Efficient QoS Computation using Adaptive Hybrid Approaches with Clustering in Manet

Kishore Kumar .P[1], Reena Raj[2]
[1, 2] Department of Electronics and Communication Engineering,
[1, 2] PSN College of Engineering and Technology, Tirunelveli.

Abstract- *In Wireless Networks Life time enhancement is challenging one based on sink and other nodes. Recent advances in micro manufacturing technology have enabled the development of low-cost, low-power, multifunctional sensor nodes for wireless communication. Diverse sensing applications have also become a reality as a result. These include environmental monitoring, intrusion detection, battlefield surveillance, and so on. We propose a novel method (Adaptive Hybrid routing Schemes) for improving the life time of network based on routing energy with respect to sink and clustering overhead. Here number of nodes are created and form a number cluster. The purpose of cluster is to reduce the routing distance and improve the packet transition energy. In static Cluster Header (CH), CH's are collected data from their respective Cluster Members. Here CH having a most energy level. After that the packets are transmitted to sink node with help of intermediate CH to balance the energy level. Where sink also relocated based on CH position. CH selections also consider the position of node with respect to sink node position. IN dynamic, All the energy is computed, and then finally the CH is selected from the highest energy level in the networks node. Here we use AODV Protocol for routing implementation. Using the above methodology, we can reduce the routing energy of the node is reduced due to sink relocation based on CH and position.*

Keywords- MANET, AODV, DSDV, Reactive, Proactive.

I. INTRODUCTION

MANET consists of dynamically establishing mobile nodes having short-lived networks in the absence of fixed infrastructure. Each mobile node is equipped with wireless transmitter and a receiver with an appropriate antenna. These mobile nodes are connected to other nodes by wireless links and they act as routers for all other mobile nodes in network. Nodes in mobile ad hoc networks are free to move in the network and they can organize themselves in an arbitrary manner. These features make MANETs very practical and its deployment is easy in places where existing infrastructure is not capable enough to allow communication, for instance, in disaster zones, or infeasible to deploy locations. MANETs are the short term temporary spontaneously wireless networks of mobile nodes communicating with each other without intervention of any fixed infrastructure or central control. It is an autonomous system of mobile nodes, mobile terminals, or mobile stations serving as routers interconnected by wireless links. The nodes move or adjust their transmission and reception parameters as MANET topology may change from time to time.

A WSN consists of small-sized sensor devices, which are equipped with limited battery power and are capable of wireless communications. When a WSN is deployed in a sensing field, these sensor nodes will be responsible for sensing abnormal events (e.g., a fire in a forest) or for collecting the sensed data (temperature or humidity) of the environment. In the case of a sensor node detecting an abnormal event or being set to periodically report the sensed data, it will send the message hop-by-hop to a special node, called The sink node will then inform the supervisor through the Internet. As shown in Fig. 1, sensor node e detects an abnormal event and then it will send a warning message to the sink to notify the supervisor via a predetermined routing path, say Pea = e − d − c − b − a. Note that the routing path may be static or dynamic, depending on the given routing algorithm The applications of WSNs are broad, such as weather monitoring, battlefield surveillance, inventory and manufacturing processes, etc. In general, due to the sensory environments being harsh in most cases, the sensors in a WSN are not able to be recharged or replaced when their batteries drain out of power. The battery drained out nodes may cause several problems such as, incurring coverage hole and communication hole problems.

