



ENHANCING ZRP TO DETECT BLACK HOLE ATTACK IN MANET USING FUZZY LOGIC

P.PADMAPRIYA¹, G.MANORANJINI²,
M.Tech. (Ph.D.),²Asst. Professor
¹*M.E CSE (Student)*
Tagore Engineering College
Chennai, India

ABSTRACT

MANET which is self -adaptive, dynamic setup of mobile nodes. Generally, there is no centralized control and the routing protocol plays a vital role to communicate between the mobile nodes. ZRP is hybrid in nature that incorporates both reactive and proactive protocol in which the nodes formed as zones and communicate with each other. Due to self-configure and adaptive nature, there may be a lot of security attacks takes place in the network layer. Black hole attack is one of the susceptible attack in which the node drops all the packet without forwarding. Sensing these malicious nodes is complex .Thus, the proposed system provides RSA algorithm incorporates with fuzzy logic technique is used to detect and isolate the black hole node in the zones which makes use of ZRP.
IndexTerms -dynamic, fuzzylogic, proactive, reactive, routing, ZRP

I.INTRODUCTION

A mobile ad hoc network (MANET) is an adaptive, self-configure, infrastructure less network having dynamic topologies. If the two nodes can communicate directly only if they are within the radio or transmission range. The nodes can also indirectly communicate via multihop routing. MANET is more liable to the various types of malicious attacks.

A. Zone Routing Protocol (ZRP)

This protocol combines the advantages of both reactive as well as proactive protocol for routing between the nodes.

B. IntraZone Routing Protocol (IARP)

IARP which means proactive routing protocol. Nodes can communicate within the zones, it uses the IARP protocol. Each node maintains a local routing table.

C. Interzone Routing Protocol (IERP)

IERP which means reactive routing protocol where route discovery process can be initiate by means of 'Border casting' (BRP, Bordercast routing protocol).In general, there are two types of attacks are to be occurred.

1. Passive attack

This attack is to be occurred only if the attackers listening the traffic information without interrupting the network routing or network. Some of the examples are eavesdropping, information leakage, traffic monitoring etc.

2. Active attack

This attack is to be occur by altering or modifying the data exchanged between the mobile nodes (that is disturb the network).Some of the examples are Black hole attack, wormhole attack, rushing attack, etc.

D. Black hole attack

Black hole attack which means the node acts as a malicious by getting the data packet by means of publicising itself to source node which is a shortest route to destination and drops all the packets.

E. Types of Black hole attack

1. Single Black hole attack

One node acts a black hole node in the network to drops the packet.

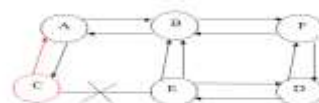


Figure 1. Single black hole attack

2. Collaborative black hole attack

Two or more nodes combines together to drops the packet.

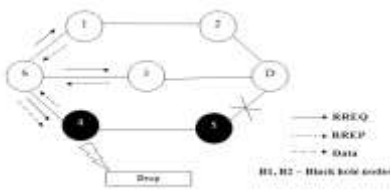


Figure 2. Collaborative attack

The proposed system is based on RSA and Fuzzy logic [6]. Fuzzy logic handles with reasoning form rather than specific. It is based on the truth values 0 and 1.

II.LITERATURE SURVEY

Sandeep Kaur, Supreet Kaur [1] performed work on “Analysis of ZRP in MANET” to show how the ZRP works and its performance compared with other protocols. The number of parameters such as throughput, load, and data dropped to be used to analyse the performance of ZRP over other protocols.

Ankita V.Rach, Yatin Shukla, Tejas R.Rohit [2] “A Novel approach for detection of black hole attacks” gave approach to detect the black hole by using EBAODV. Node gets RREP before time expires, if so send fake packet and check the ACK is received. If no ACK, the number of packet drop is higher than the threshold, then leader send packet that node as black hole to all others.

Mr.Rajdipsinh, D.Vaghela, Prof.NishantJ. Goswami [3] performed work on “A Modified Hybrid Protocol (ZRP) Used for Detection and Removal of Black Hole Node in MANET”. ZRP is used to detect black hole by choosing one reliable node. If malicious node is detected, reliable node sends alarm packet and discard that node from routing table.

T.Ramesh, T.Jothimani [4] gave paper on “A survey on Black hole attack detection methods in MANET”. It shows the approach of using RSA to detect black hole. By using key generation, Encryption and decryption detect the malicious.

Mamta Sengar, Pavan Prakash Singh, snaita Shivani[5] performed work on the paper “Detection of black hole in manet using FBC technique”.

Here, fuzzy based controller has to be used for secure route and detect black hole. To calculate the trust value by using formula for reliability of node.

