Volume 2, Issue 1, January 2017 ISSN (online): 2456-0006

International Journal of Science Technology Management and Research

Available online at: www.ijstmr.com

PAAP: Packet Drop Attack Avoidance Protocol with Attack Variation Scenario

Gayatri Bendale
Department of Computer Science & Engg.
Sri Aurobindo Institute of Technology
Indore, India

Prof.Sameeksha Shrivastava
Department of Computer Science & Engg.
Sri Aurobindo Institute of Technology
Indore, India

Abstract: ***MANET is a decentralized network that has no infrastructure and nodes can communicate with each other by multi-hoping the messages. Due to this nature of MANET, it is prone to many security attacks in which packet drop attacks are very common. Various packet drop attacks like Blackhole attacks, Grayhole attack, Cooperative Blackhole attack, etc are the attacks that become a bottleneck in efficient routing and security in MANET. Various mechanisms are devised in past but none of them prove to be effective against all types of packet drop attacks. In this paper, a mechanism is formulated that enhances the AOMDV routing protocol by use of AOMDV modification. Here we present 2 different scenarios of the black-hole attack. 1) When there are nodes available. For single attacker, 2) when there are more than one attackers are available. The all procedure show by the experimental result provided using network simulator version 2.***

Keywords : MANET, Black-hole, NS2, Security, Routing, AOMDV.

I. INTRODUCTION

NETWORK security is a weak link in wired and wireless network systems. Malicious attacks have caused tremendous loss by impairing the functionalities of the computer networks. Therefore, security is a major concern for protected communication between mobile nodes in a hostile environment. In hostile environments adversaries can bunch active and passive attacks against intercept able routing in embed in routing message and data packets [1]. Mobile ad hoc network (MANET) is one of the most up-and- coming fields for research and review of wireless network. Essential requirement in MANET is security. In ad hoc network the communicating nodes sets new challenges for the security architecture because it doesn't necessarily feed on fixed infrastructure. The ad-hoc network is more vulnerable to Packet drop attack i. e. Black-hole attack forcefully initiate through malicious nodes or attacker. In networking, Nodes can be anything like systems or devices i.e. mobile phone, laptop, personal digital assistance, MP3 player and personal computer that are participating in the network and free to moving in and out in the network. At the same time nodes can act as host as well as router and form inconsistent topologies pivot on their comparability with each other in the network. Because of their self-alignment ability these nodes have the capability to reconfigure itself [2].

II. BACKGROUND

This section describes the key features of different routing protocols that are supporting the Mobile ad hoc network such as DSDV, DSR, and AODV protocols. That also describes the particular parameters that are used for implementing protocols:

A. Destination-Sequenced Distance Vector (DSDV)

Destination-Sequenced Distance-Vector Routing (DSDV) is a table-driven routing scheme for ad hoc mobile networks based on the Bellman-Ford algorithm. The improvement made to the Bellman-Ford algorithm includes freedom from loops in routing tables by using sequence numbers. It was developed by C. Perkins and P. Bhagwat in 1994. The DSDV protocol can be used in mobile ad hoc networking environments by assuming that each participating node acts as a router. Each node must maintain a table that consists of all the possible destinations. DSDV requires a regular update of its routing tables, which uses up battery power and a small amount of bandwidth even when the network is idle. Whenever the topology of the network changes, a new sequence number is necessary before the network re-converges; thus, DSDV is not suitable for highly dynamic networks [3].

B. Dynamic Source Routing (DSR)

Dynamic Source Routing (DSR) is a routing protocol for wireless mesh networks and is based on a method known as source routing. It is similar to AODV in that it forms a route on-demand when a transmitting computer requests one Except that each intermediate node that broadcasts a route request packet adds its own address identifier to a list carried in the packet. The destination node generates a route reply message that includes the list of addresses received in the

route request and transmits it back along this path to the source. Route maintenance in DSR is accomplished through the confirmations that nodes generate when they can verify that the next node successfully received a packet. These confirmations can be link-layer acknowledgements, passive acknowledgements or network-layer acknowledgements specified by the DSR protocol. However, it uses source routing instead of relying on the routing table at each intermediate device. When a node is not able to verify the successful reception of a packet it tries to retransmit it. When a finite number of retransmissions fail, the node generates route error message that specifies the problematic link, transmitting it to the source node [4].

