International Journal of Technical Innovation in Modern Engineering & Science (IJTIMES)
Impact Factor: 5.85 (SJIF-2019), e-ISSN: 2455-2585
Volume 6, Issue 1, January-2019

DETECTION, PREVENTION AND PERFORMANCE ANALYSIS AGAINST GRAY HOLE ATTACK IN MANET

Akshay Mishra[1] Anand Singh Rajput[2]
[1]M.Tech Scholar, Dept of Electronics & Communication Engineering, AITR, Bhopal
[2]Assistant Professor, Dept of Electronics & Communication Engineering, AITR, Bhopal
Dept of Electronics & Communication Engineering, Acropolis Institute of Technology and Research, Bhopal, India

ABSTRACT

Wireless ad hoc network is an amassment of mobile nodes & all nodes acquits as a router as well as host. By the cause of scarcity of a centralized management, mobility, threats from compromised nodes inside the network, dynamic topology, mobility, scalability MANET network become more unguarded & unprotected than that of a wired network which has a way more efficient & substantial security. Owing to this factor of foible & debilitated environment, As a MANET network is more susceptible to detrimental attacks & network hijacks committed by an immigrant invader. Therefore getting a security fix becomes remarkably oppressive & incommodious assignment in a MANET. Many different nodes exhibiting in the network fall in with diverse class of security hazards that can potentially divulge out the personal or any vital information of attackers concern & benefit. An intruder can exert & utilize a multitudes of means available at his disposal to name few of them are Gray hole attack, black hole attack, worm hole attack denial of service, Sybil attack, encryption & jamming as implements to gain access to crucial & cryptic information as well as can undermine the network intervened. Grayhole attack is one such kind of a dormant security threat which selectively drops the data packets in the network causing loss or theft of information. This thesis work, contemplate a probabilistic approach with IDS (Intrusion Detection System) which identify and tranquillize the grayhole attack effectively& efficiently. The simulation of the objective & propose approach is done in NS2.34 network simulator. The simulation environment is setup to simulate the algorithm in which an area of 900x900 is taken to transmit the data packets over TCP/FTP, UDP/CBR protocols. For the implementation & application Ad-hoc On-demand Distance Vector (AODV) routing protocol and 802.11 wireless channel models are utilized. This work, mainly & majorly focuses & concentrates on providing better security by consuming less energy & comparative testing, a thorough analysis is performed among the performance metrics such as Throughput, Packet Delivery Ratio and Routing load etc.

ABBRIEVIATION	**DESCRIPTION**
(MANET)	MOBILE AD-HOC NETWORK
(WRP)	WIRELESS ROUTING PROTOCOL
(DSDV)	DESTINATION SEQUENCED DISTANCE VECTOR
(OSLR)	OPTIMIZED LINK STATE ROUTING PROTOCOL
(AODV)	AD-HOC ON-DEMAND DISTANCE VECTOR
(DSR)	DYNAMIC SOURCE ROUTING PROTOCOL
(HRP)	HYBRID ROUTING PROTOCOL
(ZRP)	ZONE ROUTING PROTOCOL
(IDS)	INTRUSION DETECTION SYSTEM
(CBR)	CONSTANT BITRATE
(PDR)	PACKET DISTRIBUTION RATIO
(RREQ)	ROUTE REQUEST
(MPR)	MULTIPOINT RELAY
(TTL)	TIME TO LIVE
(TORA)	TEMPORAILY ORDERED ROUTING ALGORITHM
(IARP)	INTRAZONE ROUTING PROTOCOL
(IERP)	ITERZONE ROUTING PROTOCOL
(BRP)	BROADCAST ROUTING PROTOCOL

Keywords: *MANET, AODV, Ad-hoc Network, DSDV, PDR, Gray Hole, Sink Hole, Black Hole, Worm Hole, IDS.*

