International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-5 Issue-5, June 2016

An Improved Detection and Prevention Method for Defending Packet Drop and DOS Attacks in Mobile Adhoc Networks

Kamlesh Patel, Abhishek Thoke

***Abstract:** In recent year with the widespread use of mobile device, Mobile Ad hoc networks (MANETs) technology has been attracted attention day by day. Specially, MANETs suit for military operations and the emergent disasters rescue that need to overcome terrain and special purpose in urgent. 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 AOMDV. Furthermore, DOS attack is a fairly new type of attack to cripple the availability of Internet services and resources. A DOS attack can originate from anywhere in the network and typically overwhelms the victim server by sending a huge number of packets. In this paper, we have proposed a solution based on malicious detection and prevention method to defend black hole and DOS attacks imposed by both single and multiple nodes. Result of a simulation study proves the particular solution maximizes network performance by minimizing generation of control (routing) packets. The effectiveness of our mechanism is illustrated by simulations conducted using network simulator ns-2.*

***Keywords:** AOMDV, Routing Protocol, Black-hole, DOS, Communication, Network Simulator*

I. INTRODUCTION

The emergence of such new networking approaches sets new challenges even for the fundamentals of routing since the mobile ad-hoc networks (MANET) are significantly different from the wired networks.

Moreover, the traditional routing protocols of the Internet have been designed for routing the traffic between wired hosts connected to a static backbone; thus, they cannot be applied to ad hoc networks because the basic idea of such networks is mobility with dynamic topology.

In a MANET, a collection of mobile hosts with wireless network interfaces form a temporary network without the aid of any fixed infrastructure or centralized administration. A MANET is referred to as an infrastructure less network because the mobile nodes in the network dynamically set up paths among themselves to transmit packets temporarily. In a MANET, nodes within each other's wireless transmission ranges can communicate directly; however, nodes outside each other's range have to rely on some other nodes to relay messages. Any routing protocol must encapsulate an essential set of security mechanism [1].

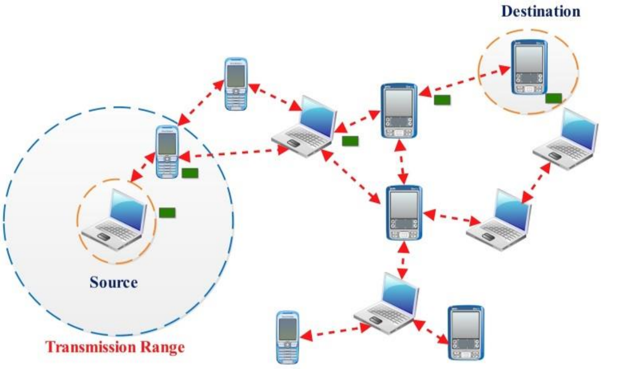


Figure 1 Mobile Ad-hoc Network

MANET can provide rapid connection between independent mobile users. Examples include establishing survivable, efficient, dynamic communication for emergency/rescue operations, disaster relief efforts, military networks, conference or campus networks, car networks, personal networks, etc.

The characteristics of MANET along with mobility and radio broadcast medium leads to some major issues for MANETs such as IP addressing, radio interference, routing protocols, power constraints, security, mobility management, service discovery, bandwidth constraints, Quality of Services (QoS), etc. [2].

Two of the most common attacks are DOS and Black-hole attacks in MANET. In Black-hole attack, the malicious node generates and propagates fabricated routing information and advertises itself as having a valid shortest route to the destined node [3]. If the malicious node replies to the requesting node before the genuine node replies, a false route will be created. Therefore, packets do not reach to the specified destination node; instead, the malicious node intercepts the packets, drops them and thus, network traffic is absorbed [4]. A DOS attack is said to be on the link layer when it can be launched by exploiting any vulnerabilities of data link layer protocols. DOS attacks may impact the network connectivity seriously and further undermine the networking functions, such as control and data message delivery. Both Black-hole and DOS attacks disturb route discovery process and degrade network's performance [5].

Manuscript published on 30 June 2016.
***** Correspondence Author (s)

Kamlesh Patel*, Scholar, Department of Information Technology, Technocrat Institute of Technology, Bhopal, India.
Abhishek Thoke, Assistant Professor, Department of Information Technology, Technocrat Institute of Technology, Bhopal, India.