C. Ad-hoc on Demand Distance Vector (AODV)

AODV is essentially a combination of both DSR and DSDV. It borrows the basic on-demand mechanism of Route Discovery and Route Maintenance from DSR, plus the use of hop-by-hop routing, sequence numbers, and periodic beacons from DSDV [4]. In order to maintain routes, AODV normally requires that each node periodically transmit a HELLO message, with a default rate of once per second. Failure to receive three consecutive HELLO messages from a neighbour is taken as an indication that the link to the neighbour in query is down. Alternatively, the AODV specification briefly suggests that a node may use physical layer or link layer methods to detect link breakages to nodes that it considers neighbours [5].

III. LITERATURE SURVEY

Numerous Researchers have worked on multiple detection and prevention of Black-hole attacks in mobile ad hoc network, based on the detection mechanism, the existing techniques of detecting and preventing Blackhole attacks can be illustrate in this section.

An ad hoc network is a group of wireless mobile computers (or nodes) wherein individual nodes cooperate by forwarding packets for each other to allow nodes to communicate beyond direct wireless transmission range. The Black hole attack is an important problem that could happen easily in ad hoc networks especially in popular on demand protocols Like the Adhoc On-demand Distance Vector Rooting (AODV). Prior research in ad hoc networking has generally looked into the routing problem in a now adversarial network setting, assuming a reasonably trusted environment In this paper Animesh Patcha et al. [6] proposes a collaborative architecture to detect and exclude malicious nodes that act in groups or alone. The focus is on the network layer, using the Adhoc On-demand Distance Vector Rooting (AODV) protocol as an example. This paper describes an extension to the watchdog method to incorporate a collaborative architecture to tackle collusion amongst nodes.

Security is an essential requirement in mobile ad hoc networks to provide protected communication between mobile nodes. Due to unique characteristics of MANETS, it creates a number of consequential challenges to its security design. To overcome the challenges, there is a need to build a multifence security solution that achieves both broad protection and desirable network performance. MANETs are vulnerable to various attacks, blackhole, is one of the possible attacks. Black hole is a type of routing attack where a malicious node advertise itself as having the shortest path to all nodes in the environment by sending fake route reply. By doing this, the malicious node can deprive the traffic from the source node. It can be used as a denial-of-service attack where it can drop the packets later. In this paper, Payal N. Raj et al [7] proposed a DPRAODV (Detection, Prevention and Reactive AODV) to prevent security threats of blackhole by notifying other nodes in the network of the incident. The simulation results in ns2 (ver- 2.33) demonstrate that our protocol not only prevents blackhole attack but consequently improves the overall performance of (normal) AODV in presence of black hole attack.

Mobile Ad hoc NETwork (MANET) is self configuring network of mobile node connected by wireless links and considered as network without infrastructure. Routing protocol plays a crucial role for effective communication between mobile nodes and operates on the basic assumption that nodes are fully cooperative. Because of open structure and limited battery-based energy some nodes (i.e. selfish or malicious) may not cooperate correctly. After becoming part of active path, theses nodes start refusing to forward or drop data packets thereby degrades the performance of network. In this paper, Aishwarya Sagar Anand Ukey et al. [8] a new reputation based approach is proposed that deals with such routing misbehavior and consists of detection and isolation of misbehaving nodes. Proposed approach can be integrated on top of any source routing protocol and based on sending acknowledgement packets and counting the number of data packets of active path.

Mobile ad-hoc networks are prone to a number of security threats. The fact that mobile ad-hoc networks lack fixed infrastructure and use wireless link for communication makes them very susceptible to an adversary's malicious attacks. Black hole attack is one of the severe security threats in ad-hoc networks which can be easily employed by exploiting vulnerability of on-demand routing protocols such as AODV. In this paper, Yibeltal Fantahun Alem [9] have proposed a solution based on Intrusion Detection using Anomaly Detection (IDAD) to prevent black hole attacks imposed by both single and multiple black hole nodes. Result of a simulation study proves the particular solution maximizes network performance by minimizing generation of control (routing) packets as well as effectively preventing black hole attacks against mobile ad-hoc networks.

In this paper, Shalini Jain et al. [10] propose an algorithm to detect a chain of cooperative malicious node in ad-hoc network that disrupts transmission of data by feeding wrong routing information along with the detection algorithm. They also propose a mechanism to detect and remove the black and gray hole attacks. Our technique is based on sending data in terms of equal but small sized blocks instead of sending whole of data in one continuous stream. The flow of message

is monitored independently at the neighborhood of both source and destination. The result of monitoring is gathered by a backbone network of trusted nodes. Our algorithm takes O(n) time on average to find the chain of malicious nodes which is better than earlier O(n^2) time bound for detecting a single black hole network.

