International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435(Online) Volume 10, Issue 3, March 2021)

The Neighbor Identification based Security Scheme for Blackhole Attack in MANET

Kirti Rajak[1], Professor B. L. Rai[2]

[1]*M.Tech. Scholar,* [2]*Professor, Department of Computer Science & Engineering, Organization – Jai Narain College of Technology, Bhopal, M.P., India*

kirtirajak08@gmail.com[1], blrai3021@gmail.com[2]

***Abstract*— In the Mobile Ad hoc Network (MANET), all nodes are free to travel in the absence of a centralized coordination mechanism. As a consequence, the attackers or malicious nodes are quickly influenced by this kind of network and are responsible for routing misbehavior. Network routing is mandatory to deliver data between source and destination. In this project, we are focusing on the security sector in MANET and have suggested a new protection scheme against routing misbehavior via black hole attack. The attacker would be influenced by all alternative routes chosen by the sender to transmit data to the network. At the time of routing, the malicious nodes are forward confident that their detection is not a dynamic process. The proposed Neighbor Identification based Security scheme for Blackhole attack (NISB) scheme detects the information of the intruder by means of the hop count mechanism. The routing details of the individual data at which the intermediate node resides is reached and the next hop information at that node is verified by the IDS scheme. The black hole attacker node Identifier is forwarded to the network by not intervening in the routing process in the potential attacker. The suggested protection scheme detects and provides for deterrent against misbehavior routing into a malicious assault. Here we compare the routing efficiency of the BAODV, SAODV and NISB security scheme. The efficiency of standard multi-path routing and the suggested NISB scheme is almost identical. The intruder degrades the overall routing efficiency but states that in the presence of the attacker, routing misbehavior is fully thwarted by the new NISB scheme and recovers higher percent of the data as opposed to SAODV routing mechanism.**

***Index Terms*— MANET, NISB, BAODV, SAODV, Blackhole Attack, Routing**

I. INTRODUCTION

The goal of mobile ad hoc network technology is to allow web access at any place and at any time, without a predefined infrastructure that supports the quality of users anywhere network intelligence is located within each mobile device.

Attributing to its self-configuration and self-maintenance functions, MANETs may have a broad range of applications, including emergency operations, military and security operations, conferencing, enforcement and residential networks. Mobile ad hoc networks are smaller infrastructures in which nodes are able to turn Affiliate to mount them in a discretionary fashion [1]. For networking, two nodes will have multiple connections between them and will be implemented in an extremely complete manner, ideal for a cost-effective and time-effective environment and for a situation where it is difficult to build the device. Due its features, such as peer-to-peer architecture, running but not central collection, complex topology, unsafe service, and frequent link breakage attributable to mobile nodes, battery time, device capacity and non-uniformity, security is difficult for MANETs. Communication in MANETs is based on single hop in connection layer protocols and multi hop in network layer protocols. Centered on the assumption that is based on the premise that in cooperation phase each of the nodes in an excessively network is cooperative, but unfortunately in violent environments this claim is not true. Through violating protocol specifications, malicious attacks will simply disrupt network operation. In MANETs, network layer activity is allowed by routing, and the forwarding of information packets is vulnerable to malicious attacks. Reactive (On Demand) Routing and Positive (Table driven) Routing are classified as routing in MANETs. Whenever required, a reactive protocol initiates routes, while proactive protocols maintain consistent and up-to-date tables containing routing information from each node to each node. We tend to consider reactive routing protocols like AODV in this article. Since AODV gives no security mechanism, an attack by any malicious node will be carried out by disobeying the requirements of the protocol. Misleading Sequence Number Increment and Hop Count Decrement are key AODV flaws.

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435(Online) Volume 10, Issue 3, March 2021)

Area Attack is an Attention Attack associate during which all packets in an overly network are routed to a single node that seems to have a contemporary route incorrectly and absorbs or loses those packets without routing them to different nodes or destination nodes.

Paper are divided into multiple section, in section I describe about introduction, section II provide the literature survey, section III describe about our proposed work, section IV define the result discussion and section V describe about conclusion of proposed approach [2].

II. Literature Survey

In this section discuss the existing work which uses to secure the wireless ad hoc network by various type of attack. Those works helps to provide new way to security of mobile ad hoc network.