The remainder of paper is organized as follows. Section II describes related work. In Section III, proposed scheme is discussed for making MANET free from the Black-hole/DOS attack. Implementation of the proposed scheme is covered in Section IV. Finally conclusion and future directions are given in Section V.

II. Literature Survey

Piyush et.al [6] proposed a solution where source and destination nodes carry out end-to-end checking to determine whether the data packets have reached the destination or not. If the checking fails then the backbone network initiates a protocol for detecting malicious nodes. But, it works on assumption that any node in the network has more trusted nodes as neighbors than malicious nodes which may not be likely in many scenarios. If malicious nodes are more in numbers, this solution becomes vulnerable.

Chen et. al [7] presented a solution consisting of two related algorithms: key management algorithm based on gossip protocol and detection algorithm based on aggregate signatures. According to their solution, each node involved in a session must create a proof that it has received the message; when source node suspects some misbehavior, Checkup algorithm checks intermediate nodes and according to the facts returned by the Checkup algorithm, it traces the malicious node by Diagnosis algorithm. This solution may generate high traffic and computational cost of detection algorithm may be very high due to the basic limitations of gossip protocol and aggregate signatures.

A mechanism is proposed by Sukla et al. [8] in which before sending any block, source sends a prelude message to destination to make it aware about communication; neighbors monitor flow of traffic; after end of transmission, destination sends postlude message containing the number of packets received. If the data loss is out of acceptable range, the process of detecting and removing all malicious nodes is initiated by collecting response from monitoring nodes and the network. The mechanism has routing overhead increased due to additional routing packets

For detecting packet forwarding misbehavior, Oscar et al. [9] proposed an algorithm that uses the principle of flow conservation and accusation of nodes that are constantly misbehaving. Selecting correct threshold of misbehavior allows distinguishing well-behaved and misbehaved nodes. However, the average throughput cannot reach that of a network where there is no misbehaving node present because the algorithm requires definite time to gather the required data to identify and to accuse misbehaving nodes. Therefore, misbehaving nodes can drop packets before being accused and isolated from the network during the preliminary phase.

Adnan Nadeem et al [10] focus on preventing denial-of-service (DOS) attacks. As an example, author considers intruders that can cause DOS by exploiting the route discovery procedure of reactive routing protocols. They show the unsuitability of tools such as control chart, used in statistical process control (SPC), to detect DOS and propose an anomaly-based intrusion detection system that uses a combination of chi-square test & control chart to first detect intrusion and then identify an intruder. When the intruder is isolated from the network, show reduced overhead and increased throughput. Simulation results show that AIDP performs well at an affordable processing overhead over the range of scenarios tested.

V. Priyadharshini et al. [11] proposed a new cracking algorithm is implementing to stop that DDOS attacks. In this algorithmic design a practical DDOS defense system that can protect the availability of web services during severe DDOS attacks. The proposed system identifies whether the number of entries of client exceeds more than five times to the same sever, then the client will be saved as an attacker in blocked list and the service could not be provided. This algorithm protects legitimate traffic from a huge volume of DDOS traffic when an attack occurs.

III. Packet Drop and DOS Attack

A. Packet Drop Attack

The packet drop attack in MANETs can be classified into several categories in terms of the strategy adopted by the malicious node to launch the attack. In particular the malicious node can intentionally drop all the forwarded packets going through it (packet drop attack), or it can selectively drop the packets originated from or destined to certain nodes that it dislikes. In order to launch a Packet Drop Attack, the first step for a malicious node is to find a way that allows it to get involved in the route forwarding path of data or control packets. To do so, it exploits the vulnerabilities of the underlying routing protocols which are generally designed with strong assumption of trustworthiness of all the nodes participating in the network. Thus, any node can easily misbehave and provide a severe harm to the network by targeting both data and control packets. Dropping data packets leads to suspend the on-going communication between the source and the destination node. More seriously, an attacker that captures the incoming control packets can prevent the associated nodes from establishing routes between them [12].

