International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 04 Issue: 05 | May -2017 www.irjet.net p-ISSN: 2395-0072

Efficient Detection and prevention of Wormhole Attacks in Wireless Mesh Network

Fayaz Ahamed Shaikh[1], Uttam Patil[2]

[1]Student, P.G. Department of Computer Science and Engineering, VTU/ KLE Dr M S Sheshgiri College of Engineering & Technology, Belguam, India, 9902760958 (e-mail: fayazmshaikh@gamil.com).
[2]Professor, P.G. Department of Computer Science and Engineering, VTU/ KLE Dr M S Sheshgiri College of Engineering & Technology, Belguam, India

---

Abstract - *Wireless Mesh Networking is a rising technology in order to offer an opportunity to construct a network that is able to grow in terms of coverage to present service access (i.e. internet access) for a large number of people with dissimilar needs. WMNs are weaker to wormhole attack (one out of much kind of attacks). In a usual wormhole attack, two or more malicious nodes plan jointly in establishing a tunnel by a well-organized communication medium. The aim of this paper is to explain a wormhole detection algorithm for WMNs which detect the wormholes by calculating neighbor list as well as directional neighbor list of the source node. The main aim of the algorithm is that it can offer approximate location of nodes and effect of wormhole attack on all nodes which is helpful in implementing countermeasures. The performance evaluation is complete in varying no. of wormholes in the network.*

Key Words: AODV(Ad hoc On-Demand Distance Vector), WMN(Wireless Mesh Networks), Wormhole attack, Wormhole Detection,Router

1. INTRODUCTION

WMN (Wireless Mesh Networks) is said to be a very optimistic technology as well as will play an ever more significant part in upcoming invention wireless mobile networks. Wireless Mesh Network is characterized by active self configuration, self organization, and self healing to allow speedy deployment, low cost, simple maintenance, reliable services, high scalability as well as attractive network facility, connectivity and flexibility.

The wireless technology is less maintenance, low price and speedily installable. According to the need of services a number of indoor and outdoor network technologies are designed. The wireless Mesh network is one of the essential technologies among different technologies. Because of its self-configuring and self-healing nature the (WMNs) wireless mesh networks are very valuable. Thus this WMN can be used for community networks, cellular mobile networks and business networks.

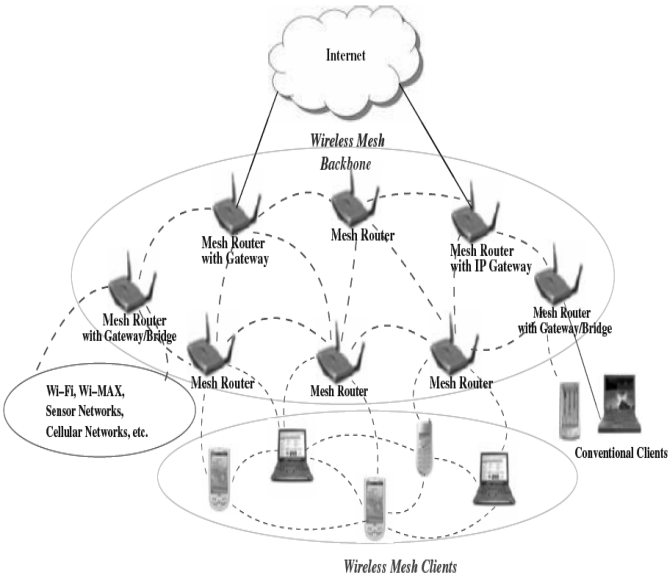

Figure 1.1 Wireless Mesh Network

Figure 1.1 shows a typical WMN is constitute of a set of stationary mesh routers (MRs) and a set of mesh clients to interact through mesh routers that form the mesh backbone.

Wireless Mesh Networks having 2 nodes: (i) mesh clients (ii) mesh routers. A wireless mesh router having extra routing features to support mesh network. By numerous network interface cards (NICs) a mesh router is usually equipped.

