Detection of Gray Hole and Black Hole Attack using DSDV in Manets

Er. Sukhdeep Singh
Department of computer science engineering
S G G S W U Fatehgarh Sahib

Abstract— Mobile Ad hoc networks (MANET) have multihop wireless connectivity, infrastructure less environment and frequently changing topology. The nodes work as router and communicate to each other. This paper aims to provide a means of understanding the issues and protocol (OSPF, DSR, AODV, TORA, OLSR, DSDV) of MANET and investigating behavior of DSR, AODV,TORA protocol using metrics Throughput and Network Load. The Behavior analysis has been done by using simulation tool opnet14.5 which is the main simulator.

Key words: OSPF, DSR, AODV, TORA, OLSR, DSDV

I. INTRODUCTION

A. *MANETS*

Mobile ad hoc networks (MANETs) are networks composed of a set of communicating devices able to spontaneously interconnect without any pre-existing Infrastructure. Devices in range can communicate in a point-to-point fashion. In addition to that, these devices are generally mobile. More and more people are interested in ad hoc networks. Not only their importance in military applications is growing, but also their impact on business is increasing.

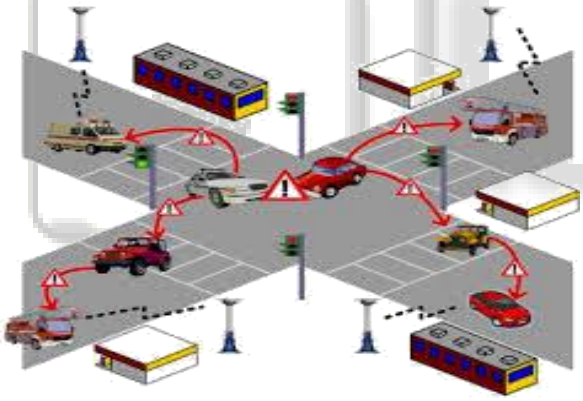


Fig. 1: MANET

The wide spread of lightweight and low-cost mobile devices—we are talking about mobile phones, PDAs, Pocket PCs, etc—which now embed Bluetooth and WiFi (IEEE 802.11) network adapters enable the spontaneous creation of city-wide MANETs.

These networks could then constitute the infrastructure of numerous applications such as emergency and health-care systems [7], groupware [11], gaming [10][13][11], advertisements, customerto- customer applications (like the UbiBay project [7], etc.

II. TYPES OF MANET

There are different types of MANETs including:

- InVANETs – Intelligent vehicular ad hoc networks make use of artificial intelligence to tackle unexpected situations like vehicle collision and accidents.
- Vehicular ad hoc networks (VANETs) – Enables effective communication with another vehicle or helps to communicate with roadside equipments.
- Internet Based Mobile Ad hoc Networks (iMANET) – helps to link fixed as well as mobile nodes.

III. CHARACTERISTICS OF MANET

- In MANET, each node act as both host and router. That is it is autonomous in behavior.
- Multi-hop radio relaying- When a source node and destination node for a message is out of the radio range, the MANETs are capable of multi-hop routing.
- Distributed nature of operation for security, routing and host configuration. A centralized firewall is absent here.
- The nodes can join or leave the network anytime, making the network topology dynamic in nature.
- Mobile nodes are characterized with less memory, power and light weight features.
- The reliability, efficiency, stability and capacity of wireless links are often inferior when compared with wired links. This shows the fluctuating link bandwidth of wireless links.
- Mobile and spontaneous behavior which demands minimum human intervention to configure the network.
- All nodes have identical features with similar responsibilities and capabilities and hence it forms a completely symmetric environment.
- High user density and large level of user mobility.
- Nodal connectivity is intermittent.