Komal Joshi and Vijaya Sagvekar[2] "Efficient technique for the prevention of cooperative blackhole attacks in the MANET using the aodv protocol" In this title, an approach was proposed to stop collective blackhole attacks using cooperative blackhole prevention techniques (CBPT). Works on the concept of using the three hop away knowledge table and three routes from Source to three hop-off nodes. The aim of this title is to have better protection and better efficiency in terms of CBPT packet distribution in the presence of a black hole with an affordable delay and overhead.

Nitesh A. Funde and P. R. Pardhi [3] they develop a System for "Detection & prevention techniques for black & gray hole attacks In MANET: A Survey" In this title, we reviewed various techniques to prevent black & grey hole attacks in MANET.

Sharndeep Kaur and Dr. Anuj Gupta [4] this title presents a modern strategy for the identification and avoidance of black hole attack in MANET to deter and eliminate black hole attacks in MANET. It's a modern methodology, really. The met heuristic search scheme, which is implemented by combining ACO min with Max versions with DRPI test tables based on the AODV Routing Protocol, is used to perform this purpose. Finally, the NS2 simulation shows that this technique detects and isolates the malicious node and reduces the loss rate of the packet while increasing the node forwarding capacity of the data.

Jaydip Sen [5] this title deals with "Detection of Cooperative Black Hole Attack in Wireless Ad Hoc Networks" It becomes more serious with the help of a network of hostile nodes. The proposed mechanism would not apply any primitive cryptography to the message routing. Rather, it safeguards the network by identification and response to the nodes' malicious behavior.

Simulation results indicate a considerably high detection performance on the computer for moderate overhead network and overhead node computing.

Rashmi and Ameeta Seehra[6] "A New Approach to Prevent Black-Hole Attack in MANETs" In this title, The clustering approach to identification and avoidance of black-hole attacks in MANETs is illustrated in an Ad-hoc On-Demand Distance Vector (AODV). This technique is used to define a distinct difference within the number of data packets received and transmitted from node by each cluster member to the cluster header. Both nodes cover the malicious nodes on the network as anomaly is perceived.

K.S. Sowmya, *et. al.* [7] In this heading, we have proposed a device for the identification and avoidance of blackhole attacks in MANET using ACO, which will be the means by notifying other nodes on the incident network. The implementation and conclusions shall be protected by Sections 5 and 6, respectively. Not only does our protocol discourage blackhole attacks but, in the case of black hole, increases the overall performance of ACOs.

Gagandeep, *et. al.* [8] In this title we analyze various types of attacks on various layers in the protocol pile under "Analysis of Different Security Attacks in MANETs on Protocol Stack A-Review" Various types of attackers are attempting to reduce network performance and latency using various approaches. The key focus of this paper is on routing and security concerns relating to mobile ad hoc networks that are needed to ensure safe communication. The attacks against MANET can be categorized as active and passive attacks on the basis of the essence of the attack encounter. There can be two types of Network attackers: intruder and outsider. Whereas an outsider attacker is not a legitimate network client, a MANET routing method is approved for an insider attacker.

Harjeet Kaur, *et. al.* [9]'Study of Blackhole Attack Using Separate Routing Protocols in MANET" This research initiative centered first on the comparative investigation of routing protocols under different types of attack, then on the development of scenarios and simulation and the investigation of performance metrics viz. Packet distribution ratio, average jitter, average latency and end-to-end latency of reactive, constructive and hybrid routing protocols such as AODV and AODV with blackhole attack, OLSR and OLSR with blackhole attack, and ZRP and ZRP with blackhole attack for various situations under different circumstances.

Fan-Hsun Tseng, *et. al.* [10] "A survey of black hole attacks in wireless mobile ad hoc networks" In this title, we review current solutions and discuss state-of-the-art routing methods.

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435(Online) Volume 10, Issue 3, March 2021)

Not only can we define these ideas as a single black hole attack and a joint black hole attack, but we also examine the types of these solutions and include a summary table. We plan to provide more researchers with detailed work in preparation.