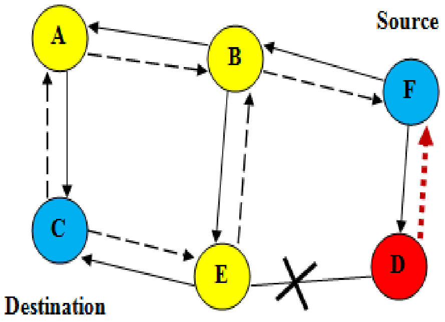


Figure 2 Black hole Attacks

In Black whole attack, using routing protocol to an attacker promotes itself as the shortest path to the objective device [13]. An attacker watches the routes appeal in an overflow based routing protocol. When the attacker receives an application for a route to the purpose node, it forms a react connecting of actually short route.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

If the naughty respond reaches the initiate node previous to the reply from the authentic node, a false route gets formed. Once the malicious device joins the network itself among the converse nodes, it is forceful to do the whole thing during the packets passing through them. It can crash the packets between them to implement a denial-of-service attack, or on the beforehand use its situation over the route is the first step of man-in-the-middle attack [14].

B. Denial of Service (DOS)

An attacker tries to avoid legitimate and authorized users for accessing services offered by the network. A DOS attack can be approved out in many ways. The natural way is to overflow packets to any merge resource available in the network so that the reserve is no longer available to nodes in the network, as an conclusion of which the network no longer operational in the method it was designed to make active. This may causes failure in delivery of certain forces to the end users. Due to the single possessions of ad hoc wireless networks, there will be accessible a variety of additional techniques to deploy DOS attack in a network, which would not be probable in wired networks. DOS attacks can be organized in close proximity to any layer in the network protocol stack [15].

As an example an adversary node could contribute in a session but basically drop a convinced number of packets, which may direct to degradation in the QoS being offered through the network. On the higher layers an adversary could depose critical services such as the key management service.

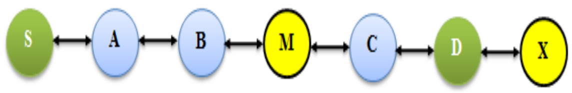


Figure 2 DOS attack

Consider a straight path present from S to X and C and X cannot listen to every previous that nodes B and C cannot listen to every previous and that M is a nasty node difficult a DOS attack. Assume S requests to communicate with X and that S has a live route to X in its cache. S conveys a data packet to X between the source route S → A → B → M → C → D (X contained in the packet's header).While M accepts the packet; it can amend the source route in the packet's header, like removing D from the source route. Accordingly, when C receives the distorted packet, it attempts to forward the packet to X. Because X cannot hear C, the transmission is unsuccessful.

IV. PROPOSED SYSTEM

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

To prevent black-hole attack first we make two or three fake route request which has destination within network as nature of black-hole attacker node he just reply to both node as same route reply in the form of sequence number but all the other nodes send the different sequence number of different number if we find this kind of reply we provide the key to all other nodes rest of them are safe to communicate For preventing the DDOS attack we also add the counting the number of route request without including this two nodes find out the variance of all nodes if the node sends more than the variance this is also set as attacker node and if any route request come from this node all other node will not process this request.