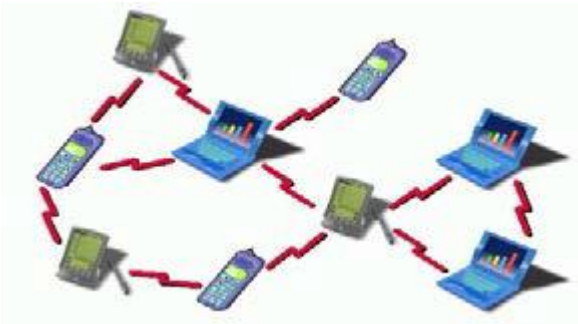

Figure 1. Mobile ad-hoc network

An ad-hoc routing protocol controls the routing of packet in MANET. In MANET, initially nodes are not aware of topology of network, they need to discover that. An ad-hoc routing protocol can be classified in reactive (on-demand), proactive (table-driven) protocol, hybrid protocol. Proactive (table-driven) Routing Protocol: The proactive routing is table-driven routing protocol. In this routing protocol, routing information is broadcasted by mobile nodes to the neighbors. Each node needs to keep their routing table which contains the information of neighborhood nodes, reachable nodes and the number of hops. In other words, all of the nodes have to find their nodes in the neighborhood as there is change in network topology. Therefore, the disadvantage of this protocol is when size of network increases, then overhead increases. The most familiar proactive type is destination sequenced distance vector (DSDV) routing protocol. Destination-Sequenced Distance-Vector (DSDV) Protocol: Table-driven DSDV protocol which is a modification in the Distributed Bellman-Ford (DBF) Algorithm which was used successfully in many of the dynamic packet switched networks. In case of DSDV, every node in the mobile network is required to send a sequence number, neighboring nodes.

Reactive (on-demand) routing protocol: This type of protocol finds routes by using the route request packet. It is a bandwidth efficient on-demand routing protocol for Mobile Ad-Hoc Networks. The protocol deals with two main functions of Route Discovery and Route Maintenance. The discovery of new route is decided by Route Discovery function and the detection of link breaks and repair of an existing route is decided by Route Maintenance function. Reactive or on-demand routing protocols route is discovered when required. Distribution of information is not required in reactive protocols. One of the reactive protocols is AODV. These protocols do not maintain permanent route table. Instead, routes are built by the source on demand. Ad Hoc On-demand Distance Vector Routing (AODV) protocol: In AODV, route establishment takes place only when there is a demand for new route. AODV is capable of unicast, broadcast and multicast routing. AODV is able to react quickly to the changes in the network topology and it updates only the hosts that may be affected by the changes in the network by using the RREQ message. The RREQ and RREP messages are responsible for the route discovery.

A Black Hole Attack is a malicious node waits for neighboring nodes to send RREQ messages. When it receives, it replies to them blindly RREQ as if it is the shortest route to the destination. When the data is actually start transferring it absorbs all the packets actually send to the destination. Black Holes are difficult to find if they start using sequence number comparable to the current sequence number of networks.

II. RELATED WORK

A. Security Aware Ad hoc Routing (SAR) SAR protocol integrates the trust level of a node and the security attributes of a route to provide the integrated security metric for the requested route. A Quality of Protection (QoP) vector used is a combination of security level and available cryptographic techniques. It uses the timestamps and sequence numbers to stop the replay attacks. Interception and subversion threats can be prevented by trust level key authentication. Attacks like modification and fabrication can be stopped by verifying the digital signatures of the transmitted packet. The main drawbacks of using SAR are that it required excessive encrypting and decrypting at each hop during the path discovery. The discovered route may not be the shortest route in the terms of hop-count, but it is secure [2] and [7].

B. Trusted Ad-hoc On-demand distance vector Routing (TAODV) TAODV is secure routing protocol which uses cryptography technologies recommended to take effect before nodes in the establish trust relationships among one another. The main salient feature of TAODV is that using trust relationships among nodes, there is no need for a node to request and verify certificates all the time. TAODV (Trusted AODV) has several salient features: (1) Nodes perform trusted routing behaviors mainly according to the trust relationships among them; (2) A node that performs malicious behaviors will eventually be detected and denied to the whole network. (3) The performance of the System is improved by avoiding requesting and verifying certificates at every routing step. That protocol greatly reduces the computation overheads. Assume that the keys and certificates needed by these cryptographic technologies have been obtained through some key management procedures before the node performs routing behaviors. Some extra new fields are added into a node's routing table to store its opinion about other nodes' trustworthiness and to record the positive and negative evidences when it performs routing with others. The main advantages of embedding trust model into the routing layer of MANET, save the consuming time without the trouble of maintaining expire time, valid state, etc. which is important in the situation of high node mobility and invalidity. Trusted AODV are mainly three modules in the whole TAODV system: basic AODV routing protocol, trust model, and trusted AODV routing protocol. Based on trust model, the TAODV routing protocol contains such procedures as trust recommendation, trust combination, trust judging,

cryptographic routing behaviors, trusted routing behaviors, and trust updating [1] and [6] and [9].

