ISSN: 2278 – 7798
International Journal of Science, Engineering and Technology Research (IJSETR)
Volume 1, Issue 5, November 2012

# Maximizing Security and Advancing Performance of a Wireless Mesh Network by Implementing a New Approach "Reference Broadcast System"

**Akshita Rana, Deepak Shrivastava**
**Research Scholar MITS, Research Scholar MITS**

**Madhav Institute of Technology and Science, Gwalior-474005, India**

***Abstract:*** ***A wireless mesh network can be seen as a special type of wireless ad-hoc network. A wireless mesh network often has a more planned configuration, and may be deployed to provide dynamic and cost effective connectivity over a certain geographic area Wireless mesh networks often consist of mesh clients, mesh routers and gateways. In wireless mesh network security of network is one of most concerned area. Here we have proposed a new approach to maximizing security of a network basically we have worked on DOS in which we have shown applied our approach in wormhole attack. The wormhole attack is one of the most severe security attacks encountered in wireless ad hoc networks. It can significantly disrupt the communications across the network, is hard to detect and can be implemented without having a cryptography key or knowing the network routing protocol. We have proposed approach called RBS (Reference Broadcast System) in this approach relative velocity of various nodes is get compared. More precisely there is a reference node in network and when a malicious node attacks into the network than velocity of a malicious node get drastically changed in comparisons of other nodes with respect to that reference node this is happened because a malicious node attacks from outside of the network so it becomes easy to detect that node on the basis of velocity. We have performed our analysis with wormhole attack and without worm hole attack and our results proved the significance of the approach that we have applied here. We have analyzed our result on the basis of various parameters and improvement in the network has been verified by simulated results in Xgraph.***

***Keywords- MAC (Medium Acess Control), Wireless mesh Networks,AODV, Throghput,End to End Delay.***

## I.Introduction

Wireless mesh networks are dynamically self-organized, self –Configured with the nodes having ad-hoc networking and maintaing the mesh connectivity. There are two types of nodes : Mesh routers and Mesh clients[4]. The mesh routers form an infrastructure of the mesh backbone for mesh clients. In general mesh routers have minimal mobility and operate just like a netwrok of fixed routers except that they are connected by wireless links through wireless technologies such as IEEE802.11. A mesh network is a configuration of peer wireless access nodes that allow for continous connections to a network infrastructure, including reconfiguration around blocked paths by hoping from node to node[8]. The term mesh network is often used synonymously with wireless ad-hoc network. However, adhoc networking typically refers to an arbitrary topology of client nodes and associated hosts, where a mesh network generally refers to a network of fixed wireless access nodes that use provide multi-hopping backhaul service between client nodes and the internet. For mesh security, this subtile distinction becomes important- while most of the underlying technologies are identical, there are implicit trust assumptions assumed in a mesh network i.e. the nodes belong to the same administrative and security domain unlike assumed random and arbitrary collection of nodes in an ad-hoc network[9,11]. Although security is a major concern in wireless mesh network due to its self configuring and self organising characteristics.One of the major issue is " Worm Hole attack"[1,2,6] . Worm hole attack is one of the Denial-of-service attacks effective on the network layer, that can affect network routing, data aggregation and location based wireless security.This is one of the strongest attacks where even if two adversary nodes collude the attack can be carried out. Wormhole attack is very difficult to detect, it is a network layer attack that can affect the network even without the knowledge of cryptographic techniques implemented.

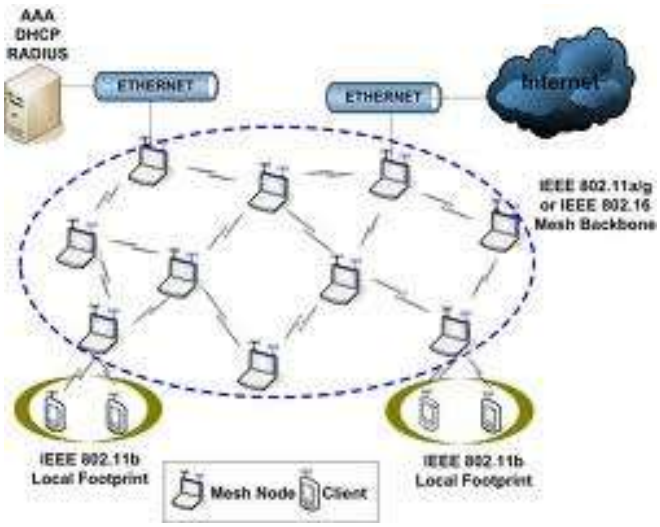



***Fig1. Wireless mesh network topology***

## II. Security Issues of WMN

1) **Availability:** Ensures survivability despite Denial of Service (DOS) attacks. On physical and media access control layer attacker can use jamming techniques to interfere with communication on physical channel. On network layer the attacker can disrupt the routing protocol. On higher layers, the attacker could bring down high level services e.g.: key management service.