IV. PROPOSED SYSTEM

The proposed work is intended to find an adoptable security algorithm formulation by which the mobile ad hoc network becomes secure**.**

A. *Methodology*

Black-hole is a severe type of routing protocol threat, accomplished by dropping packets and interrupted wireless services, which can be easily employed against routing in wireless ad-hoc networks, and has the effect of making the destination node unreachable or downgrade communications in the network. The black holes are invisible and can only be detected by monitoring lost traffic. The emergence of new applications of these networks necessitates the need for strong privacy protection and security mechanisms . Description:

The proposed routing process is taken place in the given manner in following figure. Some of basic steps of the proposed routing protocol can be described as:

Firstly, we configured the network in idealized manner that is initiation of the network system. In this condition, different nodes are created for communication so those nodes have been created route discovery from source to destination using Route Reply and Route Request. For route discovery process in this phase the routing protocol is initiate a communication session for that purpose first the source router send a RREQ message and waits for reply. As the source router get the route reply RREP packets. The entire routes are listed in source router. According to the surveys the malicious attacker finds on the first routes always thus first routes are discarded in most of the prevention technique. Moreover, for threshold calculation different routing constraints for process are placed. Therefore we estimated thresholding average value. This average value broadcast the entire network. This broadcast value used for checks where we find out malicious attacker are exists or not. For all we have repeated this process for same number of nodes. After this process, we check efficient multipath route available or not, if there are multiple routes are exists we select most efficient path and forward packet to destination, if a route is not valid or secure then jump to the check condition of route validation.

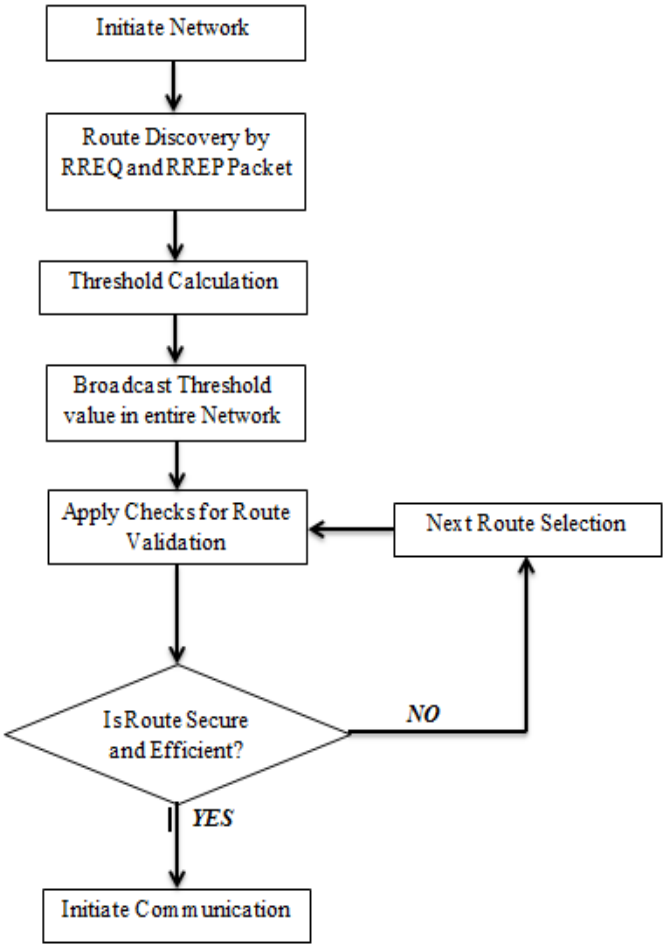

Figure 1: Proposed Flow Chart

B. Proposed Algorithm

Table 1: Threshold Estimation

Input: Number of Nodes **Output:** Threshold Data for initiation of Malicious Detection
1: Initialize the Network, with N nodes where $N = 1, 2, 3, \ldots\ldots$., in ideal condition. **2:** Initialize Route Discovery by Source Node N_s **3:** N_s sends RREQ Packets to Destination N_d **4:** Wait Until all Route Replies not received **5:** Compute Timestamp T_s for each node $\Delta T_s = t_n - t_m$ **6:** Compute Average Threshold of all nodes $\delta_{threshold} = \frac{1}{N}\sum_{i=0}^{N} \Delta T_{s_i}$ **7:** Count Number of Packet drop during simulation $Packet\ Drop = Total\ Send - Total\ Received$ **8:** Compute Average Threshold of all nodes $\emptyset_{Pd} = \frac{1}{N}\sum_{i=0}^{N} PacketDrop_i$ **9:** Count Remain Energy for each node $\mu_{Energy} = \frac{1}{N}\sum_{i=1}^{N} E_i$ Where the E_i is the amount of energy dropped by a node i **10:** Compute Average Threshold value for Energy $\rho_E = \frac{1}{N}\sum_{i=1}^{N}(E_i - \mu_{Energy})^2$ **11:** Broadcast the $\delta_{threshold}$, $\emptyset_{Pd}$, ρ_E to the entire network

