RESEARCH ARTICLE OPEN ACCESS

Optimization of Number of Nodes for AODV, OLSR And ZRP Protocols with and Without Black Hole Attack in MANET by Using Taguchi Method

Sukhman Sodhi [1], Rupinder kaur Gurm [2], Harsimran Singh Sodhi [3]
Research Scholar [1], Assistant Professor [2] & [3]
RIMT-IET, Mandi Gobindgarh [1] & [2]
Chandigarh University, Mohali [3]
India

ABSTRACT
MANET is used in various fields because of its low cost and ease of development. But due to its open medium and lack of infrastructure, it becomes vulnerable to Black hole attack. Black hole attack and other noise factors present in the network effects the data transmission and as per the advancements in the present data transfer technology scenario, the optimisation of data transfer parameters are of great importance to meet the recent demands. Therefore this paper is focused to optimize the number of nodes so in order to obtain the highest data transmission with least end to end delay for AODV, OLSR and ZRP protocols with and without black hole attack in MANET. In order to conduct no of experiments taguchi orthogonal L8 matrix has been formulated by using MINITAB 16 software. Afterword's Regression testing of various effecting parameters has been done in order to examine the significance of whole process.

Keywords: - MANET, AODV, OLSR, ZRP, Black hole and Taguchi

I. INTRODUCTION

MANET stands for mobile Ad hoc network; it is a temporary network between mobile devices. Mobile devices are the devices that can move from one place to another place like cell phones, PDA, laptops etc. In MANET all nodes are connected with wireless link. MANET nodes are equipped with Omni – directional antennas through which it transmit and receive the signals. At a given point in a time, depending on the parameters like node's position, transmitter and receiver coverage pattern, transmission power level and co – channel interference levels, a wireless connectivity in the form of random, multi hop graph or ad hoc networks exists between the nodes. This ad hoc topology may change with time as the nodes move or adjust their transmission and reception parameters. MANET nodes perform the routing among themselves .Therefore the nodes depends on ne another to forward packets to the destination.

II. APPLICATIONS

1. Military Battlefield:
Military equipment now routinely contains some sort of computer equipment. Ad- hoc networking would allow the military to take advantage of commonplace network technology to maintain an information network between the soldiers, vehicles, and military information headquarters. The basic techniques of ad hoc network came from this field.

2. Commercial Sectors:
Ad hoc can be used in emergency/rescue operations for disaster relief efforts, e.g. in fire, flood, or earthquake. Emergency rescue operations must take place where non-existing or damaged communications infrastructure and rapid deployment of a communication network is needed. Information is relayed from one rescue team member to another over a small hand held. Other commercial scenarios include e.g. ship-to-ship ad hoc mobile communication, law enforcement, etc.

3. Local Levels:
Ad hoc networks can autonomously link an instant and temporary multimedia network using notebook computers or palmtop computers to spread and share information among participants at e.g. conference or classroom. Another appropriate local level application might be in home networks where devices can communicate directly to exchange information. Similarly in other civilian environments like taxicab, sports stadium, boat and small aircraft, mobile ad hoc communications will have many applications.

4. **Personal Area Network (PAN):**

Short-range MANET can simplify the intercommunication between various mobile devices (such as a PDA, a laptop, and a cellular phone). Tedious wired cables are replaced with wireless connections. Such an ad hoc network can also extend the access to the Internet or other networks by mechanisms e.g. Wireless LAN (WLAN), GPRS, and UMTS. The PAN is potentially a promising application field of MANET in the future pervasive computing context.

III. BROADCASTING APPROACHES IN MANET

1. **Unicasting:** Sending a message from a source to a single destination.
2. **Multicasting:** Sending a message from a source to a set of destinations.
3. **Broadcasting:** Flooding of messages from a source to all other nodes in the specified network.
4. **Geocasting:** Sending a message from a source to all nodes inside a geographical region.

IV. ROUTING PROTOCOLS

The process of sending and receiving data from one node to another node is done with the help of routing protocols. In MANET each node works as a router. The Chief goal in ad hoc network is to create an accurate and capable route among couples of nodes and to make sure that the proper and timely release of packets. The routing protocols for MANET can be categorised into three types according to procedure used for route discovery and route maintenance: reactive or on – demand, proactive or table driven and hybrid routing protocols.

1.Reactive Routing Protocols

Reactive Routing protocols are on demand routing protocols in which route is required, when its demand for the data packets. At any time, if source wants to send message to receiver, then the protocol create a path as soon as when demand for the route. Ad hoc On-Demand Distance Vector Routing (AODV), Cluster based Routing Protocols (CBRP) and Dynamic Source Routing Protocol (DSRP) are On-Demand Routing protocols.

AODV

AODV have some combine properties of DSR and DSDV. It is based on Bellman-ford Distance Algorithm. AODV always discover a route source to destination only on-demand. It used route finding procedure and routing tables for maintaining route information. AODV used REEQ AND RREP for communication. A RREQ holds the senders' address, the address of the wanted node and the last sequence number inward starting that node, if there is present one.