1.1Overview of WMNs Potential Attacks

To WMNs there are two sources of threats. First, external attackers not belong to the mesh network can add erroneous information or jam the communication. Second, from internal compromised nodes there are additional harsh threats come, since internal attacks are not as simple to stop as external attacks. The attack can be normal, i.e., the opponent misbehaves simply if misbehaving is helpful in conditions of cost, resource reduction or obtained excellence of service, if not it is malicious. Active and Passive attacks be able to be notable. Passive attacks plan to take information and within the network eavesdrop on the communication. In case of active attacks, the attacker injects as well as into the network modifies packets.

1.2 Aim and Objective of the Project

A big challenge in all kind of network is security. Network failure can cause by various types of attacks and threats in addition to they be able to change, disturb the routing data, updates as well as reduce the performance of the network. This project is supposed to simulate probable wormhole attack against WMNs with present counter trial against such attacks in a WMN.

The goal is to recommend a method for wormhole detection in wireless mesh network as well as performance estimation of projected method in the network by varying number of wormholes. Increase Throughput, minimize Packet Dropping.

As the WMN's are deployed in several places and need to be protected from attacks. WMN is vulnerable to many attacks because of the several constraints. Providing security and understanding the attacks in the network is of great need. By using the Mat Lab Simulation program, the attacks can be simulated. The attacks can be understood obviously and correct measures to identify and avoid the attacks can be taken by the simulation of the attack. It is also closer and cost effective to a real time scenario.

2 LITERATURE SURVEY

This section presents the review of past researches in WMN and Wormhole attack detection. The work done by the distinct research's as explained below:

In paper [1] provides the wormhole attack presents a major risk to the honesty of WMN as well as MANETs. A wormhole is a specific man-in-the-middle attack wherein the opponent connects the network of two or else distant regions. Stations nearby single stop of the wormhole emerge to be neighbors of stations on the additional. The existence of the wormhole subverts the network topology and therefore the algorithm of network routing need to undermine. Routes during the wormhole advantage as of lower hop-counts than legitimate routes as well as enhance the chance that traffic will be routed by the adversary. Once the wormhole is established the opponent is capable to carry out more attacks as well as perform thus by a little chance of detection.

This paper proposes finding of frame-relaying (wormhole and man-in-the-middle) attacks against wireless networks by a novel MAC-layer intrusion detection method. A little modify to the wireless MAC layer detects the existence of the adversary even before they contain proceeded to carry out additional, extra noticeable attacks. The proposed method is precise to wireless networks at the MAC layer as it exploits the utilize of positive acknowledgement.

In paper [2] proposes a mostly harsh security attack, known as the wormhole attack, has been introduced in the circumstance of ad-hoc networks. During the attacks a malicious node takes packets from one place in the network, as well as tunnels them to a different malicious node at a remote point, which replays them nearby. The tunnel is able to recognize in several special methods, such as packet encapsulation, during high powered communication or an out-of-band hidden channel for e.g. a wired link. This tunnel makes the tunneled packet appear any faster or with fewer number of hops compared to the packets transmitted above usual multi-hop routes. This creates the illusion that tunnel are very close to both of the two end points. This paper explains its threats and point to the crash of this attack and attack modes. From an attacker's point of view, we examine how to improve the wormhole attack and all of the attack's modes' benefits as well as appropriate conditions through introducing the concept of "complex wormhole attacks".

In paper [3] proposes, in passive attacks only eavesdrops upon packet contents by malicious node, as in active attacks it can modify, drop otherwise imitate legitimate packets. When these are performed in collusion the severity of such attacks increases multifold. A classic case of such a supportive attack is a wormhole within which a malicious node tunnels the packets starting from one end to a different end of the network. The tunnel basically emulates a shorter route through the network and so naive nodes favor to use it rather than vary longer routes. The benefit gained by the colluding nodes is clear as they are now for all purposes and intents, in charge of a more usage route during the network. The cost of such a wormhole on the network capable to be catastrophic, with in worst-case scenarios, can lead to a vertex slash in the network.

To identify and evade wormhole attacks we concern Dynamic Source Routing (DSR) protocol in a pure ad-hoc network. In the network each node maintains its own evaluation and autonomously executes the trust model concerning other nodes in the network.