Irshad Ullah, and Shahzad Anwar[11] "Effects of Black Hole Attack on MANET Using Reactive and Proactive Protocols" this title is intended to research the effects of a Black Hole Attack on MANET using both the Proactive Routing Protocol (i.e. Optimized Connection State Routing (OLSR) and the Ad-Hoc On Demand Distance Vector (AODV) protocol. A comparative study of the Black Hole attack with both protocols is taken into account. The effect of the Black Hole attack on the MANET efficiency was tested by investigating which protocol was more vulnerable to the attack and it was found that AODV was 10% more vulnerable to the Black Hole attack compared to OLSR. Measurements were made with respect to throughput, end-to-end delay and network load. Simulation is conducted in the Optimized Network Engineering Tool (OPNET).

Shashi Gurung, *et. al.* [12] "Detection of Black Hole Attack in Mobile ADHOC Networks" In this title, we suggest an algorithm to detect and avoid black hole attacks in AODV routing. The suggested approach uses the conformation acknowledgement request to verify whether or not the destination has received a dummy packet.

III. Proposed Security Scheme

Network security is essential part for any type of communication, in the network various type of mis-activity happen in the network. Mobile ad hoc network is more vulnerable as compare to wire or infrastructure based network. In this dissertation secure the mobile ad hoc network from blackhole attack using neighbor identification based security (NISB) technique. Black hole attack is network layer attack which generates the higher sequence number and spoof the source node for fresh route and source node immediately sends the data to higher sequence number generated route and data captured by attacker node. In the last decades in research various security mechanism are used to detect and prevent the network. In our neighbor identification based security (NISB) mechanism every node watches the activity of its neighbour node and stored the activity. While the watcher node identify neighbour node generate higher sequence number during route reply or capture or drop the data packet then set as suspicious.

Similarly its entire neighbour also found same behavior for that node, then all neighbors are collaborative take decision to block the suspicious node for their blackhole behavior and intimate to reset of the network for do not take communication the blackhole node. Proposed NISB security mechanism provides more security as compare to existing security for blackhole attack.

By not sending the data packets on the network, the black hole attacker is decided. The attacker node updates the initial routing plan by finding the attacker in the network. The way nodes control a network will divide attacks resulting from malicious behavior. In this analysis, the work is about "black hole node" a malicious node. The suggested safety mechanism is based on MANET's experience of routing packets. The current case of packet falling happens due to nodes, congestion and energy scarcity. Yet blackhole aggressor conducts continuous destructive operations, which are signs of irregular routing. Adequate identification is not very simple for NISB, but an attacker is detected and the routing efficiency can also be increased by blocking an attacker. If a network is invaded by hostile inner nodes, identification and exclusion of malicious nodes is the most crucial thing.

Proposed Algorithm:

Proposed neighbor identification based security (NISB) technique detect and secure the network from blackhole attack under MANET. In this section formally describe the algorithm which provide reliable and secure communication.

Algorithm: Detection and Prevention Black Hole attack using NISB

Input:

M_j: Mobile Nodes
B: Blackhole nodes $\in M_j$
P_i: Set of Neighbour preventer node $\in M_j$
S: set of Source Nodes $\in M_j$
D: set of Receiver Nodes $\in M_j$
R_r: radio Range $550m^2$
I: set of intermediate nodes $\in M_j$
Routing: AODV

Output:

Blackhole node detection, PDR, percentage of attack, delay, throughput

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435(Online) Volume 10, Issue 3, March 2021)

Procedure:

S← execute-route(S, D, AODV)
While (M_j =in range of R_r) do
I ← receive routing packets
For each I in range
While I ≠ D do
Store the S address and forward to next hop
End do
If (I== D) then
Receives route packets
Send back Ack to S node
Call data_pkt()
Else
R not in zone
End if
End do
// Attacker Activity Module
If I receive routing packets & forward == Null Then
I work as B node
B← update route
B← set sequence number is higher
B send route ack to S node
Data_pkt(S,D,pkt)
B← receives data and not forward to D node
Data capture by B node
Else
I work as normal
Forward Data_pkt(S,D,pkt) to next hop
End if
// Data Sending Module
Data_pkt(S,D,pkt)
If path is available then
S Generate data packet
Forward data by established path
P_i watch ∀I node in path
While pkt incoming in I do
If I receives && pkt_forward = true then
I← trusted-node
Else
Watch I profile by individual P_i nodes
Collaborative Calculated trust value by P_i
If I found as Blackhole Then
I-Un-trust ← not forward to D
B← I set as
Call-Prevention ();
Else
I not a Blackhole
I treated as congested node
End if
End if
End do
// Detection Prevention Module
Prevention (P_i, M_j)
If M_j range in P_i && suspicious B nodes Then
If (B updated routing packet) Then
P_i watches the B activity
While P_i identifies B not forward message to D do
P_i← Detect B drop message
P_i spread the B activity to all M_j
Block the B node by P_i
S ← Execute Re-Route message
Search new path where B not present
M_j respond B by blocking message
Else
B not a suspicious
M ← B
B is Normal Node
End If

