Combined Approach for Detection and Prevention of Flooding and Black-hole Attack in MANET

Ashok Panwar, D.Srinivasa Rao, G. Sriram

***Abstract*— Wireless network is the network of mobile computer nodes that are not physically wired. The main advantage of such network is communicating with rest of the world while being mobile. The risks to users of wireless technology have increased as the service has become more popular. Due to the dynamically changing topology, open environment and lack of centralized security infrastructure, a mobile ad hoc network (MANET) is vulnerable to the presence of malicious nodes and to ad hoc routing attacks. There are a wide variety of routing attacks that target the weakness of MANETs.**

In this paper, we proposed a novel approach for analysis of black-hole and Flooding attack and intended to find methodology. The proposed solution is based on PDR and generating fake request threshold computation by which we can conclude there is availability of malicious attacker. The implementation of the proposed Secure Routing Testing concept of finding malicious attacker is performed using NS 2 i.e. network simulator 2 and for implementing the security protocol in existing routing the AODV routing protocol with modifications are performed. The experimental results shows the adoptable performance of the algorithm and improves the different performance parameters i.e. throughput, end to end delay, packet delivery ratio, and energy consumption.

***Index Terms*— Mobile ad-hoc Networks Black-hole, NS2, AODV, Routing Protocol, Mobile nodes, RREQ, RREP, Flooding.**

I. INTRODUCTION

In recent years, the explosive growth of mobile computing devices, which mainly include laptops, personal digital assistants (PDAs) and handheld digital devices, has impelled a revolutionary change in the computing world: computing will not merely rely on the capability provided by the personal computers, and the concept of ubiquitous computing emerges and becomes one of the research hotspots in the computer science society [1]. The Mobile Ad Hoc Network is one of the wireless networks that have attracted most concentrations from many researchers. In ad hoc networks the communicating nodes do not necessarily rely on a fixed infrastructure, which sets new challenges for the necessary security architecture they apply. In addition, as ad hoc networks are often designed for specific environments and may have to operate with full availability even in difficult conditions, security solutions applied in more traditional networks may not directly be suitable for protecting them. In concern of network security different attack harm the privacy of system gradually. One of the most popular and serious attacks in wireless ad hoc networks is Denial of Service attack and most proposed protocols to defend against this attack used positioning devices, synchronized clocks, or directional antennas [2].

II. MANET

An ad hoc network is a collection of nodes that do not need to rely on a predefined infrastructure to keep the network connected. Ad hoc networks can be formed, merged together or partitioned into separate networks on the fly, without necessarily relying on a fixed infrastructure to manage the operation. Nodes of ad hoc networks are often mobile, which also implicates that they apply wireless communication to maintain the connectivity, in which case the networks are called as mobile ad hoc networks (MANET). Mobility is not, however, a requirement for nodes in ad hoc networks, in ad hoc networks there may exists static and wired nodes, which may make use of services offered by fixed infrastructure [3, 4]. Fig 1 is the depiction of mobile ad hoc structure:

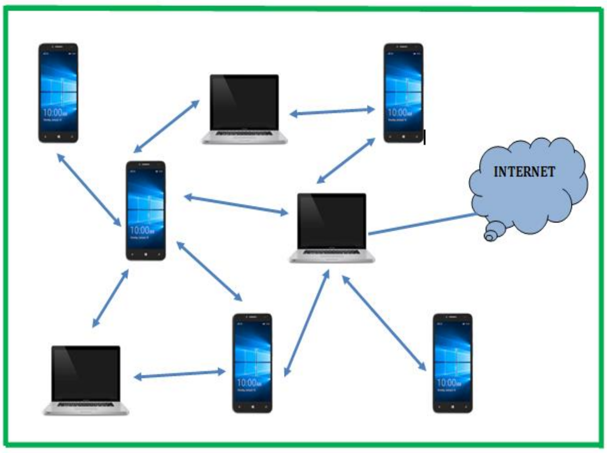


Fig 1. MANET Structure

1.2 Flooding Attack

An attacker tries to avoid legitimate and authorized users for accessing services offered by the network. 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 Flooding attack in a network, which would not be probable in wired networks. Flooding attacks can be organized in close proximity to any layer in the network protocol stack [5].