In paper [4] explains in multihop wireless adhoc networks, collaboration among nodes to route all other's packets exposes these nodes to a broad choice of security attacks. The wireless ad-hoc networks look many security risks suitable to the vulnerability of the routing protocols. A mostly rigorous security attack to affects the adhoc network routing protocols, is identified as the wormhole attack. By one or more malicious nodes the wormhole attack is approved out as a two stage method launched. In the primary stage wormhole nodes attempt to attract legal nodes to send data through them with participating within the network. In the next stage, wormhole nodes can use the data and change the communication by mischievous. Within this paper Manet's as well as wireless adhoc networks we have simulated the wormhole attack. And then we discussed along with evaluated the impact on the network in comparing the outcome with and without wormhole attack. Using different scenarios the Wormhole attack was

simulated. Therefore on the respective networks we studied the collision of the wormhole attack. By special scenarios for evaluating the impact on wireless adhoc networks as well as MANET's the parameters like end to end delay, throughput as well as packet loss were calculated.

Within paper [5] explains about importance of Wireless Mesh Network and architecture, the WMN is a hopeful technology if the final mile broadband access. Within a WMN, the internet is able to access by a client during formed wireless mesh routers which are interrelated in a multi-hop style. WMN is a future technology that has the potential to deliver wireless local area network coverage, network connectivity and Internet broadband access, and for network customers and operators at low costs. Because of its rapid developing and growing of wireless technologies recently a communication network that have ever more attracted ISPs (Internet Service Providers). Wireless Mesh Network is a hopeful technology and gives high bandwidth network coverage. WMNs will really assist the users to be always-online, anytime, anyplace through connecting to wireless mesh routers. In addition, the mesh routers contain the bridge functionality to connect WMNs by different obtainable wireless networks such as wireless sensor, cellular, universal interoperability for microwave access (WiMAX), wireless-fidelity (Wi-Fi), WiMedia networks. Therefore, WMNs will send wireless services in support of a huge range of applications.

3 Design methodology

Every project has certain extremely important aspects and one of them is system design. It will define the different elements of a system such as the architecture modules and components. The main focus of the system design is to accomplish all needs and requirements of the project.

3.1 Mesh Routers

Mesh routers are primarily fixed devices. They are able to attain the similar coverage as a conservative router does through multi-hop technology and with much a lesser amount of power. Mesh networking is possible because of Mesh routers have extra routing functions. Even though they do not have wireless Network Interface Cards it's really assist the users through connecting them by wireless mesh routers throughout Ethernet. Therefore user is able to be for all time online, anytime as well as anywhere. Throughout bridge otherwise gateway functions they mix with special accessible wireless networks such as Wi-Fi 802.11 a,b,g , 802.11n as well as cellular.

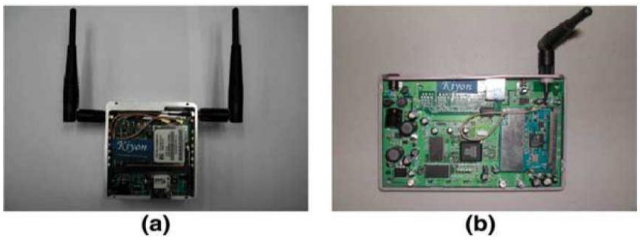

Figure 3.1: Examples of mesh routers based on special embedded systems: (a) PowerPC

3.2 Mesh Clients

Mesh clients be able to be stationary otherwise mobile. Mesh clients include essential mesh functions as well as they do not have bridge or gateway functionality but they can acts as a router. They simply contain single wireless interface. We contain huge range of devices that are able to acts like mesh clients.

Figure 3.2: Examples of mesh clients: (a) Wi- Fi IP Phone, (b) Wi-Fi RFID Reader, (c) Laptop (d) PDA.

3.2 WMN Architecture

Based on the functionality and node's network topology AWMN can be categories in three dissimilar network architectures. These categories are discussed in brief below.

3.2.1. Infrastructure of Wireless Mesh Networks

Within this category of design the network is created in linking dissimilar kind of nodes that are together clients as well as routers. Every node is at the similar stage as that of its peers. A communications in favor of clients that connect to them is form by including mesh routers.

Mesh routers are able to be connected to the Internet through gateway functionality and in the mesh network provides backbone for conventional clients.

