International Journal of Engineering Research in Computer Science and Engineering (IJERCSE) Vol 2, Issue 8, August 2015

Improved RED Strategy for Enhancement in Performance of MANETs

[1]Chetan Batra,[2]Vishal Kumar Arora
[1][2]B.Tech, SR engineering college
[1]Research Scholar(Department of Computer Science)Shaheed Bhagat Singh State Technical Campus, Ferozepur (Pb.),India
[2]Assistant Professor, (Department of Computer Science)Shaheed Bhagat Singh State Technical Campus , Ferozepur (Pb.), India

Abstract: **MANETs have been focused for many years but still it is main area for research due to its challenges. Various types of attacks and problem like congestion are major reasons for its existence in research. Various attacks are DOS attack, black hole attack, grey hole attack, wormhole attack, Sybil attack, fabrication attack and replay attack etc. congestion occurs when demand is greater than available resources. This problem can be avoided by RED (random early detection) scheme. Congestion can occurs due to various reasons like by replay attack, by limited resources, by link failure, by malicious attacker. Congestion lead to dos attack. In previous work congestion can be avoided by using improved RED. In our work we try to remove congestion by using improved random early detection scheme but the difference is, we using window size approach which in directly solves the denial of service attack. This approach doubles the security because if DOS is due to the retransmissions or replays then it can be detected by keep check on messages.**

I. INTRODUCTION

A MANET is a multi-jump remote system that is shaped alertly from an aggregation of versatile nodes without the help of a concentrated organizer. Presently engendering extent is restricted, every portable node has just constrained data, for example, its own ID and the Medium Access Control (MAC) location of its one-jump neighbors [2]. Thusly, if two hubs are not inside of the radio spread range, a multi-bounce, through one or more moderate hubs, is obliged to forward bundles. With late execution progression in remote innovation, compact registering stages and little remote gadgets get to be basic gadgets of our everyday life. The utilization of a convenient gadget is obliged by its vitality, making force preservation the most discriminating issue for compact gadgets and their applications [10].

1.1 Mobile Ad Hoc Network

A mobile ad-hoc network (MANET) is composed of a group of mobile, wireless nodes which cooperate in forwarding packets in a multi-hop fashion without any centralized administration [1]. Uses of MANETs happen in circumstances like front lines, real hazardous situations, and outside get-togethers. A working gathering called "MANET" has been shaped by the Internet Engineering Task Force (IETF) to concentrate on the related issues and empower explore in MANET. MANETs are self-arranging remote systems with no unified control. At this very moment scope of versatile hubs is normally little, the hubs must coordinate with one another to keep the system alive [2]. The correspondence between two hubs ordinarily incorporates a few halfway hubs sending the information bundles between the endpoints. Each hub goes about presently. The hubs can impart with no settled foundation. The hubs, for example, cell telephones, portable PCs and PDAs, inMANETs are for the most part lightweight and they work on batteries. The life of a hub is straightforwardly corresponding to the battery in the gadget working at the hub. There are numerous endeavors going on both in the business and the scholarly research group to outline components to spare battery-life in these low fueled devises. Equipment makers are presently making more vitality effective gadgets, for example, vitality proficient CPUs, low power show units, productive calculations for equipment preparing and high-thickness batteries [8].

Battery force of the hubs is fundamentally devoured while transmitting parcels (notwithstanding performing the handling in the hubs). At this very moment, multi-jump, there are shots of a hub's contribution in information exchange regardless of not being an objective or a source. The steering calculation chooses which of the hubs should be chosen in a specific correspondence. In this way, directing calculations assume a vital part in sparing the vitality of a correspondence framework and the life of the hubs and accordingly of the entire system [6].

Portable Ad Hoc Networks (MANETs) give an alluring answer for systems administration in the circumstances where system foundation or administration membership is not accessible. Its utilization can further be stretched out by empowering interchanges with outer systems, for example, Internet or cell organizes through entryways. Then again, information access applications in MANETs experience the ill effects of element system associations and limited vitality supplies. While the vast majority of the exploration

concentrates on Media Access Control (MAC) and directing layer arrangements, we address these issues by application level collaboration which uses the region standard and shared trait to clients' greatest advantage [3].
The components of MANETs and the created issues/issues are compressed at this very moment:

1.1.1 Wireless medium: Versatile hubs speak with one another through remote medium, which implies one transmission can cover all gatherings of people inside of the transmission range. This telecast nature is likewise alluded right now Multicast Advantage (WMA) [10].

