ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 6, June 2017

A Black-hole Attack Detection Algorithm Based on Analysis of Node Behaviour in MANET

Sonali Khandelwal[1], Amit Shrivastava[2]

P.G. Student, Department of Computer Science Engineering, SVCE College, Indore, Madhya Pradesh, India

Assistant Professor, Department of Computer Science Engineering, SVCE College, Indore, Madhya Pradesh, India

ABSTRACT: Remote system is the network of mobilee PC hubs that are not physically wired. The fundamental favorable position of such system is speaking with whatever is left of the world while being mobile. The dangers to clients of remote innovation have expanded as the administration has turned out to be more prevalent. Security is an essential requirement in mobile ad hoc networks to provide protected communication between mobile nodes. This paper proposed an effective approach for investigation of black-hole intended to find security against malicious activity. The proposed method is based on node behaviour analysis by which different constraints apply to processing signal strength, number of repeating replies of the same node and to check the destination sequence number of all nodes and computing threshold by which we can demonstrate there is availability of malevolent attacker. The implementation of the proposed Secure routing method of finding the malicious attacker is execute using NS 2 i.e. network simulator 2 and for implementing the security protocol in the existing AOMDV routing protocol with alteration are simulated. The developed results show the adoptable performance of the algorithm and recover the different performance parameters, i.e. throughput, end to end delay, packet delivery ratio, and energy utilization.

KEYWORDS: Mobile ad-hoc Networks, NS2, AODV, Routing Protocol, Mobile nodes, RREQ, RREP, Black-hole

I. INTRODUCTION

NETWORK security is a weak link in wired and wireless network systems. In the recent years, wireless technology has enjoyed a tremendous rise in popularity and usage, thus opening new fields of applications in the domain of networking. Without using any fixed structural support the information is exchanged in the network of mobile devices. Such networks are termed as ad –hoc network. Correspondence protocol should manage an as often as possible changing system topology. Be that as it may, numerous applications require stable associations with certification a specific level of QoS (Quality of Service). In get to systems, get to point handovers may disrupt the information exchange. Maybe likewise, benefit settings ought to be exchanged to the new get to focuses, acquainting additional overhead and delay with the connection [1, 2].

A. MANET Overview

A ad-hoc system is an arrangement of hubs that don't need to depend on a predefined foundation to keep the network linked. Ad hoc networks can be shaped, merged together or partitioned into split networks on the soar without necessarily relying on a fixed infrastructure to manage the process. Nodes of ad hoc networks are frequently mobile, which also associate that they apply wireless communication to preserve the connectivity, in which case the networks are called as mobile ad hoc networks (MANET). Mobility is not, though, a obligation for nodes in ad hoc networks, in ad hoc networks, there may exists, static and wired nodes, which may which may utilize services offered by fixed infrastructure [3, 4].

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 6, June 2017

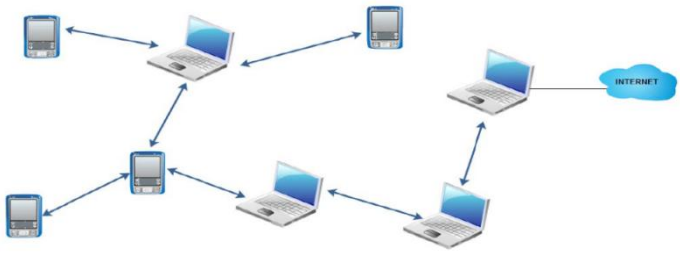

Figure 1: Example of MANET

Figure 1 is the depiction of example of mobile ad hoc structure: In this figure, every system is connected to each other. Whenever communication initiated, source node fund the destination through intermediate node. Once destination find it will transmit the information in an interval of time. Node can be any types of PDA devices.
A Mobile Ad hoc NETwork (MANET) is an arrangement of remote portable hubs that powerfully self-sort out in discretionary and brief system topologies. Individuals and vehicles can subsequently be internet worked in regions without a previous correspondence foundation or when the utilization of such framework requires remote augmentation. In the versatile, uniquely delegated framework, center points can clearly talk with the different centers inside their radio ranges; while centers that not in the prompt correspondence go utilize halfway hub (s) to speak with each other
The remainder of paper is planned as follows. Section II describes related work. Section III gives details about Black-hole Attack. In Section IV, proposed scheme is discussed for making MANET flexible for data transmission, Implementation of the proposed scheme is covered in Section V and Result Section is in VI. Finally conclusion and future directions are given in Section VII.

