www.ioirp.com
International Journal of Innovative Research in Computer Science and Engineering (IJIRCSE)
ISSN: 2394-6364, Volume – 1, Issue – 8. July 2015

DETECTION OF BLACK HOLE ATTACK IN MOBILE AD HOC NETWORK

[1]Chittibabu
Master of Computer Applications
St. Joseph's college of Engineering, Chennai, India
chitti.seetharaman92@gmail.com

[2]V.Anjana Devi
Associate Professor, Master of Computer Applications
St. Joseph's college of Engineering, Chennai, India
anjanadevi_anne@yahoo.com

***Abstract*— Mobile Ad hoc Network (MANET) are wireless networks without fixed infrastructure based on the cooperation of independent mobile nodes. Security is an essential requirement in mobile ad hoc networks to provide protected communication between mobile nodes. Due to unique characteristics of MANET, it creates a number of consequential challenges to its security design. To overcome the challenges, there is a need to build a powerful, multifeatured security solution that achieves both broad protection and desirable network performance. MANET are vulnerable to various attacks, black hole, is one of the possible attacks. The objective of the paper is to detect black hole attack, and propose solution that checks authenticity of reply messages from actual destination node. This system detects the fake reply messages at routing process itself. So malicious node cannot be participated in data transmission. Hereby maximum of secure data transmission is achieved with better performance.**

Keywords—MANET, Blackhole attack, RREQ(Route Request), RREP(Route Reply), RERR(Route Error), Watchdog, Pathrater.

I. INTRODUCTION

A mobile ad hoc network (MANET) is a self-configuring infrastructure less network of mobile devices connected by wireless links. It is a collection of communication devices or nodes that wish to communicate without any fixed infrastructure and pre-determined organization of available links. The primary challenge in building a MANET is equipping each device to continuously maintain the information required to properly route traffic[12][14]. The main challenges in MANET are security attacks.

Routing protocols proposed for MANET can be categorized to three types

i) Proactive Routing Protocols

ii) Reactive Routing Protocols

iii) Hybrid Routing Protocols

Proactive protocols also known as Table-driven, find the path to every other individual node in the network whether if there is a packet sending request or not, and attempt to maintain consistent up-to-date routing information from each node to every other node in the network. These protocols require each node to maintain one or more tables to store routing information, and any changes in network topology need to be reflected by propagating updates throughout the network in order to maintain a consistent network view. Examples include Destination Sequenced Distance Vector routing protocol (DSDV) and Optimized Link State Routing Protocol (OLSR)[8][9]

Reactive protocols are also known as demand driven protocols. They do not require constant update of paths and they only create routes when desired by the source node that is they don't find route until demanded. Examples of reactive protocols are Ad hoc On-demand Distance Vector Routing protocol (AODV) and Dynamic Source Routing (DSR).

Hybrid routing protocol is combination of proactive and reactive routing protocol. Zone-based Hierarchical Link State (ZHLS) is typical example of hybrid routing protocol.

In mobile ad hoc networks (MANET), nodes usually cooperate and forward each other's packets in order to enable out of range communication. Routing protocols are exposed to a variety of security attacks. Black hole attack is one such type of attack in which a malicious node makes use of the vulnerabilities of the route discovery packets of the routing protocol to advertise itself as having the shortest path to the node whose packets it wants to intercept. During the route discovery process, the source node sends route discovery packets to the intermediate nodes to find a fresh path to the intended destination. Malicious nodes responds immediately to the source node as these nodes do not refer the routing table. The source node assumes that the route discovery process is completed and then ignores other route reply messages from other nodes and selects the path through the malicious node to route the data packets. The malicious nodes do this by assigning a high sequence number to the reply packet. The attacker node now drops the received packets instead of forwarding.

The scope of the project is to detect Black hole attack in MANET, is identified in path routing process itself. The fake RREP packet is identified by using random number which is assigned in RREP messages. Random number is same for all RREQ packets that are received from same source node. This random number is attached in every RREP packet by destination node. When fake RREP is received from a path, this path again checked to identify which is attacker. Data collection table also used to confirm whether suspicious node is attacker or not.

II. RELATED WORKS

Intrusion detection is a mature field in network security. While there are many possible approaches, such as rule-based systems, trust based system and cluster based system. This paper focuses particularly on systems based on Trust based and promiscuous listening. In particular this system investigate how these algorithms can be employed most appropriately.