For example: neighborhood and Community networks are able to build. The mesh routers are able to be located on top which provide as access position in favor of client whether they are utilizing it on the road or home users.

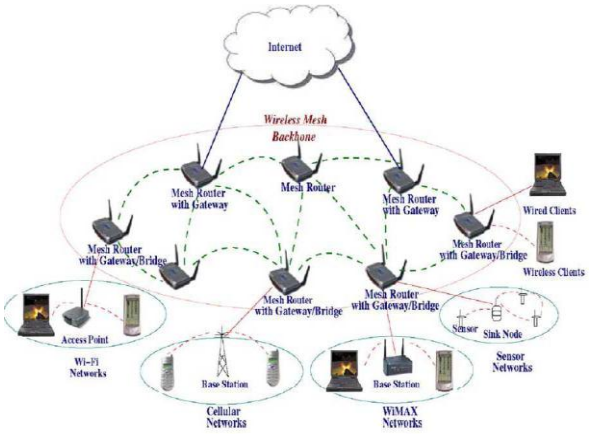

Figure 3.3: Infrastructure/backbone WMNs.

3.2.2. Client Wireless Mesh Networks

Among clients WMN provides the networks of peer to peer technology, the client nodes do the routing as well as providing end-user applications to customers as well as other design functionalities. The clients themselves do these tasks as well as maintain the network connectivity. Within this we contain end devices extra stressed than communications meshing. For performing usual networking functions we do not contain essential infrastructure client mesh resembles a MANET. Mesh router use not require for performing these types of functions.

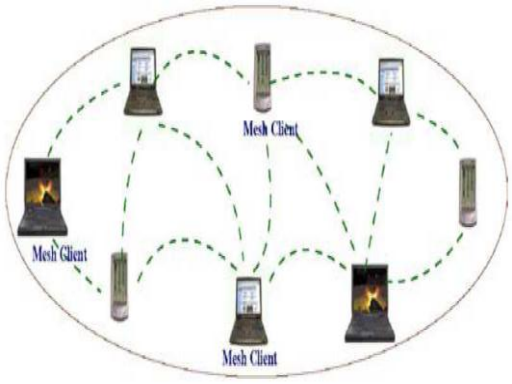

Figure 3.4: Client WMNs.

3.2.3. Hybrid WMNs

This is the mixture of together meshing architectures (client as well as infrastructure). Within Hybrid mesh by straight meshing clients with additional mesh clients or through mesh routers are able to access the network. Communications provides connectivity to additional networks like Wi-Fi, the Internet, sensor, WiMAX and cellular networks. The routing capabilities of clients give coverage within the WMN and enhanced connectivity. As the development of Wireless Mesh Networks depend greatly happening how it works by additional accessible wireless networking solutions, this design becomes most appropriate and extremely essential in WMNs.

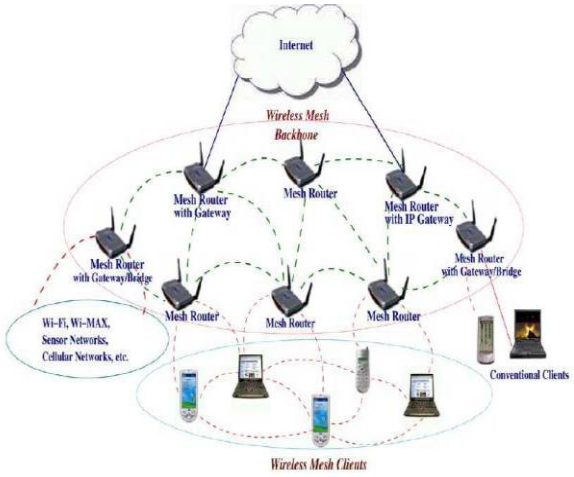

Figure 3.5: Hybrid WMNs

3.2.4 Ad hoc on-demand Distance Vector Routing Protocol (AODV)

For MANETs AODV is an extremely accepted routing protocol. It is an immediate routing protocol. On demand Routes are set up, and maintained just active routes. By this routing transparency get reduce, except suitable to the on-demand route system introduce little initial latency. Recently, for WLAN mesh networking an adaptation of AODV has been planned. For the detection of routes AODV uses a straightforward request–reply method. Hello messages can be use for connectivity information as well as on active routes signals connection breaks by fault messages.