INTRODUCTION

In telecommunications industry wireless communications is the most progressive & fastest ever growing segment. As such, it has captured an acute & ample amount of attention of the media and people worldwide. A progressive & exponential growth in wireless network over wired-network worldwide is expeditiously succeeding antiquated wired networking systems in almost every possible field of communication. Highly useful in new applications, including a class of wireless sensor networks, Hi-End communication devices, industries, smart & connected homes and appliances & remote tele-medicine healthcare & every single field one can imagine. Wireless technology has become a new trendsetting standard of communication in recent few years & simultaneously continued to grow at an incredible rate. Due to the convenience, availability and economic cost of wireless hardware & other communication devices, there is an extravagant growth in wireless networking deployment and manufacturing of wireless networking hardware. The evolution of modern electronics on one side reduced the overall size of communication devices making them portable, handy & on another side advanced & feature packing personal computers, laptops, cellular devices, & healthcare devices has advanced the pace of utilization of wireless networks. Indeed, many technical challenges persist in designing a robust & reliable wireless networks capable of delivering optimum & peak performance essential to support & deploy emerging applications. Wireless ad hoc networking has turned into one of the most versatile, sophisticated & active fields of communication and networking research. Mobile ad hoc networks (MANETs) have many fantastically interesting future applications but the same also suffers from some of the very critical & crucial constraints & open problems to be solved & sorted out. MANET is the new emanating technology which facilitates in communication without any physical infrastructure to users regardless to their geographical location, due to this it is also called Infrastructure less network. It is abstain & economic, small and more powerful devices make MANET a fastest growing network. It is kind a self-organizing and adaptive network. All devices and their presence should be detected by Mobile ad hoc network devices and perform necessary set up to facilitate communication, services and data sharing. Wireless ad-hoc network allows devices to perpetuate their connections as well as easy to remove and add to the network and from the network. The traditional set of applications for MANETs are, too small, mobile, highly dynamic, diverse, and ranging from large-scale and static networks that are inhibited by power sources. Additionally in legacy applications of MANET, the traditional infrastructure environment moved into the ad hoc context. The prevailing applications of MANET got significantly intensified over the past years. Due to lack of centralized management, mobility, threats from compromised nodes inside the network, dynamic topology, mobility, scalability and security MANET become more vulnerable than wired network. Because of these vulnerabilities, MANET is more prone to pernicious attacks. Based on security threats MANET can be categorized in five layers, as Physical layer, Application layer, Network layer, Link layer, and Transport layer. However, to preserve the MANET routing protocols we only focus on network layer which it relates & deal to the security issues. Wired networks have dedicated & straight to the end routers but in an ad hoc network each mobile node may act as a router as well as forward data packets for other intermediate nodes. So in ad-hoc network have more security challenges than wired network. Security issues are the key challenge in mobile ad hoc network in which Gray Hole is marked as the most precarious attack.

LITERATURE REVIEW

RELATED WORK

Neha Sharma et al. [10] "Detection as well as Removal of Grayhole and Blackhole attacking MANET". In this paper proposed a technique for detection of the black-hole or malicious node. In this technique, a new procedure a kind of trap method is added in AODV protocol for the detection of malicious nodes. When the Black-hole node is detected after that an alarming method is triggered to make other nodes aware of malicious nodes. This method is work in two phase (a) Route Discovery (b) Monitoring phase. In Route Discovery phase this method uses trap RREQ for trap the malicious node and also uses promiscuous mode for monitoring malicious behavior of any node. In this method sender node first send the trap RREQ which contain destination address which does not exists in the network so when black hole node receive RREQ then they doesn't check own's routing table and immediately send reply to source node, after receiving the fake RREQ response sender node record the source of fake RREP and add it to his malicious list. This informs to all nodes then all nodes isolate the malicious node from his routing table. In Monitoring phase all the nodes work in promiscuous mode means all the nodes monitoring its neighboring nodes activities, if there is any malicious node left in the network, it does not forward data to next node so its forwarding ratio is decreased, if this ratio is less than threshold value the monitoring node immediately send alert message to source node then source node discard entry from routing table and send data through neighbor node.

Kavita, et. al. [11] "Removal of Gray Hole Attack Using Directional Based Credit Technique in MANET". This paper proposed a technique for detection and elimination of 14 grayhole attack in AODV routing protocol by Directional Credit Based Technique. The detection of grayhole attack depend on the credit value, this value continuously increases or decreases. The simulation results compared with compared with different parameters like Packet Delivery Fraction, End to End delay and Throughput, which analyze performance of each parameter.

