV etc.

2.3 Hybrid routing protocols

Hybrid routing protocols exploit the strengths of both proactive and reactive routing protocols in order to deliver better performance. In hybrid routing, entire network is divided into zones so that, one protocol is used within a zone and another protocol is used between the zones. ZRP is an example of such routing protocol.

Performance of the On-demand routing protocol, AODV is determined in this paper. Ad-hoc On-demand Distance Vector (AODV) routing protocol AODV is an on-demand routing protocol. It does not maintain any routing information and participate in any periodic routing table exchanges prior to the necessity of communication. It finds the route between the mobile nodes only when needed (on-demand). AODV routing protocol adopts the concept of destination sequence numbers from DSDV to maintain the most recent information about the mobile nodes and the concept of on-demand route discovery and maintenance from DSR. Each entry in the routing table consists of the destination node, destination sequence number, number of hops, next hop, expiration table for the entry in the tables containing the routing information etc. AODV routing protocol makes use of various control messages such as Route Request (RREQ), and Route Reply (RREP) for establishing a path from source to destination. Header information of various control messages used in AODV is listed out in [C. E. Perkins et al, 2004]. Whenever a source node needs to communicate with another node for which it has no route, the process of route discovery is initiated by the source which broadcasts a RREQ packet to its neighborhood nodes. Each neighboring node either responds to the RREQ by sending Route Reply (RREP) packet back to the source node or it further transfers the RREQ packets to its neighborhood nodes after incrementing the hop count. This route discovery process is carried on until the RREQ packet reaches the destination node or an intermediate node that has a fresh enough route entry for the destination in the routing table. Once the intermediate node has a valid route towards destination, it sends a RREP packet back to the source node in the reverse path. Making use of the reply from an intermediate node rather than the destination node reduces the route establishment time and also the control traffic in the network. Sequence numbers are used in these control packets and they serve as time stamps which are used by the nodes to compare the freshness in the routing information [Ranjeet et al,2012]. When a node sends any type of routing control message, it increases its own sequence number in the message. Routing information with highest sequence number is considered to have more fresh or up-to-date information. If a node receives more than one RREP, it updates its routing information, and propagates the RREP with the highest sequence number discarding others. The source starts the data transmission as soon as it receives the first RREP, and then its updates its routing information of better route to the destination node. If at all any of the nodes in the data path moves away causing the breakage of the link, the route discovery process is reinitiated to establish a new route to the destination node, Route Error (RERR) control packet is sent to all the nodes in the network which are using this broken link for communication. Routing protocol assumes that all the nodes are cooperative in nature in broadcasting information.

III. SIMULATION SETUP

In order to analyze the performance of AODV and DSDV, network simulator NS-2.35 is used. NS-2.35 uses the collaborative environment for simulation making use of discrete event simulation. Here various quantitative metrics like packet delivery ratio, average end-to-end delay, normalized routing load and jitter. The performance of the network is determined with the following network parameters summarized in Table 1.

Table 1:Parameters and Values

parameters	values
simulator	ns-2.35
network dimentions	1000 x 1000
simulation time	200sec
channel	wirelesschannel
propagation	TwoRayGround
routing protocols	AODV,DSDV
application	UDP,TCP
No.of nodes	20,40,60,80,100
Mac	IEEE 802.11
pause time	0 sec
queue type	priority queue

3.1.SIMULATION METHODOLOGIES:

Based on the QoS metrics here the AODV & DSDV routing protocols are compared.

SCENARIO 1: This scenario is used to compare the Packet Delivery Ratio of both AODV and DSDV .Show in figure 7

SCENARIO 2: This scenario is used to compare the Jitter of both AODV and DSDV. Show in figure 8

SCENARIO 3: This scenario is used to compare the throughput of both AODV and DSDV. Show in figure 9

SCENARIO 4: This scenario is used to compare the delay ratio of both AODV and DSDV. Show in figure 10

SCENARIO 5: This scenario is used to compare the control overhead of both AODV and DSDV. Show in figure 11

IV. PERFORMANCE EVALUATION

In this paper, the comparision of AODV and DSDV is determined by considering the quantitative metrics such as packet delivery ratio, average end-to-end delay, control overhead, throughput and jitter. However, the network performance is evaluated with different nodes. In these cases, the following metrics are considered to evaluate the performance under varied node mobility and node density.