IV. MANET CHALLENGES

A Manet environment has to overcome certain issues of limitation and inefficiency. It includes:

- The wireless link characteristics are time-varying in nature: There are transmission impediments like fading, path loss, blockage and interference that adds to the susceptible behavior of wireless channels. The reliability of wireless transmission is resisted by different factors.
- Limited range of wireless transmission – The limited radio band results in reduced data rates compared to the wireless networks. Hence optimal usage of bandwidth is necessary by keeping low overhead as possible.
- Packet losses due to errors in transmission – MANETs experience higher packet loss due to factors such as hidden terminals that results in collisions, wireless channel issues (high bit error rate (BER)), interference, frequent breakage in paths caused by mobility of nodes, increased

collisions due to the presence of hidden terminals and uni-directional links.
- Route changes due to mobility- The dynamic nature of network topology results in frequent path breaks.
- Frequent network partitions- The random movement of nodes often leads to partition of the network. This mostly affects the intermediate nodes.
- The application of this wireless network is limited due to the mobile and ad hoc nature. Similarly, the lack of a centralized operation prevents the use of firewall in MANETs. It also faces a multitude of security threats just like wired networks. It includes spoofing, passive eavesdropping, denial of service and many others. The attacks are usually classified on the basis of employed techniques and the consequences

V. Routing Protocols In Manet

Three proposed protocols have been accepted as experimental RFCs by the IETF. Two of these are presented here. They are both based on well known algorithms from Internet routing. AODV uses the principals from Distance Vector routing (used in RIP[614]) and OLSR uses principals from Link State routing (used in OSPF[11]). A third approach, which combines the strengths of proactive and reactive schemes is also presented. This is called a hybrid protocol.

- Reactive protocols - AODV
- Proactive protocols - OLSR
- Hybrids - ZRP

A. Reactive protocols - AODV

Reactive protocols seek to set up routes on-demand. If a node wants to initiate communication with a node to which it has no route, the routing protocol will try to establish such a route.

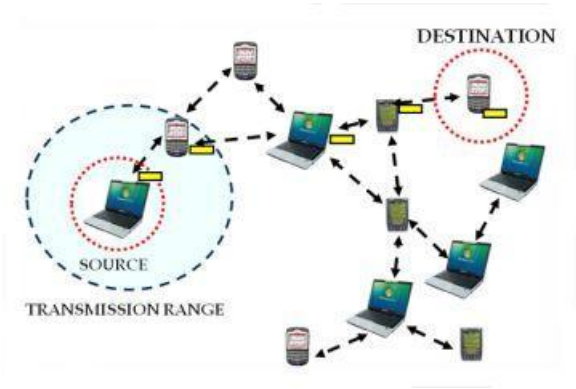


Fig. 2: Reactive Protocols

The Ad-Hoc On-Demand Distance Vector routing protocol is described in RFC 3561[54]. The philosophy in AODV, like all reactive protocols, is that topology information is only transmitted by nodes on-demand. When a node wishes to transmit traffic to a host to which it has no route, it will generate a route request(RREQ) message that will be flooded in a limited way to other nodes. This causes control traffic overhead to be dynamic and it will result in an initial delay when initiating such communication. A route is considered found when the RREQ message reaches either the destination itself, or an intermediate node with a valid route entry for the destination. For as long as a route exists between two endpoints, AODV remains passive. When the route becomes invalid or lost, AODV will again issue a request.

B. Proactive Protocols

A proactive approach to MANET routing seeks to maintain a constantly updated topology understanding. The whole network should, in theory, be known to all nodes. This results in a constant overhead of routing traffic, but no initial delay in communication.

