MHACK Based Misbehavior Node Detection Scheme for DSR

Garima Mishra
M Tech Scholar, Department of CSE
TIT, Bhopal. India
E-mail- mishragarima25@gmail.com

Arjun Rajput
AP, Department of CSE
TIT, Bhopal. India
E-mail- rajarjun07@gmail.com

ABSTRACT
A Mobile Ad hoc NETwork (MANET) is a set of mobile devices (nodes), which over a shared wireless medium communicate with each other without the presence of a predefined infrastructure or a central authority. The member nodes are themselves responsible for the creation, operation and maintenance of the network. The nature of the networks places two fundamental requirements on the routing protocols. First, it has to be distributed. Secondly, since the topology changes are frequent, it should compute multiple, loop-free routes while keeping the communication overheads to a minimum. Due to the dynamic change in topology finding route is very difficult. Some nodes misbehave as they participate in route establishment phase but refuse to forward the data packets to conserve their own energy. However, due to the absence of central Infrastructure the devices in the ad-hoc network can move randomly gives rise to various kind of problems, such as routing and security. In this chapter, two approaches are presented to improve the performance of original DSR protocol. The first approach Energy efficient-DSR decreases the energy consumption of the network. The second approach Secure-DSR increases the reliability of the routes between source and destination. And then the performance evaluation parameters for energy efficiency and security of mobile ad-hoc network are presented. proposed schemes are provably secure and highly efficient.

Keyword:- MANET, QOS, AODV, DSDV, DSR.

INTRODUCTION
Ad hoc wireless networks simply are self-creating, self-organizing, and self-administering collection of wireless mobile nodes. They come into being solely by interactions among their constituent wireless mobile nodes, and it is only such interactions that are used to provide the necessary control and administration functions supporting such networks[1][2].

Routing protocols are rules that define the communication mechanism in a network. Due to dynamism of topology, lack of central infrastructure, energy and bandwidth constraints, the routing protocols that apply to conventional wired or wireless networks cannot be directly applied to MANETS. Listed below are certain characteristics of ideal routing protocols for ad hoc networks [3].It must be fully distributed. It must be adaptive to dynamism of topology. Connection set up time should be minimal. State maintenance must be localized. Changes in remote part of the network not affecting a particular node should not cause updates in the topology information stored in that node. It must be loop free. Stale routs should be obliterated. It should be able to minimize the packet collisions. The convergence to optimal route should be quick. The resource constraints like energy, memory, computation, bandwidth etc should be optimally considered. It should be able to provide a certain level of Quality of Service (QOS).

Routing protocols have been in the centre of research in the recent past and based on above characteristics a number of solutions have been reached to. Based on different criteria the MANET routing protocols can be classified into several types. The classification is not mutually exclusive and some protocols are represented in more than one class. Classification based on Routing Information Update Mechanism:

Proactive or Table Driven Routing Protocols: In these protocols every node in the network maintains the network topology information in the form of routing tables. This is done by flooding and periodically exchanging the routing information in the network. On requirement of a path to a destination, the node looks into the routing table in store to find an optimum path. Routing overhead is high but latency is low in these protocols. DSDV [4], WRP [5], CGSR [6], STAR [7], OLSR [8], FSR [9], HSR [10], GSR [11] are routing protocols that fall under this category.

Reactive or On Demand Routing Protocols: No routing information is stored on the nodes in these types of protocols. As and when a node requires a path to a destination node, it initiates a path finding process. The routing overhead is low but latency is high in these types of protocols. DSR [12], AODV [13], ABR [14], SSA [15], FORP [16], PLBR [17] are routing protocols that fall under this category.

Hybrid Routing Protocols: Protocols in this category try to fuse the best features of the reactive and proactive type of protocols. Nodes in a particular zone of a node are routed by

table driven process and outside this zone are routed by reactive process. CEDAR [18], ZRP [19], ZHLS [20] are some of the protocols under this category. All of the routing protocols in MANETs depend on active cooperation of nodes to provide routing between the nodes and to establish and operate the network. The basic assumption in such a setup is that all nodes are well behaving and trustworthy. Albeit in an event where one or more of the nodes turn malicious, security attacks can be launched which may disrupt routing operations or create a DOS (Denial of Service)[20] condition in the network.

