Detection of Performance Using Black Hole Attack

[1]Sonia Sharma, [2]Sandeep Mehla
[1]Research Scholar, [2]Assistant Professor
SBIET, Department of Computer Science & Engineering
Kurukshetra University

***Abstract* - Security in Mobile Ad-Hoc Network (MANET) is the most important concern for the basic functionality of network. Availability of network services, confidentiality and integrity of the data can be achieved by assuring that security issues have been met. MANET often suffer from security attacks because of its features like open medium, changing its topology dynamically, lack of central monitoring and management, cooperative algorithms and no clear defense mechanism. These factors have changed the battle field situation for the MANET against the security threats.**

***Keywords*— Manet,Protocol,Black Hole Attack,Ns2**

I. INTRODUCTION

MANETs work without a centralized administration where the nodes communicate with each other on the basis of mutual trust. This characteristic makes MANETs more vulnerable to be exploited by an attacker inside the network. Wireless links also makes the MANETs more susceptible to attacks, which make it easier for the attacker to go inside the network and get access to the ongoing communication. Mobile nodes present within the range of wireless link can overhear and even participate in the network.

MANETs must have a secure way for transmission and communication and this is a quite challenging and vital issue as there is increasing threats of attack on the Mobile Networks. Security is the cry of the day. In order to provide secure communication and transmission, the engineers must understand different types of attacks and their effects on the MANETs. Wormhole attack, Black hole attack and Denial of Service (DoS) [2], selfish node misbehaving, impersonation attack are kind of attacks that a MANET can suffer from. A MANET is more open to these kinds of attacks because communication is based on mutual trust between the nodes, there is no central point for network management, no authorization facility, vigorously changing topology and limited resources.

II. ROUTING PROTOCOL

Mobile Ad-Hoc Network is the rapid growing technology from the past 20 years. The gain in their popularity is because of the ease of deployment, infrastructure less and their dynamic nature. MANETs created a new set of demands to be implemented and to provide efficient and better end-to-end communication. MANETs works on TCP/IP structure to provide the means of communication between communicating work stations. Work stations are mobile and they have limited resources, therefore the traditional TCP/IP model needs to be refurbished or modified, in order to compensate the MANETs mobility to provide efficient functionality. Therefore the key research area for the researchers is routing in any network. Routing protocols in MANETs are a challenging and attractive tasks, researchers are giving tremendous amount of attention to this key area.

Routing protocols in MANETs are classified into three different categories according to their functionality

1. Reactive protocols
2. Proactive protocols
3. Hybrid protocols

1. Reactive Protocols

Reactive protocols are also known as on demand driven reactive protocols. The fact they are known as reactive protocols is, they do not initiate route discovery by themselves, until they are requested, when a source node request to find a route. These protocols setup routes when demanded [1, 2]. When a node wants to communicate with another node in the network, and the source node does not have a route to the node it wants to communicate with, reactive routing protocols will establish a route for the source to destination node. Normally reactive protocols

- Don't find route until demanded
- When tries to find the destination "on demand", it uses flooding technique to propagate the query.
- Do not consume bandwidth for sending information.
- They consume bandwidth only, when the node start transmitting the data to the destination node.

2. Proactive or Table-Driven routing protocols

In proactive protocols, each node maintains individual routing table containing routing information for every node in the network. Each node maintains consistent and current up-to-date routing information by sending control messages periodically between the nodes which update their routing tables. The proactive routing protocols use link-state routing algorithms which frequently flood the link information about its neighbors. The drawback of proactive routing protocol is that all the nodes in the network always maintain an updated table. Some of the existing proactive routing protocols are DSDV [4] and OLSR [5], [6].

3. Hybrid Routing Protocol

Hybrid routing protocol combines the advantages of both proactive and reactive routing protocols. The routing is initially established with some proactively prospected routes and then serves the demand from additionally activated nodes through reactive flooding. Some of the existing hybrid protocols are ZRP[7] and TORA.

III. BLACK HOLE ATTACK

MANETs face different securities threats i.e. attack that are carried out against them to disrupt the normal performance of the networks. In black hole attack, a malicious node uses its routing protocol in order to advertise itself for having the shortest path to the destination node or to the packet it wants to intercept [4, 8 and 9].This hostile node advertises its availability of fresh routes irrespective of checking its routing table. In this way attacker node will always have the availability in replying to the route request and thus intercept the data packet and retain it [1]. In protocol based on flooding, the malicious node reply will be received by the requesting node before the reception of reply from actual node; hence a malicious and forged route is created. When this route is establish, now it's up to the node whether to drop all the packets or forward it to the unknown address [5].