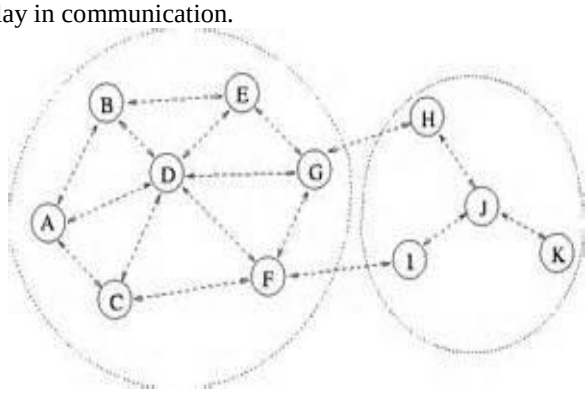


Fig. 3: proactive protocols

The Optimized Link State routing(OLSR) is described in RFC3626[23]. It is a table-driven pro-active protocol. As the name suggests, it uses the link-state scheme in an optimized manner to diffuse topology information. In a classic link-state algorithm, link-state information is flooded throughout the network. OLSR uses this approach as well, but since the protocol runs in wireless multi-hop scenarios the message flooding in OLSR is optimized to preserve bandwidth. The optimization is based on a technique called MultiPoint Relaying.

C. Hybrids-ZRP

Hybrid protocols seek to combine the proactive and reactive approaches. An example of such a protocol is the Zone Routing Protocol(ZRP)[39]ZRP divides the topology into zones and seek to utilize different routing protocols within and between the zones based on the weaknesses and strengths of these protocols. ZRP is totally modular, meaning that any routing protocol can be used within and between zones. The size of the zones is defined by a parameter r describing the radius in hops. Figure 2.4 illustrates a ZRP scenario with r set to 1. Intra-zone routing is done by a proactive protocol since these protocols keep an up to date view of the zone topology, which results in no initial delay when communicating with nodes within the zone. Inter-zone routing is done by a reactive protocol. This eliminates the need for nodes to keep a proactive fresh state of the entire network.

VI. Applications Of MANET

In the occasion where there is a group effort required, the MANET plays a major role in wireless communication and provides effective communication. At the time of disaster, it is easy to develop a wireless network rather than a wired network. The places where wired network may be affected by the disasters, MANET can be implemented.As far as the Personal Area Networks (PAN) are concerned, they need

not much coverage. They just need the coverage of very limited area. MANETs server the purpose in such situations.

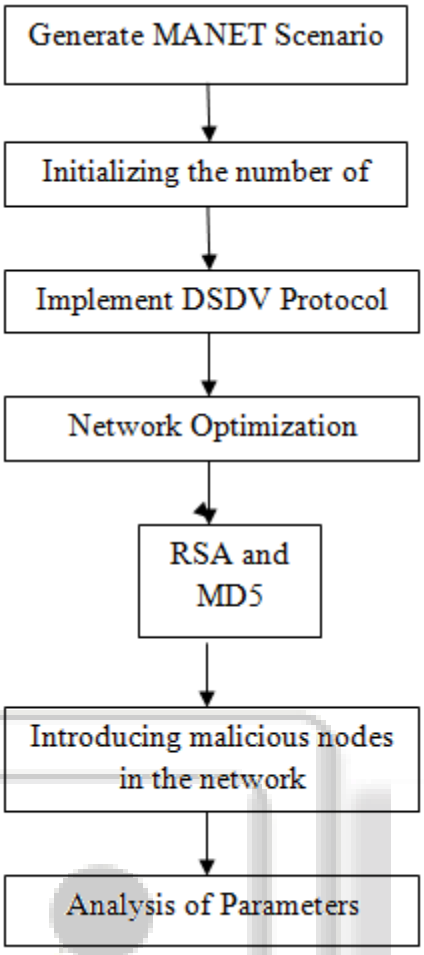
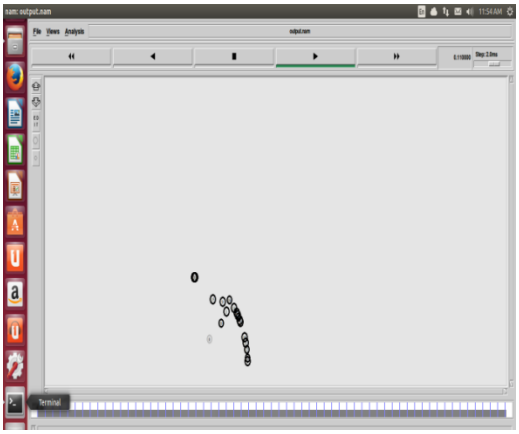