Due to dynamic, distributed infrastructure-less nature of MANETs, and lack of centralized authority, the ad hoc networks are vulnerable to various kinds of attacks. The challenges to be faced by MANETs are over and above to those to be faced by the traditional wireless networks. The accessibility of the wireless channel to both the genuine user and attacker make the MANET susceptible to both passive eavesdroppers as well as active malicious attackers. The limited power backup and limited computational capability of the individual nodes hinders the implementation of complex security algorithms and key exchange mechanisms. There is always a possibility of a genuine trusted node to be compromised by the attackers and subsequently used to launch attacks on the network. Node mobility makes the network topology dynamic forcing frequent networking reconfiguration which creates more chances for attacks.

The attacks on MANETs can be categorized as active or passive. In passive attacks the attacker does not send any message, but just listens to the channel. Passive attacks are non disruptive but are information seeking, which may be critical in the operation of a protocol. Active attacks may either be directed to disrupt the normal operation of a specific node or target the operation of the whole network. A passive attacker listens to the channel and packets containing secret information (e.g., IP addresses, location of nodes, etc.) may be stolen, which violates confidentiality paradigm. In a wireless environment it is normally impossible to detect this attack, as it does not produce any new traffic in the network. The action of an active attacker includes; injecting packets to invalid destinations into the network, deleting packets, modifying the contents of packets, and impersonating other nodes which violates availability, integrity, authentication, and non-repudiation paradigm. Contrary to the passive attacks, active attacks can be detected and eventually avoided by the legitimate nodes that participate in an ad hoc network [21].

II PROBLEM STATEMENT

Adhoc wireless network maximizes network throughput by using all available nodes for routing and forwarding. Therefore, the more nodes that participate in packet routing, the greater the aggregate bandwidth, the shorter the possible routing paths, and the smaller the possibility of a network partition. However, a node may misbehave by agreeing to forward packets and then failing to do so, because it is overloaded, selfish, malicious, or broken. An overloaded node lack the CPU cycles, buffer space or available network bandwidth to forward packets. A selfish node is unwilling to spend battery life, CPU cycles, or available network bandwidth to forward packets not of direct interest to it, even though it expects others to forward packets on its behalf. A malicious node launches a denial of service attack by dropping packets. A broken node might have a software fault that prevents it from forwarding packets [2]. Misbehaving nodes can be a significant problem. There are three types of selfish nodes as follows:

Selfish Nodes Type 1 (SN1) - These nodes participate in route establishment but refuse to forward data packets (which are usually much larger than the routing control packets).

Selfish Nodes Type 2 (SN2- These nodes participate in neither the route establishment phase nor forward data packets. They only use their energy for transmissions of their own packets.

Selfish Nodes Type 3 (SN3) - These nodes behave (or misbehave) differently based on their energy levels. When the energy lies between full energy E and a threshold T1, the node behaves properly. For an energy level between T1 and another lower threshold T2, it behaves like a node of type SN1. Finally, for an energy level lower than T2, it behaves like a node of type SN2

III THE PROPOSED SCHEMES

Due to the dynamic change in topology finding route is very difficult. Some nodes misbehave as they participate in route establishment phase but refuse to forward the data packets to conserve their own energy. However, due to the absence of central Infrastructure the devices in the ad-hoc network can move randomly gives rise to various kind of problems, such as routing and security. In Mobile and Ad-hoc Network (MANET) resources are very limited. Battery power of the node (Energy of the node) is an important resource for the MANET. In this chapter, two approaches are presented to improve the performance of original DSR protocol. The first approach Energy efficient-DSR decreases the energy consumption of the network. The second approach Secure-DSR increases the reliability of the routes between source and destination. And then the performance evaluation parameters for energy efficiency and security of mobile ad-hoc network are presented.