Sen et al[1] claims to show improvement over previous algorithm to find data packet dropping. This solution is based on trust based approach. It is implemented for distributed architecture and it isolates attackers. Gonzalez et al[2][3] proposed a solution to provides secure packet delivery. This solution based on flow conservation. It is implemented in hierarchical architecture. Mari et[4] al presents a solution to detect packet dropping. This solution used watchdog and pathrater concept. It is implemented using Dynamic Source Routing protocol.

Yi et al[4] proposed a solution in AODV protocol to find malicious nodes using concept of priority queue for incoming RREQs. It addressed attack of sleep deprivation by malicious RREQ flooding. Yu & Ray[5] proposed a solution to find packet dropping attacks by checking neighbouring node's RREQs packets. This solution is constructed by origin of neighbor node's request packets send and received. It addressed sleep deprivation attack. Medadian et al[6][7] proposed a solution to detect black hole attack by using concept of neighbor supervision. It uses neighbor node's transmission details and all nodes supervises its neighbor nodes.

K.S.Sujatha[15] have proposed a technique to analyze the exposure to attacks in AODV, specifically the most common network layer hazard, Black Hole attack. A specification based Intrusion Detection System (IDS) is developed using Genetic Algorithm approach. This system depends on Genetic Algorithm, which analyzes the behaviors of every node and provides details about the attack. Genetic Algorithm Control (GAC) is a set of various rules based on the vital features of AODV such as Request Forwarding Rate, Reply Receive Rate and so on. The performance of MANET is analyzed based on GAC. The misbehaving attacks that affect the security of the network are not detected.

D. Vydeki[16] have proposed a hybrid intrusion detection system for MANETs that detects black hole attack, by combining anomaly and specification-approaches of IDS. The proposed system aims at designing two different IDS using the two fundamental soft computing mechanisms such as, Fuzzy and Genetic Algorithm (GA). The fuzzy based system produces 81.8% true positive rate and the GA based system results in a 100% efficient detection. The mechanism to eliminate the detected attacks is not given.

Vydeki, D[17] have proposed the application of adaptive neuro-fuzzy inference system (ANFIS) in the design of a hybrid wireless intrusion detection system (WIDS) that detects the black hole attacks in mobile ad hoc networks (MANETs). The WIDS provides additional security to such networks and the proposed system consists of a hybrid scheme that combines the specification and anomaly based approaches. Executing the hybrid IDS using ANFIS improves the detection rate in MANETs. The proposed scheme uses Sugeno type FIS with fuzzy c-means clustering (FCM) and a hybrid neural network. The misbehaving or misuse attacks cannot be detected.

Maha Abdelhaq[18] have proposed a Local Intrusion Detection (LID) security routing mechanism for Black Hole Attack (BHA) detection over Ad hoc On Demand Distance Vector (AODV) MANET routing protocol. Here, the previous node of the attacker node was used for intrusion detection instead of using the source node as in Source Intrusion Detection (SID) security routing mechanism. The security mechanism overhead would be decreased. This mechanism can detect the attacks by individual nodes. If the attacks are made by a group of nodes, this mechanism will not detect the attack.

Anajana Devi[13] have proposed a scheme to detect misbehaving nodes as that set of monitoring nodes calculates the probability of forwarding packets, dropping packets, injecting packets because of malicious activity and the probability of loss packets due to exhausted battery power or malfunction. Then the nodes attack symptoms are estimated. The estimated set of misbehavior attack probabilities and symptoms are given as the input to the fuzzy membership functions. Based on the fuzzy rules, the attack confirmation and category is estimated.

III. OVERVIEW OF AODV PROTOCOL

The Ad hoc On-Demand Distance Vector (AODV) protocol enables dynamic, self-starting, multi-hop routing between participating mobile nodes wishing to establish and maintain an ad hoc network. AODV allows mobile nodes to obtain routes quickly for new destinations and does not require nodes to maintain routes to destinations that are not in active communication. AODV allows mobile nodes to respond to link breakages and changes in network topology in a timely manner. The operation of AODV is loop-free, and by avoiding the counting to infinity problem offers quick convergence when the ad hoc network topology changes (typically, when a node moves in the network). When links break, AODV causes the affected set of nodes to be notified so that they are able to invalidate the routes using the lost link.