A Black hole Attack has two properties:

- The node exploits the ad hoc routing protocol, such as AODV, to advertise itself as having a valid route to a destination node, even though the route is spurious, with the intention of intercepting packets.
- The node consumes the intercepted packets.

IV. RELATED WORK

Muhammad Shoaib Siddiqui, Syed Obaid Amin, Jin Ho Kim [1] proposed a Secure Multi-Path Hybrid Routing Protocol for Wireless Mesh Network. Wireless Mesh Network is a new and promising paradigm in wireless networks that allows network deployment at a much lower cost. Routing is the main research issue in the development of Wireless Mesh Networks. Many of the routing approaches have been borrowed from Wireless Mobile Ad hoc Network to achieve routing solutions in Wireless Mesh Networks but these approaches are not ideal or optimal. These routing protocols can be distinguished as proactive and reactive routing protocols. As a Wireless Mesh Network is itself a hybrid network solution among ad hoc and static networks, a hybrid routing approach is required. In this paper, they provide the secure multi-path version of this hybrid routing protocol, which enhances the reliability in the network, provide secure routing and has efficient techniques of finding alternate routes when a route is lost. They provide comparisons of this routing protocol with other routing protocols that are available for Wireless Mesh Networks.

In this paper, they have presented a secure multi-path routing protocol for wireless mesh network. Their routing scheme is hybrid in nature as it uses both proactive and reactive approach in finding the routes to the destination. Their security mechanism also sufficiently decreases the control overhead induced by a secure routing protocol. MHRP provide better data throughput with less route latency and overhead and consume less amount of energy at each node. It efficiently utilizes the characteristics of WMN to find alternate routes and provide reliable secure communication.

Asad Amir Pirzada, Ryan Wishart and Marius Portmann[2] proposed an Congestion-Aware Routing In Hybrid Wireless Mesh Network. Multi-radio Wireless Mesh Networks (WMN) are gaining lot of popularity owing to their increased application to community and public safety networks. WMNs form a static wireless backhaul to provide connectivity to mobile clients. The wireless medium, being shared and contended for, creates a number of hurdles including congestion, interference and noise. Multiradio nodes can take advantage of the wider frequency spectrum. However, current mesh technologies employ a simplistic approach by assigning one channel for client servicing and another for the backhaul network. The improper reuse of the same channel across multiple hops causes extensive co-channel interference leading to lower bandwidth. The problem is aggravated in a hybrid WMN where the mobile clients act as routers for other clients. In this paper, they propose a congestion aware routing protocol, which can successfully establish channel diverse routes through least congested areas of a hybrid WMN. The prime advantage of the protocol is its ability to discover optimal routes in a distributed manner without the requirement of an omniscient network entity. Simulation results show that the congestion aware routing protocol can successfully achieve a high packet delivery ratio with lower routing overhead and latency in a hybrid WMN.

Hybrid Wireless Mesh Networks, which present the most versatile form of mesh technology, enable mobile Mesh Clients to connect to a high speed wireless backhaul network formed using static Mesh Routers. A major advantage of the Hybrid Mesh Network is its ability to support the backhaul using Mesh Clients in addition to the Mesh Routers. A common problem observed in these networks is the performance degradation over multiple wireless hops. This occurrence is generally caused due to intra-flow and inter-flow co-channel interference. Although the Mesh Routers are equipped with multiple radios tuned to orthogonal channels, minimal effort is made to achieve channel diversification on a per flow basis. This in turn induces extensive contention for the physical medium causing significant packet losses. In this paper, they have proposed a routing protocol with a channel diverse and congestion aware metric. This metric assures channel diversity on a per flow basis. In addition, it utilizes the local congestion information in scenarios where optimal channel diversity cannot be assured. The simulation results indicate that the routing protocol is able to achieve a significantly high packet delivery rate with extremely low latency in a Hybrid Wireless Mesh Network.

Uyeng trang and Jin Xu. [3] Proposed two fundamental approaches to multicast routing: shortest path trees (SPTs) and minimum cost trees (MCTs). The SPT algorithms minimize the distance (or cost) from the sender to each receiver, whereas the MCT algorithms minimize the overall cost of the multicast tree. Due to the very large scale and unknown topology of the Internet, computing MCTs for multicast routing in the Internet is a very complex problem. As a result, the SPT approach is the more commonly used method for multicast routing in the Internet, because it is easy to implement and gives minimum delay from the

sender to each receiver, a property favored by many real-life applications. Unlike the Internet, a wireless mesh network (WMN) has a much smaller size, and its topology can be made known to all nodes in the network. This makes the MCT approach an equally viable candidate for multicast routing in WMNs. However, it is not clear how the two types of trees compare when used in WMNs. In this article we present a simulation- based performance comparison of SPTs and MCTs in WMNs, using performance metrics, such as packet delivery ratio, end-to-end delay, and traffic impacts on unicast flows in the same network.