2) **Confidentiality:** Ensures certain information is never disclosed to unauthorized entities.

3) **Integrity:** Message being transmitted is never corrupted.

4) **Authentication:** Enables a node to ensure the identity of the peer node it is communicating with. Without which an attacker would impersonate a node, thus gaining unauthorized access to resource and sensitive information and interfering with operation of other nodes.

5) **Non-repudiation:** Ensures that the origin of a message cannot deny having sent the message.

## III. Challenges of WMN

Use of wireless links renders a WMN susceptible to link attacks ranging from passive eavesdropping to active impersonation, message replay and message distortion. Eavesdropping might give an attacker access to secret information thus violating confidentiality [3, 5, and 7]. Active attacks could range from deleting messages, injecting erroneous messages; impersonate a node etc thus violating availability, integrity, authentication and non-repudiation. Nodes roaming freely in a hostile environment with relatively poor physical protection have non-negligible probability of being compromised. Hence, we need to consider malicious attacks not only from outside but also from within the network from compromised nodes. For high survivability WMNs should have a distributed architecture with no central entities, centrality increases vulnerability [12]. WMN is dynamic due to frequent changes in topology. Even the trust relationships among individual nodes also changes, especially when some nodes are found to be compromised. Security mechanism need to be on the fly (dynamic) and not static and should be scalable.

## IV. Wormhole attack:

Wormhole attack is very severe kind of attack and its one of the strongest attack as compared to other DOS attacks as to detect that attack is much more difficult. Wormhole attack appears in the network layer and affects the routing of the network because routing control messages are replayed by the malicious nodes of the network from one network location to another. A wormhole tunnel is created by the malicious nodes in the network which is a direct link between them and it can be either wired link or wireless link, after establishing this tunneling path the packets are transmitted through the malicious nodes. This path is called a “wormhole” since the adversary nodes virtually created a tunnel between the source and the destination. It sniffs the packets from the sender and communicates it to other end of the tunnel. The packet is replayed at this end locally. Wormhole attacks obtained easily since it does not need any special hardware or special routing protocol.

## V. Related Work:

In every research it is essential to refer the previous work done. It is important to understand how much work have been done till now, what were the strategies that had been implemented for the research and what are the problems and limitations of the previous research papers of the similar topic. After understanding the previous research papers and their work, we believe that there is much scope for the research in the area of maximizing security and increasing performance of a wireless mesh network.
The idea of maximizing security and increasing performance of a wireless mesh network referenced from [1, 6, 8, and 11].These references gives the elaboration about implementing concept of new approach REFERENCE BROADCAST SYSTEM (RBS) which are used to enhance the security and increasing performance of a wireless mesh network.

Wireless mesh network are potentially vulnerable to a broad variety of attacks. Hence security is an important consideration for the practical operation of wireless mesh network. Also Wireless mesh networks presents additional challenges due to their decentralized nature, dynamic network topology, and easy access to the radio medium [12]. So it is necessary to maximize its security and enhance its performance of a wireless mesh network.
One of the major challenges for Wireless mesh network is to deal with wormhole attacks. Wormhole attacks can be severely problematic. With such attacks, the hostile adversary doesn’t need to control any legitimate stations but still poses a significant outsider the WMN’s routing integrity. The wormhole attack forms a tunnel connecting different parts of the network, thus tricking stations adjacent to one end of the wormhole into believing that they’re neighbors with stations at the other end. Wormhole attacks in wireless ad-hoc networks can severely deteriorate the network performance and compromise the security through spoiling the routing protocols and weakening the security enhancements. From the and above references we have a fair knowledge that the wormhole attack is very powerful and preventing this attack has proven to be very difficult.

Our research paper addresses the aforementioned gap by introducing a new technique based on Reference Broadcast System (RBS)

## VI. Proposed scheme:

We have discussed various aspect of wireless mesh network so far but the critical issue in wireless mesh networking is security. Many papers have been published in this area these research papers have covered security issues with practicability one the concerning issue is DOS (Denial of Service)[14]. There are many of attacks into this category they are Black hole, Grey hole, Worm hole and Jellyfish and many more on different layers of the network. One of the severe kinds of attack is Wormhole attack we have proposed our approach to mitigate that type of attack. Wormhole attack is observed at network layer that is why we analyzed this approach at network layer. Our approach is to minimize the wormhole attack so that security of wireless mesh network is increased although wormhole attack cannot be fully removed but we have tried our efforts to reduce it as much as we can. The concept of our approach is basically designed on the basis of relative velocity of the nodes. As we measure the relative velocity of different nodes in the network with reference to the Reference node which we assume with our convenience. Since nodes in the wireless mesh network move randomly so the relative velocity of the nodes changes with the movements of the nodes, whenever a malicious node attacks in the network then its relative velocity also measured with respect to that reference node and then we find that its relative velocity has either very high or very low value so that we can identify this malicious node in the network. Whenever that malicious node comes into the network it has the tendency to unsecure the network by applying our approach we can not only detect the wormhole attack but also we can mitigate its affects to the network, this is the way how we work on wormhole attack in wireless mesh networks.