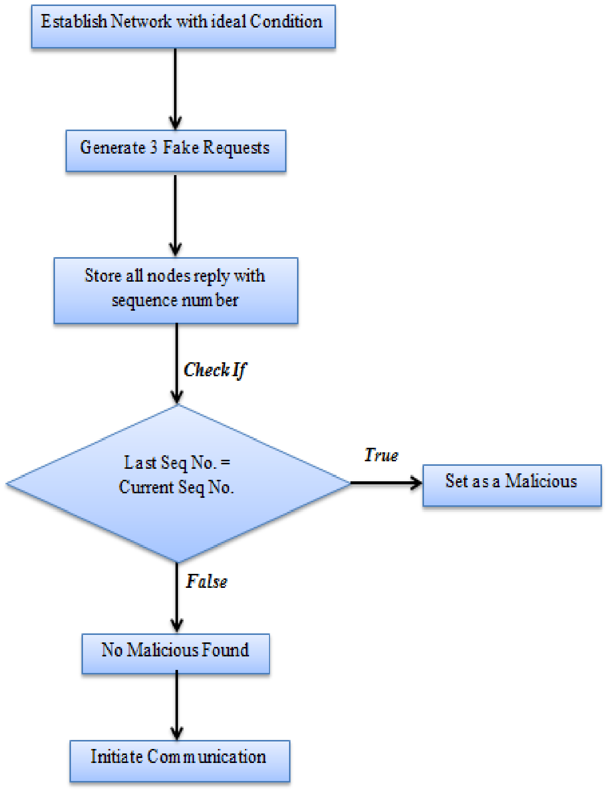

Establish Network with ideal Condition
Generate 3 Fake Requests
Store all nodes reply with sequence number
Check If
Last Seq No. = Current Seq No.
True
Set as a Malicious
False
No Malicious Found
Initiate Communication

Figure 4 Proposed Flow Work

A. Threshold Valuation

a. **Capture No. of Requests for Every Node:** In this step each number of connection requests is recorded during transmission of a RREQ packet. That is experimented separately and in ideal conditions the number of request send by the node is estimated.

b. **Calculate Pre Threshold Value:** Let us N numbers of nodes are participating in a network communication. Thus some of the nodes are making more requests for obtaining the connectivity due to arbitrary and frequent mobility. Therefore first the mean number of request is obtained. The Pre threshold is given by the following formula.

$$\alpha_{pre} = \frac{1}{N}\sum_{i=1}^{N} d_i^{req}$$

where

$$\alpha_{Pre} = \textit{pre threshold value}$$

$$N = \textit{Number of Nodes in Network}$$
$$d_i^{req} = \textit{Number of Request Send by Node}$$

During this that is observed sometimes some needs additional packets to establish the connection. Therefore this limit is extended using the soft threshold computation. This soft threshold is allowing some nodes to flood more during connection request. For better filtering a two-step procedure is used for effective prevention of malicious node.

c. **Compute the Post Threshold for the Network:** As discussed before due to frequently changing positions and the node mobility additional request packets are required to send. Therefore the variance of number of request is estimated. For allow some node the variance of number of RREQ flooding is recovered also using the following formula.

$$\alpha_{post} = \sqrt{\frac{1}{N}\sum_{i=1}^{N}\left(d_i^{req} - \alpha_{Pre}\right)^2}$$

Where,

α_{post} = *Post Threshold used for comparing the additional of Nodes Flooding*

$$N = Number\ of\ Number\ of\ Nodes$$
$$d_i^{req} = Number\ of\ Request\ Send\ by\ Node$$

Therefore the total threshold packets requests of nodes are:

$$\alpha_{total} = \alpha_{post} + \alpha_{Pre}$$

B. Algorithm Study

Table 1 Proposed Algorithms

Algorithm for Packet Drop and DOS

```
Repeat all steps after every t time
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: Generates 3 fake request
6: Store the all reply with node and their sequence number
7: Check if the last Sequence number and Current Sequence number is same
    $if\ (lastSeqNum == currentSeqNum)$ {
        set as malicious
    }
    else {
        No Malicious Found and Start Communication
    }
8: Provide other than malicious node key for communication.
9: If reply doesn't contain key drop the reply not safe for communication.
10: Store the request generated by the nodes
11: Find out the variance and set as total threshold ($\alpha_{total}$) value
12: If node send more request as compare total threshold ($\alpha_{total}$)
    $if(nodeSendReq > \alpha_{total})$
    {
        set as flooder
    }
13: Stop the communication with this node also
```