Fig. 4.1: Flow of Work

VII. RESULTS

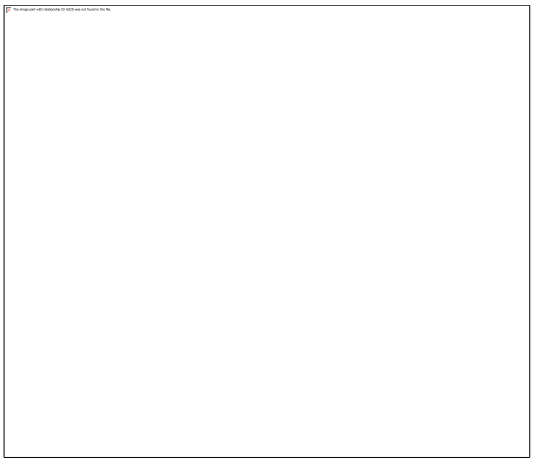
A. *Scenario 1*

In this scenario number of nodes are initialized.



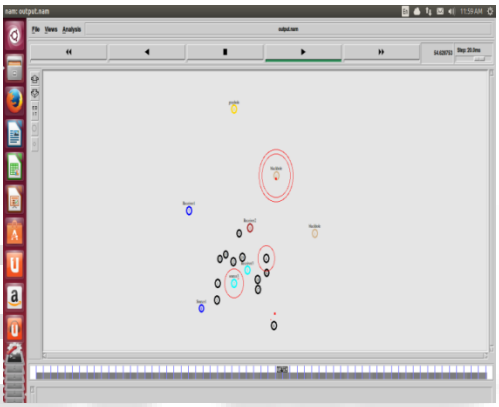
B. *Scenario 2*

In this scenario number of nodes are 20 and out of which 3 pair are sender and receiver, one pair is having blue color second is having red color and third one is having sky blue color. Here the circles around nodes represent broadcasting between nodes.



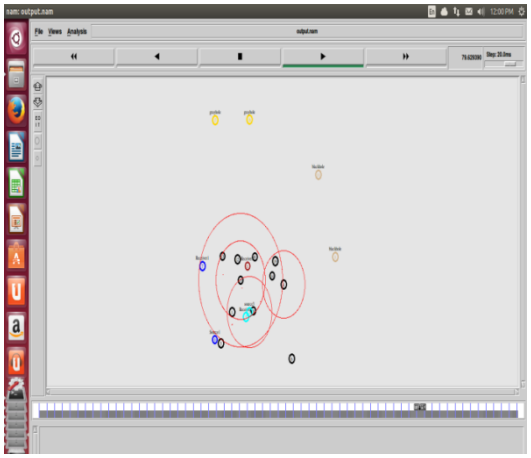
C. *Scenario 3*

In below scenario the node with black hole attack and grey hole attack are shown and these nodes are going out of the network when detection is done. Nodes with black hole attack are start dropping packets and nodes with grey hole attack are start sending wrong message



D. *Scenario 4*

It represents 4 nodes are having attack out of which two having grey hole and 2 having black hole and these nodes are now not considered in network and communication between another nodes are not effected.



E. *Graphs*

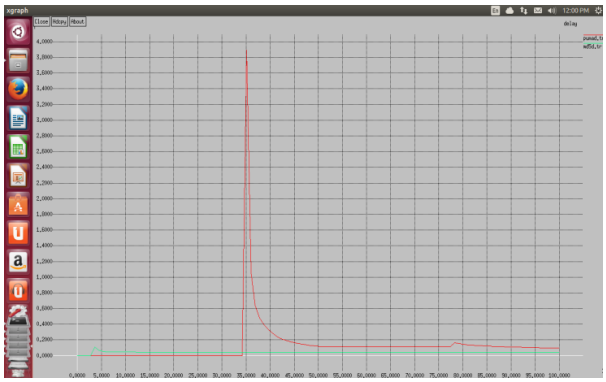


Fig. 5: Represents delay

Here delay is represented for MD5+RSA which represent by the green line and it is than compared with the puma protocol which represent by the red line . it is clear from the plot that MD5 and RSA are better because these gives minimum value for delay than PUMA.