Route Requests (RREQs), Route Replies (RREPs) and Route Errors (RERRs) are message types defined by AODV. When a route to a new destination is needed, the node broadcasts a RREQ to find a route to the destination. Each node receiving the request caches a route back to the originator of the request, so that the RREP can be unicast from the destination along a path to that originator. A route can be determined when the RREQ reaches a node that offers reachability to the destination. The route is made available by unicasting a RREP back to the origination of the RREQ.

For nodes monitoring the link status of next hops for active routes, when a link break in an active route is detected, the broken link is invalidated and a RERR message is typically transmitted to notify other nodes that the loss of that link has occurred. The RERR message indicates the destination that is no longer reachable by way of the broken link.

AODV is a routing protocol, and hence it deals with routing table management. Routing table information must be kept for all known routes. AODV uses the following fields with each routing table entry:

- Destination IP Address
- Prefix Size
- Destination Sequence Number
- Next Hop IP Address
- Lifetime (expiration or deletion time of the route)
- Hop Count (number of hops to reach the destination)
- Network Interface
- Other state and routing flags (e.g., valid, invalid)

Managing the sequence number is crucial to avoiding routing loops. A destination becomes unreachable when a link breaks or it is deactivated. When these conditions occur, the route is invalidated by operations involving the sequence number and marking the routing table entry state as invalid.

In AODV protocol, path selection for data transmission sequence number is used as main attribute. Which node sends reply with high sequence number in RREP packet is selected for transmission. Hereby Black hole attack is performed by modifying sequence number randomly by attacker node i.e. attacker node will set high sequence number randomly. So this scheme deals with authentication for identifying attackers by adding random number with RREP messages. If RREP message has random number that indicates RREQ is reached to destination and reply message is generated by destination node.

IV. BLACK HOLE ATTACK

The attacker or malicious node usually exploits some routing protocols to distribute itself as having the direct and shorter route to source whose packets it wants to grab. Once the attacker adds itself between the communicating nodes, it can do anything malicious with the packets passing between them. It can then choose to drop the packets thereby creating Denial of Service attacks. Security in mobile ad-hoc network is the most vital concern for basic functionality of a network . Accessibility of network services, confidentiality and integrity of data can be achieved by assuring that security issues have been met. MANET suffer from security attacks because they possess open medium, rapidly changing topology, lack of central administration and non-robust defense mechanism. Black hole Attacks are classified into two categories. In single black hole attack there is only one malicious node within a zone. Whereas in collaborative black hole attack multiple nodes in a group act as malicious nodes

In black hole attack[10][11], source nodes floods RREQ packets to its neighbors in order to reach destination. When malicious node receives an RREQ packets, intermediate node will not check its routing table, immediately sends a false RREP packet giving a route to destination over itself, by assigning a high sequence number to set in the routing table, before other nodes send a true

RREP packet. Therefore source nodes assume that route discovery process is completed and ignore other RREP messages and begin to send packets over malicious node. Malicious node attacks all RREQ messages this way and takes over all routes. Therefore all packets are sent to this malicious node and they will not be forwarding anywhere. This scenario is explained in fig.1

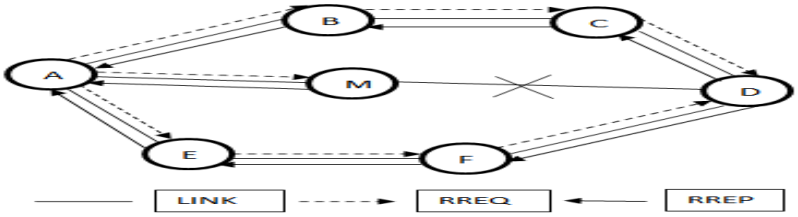

Fig. 1. Black Hole Attack

The above fig.1 depicts single black hole attack. Node S is source, node D is destination and Node M is malicious. Here source node broadcasts RREQ. All nodes including malicious node received this RREQ message. Then malicious node M set high sequence number in RREP message and sent it to source node S. Source node assumes received reply is gives fresh path and ignore other reply message and starts transmission via malicious node M.

V. PROPOSED WORK

In this proposed solution, during path detection process source node floods RREQ message to its neighbor nodes. This RREQ message will forwarded to all nodes. Malicious node and legitimate nodes are received this RREQ message. Normally in AODV protocol, RREP message can be generate by an intermediate node if it have fresh route to destination. But in this solution RREP should be generated by destination node only. It is done by set D field in RREQ message.