C. ARAN (Authenticated Routing for Ad-hoc Networks) ARAN provides authentication, message integrity and non-repudiation in ad-hoc networks by using a preliminary certification process which is followed by a route instantiation process that ensures end-to-end security services. But it needs the use of trusted certification server. The main disadvantage with the protocol is every node that forwards a route discovery or a route reply message must also sign it, which is very power consuming and causes the size of the routing messages to increase at each hop. It is clear from the above mentioned security analysis of the ARAN protocol that ARAN is a secure MANET routing protocol providing authentication, message integrity, confidentiality and non-repudiation by using certificates infrastructure. As a consequence, ARAN is capable of defending itself against spoofing, fabrication, modification, DoS and disclosure attacks. However, erratic behavior can come from a malicious node, which will be defended against successfully by existing ARAN protocol, and can also come from an authenticated node. The currently existing ARAN secure routing protocol does not account for attacks that are conducted by authenticated selfish nodes as these nodes trust each other to cooperate in providing network functionalities. This results in that ARAN fails to detect and defend against an authenticated selfish node participating in the mobile ad hoc network. Thus, if an authenticated selfish node does not forward or intentionally drop control or data packets, the current specification of ARAN routing protocol cannot detect or defend against such authenticated selfish nodes. This weakness in ARAN specification will result in the disturbance of the ad hoc network and the waste of the network bandwidth [8] and [10].

III. THE PROPOSED METHOD

The module in the proposed method is mentioned below.

- Network creation
- Configurations
- AODV Routing metrics implementation
- Hybrid approach implementation with static and dynamic CH selection

A. Network creation Module

In this module, we create number of nodes, where we differentiate with cluster member, Cluster Head node and sink etc., Here we predefined the routing protocol, link way, link layer, number of nodes and area of window size (ns2) etc., We defined the trace file based on that configuration module

B. Configuration Module

In this module, we configure the node characteristics like packet size, energy, power, distance than another node etc., Configuration is basic procedure of any network module. In our work, we create four clusters with cluster head(both static and dynamic) & sink with respect to intermediate node (ICH)

C. AODV Routing metrics implementation

i) Working with single black hole attack

Step 1: Suppose S is a source and D is destination and S wants to send data to D.

Step 2: When S wants to send data to destination then it will send request to destination. If that node is a valid destination then it will send reply to the source.

Step 3: RTRPLYN (Route Reply Node) is the intermediate node between source and destination. Then it will send verify packet to destination node.

Step 4: When S receives RTRPLY (Route Reply), then it will send a CHECKVRF (Check Verification) packet to D via a path suggested by RTRPLYN.

Step 5: When D gets VERIFY packet from intermediate node, it stores its contents in a table to prepare Final reply.

Step 7: When D receives CHECKVRF packet from S, it checks in table if it got any VERIFY packet with matching source ID.

Step 8: If it matches, it sends a FINALREPLY packet.

Step 9: In case of black hole, FINALREPLY packet will not reached the source because VERIFY and CHECKVRF packets are not forwarded to the destination node.

ii) Working with collaborative black hole attack

In case of collaborative black hole, suppose node 5 and 6 are black holes working in collaboration that is node 5 will send data packets received by it to the next node that is node 6 and node 6 will drop all these data packets. In this case, same procedure is used as it is dropping all packets and not allowing to pass to destination then there is no VERIFY and CHECKVRF is received by destination node and hence FINALREPLY is not generated. Hence those nodes will mark as black holes working in collaboration and routing table is updated. Hence packets are transmitted to destination via intermediate nodes except node 5 and node 6.

D. Hybrid approach implementation with static and dynamic CH selection

CH select with static and dynamic way. In this module, the packets are received by CH in every cluster from cluster members. After that, CH is transmitted the packets to sink through intermediate CH(nodes) with respect to distance and routing time etc., Here communication and other characteristics performed by hybrid approaches protocols.