II. RELATED WORK

This section describes the previous works that are being carried out and how it could be related to our proposed work. To analyze the Black hole various approaches have been proposed. Some of the methods have been listed here:
Authors analyze the black-hole attack which is one of the possible attacks in ad hoc networks. However, in mobile ad hoc networks where the network topology dynamically changes, such static training method could not be used efficiently. In this paper, ***Satoshi Kurosawa et al. [5]*** propose an anomaly detection scheme using dynamic training technique in which the training data is updated at regular time intervals. The simulation results show the effectiveness of this scheme compared with conventional scheme. Mobile ad hoc networks (MANETs) are active wireless networks with no any infrastructure. These networks are feeble against many types of attacks. One of these attacks is the black hole. In this attack, a malevolent node advertises itself as having freshest or direct path to precise node to take up packets to it. The consequence of black hole attack on ad hoc network using AODV as a routing protocol will be examined. Furthermore, ***H. A. Esmaili et al. [6]*** examine solution for growing security in these networks. Simulation results using OPNET simulator represent that packet delivery ratio in the attendance of malicious nodes, decreases notably.
A wireless ad-hoc network is a temporary network set up by wireless nodes typically moving arbitrarily and communicating with no network infrastructure. Because of defense vulnerabilities of the routing protocols, however, wireless ad-hoc networks may be undefended against attacks by the malicious nodes.
In this study ***Semih Dokurer et al. [7]*** investigated the property of Black Hole attacks on the network performance. They simulated black hole attacks in Network Simulator 2 (ns-2) and measured the packet loss in the network with and without a black hole. Authors also proposed a simple solution beside black hole attacks. This solution enhanced the network presentation in the company of a black hole by about 19%.
An ad hoc network is a group of mobile nodes that dynamically form a provisional network. It functions without the use of obtainable infrastructure. One of the principal routing protocols used in ad hoc networks is AODV (ad hoc on demand distance vector) protocol. This is predictable to offer a variety of supple services to mobile and roving users by means of included homogeneous architecture. Energy constrained node, low channel bandwidth, node mobility, high

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 6, June 2017

channel fault rates, channel inconsistency and packet beating are some of the limitations of MANETs. The protection of the AODV protocol is compromised by a exacting type of attack called 'Black Hole attack'. Black hole attack is one of the security hazard in which the traffic is redirected to such a node that really does not exist in the network. In this attack a malicious node advertises itself as having the direct path to the node whose packets it wants to interrupt. In this paper, ***Pooja Jaiswal et al. [8]*** shows simulation results, supply fast message verification, identifies black hole and determines the safe routing and avoid the black hole attack.

In Mobile Wireless Ad Hoc Networks (MANET) every node functions as transmitter, router and data sink is network without infrastructure. It must discover its local neighbours and through them it will communicate to nodes that are out of its transmission range. Various features like open medium, dynamic topology, lack of clear lines of defense, makes MANET vulnerable to security attacks. Ad hoc on-demand distance vector routing (AODV) is one of the best and popular routing algorithm. AODV is severely affected by well-known black hole attack in which a malicious node injects a faked route reply message that it has a fresh route to destination. In this paper, ***Kamini Maheshwar et al. [9]*** present Intrusion Detection and Response Protocol for MANETs have been demonstrated that perform better than AODV protocol in presence of Black Hole Attack, in terms of false positives and percentage of packets delivered. Security in MANET against Black Hole attack is provided by using IDS AODV routing protocol and the result are analysed using an Optimized Network Engineering Tool NS-2, through various network parameter bases like TCP analysis, UDP analysis, Packet delivery ratio, Routing load etc.