Consider the following Fig 2. Consider a straight path present from S to X and C and X cannot listen to every previous that

Ashok Panwar, Research Scholar, MITM, Indore, India, 9039477119
D.Srinivasa Rao, Associate Prof. in CSE , MITM, Indore, India 8109792743
G. Sriram, Assistant Prof. in Computer Science, School of Distance Education, AU , Visakhapatnam, India, 8801717646

nodes B and C cannot listen to every previous and that M is a nasty node difficult a Flooding 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 [6].

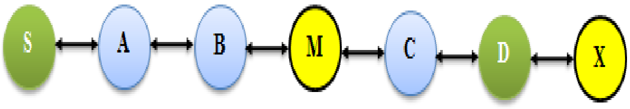


Fig 2. Flooding Attack

1.3 Black-hole Attack

In MANET, a packet dropping attack is a type of denial of service in which a node in the network will drop the packets instead of forwarding them, which is shown in the figure 24. The packet dropping attack [7] is very hard to detect and prevent because it occurs when the node becomes compromised due to a number of different causes. The packet dropping attack in MANETs can be classified into several categories in terms of the strategy adopted by the malicious node to launch the attack [8]:

- The malicious node can intentionally drop all the forwarded packets going through it (black hole).
- It can selectively drop the packets originated from or destined to certain nodes that it dislikes.
- A special case of black hole attack dubbed gray-hole attack is introduced. In this attack, the malicious node retains a portion of packets, while the rest is normally relayed.

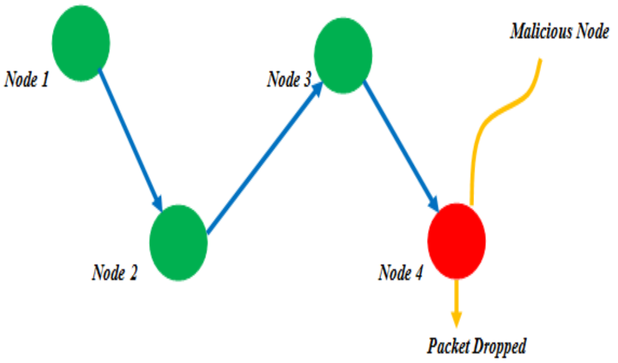


Fig 3. Black-hole Attack

III. Proposed Solution

2.1 Problem Statement

With the rapid growth in the internet, users are opting for online trading, shopping and other critical online activities. These resources have to be protected from various types of attacks. The main purpose of the DoS flooding attack is usually to degrade – or even disrupt – the normal operation of the attacked network, its constituting components, or provided services. At present, the vast majority of flooding DoS attacks is directed against individual network components and the services they are offering. Their targets predominantly comprise network components that provide end user services, such as Web servers or other kinds of service access points. Similarly, in black-hole attack scenario most of the security concern is affected. In this, the attacker targets some nodes in the wireless network and then drop the packets sent towards the intended nodes. Attackers try to drop/delay the packets in the routine manner.

Therefore a security model for finding the malicious attackers is available and most of techniques are providing solutions for single and multiple. If the solution is formulated as a framework, to secure the network from more than one attacker using single solution is more effective. Thus an effective technique is required to adopt more parameters by which the other kinds of attackers are also distinguished. The proposed security technique involves the following issues to resolve in the proposed solution.

- Due to DDOS flooding attacker injects routing overhead is increases significantly. The routing overhead directly impact on the network performance in terms throughput and packet delivery ratio and end to end delay also.
- The energy of the network nodes is limited due to the limited power source. The DDOS attacker tries to consume the node energy, attacker the data packets. Thus energy consumption is increases and packet delivery ratio becomes too low.
- Due to the black-hole attack, packets are lost continuously therefore packet lost rate is increased therefore network throughput considerably reduced of the network. So the need to find black-hole nodes using detection and prevention.

2.2 Methodology

The proposed technique needs to develop a method by which the routing algorithm self-detect and prevent the routing attack in network. Therefore the proposed technique needs to incorporate the following solution.