III.PROPOSED WORK

The proposed system is to be designed based on RSA and fuzzy logic to detect and eliminate the black hole node in

network. The system model makes use of ZRP to form the zones which consists of Forward node, delegation node, Trusted Authority (TA). TA finds the black hole node based on contact history of node and isolate that node using fuzzy logic. Using RSA algorithm to encrypt the data packet before send it to the forward node. Forward node gets the packet and analyse neighbours on other zones to identify the delegation node.

One of the node chosen as a delegation node in which it accepts the maximum request send by the others. This node sensing all the zones.

TA sensing all nodes on the zones and get contact history through delegation node. The node which is valid get the data packet and forward it to the neighbour. This forwarding information is present in the contact history. If it is malicious, the forward information is not present, get the packet and drop without forwarding it. Removing those black hole nodes and input the nodes into the fuzzy computation process for again checking the black hole node is present in the network or not based on fuzzy rules.

A. Fuzzy Parameter Extraction The parameters loss rate and data transmission rate can be get from all the nodes and input it to the fuzzy computation process.

B. Fuzzy Computation to remove black hole TA inform all the nodes to isolate the black hole nodes from the network. For removing those black hole nodes based on the parameters, the fuzzy priority cost can be computed.

If the output is expensive, that is the cost value as ‘1’, then all the nodes present in the network are valid and takes part in the routing.

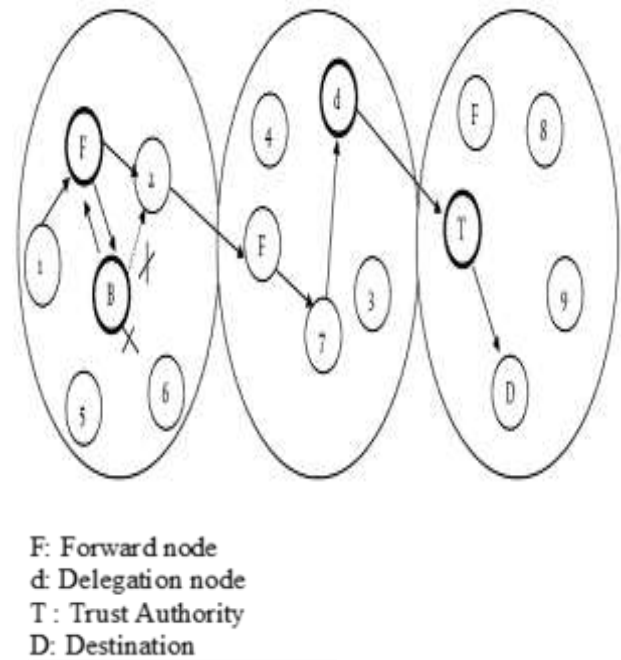


Figure 3. Architecture diagram

IV. ANALYTICAL MODEL

For encrypt and decrypt the data packets, RSA algorithm to be used.

First, by providing the data as string and to encrypt this data by giving two prime numbers as p, q such that n= p *q

For calculating the key values private and public key as e and d. To find 'd',

$$\text{GCD}(d, (p-1)*(q-1)) = 1$$

Then to compute the private key 'e' as,

$$e * d = 1 \pmod{((p-1)*(q-1))}$$

Thus, to encrypt the data

$$C = M^e \% n \text{ (e - private key)}$$

To decrypt the data using,

$$M = C^d \% n \text{ (d - public key)}$$

Algorithm to isolate black hole

1. Define network with N number of nodes
2. Input the nodes
3. Identify and analysis the parameter of each node called loss rate, data rate and Set Expensive =1, low=0, moderate=0
4. For each node (i), fuzzy the following rules,
5. If (fuzzy (loss rate (i) =low) &&fuzzy (data rate (i) = high)) then Set priority cost (i) = Expensive
- 6.If(fuzzy(lossrate(i)=moderate)&&(fuzzy(datarate(i)= moderate)) the Set priority cost (i) = moderate
- 7.if(fuzzy(lossrate(i)=high)&&fuzzy(data rate(i)=low) then Set priority cost (i) = low (black hole node)
8. If nodes having no low cost, then no black hole nodes found in the network, these nodes are takes part in the routing path.

Energy level and the priority can be increased by data rate.

V. PERFORMANCE EVALUATION

A. Simulation Parameter

To study the performance of detecting black hole node in terms of loss rate, delay, PDR under ZRP routing in the network using NS2[13] simulator.

Simulation parameters to be explained as follows.

Parameters	Values
Simulator Ns2	
Routing protocol	ZRP
No. of nodes	25
Simulation time	72ms
Traffic type	CBR
No.of Black hole nodes	5
Packet size	1000bytes

Table 1. Simulation parameters

In this paper, for routing ZRP protocol is used in the network. The nodes are formed as zones. Different metrics are used to calculate the performance of the network under black hole attack.

B. Experimental Result

Using Xgraph to analyze these parameters, the following results are obtained as shown below.

Packet loss rate: Number of packets dropped by the node.