III. BLACK-HOLE ATTACK

From the analysis of basic on-demand routing protocol's process, it is naturally reasonable that the plan accept the members to forward others packets, which is an impossible foresight in a free system like MANET. The result of not sending others packets or dropping others ppackets keeps any sort of correspondence to be set up in the system. Subsequently given an inclination between the need to secure administrations or to make sure basic functioning of the network, essentially the preference falls for the latter. Therefore, the need to tackle the packet dropping event takes superior priority for the mobile ad hoc networks to emerge and operate effectively [10].

A packet may be dropped under various reasons, which in revolve can be grouped into the following categories [11]

- Unevenness of the medium,
  - ✓ A packet may be dropped because of disputation in the medium
  - ✓ A packet may be dropped because of jamming and corruption in the average medium
  - ✓ A packet may be dropped because of wrecked link
- Authenticity of the node
  - ✓ A packet may be dropped because of flood of the transmission queue
  - ✓ A packet may be dropped because of lack of energy resources
- Selfishness of the node
  - ✓ A packet may be dropped because of the egotism of a node to keep its resources
- Maliciousness of the node
  - ✓ A packet may be dropped because of the hateful act of a malevolent node

In MANET, a packet dropping attack is a kind of denial of service in which a node in the network will fall the packets in its place of forwarding them, which is shown in the figure 2: This figure illustrate the demonstration of black-hole attack scenario. In this, different number of node dispersed in network whereas 2 node named as source and destination characterized by S and D respectively. Remaining node as noramal node. Simulataneously, a node which is characterized by A, is a malicious node called black-hole attack. In this situation, this node advertise shortest path for the destination node by which maximum traffic goes through by A. Source node broadcast the packet to all node including attacker node. Once a node A receive the packet it gives the fake acknowledgement toword the source node and start to drop packet. Therefore source node assume node A is acknowledged correctly and performace of the network is degraded.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 6, June 2017

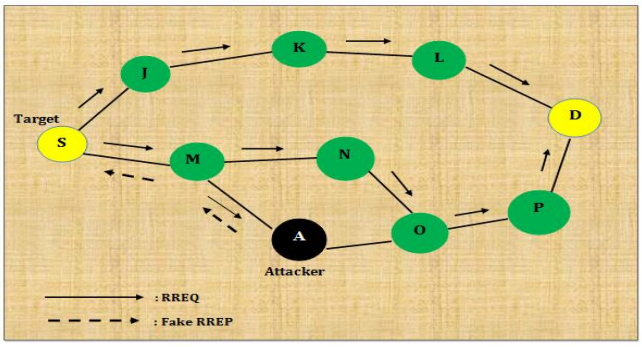

Figure 2: Black-hole Attack

In a black-hole attack, a malevolent node sends false routing information, claiming that it has an best route and causes other excellent nodes to route data packets during the malicious one. For example, in AODV, the attacker can send a false RREP (including a false destination sequence number that is made-up to be equivalent or higher than the one contained in the RREQ) to the source hub, guaranteeing that it has an enough new route to the goal node. This makes the source node pick the route that goes all through the attacker. Subsequently, all activity will be routed throughout the attacker [12].

IV. PROPOSED WORK

The proposed work is intended to find an adoptable security algorithm formulation by which the mobile ad hoc network becomes secure. We enlist basic 3 modules of our methodology that construct entire system that proving efficiency and effectiveness of this work.

1. **Initiate Route Discovery**
2. **Assigning Parameter**
3. **Formulate Algorithm**

1. Initiate Route Discovery

For securing network, the proposed algorithm is developing using different constraint. So that we basically we need to assume some constraints to progress further. For this we need to establish an idle network for demonstrating the concept, firstly we create a normal network where with different number of network e.g. 20, 40, 60, 80 and 100.
Initialize the Network, with N nodes where$N = 1, 2, 3, \ldots..$,, in ideal condition
S initiates a RREQ message with the following components:
– The IP addresses of S and D
– The present sequence number of S and the last known sequence number of D
– A broadcast ID from S. This broadcast ID is incremented each time when S sends a RREQ message.The couple of the source S forms a exclusive identifier for the RREQ.
For route discovery, we process a route request RREQ to all other node except the node which is generating request. Therefore, source node wait for the route reply i.e. RREP which is coming from that node to its match broadcast ID and IP address.
Secondly, for processing proposed method, we use some network parameter to process the algorithm from this we get the efficient output that outlines the securing network. In next point we assume some checking constraints which is used to build algorithm.