Description: By using Bayesian classifier for detect black-hole attack for the first input data, make some fake request to the destination and wait for the reply of acknowledge and training out the classifier with sending and receiving data packets and packet delivery ratio. Here calculate average threshold value of PDR with 0 and 1 class level. Hence, apply checks for PDR find out the black-hole attack. If PDR is less than 30% of individual PDR then set as class level 0 other wise class level is 1 which indicate black-hole attacker found. Now for flooding DoS the original packet test using Bayesian classifier and set as malicious or non malicious node and did not process the request for the same request For flooding attack, count number of request send by the nodes in the network and sum all these request and find out the average value of all request. So that at the time of testing find out mean average value and compare average request with all other node request, and find out the labeling of node as they are malicious of legitimate

2.3 Proposed Algorithm

The entire process of the solution development is described using the summarized step of algorithm and described in training and testing pattern to calculate the malicious request both attack classification. The given Table 3.1 contains the algorithm for computing the threshold value and this also contains detection and prevention process of malicious node reported. Both the process is working individually and both are depending on each other.

Table 1. Combined Algorithm for Attack Detection and Prevention

```
Input: Number of Node
Output: No Attacker found

Process:
Training and Testing using Bayesian classifier
1: Generate some fake request by $N_s$ and wait for reply
2: Train the classifier using send and receive data packets
3: Compute the Received Packet threshold and find class level of node
4: Compute Average threshold of all nodes
   $PDR = \frac{\text{Total Delivered Packet}}{\text{Total Sent Packet}} * 100$
For each node in suspected list
5: $if\ (PDR < 30\%)$
   $setclasslevel = 0$
   Label node as Malicious Node
$else$
   $setclasslevel = 1$
   Label node as legitimate
$endif$
6: For original packets don't process for same fake request
7: Count total number of request $R$, send by the node as $R_1, R_2, R_3 \dots\dots, R_n$
8: Compute Average number of node request $\delta_R$
   $\delta_R = \frac{R_1 + R_2 + R_3 + \dots + R_n}{n}$
9: For each Flooding Attack
10: $if\ \ (\delta_R < R_{eachNode})$
   Node as a flooding attacker
$else$
   Node as a genuine
$endprocess$
```

IV. Implementation

3.1 Simulation Scenario

This section provides the understanding about the simulation scenarios under which the experiments are performed. To demonstrate the security technique their two key simulation scenarios are proposed in this section. Both the simulation scenarios are conducted with different number of nodes that are 20, 40, 60, 80 and 100 nodes for both attacks.

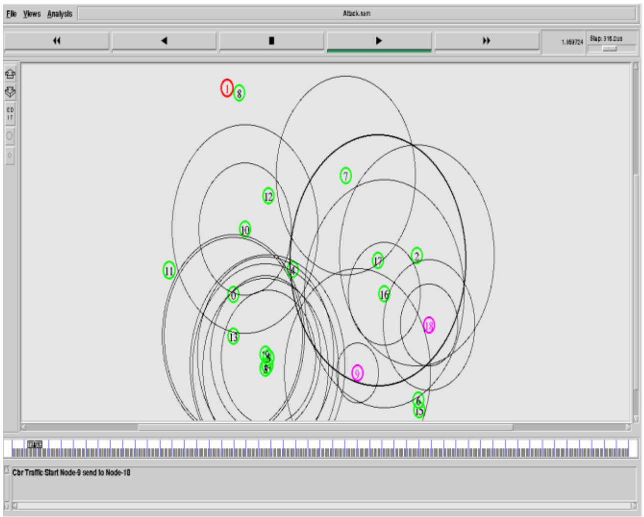
The simulation is being implemented in the Network simulator [9]. Protocol used here is AODV.

Table 2. Simulation Scenarios

Parameters	Values
Antenna Model	Omni Antenna
Dimension	1000X1000
Radio-Propagation	Two Ray Ground
Channel Type	Wireless Channel
Traffic Model	CBR
Routing Protocol	AODV
Number of Nodes	20, 40, 60, 80, 100

3.2 For Flooding Attack

Simulation of AODV Routing under Attack: In this network simulation the network is configured with the traditional AODV routing protocol in attack condition and the network performance is evaluated. That simulation also contains a malicious DOS which demonstrates the effects on security in normal network and consumes network resources. The simulation of the Flooding attack is given in the figure 4. In this diagram the green nodes show the client nodes involved in the network and the sender and receiver for the network is demonstrated using the pink color nodes. Additionally the malicious nodes demonstrated using the red color nodes.