1) Packet Delivery Ratio: Packet Delivery Ratio (PDR) is the ratio between the number of packets transmitted by a traffic source and the number of packets received by a traffic sink. It measures the loss rate as seen by transport protocols and as such, it characterizes both the correctness and efficiency of ad hoc routing protocols. It represents the maximum throughput that the network can achieve. A high packet delivery ratio is desired in any network.

PDR = TOTAL NO.OF RECEIVED PACKETS / TOTAL NO.OF PACKETS SENT

2) Average End-to-End Delay: The packet end-to-end delay is considered as the average time a packet takes to traverse the network. This is the time from the generation of a packet by the source, till its reception at the destination's application layer and is expressed in seconds. It therefore includes all the delays in the network such as buffer queues, transmission time and delays induced by routing activities and MAC control exchanges. The end-to-end delay is therefore a measure of the how well a routing protocol adapts to the various constraints in the network and represents the reliability the routing protocol.

DELAY=∑(RECEIVED TIME - SENT TIME) / TOTAL DATA PACKETS RECEIVED

3) Jitter: Jitter is the variation in the time between packets arrival, caused by network congestion, timing drift, or route changes. A network with constant delay has no variation (or jitter). Hence jitter should be minimum for a routing protocol to perform better.

4)Throughput:-

Throughput defined as the ratio of the total amount of data that reaches a receiver from a sender to the time it takes for the receiver to get the last packet.

5)Control overhead:-

Refers to the time it takes to transmit data on a packet switched wireless network. Each packet requires extra bytes of format information that is stored in the packet header and combined with the assembly and disassembly of packets, decreases the overall transmission speed of the raw data.

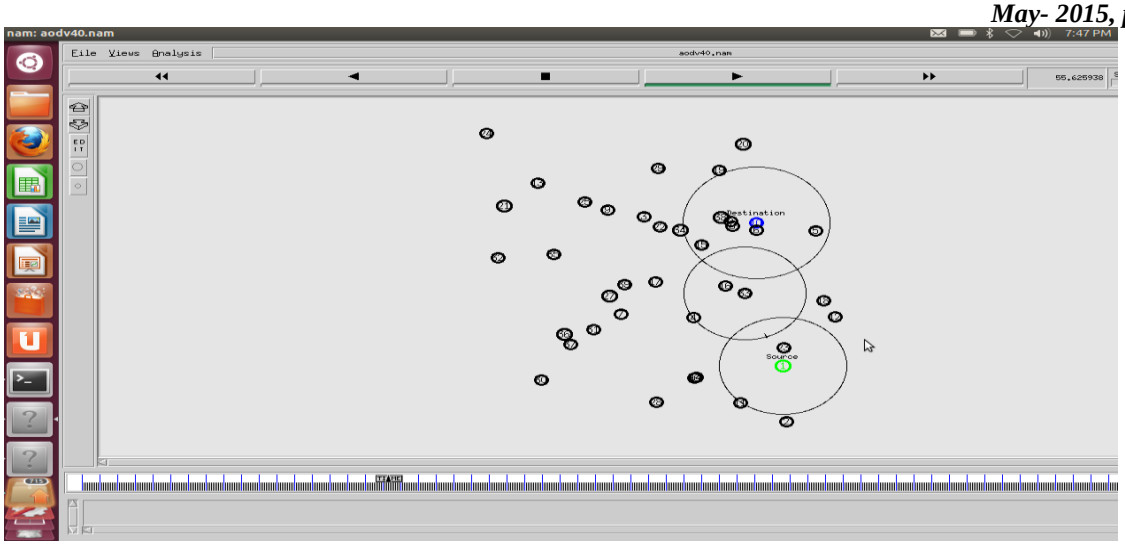

Figure 1:packets transferring from source to destination in ns-2.35 simulator

AODV WITH SIMULATION TIME 200 Sec					
	20 nodes	40 nodes	60 nodes	80 nodes	100 nodes
PDR	62.4931	97.5014	92.9206	98.2752	99.1754
CONTROL OVERHEAD	2242	1402	4836	233	1571
DELAY	0.247213	0.156685	0.166979	0.05	0.084666
THROUGHPUT	102045	159211	151731	161313	161976
JITTER	0.065134	0.051032	0.053929	0.050597	0.049685
OVERALL RESIDUAL ENERGY	-19	-39	-59	-79	-99
AVG RESIDUAL ENERGY	-1	-1	-1	-1	-1