1.1.2 Multi-hop routes: In MANETs, multi-jump courses are utilized when a hub corresponds with the hubs that are out of its quick transmission range. At this very moment Li and so forth., the ideal throughput for a multi-jump correspondence is around 1/3 of the throughput of a solitary bounce correspondence, presently hub can't transmit and get in the meantime, and the upstream and downstream hubs of the sending hub can't transmit in the meantime on the grounds that the bundles would clash at the sending hub [9].

1.1.3 Dynamic topologies: Network topology may change for MANETs due to node mobility, exhausted power, and interferences etc. Changing of network topologies may break existing routes and cause extra overhead for establishing new routes [2].

1.1.4 Limited resources: In MANETs, the portable hubs for the most part have limited power supply, restricted figuring ability, and constrained storage room. Because of this, information access applications might have the capacity to work appropriately with minimum re-source conceivable. That is, information access applications should be vitality effective and light-weight (not figuring hungry or memory-hungry)[8].

1.2 Types of Mobile Ad hoc Network
1. Vehicular Ad-Hoc Networks
2. Intelligent Vehicular Ad-Hoc Networks
3. Internet Based Mobile Ad-Hoc Networks

1.3 Attacks in MANET
1.3.1 Passive vs. Active attack
Regularly, inactive assaults intend to take profitable data in no less than two imparting hubs (presently Figure 4.1(a)) or even in the entire system. There are numerous varieties of detached assaults, yet in MANET, there exist two sorts: listening in and activity examination. Essentially, contingent upon circumstances, uninvolved assaults can be considered right now illegitimate activities [5]. On the off chance that the intention is benevolent, for instance, if the chairman needs to utilize a few instruments to test the system activity, keeping in mind the end goal to investigate or account the system then it is real. In actuality, if the reason for existing is malignant, one assailant can take important data by testing the system activity, for example, Mastercard data, certification email, and after that utilization the data to illicitly withdraw cash from ledgers or extortion the casualties [9]. Generally talking, inactive assaults don't plan to upset the operation of the specific system, yet dynamic assaults have the capacity to modify the ordinary system operation [5].

1.3.2 Internal vs. External attack
At this very moment suggests, outer assaults are propelled by assailants who physically remain focused of the assaulted system [2]. These assaults more often than not expect to deny access to particular capacity in the system (i.e. http movement), or to bring about system clogging or even to disturb the entire system. While outside assaults would be hard to be propelled if the system was legitimately arranged and secured, the interior assaults are much harder to protect against. One of the reasons is on account of we have a tendency to shield the system from being assaulted by untouchables instead of insiders. Additionally on account of the way that an outer assault can without much of a stretch be followed contrasted with the inner assault. An outside assault can turn into an inward assault and the outcome of the assault would be more genuine. In this manner, there exist two sorts of interior assailant hubs, one is the bargained hub, which was examined above, and the other one is the acting mischievously hub, which is approved to get to the framework assets however neglect to utilize them as indicated by the way it ought to be utilized. Assaults brought about by these inside getting rowdy hubs are hard to distinguish, for instance, self centered assault in which the hub is unwilling to expend battery power, CPU cycles or system transfer speed to forward uninterested parcels, despite the fact that it anticipates that different hubs will forward bundles for it [3].