The results shows that MST and MNT algorithm produces longer path than SPT algorithm because of this packet delivery rate of MST and MNT are lesser than SPT and average end to end delay in SPT is better as compared to MST and MNT due to shorter distance between source and destination. Result also shows that performance difference between SPT and MST/MNT increases as the number of nodes increases. The only drawback in SPT is that average packet delivery rate of the unicast flow is less in SPT only when traffic load is there because more nodes are involved in data forwarding task causing collision.

Youiti Kado, Azman Osman Lim, and Bing Zhang [4] analyzed an Of Wireless Mesh Network Routing Protocol For Push-to-Talk Traffic. Wireless mesh networks (WMNs) are becoming well-known as a new broadband Internet access technology through multihop transmission nowadays. With the tremendous popularity of the group communication, such as Push-to-Talk service, the need to deliver the traffic of Push-to-Talk over WMNs is becoming important. Since the Push-to-Talk traffic over WMNs is delay-sensitive traffic, a proactive routing protocol that keeps routes continuously updated is ideally best-suited protocol. Among the proactive routing protocols, a tree-based routing (TBR) protocol is a viable routing protocol for WMNs because traffic that is directed to/from a wired network can be well-handled via a portal (a root). However, the performance of TBR protocol can be degraded rapidly when the number of group talking increases, which also leads to the intra-mesh traffics increases in the network. To mitigate this problem, they proposed a centralized tree-based routing protocol, which enables the root to provide the best metric route for intra-mesh traffics. In other words, the proposed protocol can disperse the intra-mesh traffics around the root when an overwhelming traffic volume occurred. Their simulation studies reveal that the proposed protocol outperforms both AODV and TBR protocols in terms of packet delivery ratio, average end-to-end delay, and data throughput as the number of active users becomes larger.

V. PURPOSED WORK

MANET is evaluated based on reactive routing protocol like Ad-Hoc On Demand Distance Vector (AODV) and its effects are elaborated by stating how this attack disrupt the performance of MANET. Very little attention has been given to the fact to study the impact of Black Hole attack in MANET using Reactive, Proactive and Hybrid Protocols and to compare the vulnerability of both these protocols against the attack. There is a need to address for three protocols under the attack, as well as the impacts of the attacks on the MANETs. This thesis analyzes Black Hole attack in MANETs using AODV, DSDV and TORA which are reactive, proactive and hybrid routing protocol respectively in nature.

MANET Model

A MANET of 50 nodes with a simulation time of 50 seconds was considered. The mobile nodes were placed on a 1000 X 1000 flat grid. AODV, DSDV and TORA were used as the routing protocols. Thus, 50 different nodes were involved in the communication. The mobility of the nodes is depend on the Random Way Point Model.

MANET Models are defined with help of two models:

1. Mobility Model
2. Traffic model

5.1.1 Mobility Model

An important factor in mobile ad-hoc network is mobility of nodes, which is defined by speed, direction and rate of change. Mobility in the physical world is unpredictable, often unpredictable and it has a dramatic effect on protocols developed to support node movement. Mobility model represents the movement of mobile users and how their location, velocity and acceleration change over time. Such models are frequently used for simulation purpose when new communication or navigation techniques are investigated. For the MANET, the topology configurations used is: 1000 m x 1000 m field with 50 nodes. At a specified time, each mobile node starts its journey from current location to a specified destination with a chosen speed (depending on the mobility scenario). Once the destination is reached, a new destination is targeted. There is no fixed pause time. If the node reaches the destination ahead of its next move, it pauses; else, it continues to move. Identical mobility model was used in simulations across protocols to yield fair result.

Currently there are two types of mobility models used in simulation of networks:

- Trace model - Traces are those mobility patterns that are observed in real life systems. Traces provide accurate information, especially when they involve a large number of participants and an appropriately long observation period.
- Synthesis models - However, new network environment i.e ad-hoc networks are not easily modeled if traces have not yet been created. In this type of simulation it is necessary to use synthetic models. Synthetic means to realistically node movement, but without using network traces.