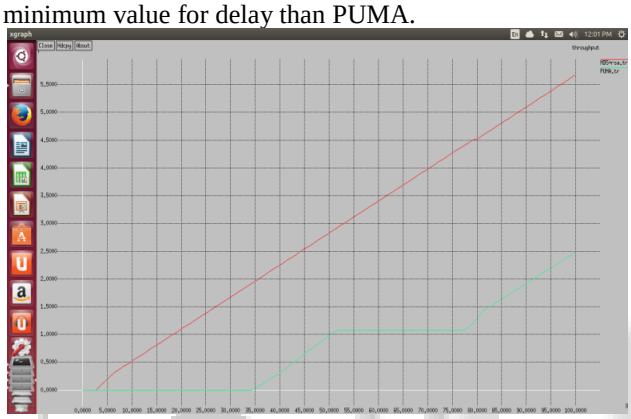


Fig. 5: Represents throughput

Here throughput is represented for MD5+RSA which represent by the red line and it is than compared with the puma protocol which represent by the green line . it is clear from the plot that MD5 and RSA are better because these gives maximum value for throughput than PUMA.

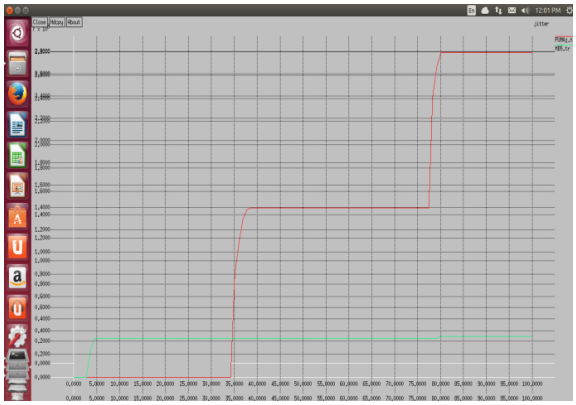


Fig. 5: Represents jitter

Here jitter is represented for MD5+RSA which represent by the green line and it is than compared with the puma protocol which represent by the red line . it is clear from the plot that MD5 and RSA are better because these gives minimum value for throughput than PUMA.

VIII. Conclusion

In this research black hole attack and grey hole attack are detected in the mobile ad hoc network and this can be done by using RSA and MD5 algorithm. Which are security algorithms. When the attack is detected on nodes then that nodes are sent out of the network. In this way communication is improved and parameter taken for this is throughput, end to end delay and jitter. These parameter are than compare with the parameter of previous work which was done using PUMA protocol. It is clear from graphs that by using RSA and MD5 results gives better output hence this system is better. In future this can be better enhance if HOOSC security algorithm will implemented for the same.

References

[1] Rutvij H. Jhaveri., "MR-AODV: A Solution to Mitigate Blackhole and Grayhole Attacks in AODV Based MANETs" 2012 Third International Conference on Advanced Computing & Communication Technologies, pp. 254-260.

[2] Thaalbi, Mariem, Tabbane, Nabil, Bejaoui, Tarek,; Meddahi, Ahmed "An enhanced Quality Aware Multi path routing protocol over MA-NETs based on cross layer approach" Proceedings of the Tenth International Symposium on Wireless Communication Systems (ISWCS), pp. 1 – 5, 27-30 Aug. 2013.

[3] Gouda, B.S; Behera, C.K.; Behera, R.K.; "Performance Evaluation of Energy Efficiency Enhancement of Routing Protocols in MANET" International Multi-Conference on Automation, Computing, Communication, Control and Compressed Sensing (iMac4s), pp. 502 – 507, 22-23 March 2013.