Step 1: Source floods RREQ packet to its neighbor
Step 2: Neighbor nodes receives RREQ packets
Step 3: Repeat
Step 4: Node n checks its IP address with received packet
Step 5: if not equal
Step 6: Forward RREQ to its neighbor
Step 7: else
Step 8: Go to step 10
Step 9: until RREQ reaches destination
Step 10: RREQ reached to destination
Step 11: Destination stores source's IP add in a variable IP_VAR and generate a Random number and store IP- RAND
Step 12: If IP_VAR is not stored before
Step 13: Store source's IP add into IP_VAR
Step 14: Generate random number
Step 15: Else If source's IP add==already stored IP_ADD
Step 16: Send reply RREP with RAN_NUM
Step 17: End if
Step 18: When source receives RREP packet checks RAND_NUM
Step 19: If all received RREP have same RAND_NUM
Step 20: There is no attack
Step 21: Else
Step 22: Attacker presented in network

Fig. 2. Black Hole Detection Algorithm

It indicates all RREQ message should reach to destination. Hereby destination only can generate RREP message. When destination generates RREP message it also add random number in each RREP packet. It deviates legitimate reply from fake reply. Overall flow diagram of the proposed system is show in figure 3.

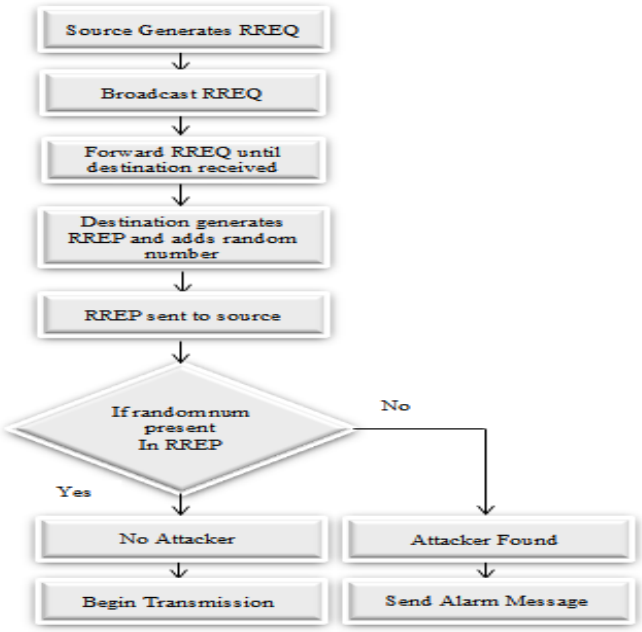

Fig. 3. Flow Diagram

Malicious node will send fake RREP message to source in order to participate in data transmission. When source will receive legitimate reply from destination and fake reply from malicious node it decided attacker is present in network. For this source node need to wait certain time to receive all RREP messages. Then source send alarm message to all nodes about attacker.

VI. PERFORMANCE ANALYSIS

A. SIMULATION METHODOLOGY

The Network Simulator (NS2) is used to simulate the proposed model. During the simulation, 26 mobile nodes move in a 1200 m x 800 meter region for 25 seconds of simulation time. All nodes have the same transmission range of 250 meters. The simulated traffic is Constant Bit Rate (CBR). The simulations are run by varying the number of attacker nodes. The following table shows parameters used in system simulation.

TABLE I. SIMULATION PARAMETER

Simulation Parameters	Value
No. Of Nodes	26
Area Size	1200 m x 800 m
MAC	IEEE 802.11
Transmission Range	250m
Simulation Time	25 sec
Traffic Source	CBR
Packet Size	512

B. PERFORMANCE METRICS

The following parameters are taken as performance metrics

1. True positive

   The ratio of attacker nodes are originally detected as attacker nodes is called true positive.

2. False positive

   The Ratio of Normal nodes are assumed as attacker nodes is called false positive.

3. Packet Delivery ratio

   It is defined as the ratio of number of packets received by the receiver to the number of packets delivered by the transmitter i.e. no of received packets / no of transmitted packets.

4. End-to-end Delay

   The time difference between actual time required to delivery all packets to destination and original time consumed to reach all packets to destination

TABLE II. PERFORMANCE METRICS

Metrics	Original Node Behavior	Detected As
True Positive	Attacked	Attacked
False positive	Normal	Attacked

C. RESULT

TRUE POSITIVE

Fig. 3 show the true positive ratio of the proposed system and the existing system for different number of attackers. The true positive ratio of the proposed system shows 7% more than existing system.

