DETECTING AND PREVENTING BLACK HOLE ATTACK IN MANET USING RSA ALGORITHM

Dr. M. Lalli [1], S. Arul Jothi[2]

[1]Assistant Professor School of Computer Science and Engineering, Bharathidasan University, Tiruchirappalli, TamilNadu, India.
[2]Research Scholar School of Computer Science and Engineering, Bharathidasan University, Tiruchirappalli, TamilNadu, India.

---***---

Abstract -*MANET is the decentralized network. It does not need any infrastructure such as a base station so that MANET becomes vulnerable to network attacks. A black hole is one type of data traffic attack of MANET. In this work, the malicious nodes act like a black hole attack. It indicating itself as the shortest path to the destination in a network by sending a fake route reply to the source node. In our work, the RSA algorithm is used to detect the multiple black hole attack and prevent the ZRP routing protocol from black hole attack. From the simulation result, the ZRP routing protocol shows better results when compared to the DSR routing protocol in terms of throughput, average end-to-end delay and packet delivery ratio, packet drop ratio, and detection time.*

Key Words**: DSR, ZRP, RSA, Black Hole Attacks [BHA], Malicious Node, Mobile Ad-Hoc Network (MANET).**

1. INTRODUCTION

MANET is a combination of three words. They are Mobile, ad-hoc and network. Mobile refers to a moving state, ad-hoc refers to temporary purpose and network refers to a collection of interconnected computers. It consists of mobile nodes that form a network without wire for a temporary purpose [8]. It is the self-organizing infrastructure-less network. That means device-to-device communication. In MANET every node act as a server, client and router. Co-operative communication is important for the MANET. In MANET, the data does not go directly from the sender to the receiver it needs an intermediate node to transfer the data. It is also called the relay network (or) multihop network. It means they do not require any fixed infrastructure. That means if the source node wants to send some information to a destination node it has to take help of the neighbor nodes in order to be able to send the data from it to the destination node. So consequently what happens it is not a single hop transmission from the source node the destination node but it goes through number of multihop (or) number of intermediate nodes. So these networks are very useful in different situations such as different times of emergency or during relief operations, video conference, virtual classroom, electronic payments and researchers and / or students on campus (academic services) [12].

2. ROUTING IN MANET

Routing means to select the best and shortest path for the packet travel among the mobile ad-hoc network with the help of some metrics such as path bandwidth, reliability, delay, current load on that path[12].In manet routing protocols are categorized into three types these are (i)Table Driven Routing Protocol (ii)On-Demand Routing Protocol (iii) Hybrid Routing Protocol. In this paper, we focused on ZRP as a hybrid routing protocol.

2.1 Table Driven Routing Protocols

It is also referred to as proactive protocols. It maintains routes to the destination even if they are not needed. Some of the examples are Wireless Routing Protocol (WRP), Destination Sequenced Distance Vector (DSDV), Source-Tree Adaptive Routing Protocol (STAR), Cluster-Head Gateway Switch Routing Protocol, and Optimized Link State Routing (OLSR).

2.2 On-Demand Routing Protocols

It is also referred to as reactive protocols. It maintains routes to a destination only when they are needed. Examples are Dynamic Source Routing (DSR), Ad Hoc-On-Demand Distance Vector (AODV), Temporally Ordered Routing Algorithm (TORA), and Associativity-Based Routing (ABR).

2.3 Hybrid Protocols

It is a combination of both reactive and proactive protocols. It maintains routes to nearby nodes even if they are not needed and maintain routes to far away nodes only when needed. Example Zone Routing Protocol (ZRP). [9][10].

2.3.1 Zone Routing Protocol

ZRP routing protocol comes under the hybrid routing protocol category. It combines the feature of both reactive and proactive protocols. ZRP has several components such as IARP, IERP, BRP, and NDP [13].