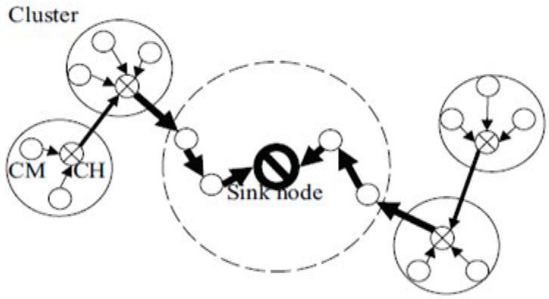

Figure 2. Proposed System Diagram

IV. PERFORMANCE ANALYSIS

A. Simulation parameters for AODV, DSDV Routing Protocol

This analysis includes the simulation of 10, 30, 40, 50, 60, 70, 80, 90, 100 nodes. Total simulation time is 150 sec. i.e. time between the starting of simulation and ending of the simulation. Traffic type is Constant Bit Rate.

B. Performance Metrics

Packet Delivery Ratio (PDR) – It is a ratio of number of packets received by destination to number of packet sent by source.

End to end Delay- End to end delay (seconds) is the time it takes a data packet to reach the destination.

Throughput - The rate of successfully transmitted data per second in the network during the simulation.

Routing Overhead - Routing overhead is the total number of routing packets divided by total number of delivered data packets. RH=Total no of routing packets/Total no of delivered data packets.

V. COMPARISONS OF ROUTING PROTOCOLS

A. Comparison of AODV and DSDV routing

Protocol Packet delivery ratio is the ratio of number of packets sent and received. As in case of AODV, destination receives almost all packets send by source. The packet delivery ratio of AODV is between 0.980403-1.00. The packet delivery ratio of DSDV is between 0.79651-0.917584. Hence AODV is having better packet delivery ratio as compare to DSDV.As throughput depends on time and as DSDV is the table driven protocol, it requires extra time to set up routing tables before delivering packets to the next node. Its throughput becomes less than that of AODV. The throughput of AODV is between 0.006536-0.006668 and the throughput of DSDV is between 0.005311-0.006118. Hence, throughput of AODV is better than DSDV

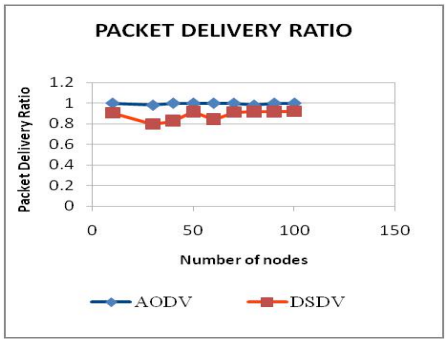

Figure 3. a) Packet delivery ratio

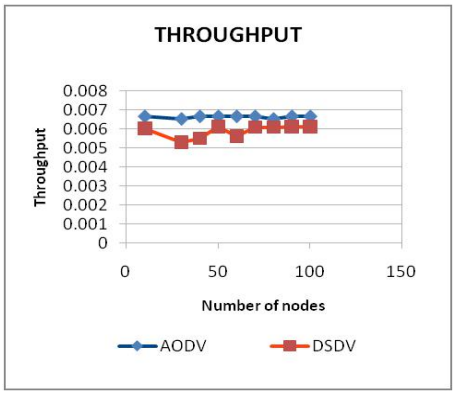

Figure 4. b) Throughput of AODV and DSDV

As the routing tables are stored in the table-driven protocols, DSDV could avoid the long set up time caused by changes of the network topology. End to end delay of DSDV is less than AODV. End to end delay of AODV is between 0.011701-0.044079 and end to end delay of DSDV is between 0.01068-0.012614.DSDV keep routing tables to deliver packets, and hence it sets up the new routes when there is a change in the network topology. On the other hand, AODV is the on-demand protocols, and it has to initiate the routing discovery mechanism whenever a new route is to be established. AODV delivers required packets on demand of communication between the nodes. And hence it reduces the network pressure caused by the heavy overload. DSDV is more likely to cause the heavy overload and congestion problems. Routing Overhead of AODV is between 0.000536 - 0.007216 and that of is DSDV is between 0.004697-0.068614 as it increases with number of nodes.