Cbr Traffic Start Node-9 send to Node-18

Fig 4. Network under flooding condition

Simulation of Proposed Scheme of Attack Prevention: In this simulation the proposed secure routing technique is implemented in the network simulator environment with the similar configuration as previous networks is configured. After that for investigating the effect of the proposed solution on the network and the network performance is evaluated. The simulation of flooding attack detection and prevention process is simulated using the network trace file the simulation performance is demonstrate for proposed and traditional AODV in attack prevention and in attack condition scenario and used for comparative performance study show in figure 5.

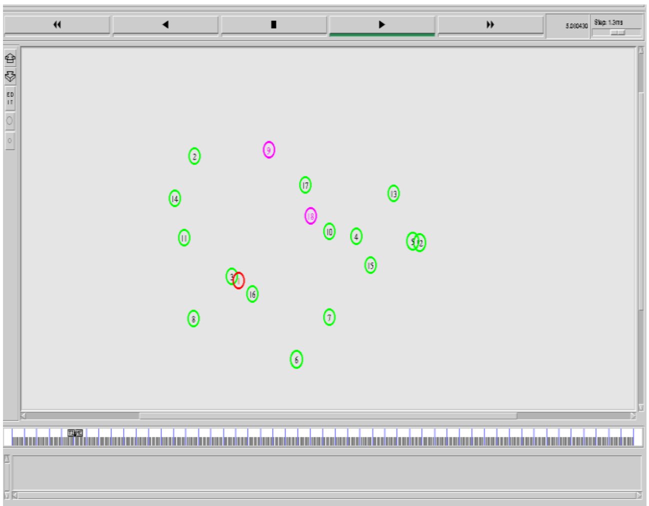
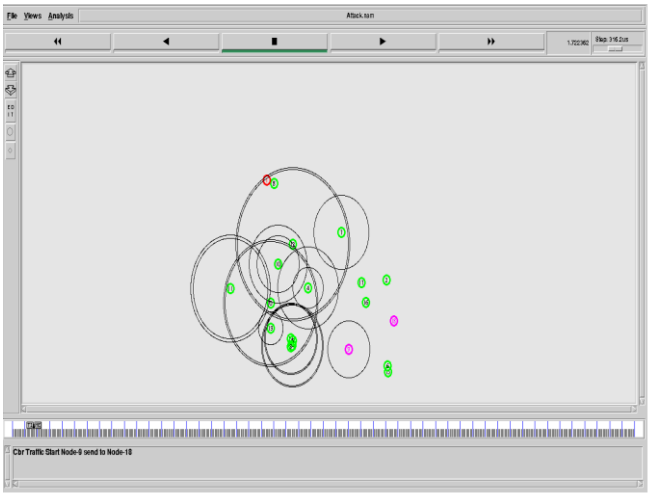


Fig 5. Proposed Solutions for Flooding (DOS Attack) Prevention

3.3 For Black-hole Attack

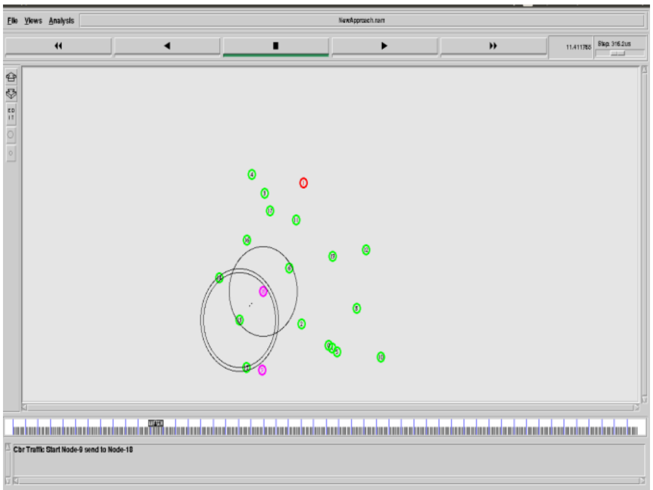
Simulation when Black-hole is deployed: In this network recreation the network is configured using the traditional AODV routing protocol. Behind necessary network organization the malevolent node is deployed on network and the network presentation is approximate on the basis of the network presentation traces. The normal network nodes are given using the green color and the malevolent attacker is established in the reproduction as given in Fig 6. In this configuration an attacker drop the packets instead of forwarding them; hence major amount of packets is dropped during attack condition. Communication is happened between source node 9 and destination node 18.