[4] Sunil J. Soni, Suketu D. Nayak, "Enhancing Security Features & Performance of AODV Protocol under Attack for MANET" International Conference on Intelligent Systems and Signal Processing (ISSP), pp. 325 – 328, 1-2 March 2013.

[5] Aarti, Dr. S. S. Tyagi, "Study of MANET: Characteristics, Challenges, Application and Security Attacks" International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 5, May 2013.

[6] Patil V.P, "Efficient AODV Routing Protocol for MANET with enhanced packet delivery ratio and minimized end to end delay" International Journal of Scientific and Research Publications, Volume 2, Issue 8, August 2012.

[7] Jaya Jacob, V.Seethalakshmi, "Performance Analysis and Enhancement of Routing Protocol in Manet" International Journal of Modern Engineering Research (IJMER), Vol.2, Issue.2, Mar-Apr 2012 pp-323-328.

[8] Simmi Jain, Prof.Hitesh Gupta, Prof.Mukesh Kumar Baghel, "Survey on MANET Routing Protocol and proposed Multipath Extension in AODV" International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 7, July 2012.

[9] G.Vijaya Kumar, Y.Vasudeva Reddyr, Dr.M.Nagendra, "Current Research Work on Routing Protocols for MANET: A Literature Survey" (IJCSE) International Journal on Computer Science and Engineering, Vol. 02, No. 03, 2010, 706-713.

[10] S.Gomathi, R.Poonkuzhali, K.Duraiswamy, "ROUTING PROTOCOLS FOR MOBILE AD-HOC NETWORKS PERFORMANCE ENHANCEMENT" http://citeseerx.ist.psu.edu/viewdoc/download?rep=rep1&type=pdf&doi=10.1.1.215.5627.
[11] Amit Shrivastava, Nitin Chander, "Overview of Routing Protocols in MANET's and Enhancements in Reactive Protocols" http://cs.lamar.edu/faculty/disrael/COSC5100/Seminar.pdf.
[12] Robinpreet Kaur & Mritunjay Kumar Rai, "A Novel Review on Routing Protocols in MANETs" *www.interscience.ac.in/URJA/journals/urja_vol1no1/urja_paper23.pdf.*
[13] International Journal of Advanced Research in Computer Science and Software Engineering Research Paper Vol. 3, Issue 5, May 2013 ISSN: 2277 128X.
[14] J. Liebeherr, J. Wang, and G. Zhang. Programming overlay networks with overlay sockets. In Proc. 5th COST 264 Workshop on Networked Group Communications (NGC 2003), LNCS 2816,Vol.7,Issue 4 pp. 242–253, Sep. 2003.
[15] Kartik Kumar Srivastava, Avinash Tripathi, and Anjnesh Kumar Tiwari, " Secure Data Transmission in MANET Routing Protocol", International journal Computer Technology & Applications,Vol.3, Issue 6,pp. 1915-1921, Nov-Dec 2012.
[16] Merin Francis, M. Sangeetha, and Dr. A. Sabari, "A Survey of Key Management Technique for Secure and Reliable Data Transmission in MANET" International Journal of Advanced Research in Computer Science and Software Engineering, Vol.3, Issue 1,pp.40-49, January 2013.
[17] N. G. Duffield and F. Lo Presti, "Network tomography from measured end-to-end delay covariance," IEEE/ACM Transactions on Networking, Vol.12, Issue 6, pp. 978–992, Dec. 2004.
[18] Ranjeet Singh, and Prof. Harwant Singh Arri, "Comparison of AAMRP and IODMRP using SBPGP" International Journal of Computer Science and Management Research, Vol.2, Issue 3,pp.54-68,March 2013.
[19] Vineetha S. H. and Shebin Kurian, " Performance Analysis of Cluster Based Secure Multicast Key Management in MANET" International Journal of Computer Science and Telecommunications, Vol.4, Issue 4, pp.1-14, April 2013.
[20] http://www.ijcem.org/.
[21] http://www.ijarcsse.com/docs/papers/Volume_3/5_May2013/V3I5-0267.pdf.