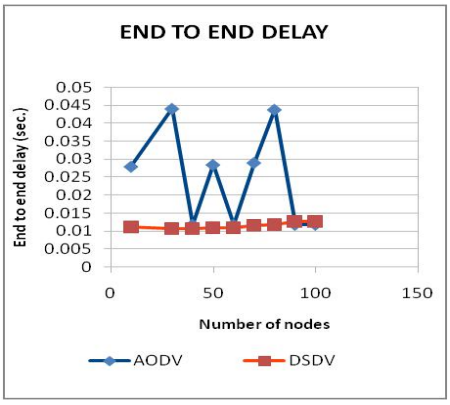

Figure 5. c) End to end delay

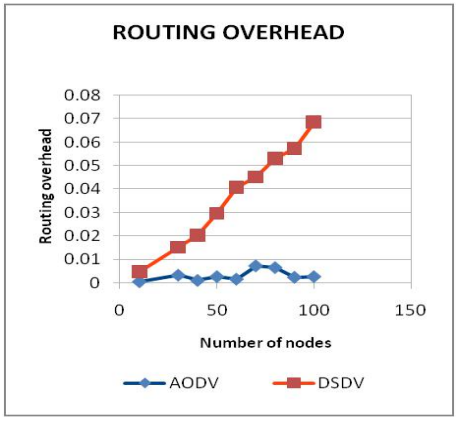

Figure 6. d) Routing Overhead of AODV and DSDV

B. Comparison of AODV and Modifications in AODV

Modified AODV helps to improve the parameters in case of black hole attack. As during black hole, the performance of AODV degraded which gives zero throughput and packet delivery ratio. But modified AODV gives the better results which are close to AODV without black hole attack.

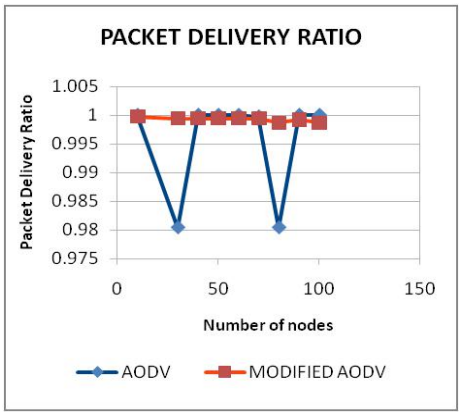

Figure 7. a) Packet delivery ratio

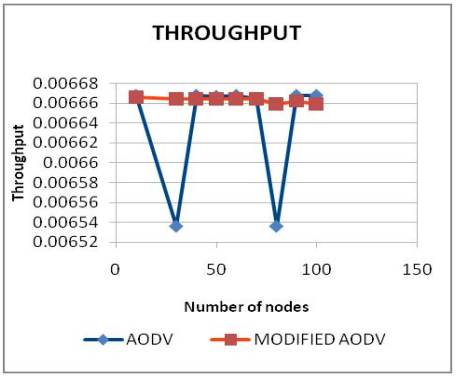

Figure 8. b) Throughput of AODV and Modifications in AODV

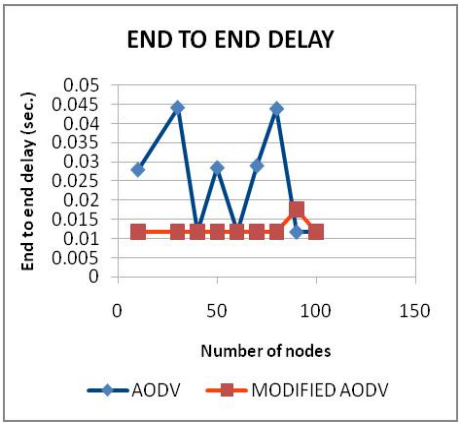

Figure 9. c) End to end delay

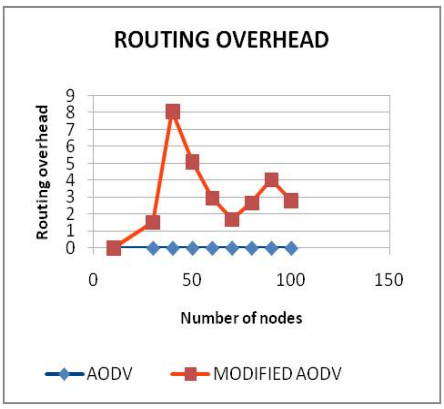

Figure 10. d) Routing Overhead of AODV and Modifications in AODV

C. Comparison of AODV and Modifications in AODV with single and collaborative black hole attack

Below figures show the comparison of modified AODV with single and collaborative black hole attack. As in the modified AODV there are packets are added in the routing as VERIFY, RTRPLY, CHECKVRF, FINALREPLY along with RREP and RREQ, therefore routing overhead is more as compare to AODV.