IV ENERGY MODEL

In this model the main aim is to reduce the energy consumption in the route maintenance case. In original DSR when any route breaks a Route Error (RERR) message is generated from the node adjacent to the broken link to inform the source node. The source node reinitiates the route establishment procedure to provide the further communication. In the proposed work the route is created locally by using those neighboring nodes of the upstream nodes which have the highest energy. By this we can increase the life of the node.

Here node maintains some energy weights on the basis of their remaining energy. If any node has the energy more than 70% it means it has sufficient energy to take part in the routing process and it can take part for the longer time, then

the highest energy weight is assigned. If it has energy less than 30% then it cannot take part in the routing process for the longer time. So the routing process avoids these type of nodes and minimum energy weight 1 is assigned to such node 1 otherwise weight 2 will be given as shown in Fig 4.1. When any route breaks during the data transmission then the upstream node creates the route locally and sends the local route request message (LRREQ) to the entire neighboring nodes then all the neighboring nodes send the route reply message with its energy weights and the upstream node selects the highest energy weight among them. After the creation of new route on the basis of the remaining energy power in the node, some node become dead due to the less remaining energy power. In the energy implementation part the dynamic route change strategy in the network is applied and it tries to recover the route locally whenever route breakage occurs due to the less remaining energy in the node.

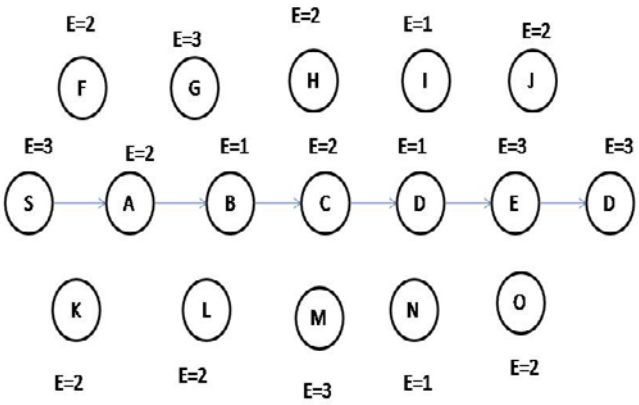

Figure 1: All the nodes with their energy weights.

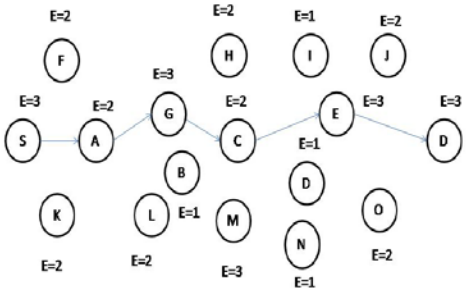

Figure 2. Selection of alternate local route on the basis of energy weights.

V SECURITY MODEL

In this model, detection of routing misbehavior due to selfish nodes is considered. A selfish node does not perform the packet forwarding function but operates in the Route Discovery and the Route Maintenance phases of the DSR protocol. Such type of nodes may also be included in the routes chosen to forward the data packets from the source. The misbehaving nodes, however, refuse to forward the data packets from the source, leads to the source being confused. This results in packet loss and the network fails to provide reliable communication for the source node.

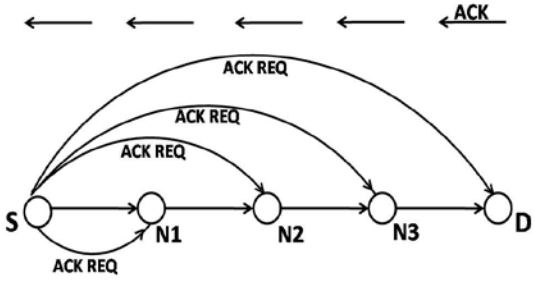

Figure 3: Working of multi hop acknowledgement scheme.