Cbr Traffic Start Node-9 send to Node-18

Fig 6. Network Simulation under Black-hole Condition

Simulation using the Proposed Method: In this simulation scenario the proposed routing technique which is developed with the help of AODV routing modifications are implemented in 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 Fig 7. demonstrates the simulation screen of network in black-hole condition.



Cbr Traffic Start Node-9 send to Node-18

Fig 7. Proposed Secure Routing Method for Attack Prevention

V. Result Analysis

4.1 For Black-hole Attack

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.

$$\text{E2E Delay} = \text{Receiving Time} - \text{Sending Time}$$

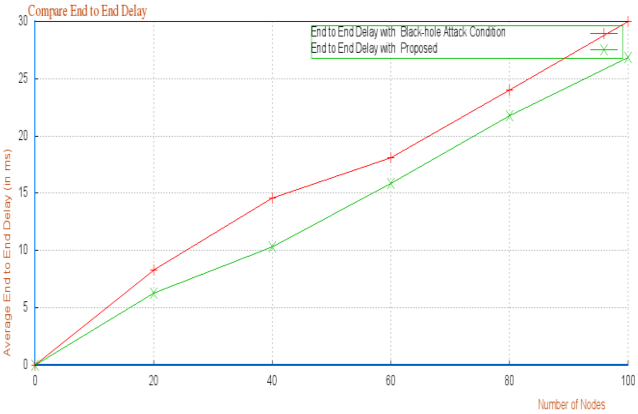


Fig 8. End to End Delays for Black-hole Attack

Fig 8. shows the comparative End to End Delay of Black-hole attack condition and the proposed secure routing technique. In this figure 8 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. Therefore the proposed technique is an efficient technique and produces less amount of delay.

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:

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

The comparative packet delivery ratio of the networks is given using Fig 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

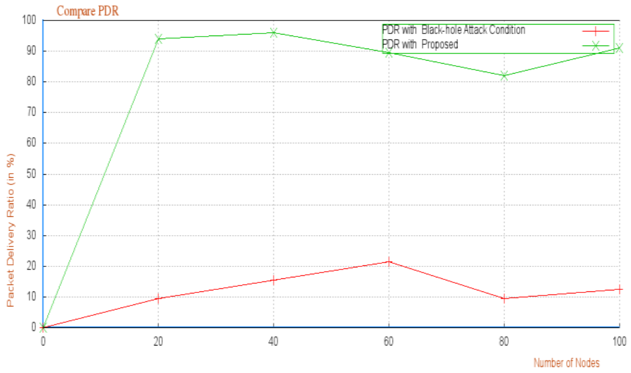


Fig 9. Packet Delivery Ratios for Black-hole Attack

The red line of diagram represents the performance of the traditional AODV technique with attack condition and green line shows the performance of the proposed technique. 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.

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.

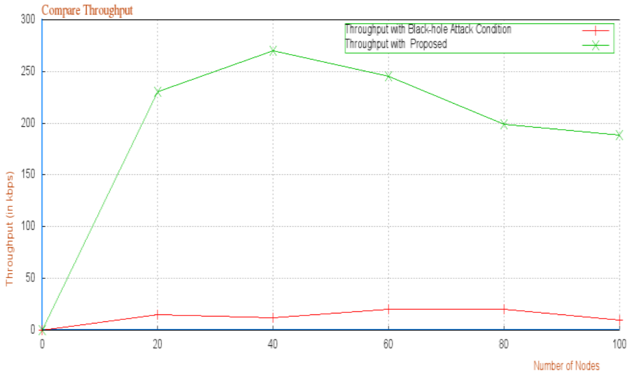


Fig10. Compare Throughput for Black-hole Attack

The comparative throughput of the network is demonstrated using Fig 10 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 red line shows the performance of the traditional AODV routing in attack condition. 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.

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. The comparative routing overhead of both the routing protocols i.e. traditional AODV and the proposed secure routing technique is given using Fig 11. In this diagram the X axis shows the amount of network nodes exist during the experimentation and the Y axis shows the routing overhead of the network. In this diagram for demonstrating the performance of the proposed technique the green line is used and for traditional technique the red line is used. According to the obtained performance of the techniques the proposed technique produces less routing overhead as compared to the traditional AODV routing under attack conditions. Therefore the proposed technique offers higher bandwidth consumption as compared to the traditional routing technique under attack situations.