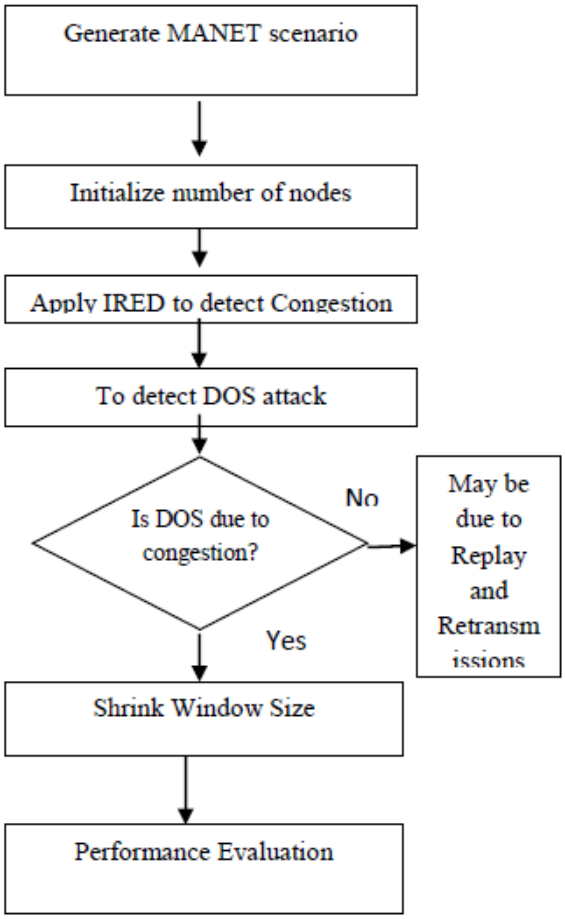
1.3.3 BLACK HOLE ATTACK:
There are two types of attack:-
1.3.3.1 Single Black hole attack: In this sort of assault, one malignant hub uses directing convention to assert itself of being most limited way to destination hub yet drops steering parcels and doesn't forward bundles to its neighbors [2].
1.3.3.2 Cooperative Black hole attack: Dull opening is a vindictive center that erroneously answers the course requests that it has a fresh course to destination and a while later it drops each tolerant bundle [2]. A dose of authentic mischief rises if vindictive centers coordinate right now. This is called useful dull opening attack [7].

II. RED algorithm

The RED figuring finds out the ordinary line size using a low pass channel with an exponential weighted moving typical. The typical line size is stood out from two constrains: a base and a most compelling edge. Exactly when the typical line size is not precisely as far as possible,

no groups are stamped. Right when the ordinary line size is more essential than the most compelling edge, every arriving package is stamped. In the occasion that stamped packs are, undoubtedly, dropped or if all source center points are useful, this ensures that the ordinary line size does not in a far-reaching way surpass the most great cutoff. Exactly when the typical line size is between the base and most prominent limits, every one arriving group is stamped with probability father, where father is a limit of the ordinary line size avg [9]. Every one time a pack is meant, the probability that a bundle is stamped from a particular affiliation is by and large in respect to that affiliation's offer of the exchange speed at the switch. Fundamentally, RED figuring has two unique parts. One is for figuring the ordinary line size, which chooses the level of burrstones that will be allowed in the switch line. It considers the period when the line is void (the unmoving period) by evaluating the number m of little packages that could have been transmitted by the switch in the midst of the unmoving period. After the unmoving period, the switch figures the ordinary line measure as if m bundles had arrived to an unfilled line in the midst of that period. The other is used to figure the group stamping probability and thereafter choose how a great part of the time the switch imprints packages, given the present level of blockage. The goal is for the change to check packages at sensibly just as separated breaks, to stay far from slants and sidestep overall synchronization, and to stamp packages adequately a significant part of the time to control the typical line size.

III. Flow of Work



RESULTS AND DISCUSSIONS

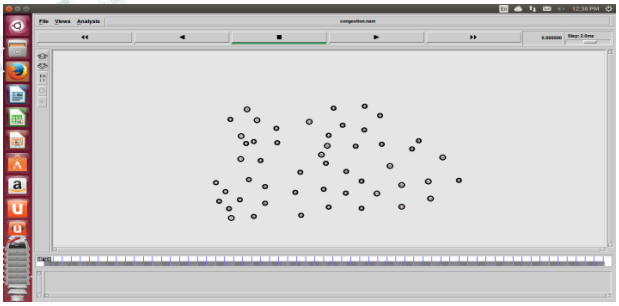


Fig 1: Initialization of nodes

By initializing the scenario parameters Queue Type, Queue Length, Antenna Type, Routing Protocols initialization of nodes is done. In this Scenario number of nodes is 50.