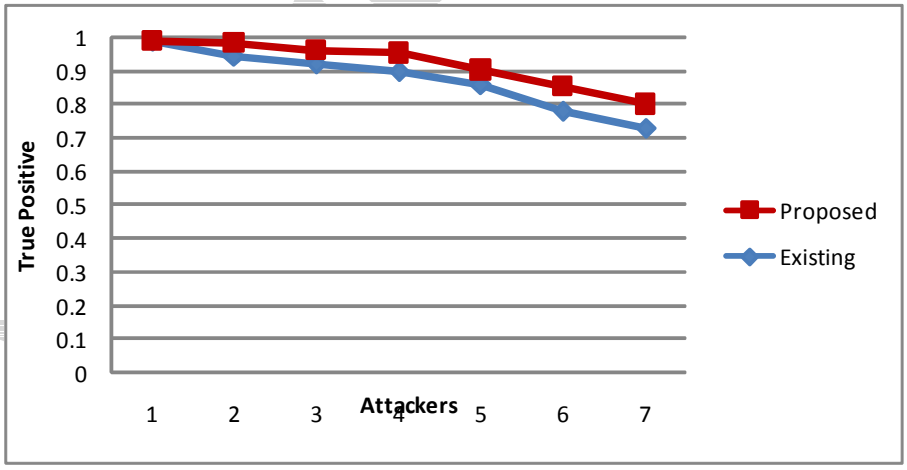

Fig. 4. True Positive

FALSE POSITIVE

Fig. 4 shows false positive ratio of the proposed system shows 16%, whereas existing system produces 20%.

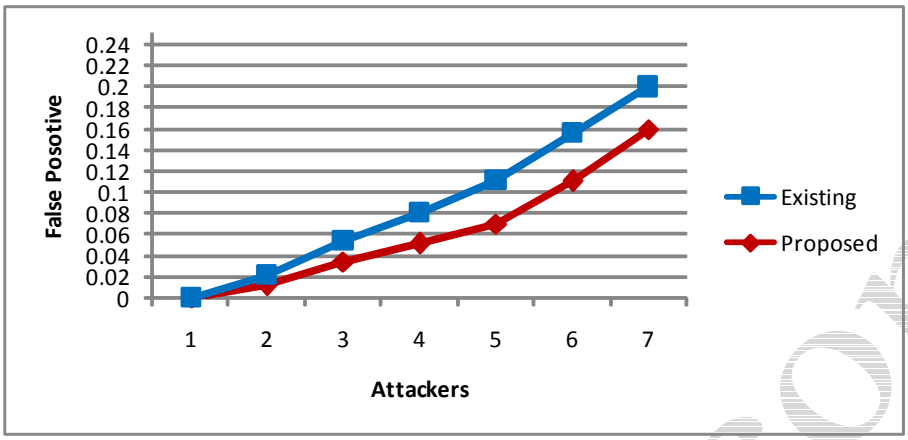

Fig. 5. False Positive

PACKET DELIVERY RATIO

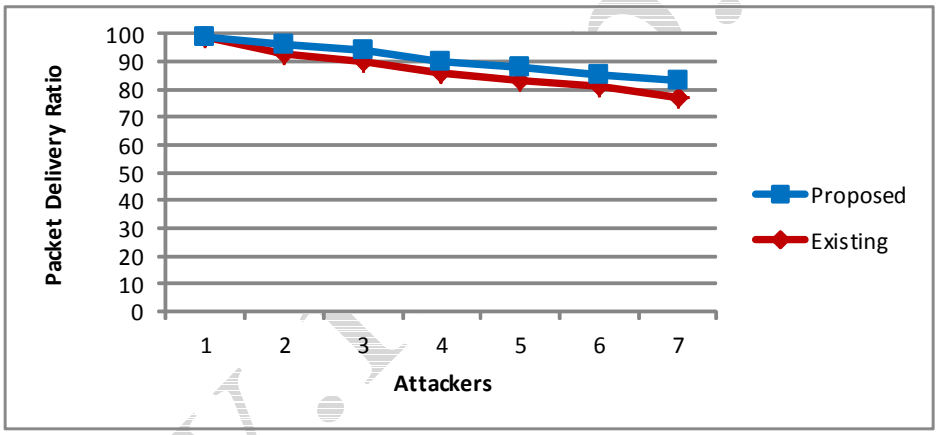

Fig. 6. Packet Delivery Ratio

Fig.5 shows packet delivery ratio of the proposed system shows 83%, whereas existing system produces 77%.