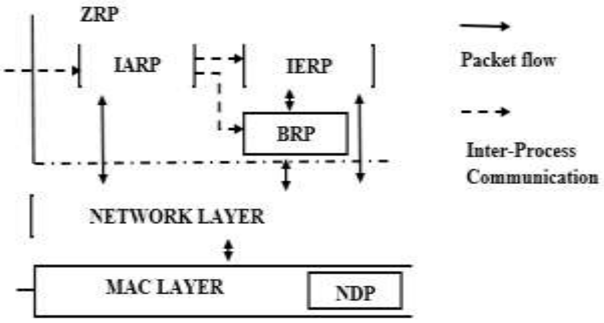

Fig - 1: ZRP Components /Architecture

(i)IARP (Intra zone Routing Protocol): It is used to maintain routes in the zone with the help of proactive routing protocol. (ii) **IERP** (Inter-zone Routing Protocol): It helps to find a route to nodes outside of zone with the help of reactive routing protocol. **(c) BRP** (Border casts Resolution Protocol): It is responsible for the forwarding of a route request from the source to destination. **(d) NDP** (Neighbor Discovery Protocol): It is used to know about the direct neighbors with the help of MAC (media access control) protocol. The NDP selects the nodes based on signal strength, frequency, delay of beacons [13]. In Zone Routing Protocol the network is divided into the different zone based on the value of the radius. The size of the zone is different from one to another.

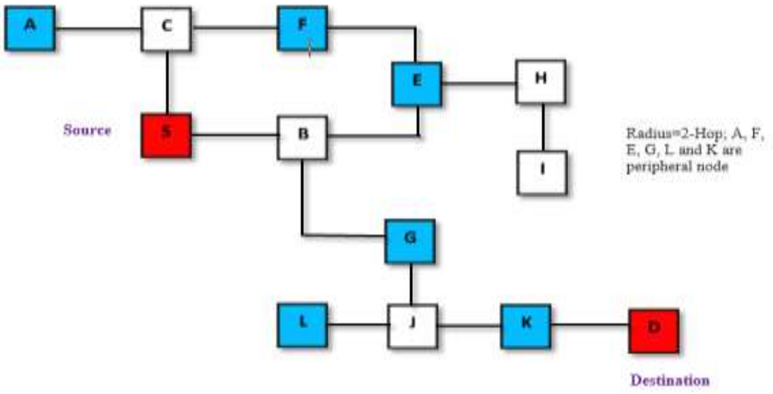

Fig - 2: ZRP Routing Protocol

From the above fig 2, source node S wants to send data to destination D by using zone radius 2. Node S will check whether the destination is present within its zone or not. If the destination node is present within the zone, then the source node will form the routing path to the destination. If D is absent in zone, then node S sends RREQ to its peripheral nodes. After receiving RREQ from the source node, peripheral nodes (A, E, F, and G) also works with the same logic. It also checks whether the destination node D is present within their zone or not. This process will continue until it reaches the destination D. Peripheral node G will be having a route for D but it is outside the zone. G also does the same thing as it forwards that RREQ packet to its peripheral nodes(S, E, K, and L). Then K node receives this RREQ packet from the peripheral node. K is also the zone of the destination node D.K also does the same things. Node K finds the destination D is in the same zone. After that destination node D sends the RREP (D, K, G, and S) to the source node S. After finding the optimal path source node S starts the data transmission to the destination node D. In large networks ZRP provides better efficiency.

3. BLACK HOLE ATTACK [BHA]

Blackhole is one type of network traffic attack of MANET [7]. In this, the malicious nodes act like a BHA, indicating itself as the shortest path to the destination in a network by sending a fake route reply to the source node [5]. It gets all the data packets from the source node and then drops the packets. The BHA is classified into two types. They are

3.1 Single Black Hole Attack

In a single BHA, only a single node act as a fake node [7]. It obtains all data packets from the source without forwarding it to the destination. From below fig.3 the source node S wants to send the data to destination D.So S starts the route searching process to the destination D by broadcasts the RREQ message to all its neighbor nodes. Then the neighbor node has also broadcast the RREQ message until to reach the destination D. After receiving the RREQ message, the destination node D will reply to the source node via RREP message. The malicious node M also generate the fake RREP message to the source node S. It indicating itself as the shortest path, spoofed sequence number, and minimum hop count to reach the destination D.Then the source node S discards other RREP coming from other authorized node and starts transmitting all its data packets via malicious node. The malicious node (M) drops all data packets without forwarding it to the destination node (D). It will crash all data packets. Then it will make the packet loss in the network.