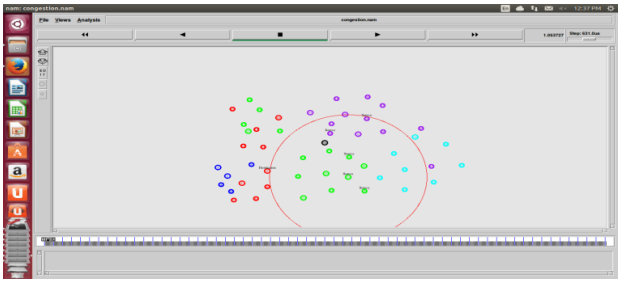


Fig 2: Movements of Nodes

In this scenario nodes Initialization of sender & receiver is done. In this identification of sender & receiver is done i.e which node will sends the packets & which will receive the packets After that nodes start moving to their respective positions

Fig 3: Communication b/w 3 nodes

In this scenario nodes start to communicate with each other. In this scenario the number of sender is 2 & number of receiver is 1.

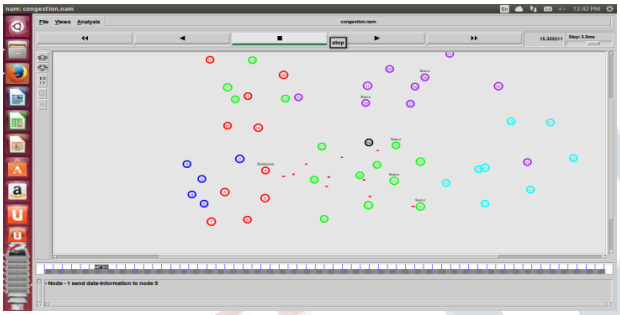


Fig 4: Communication b/w 4 nodes

In this scenario nodes start to communicate with each other. In this scenario the number of sender is 3 & number of receiver is 1.

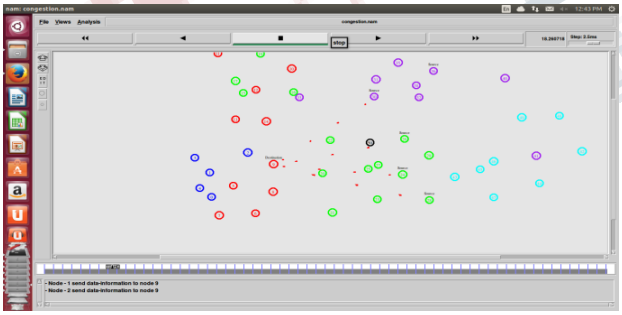


Fig 5: Communication b/w 5nodes

In this scenario nodes start to communicate with each other. In this scenario the number of sender is 4 & number of receiver is 1. If number of sender is increase than the problem of congestion is also occurred.

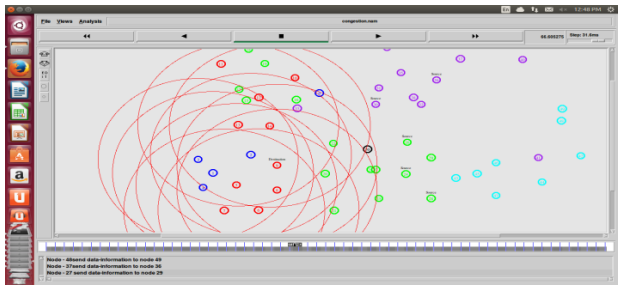


Fig 6: Remove Congestion Problem

By increasing the number of sender the problem of congestion is also increase. In this two algorithms is apply first is Random Early Detection Algorithm & Second is Window Sliding Algorithm. Random Early Detection Algorithm is use to decrease the probability of congestion problem before occurrence. In this before the occurrence of congestion, Messages is sends to the nodes. After receiving this massage node stop to send the packets. If the problem is occurred than by using

Window Sliding algorithm, we remove the congestion problem. Window Sliding algorithm is use to divide in to small packets due to which congestion not occurred