Vaishali et. al. [15] **"**Gray Hole Attack Prevention and Elimination in Mobile Ad-Hoc Networks by Enhanced Multipath Approach". The Proposed algorithm, generate a number in between 0 to maximum number of nodes randomly and as gray hole attack is done by transmitter and receiver so have to decide the transmitter and receiver make the node with same number as transmitter node. Then generate the route with specified average route length from selected transmitting node to any destination node. After this according to selected destination it will send packet and start timer to count number of hop and delay. It will be required to store routes and their hops and delay, repeat the entire process. Now to detect malicious node; for a particular route if the hop count decline suddenly for average hop count then at least one node in the route present as an attacker. In this algorithm check the delay of all previous routes which involve any one attacker node in the suspicious route. The node not encounter previously should be malicious. Now to find out exact malicious node, the whole process need to be repeated if more than one node is misbehaving and that will take time and resources. So to avoid this situation, transmitter will be looking for help 15 from directly connected neighbors. Neighbors can tell the history of particular node under suspect. The node considered to be the malicious node which is not involved in any of the previous activity. Malicious nodes have been blacklisted by the nodes and hence they are not involved in future routes.

Deepali et. al. [16] "Prevention& Performance analysis of Gray Hole and Black Hole Attack in MANET", proposed a methodology which was discovered on a course based scheme. In which a node only observes the next hop node in existing route path it does not observe each neighbor node in the network. This approach represents the intentional selective dropping attack by a node and by examining the forwarded packets sent by the neighbor downstream node. When all the packets are dropped by any node it will detect as a black hole attack. If the overhear rate is less than the threshold value, the detecting node considered the next hop as a black or gray hole. Later, the detecting node would avoid sending packets through this attacker node.

Avenash et. al. [18] **"**Destination Based Group Grayhole Attack detection in MANET". This paper presents a technique for detection of group gray hole attack while more than one malicious node are present in MANET. The proposed work contains three steps:

1. Store the RREP packet on previous node.
2. Check 2 hop distance of a doubted node.
3. Refusal of RREP packet.

To identify the doubted node, the common neighbors of previous node and doubted node check the two hop distance node have ability to reach the destination. For this first it stores the RREP packet at previous node and attaches one hop distance of doubted n ode otherwise previous node will reject the RREP message.

Chundong et. al. [17] "Intrusion Detection System for Black Hole and Gray Hole Attack in MANETs". This paper proposed a path-based technique for detection on network layer attacks to overhear the next hop's action. This system proposed to saves the system resource and power for the detection of malicious nodes. In MAC layer to estimate dynamic detecting threshold a collision rate reporting system established to lower the false positive rate under high network overload. This used DSR protocol to test algorithm and NS-2 as a simulation tool. For implementation of the algorithm, every node should have a FwdPkt Buffer, which is a packet signature buffer. The algorithm is performed in three steps:

1) When a packet is transmitted, a signature is added into the FwdPkt Buffer and the watching node overhears.
2) The next hop node forward the packet is overheard and signature released from the Fwd Pkt Buffer.
3) The detecting node compute overhear rate of its next hop count in a fixed time period and compared with particular threshold value.

Overhear rate in the nth period of time can be defined as it is the ratio of Total overheard packer number to the Total sent packer number. 16

Sarita Choudhary et. al. [19] **"**Discovering a Secure Path in MANET by Avoiding Black/Gray Holes". In this paper proposed a complete protocol by using OPNET network simulator 14.5 for detection & removal of networking Black/Gray Holes; it is the newest version of simulation software. Proposed two different networks with 15 nodes and 35 nodes and evaluate a security attack against MANET. Packet loss rate, Packet delivery ratio, Average end to end delay has been used as different statistics or performance metrics.

Megha et. al. [20] "Grayhole Attack Detection & Prevention in Mobile Ad-hoc Network". To monitors the network or system activities for malicious actions, this paper proposed an intrusion detection system (IDS) and produces reports to a Management Station. This takes over the transmitting packets, if intermediate nodes try to transmit packets over attacker nodes, break the connection to destination node then find a route again and broadcasting Route Request (RREQ) messages. We changed the receive RREP function of the grayholeaodv.cc file to implement the gray hole attack but to implement the solution we had 17 to change the receive RREP and create RREP caching mechanism to count the second RREP message.