2. Assigning Parameter

In this section we describe assigned parameter need to process the proposed approach by we construct the algorithm

- ✓ **Signal Strength Power:** The signal strength of a node shows the transmission power capacity thus for extra optimal node collection the signal strength of the node is used. The signal strength of the node can be signify using

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 6, June 2017

the letter S for further discussion. We compute signal strength of all individual nodes and make average threshold value of all nodes. Compute signal strength by using following formula:

A single line-of-sight path among two sensor nodes is rarely the only means of propagation. The two ray ground reflection model believe both the direct route and a soil reflection path. It is shown that this model gives more precise forecast at a lengthy distance than the free space model. The received power is predicted by

$$\text{Recevied Signal Strngth Power } (S_S) = \frac{P_t G_t G_r (H_t)^2 \ (H_r)^2}{d^4 \ L}$$

- ✓ **Number of Repeated Replies:** In this constraints, once source node broadcast the number of packet to all other neighbors that node can forward the packet to the destinations. When we discover the route all node on that path participate for communication. As well as neighbor receive the packet give acknowledge to the source. In the network a particular node receives the data packets and always gives the same replies to the source node even node is receiving diverse number of packets on different time interval. There is a case of malicious attacker that consumes packet and repeating same reply each time for each packet request.
- ✓ **Sequence Number:** AOMDV uses sequence numbers to determine an up-to-date path to a destination. Every entry in the routing table is associated with a sequence number. The sequence number act as a route timestamp, ensuring freshness of the route. A node may change the sequence number in the routing table entry of a destination only if:
  - It is itself the destination node, and offers a new route to itself, or
  - The path towards the destination node expires or breaks.

In our case we always check the destination sequence number of every data transmission interval. To validate the freshness of the path that AOMDV always hits the highest sequence number of the packets. Here, when a packet arrives at the particular node it checks the current sequence number with stored previous sequence number or with maximum sequence number. Therefore apply check for ensuring there is availability of the malicious node.

3. Formulate Algorithm

The proposed work is indented to secure the network, thus the AOMDV routing protocol is modified to identify the malicious node among the available routes between source and destination.

Table 1: An Algorithm for Attack Detection and Prevention

Input: Number of Nodes;
Output: No Attacker found;

Process:

1: Initialize the Network, with N nodes where $N = 1, 2, 3, \ldots\ldots , ,$ in idle 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 Average threshold of signal strength for all nodes

$$\text{Recevied Signal Strngth Power } (S_S) = \frac{P_t G_t G_r (H_t)^2 \ (H_r)^2}{d^4 \ L}$$

$$\alpha_{s_s} = \frac{1}{N} \sum_{i=0}^{N} S_{s_i}$$

6: For each node in suspected list
7: if $(\emptyset_{S_s} < S_{s_i})$
Label node as Malicious Node
else
Label node as legitimate
8: end if
9: Source node broadcast packet towards the neighboring node

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 6, June 2017

10: if N_s get same reply from same node for each packet, then
11: Stop Packet Transmission to Intended Node and Change the Route
12: for each received packet, check Destination Sequence Number (DSN)
13: if (last Seq_No. = = Current Seq_No.)
Attacker node is available
14: end if
15: Always check higher sequence number with all received sequence Number
16: For this, route is not reliable
17: end process

V. IMPLEMENTATION

A. *Simulation Scenario*

The simulation is being implemented in the Network simulator [13]. Protocol used here is AOMDV.

Table 2: 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
Number of Nodes	20, 40, 60, 80, 100

This area gives the comprehension about the reproduction situations under which the examinations are performed. To exhibit the security procedure their two key reproduction situations are proposed in this area. Both the reproduction situations are led with various number of hubs that are 20, 40, 60, 80 and 100 nodes for black-hole attack

1. Simulation when Black-hole is deployed: In this network recreation the network is configured using the existing RDBR approach with AOMDV routing protocol. For constitute the visualization the malevolent node is deployed on network and the network presentation is animated 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 figure 3. 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.