FIG 3: AODV QOS METRICS OUTPUT VALUES

DSDV WITH SIMULATION TIME 200sec					
	20 nodes	40 nodes	60 nodes	80 nodes	100 nodes
PDR	11.4659	43.5591	31.1771	53.9423	48.3898
CONTROL OVERHEAD	620	1688	3340	4670	6649
DELAY	0.048606	0.044316	0.078	0.052885	0.029904
THROUGHPUT	18723.6	71128	50909.3	88082.7	79016
JITTER	0.083901	0.108967	0.148107	0.073086	0.079273
OVERALL RESIDUAL ENERGY	-19	-39	-59	-79	-99
AVG RESIDUAL ENERGY	-1	-1	-1	-1	-1

FIG 4: DSDV QOS METRICS OUTPUT VALUES

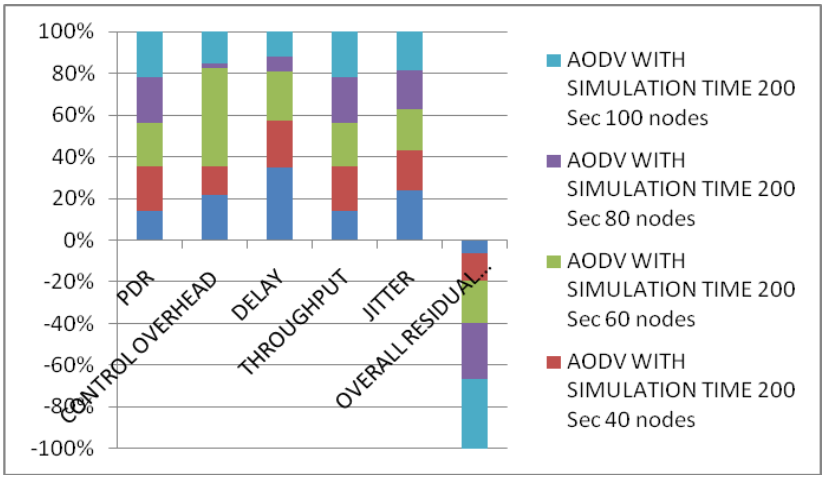

FIG 5:GRAPH FOR ALL QOS METRICS COMPARISION OF AODV

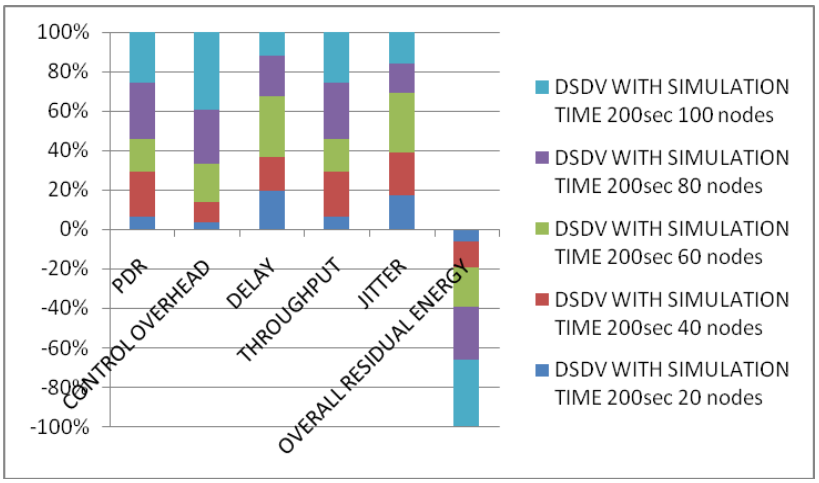

FIG 6:GRAPH FOR ALL QOS METRICS COMPARISION OF DSDV

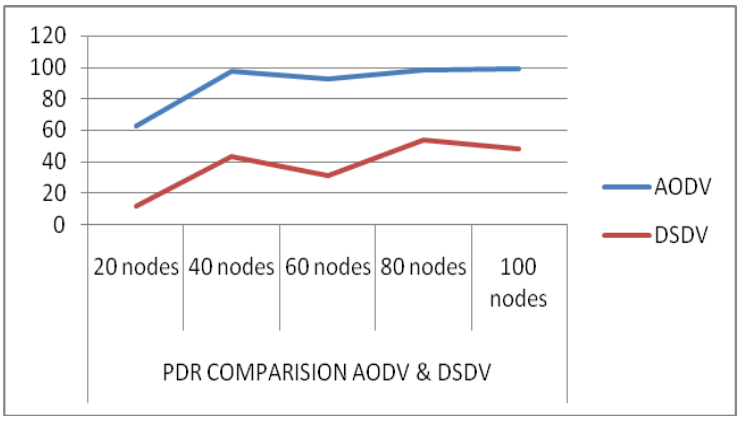

fig 7: packet delivery ratio :AODV &DSDV

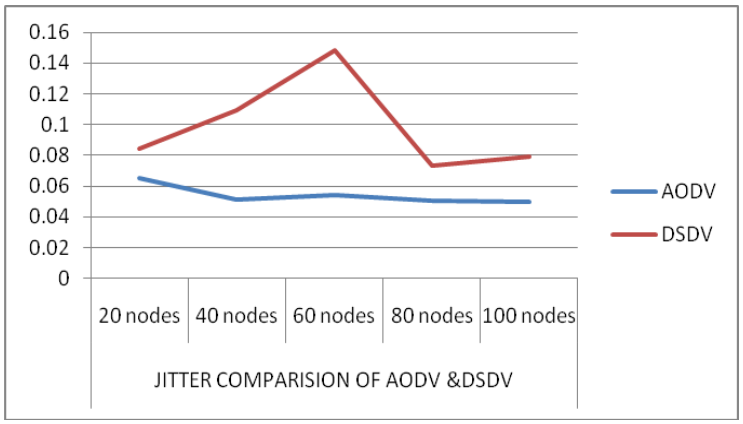

fig 8: Jitter : AODV &DSDV

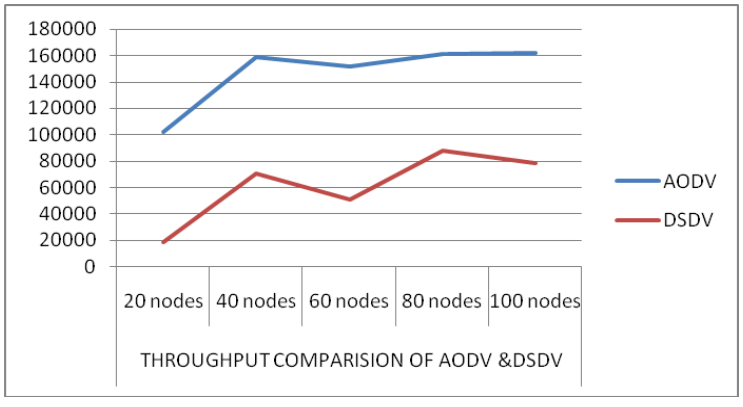

fig 9:Throughput :AODV &DSDV

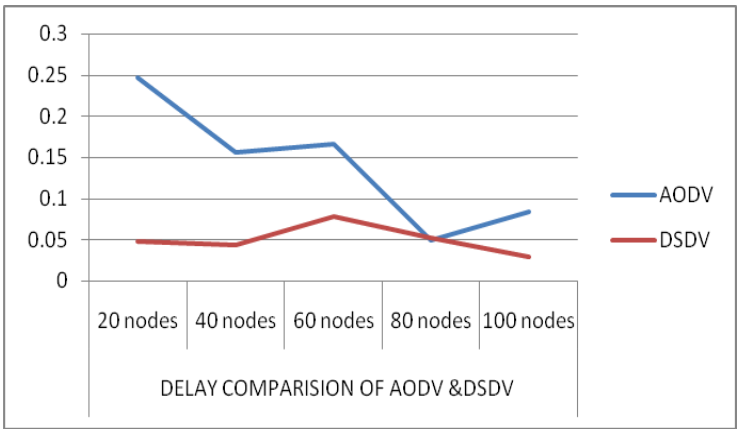

fig 10:Delay : AODV &DSDV

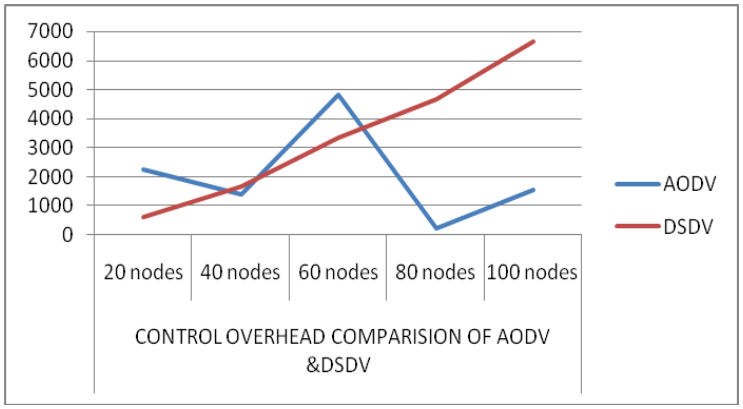

fig 11: Control overhed : AODV & DSDV

SIMULATION RESULTS:

SCENARIO 1: Table driven routing protocol(DSDV) lower pdr than reactive protocol(AODV).Among these Two protocols AODV is better pdr than DSDV.

SCENARIO 2: Table driven routing protocol(DSDV) HIGHER JITTER than reactive protocol(AODV).Among these Two protocols AODV is LOWER JITTER than DSDV.

SCENARIO 3: Table driven routing protocol(DSDV) lower THROUGHPUT than reactive protocol(AODV).Among these Two protocols AODV is better THROUGHPUT than DSDV.

SCENARIO 4: Table driven routing protocol(DSDV) lower DELAY than reactive protocol(AODV).Among these Two protocols AODV is better DELAY than DSDV.

SCENARIO 5: Table driven routing protocol(DSDV) HIGHER Control Overhead than reactive protocol(AODV).Among these Two protocols AODV is LOWER Control Overhead than DSDV.

CONCLUSION

Our simulation work illustrates the performance of two routing protocols AODV and DSDV. The paper presents a study of the performance of routing protocols, used in MANETs, in high mobility case under low, medium and high density scenario. We vary the number of nodes from 20 (low density) to 100 (high density) in a fixed topography of 1000*1000 meters. Moreover, since Random Waypoint(two ray ground) Mobility Model has been used in this study to generate node mobility. We find that the performance varies widely across different number of nodes and different types of speed in node mobility. AODV performance is the best considering its ability to maintain connection by periodic exchange of data's. As far as Throughput is concerned, AODV perform better than the DSDV even when the network has a large number of nodes. Overall, our simulation work shows that AODV performs better in a network with a larger number of nodes . Average End-to-End Delay is the least for DSDV and does not change if the no of nodes are increased. Thus, we find that AODV is a viable choice for MANETs. In this paper, we have done complete analysis of the two MANET's routing protocols. Our future plan is to evaluate security issues in AODV with different scenarios..

REFERENCES

[1] Ketan Sureshbhai Chavda (2014) A Performance analysis of AODV under Black hole attack in MANET, IJTCSE, Vol.1, No.2, pp. 82-87.

[2] Jaspal Kumar, M. Kulkarni, Daya Gupta (2013) Effect of Black hole Attack on MANET routing protocols, IJCNIS, Issue 5, pp. 64-72.