Chandure, Gaikwad et al. [21] "A Mechanism for detection & Eradication of Gray HoleAttack using Ad-hoc On Demand Vector routing protocol in MANET". In this paper developed a security based mechanism using some routing protocol to identify & eliminate the problem of grayhole attack in mobile ad-hoc network. In first phase developed the method to handle the malicious node. The next phase of protocol is develop to implement the gray hole attack so as to detect gray hole attack & find out its impact on the ad-hoc network. Once a node is identified to be truly malicious, this scheme uses a notification mechanism to all those nodes that are not yet suspected to be malicious for transferring messages, so that the malicious node can be cut off from path and not permitted to use any network resources.

J Paul, Vishnu K et al. [22] "Detection As well as Elimination of Cooperative Black & Grayhole attack in MANET". This paper has been proposed a method to detect and eliminate two types of attack i.e. Black hole and Grayhole attack. Originally a backbone network has been established by using trusted nodes over the ad-hoc network. Source node periodically request to any one of the backbone nodes for a restricted IP address.

Banerjee et al. [23] "Cooperative Gray and Black Hole Attack Detection and Removal in MANET". This paper proposed for the detection and removal of grayhole and black hole attack. In this paper a methodology in which the total traffic divided into small sized blocks instead of sending total data traffic. Thus in between sending of two such blocks malicious nodes can be detected and removed by ensuring an end-to-end checking.

Jyoti Jain et. al. [25] "Overview and Challenges of Routing Protocol and MAC Layerin Mobile Ad-Hoc Network". This paper describe the challenges occurred at MAC layer and Network layer in MANET. Also discussed the designing of MAC layer and routing protocols for Network layer.

Sushma B. et al. [35] "Monitoring & Recognition of Gray Hole Attacks in MANET to Achieve Minimum Packet Drop Rate". Proposed algorithm is to detect grayhole nodes and 18 removes the normal nodes with higher sequence number to enter in black list. Proposed approach dynamically calculates peak value like in DPRAODV, but it uses some more parameters than DPRAODV. Proposed Approach uses false reply, black list, and reputation concept.

Disha G. et al. [36] "Detection of Black and Gray Hole Attacks in Using an Adaptive Method". This paper proposed an adaptive method based on layer design for the detection of grayhole node in ad-hoc network and a collision rate reporting system to detect dynamic threshold value in MAC layer. This system save power and system resources and overhear next hop count action.

PROPOSED MEHTODOLOGY

Mobile Ad-hoc networking is very challenging field in wireless communication. There are number of researches has been developed and continuously increasing day by day. The research is very vast in this field. Due to infrastructure less network design, dynamic topology, open wireless medium, mobility, limited resources etc are the major problems occur in MANET, become vulnerable to various kind of attacks or mischief.

OBJECTIVE

Ad hoc networking in this era is a key part for wireless communication. Due to open or wireless medium it suffers from many security threads like black hole, gray hole, worm hole attack etc. That will loss the important information and degrades the network performance. Many researchers provide the solution for detection and prevention of security attacks in AODV routing protocol. Main objective of this thesis work is to provide reliable and efficient communication after detection and removal of grayhole attack and improve performance metrics as compared to existing method. Objectives of this thesis work are summarized as follow:

1) This research focus on analysis of grayhole attack in MANET and its consequences.
2) Analyzing the Route Discovery Process
3) Identification of Gray Hole attack.
4) Removal of Gray Hole node and remove the entire malicious nodes from the path through Intrusion Detection System.
5) Minimize number of packet dropped through malicious nodes.
6) Increase network performance with respects to packet delivery ratio, throughput etc.
7) Improve network Routing load.

PROPOSED WORK

In the proposed scheme use a probabilistic based rebroadcasting approach to keep away redundant packets and overdoing packets transmission. In probabilistic based scheme each node forwards the packets with probability *P* on receiving side at first time. When *P=1*, then it is indicating something happening wrong into the entire network. So as soon as node receiving RREQ (route request) packet, it retransmits with probability *Prt* and with probability (1-*Prt*) it disallows the packet acceptance. Retransmit RREQ packet occurs only once, which is identifies through sequence number. Source node set *Prt* is equal to 1, to initialize RREQ.