## VII. Performance indexes:

(a) PDR

Packet delivery ratio: The ratio of the number of delivered data packet to the destination. This illustrates the level of delivered data to the destination.

(b) End to end delay

The End to end delay over the path is the summation of delays experienced by all the hops along the path. The End to end delay is sum of queuing and transmission delays at mesh routers.

## VIII. Simulation methodology:

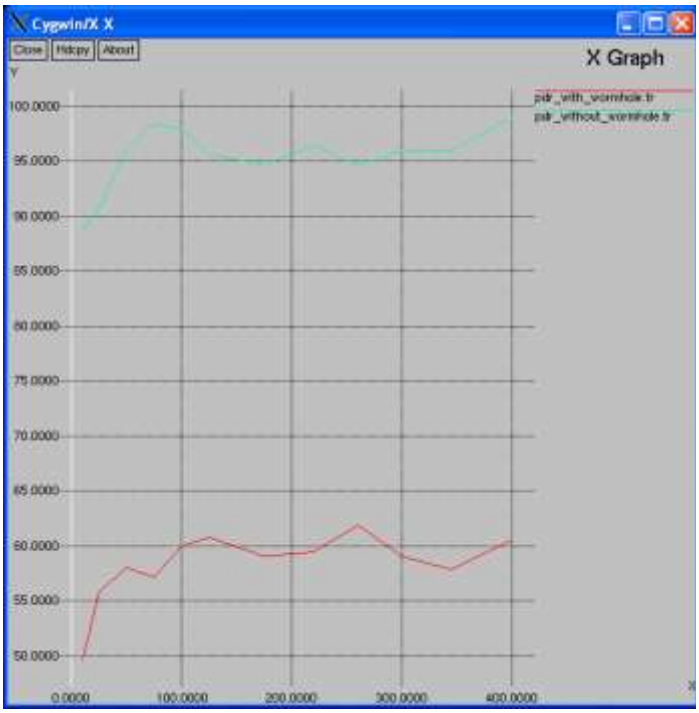
We have simulated our proposed work under NS2 simulator. The Network Simulator version 2 (ns-2) is a deterministic discrete event network simulator, initiated at the Lawrence Berkeley National Laboratory (LBNL) through the DARPA funded Virtual Inter Network Testbed (VINT) project [13,15]. It is worth noting that ns-2 is a research effort and not a commercial software release. The difference is that there are very few people in the ns project group compared to ordinary software, leading to difficulties in supporting all the users. That problem has lead to the solution of having a huge mailing list Ns-2 is made up of hundreds of smaller programs, separated to help the user sort through and find what he or she is looking for. Every separate protocol, as well as variations of the same, sometimes has separate files. Though some are simple, still dependent on the parental class. In ns 2 when we run the program two types of file created they are NAM file and TR file .the first one is Network Animator file which is use to visualize the simulation.TR file stands for trace file which keep records of various quantities. Gawk files are used to calculate various parameters these parameters are calculated by using TR file using this file we can calculate no. of sent packets, no. of received packets, PDR, and e to e delay packet loss.