Table 2: Detection and Prevention of Black-hole Attack

Input: Number of Nodes **Output:** Found Malicious Activity, Detection and Prevention
Process: **1:** for each node in suspected list **2:** ***if*** $(\Delta T_s > \delta_{threshold} \&\& \mu_{Energy} < \rho_E)$ ***then*** **3:** Label node as malicious **4:** ***else*** **5:** Route is secured and initiate communication **6:** For each reliable route in network **7:** ***if*** $(PacketDrop_i > \emptyset_{Pd})$ ***then*** **8:** for this, route is not reliable **9:** ***else*** **9:** Select alternative route for transmission **10:** ***end if*** **11:** ***end for***

V. IMPLEMENTATION

The simulation is being implemented in the Network simulator [11]. Protocol used here is AOMDV.

Table 3: Simulation Scenarios

Parameters	***Values***
Antenna Model	Omni Antenna
Dimension	1000 X 1000
Radio-Propagation	Two Ray Ground
Channel Type	Wireless Channel
Traffic Model	CBR
Routing Protocol	AOMDV
Mobility Model	Random Waypoint
Number of Attackers	5
Number of Nodes	100

Network Scenarios 1

I. Simulation of AOMDV protocol when Attack Condition:

In this phase, we demonstrated the basic AOMDV routing protocol with attack condition. Therefore the second simulation is prepared for attack prevention which is confirmed in figure 2. In this simulation screen the green nodes demonstrate as normal legitimate node in network. The given simulation is developed using the AOMDV routing protocol. When the proposed method is deployed network performance is improve and large number of packet is delivered to the destination. Communication is happened between source node 9 and destination mode 18.

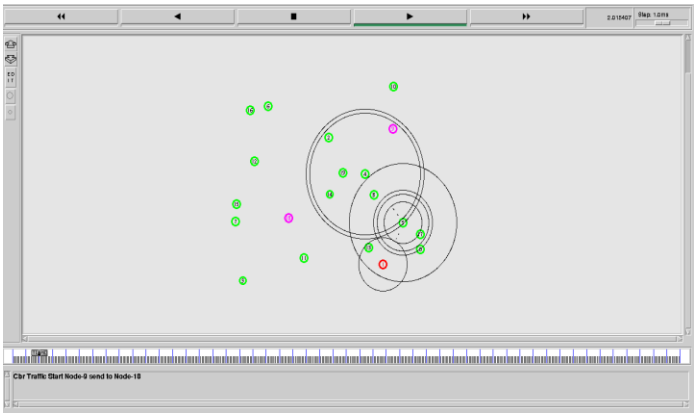

Figure 2: AOMDV under Attack Condition

II. Simulation using the Proposed Secure Routing Technique:

In this simulation scenario the proposed routing technique which is developed with the help of AOMDV routing modifications are implemented with the Mobile ad hoc network. Additionally a similar kind of attacker node on the network is deployed. The deployed attacker is normalized using the technique and their performance is estimated on the basis of the network trace files. Additionally the measured performance is compared with the base RBDR approach performance under attack conditions. The figure 2 demonstrates the simulation screen of the proposed secure routing technique for Blackhole Attack prevention.

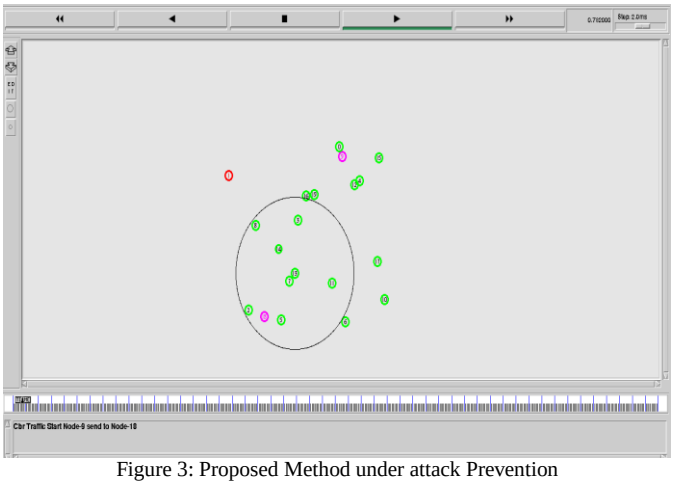

Figure 3: Proposed Method under attack Prevention

Network Scenarios 2

In this scenario, below figures shows the distinction of attacker situation and their description. We implemented 1, 2, 5, 7, 10 nodes of attack variation. Here we are showing only 5 black-hole nodes in the network