Each mobile node maintains a routing table that holds the next hop node details for the path to the destination node. If the source node wants to route the packet to the destination node, it will use the specified route if there is a fresh route to the destination node in its routing table. The proposed NISB not only detects routing performance, but also prevents an attacker from using a complex network. The proposed NISB shall have the equivalent performance of normal routing and the proposed NISB presence routing. The key idea behind this approach is to list a collection of malicious nodes locally at each node whenever they behave as a regular node.

IV. Result Description

A. Simulation Parameters

Table 1 are represents the following simulation parameters to make the scenario of routing protocols. The detailed simulation model is based on network simulator-2 (ver-2.31), is used in the evaluation. The NS instructions can be used to define the topology structure of the network and the motion mode of the nodes, to configure the service source and the receiver etc.

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435(Online) Volume 10, Issue 3, March 2021)

Table 1:
Simulation parameters will uses for simulation

Parameters	Configuration Value
Routing Protocol	AODV
Simulation Area	1000m*1000m
Number of Nodes	20,60,100
Misbehaving Percentage	0-40%
Attack Type	Blackhole
Security Technique	SAODV, NISB
Physical Medium	Wireless, 802.11
Initial Energy (joule)	100J
Mobility Speed	Random
Mobility Model	Random Waypoint
Simulation Time (Sec)	100Sec
Transmission Range	550m
MAC Layer	802.11
Antenna Model	Omni Antenna
Traffic Type	CBR, FTP
Propagation radio model	Two ray ground

B. Result Description

The results analysis in case of proposed Neighbor Identification based Security scheme for Blackhole attack (NISB), previous SAODV and BAODV are mentioned and observe that the NISB is provides secure and better performance in MANET.

1. Packet Delivery Ratio

The packets receiving in network is showing the improvement in performance. The number of mobile nodes are continuously sends the information of sender to receiver. Packet Delivery Ratio is the percentage of packets received at destination in a given simulation time of 100 seconds.

The PDR of attack at start is about 20 % maximum in scenario of 100 nodes. The PDR of previous SAODV is less and about at an average the 6% improvement in performance in NISP scheme in MANET. The performance of Secure is better to Normal routing performance i.e. more than 94.34 % in 60 node density scenario. The exact value of performance is mention in figure 1.

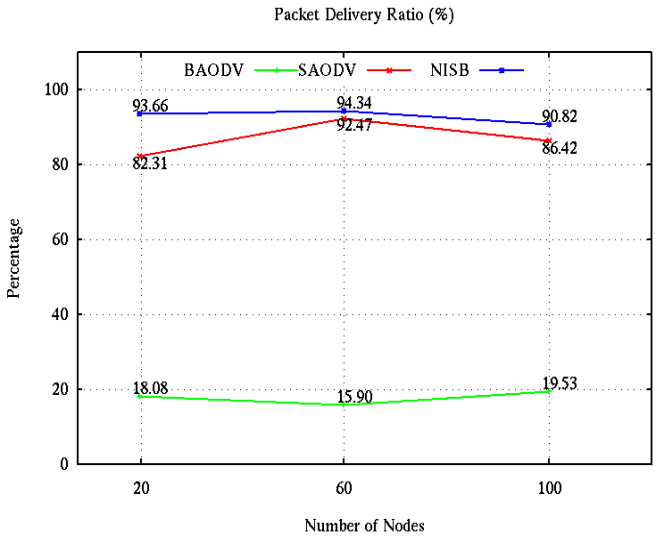

Figure 1: PDR Performance

2. Routing Overload

Routing Load Analysis of the network is define as, it is measured as the number of routing packets transmitted for the each data packet delivered at the destination. The Routing Load in the attacker presence is about the 8.18(max), in case of previous scheme is 3.38(max) but after applied NISB scheme means it is about 2.99(max) overhead in 100 seconds. In the routing load analysis of Secure is better than previous and Malicious because the load of 8.18 has no sense and at malicious only few data Packets communicate in complete time period of communication. That means performance is very low. So we can say our secure scheme is better than previous scheme. The exact figure of performance is mention is mention in figure 2.