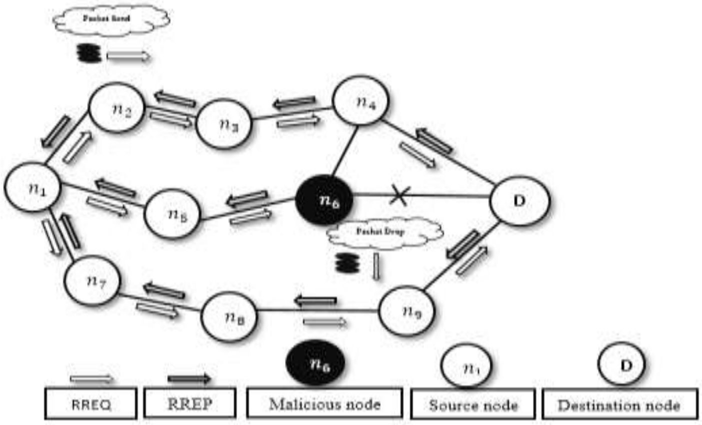

Fig - 3: Single Black Hole Attack

3.2 Multiple Black Hole Attack

In multiple BHA, more than one node act as a malicious node. This will affect network performance than the single BHA. The multiple BHA is shown in fig 4

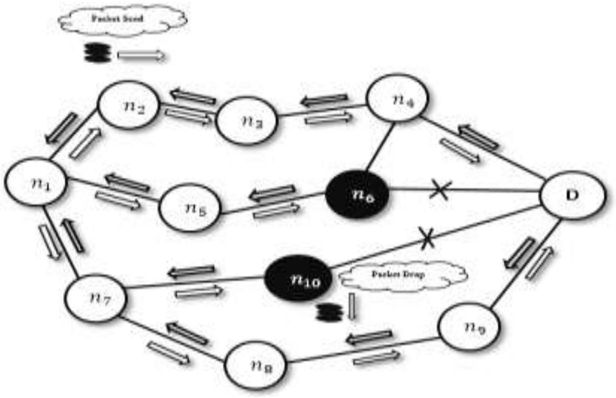

Fig - 4: Multiple Black Hole Attack

4. RELATED WORKS

This section reviews some articles regarding detection and prevention of BHA by different methods like multiple route reply forward, Diffie-Hellman key exchange and advanced encryption standards [AES] algorithm, RSA algorithm, etc.

Taku Noguchi et al [1] in this method to prevent the BHA using multiple RREPs forwarding and RREP filtering mechanisms.it proposes a new threshold-based BHA prevention method using multiple RREPs. It also shows the performance metrics in terms of packet delivery rate, throughput and routing overhead. Ankit Singh et al [2] the purpose of this paper is to analyze the performance of various routing protocols like AODV, DSR, OLSR, DSDV, ZRP during the BHA in MANET. From the results, the ZRP routing protocol shows better performance than all other routing protocols in terms of packet delivery ratio, average throughput, packet-drop-ratio, average end-to-end delay. Mangesh A.Suryawanshi et al [3] the purpose of this paper is to prevent the BHA in the AODV routing protocol by Diffie-Hellman key exchange and advanced encryption standards[AES] algorithm. This method isolates the malignant node on the selective path in the AODV routing protocol and secures the channel by utilizing two algorithms such as D-H exchange and AES algorithm. Helmi Hartadi et al [4] the purpose of this paper is to analyze the performance of two routing protocols such as AODV and DSR during a BHA in MANET. From the results, the AODV routing protocol shows better performance than DSR routing protocols in terms of throughput, delay, and packet loss. A. A Chavan et al [5] this paper analysis the performance of AODV and DSDV routing protocols in terms of routing overhead, packet delivery ratio, throughput, and end-to-end delay. The performance of modified AODV is better than DSDV in terms of throughput, packet delivery ratio and routing overhead. This paper did some modifications in AODV to improve the performance of AODV in the presence of a BHA. Jyoti Prabha et al [6] have proposed from this method conjunct blackhole attack eliminate from the DSR routing protocol using the RSA algorithm. It also shows the performance metrics in terms of delay and throughput of the network in the ad hoc network environment. Harjeet Kaur et al [11] this paper is to analyze the performance of three different routing protocols like AODV, OLSR and ZRP routing protocols with the black hole and without blackhole attack in MANET. From the result, the AODV routing protocol shows better performance than OLSR and ZRP with attack and without attack in terms of packet delivery ratio, average jitter, average throughput and average end to end delay. Shaily Mittal et al[12] the purpose of this paper is to analyze the performance comparison of 3 different routing protocols like AODV, DSR, ZRP routing protocol in MANET. From the results, the AODV shows better performance than DSR and ZRP routing protocols in terms of average end-to-end delay and packet delivery ratio.