The receipt node checks if it has a route to the particular node, if there exists a route and the sequence-number to set up a fresh route. The node response to the requesting by transfer a route replies (RREP). But on the other hand supply a route does not stay alive the receipt node sends a RREQ itself to attempt to discover a route for the request node .AODV perform both unicast and multicast routing and it preserve a path while needed for communication.

2. Proactive Routing Protocols

Proactive Routing protocols are table driven and there is require retaining regular up-to-date routing information about the every node inside the network and it stores the entire information within route table in the type of cache .Destination Sequenced Distance Vector (DSDV) routing protocol, Global State Routing (GSR), Wireless Routing Protocol (WRP), Zone Based Hierarchical Link State Routing Protocol (ZHLS) and Clustered Gateway Switch Routing Protocol (CGSR) are table driven routing protocols .

OLSR

OLSR is a hop by hop proactive routing protocol. It is optimizations of clean connections state algorithm in ad hoc networks. The routes are always all the time at once presented when required suitable to its proactive nature [10]. OLSR used multipoint relay (MPR). MPR are responsible for generating and forwarding topology information. OLSR always need to maintain routing tables. OLSR has three types of control messages, Hello, Topology Control (TC), and Multiple Interface Declaration (MID).

1. **Hello:** OLSR makes use of "Hello" messages to find it is one hop neighbours and it is two hop neighbours through their responses. This control message is transmitted for sense the neighbour and used for MPR calculation.

2. **Topology Control:** OLSR uses topology control (TC) messages along with MPR forwarding to

disseminate neighbour information throughout the network.

3. **Multiple Interface Declaration:** MID message includes the record of every IP addresses use by every node in the network. Every single nodes running on OLSR broadcast messages on extra than single interface.

4. **Multi Point Relaying:** MPR are used nodes to transmit route message. The choice of MPR is base on HELLO communication send between the neighbour nodes.

3. Hybrid Routing Protocols

Hybrid routing protocol have both the combines feature of Reactive and Proactive Routing protocols. It decreased the latency in reactive protocol and reduce the control overhead of proactive routing protocols. This protocol is based on hierarchical or layered system structure. Temporally ordered routing algorithm (TORA) and Zone routing protocol (ZRP) are Hybrid routing protocols.

1. ZRP

The Zone Routing protocols combine the feature of both reactive and proactive protocol into Hybrid Routing Protocol. ZRP is adaptive in nature and it depends on the present organization of network. As the name infer ZRP is based on idea of the zone. A routing zone is distinct for all nodes, and the zones of adjacent nodes partially cover one by one .ZRP can be considered like a flat protocol. Zone Routing Protocol consists of numerous components, which simply jointly offer the full routing advantage of ZRP, each component work by itself. Components of ZRP are: IARP, IERP and BRP.

1. ARP: The first protocol of ZRP is the IARP (Intra zone Routing Protocol). This protocol is used to
Communicate through the inner nodes of its zone and is partial by the zones radius suitable to differ in topology, limited neighbourhood of a node can modify rapidly. This node always desires to update the routing information IARP protocol is use indoor routing zones.

2. IERP: Inter zone Routing Protocol is global reactive routing component of the ZRP, the Inter zone Routing Protocol takes gain of the well-known local topology of a node's zone and using a reactive move towards enables communication using nodes in previous zones. In Reactive routing protocol IERP is used among routing zones.

3. BRP: The Border casts Resolution Protocol is used in the ZRP to nonstop the route requests start with the global reactive IERP to the minor nodes and removing disused queries and maximize effectiveness [13]. It uses the Intra zone routing information provided by IARP to create a border cast tree.

V. BLACK HOLE ATTACK

Black hole attack is denial of service (DOS) attack in which malicious node send fake information by claiming that it has a fresh or shortest route to destination node and hence source nodes select this shortest path and go through this malicious node and result data misuse or discarded. Once the route is set up, at the moment it's up to the node whether to drop all the packet or familiar it to the nameless address. This special node, which disappear the data packet, is named as malicious nodes. Black hole attack be an active insider attack. Black hole has two properties. First the node announces itself when having a suitable route to a destination node and second one the node consumes the intercepted packets.

Black hole Attacks are categories as:-

- Single Black hole Attack
- Collaborative Black hole Attack

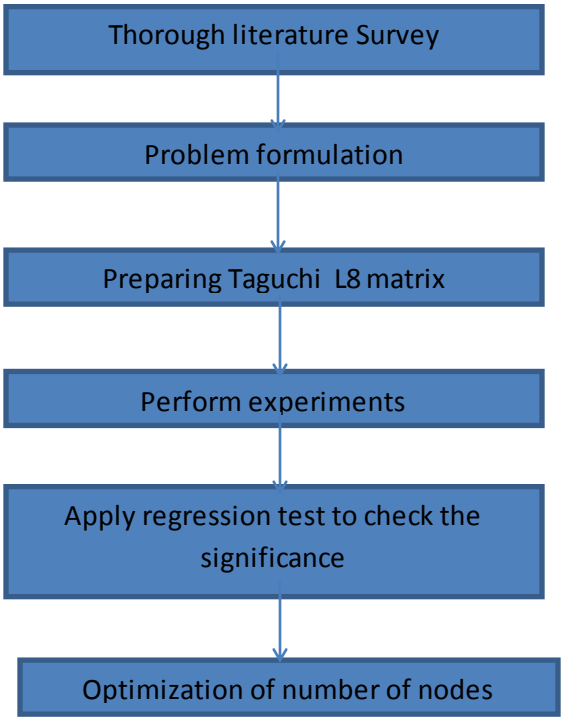
1. Single Black hole Attack

Single Black hole Attack in which one node acts as malicious node which drops all the data. Single black hole attack is also known as Black Hole Attack with single malicious node.