END-TO-END DELAY

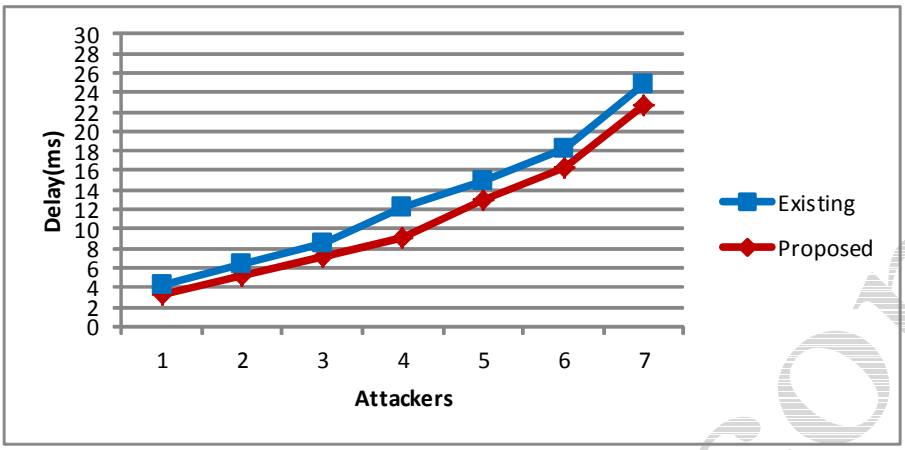

Fig. 7. End-to-End Delay

Fig.6 shows End-to-End delay of the proposed system shows 22.65ms whereas existing system exhibits 24.89ms.

4. PERFORMANCE RESULTS

TABLE III. TABLE PERFORMANCE RESULTS

Number of Attackers	True Positive (%)		False Positive (%)		Packet Delivery Ratio (%)		End-to-End Delay (%)	
	Existing	Proposed	Existing	Proposed	Existing	Proposed	Existing	Proposed
1	98.9	98.90	0	0	98.83	98.83	4.20	3.20
2	94.3	98.40	2.11	1.20	92.88	96.00	6.43	5.14
3	92	96.00	5.38	3.40	89.99	93.89	8.43	7.12
4	90	95.20	8.07	5.10	86.10	90.11	12.13	9.13
5	85.91	90.11	11.10	7.00	82.92	88.01	14.86	12.99
6	78.1	85.22	15.61	11.00	81.20	85.12	18.30	16.19
7	73	80.00	20.00	16.00	77.00	83.00	24.89	22.65

The detailed simulated data presented in Table III.

VII. CONCLUSION

A MANET is more open to many 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. Black hole attack is a kind of attack, which 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. 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 for future attacks. To counter this attack, data collection table is used. This table mainly stores two types of information- the node from which the packets comes and the node through which its forwards the packets.

In this paper the black hole attack is handled in path routing process itself. The attacker node is identified and isolated from network before data transmission is started. Also performance metrics are gained with high results. Attacker node is identified before data transmission is started so data delivery ratio is achieved with good results. Meanwhile End-to-end delivery ratio also reduced. According to performance analysis, this project exposes feasible result in every parameter. In true positive, proposed project achieves more 7% of attacker detection compare existing system. Existing system produces 73% of true positive in same

network features. In False positive proposed system results 16% when existing produces 20%. False positive is a crucial decision in detection of black hole attack. So every proposed solution should be minimum as much as possible in this parameter. In packet delivery ratio, proposed project finds attacker in routing path itself. So maximum of packet delivery ratio is gained. The proposed system exhibits 98.83% with 3 attackers. In end-to-end delay, proposed system show 26s of delay. But existing system produces 3s more in detection process.

A. FUTURE ENHANCEMENT

Co-operative attack is type of network layer attack where two nodes (i.ie. Within range) compromised and aim to drop packets. Adding of energy and distance based solutions provides more feasible solution to this co-operative attacks. Constructing of new protocol leads to minimum time required to detect attacker. In future solution constructing of strong novel solution that produce better results in performance metrics like packet delivery ratio and end-to-delay etc.