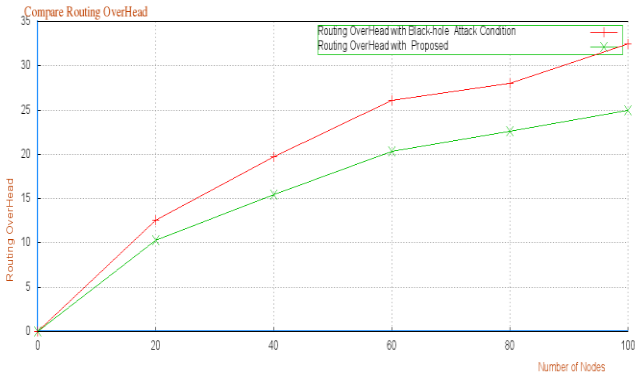


Fig 11. Routing Overhead for Black-hole Attack

4.2 For Flooding Attack

End to End Delay

End-to-end delay refers to the time taken for a packet to be transmitted across a network from source to destination.

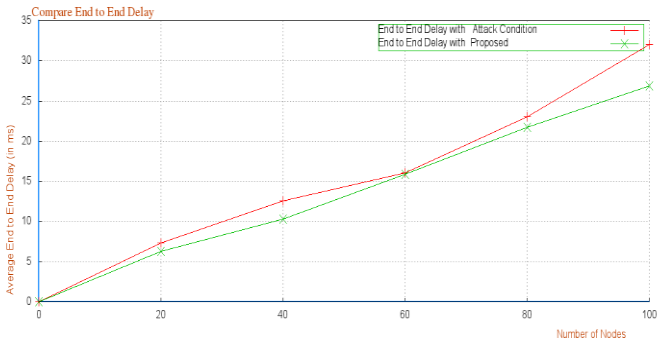


Fig 12. End to End Delay for Flooding Attack

In the similar way, during Flooding attack as given using 12 simulate which is generate fack request between nodes. That delay basically arises due to additional computational overhead and increasing number of random traffic and Routing Congetion by the Network. In the anlyzed scenario it is found that, the average end to end delay under the traditional AODV attack condition is higher as compare to the proposed network technique in case 20, 40, 60, 80 and 100 nodes scenario.

Packet Delivery Ratio

The presentation parameter Packet delivery ratio from time to time termed as the PDR ratio provides in sequence about the presentation of any routing protocols. That reports the amount of productively delivered packets to the target purpose.

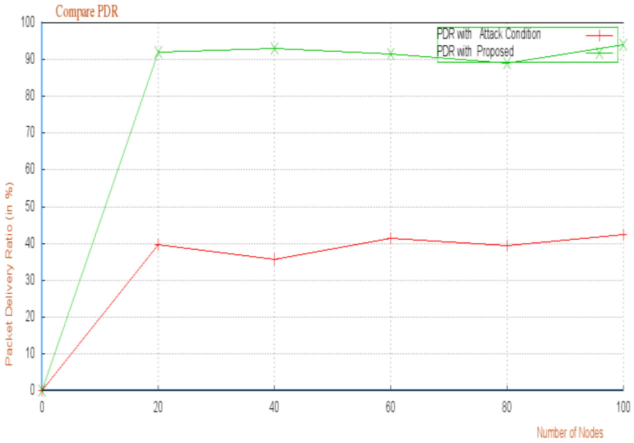


Fig 13. Compare Packet Delivery Ratios for Flooding

The packet delivery ratio of the network can be approximate using the method given

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

The Flooding attack is given using figure 13, in this condition; the Packet Delivery Ratio of normal network is about 50% because the attacker nodes consume the resources and reduce energy of network. Thus, some of the packets are delivered and some of the data is dropped. On the other hand, the proposed secure network is able to prevent the Flooding attack thus the performance is remain constant in all the scenarios. Thus the proposed method is effectively able to recover the network from the malicious attacker in network.

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. Additionally, in case of the DOS attack as given in figure 5.7, the network performance in terms of routing overhead is increasing and decreasing much frequently because of the nature of flooding attack that is hard to classify and also does not significantly provide the characteristics of attack deployment. In the analyzed scenario it is found that, in case of 20, 40, 60 80 and 100 nodes is lesser as compare to the DoS flooding attack condition depict using figure 14. In both scenarios, nodes are moving constantly as around network path, where we apply proposed method to reduce routing overhead for improving network performance.