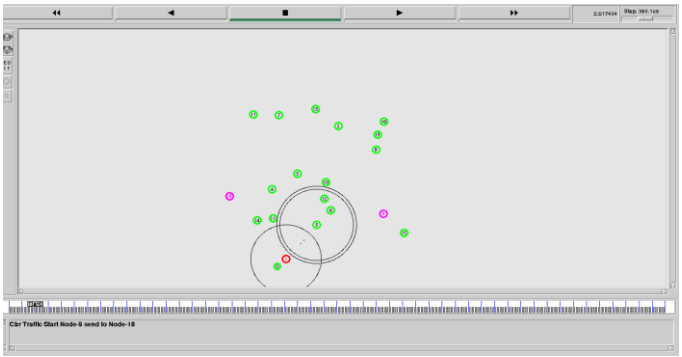

Figure 3: Network under Black-hole Attack using RBDR Approach

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 6, June 2017

2. Simulation using the Proposed Secure Routing Technique: In this simulation scenario the proposed routing approach which is developed with the help of AOMDV routing modifications are implemented with the Mobile ad hoc network. In addition a like kind of attacker node on the network is deployed. The deployed attacker is normalized using the technique and their act is estimated on the basis of the network trace files. Additionally the measured performance is compared with the traditional RBDR approach under attack conditions. The figure 4 demonstrates the simulation screen of the proposed secure routing technique for Black-hole Attack prevention.

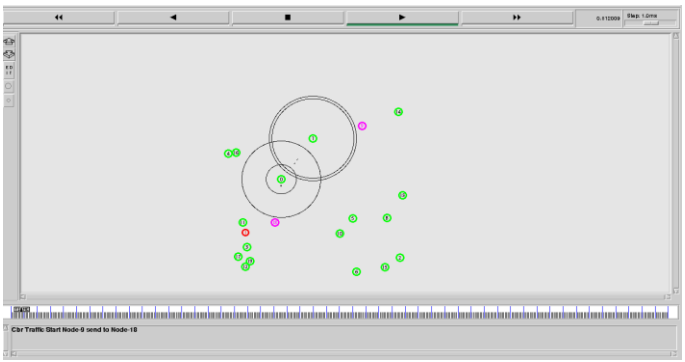

Figure 4: Proposed Secure Routing Method for Attack Prevention

VI. RESULT ANALYSIS

A. End to End delay

End to end delay is the time taken by a packet to travel from source to destination. Delay depends on number of hops and congestion on the network. End-to-end delay of data packets includes all possible delays caused by buffering during route discovery, queuing at interface queue, retransmission delays at MAC layer, propagation and transfer time:

$$\text{E2E Delay} = \text{Receiving Time } (R_t) - \text{ Sending Time}(S_t)$$

Figure 5 shows the comparative End to End Delay of the traditional RBDR 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 consume delay time during packet transmission as compared to base approach when black-hole attack is deployed.

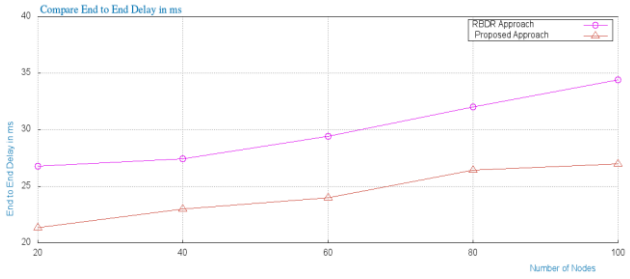

Figure 5: End to End Delays

B. Packet Delivery Ratio

Packet delivery ratio is defined as the ratio of data packets received by the destinations to those generated by the sources. Mathematically, it can be defined as:

$$\text{Packet Delivery Ratio (PDR)} = \frac{S_1}{S_2} \text{X100}$$

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 6, June 2017

Here, S_1 is the sum of data packets received by the each destination and S_2 is the sum of data packets generated by the source node. Graphs show the fraction of data packets that are successfully delivered during PDR versus the number of nodes.