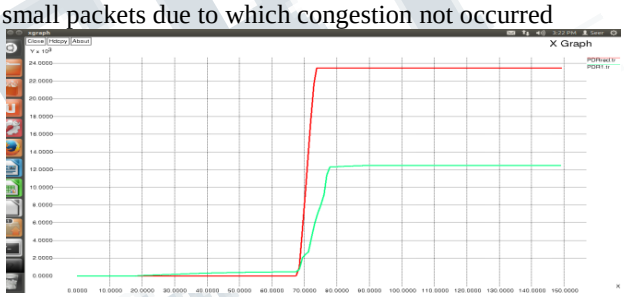


Fig 7: Packet Delivery Ratio

In this X-axis represent the Time and Y-axis represent the Bytes send over the network. This figure is use to represent the Packet Delivery Ratio. Packet Delivery Ratio is defined as the number of packet deliver with respect to time. Is has clear from graph that PDR with improved red protocol (represented with red line) is high as compare to other one.

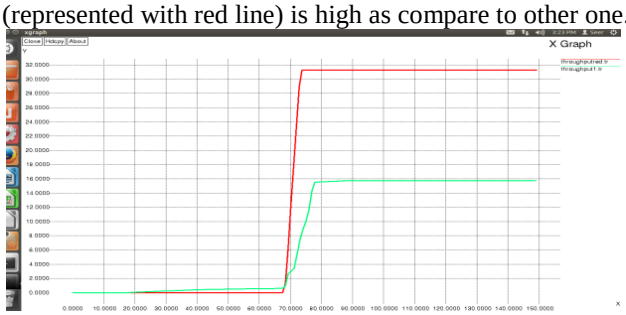


Fig 8 Throughput

This figure is use to represent the Throughput. Throughput is defined as the number of packet delivered successfully over the network. Is has clear from graph that throughput with improved red protocol (represented with red line) is high as compare to other one.

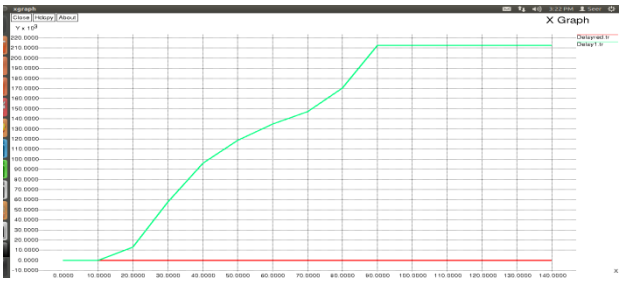


Fig 9 Packet Delay

This figure is use to represent the Packet Delay. Packet Delay is defined as the Delay between packets during transmission. Is has clear from graph that packet delay with improved red protocol (represented with red line) is less (almost zero) as compare to other one.

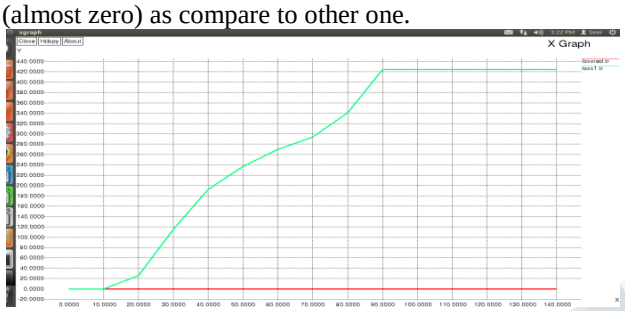


Fig 10 Packet Loss

This figure is use to represent the Loss of packets. Loss is defined as the number of packet loss when we transfer packets over the network. Is has clear from graph that packet loss with improved red protocol (represented with red line) is less (almost zero) as compare to other one.

CONCLUSION

MANET uses wireless connection between nodes. MANETs have been focused for many years but still it is main area for research due to its challenges. Various types of attacks and problem like congestion are major reasons for its existence in research. Various attacks are DOS attack, blackhole attack, greyhole attack, wormhole attack, Sybil attack, fabrication attack and replay attack etc. congestion occurs when demand is greater than available resources. This problem is avoided by RED (random early detection) scheme in the work. We have tried to remove congestion by using improved random early detection scheme but the difference is, we using window size approach which indirectly solves the denial of service attack. This approach doubles the security because if DOS is due to the retransmissions or replays then it can be detected by keep check on messages.