Additionally in proposed approach set IDS (Intrusion Detection System) node that observe the neighboring nodes. Furthermore if IDS gets any discarded activity in close proximity range, it continuously observe the malicious node that receive but not forward packet, consequently that node set as attacker and it gets to be blocked. Also an additional mania is that if several nodes continues throwing the routing packet to the particular node, then it will also treated as attacker node, then it will be also blocked into entire network. However the successfully blocking of nodes changes the entire route moreover starts sending data to the destination node. During the transmission of packets, also observe the performance of PDR, if it gets decreases at any time moment then it should be go to the observation period until not identified the reason of that.

PROPOSED ALGORITHM

For the simulation of our proposed methodology on Network Simulator-2 consider variables as Total number of mobile nodes, sender node, receiver node, grayhole node, simulation time, radio range etc.

Set mobile node	=	node //Total Mobile Nodes
Set Sender node	=	S//S GrhlNd
Set Receiver Node	=	R//R GrhlNd
Set Routing Protocol	=	AODV
Start simulation time =	=	t_0
Set radio range	=	rr//initialize radio range

To initialize RREQ in AODV set variables as probability Prt, Sender node S, Receiver node R, Radio Range rr.

AODV-RREQ_B (Prt, S, R, rr)

Check there is need for retransmit packet or not. If IRet (i) = 0, it means node doesn’t accept the retransmit Request.

For the simulation choose 550 meter radio range for the communication.

If those nodes exits out of this range, cannot be communicated with them and Destination is unreachable.

To transmit the packets from source to destination generate packets sequence numbers. Each packet has a particular sequence number and transmitted randomly as in the form of $2pn^i+i$ where “i” is a fixed constant i = 0, 1, 2, 3………so on

```
{
        If IRet (i) = 0 Then
        {
                //Node is not authorized for retransmitting request for while Set IRet (i) = 0;
                If (rr>550 &&S! = true)
                        Destination is unreachable
        }
        Pkt_rndno= rnd()
        {
        Generate random sequence number as $2pn^i+i$ // pn = packet number, i is a fixed constant
}
```

For the route discovery process each node maintain its routing table in which exist the information about total number of hop count, next hope sequence number, source and destination IP addresses and their sequence numbers.

Initially for finding route source node broadcast the RREQ message to nearest node to establish connection from source to destination and forwarded hop by hop until it reaches to the destination node. If the current node is destination node send acknowledgement to source node to permit the route setup then data can be send through this route. If destination is unreachable change the packet sequence number.

```
TravesreRoute ()
        {
         rtable->insert(rtable->rt_nexthop); // nexthop to RREQ source
         rtable1->insert(rtable1->rt_nexthop); // nexthop to RREQ destination
        if (dest==true)
            {
        Send ack to source node with rtable1;
        Data_packet_send (s_no, nexthop, type)
            }
            Else
            {
       Destination node is unreachable;
       Pkt_rndno= rnd()  //change packet sequence no

            }
        }
```

If the Retransmission Probability *Prt* is greater than or equal to the *1-Prt*, it retransmit the route request again and set IRet (i) = 1. Then again send route request RREQ from source, update its routing table and update the node retransmission index.

If the retransmission Probability is less than the1-*Prt*, no need to retransmit the route request and drop the current packet.

```
    If (1-Prt<=Prt)
    Then Retransmit request again
And
Set IRet (i) = 1;
    {
    rtable->insert(rtable->rt_nexthop); // nexthop to RREQ source
    rtable1->insert(rtable1->rt_nexthop); // nexthop to RREQ destination //Update routing table also Update
    the node retransmission index IRet (i) by 1
     }
Else
Drop the current pkt
    End if
End if
}
```

Check the any suspicious activity occurs in the route; detect any gray hole present in the route.

For this continuously check the packet delivery ratio (PDR) of path, total broadcast messages and total received messages.