5. PROPOSED WORK

In this research work, the RSA based cryptographic solution is based on the computation of the sequence number to detect and eliminate the conjunct black-hole attack. For RSA based detection method, we are considering six large prime numbers to calculate encryption packet e and decryption packet d value. M value is taken as RREQ. The sender sends the RREQ to the neighbor nodes (or) peer node. The six large prime numbers are taken as an input. If the neighbor node knows about the key-value then it can able to decrypt the RREQ and generate RREP which is to be sent to the sender. The proposed work represents the Conjunct Black-hole detection and the prevention methods of the BHA described below. RSA algorithm is used to avoid the behavior of a BHA.

1. Consider 6 large prime numbers p, q, r, s, t, and u.
2. Compute n=p*q*r*s*t*u.
3. Compute $\varphi(n)$= (p-1)*(q-1)*(r-1)*(s-1)*(t-1)*(u-1). Where φ is Euler's totient function. This value is kept private.
4. Select an integer e such that 1 < e <φ (n) and gcd (e, φ (n)) = 1; i.e., e and φ (n) are co-prime.
5. Find d, such that d*e mod $\varphi(n)$=1.

   Public key= {e, n}

   Private Key= {d, n}

Encryption

6. C= m^e (mod n)

Decryption

7. M= c^d (mod n)

Such a compromised/malicious node alters its forwarding behavior as described in the following variants of blackhole attacks.

Blackhole Reordering

As the name suggests, an attacker node reorders some of the packets before forwarding them. As ACKs of some of the reordered packets are not received in time, the sender needs to retransmit them again. From the receiver's perspective, each time a packet is received, an ACK is generated. For out-of-order packets, the sender shall receive duplicate ACK messages. TCP initiates its flow control mechanism if duplicate ACK messages exceed a threshold. In the implementation of a reordering attack, the blackhole node creates a reordering buffer of size in its input queue.

Blackhole periodic dropping

In this attack, a blackhole node randomly discards some packets over a specified period during the communication process. In this way, incorrect route congestion information is conveyed to TCP, which uses the dropping of packets as an indication of congestion on the route. The BH-node may either choose to discard a fraction of packets (e.g., 10 packets from every 100 packets) or may discard all the packets received during a slice of time (e.g., discarding data packets for few milliseconds every second near the TCP sender timeout). This forces TCP to enter the retransmission timeout (RTO) and to increase its RTO value. As the flow becomes stable, the attacker repeats the above strategy to sustain the attack and keep the data flow rate low.

Blackhole Delay Variance Attack

Round trip time (RTT) of data packets varies considerably due to congestion. Though TCP has a flow control mechanism to adapt to the changes, it cannot determine if the change in RTT is due to dynamic wireless topology, network congestion or blackhole attack. Also, changes in RTT force TCP to increase RTO. By delaying packets randomly, a blackhole node can initiate this attack resulting.

Blackhole Hop Count

According to the conventional routing mechanism, a blackhole node can be adjusted to the values of (hop count) and destination sequence number (DSN) easily to mislead the source node. In this attack, the source node after sending a route request (RREQ), it will respond to the first route reply (RREP), that will be coming from the black hole node and not reply to other intermediate nodes. As a result, it will be terminated the cooperation work in MANET.

Blackhole Source to Destination List

Upon receipt of an RREQ or RREP packet from its neighbors, each node adds the source node of the received packet to its list. A path list entry has four information fields, such as node address, RREQ flag, RREP flag, and membership of round trip time. The node address is the address of the source node of the RREQ/RREP packet. When a node receives an RREQ/RREP packet and then adds an entry to its path list, it sets the RREQ/RREP flag to 1. The membership time is the lifetime of the list membership; the entry is deleted from the list after the membership time has elapsed.

Blackhole Threshold

In the proposed method, each node calculates the packet threshold dynamically based on the total number of active nodes in the network and the time elapsed after it knows the last sequence number of the destination node. We performed preliminary experiments to find appropriate calculation methods for threshold. Because of space constraints, we leave the details of the preliminary experiments. It was found that a destination sequence variety is roughly proportional to each of the overall variety of active nodes and time. These are considering as 6 large prime numbers

6. PERFORMANCE ANALYSIS OF ROUTING PROTOCOL

6.1 SIMULATION PARAMETERS OF ZRP-RSA ROUTING PROTOCOL

The simulation process is performed with 40 nodes in ZRP. It distributes over 1500*1500 area in NS2.simulation using CBR traffic and MAC Layer 802.11 and within the time duration of 5.0sec [11]. The simulation parameters are summarized in table-1