  Seven different synthetic entity mobility models based on random directions and speed are being discussed:

  1. Random Walk Mobility Model: A simple model based on random directions and speed.
  2. Random Waypoint Mobility Model: A model based on random waypoints and random speeds that includes pause times between changes in destination and speed.
  3. Random Direction Mobility Model: A model that forces mobile nodes to travel to the edge of simulation area before changing direction and speed.

4. A Boundless Simulation Area Mobility Model: A model that converts a 2D rectangular simulation area into torus-shaped simulation area.
5. Gauss- Markov Mobility Model: A model that uses one tuning parameter to vary the degree of randomness in mobility pattern.
6. A Probabilistic Version of Random Walk Mobility Model: A model that utilizes a set of probabilities to determine the next position of a mobile node.
7. City Section Mobility Model: A simulation area that represents streets within a city.

5.1.2 Traffic Model

Continuous bit rate (CBR) traffic source were used. The CBR traffic, once started, continued throughout the simulation. 50 sources –destination pairs are chosen in such a manner that they are spread across the network and the path between them changes often. The hop distance of some paths is less and some is more. The forwarding nodes that participate in data plane operation (i.e. routing) were chosen from nodes that handle multiple traffic at some point in time. At different pause time different traffic model were used like TCP, UDP etc. For Fair results these same traffic were used at that particular pause time in different scenarios.

Simulation Parameters

The communication pattern randomly created by the setdest tool defined in ns2 simulator. The tool contains following arguments. The Simulation Parameters which are used in my thesis work are shown in table 1.

Table 1 Simulation Parameters

Parameter	Value
Simulation Time	50 Sec
No. of Nodes	50
No. of Receivers	50
Traffic Type	CBR
Pause Time	10 Sec
Maximum X-coordinate value	1000 M
Maximum Y- Coordinate value	1000 M
Packet Size	512 byte
MAC Protocol	802.11
Mobility Model	Random Waypoint
Routing Protocols	AODV,DSDV,TORA
Observation Parameters	EED, Throughput, PDF

End-To-End Delay

For End-To-End delay, when the packet is send from node 1 to node 2 then start time of packet is subtracted from end time. The performance of protocol is better whose end-to-end delay is less than other protocol.

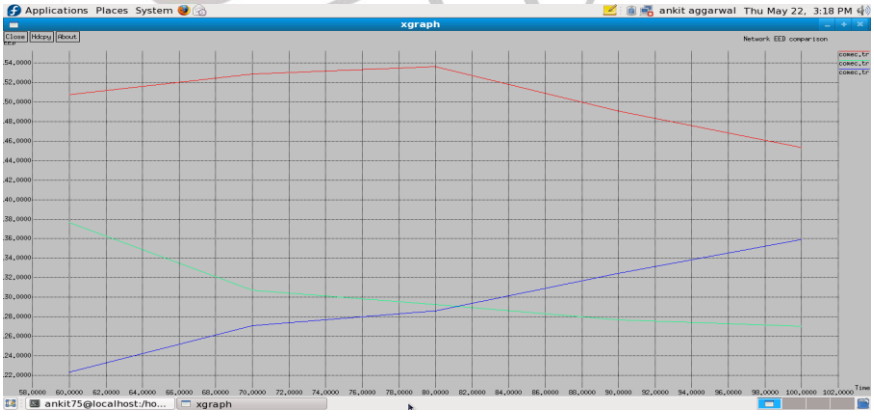

Fig 1

Throughput

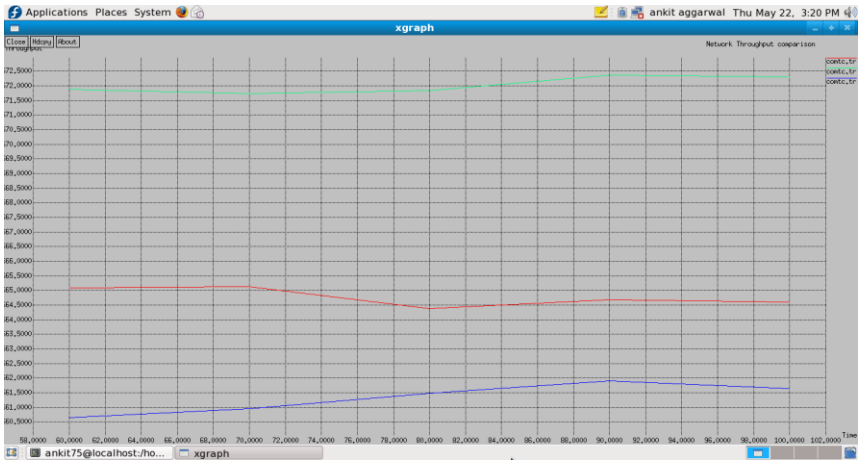

Fig 2

Average throughput of each routing protocols are obtained with probably same start and end time. It is the ratio of total amount of data which reaches the receiver from the sender to the time it takes for the receiver to receive the last packet. It is represented in bits per second or packets per seconds. The protocol whose average throughput is better, perform better. Same traffic models are used at different pause time for different protocol for fair results