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435(Online) Volume 10, Issue 3, March 2021)

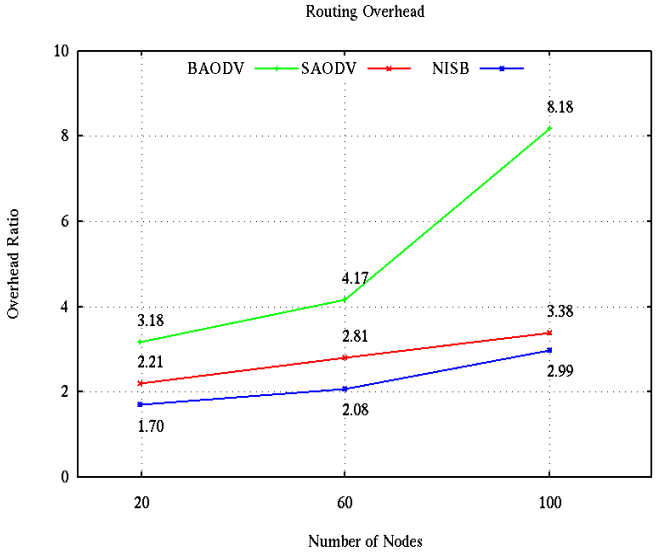

Figure 2: Routing Overhead Performance

3. End to End Delay Analysis

The packets receiving performance of all protocols is evaluated in this graph and observe that the proposed NISB provides the highest receiving that is the sign of better security scheme in MANET. The delay performance is easily affected because of dropping packets in network.

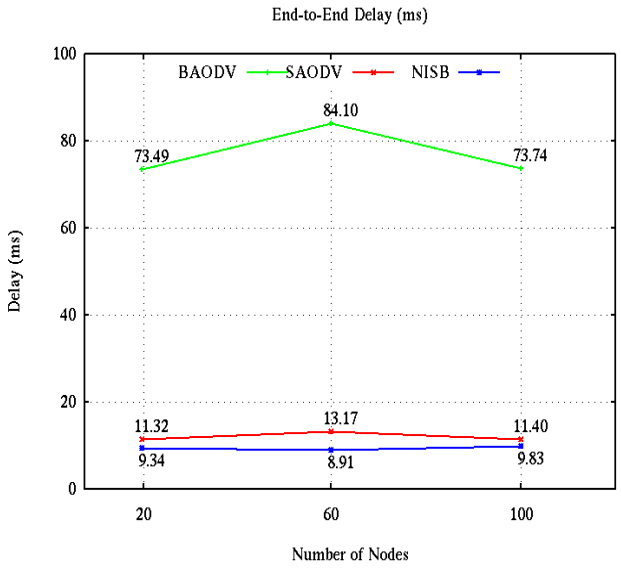

Figure 3: End to End Delay in [ms]

The only attacker performance is about negligible in term of packets receiving. The better and more packets receiving is provide the better performance of network and this performance is provides by case of proposed NISB scheme. The delay in BAODV is more and the delay in NISB is less as compare to SAODV or previous scheme in MANET. The exact performance is mention in figure in figure 3.

4. Residual Energy of Network (joule)

The data retransmission consumes maximum amount of energy and after that the energy is consume in receiving. The data dropping in network means the again sending and receiving energy is require for new data packets and by that the proper utilization of limited energy resource is affected. This graph represents the residual energy analysis in case of proposed NISB, previous SAODV and BAODV. In this graph we clearly notice the smooth depletion of energy from initial energy to energy remain in nodes after the end of simulation time. It means the proposed scheme based routing selection strategy are maintained the reliability in network. The analysis in tabular form is available in figure 4.