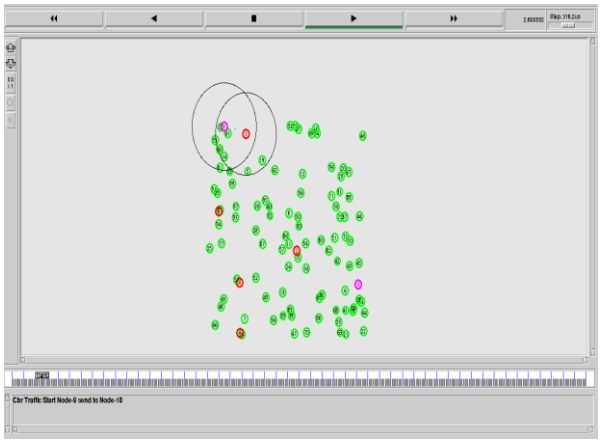

Figure 4: Attacker deployed in Network

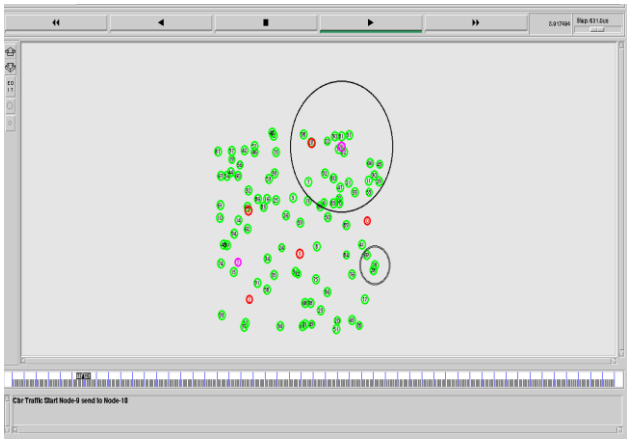

Figure 5: Traditional RBDR Approach

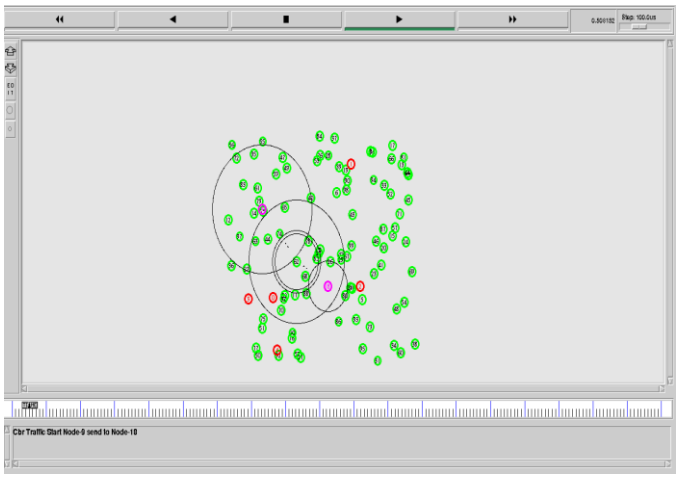

Figure 6: Proposed Method for Attack Variation

In black-hole attack, that initiate dos attack condition, thus have to be compelled to avoid and prevent from Attacker to network. Here, we have a tendency to area unit showing depiction of the network state of affairs with attack variation. In figure 3,show that standard network once there area unit five black-hole attackers deployed. Once there's range of Attacker will increase within the network, it's serious issue of the safe communication. Whereas there Attacker resides in network, have to be compelled to be deployed technique to the mobile network from the malicious activity. Therefore we have a tendency to deployed a way PAAP i.e. packet drop attack avoidance protocol for mobile network. This technique shows exploitation figure four. In next, we have a tendency to discuss state of affairs of old approach that is depicting in figure five. All told this, clearly show that RDBR not giving satisfactory performance as compared to our technique PAAP.