2. Collaborative Black hole Attack

Collaborative Black hole Attack in which many nodes in a group's act as malicious nodes and these nodes misuses or destroys the data traffic. Collaborative black hole attack is also known as Black Hole Attack by multiple malicious nodes.

VI . PROPOSED METHODOLOGY



VII. TAGUCHI METHOD

Design of Experiment (DOE) methods were developed originally by Fisher. However, classical experimental design methods are too complex and not easy to use. Furthermore, a large number of experiments have to be carried out as the number of the process parameters increases. To solve this important task, the Taguchi method uses a special design or orthogonal array to study the entire parameter space with only a small number of experiments. The experimental results are then transformed into a signal-to-noise(S/N) ratio. The S/N ratio can be used to measure the deviation of the performance characteristics from the desired values. Furthermore, a statistical analysis of variance (ANOVA) is performed to identify the process parameters that are statistically significant. The optimal combination of the process parameters can then be predicted based on the analysis.

VIII. PERFORMANCE PARAMETERS

MANET has number of qualitative and quantitative metrics that can be used to compare ad hoc routing protocols. This paper has been considered the following metrics to evaluate the performance of ad hoc network routing protocols.

1) End-to-end Delay:

This metric represents average end-to-end delay and indicates how long it took for a packet to travel from the source to the application layer of the destination. It includes all possible delay caused by buffering during route discovery latency, transmission delays at the MAC, queuing at interface queue, and propagation and transfer time. It is measured in seconds.

2) Packet Delivery Ratio:

Packet delivery ratio is calculated by dividing the number of packets received by the destination through the number of packets originated by the application layer of the source (i.e. CBR source). It specifies the packet loss rate, which limits the maximum throughput of the network.

3) Throughput:

It is the measure of the number of packets successfully transmitted to their final destination per unit time. It is the ratio between the numbers of received packets vs sent packets.

IX. CONCLUSION

In future the study will be performed to see that up to how much number of nodes highest packet delivery ratio and throughput can be achieved with lowest end to end delay for AODV, OLSR and ZRP protocols with and without black hole attack and later on by applying the regression test we will see that up to how much percentage other factors are effecting the transmission.

REFERENCES

[1] Payal N. Raj and Prashant B. Swadas , (2009), "*DPRAODV: A Dynamic learning system against black hole attack in AODV based on MANET* ", International Journal of Computer Science Issues, Vol. 2,pp. 54 -59.

[2] Mamta and Suman Deswal , (2013) , "*DDBA – DSR : Detection of Deep Black Hole Attack In DSR*" , International Journal of Computer Applications , Volume 73 , No. 21 .

[3] Shilpa Jaiswal and Anil Kumar Patidar , (2013), "*Comparative analysis and Simulation of Black hole attack perception and its Preventive Method using Enhanced Proactive Routing* " , International Journal of Advanced Research in Computer Science and Software Engineering , Volume 3 , Issue 9, pp. 839 -845.

[4] Neeraj Arora and Dr. N.C. Barwar , (2014) , "*Evaluation of AODV , OLSR and ZRP Routing Protocols under Black hole attack*" , International journal of Application in Engineering & Management , Volume 3 , Issue 4 ,pp. 2319 – 4847.

[5] 5.Monika verma and Dr. N.C ,Barwar ,(2014), "A Comparative analysis of DSR and AODV protocols under black hole attack and grey hole attack in MANET" , IJCSIT , Volume 5 pp.1228 -7231.

[6] Monika Verma and Dr. N.C . Barwar, (2014) , "*A comparative analysis of DSR and AODV Protocol under Black hole and Grayhole attacks in MANET"* , International Journal of Computer Science and Information Technology , Volume 5 , Issue 4, pp. 7228 – 7231.

[7] 7.Harjeet Kaur ,Manju Bala and Varsha Sahni ,(2013), "Performance evaluation of AODV ,OLSR and ZRP routing protocols under the black hole attack in MANET ",International Journal of Advanced Research in Electrical ,Electronics and Instrumentation Engineering ,Vol 2,Issue 6 .

[8] 8. K.P.Thooyamani , R. Udayakumar and V. Khanaa , (2014), "An Anomaly Detection Scheme in Mobile Ad hoc Network",World Applied Science Journal , pp. 126 – 130.

[9] 9. Neetika Bhardwaj and Rajdeep Singh , (2014) , "Detection and Avoidance of Black hole attack in AOMDV Protocol in MANETs" ,Internatinal Journal of Application or Innovation in Engineering and Management , Volume 3 , Issue 5.