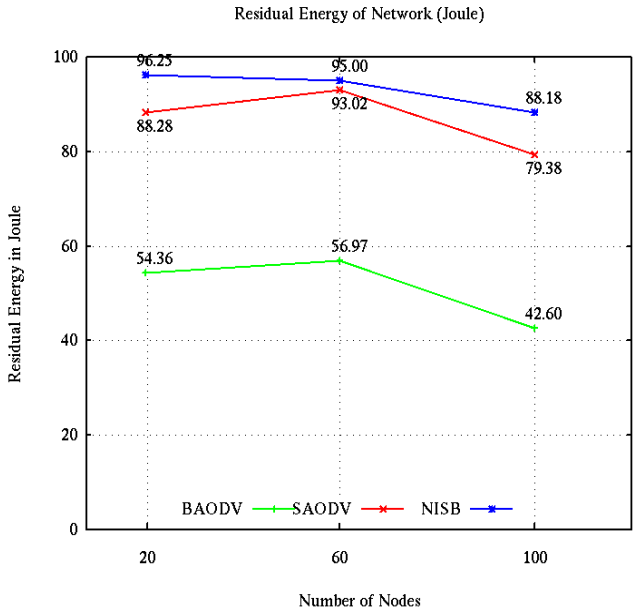

Figure 4: Remaining Energy Performance

5. Throughput Analysis

Throughput analysis shows the total number of data packets send in per unit of time.

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435(Online) Volume 10, Issue 3, March 2021)

At the normal stage as the figure 5 shows that in NISB the packets per unit of time receiving is maintain high at the time about 100 seconds approximate 90.83(max) and only 8.39% (max) in presence of attacker and that shows the degradation in performance due to the presence of attacker. The performance of SAODV is also about 87.83(max) but not higher than NISB. The better throughput performance is also shows the packet receiving is more. So proposed approach is better than the previous approach and the exact figure of performance is mention in figure 5.

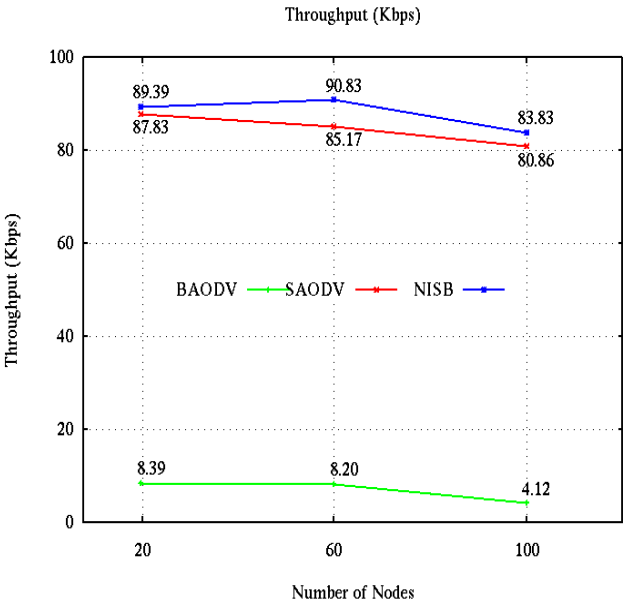

Figure 5: Throughput Performance

5. Blackhole Attacker Analysis

The proposed scheme is provides the secure communication in presence of proposed NISB scheme. In this graph the number of packets drop in presence of attacker is evaluated and observe that in difference node density scenarios up to at the end of simulation. The packets drop in presence of attacker is 1165(max). The attacker infection in presence of NISB is zero that is the positive and strong effect of security scheme. The performance in term of figure is mention in figure 6.