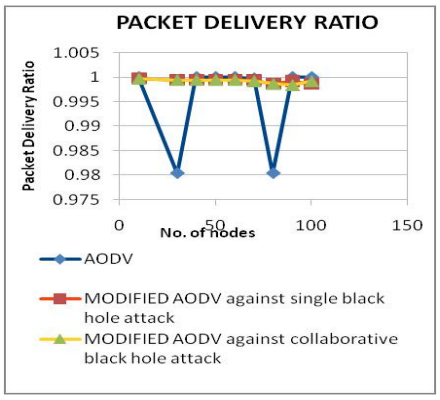

Figure 11. a) Packet delivery ratio

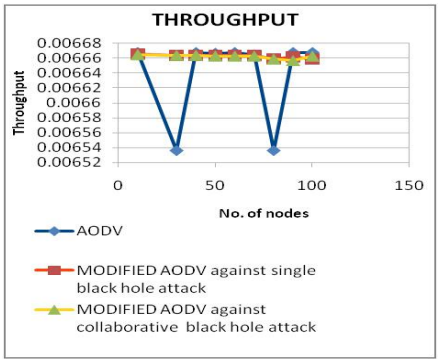

Figure 12. b) Throughput of AODV, Modifications in AODV with single and collaborative black hole attack

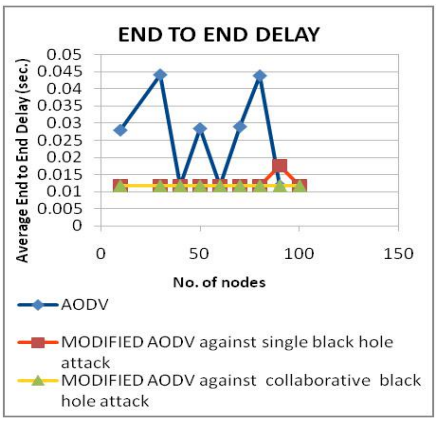

Figure 13. c) End to end delay

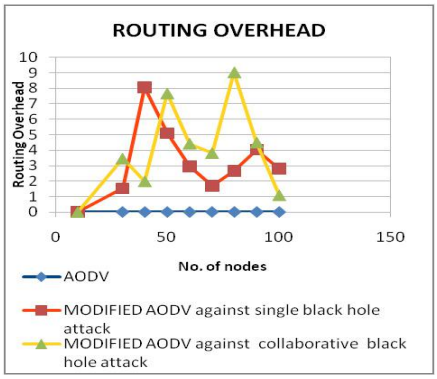

Figure 14. d) Routing Overhead of AODV, Modifications in AODV with single and collaborative black hole attack

V. CONCLUSION

MANET is a collection of mobile nodes, dynamically establishing short-lived networks in the absence of fixed infrastructure. This paper compares of AODV and DSDV routing protocols which are proposed for ad-hoc mobile networks. In DSDV routing protocol, mobile nodes periodically broadcast their routing information to the neighbors. Each node requires to maintain their routing table. AODV protocol finds routes by using the route request packet and route is discovered when needed. The comparison of these protocols is done with the parameters packet delivery ratio, throughput, end to end delay, routing overhead. AODV performs better than DSDV in packet delivery ratio, throughput and routing overhead. The delay of AODV is more than DSDV. The performance of AODV gets affected by black hole attack. It reduces the packet delivery ratio and throughput to zero and hence modifications are done in AODV which gives better results even in the presence of black hole attack. Packet delivery ratio and throughput in case of AODV and AODV after modifications are same. But for modifications, new packets are added in routing and hence routing overhead is more as compare to AODV without modification.