VI. RESULT ANALYSIS

The given section provides the 2 result situation with number of node and with number of attackers, understanding and detailed description of the obtained results :

A. End to End delay

End to end day on network refers to the time taken, for a packet to be transmitted across a network from source to destination device, this delay is calculated using the below given formula.

$$E2E\ Delay = Receiving\ Time - Sending\ Time$$

Figure 7 shows the comparative End to End Delay of the traditional AOMDV routing and the proposed secure routing technique. In this figure the X axis contains the number of nodes in network and the Y axis shows the performance of network in terms of milliseconds. According to the obtained results the proposed technique is produces less end to end delay as compared to traditional routing technique under attack conditions.

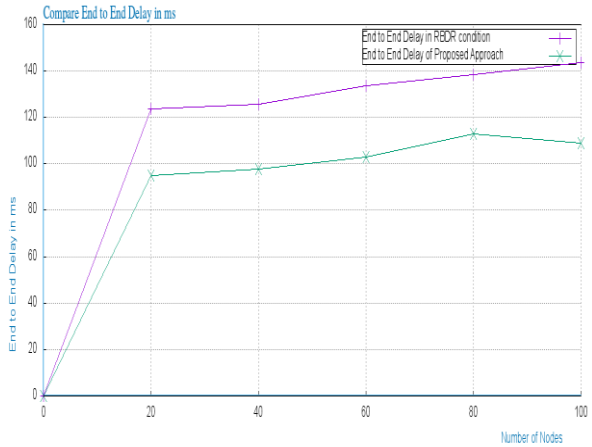

Figure 7: End to End Delays

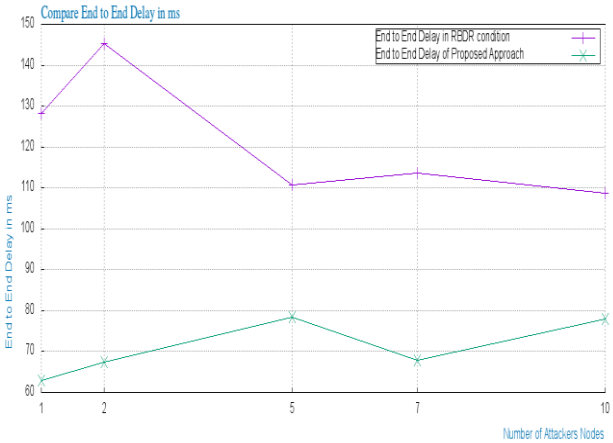

Figure 8: End to End Delays with number of attack

Figure 7 shows the different attacker node of end to end delay parameter. Therefore the proposed technique is an efficient technique and produces less amount of time.

B. Packet Delivery Ratio

The performance parameter Packet delivery ratio sometimes termed as the PDR ratio provides information about the performance of any routing protocols by the successfully delivered packets to the destination, where PDR can be estimated using the formula given

$$Packet\ Delivery\ Ratio = \frac{Total\ Delivered\ Packets}{Total\ Sent\ Packets}$$

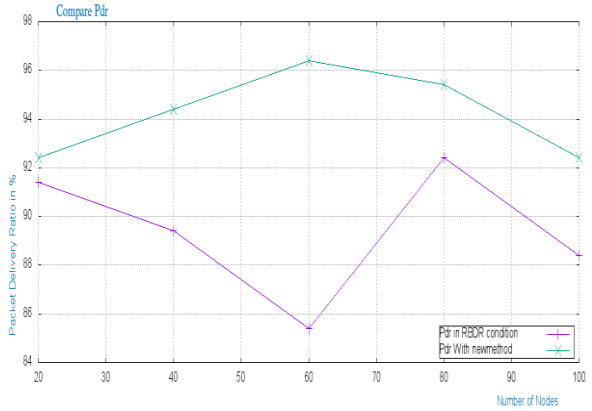

Figure 9: Packet Delivery Ratios

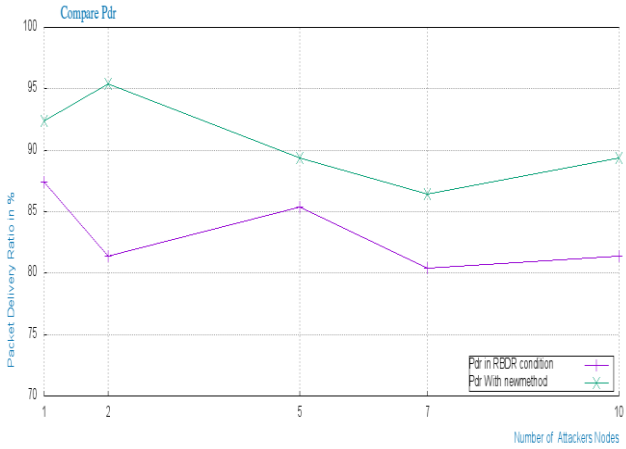

Figure 10: Packet Delivery Ratios with number of attack

The comparative packet delivery ratio of the networks is given using figure 9, in this diagram the X axis shows the number of nodes in the network and the Y axis shows the amount of packets successfully delivered in terms of the percentage. The blue line of diagram represents the performance of the traditional RBDR technique and the green line shows the performance of the proposed PAAP technique. Similarly figure 10 given the scenario of the 5 attacker node in the network. According to the obtained results the proposed technique delivers more packets as compared to the