V. Implementation

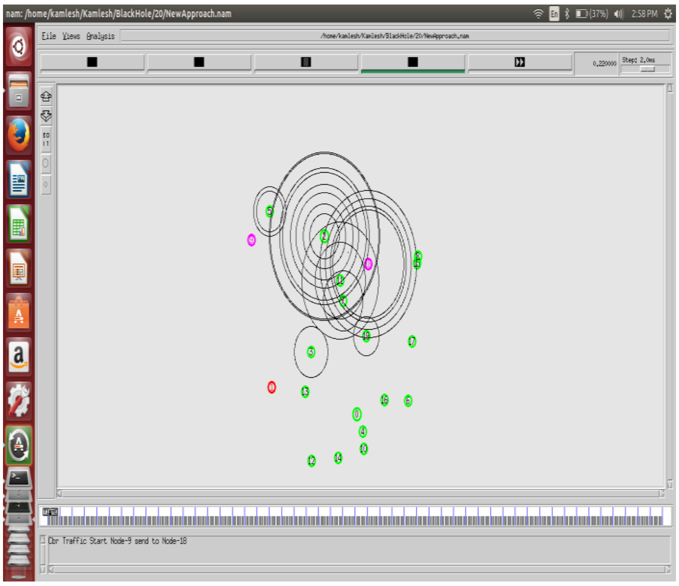
The simulation is being implemented in the Network simulator [16]. Protocol used here is AOMDV.

Table 2 Simulation Scenarios

Parameters	Values
Parameters	Values
Antenna Model	Omni Antenna
Dimension	750 X 550
Radio-Propagation	Two Ray Ground
Channel Type	Wireless Channel
Traffic Model	CBR
Routing Protocol	AOMDV
Mobility Model	Random Waypoint

A. For Black-hole Attack

Simulation using Proposed Routing Method: In this phase, of proposed secure routing method is simulated when attack prevention is established. Therefore the second simulation is prepared which is demonstrated in figure 4.3. In this simulation screen the green nodes demonstrate as normal legitimate node in network. The given simulation is developed using the proposed secure routing technique. 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.


nam: /home/kamlesh/Kamlesh/BlackHole/20/NewApproach.nam
En
(37%)
2:58 PM
File
Views
Analysis
/home/kamlesh/Kamlesh/BlackHole/20/NewApproach.nam
0.220000
Step: 2.0ms
TIME

Cbr Traffic Start Node-9 send to Node-18

Figure 5 Proposed Routing under Attack

B. For Denial of Service Attack

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 traditional AODV performance under attack conditions. The figure 4.5 demonstrates the simulation screen of the proposed secure routing technique for DOS Attack prevention.

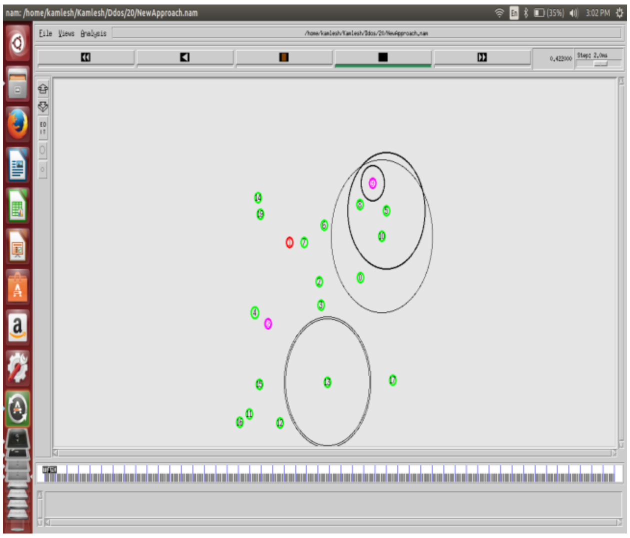

nam: /home/kamlesh/Kamlesh/Ddos/20/NewApproach.nam
File Views Analysis
/home/kamlesh/Kamlesh/Ddos/20/NewApproach.nam
0.422000
Step: 2.0ms
3:02 PM

Figure 6 Proposed Method under attack Prevention

Simulation Matrices

The simulation here is done on the basis of the following parameters:

a. *Throughput:* It basically describes the ratio of total packets sent to the total packets received in prescribed simulation time depending on the no. of malicious nodes present here.

b. *End to End Delay:* Here, in this parameter the delay factor is taken under consideration in which the total time is calculated. Total extra time the packet takes to reach to the destination is termed as delay.

c. *Overhead:* It provides all the information that tells about the routing just like the route reply and route request.

d. *Packet Delivery Ratio:* PDR tells the ratio of total number of packets sent from the source node to the destination node via intermediate node.

VI. RESULT ANALYSIS

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.