Table – 1: Simulation Parameters

PARAMETERS	VALUE
Channel Type	Wireless Channel
MAC Layer	802.11
Area	1500*1500 m square
No .of Nodes	40
Mobility Type	Random Waypoint
Antenna Type	Omni Directional Antenna
Omni Type	Omni Directional Antenna
Traffic	CBR
Malicious Noes	1, 2, 4
Attack Types	Blackhole Attack
Routing Protocols	ZRP
Simulation START/STOP Time	0.0/5.0s

6.2 PERFORMANCE METRICS

In this paper, we have used the following performance metrics for evaluating effects of BHA and effectiveness of our detection algorithm:

6.2.1 Throughput (T):

It is the ratio of the total number of bits transmitted (B_{tx}) to the time required for this transmission, i.e. the difference of data transmission end time (t_{end}) and start time (t_{start}). This metric depicts how the congestion control mechanism at the source node is affected by the packet losses caused by a BHA. The unit of throughput is bps.

$$T = \frac{B_{tx}}{t_{end} - t_{start}}$$

6.2.2 End-End Delay

The total time it takes data packets to reach the destination from the source across the network is END-END DELAY. D is computed as the ratio of the sum of the individual delay of each received data packet to the total number of data packets received. This metric is used to evaluate the impact of a BHA on delay-sensitive applications of ZRP-based MANETs. By intentionally discarding, delaying or reordering packets, a blackhole node can increase the value of this metric; increase being caused by re-transmissions of such packets due to timeout at the source. N_{rec}, No. of received packets.

$$D = \frac{\sum_{i=1}^{N_{rec}} D_i}{N_{rec}}$$

6.2.3 Packet Delivery Ratio

The ratio of the total number of packets received by the receiver to the total number of packets sent out by the sender.

$$PDR = \frac{\sum no.\ of\ packets\ received\ by\ destination.}{\sum no.\ of\ packets\ send\ by\ source}$$

6.2.4 Packet Drop Ratio

The PDR is defined as the ratio of the total number of lost packets to the total number of sent out by the source.

$$PDR = \frac{\sum\ no.\ of\ packets\ send - \sum no.of\ packet\ received}{\sum no.\ of\ packets\ send\ by\ source}$$

6.2.5 Detection Rate

We evaluate the accuracy of the detection of a black hole node by the detection rate R_t.

$$R_t = \frac{N_{black}}{N_{fakeRREP}} * 100$$

Here, $N_{fakeRREP}$ is the total number of fake RREPs received by nonblack hole nodes during the simulation. N_{black} is the total number of blacklist entries (excluding the entries for the nodes blacklisted falsely) of all non–black hole nodes.

7. ANALYSIS AND RESULTS

The result is shown in the table 1-2 for the various number of node 5, 10, 15, 20, 25, 30, 35, 40 respectively. In each case, no of packets transmitted between the sender and receiver, packet delivery ratio, packet drop ratio, throughput, and average end-to-end delay values are taken from the trace file.

Table - 1: Comparison of Existing Method and ZRP-RSA Protocol under the BHA in terms of Throughput and Packet Delivery Ratio

NO OF NODES	THROUGHPUT(bps)		PACKET DELIVERY RATIO (%)	
	EXISTING METHOD	ZRP-RSA	EXISTING METHOD	ZRP-RSA
5	47.2591	60.229	12.298	20.2341
10	65.2678	88.9218	33.4091	42.0129
15	70.1592	95.2549	55.2901	58.5477
20	87.1498	108.149	69.5918	71.859
25	95.7125	123.726	82.8122	84.2091
30	118.32	148.197	94.9153	96.1667
35	119.5471	150.359	95.0247	97.5701
40	120.4879	153.749	95.1578	98.1453

Table-1 explains the comparison of existing and ZRP-RSA protocol in terms of throughput. The throughput of the existing protocol is between 47.2591-120.4879 and the throughput of ZRP-RSA is between 60.229-153.749. Hence, the throughput of ZRP-RSA is better than the existing protocol and also it describes the packet delivery ratio of the existing method and ZRP-RSA. The packet delivery ratio of existing method is between 12.298-95.1578. The packet delivery ratio of ZRP-RSA is between 20.2341-98.1453. hence, ZRP-RSA is having better packet delivery ratio as compared to the existing method.