traditional technique even when the network contains the attacker node therefore the proposed technique able to escape the attack effect and improve the network performance.

C. Throughput

Network throughput is the average rate of successful message delivery over a communication channel. This data may be delivered over a physical or logical link, or pass through a certain network node. The throughput is usually measured in bits per second (bit/s or bps), and sometimes in data packets per second or data packets per time slot.

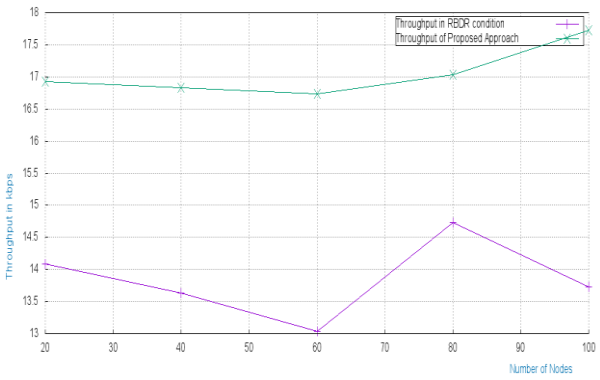

Figure 11: Compare Throughput

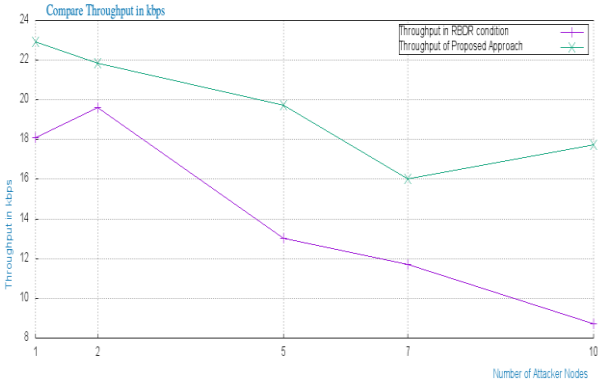

Figure 12: Compare Throughput with number of attack

The comparative throughput of the network is demonstrated using figure 11, in this diagram the X axis shows the number of nodes in network and the Y axis shows the throughput of the network in terms of KBPS. The green line in this diagram shows the performance of the proposed technique and the blue line shows the performance of the traditional RBDR routing. According to the obtained performance the proposed technique improve the throughput of the network during the attack conditions also therefore the technique is effectively avoid the attack effect as compared to the traditional routing technique. Also while malicious node increases in network performance is decreases. Therefore our proposed approach is applicable where there is large number of black-hole nodes are available. This process shows in figure 12.

D. Routing Overhead

Routing overhead is described as the amount of additional packets injected in network for communication. The key reason behind to compute this parameter is, because the routing overhead reduces the packet delivery ratio and transmission rate of the data. The given figure 6 shows the performance of network in terms of routing overhead. The routing overhead increases the amount of bandwidth consumption.