REFERENCES

[1] Priya Dharshini.R, Prabhu.V,Rajes Singh .S, "Research on Implementation and Comparison of Routing Protocols in MANET Using NS2", in International Journal of Science and Research, Volume 3, Issue 4, April 2014, Publication Year: 2014

[2] Kanchan Ubnare , Prof. Navneet Manghi , Prof. Vimal Shukla, "A Comparative Study of Routing Protocols in Mobile Ad-hoc Networks" ,in International Journal of Emerging Technology and Advanced Engineering; Volume 4, Issue 3, March 2014 Publication Year: 2014

[3] M. Swathi, B. Pravallika, N. V. Muralidhar, "Implementing And Comparison of MANET Routing Protocols Using NS2",in International Journal of Emerging Technology and Advanced Engineering; Volume 4, Issue 2, February 2014; Publication Year: 2014

[4] Sunil Kumar Yadav, Shiv Om Tiwari, "An Efficient Approach for Prevention of Cooperative Black Hole Attack on DSR Protocol", in IOSR Journal of Computer Engineering,8727 Volume 16, Issue 1,Jan 2014. Publication Year:2014

[5] Pankaj Rohal, Ruchika Dahiya, Prashant Dahiya, "Study and Analysis of Throughput, Delay and Packet Delivery Ratio in MANET for Topology Based Routing Protocols (AODV, DSR and DSDV)", in International Journal For Advance Research in Engineering and Technology, Vol. 1, Issue II, Mar. 2013, Publication Year:2013

[6] Harjeet Kaur, Varsha Sahni, Dr. Manju Bala, "A Survey of Reactive, Proactive and Hybrid Routing Protocols in MANET: A Review",in International Journal of Computer Science and Information Technologies, Vol. 4 (3) , 2013, 498-500; .Publication Year: 2013

[7] Deepak Kumar Patel, Rakesh Kumar, A.K.Daniel, "Performance Analysis and Behavioural Study of Proactive and Reactive routing protocols in MANET ",in International Journal of Advanced Research in Computer Science and Software Engineering, vol 2, April 2013; Publication Year: 2013.

[8] V.RAJESHKUMAR, P.SIVAKUMAR, "Comparative Study of AODV, DSDV and DSR Routing Protocols in MANET Using Network Simulator-2", International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 12, December 2013; Publication Year: 2013

[9] Vipin Khandelwal, Dinesh Goyal, "BlackHole Attack and Detection Method for AODV Routing Protocol in MANETs" in International Journal of Advanced Research in Computer Engineering & Technology, Volume 2, Issue 4, April 2013. Publication Year: 2013

[10] Ms.Nidhi Sharma Mr.Alok Sharma, "The Black-hole node attack in MANET", in Second International Conference on Advanced Computing & Communication Technologies, 2012, Publication Year:2012

[11] G. RAJKUMAR, DR. K. DURAISAMY, "A Review of Ad Hoc On-Demand Distance Vector Routing Protocol for Mobile Ad Hoc Networks", in Journal of Theoretical and Applied Information Technology, Vol. 36 No.1, 15th February 2012, Publication Year: 2012

[12] Meenakshi, Vinod Kumar Mishra, Kuber Singh, "Simulation & Performance Analysis of Proactive, Reactive & Hybrid Routing Protocols in MANET", in International Journal of Advanced Research in Computer Science and Software Engineering, vol2, July 2012; Publication Year: 2012

[13] G. Jose Moses, D. Sunil Kumar Prof.P.Suresh Varma N.Supriya, "A Simulation Based Study of AODV, DSR, DSDV Routing Protocols in MANET Using NS-2",in International Journal of Advanced Research in Computer Science and Software Engineering Volume 2, Issue 3, March 2012; Publication Year: 2012

[14] Fan-Hsun Tseng, Li-Der Chou, Han-Chicj Chao, "A survey of black hole attacks in wireless mobile ad hoc networks",Human-centric Computing and Information Sciences, 2011; Publication Year: 2011

[15] Anil Kumar Sharma and Neha Bhatia, "Behavioural Study of MANET Routing Protocols by using NS-2",in IJCEM International Journal of Computational Engineering & Management, Vol. 12, April 2011; Publication Year: 2011

[16] Qian Feng, Zhongmin Cai, Jin Yang, Xunchao Hu, "A Performance Comparison of the Ad Hoc Network Protocols",in Second International Workshop on Computer Science and Engineering,2009 IEEE, Publication Year: 2009.