Table – 2: Comparison of Existing Method and ZRP-RSA Protocol under the BHA in terms of Packet Drop Ratio and Avg End-to-End Delay

NO OF NODES	PACKET DROP RATIO (%)		AVG END-TO-END DELAY(ms)	
	EXISTING METHOD	ZRP-RSA	EXISTING METHOD	ZRP-RSA
5	0.9231	0.0591	0.0945	0.0055
10	1.5904	0.9287	0.1198	0.0118
15	2.8329	1.4958	0.1298	0.0258
20	3.8322	1.9998	0.1351	0.0301
25	4.5092	2.6823	0.1559	0.0397
30	5.0847	3.8333	0.1934	0.0447
35	5.9041	3.9501	0.2195	0.0492
40	6.5483	4.5548	0.2521	0.0512

Table-2 describes the packet drop ratio of existing method and ZRP-RSA. The packet drop ratio of the existing method is between 0.9231-6.5483. The packet drop ratio of ZRP-RSA is between 0.0591-4.5548.from the result, ZRP-RSA is having better packet drop ratio as compared to the existing method and also it shows the average end-to-end delay of existing and ZRP-RSA protocol. The average end-to-end delay of existing method is between 0.0945-0.2521 and the Average end-to-end delay of ZRP-RSA between 0.0055-0.0512. From this result, the end-to-end delay of ZRP-RSA is less than the existing method.

Detection time

Blackhole attack detection time of existing routing protocol is 7.8978ms and ZRP is 2.8663ms. From the above detection time values, ZRP finds blackhole node quickly than existing routing protocol.

8. ANALYSIS

From the below Chart-1, it analyzed that which method achieves the high throughput. From the comparative analysis, ZRP-RSA increases the throughput than the existing method.

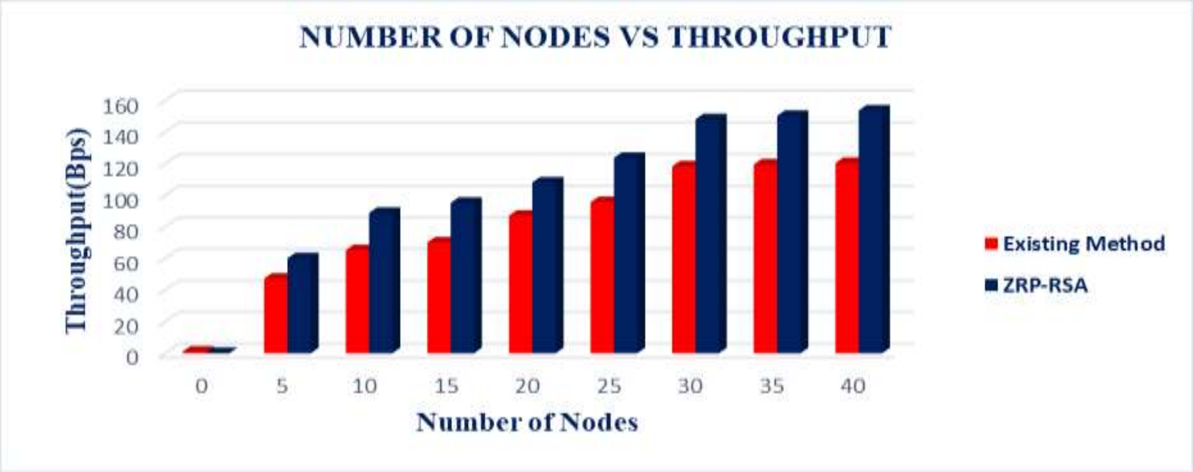

Chart- 1: Throughput vs. No.of Nodes of Existing Method and ZRP-RSA

Chart 2 shows the packet delivery ratio of the existing method and ZRP-RSA. From this comparative analysis, ZRP-RSA achieves a high packet delivery ratio than existing method.