The multi hop acknowledgment scheme extends the 2ACK scheme in trying to isolate misbehaving nodes in MANET. The process starts when a source node has data packets to be sent to the destination, it initiates a Route Request packet. This RouteRequest is flooded throughout the network. The destination node, on receiving a RouteRequest packet responds by sending a RouteReply packet back to the source, which carries the route traversed by a RouteRequest packet received. Now consider a path of S→N1→N2→N3→D in which S is source node, D is destination node and N1, N2 and N3 are intermediate nodes between S and D of the active route. When node S wants to send data packet to node D, it forwards the data packet to node N1 which then forwards the data packet to node N2. The process remains continue till the data packet reaches to node D. Node S sends ACK Request to each node in the active route in the form of data packet. After receiving the data packet the node D sends an ACK packet to node S which is forwarded by the intermediate nodes, for the response of ACK Request data packet. The ACK would try to reach the source from the destination with the help of the path, which is found to be misbehaving. The data packet and the ACK packet keep track of the route they travel which is compared by the source node S. If the paths are same, source node concludes that there are no misbehaving nodes exist in the path. But if the paths vary, node in source to destination path from where path varies in destination to source path is detected as misbehaving node as it is supposed to drop data packet and is isolated.

VI SIMULATION AND RESULTS

The proposed algorithms for energy efficiency and security are applied on various parameters like packet delivery ratio, average end-to-end delay, throughput and energy consumption by varying number of nodes and pause time. Simulation parameters and results are shown in this section

Parameters	Values
Simulation Tool	NS-2.34
Transmission Range	250 M
Number of nodes	10, 20, 30, 40, 50

Number of communication pair	5, 10
Topology size	600*600m^2
Mobility model	Random Way-point
Mobile Speed	10m/s
Routing Policy	DSR
Traffic type	CBR
Packet Rate	20packets/sec
Packet size	512 bytes
Path loss model	Two-ray Ground
Mac Protocol	802.11 DCF
Interface queue type	CMUPriQueue
Pause Time	0,100, 200,300, 400
Simulation Time	120

Figure 4,5,6 and 7 show the simulation results when varying the number of nodes from 10, 20, 30, 40 and 50 while maintaining the packet delivery ratio, average end to end delay, throughput and energy consumption respectively. The energy efficiency model and security model is working simultaneously to make MANET secure and energy efficientThe Packet Delivery Ratio (PDR) in the proposed method has been compared between the original DSR and modified DSR (MDSR) and the plot of PDR against number of nodes is shown in the following Fig 6.1.

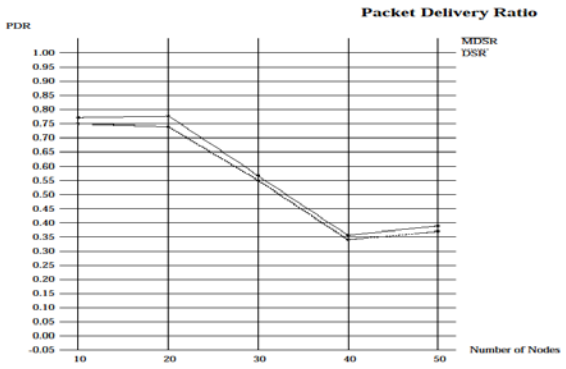

Figure 4: Packet delivery ratio comparison for varying number of nodes.

We can clearly see from the Figure 4 that the proposed method is producing higher PDR for MDSR in comparison to the original DSR. Therefore, the proposed method is more efficient and gives better results in terms of packet delivery. Similarly, the average end-to end delay in the proposed method has been compared between the original DSR and MDSR and the plot of average end-to-end delay against number of nodes is shown in Figure 5.

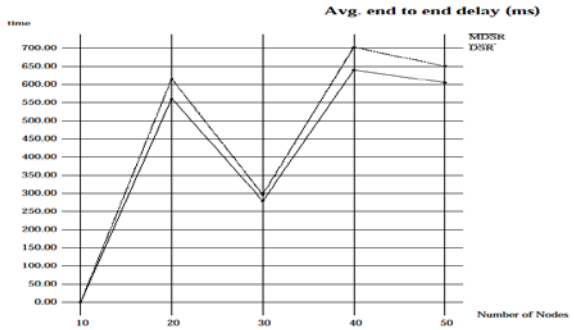

Figure 5: Average end-to-end delay comparison for varying number of nodes.