3.2.5 Wormhole Attack Detection Algorithm

The proposed wormhole attack detection algorithm is:
1: Define Simulation parameters
X-Range, Y-Range of terrain area, Number of Nodes, Radio Range, Directional Range
2: Initialize the location of arbitrarily dispersed nodes.
3: Initialize the neighbor nodes
4: For every one node, initialize the array as well as for all direction apply the next clauses:
Clause 1: No node in this path of wormhole so the attack is meaningless.
Clause 2: At least single node in additional path is able to identify irregularity.
Seek within dissimilar five paths
5: Calculate average neighbor numbers, average faith neighbor num, separated num
6: Free the neighbor list as well as Key list.
7: Locate the distance of both the nodes.

3.2.5 Wormhole Attack Detection Flowchart

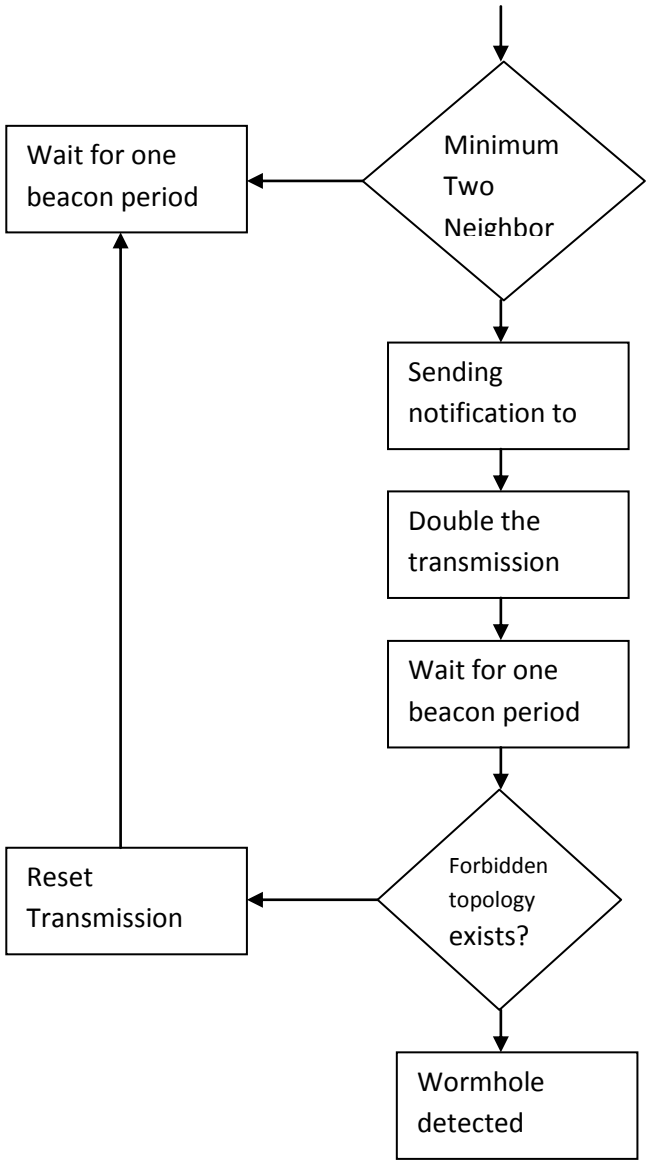

Figure 3.1 Detection Flowchart

3. RESULT ANALYSIS

Simulation Parameters

The scenario consists of 100 nodes in which up to three wormholes created. For our simulation the parameters arrangement are shown here:

PARAMETER	VALUE
Area	100 mtrx100 mtr
Number of Nodes	100
Radio Range	15 mtr
Node-placement	Uniform Random
Traffic Model	CBR
Wormholes	Up to 3
Routing Protocol	AODV