Packet Delivery Fraction

Packet Delivery Fraction is calculated for each routing protocol. It is the percentage of number of packets received by the destination which are originated by source. The protocol which has better PDF, performs better.

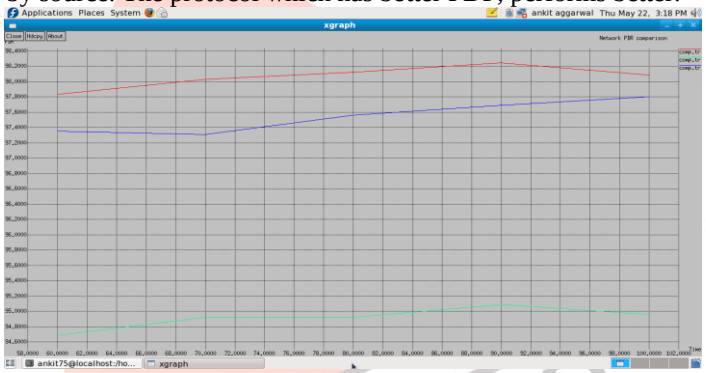

Fig 3

VI. CONCLUSION

Performance comparison of routing protocol in MANET is one of the important aspects. In this paper I have analyzed the behavior and different performance matrices for MANETs using different protocols (AODV, DSDV and TORA) and compared their performance matrices, like End to end delay, Packet delivery Fraction and Throughput with black hole attack.

Other types of attacks such as Wormhole, Jellyfish and Sybil attacks are needed to be studied in comparison with Black Hole attack. They can be categorized on the basis of how much they affect the performance of the network. Black Hole attack can also attack the other way around i.e. as Sleep Deprivation attack

REFERENCES

[1] Muhammad Shoaib Siddiqui, Syed Obaid Amin, Jin Ho Kim, "Secure Multi-Path Hybrid Routing Protocol for Wireless Mesh Network" {1-4244-1513-06/07/©2007 IEEE}

[2] Asad Amir Pirzada, Ryan Wishart and Marius Portmann, "an Congestion-Aware Routing In Hybrid Wireless Mesh Network "{ 1-4244-1230-7/07/© 2007 IEEE}

[3] Uyeng trang and Jin Xu,"Fundamental approaches to multicast routing "{0163-6804/07/$20.00 © 2007 IEEE}

[4] Youiti Kado, Azman Osman Lim, and Bing Zhang, "Analysis Of Wireless Mesh Network Routing Protocol For Push-to-Talk Traffic "{ 1-4244-1251-X/07/©2007 IEEE.}

[5] Miguel Elias M. Campista , Lu´ıs Henrique M. K. Costa, "WPR*:* A Proactive Routing Protocol Tailored to Wireless Mesh Networks"{ 978-1-4244-2324-8/08/© 2008 IEEE.}

[6] Azzedine Boukerche, Lucas Guardalben and Joao B. M. Sobral, "Analyzed an Performance Evaluation of OLSR and AODV Routing Protocols Using a Self-Configuration Mechanism for Heterogeneous Wireless Mesh Networks"{ 978-1-4244-2413-9/08/©2008 IEEE}

[7] Sheenu Sharma, Roopam Gupta, "Analyzed an Black hole Attack in AODV Routing Protocol" India, Journal of Engineering Science and Technology Vol. 4, No. 2 (2009) 243 – 250 © School of Engineering, Taylor's University College.

[8] Dong-Won Kum, Jin-Su park, You-Ze Cho, Byoung-Yoon Cheon and Daejea Cho., "Proposed an Mobility –Aware Hybrid Routing Approach For Wireless Mesh Network"{ 978-0-7695-4092-4/10 © 2010 IEEE}

[9] Amitangshu Pal and Asis Nasipuri, "Analysis of Quality Aware Anycast Routing Protocol For Wireless Mesh Network"{978-1-4244-5638-3/10/©2010 IEEE}