It is stated from the Figure 5 that average end to end delay minimizes in proposed algorithm in comparison to original DSR. MDSR has the shortest end-to-end delay than DSR. Hence, it consumes lesser time and is more reliable. The computation of throughput against various values of number of nodes is shown in the Figure 6 between DSR and MDSR.

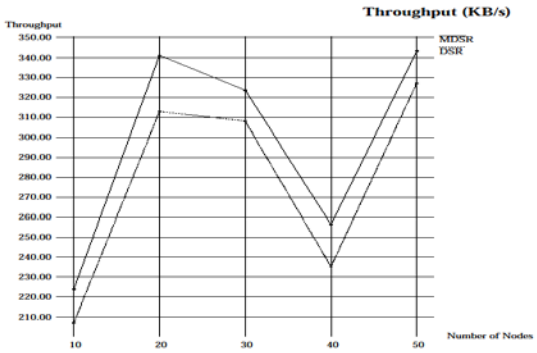

Figure 6: Throughput comparison for varying number of nodes.

It can be seen from the figure that the proposed method gives better throughput for MDSR as compared to DSR. As the number of nodes increases the value of throughput is high for MDSR than DSR. It shows the effectiveness of routing by using proposed method. Figure 7 shows the simulation results when varying the number of mobile nodes while maintaining the energy consumption.

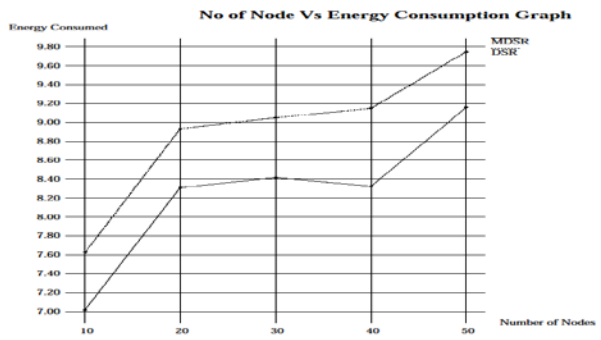

Figure 7: Comparison of the energy consumption for varying number of nodes.

The increase in number of nodes in the network increases the energy consumption. In this case the proposed algorithm again works better than the DSR protocol. It is shown in Fig 5.4 that MDSR consumes less energy than DSR thus making the network more efficient.

VII CONCLUSIONS

This chapter discusses the conclusions arrived from the research conducted. The implementation of the algorithms and the results of the various simulations are consolidated and presented. This Chapter also suggests some of the possible future enhancements and improvements that could be carried out. MANET is a collection of mobile nodes that communicate with each other by forming a multi-hop radio network and maintaining connectivity management without an existing network infrastructure. Such networks are expected to play increasingly important roles in various applications.

In the aforesaid study and evaluation of approach, we found our approach more effective and suited for congestion prone network to avoid the congestion and to control the delay and buffer overflow caused by the congestion and improve network performance as compare to the previous work. The work can be extended and enhanced by implementing it in other protocols, other topology, wireless sensor network and virtual sensor network in future work to show its better performance.

REFERENCES:-

[1] Aad I., Hubaux J.-P, "Denial of Service Resilience in Ad Hoc Networks",Proc. MobiCom, pp. 202-215, 2004.

[2] Baker M, Giuli T., Lai K. and Marti S, "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks", Proc. MobiCom, pp. 255-265.

[3] Balakrishnan K., Deng J., and Varshney P. K, "TWOACK: Preventing Selfishness in Mobile Ad Hoc Networks", Proc. IEEE Wireless Comm. and Networking Conf. (WCNC '05), pp.2137-2142 Mar. 2005.

[4] C.E.Perkins and P.Bhagwat, "Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) For Mobile Computers," Proceedings of ACM SIGCOMM 1994, pp. 233-244, August 1994.