Table 4.1Simulation parameters

. Attack Attempts

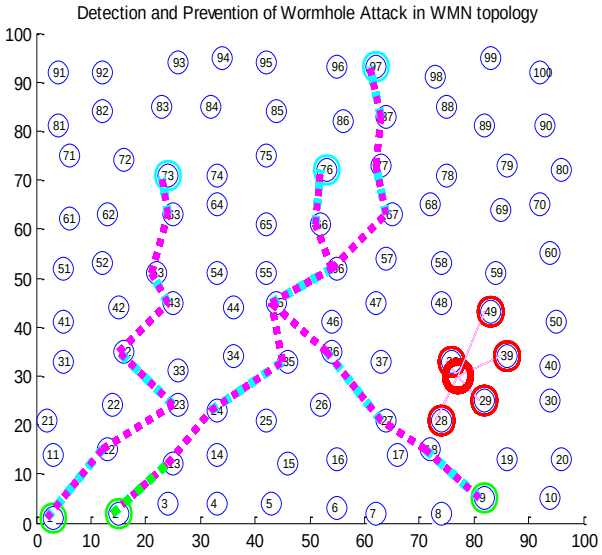

Fig 4.1: Wormhole Attack Attempt

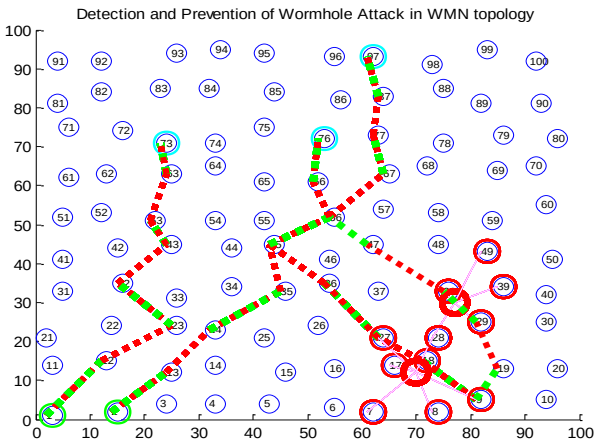

Figure 4.2 Path Change (Black) from 9 to 76 as Successful Attack

Following table shows number of attacks and the analysis parameters

No. of Attacks	Packet Drop (%)	PDR (%)	Through Put (kbps)
0	0.00	100.00	0.23
1	10.15	89.85	0.16
2	11.67	88.33	0.05

Table 4.2 Performance Analysis after each attack

Table 3.2 show packet delivery ratio (PDR) is 100% when no attack, as attack increases the PDR decreases, also through put decreased considerably.