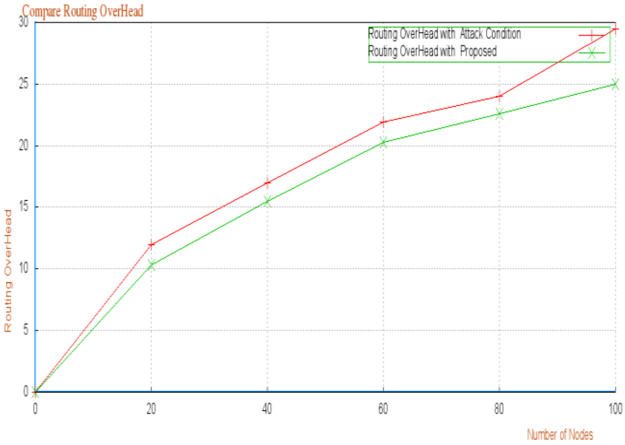


Fig 14. Compare Routing Overhead for Flooding Attack

Throughput

In the different experimental aspects the throughput is measured for finding the performance of the designed system. Network throughput is denoted by the regular rate of victorious delivered message using the communication channel. This data may be delivered over a corporeal or logical link, or pass through a certain network node. Comparative throughput of the normal AODV with attack and the proposed secure AODV routing technique is demonstrated using the Fig. 15. that shows the throughput of network during DoS attack conditions and proposed network condition.

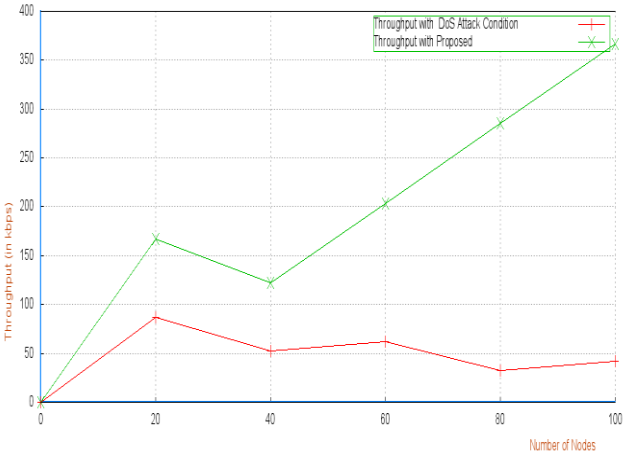


Fig 15. Compare Throughputs under Flooding Attack

It is found that throughput during attack condition is significantly decreased due to attacker nodes but in the proposed work throughput is increased as number of packet is delivered to the destination. Therefore the proposed technique is effectively reduces the impact of the DOS flooding attack in the MANET using the proposed approach.

Energy Consumption

The amount of energy consumed during the network events is termed as the energy consumption or the energy drop of the network. In networking for each individual event a significant amount of energy is consumed. The given Fig 16. shows the energy

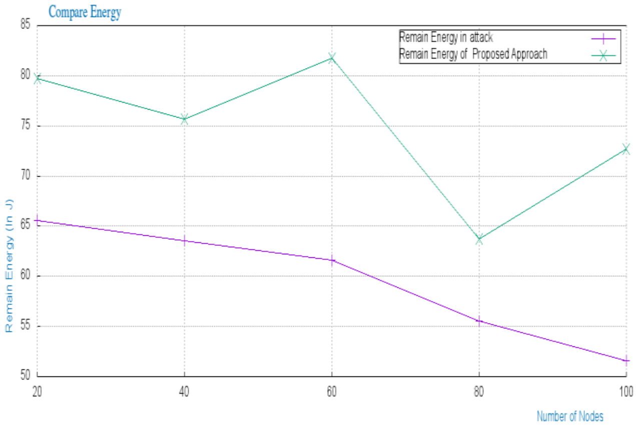


Fig 16. Remain Energy for DOS Flooding Attack

Fig 16. shows remain energy of the network in both the simulation scenarios. The blue line of the diagram shows the amount of energy consumed with the AODV routing protocol under attack condition additionally the green line shows the amount of energy consumed during the proposed algorithm based network. In the Attack condition the network energy is frequently consumed as compared to the proposed routing protocol because the DOS flooding attack targeting the network by consuming the resources of the network. Therefore the proposed technique is effective and able to recover the network from the attack situations.