References

[1] J. Sen, M. Chandra, P. Balamurlidhar, S.G. Harihara and H.Reddy, "A Distributed protocol for detection of packet dropping attack in Mobile Ad hoc Networks", Proc. IEEE Conference on Telecommunication and Malaysian International Conference on Communication (ICT-MICC), 2007.

[2] O.F. Gonzalez-Duque, M. Howarth and G. Pavlou, "Detection of packet forwarding misbehaviour in Mobile Ad hoc Networks", Proc. International Conference on Wired/Wireless Internet Communications (WWIC 2007), pp 302-314, Portugal, June 2007.

[3] O.F. Gonzalez-Duque, G. Ansa, M. Howarth and G. Pavlou, "Detection and accusation of packet forwarding misbehavior in Mobile Ad hoc Networks", Journal of Internet Engineering, Vol.2, No.8, pp 181-192, June 2008.

[4] S. Marti, T.J. Giuli, K.Lai and M. Baker, "Mitigating routing misbehavior in Mobile Ad Hoc Networks", Proc. International Conference on Mobile Computing and Networking, pp 255- 265, 2000.

[5] P.Yi, Z.Dai, Y. Zhong and S.Zhang, "Resisting flooding attack in Ad Hoc Networks", Proc. IEEE International Conference on Information Technology Coding & Computing ITCC, April 2005.

[6] W.Yu and K.Ray, "Defense against injecting traffic attack in cooperative Ad Hoc Networks", Proc. IEEE GLOBECOM, St. Louis, Missouri,
USA, Dec. 2005.

[7] M. Medadian, M.H. Yektaie and A.M. Rehmani, "Combat with Black Hole Attack in AODV Routing Protocol in MANETs", Proc. IEEE Asian Himalayas International Conference on Internet, Nov. 2009.

[8] Harmandeep Singh, Manpreeet Singh, "Effect of Black Hole attack on AODV, OLSR and ZRP protocol in MANET", International Journal of Advanced Trends in Computer Science and Engineering, pp volume 2 May-2013

[9] Jaspal Kumar, M. Kulkarni, Daya Gupta, "Effect of Black Hole Attack on MANET Routing Protocols", I. J. Computer Network and Information Security, pp vol 5 April 2013.

[10] Vipan Chand Sharma, Atul Gupta, Vivek Dimri, " Detection of Black Hole Attack in MANET under AODV Routing Protocol", International Journal of Advanced Research in Computer Science and Software Engineering, pp volume 3 june 2013.

[11] Anjana Devi V & Bhuvaneswaran, RS, "Agent based Cross layer intrusion detection system for MANET", In the Proceedings of 4th international conference, CNSA 2011, July 2011 Springer-Heidelberg (CCIS) vol. 196, pp.427-440.

[12] Anjana Devi V & Bhuvaneswaran, RS, "Adaptive association rule mining based cross layer intrusion detection system for MANET", International journal of network security and its applications, vol.3, no. 5, pp.243-256 September 2011.

[13] Anjana Devi V & Bhuvaneswaran, RS, "Fuzzy based decision model for detecting misbehaving attacks in MANET", International Journal of Applied Engineering Research, vol.9, no.23, pp.20059-20083, 2014.

[14] Anjana Devi V & Bhuvaneswaran, RS, 'ECC based malicious node detection system for MANET', Journal of Theoretical and Applied Information Technology, vol.68, no.2, pp.239-248. Oct.2014.

[15] K.S.Sujatha, Vydeki Dharmar et al, "Design of Genetic Algorithm based IDS for MANET", Recent Trends in Information Technology (ICRTIT), 2012 International Conference on IEEE 2012.

[16] D. Vydeki, K. S. Sujatha et al, "Design of Soft Computing based Black Hole Detection in MANET", International Conference on Wireless Information Networks and Systems, WINSYS 2012.

[17] D. Vydeki et al, "Design of Wireless IDS using Adaptive Neuro-Fuzzy Inference System", European Journal of Scientific Research ISSN 1450-216X Vol. 90 No 1 November, 2012.

[18] Maha Abdelhaq, Sami Serhan, Raed Alsaqour and Rosilah Hassan, "A Local intrusion detection routing security over MANET Network", International Conference on Electrical Engineering and Informatics,17-19 July 2011, Bandung, Indonesia, 2011.