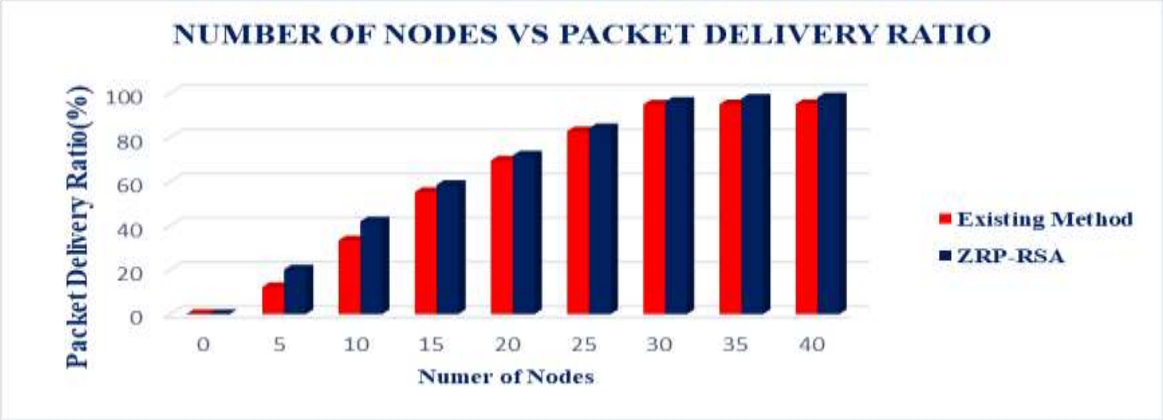

Chart - 2: Packet Delivery Ratio vs No.of Nodes of Existing Method and ZRP-RSA

From the below chart -3, it analyzed that which method achieves the minimum packet drop ratio. From the comparative analysis ZRP-RSA decrease the packet drop ratio than the existing method.

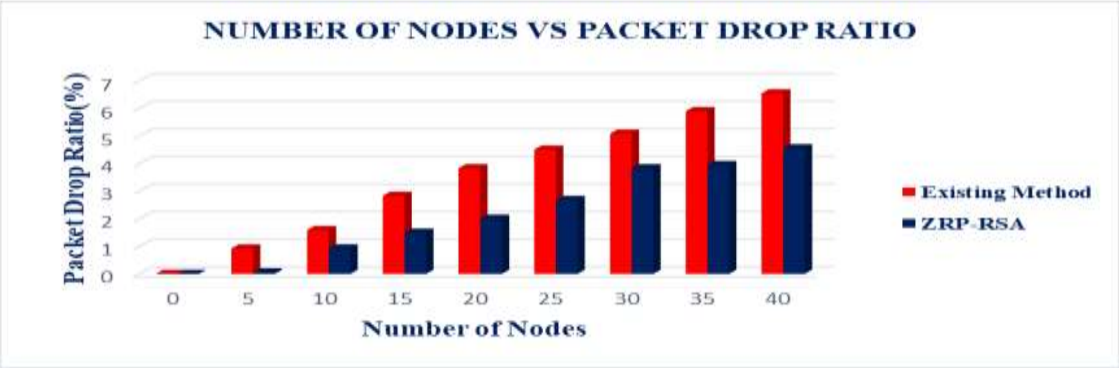

Chart – 3: Packet Drop Ratio vs No.of Nodes of Existing Method and ZRP-RSA

Chart -4 shows the average end-to-end delay of the existing method and ZRP-RSA. From this comparative analysis, ZRP-RSA decreases delay than the existing method.