VI. Conclusion

For many real time applications secure routing is critical to the acceptance and use of mobile networks. The definition and the existing work done by different authors are very important in understanding the threat and in propos ing an effective scheme for detecting and preventing from malicious attackers. Therefore, some of the most exciting attacks done on networks today are those that are difficult to track, and requires very minimal effort on the attacker's part.

In this paper, DOS flooding and Black-hole attacks are targeted for the investigation and study for proposed work. Hence in short, a flooding attack is regarded as an attempt to prevent the legitimate use of a service. DDoS flooding attack does not rely on particular network protocol or system weakness. It simply exploits the huge resource asymmetry between the Internet and the victim, while black hole attack attacker nodes capture the packets and drop without forwarding them. Due to this behavior it is very tricky for the network to figure out such kind of attack. Therefore, we present a Bayesian classification based combined routing approach for detecting and preventing black-hole and DoS flooding attack in which we classify node category as malicious node and normal node. This approach broadly secure from malicious attacker by means of black-hole and flooding attack

REFERENCES

[1] Obi, Obowoware O. "Security issues in mobile ad-hoc networks: a survey." The 17th White House Papers Graduate Research In Informatics at Sussex (2004).

[2] Karpijoki, Vesa. "Security in ad hoc networks", Proceedings of the Helsinki University of Technology, Seminars on Network Security, Helsinki, Finland. 2000

[3] Mäki, Silja, "Security Fundamentals in Ad Hoc Networking", Proceedings of the Helsinki University of Technology, Seminar on Internetworking-Ad Hoc Networks. 2000.

[4] Amitabh Mishra and Ketan M. Nadkarni, Security in Wireless Ad Hoc Networks, in Book the Handbook of Ad Hoc Wireless Networks (Chapter 30), CRC Press LLC, 2003

[5] BounpadithKannhavong, Hidehisa Nakayama, Yoshiaki Nemoto, and Nei Kato, Abbas Jamalipour, "A survey of routing attacks in mobile ad hoc networks

[6] D. Karig, R. Lee, Remote Denial of Service Attacks and countermeasures, Department of Electrical Engineering, Princeton University, Technical Report CE-L2001-002, October 2001

[7] S. Djahel, F.N. Abdesselam, Zonghua Zhang, Mitigating Packet Dropping Problem in Mobile Ad-hoc Networks : Proposals and Challenges, IEEE Communications Surveys & Tutorials, Volume 13, No.4, Fourth Quarter 2011.

[8] NeetikaBhardwaj, 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.

[9] The Network Simulator. NS-2 [Online] http://www.isi.edu/nsnam/ns/

AUTHORS PROFILE

ASHOK PANWAR Three Year Polytechnic Diploma,B.E./ B. Tech., M.E. / M.Tech. He is working in Defence Research & Development Organisation**(DRDO)** in Defence Scientific Information & Documentation Centre **(DESIDOC)** Lab, Govt. of India, Ministry of Defence, in the Department of Knowledge Management Division **(KMD)**, Metcalfe House, Near Civil Lines, New Delhi, Delhi-110054, India. He has one year of teaching experience in Computer Networking. He has attended Two Day's National Workshop in Network Simulator and Design.

D.SRINIVASARAO M.Tech, Ph.D is working as an Associate Professor in the Department of Computer Science & Engineering at Medicaps Institute of Technology and Management, Indore, Madhya Pradesh, India. He has 20 years of teaching experience. His area of interest is Adhoc Networks, Distributed Systems, Network Security & Image Processing. He has guided more than 60 Post Graduate Students. He has published 2 books and 15 papers in international journals. He presented 2 papers in National Conferences, 1 paper in International Conference and has attended 35 National Workshops / FDP / Seminars etc. He is a life member of Professional Society like ISTE.

G. SRIRAM M.Tech, Ph.D is working as an Assistant Professor in the Department of Computer Science , School of Distance Education, Andhra University, Visakhapatnam, India. He has 11 years of teaching experience. His area of interest in Adhoc Networks, Data Mining, & Network Security. He has guided 20 Graduate Students. He has published 5 papers in international journals. He has attended 10 National Workshops / FDP / Seminars etc.