[5] M.Gerla, X.Hong, L.Ma and G.Pei, Landmark Routing Protocol (LANMAR) for Large Scale Ad Hoc Networks, IETF Internet Draft, v.5, November 2002.

[6] C.C.Chiang, H.K.Wu, W.Liu and M.Gerla, "Routing in Clustered Multi Hop Mobile Wireless Networks with Fading Channel," Proceedings of IEEE SICON 1997, pp. 197-211, April1997.

[7]C.E.Perkins and E.M.Royer, "Ad Hoc On-Demand Distance Vector Routing," Proceedings of IEEE Workshop on Mobile Computing Systems and Applications1999, pp. 90-100, February 1999.

[8] D.B.Jhonson and D.A.Maltz, "Dynamic Source Routing in Ad Hoc Wireless Networks," Mobile Computing, Kluwer Academic Publishers, vol.353, pp. 153-181, 1996.

[9]V.D.Park and M.S.Corson, "A Highly Adaptive Distributed Routing Algorithm for Mobile Ad Hoc Networks," Proceedings of IEEE INFOCOM 1997, pp. 1405-1413, April 1997.

[10] I. Chakeres and C. Perkins, Dynamic MANET On-demand (DYMO) Routing Rrotocol, IETF Internet Draft, v.15, November 2008, (Work in Progress).

[11] P.Sinha, R.Sivakumar and V.Bharghavan, "CEDAR: A Core Extraction Distributed Ad Hoc Routing Algorithm," IEEE Journal on Selected Areas in Communications, vol.17, no.8, pp. 1454-1466, August 1999.

[12] Z.J.Haas, "The Routing Algorithm for the Reconfigurable Wireless Networks," Proceedings of ICUPC 1997, vol. 2,pp. 562-566, October 1997.

[13] M.Joa-Ng and I.T.Lu, "A Peer -to-Peer Zone-Based Two-Level Link State Routing for Mobile Ad Hoc Networks," IEEE Journal on Selected Areas in Communications, vol. 17, no. 8, pp. 1415-1425, August 1999.

[14] A.Shevtekar, K.Anantharam, and N.Ansari, "Low Rate TCP Denial-of-Service Attack Detection at Edge Routers," IEEE Commun. Lett., vol. 9, no. 4, pp. 363–65, April 2005.

[15] Hao Yang, Haiyun Luo, Fan Ye, Songwu Lu and Lixia Zhang, "Security in mobile ad hoc networks: Challenges and solutions," IEEE Wireless Communications, vol. 11, pp. 38-47, Feb., 2004.

[16] D. Wang, M. Hu, H. Zhi, "A Survey of Secure Routing in Ad Hoc Networks," IEEE Ninth International Conference on Web-Age Information Management, 2008, (WAIM '08), pp.482-486, July 2008.

[17] K.Sanzgiri, D.LaFlamme, B.Dahill, B.N.Levine, C.Shields, and E.M.Belding-Royer, "Authenticated Routing for Ad Hoc Networks," Proceedings of IEEE journal on selected areas in communications, vol. 23, no. 3, March 2005.

[18] Y.C.Hu, A.Perrig, and D.B.Johnson, "Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks," Proc. MobiCom'02, Atlanta, GA, pp. 12-13 September 2002.

[19] M.G.Zapata and N.Asokan, "Securing Ad-Hoc Routing Protocols," Proceedings of ACM Workshop on Wireless Security, pp. 1–10, September 2002.

[20] Y.C.Hu, D.B.Johnson and A.Perrig, "SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad hoc Networks," Proceedings of 4th IEEE Workshop on Mobile Computing Systems and Applications, Callicoon, NY, pp. 3-13. June 2002.

[21] K.Sanzgiri, B.Dahill, B.N.Levine, C.Shields and E.M. Royer, "A Secure Routing Protocol for Ad hoc Networks", Proceedings of 10th IEEE International Conference on Network Protocols (ICNP'02), IEEE Press, pp. 78-87, 2002,.