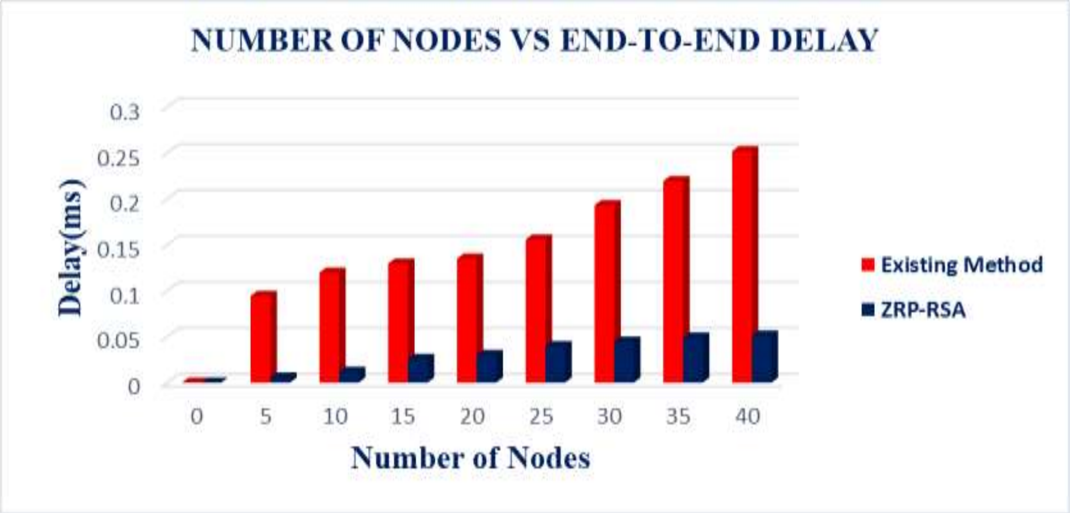

Chart - 4: End-to-End Delay vs No.of Nodes of Existing Method and ZRP-RSA

8. CONCLUSION AND FUTURE WORK

A mobile ad hoc network (MANET) is a self-organizing network consisting of mobile nodes that are connected through wireless media. From the performance analysis carried out in this paper, it is found that ZRP-RSA routing protocol performs better than the existing routing protocol. This proposed method achieved a better packet delivery ratio. It increases the throughput, decreases the average end-to-end delay, packet drop ratio and also it detects and prevents the multiple BHA. This proposed work aims to improve security as well as the performance of the network. In the future, this research work will extend with another routing protocol instead of the ZRP routing protocol to detect and prevent the black hole attack.

REFERENCES

1. T. Noguchi and M. Hayakawa, "Black Hole Attack Prevention Method Using Multiple RREPs in Mobile Ad Hoc Networks", 17th IEEE International Conference on Trust, Security, and Privacy in Computing and Communications, 2018, pp. 539-544.

2. A. Singh, G. Singh and M. Singh," Comparative Study of OLSR, DSDV, AODV, DSR, and ZRP Routing Protocols under Blackhole Attack in Mobile Ad Hoc Network" Springer, 2018, pp. 443-453.
3. Mangesh A.S. Priyanka, G.B. Harish, B. M and Bhagyashri. A. H, "Detection and Prevention of Black Hole Attack in MANET", International Journal of Science, Engineering and Technology Research (IJSETR), 06, 2017, pp. 923-926.

4. I. Nurcahyani and H. Hartadi," Performance Analysis of Ad-Hoc on-Demand Distance Vector (AODV) and Dynamic Source Routing (DSR) Under Black Hole Attacks in Mobile Ad Hoc Network (Manet)", IEEE, 2018.

5. A. A. Chavan, Prof. D. S. Kurule and Prof. P. U. Dere, "Performance Analysis Of AODV And DSDV Routing Protocol In Manet And Modifications In AODV Against Black Hole Attack", 7th International Conference on Communication, Computing, and Virtualization, 2016, pp. 835-844.

6. J. Prabha, D. Goyal, S. Shivani and A. Sanghi," Prevention of Conjunct Black Hole Manet on DSR Protocol by Cryptographic Method", Springer Nature Singapore Pte Ltd, 2018, pp. 233-240.

7. Hardik, N. T, and Prof. Zishan, N," A Survey on Techniques to Handle Black Hole Attack for AODV in MANET",International Journal for Innovative Research in Science & Technology (IJIRST),2018, 4, pp.33-37.

8. Pooja and Prof.V. Kumar, "A Review on Detection of Blackhole Attack Techniques in MANET", International Journal of Advanced Research in Computer Science and Software Engineering, 2014, 4, pp. 364-368.

9. https://www.scribd.com/doc/71867535/MC-Unit-7-MANET-s

10. C.Sivaram, M., &B.S Manoj, Ad-Hoc Wireless Network-Architecture &Protocols, 2011.

11. H. Kaur, M. Bala and V. Sahni ," 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, 2013, Vol. 2, Issue 6, Pp. 2555- 2563.

12. S. Mittal, P. Kaur ," Performance comparison of AODV, DSR and ZRP routing protocols in MANETs",International Conference on Advances in Computing, Control, and Telecommunication Technologies,2009,pp. 165-168

13. https://www.brainkart.com/article/Zone-Routing-Protocol-(ZRP)--Algorithm,-Illustration,-Advantages,-Disadva

BIOGRAPHIES

Dr. M. Lalli presently she is an Assistant Professor in School of Computer Science, Engineering and Application, Bharathidasan University,Tiruchirappalli, India. Her area of research includes Computer Networks, Network Security, Data Mining.

Ms. S. Arul Jothi is the research scholar, pursuing M.Phil., in School of Computer Science, Engineering and Application, Bharathidasan University, Tiruchirappalli, India. Done her Master studies in Madurai Kamaraj University, Madurai. Her area of interest includes Network Security.