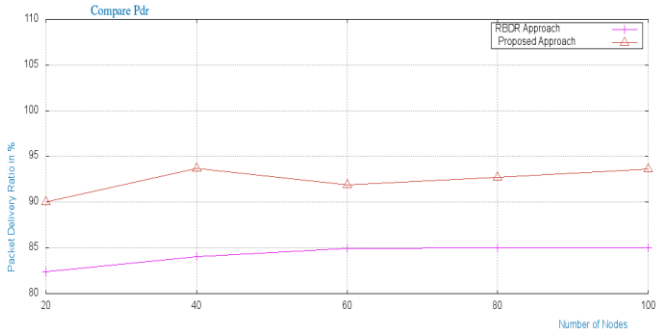

Figure 6: Packet Delivery Ratios

The comparative packet delivery ratio of the networks is given using figure 6, in this figure the X axis shows the number of nodes for simulation in the network and the Y axis shows the amount of packets successfully delivered to the destination in terms of the percentage. The pink line of figure represents the performance of the traditional RBDR technique and the green purple line shows the performance of the proposed technique.

C. Throughput

It is defined as the total number of packets delivered over the total simulation. This information might be conveyed over a physical or logical connection, or go through a specific system node. The throughput is generally measured in bits every second (piece/s or bps), and now and again in information bundles every second or information parcels per availability.

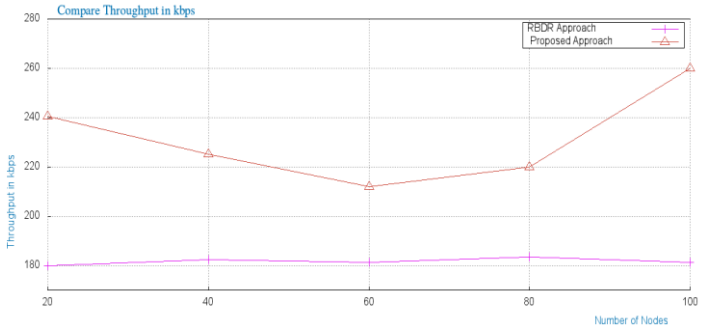

Figure 7: Throughput

The comparative throughput of the network is demonstrated using figure 7, X axis of this graph shows the number of nodes in network and the Y axis shows the throughput of the network in KBPS. The purple line in this figure shows the performance of the proposed technique and the blue line shows the performance of the traditional RBDR routing. According to the achieve performance the proposed method recover the throughput of the network during the attack conditions also consequently the technique is efficiently avoid the attack effect as compared to the existing routing. Also while malicious node increases in network performance is decreases.

D. Routing Overhead

Routing overhead is depict as the amount of extra packets injected in network for communication. The key reason behind to calculate this parameter is, because the routing overhead decreases the packet delivery ratio and transmission rate of the data. The given figure 8 shows the performance of network in terms of routing overhead. The routing overhead increases the amount of bandwidth consumption is decreases network performance.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 6, June 2017

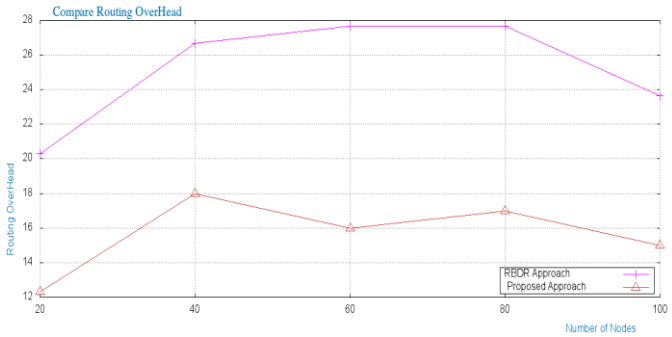

Figure 8: Compare Routing Overhead

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 number of node is not performing proper functioning.