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

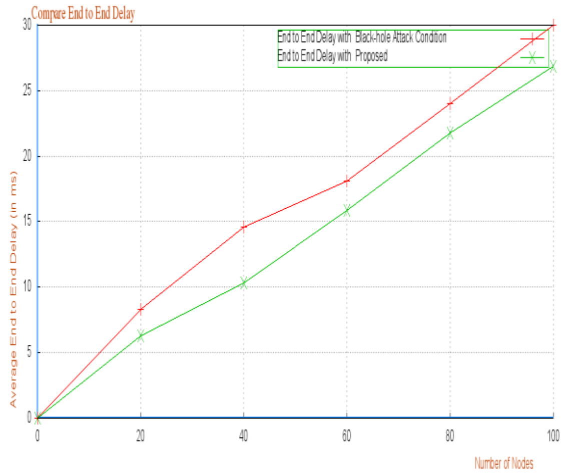


Figure 7 End to End Delays for Black-hole

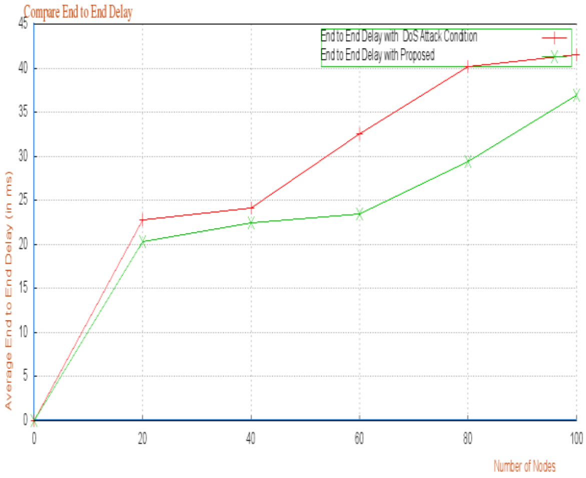


Figure 8 End to End Delay for DOS Attack

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:

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

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

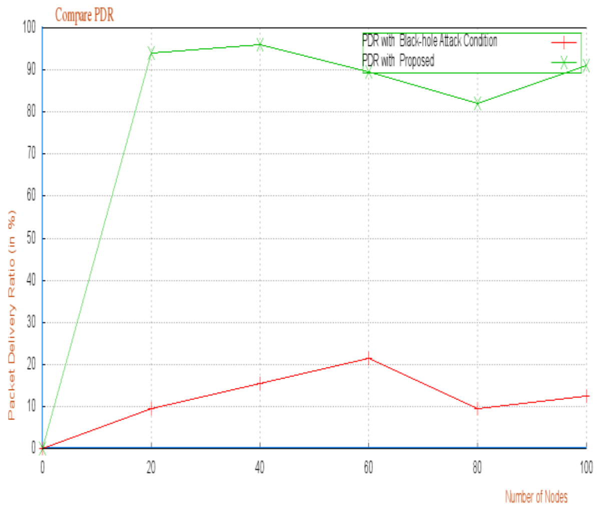


Figure 9 Packet Delivery Ratios for Black-hole

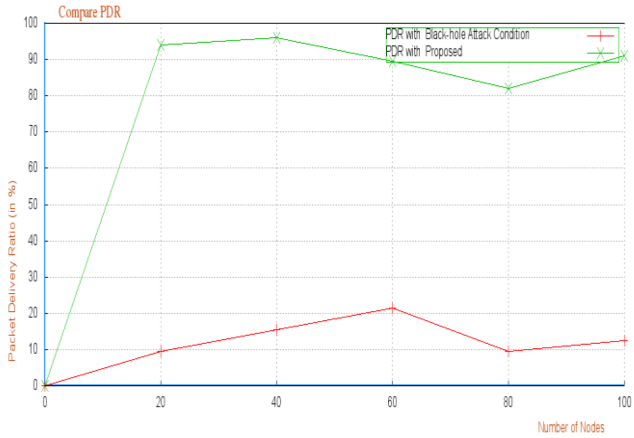


Figure 10 Compare Packet Delivery Ratios for DOS

C. Routing Overhead

During the communication scenarios it is required to exchange the packets for different tracking and monitoring purpose. Therefore the additional injected packets in network is termed as the routing overhead of the network.