[3] Ranjeet Suryawanshi, Sunil Tamhankar,(2012) Performance Analysis and Minimization of Black hole attack in MANET, IJERA, Vol. 2, Issue-4,pp. 1430-1437.

[4] Punardeep Singh, Er. Harpal Kaur, Satinder Ahuja (2012) Brief Description of Routing Protocols in MANETs and Performance and Analysis (AODV, AOMDV, TORA), IJARCSSE, Vol. 2, Issue. 1.

[5] Ming-Yang Su, Kun-Lin Chiang and Wei-Cheng Liao(2010),Mitigation of Black Hole Nodes in Mobile Ad Hoc Networks,IEEE International Symposium on Parallel and Distributed Processing with Application.

[6] Anuj K. Gupta, Harsh Sadawarti (2009),Secure Routing Techniques for MANETs, International Journal of Computer Theory and Engineering (IJCTE), ISSN: 1793-8201**,** Article No. 74, Vol.1 No. 4, pp. – 456-460.

[7] R. H Rashid Khokhar , Md. A. Nagdi(2009), A Review of Current Routing Attacks in Mobile Ad Hoc Networks, International Journal of Computer Science and Security, pages 18-29.

[8] K. Sanzgiri, D. LaFlamme, B. Dahill, B. N. Levine, C. Shields, and E. M. B. Royer,(2005) Authenticated routing for ad hoc networks, IEEE Journal on Selected Areas in Communications, vol. 23, no. 3, pp. 598-610.

[9] M. A. Shurman, S. M. Yoo, and S. Park (2004), Black hole attack in wireless ad hoc networks. proceedings of the ACM 42nd Southeast Conference (ACMSE'04), pp 96-97.

[10] C. E. Perkins, E. Beliding Royer, S. Das (2004) Ad hoc On-demand Distance Vector (AODV) routing, IETF Internet Draft, MANET working group.

[11] B. Dahill, B. N. Levine, E. Royer, and C. Shields,(2002),A secure routing protocol for ad hoc networks,‖ in Proceedings of the International Conference on Network Protocols (ICNP), pp. 78-87.

[12] Y. Hu, A. Perrig and D. Johnson, Ariadne(2002), A Secure On-demand Routing Protocol for Ad Hoc Networks, in Proceedings of ACM MOBICOM'02.

[13] H. Deng, W. Li, and D. P. Agarwal (2002) Routing security in ad hoc networks, IEEE Communications Magazine, Vol. 40, No. 10, pp. 70-75.

[14] Nital Mistry, Devesh C Jinwala, Mukesh Zaveri (2000) Improving AODV Protocol against Black hole Attacks,Proceedings of the international multi conference of engineer and computer science vol. 2.

[15] C. E. Perkins and E. M. Royer (1999)Ad Hoc On-Demand Distance Vector Routing Proc. 2nd IEEE Workshop. Mobile Computing System and Apps. New Orleans, LA, pp. 90–100. ns-2, Network simulator, http:// www.isi.edu/ nsnam/ns

ABOUT AUTHOR

Mattareddy S received Diploma in Computer Engineering from Government Polytechnic, Hyderabad ,in 2009. Bachelor Degree in Electronics and Computer Engineering from KLCE , Guntur , in 2012 , and now pursuing M.Tech degree in Information Technology from University Campus , JNTU KAKINADA ,Andhra Pradesh . His research interests include network security , Data mining and MANETs

Kanthi Rekha M received B.Tech Degree in Computer Science and Engineering GMRIT, Rajam under JNTUK university in 2011 and now pursuing M.Tech degree in computer science from University Campus , JNTU KAKINADA ,Andhra Pradesh . Her research interests include network security , Data mining and MANETs.

B.A.S Roopa Devi ,currently working as a associate prof. in Pragathi Engineering College ,East Godawari, A.P. She has completed her B.Tech in Computer Science & Engineering, J.N.T University Hyderabad, A.P. India in the year 2004, M.Tech in Software Engineering, J.N.T University Hyderabad, A.P. India in the year 2006, and her Ph.D in Computer Science and Engineering, from J.N.T. University Kakinada.