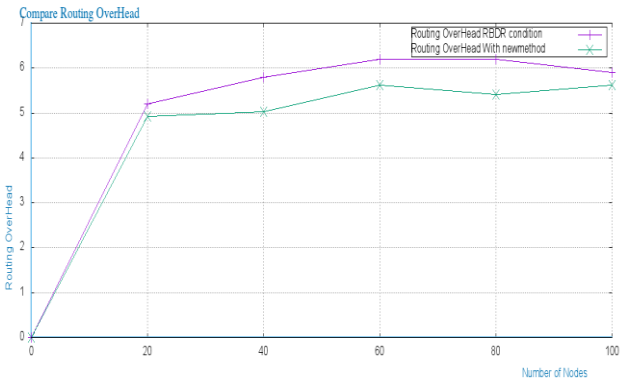

Figure 13: Compare Routing Overhead

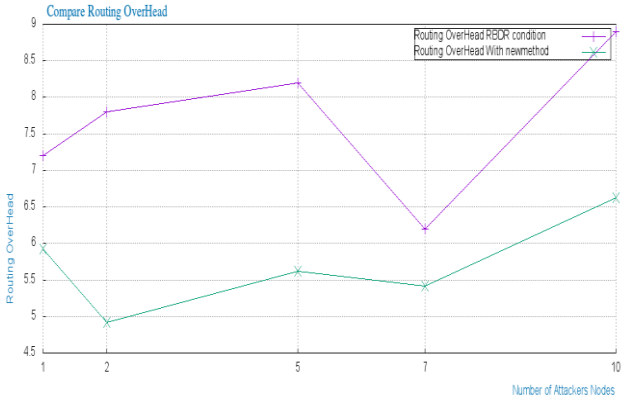

Figure 14: Compare routing overhead with number of attack

According to the obtained results the network under the attack condition increases the routing overhead of the network thus the traditional RBDR routing protocol shows increasing routing overhead of network. On the other hand when the network is configured through the proposed routing protocol the routing overhead becomes constant. Therefore the proposed method is able to recover the network from the Black hole attack. Routing overhead is great impact on the network while malicious node is in majority or node. Since therefore figure 14 demonstrate 5 attacker node on x-axis and y-axis show network performance in terms of routing overhead.

CONCLUSION

Perhaps the most widespread notion of a mobile ad hoc network is a network formed without any central administration which consists of mobile nodes that use a wireless interface to send packet data. Since the nodes in a network of this kind can serve as routers and hosts, they can forward packets on behalf of other nodes and run user applications. In this paper, we investigated some of the existing solutions for Black-hole attacks. Therefore Timestamp based security approach is proposed for implementing extensive reactive based routing protocol AOMDV. In this paper we enlarge the work with two different scenarios. First one is normal AOMDV protocol network and second is number of attacker nodes. With successful implementation of both scenarios are listed in result section. As a result of time stamped based routing, PDR, throughput is increased and End-to-End Delay and routing overhead is decreased.

REFERENCES

1. Priyanka Goyal, Sahil Batra and Ajit Singh, "A Literature Review of Security Attack in Mobile Ad-hoc Networks", International Journal of Computer Applications, Volume 9– No.12, November 2010.
2. Khushboo Sawant and Dr. M.K Rawat, "Survey of DOS Flooding Attacks over MANET Environment", International Journal of Engineering Research and Applications, Volume 4, Issue 5, Version 6, PP.110-115, May 2014.
3. S. A. Ade and P. A. Tijare, "Performance Comparison of AODV, DSDV, OLSR and DSR Routing Protocols in Mobile Ad-Hoc Networks", International Journal of Information Technology and Knowledge Management, Volume 2, No. 2, pp. 545-548, July - December 2010
4. Nikhil Kumar, Vishant Kumar and Nitin Kumar, "Comparative Study of Reactive Routing Protocols AODV and DSR for Mobile Ad hoc Networks", International Journal of Computer Science and Information Technologies (IJCSIT), Volume 5, pp.6888-6891, 2014.
5. M. S. karthikeyan, K. Angayarkanni, and Dr. S. Sujatha, "Throughput Enhancement in Scalable MANETs using Proactive and Reactive Routing Protocols", In Proceedings of the International Multi Conference of engineering and computer science, Volume 2, March 2010.
6. Patcha, Animesh, and Amitabh Mishra, "Collaborative security architecture for black hole attack prevention in mobile ad hoc networks," Radio and Wireless Conference, RAWCON'03, Proceedings, IEEE, 2003.
7. Raj, Payal N., and Prashant B. Swadas. "Dpraodv: A dyanamic learning system against blackhole attack in aodv based manet." arXiv preprint arXiv:0909.2371 (2009).
8. Ukey, Aishwarya Sagar Anand, and Meenu Chawla. "Detection of packet dropping attack using improved acknowledgement based scheme in MANET." IJCSI International Journal of Computer Science Issues 7.4 (2010): PP. 12-17.
9. Alem, Yibeltal Fantahun, and Zhao Cheng Xuan. "Preventing black hole attack in mobile ad-hoc networks using Anomaly Detection", Future Computer and Communication (ICFCC), 2010 2nd International Conference on, Vol. 3, IEEE, 2010.
10. Jain, Shalini, Mohit Jain, and Himanshu Kandwal, "Advanced algorithm for detection and prevention of cooperative Black and Gray-hole attacks in mobile ad hoc networks." International Journal of Computer Applications 1.7 (2010): PP. 37-42.
11. The Network Simulator. NS-2 [Online] http://www.isi.edu/nsnam/ns/