E. Remain Energy

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 figure 9 shows the energy

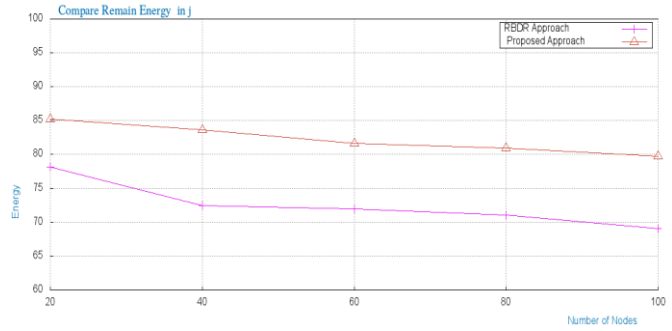

Figure 9: Remain Energy for Black-hole Attack

Figure 9 shows remain energy of the network in both implemented simulation scenarios. The pink line of the diagram shows the amount of energy remains during communication events with the AOMDV routing protocol under attack condition for RDBR approach. Additionally the purple line shows the amount of energy remains 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 Black-hole attacks targeting the network by dropping the legitimate packets of the network. Therefore the proposed technique is effective and able to recover the network from the attack situations.

VII. CONCLUSION

The present era is completely dependent on Internet. Internet serves as a global information source for all users, so the availability of internet is very important. As the need of internet is growing with time, various issues related to its security comes insight. In this research work Black-hole attack is targeted for the investigation and research study. In black hole attack attacker node 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 proposed a secure routing algorithm which

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 6, June 2017

analysis of node (s) behaviour using signal strength, number of repeated replies and sequence number of current and previous packet constraints for establishing secure path using AOMDV routing protocol enhancing the detection rate of malicious attackers. The implementation of the required secure solution is performed on the help of NS - 2 network simulation environment, additionally AOMDV routing protocol is modified for incorporating the concept of security in mobile ad hoc network. The proposed technique is implemented and simulated with the 20, 40, 60, 80 and 100 nodes.

REFERENCES

[1] Xin Ming Zhang, Feng Fu Zou, En Bo Wang, and Dan Keun Sung "Exploring the Dynamic Nature of Mobile Nodes for Predicting Route Lifetime in Mobile Ad Hoc Networks" IEEE Transactions on Vehicular Technology, vol. 59, no. 3, March 2010.
[2] Taneja,S., & Kush, A.,"A Survey of routing protocols in mobile ad hoc networks", International Journal of Innovation Management and Technology, vol. 1, no. 3, pp. 2010 - 0248, 2010.
[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] Kurosawa, Satoshi, et al. "Detecting blackhole attack on AODV-based mobile ad hoc networks by dynamic learning method." IJ Network Security 5.3 (2007): 338-346.
[6] Esmaili, H. A., and M. R. Shoja. "Performance analysis of AODV under black hole attack through use of OPNET simulator." arXiv preprint arXiv:1104.4544 (2011).
[7] Dokurer, Semih, Y. M. Erten, and Can Erkin Acar, "Performance analysis of ad-hoc networks under black hole attacks", SoutheastCon, 2007, Proceedings, IEEE, 2007.
[8] Pooja Jaiswal, Dr. Rakesh Kumar, "Prevention of Black Hole Attack in MANET", International Journal of Computer Networks and Wireless Communications (IJCNWC), Vol. 2, No. 5, PP. 599-606, Oct 2012
[9] Kamini Maheshwar; Divakar Singh, "Black Hole Effect Analysis and Prevention through IDS in MANET Environment", European Journal of Applied Engineering and Scientific Research, 1 (4), PP. 84-90, 2012.
[10] O. F. Gonzalez, 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. 1, June 2008.
[11] V. L. L. Thing and H. C. J. Lee, "IP Traceback for Wireless Ad-hoc Networks", Available from: http://www.diadem-firewall.org/publications, Accessed on: 28th November 2016.
[12] Kannhavong, Bounpadith and Hidehisa Nakayama "A survey of routing attacks in mobile ad hoc networks", IEEE Wireless communications 14.5 (2007).
[13] The Network Simulator. NS-2 [Online] http://www.isi.edu/nsnam/ns/