Calculate time between message sent time and message received time, count total send messages. If PDR < 80 then this is not our acceptable limit and black that node and RREQ.

If PDR > 80 and increasing continuously means there is a valid path for communication and nodes accepts the packets.

If PDR decreasing from this limit again route discovery process will starts for valid path.

```
RREQ_Limit_Check (S, R, BlcNd)
    {
        If   PDR < 80
        {
            Node is blacklisted node
RREQ_Blocked()
        }
ElseIF ((node € BlcNd) && (incoming = listening&& outgoing ==true))
      {
        RREQ accepted by neighbor node;
        Calculate PDR =∑ no of packet receive / ∑no of packet sent
      }
RREQ_Blocked()
         {Can't accept by neighbor;
Blocked RREQ by sender;
   PDR = 0.0;
         }
    If (PDR>80.00) //and increasing continuously
        {
      Valid path
    And accepts packets
        }
```

```
                    Else
{
Start Discovery of new path
}
            }
                }
```

IMPLEMENTATION RESULTS

RESULT ANALYSIS

In this thesis report performance analysis of the proposed methodology are done by using some parameters such as Packet Delivery Ratio (PDR), Throughput and Routing Load (RL).

Packet Delivery Ratio Analysis

Packet delivery ratio is the fraction of total number of data packets received by the destinations to the data packets generated by the sources the impact on packet delivery ratio with increment in simulation time runs according to source. The PDR performance comparison of normal AODV, AODV with Gray Hole attack and AODV with IDS is showing in the graph. 200 seconds has taken simulation time for implementation. X axis is used for plotting the Simulation time and taken 10 second time difference on this axis. Y axis is used for plotting PDR in graph. Blue line is showing the variation in PDF in normal AODV protocol with respect to simulation time, red line is showing variation in PDF in AODV with grayhole attack and green line is showing the variation in PDF in AODV with IDS with Simulation time.

Here normal AODV protocol has high throughput then AODV with gray hole attack because it provide secure path for data transmission and there is no disturbance in the normal operation of network. Proposed AODV having higher throughput than other existing method, it detect gray hole attack in the path by IDS and after blocking this attacker node providing secure route for transmission. In the PDR analysis it has found that the proposed work gives best results.

Throughput Analysis

Throughput is defined as the ratio of number of data packets received by destination node coming from source node to the destination node takes time to get last packet. It is also defined as average rate of successful message delivery over a communication channel the impact on Throughput with increment in simulation time. The throughput performance comparison of normal AODV, AODV with Gray Hole attack and AODV with IDS is showing in the graph. 200 seconds has taken simulation time for implementation. X axis is used for plotting the Simulation time and taken 20 second time difference on this axis. Y axis is used for plotting throughput in graph. Blue line is showing the variation in throughput in normal AODV protocol with respect to simulation time, red line is showing variation in throughput in AODV with grayhole attack and green line is showing the variation in throughput in AODV with IDS with Simulation time.

Here normal AODV protocol has high PDF then AODV with gray hole attack because it provide secure path for data transmission and there is no disturbance in the normal operation of network. Proposed AODV having higher throughput than other existing method, it detect gray hole attack in the path by IDS and after blocking this attacker node providing secure route for transmission. In the throughput analysis it has found that the proposed work gives best results.

Routing Load Analysis

Routing Load is the number of routing packets transmitted per data packet delivered at the destination. Also each forwarded packet is counted as one transmission shows the impact on Routing Load with increment in simulation time. The normalized routing load of the existing and proposed methodology differs as we increase the simulation time. Graph showing the routing load comparison between existing work and proposed methodology. Blue line is showing the variation in routing load in normal AODV protocol with respect to simulation time, red line is showing variation in routing load in AODV with grayhole attack and green line is showing the variation in routing load in AODV with IDS with Simulation time.

Here, AODV protocol seeing by blue color in the graph shows maximum routing load but in case of AODV with grayhole attack routing load is minimum and routing of packets minimum this is major drawback of this because malicious node can't transmit routing packets in network. Thus flooding of routing packets becomes low. But after adding IDS Module shown in proposed graph gives better results than AODV with attack, it recover routing flooding scheme.