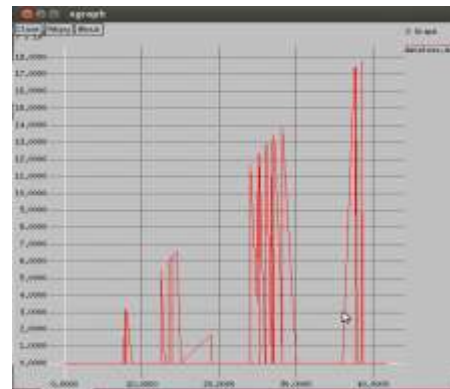


Figure 4. Packet loss rate

The above figure shows that the packet loss is higher under black hole attack in the network. It shows 38% loss rate with respect to the black hole nodes.

Delay: time taken for packet to transmit from source to destination. The following graph shows the delay performance with respect to removing the black hole node from the network.

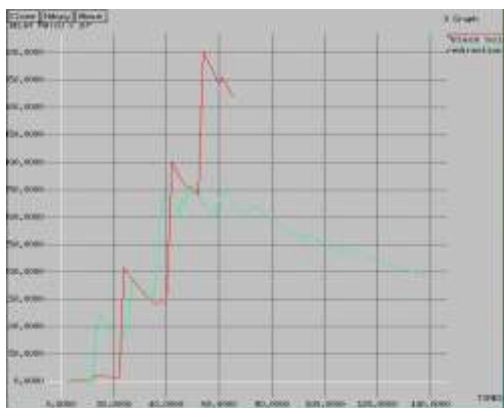


Figure 5 .Time vs Delay

VI. CONCLUSION

In this proposed technique is hybrid in nature and we have provided the RSA algorithm and fuzzy logic to easily detect and isolate the black hole node from the zones. In this method, we have used the trusted authority node to provide the security under ZRP against black hole attack. Based on the simulation results by analyzing the parameters, the packet loss rate is higher in the network under black hole attack as illustrated in the graph. This proposed technique provides better PDR and minimum delay after isolating the black hole node from the network.

VII.FUTURE WORK

The boundary overlapping is a major issue in ZRP protocol implementation. So, there is a need to analyze this issue. Analyze the performance of MANET by fully implementing the zone routing protocol.

REFERENCES

- [1] Sandeep Kaur, Supreet Kaur "Analysis of Zone Routing Protocol in MANET" *IJRET: International Journal of Research in Engineering and Technology* eISSN: 2319-1163 | pISSN: 2321-7308.
- [2] Ankita V. Rachh, Yatin V. Shukla, Tejas R. Rohit, "A Novel Approach for Detection of Black hole Attacks" *IOSR Journal of Computer Engineering (IOSR-JCE)* e-ISSN: 2278-0661, p- ISSN: 2278-8727 Volume 16, Issue 2, Ver. V (Mar-Apr.), PP 69-74.
- [3] Mr.Rajdipsinh, D.Vaghela, Prof.Nishant J. Goswami" *A Modified Hybrid Protocol (ZRP) Used for Detection and Removal of Black Hole Node in MANET* "ISSN: 0975 – 6760| Nov 12 to Oct 13 | volume – 02, issue – 02.
- [4] T.ramesh, T.Jothimani," *A survey on blackhole attack detection methods in MANET*", *International journal of engineering sciences & research Technology*
- [5] Mamta Sengar,Pawan Prakash Singh, Savita shiwani " *Detection of black hole attack in MANET using FBC technique*" vol.2,issue – 2,IJETTCS.
- [6] *Fuzzy logic with engineering applications* by Timothy J.Ross McGraw hill.inc
- [7]MonitaWahengbam,NingrinlaMarchag ,"*Intrusion Detection in MANET using Fuzzy logic*",2012 IEEE.
- [8] Latha Tamilselvan "Prevention of co-operative Black hole attack in MANET" *Journal of Networks*, vol.3, no.5, May 2008.
- [9] Jian-Ming chang, Po-chun Tsou "Defending against collaborative attacks by malicious nodes in MANETs: A Cooperative Bait Detection Approach", *IEEE* 2014
- [10] Mamta Sengar,Pawan Prakash Singh, Savita shiwani " *Detection of black hole attack in MANET using FBC technique*" vol.2,issue – 2,IJETTCS.
- [11] Ramkumar, Murugeshwari "Fuzzy logic approach for detecting black hole in hybrid wireless mesh network" *issue -3, ICIET* 2014.
- [12] *MANET charter*, (1998) available at <http://www.ietf.org/html.charters/manet-charter.html> (1998-11-29).
- [13] ns-2:<http://www.isi.edu/nsnam/ns/>
- [14]Introduction to algorithms, Thomas H.Cormen, Charles E.Leiserson, Ronald L.Rivest,Clifford Stein, eastern Economy edition, 3rd edition.