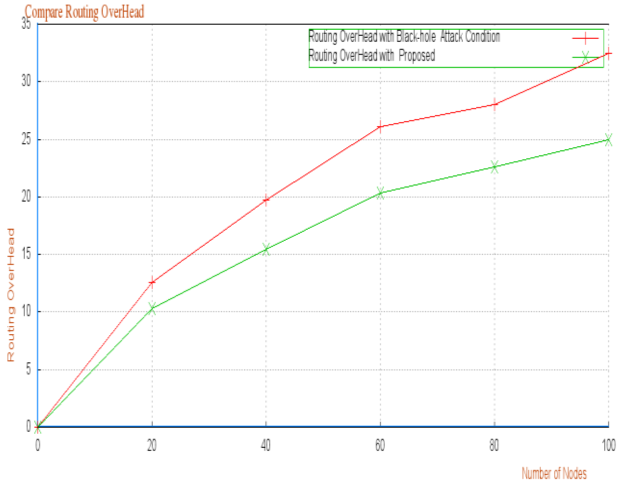


Figure 11 Routing Overhead for Black-hole

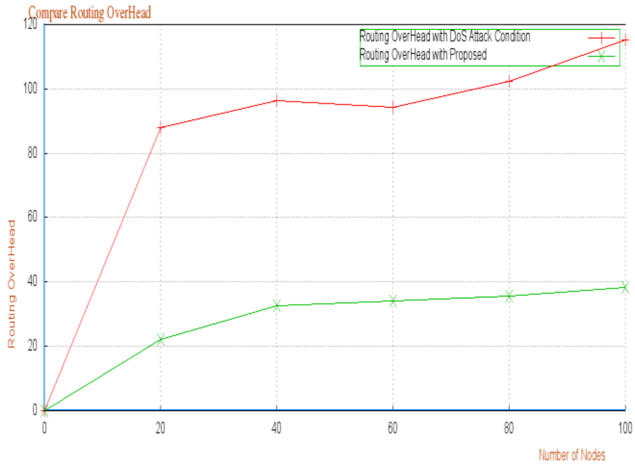


Figure 12 Routing Overhead for DOS

D. 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

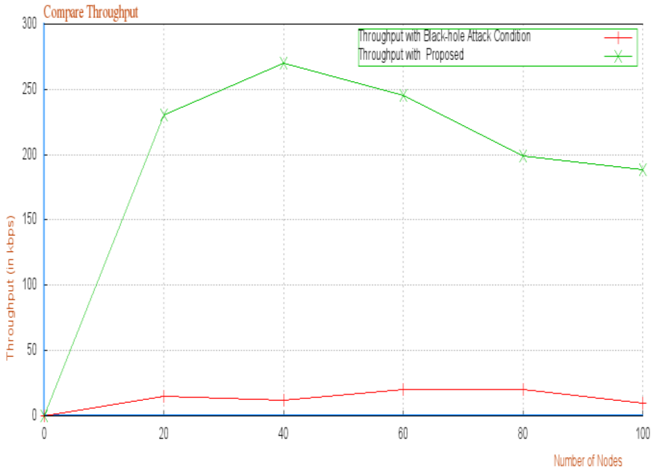


Figure 13 Compare Throughput for Black-hole

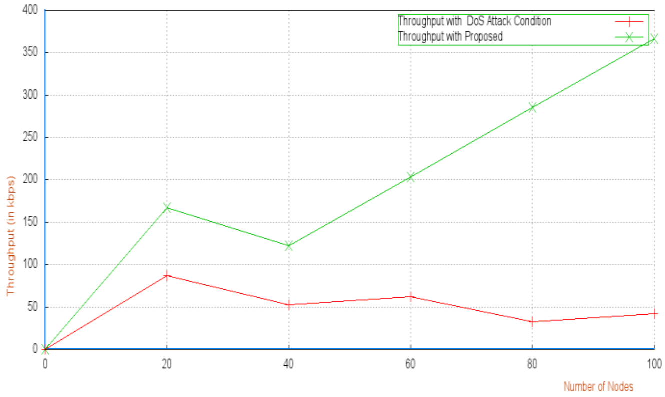


Figure 14 Compare Throughputs under DOS Attack

VII. Conclusion and Future Work

In this paper, the detailed study about the black hole and DOS attack is done. In this paper, we investigated some of the existing solutions for these attacks and proposed a novel approach to counter these attacks that efficiently finds short and secure route to the destination. The Simulation analysis shows that our approach would greatly increase PDR, throughput and reduces delay with negligible difference in routing overhead. The algorithm is equally applicable to other reactive protocols. In near future the work is enhanced more with adding more parameters to distinguish more or different kinds of network attacks. The solution is based on iterations so consumption of time is also a scope for future work. The whole research work can be extended in the future in other protocol rather than AOMDV.

References

1. Pradip M. Jawandhiya and Mangesh M. Ghonge, “A Survey of Mobile Ad Hoc Network Attacks”, / International Journal of Engineering Science and Technology, Vol. 2(9), PP. 4063-4071, 2010.
2. G.S. Mamatha and S.C. Sharma, “A Robust Approach to Detect and Prevent Network Layer Attacks in MANETS”, International Journal of Computer Science and Security, vol. 4, issue 3, Aug 2010, pp. 275-284.
3. Mohammad Al-Shurman, and Seungjin Park, “Black Hole Attack in Mobile Ad Hoc Networks”, ACMSE, April 2004, pp.96-97.
4. Anu Bala, Munish Bansal and Jagpreet Singh, “Performance Analysis of MANET under Black-hole Attack”, First International Conference on Networks & Communications, 2009, pp. 141-145.
5. Gao Xiaopeng and Chen Wei,”A Novel Gray Hole Attack Detection Scheme for Mobile Ad-Hoc Networks”, 2007 IFIP International Conference on Network and Parallel Computing – Workshops, 2007, pp. 209-214