ACKNOWLEDGMENT

This is to convey my sincere gratitude to Mr Vishal Kumar Arora, Assistant Professor, Department of Computer Science & Engineering, SBS State Technical Campus, Ferozepur (Punjab), India, for sparking in me the enthusiasm and initiative to learn. I am truly thankful to him for guiding me through the entire research and being my mentor and guide in this learning curve.

7.REFERENCES

[1] MahaAbdelhaq, Sami Serhan, RaedAlsaqour and Rosilah Hassan "A local Intrusion Detection Routing Security over MANET Network", IEEE, July 2011, Bandung, Indonesia.

[2] YiebeltalFantahunAlem, Zhao Chenh Xuan, " Preventing Black Hole Attack in Mobile Ad-hoc Networks Using Anamoly Detection",2nd International Conference on Future Computer and Communication, IEEE, Volume 3, 2010.

[3] S.Marti, T.J.Giuli, K.lai and M.bakery "Mitigating routing misbehaviour in mobile ad hoc networks", 6th MobiCom, Boston, Massachusetts, August 2000.

[4] J.Sen, S.Koilakonda and A.Ukil, "A mechanism for detection of cooperative black hole attack in mobile ad hoc networks", Second International Conference on Intelligent System, Modeling and Simulation ,Innovation lab, Tata consultancy services ltd. , Kolkata, 25-27January 2011.

[5] Rakesh Kumar Sahu, Dr. Narendra S. Chaudhari,"Efficient Techniques to Detect the Various Attacks in Ad-Hoc Network", **November** 2002**.**

[6] Sanjay Ramaswamy, Huirong Fu, John Dixon "Prevention Of Cooperative Black Hole Attack In Wireless Ad Hoc Network", Department of Computer Science, IACC 258, North Dakota State University, Fargo, ND 58105.

[7] NishuKalia, KundanMunjal, "Multiple Black Hole Node Attack Detection Scheme In MANET By Modifying AODV Protocol" , International Journal of Engineering and Advanced Technology (IJEAT), Volume-2, Issue-3, February 2013.

[8] Kartik Kumar Srivastava, AvinashTripathi, and Anjnesh Kumar Tiwari, " Secure Data Transmission in MANET Routing Protocol" IJCTA , Int.J.Computer Technology &Applications,Vol 3 (6), 1915-1921 Nov-Dec 2012. Available online@www.ijcta.com

[9] Vineetha S. H. and Shebin Kurian, "Performance Analysis of Cluster Based Secure Multicast Key Management in MANET" **I**nternational **J**ournal of **C**omputer **S**cience and **T**elecommunications [Volume 4, Issue 4, April 2013.

[10] 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, Volume 3, Issue 1, January 2013, ISSN: 2277 128X.

[11] 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, pages 242–253, Sep. 2003.

[12] H. Lundgren, E. Nordstrom, and C. Tschudin. Coping with communication grayzones in IEEE 802.11b. In Proc. of

5th ACM International Workshop on Wireless Mobile Multimedia (WoWMoM 2002), Sep. 2002.
[13] H. Luo, J. Kong, P. Zerfos, S. Lu, and L. Zhang. Ursa: Ubiquitous and robust access control for mobile ad hoc networks. ACM/IEEE Transactions on Networking, 2005. To appear.
[14] C. E. Perkins and E. M. Royer. Ad-hoc on-demand distance vector routing. In Proc. 2nd IEEE Workshop on Mobile Computing Systems and Applications, pages 90–100, Feb. 1999.
[15] K. Lakshmi et al. "Modified AODV Protocol Against Black hole Attacks in MANET" International Journal of Engineering and Technology Vol.2 (6), 2010, 444-449.
[16] H. Rangarajan "Robust loop-free on-demand routing in Ad-hoc networks" PhD dissertation, University of California, USA, June 2006.
[17] Chetan Batra,Vishal Arora,"RED Strategy for Improving Performance in MANET: A Review", Journal of Information Sciences and Computing Technologies(JISCT,Volume 3, Issue 2, pp 217-221.
[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 March 2013.ISSN 2278-733X.