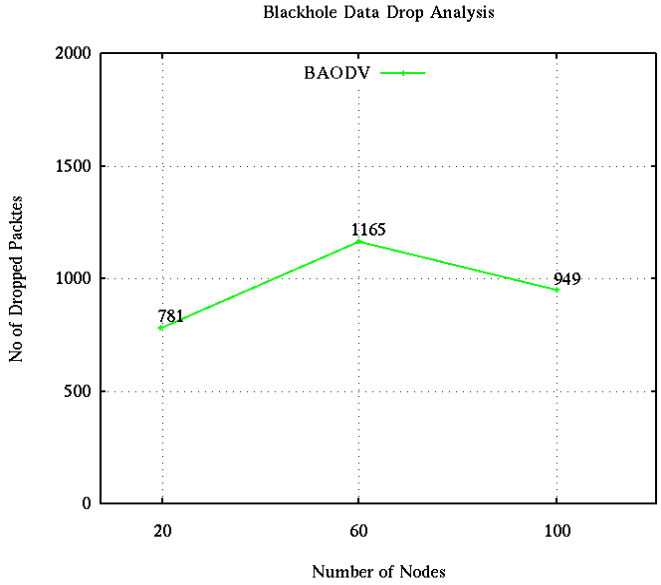

Figure 6: Attacker Drop Analysis

V. Conclusion And Future Work

Security is important to this type of decentralized network. In this research, simulate the scenario of BAODV, SAODV and NISB and find its effects in network in term of measures performance. We used the AODV routing protocol in our research. However, the other different routing protocols may also be simulated. In this paper, we're trying to overcome the network's cooperative impact. However, it is possible to detect the drop attack of the packer by means of the proposed Neighbor Identification based Security scheme for Blackhole attack (NISB) protection scheme. The routing efficiency of the BAODV, SAODV and NISB security scheme is compare and identified that the performance of NISB is better. The efficiency of standard multi-path routing and the suggested NISB scheme is almost identical. As a malicious server, it is the key security threat that affects the performance of the AODV routing protocol. The proposed (NISB) scheme detects the information of the intruder by means of the hop count mechanism. The routing detail of the individual data at which the intermediate node resides is reached and the next hop information at that node is verified by the NISB scheme.

The effect on packet loss is clearly seen in throughput and other metrics. As a malicious server, it is the key security threat that affects the performance of the AODV routing protocol. Its identification is a big concern. Therefore, the proposed IDS algorithm work would be outstanding for detecting and protecting the network against a malicious attack. Improvement in overcoming the impact of the assault should be geared at controlling the pause.

The other intruder, like a wormhole, often drops the packets by making a tunnel. In future any strategies for detect wormhole attacker in proposes. Even attackers like packet drop and wormhole for AODV routing algorithm can be applied in real-life situations and their analysis can be compared to the results of the proposed NISB analysis.

REFERENCES

[1] Mahuwa Goswami, Prashant Sharma, Ankita Bhargava **"**Black Hole Attack Detection in MANETs using Trust Based Technique" (IJITEE) ISSN: 2278-3075, Volume-9 Issue-4, February 2020.

[2] Komal Joshi, Vijaya Sagvekar "an efficient technique for preventing cooperative blackhole attack in manet using aodv protocol" International Journal of Innovative Research in Computer and Communication Engineering Vol. 1, Issue 2, April 2013.

[3] Nitesh A. Funde, P. R. Pardhi "Detection & Prevention Techniques to Black & Gray Hole Attacks In MANET: A Survey" International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 10, October 2013.

[4] Sharndeep Kaur, Dr. Anuj Gupta, "A Novel Technique to Detect and Prevent Black Hole Attack in MANET"IJIRSET Vol. 4, Issue 6, June 2015.

[5] Jaydip Sen "Detection of Cooperative Black Hole Attack in Wireless Ad Hoc Networks" Innovation Lab Tata Consultancy Services Ltd.

[6] Rashmi, Ameeta Seehra "A Novel Approach for Preventing Black-Hole Attack in MANETs" (IJASA) Vol.2, No.3, September 2014.

[7] Sowmya K.S, Rakesh T. and Deepthi P Hudedagaddi "Detection and Prevention of Blackhole Attack in MANET Using ACO" IJCSNS International Journal of Computer Science and Network Security, VOL.12 No.5, May 2012.

[8] Gagandeep, Aashima, Pawan Kumar "Analysis of Different Security Attacks in MANETs on Protocol Stack A-Review" International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-1, Issue-5, June 2012.

[9] Harjeet Kaur , Manju Bala , Varsha Sahni "Study of Blackhole Attack Using Different Routing Protocols in MANET" International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering Vol. 2, Issue 7, July 2013.

[10] Fan-Hsun Tseng, Li-Der Chou, 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

[11] Irshad Ullah, and Shahzad Anwar, **"**Effects of Black Hole Attack on MANET Using Reactive and Proactive Protocols" IJCSI International Journal of Computer Science Issues, Vol. 10, Issue 3, No 1, May 2013.

[12] Shashi Gurung , Aditya Kumar , Dr. Krishan Kumar Saluja, "Detection of Black hole attack in Mobile ADHOC Networks" IJCNS Volume 3. 09 September 2013.