6. Piyush Agrawal, R and Sajal K. Das, “Cooperative Black and Gray Hole Attacks in Mobile Ad Hoc Networks**”,** 2nd international conference on Ubiquitous information management and communication, 2008, pp.310-314.
7. Chen Wei, and Gao Xiaopeng,“A New Solution for Resisting Gray Hole Attack in Mobile Ad-Hoc Networks”, Second International Conference on Communications and Networking in China, August 2007, pp. 366-370.
8. Sukla Banerjee, “Detection/Removal of Cooperative Black and Gray Hole Attack in Mobile Ad-Hoc Networks”, World Congress on Engineering and Computer Science, October 2008, pp. 337-342.
9. Adnan Nadeem and Michael Howarth, “Adaptive Intrusion Detection & Prevention of Denial of Service attacks in MANETs”, Proceedings of the 2009 International Conference on Wireless Communications and Mobile Computing: Connecting the World Wirelessly Pages 926-930
10. V. Priyadharshini and Dr. K. Kuppusamy, “Prevention of DDOS Attacks using New Cracking Algorithm”, International Journal of Engineering Research and Applications, Vol. 2, Issue 3, May-Jun 2012, pp.2263-2267
11. “Analysis on Impact of Black Hole Attack on AODV and AOMDV”, CHAPTER 2, available online: http://shodhganga.inflibnet.ac.in/bitstream/10603/24748/7/07_chapter2.pdf.
12. Juan-Carlos Ruiz, JesúsFriginal, David de-Andrés, Pedro Gil, “Black Hole Attack Injection in Ad hoc Networks”.
13. Fan-Hsun Tseng1, and Han-Chieh Chao, “A survey of black hole attacks in wireless mobile ad hoc networks”, Tseng et al. Human-centric Computing and Information Sciences 2011
14. Neetika Bhardwaj, Rajdeep Singh, “Detection and Avoidance of Black-hole Attack in AOMDV Protocol in MANETs”, International Journal of Application or Innovation in Engineering & Management (IJAIEM), PP. 376 – 383, Volume 3, Issue 5, May 2014.
15. Bounpadith Kannhavong, Hidehisa Nakayama, Yoshiaki Nemoto, and Nei Kato, Abbas Jamalipour, “A survey of routing attacks in mobile ad hoc networks”
16. The Network Simulator. NS-2 [Online] http://www.isi.edu/nsnam/ns/

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)