## IX. Simulation Parameters:

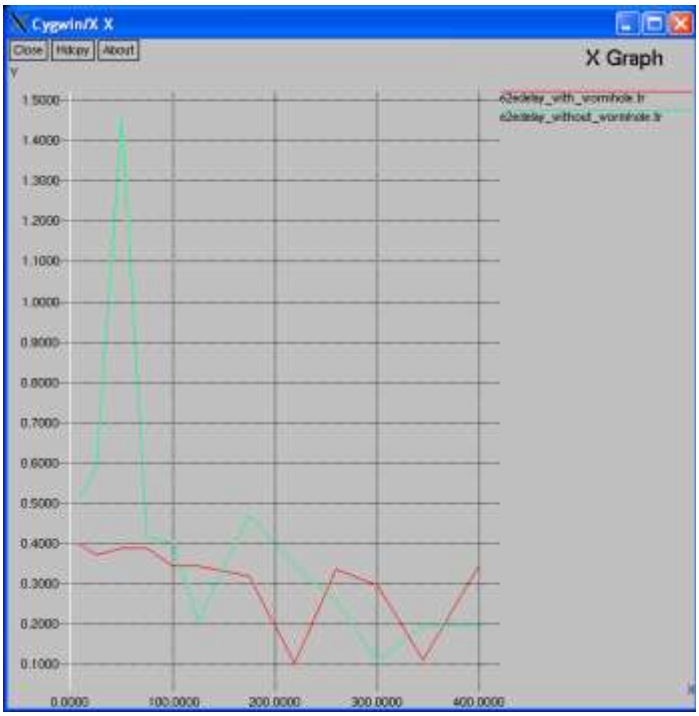
Table1 Simulation parameters values

| Parameter | value |
|---|---|
| Channel type | wireless |
| Protocols | AODV |
| Traffic type | CBR |
| Antenna | Omni Antenna |
| Source type | udp |
| Link Layer | LL |
| Number of mobile nodes | 50 |
| Nodes | 50 |
| Mac | 802_11 |
| X | 800 |
| Y | 600 |

## X. Results




Graph1. PDR with and without wormhole




Grpah2 E2E Delay with and without wormhole

## XI. Discussion:

Simulations have been performed to ensure that the proposed mechanism works and is feasible for wireless mesh networks. The first step was simulation of a wireless mesh network to demonstrate that networks with different radio technologies can communicate with each other here we have Xgraph of all simulated parameters with respect to our proposed work. With the help of these graphs we can comments that by proposing our method we have increased performance of the wireless mesh network .we have shown these graphs with respect to PDR, and E2E Delay. There are two types of scenarios that we have simulated first one is with respect to with wormhole while another one is with respect to without wormhole condition and by analyzing results from graphs we can conclude that by using this approach our performance has been improved.

## XII. Conclusion:

In this research paper we have simulated our proposed work in two scenarios one is under wormhole while another without wormhole when we simulated these scenarios under NS-2 we found that by introducing our algorithm performance of WMN improved. We completed this simulation on the basis of two parameters these are PDR and E2E Delay. By introducing this algorithm delay for packet delivering has been reduced to a significant value more over of it packets are dropped less in comparison to without approach applied so PDR also got increased .Graphs for PDR and E2E Delay have been calculated through Xgraph. We can extend this work further for analyzing other parameters like PDR, Jitter and for Network Efficiency. This approach can be further modified for other attacks in wireless mesh network.

## XIII. *References:*

[1] Yih-Chun Hu, *Member*, *IEEE*, Adrian Perrig, *Member*, *IEEE*, and David B. Johnson, *Member*, *IEEE,* "Wormhole Attacks in Wireless Networks" , in IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, VOL. 24, NO. 2, FEBRUARY 2006.

[2] Dhara Buch and Devesh Jinwala, "PREVENTION OF WORMHOLE ATTACK INWIRELESS SENSOR

NETWORK", in International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.5, Sep 2011.

[3] N.B. Salem and J.-P. Hubaux, "Securing Wireless Mesh Networks," *Wireless Comm.*, vol. 13, no. 2, 2006.

[4] I.F. Akyildiz, X. Wang, and W. Wang, "Wireless Mesh Networks: A Survey," *Computer Networks and ISDN Systems*, vol. 47, no. 4, 2005.

[5] Pirzada Gauhar Arfaat, Dr. A.H. Mir "The Impact of Wormhole Attack on the Performance of Wireless Ad-Hoc Networks" in IJCST Vol. 2, Issue 4, Oct. - Dec. 2011.

[6] Dezun Dong, Mo Li, et-al, "Worm Circle, Connectivity-based Wormhole Detection in Wireless Ad Hoc and Sensor Networks", 15th International Conference on Parallel and Distributed Systems, 2009.

[7] Stephen Glass, Vallipuram Muthukkumurasamy, "Detecting Man-in-the-Middle and Wormhole Attacks in Wireless Mesh Networks", IEEE publication, 2009.

[8] Khin Sandar Win, "Analysis of Detecting Wormhole Attack in Wireless Networks", Proceedings of world academy of science, engineering and technology. vol36, ISSN 2070-3740, Dec 2008.

[9] Mewada Shivlal and Singh Umesh Kumar, "Performance Analysis of Secure Wireless Mesh Networks", in *Research Journal of Recent Sciences* Vol. 1(3), 80-85, March (2012).

[10] Muhammad S. Siddiqui and Choong Seon Hong, Security Issues in Wireless Mesh Networks, IEEE International Conference on Multimedia and Ubiquitous Engineering **(2007).**

[11] Zhang W., Wang Z., Das S.K. and Hassan M., "Security Issues in Wireless Mesh Networks", In Book Wireless Mesh Networks: Architectures and protocols, New York, *Springer* **(2008).**

[12] Yih-Chun Hu, Adrian Perrig and David B. Johnson, "Packet Leashes: A Defense against Wormhole Attacks in Wireless Networks", in IEEE INFOCOM 2003.

[13] http://www.isi.edu/nsnam/ns/ns

[14] www.wikipedia.com

[15] http://www.ns2ultimate.com

.