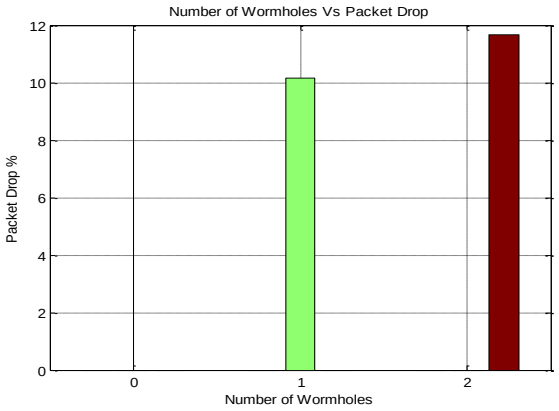

Figure 4.3 Packet Drop Analysis with change in number of wormholes

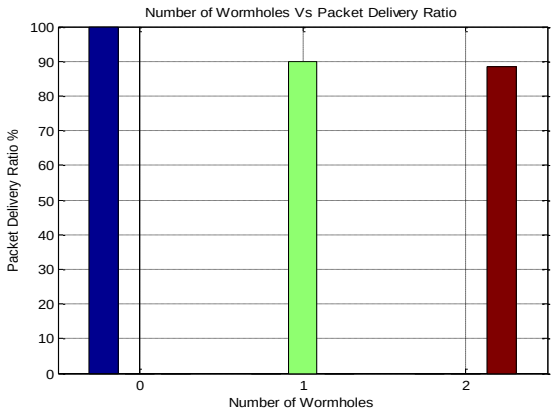

Figure 4.4 Packet Delivery ratios Analysis with change in number of wormholes

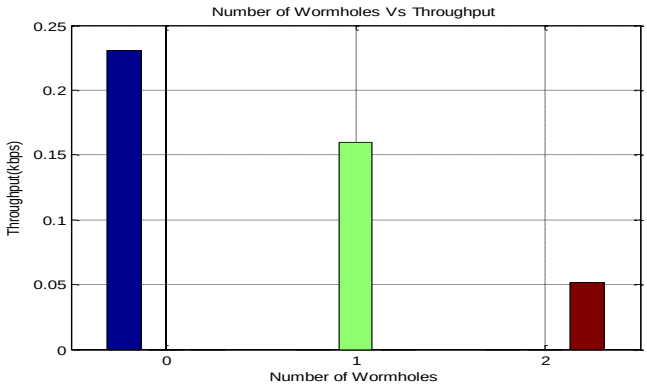

Figure 4.5 Throughput Analysis with change in number of wormholes

4 CONCLUSION

The wormhole attack is a major setback of wireless sensor technology. Hence, there is an utmost significance of overcoming this problem. The wormhole attack is a powerful attack that is able to have serious consequences on WMN protocols. An attacker who can carry out a victorious wormhole attack can reject service to big segments; disturb routing of a network, creation of unconnected component within a network. In the proposed we have analyzed results indicates that impact of wormhole attack is affected the throughput of packet ratio in terms of packet received, packet sent and packet drop at the nodes in WMN.

The Proposed algorithm is simple and efficient in detecting the attack. The results of wormhole attack on the network have exposed the simulation outcome. We guess this algorithm will assist to protect wireless mesh network against wormhole attacks. The performance is analyzed through changing number of wormholes showing reliable outcome.

ACKNOWLEDGEMENT

I have been bestowed the privilege of expressing my gratitude to everyone who helped me in completing the dissertation work. The sense of Contentment and elation that accompanies the successful completion of my project and its report would be incomplete without mentioning the names of the people who helped me in accomplishing this work.

I express my sincere gratitude to my guide Prof. Uttam Patil for his valuable guidance and P.G. Coordinator Dr. V.S.Malemath for his help during the course of project. Without his advice and cooperation I would not have succeeded in my endeavor. His thoughtfulness and understanding were vast and thoroughly helpful in successful completion of my Project. I am immensely thankful to Head of the Department Prof. B.A.Patil for his encouragement and providing lab facilities needed for accomplishing of this project.

I would like to express my sense of gratitude to our Principal Dr. Basavaraj Katageri, for providing healthy environment in the college, which helped in concentrating on the task.

REFERENCES

[1] Stephen Glass, Vallipuram Muthukkumurasamy ,Marius Portmann. Detecting Man-in-the-Middle and Wormhole Attacks in Wireless Mesh Networks , 2009 International Conference on Advanced Information Networking and Applications, © 2009 IEEE.

[2] Marianne Azer,Sherif El-Kassas,Magdy El-Soudani. A Full Image of the Wormhole Attacks Towards Introducing Complex Wormhole Attacks in wireless Ad Hoc Networks, (IJCSIS) International Journal of Computer Science and Information Security, Vol. 1, No. 1, May 2009.

[3] Shalini Jain, Dr.Satbir Jain. Detection and prevention of wormhole attack in mobile adhoc networks, International Journal of Computer Theory and Engineering, Vol. 2, No. 1 February, 2010.

[4] Pirzada Gauhar Arfaat, Dr. A.H. Mir.The Impact of Wormhole Attack on the Performance of Wireless Ad-Hoc Networks, ISSN: 0976-8491.

[5] Mojtaba Seyedzadegan, Mohamed Othman, Borhanuddin Mohd Ali and Shamala Subramaniam. Wireless Mesh Networks: WMN Overview, WMN Architecture, 2011 International Conference on Communication Engineering and Networks IPCSIT vol.19 (2011) © (2011) IACSIT Press, Singapore.

[6] Saurabh Upadhyay and Brijesh Kumar Chaurasia. Impact of Wormhole Attacks on MANETs, International Journal of Computer Science & Emerging Technologies (E-ISSN: 2044-6004) 77 Volume 2, Issue 1, February 2011.