CONCLUSION

Security issues are major challenging task in wireless ad hoc network. It has been seen at the time of designing of routing protocols by the researcher for ad-hoc networks. Ad-hoc routing protocol is highly vulnerable to various attacks including Gray hole and Black hole attacks. The main goal of proposed work to show the performance of AODV under normal surroundings, under gray hole attack and performance after elimination of gray hole attack in term of Packet Delivery Ratio, throughput and Routing load. In this thesis work it has been studied and investigates certain existing detection and prevention solutions for these attacks and proposed a probabilistic based approach and Intrusion Detection System to overcome Grayhole attack in MANET so that efficiently discover safe and short path to the destination. The result and experimental analysis show that in proposed approach there is greatly increment in PDR and throughput with negligible difference in routing load. Concepth as shown improved results after elimination of the gray-hole attack in the simulation.

Result analysis showing that Packet delivery ratio of Proposed work (AODV with IDS) increased by 20% approximately than AODV with grayhole attack and by 10% than Normal AODV. Throughput of proposed work increased by 1000 kbps as compares to AODV with grayhole attack and 100 kbps as compares to Normal AODV. Routing load of proposed work decreased by 5kbps as compare to Normal AODV and minor difference with respect to AODV with grayhole attack.

REFERENCES

[1] Nishu Garg, R.P. Mahapatra, "MANET Security Issues", IJCSNS International Journal of Computer Science and Network Security, VOL.9 No.8, August 2009.

[2] Rashid HafeezKhokhar, MdAsriNgadi&Satria Mandala, "A Review of Current Routing Attacks in Mobile Ad Hoc Networks", International Journal of Computer Science and Security, volume (2) issue (3) 2008.

[3] Priyanka Goyal, Sahil Batra, Ajit Singh "A Literature Review of Security Attack in Mobile Ad-hoc Networks", International Journal of Computer Applications (0975 – 8887) Volume 9– No.12, November 2010

[4] KavitaTaneja, R.B.Patel "An Overview of Mobile Ad hoc Networks: Challenges and Future", 14 July 2015.

[5] T. S. Rappaport, "Wireless Communication: Principles and Practice", Prentice-Hall, 1996

[6] RatulDey, HimadriNathSaha, "Secure Routing Protocols for Mobile Ad-Hoc Network (MANETs)–A Review", International Journal of Emerging Trends & Technology in Computer Science (IJETTCS) Volume 5, Issue 1, January - February 2016.

[7] 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.

[8] C. Siva Ram Murthy, B. S. Manoj, "Ad-hoc Wireless Network Architecture and Protocols", 2nd ed, Pearson Education, 2005.

[9] Aarti, Dr. S.S. Tyagi "Study of MANET: Characteristics, Challenges, Application and Security Attacks", International Journal of Advanced Research in Computer Science and Software EngineeringVolume 3, Issue 5, May 2013.

[10] Neha Sharma, Anand Singh Bisen "Detection As Well As Removal Of Black hole And Gray hole Attack In MANET", International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT) 2016.

[11] Kavita Rani, Aarti "Elimination of Gray Hole Attack Using Directional Based Credit Technique in MANET", International Journal of Engineering Science and Computing, June 2016.

[12] Sweta Dixit, Priya Pathak, Sandeep Gupta "A Novel Approch For Gray hole And Black hole Detection And Prevention", Symposium on colossal Data Analysis and Networking (CDAN) IEEE,2016.

[13] Swati Pokhariyal, Pradeep Kumar "A Novel Scheme for Detection and Elimination of Blackhole/Grayhole Attack in Manets", International Journal of Computer Science and Mobile ComputingVol.3 Issue.12, December- 2014.

[14] Joshi Shraddha, Dipak kumar, Ashish Kumar Srivatava , Sunil K.Vithlani "Simulation Based tudy of Gray Hole Attack in MANET", International Conference on Computing for Sustainable Global Development (INDIACom) IEEE,2016.

[15] Vaishali Mittal "Prevention and Elimination of Gray Hole Attack in Mobile Ad-Hoc Networks by Enhanced Multipath Approach", International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 4 Issue 5, May 2015.

[16] Deepali Raut, Kapil Hande "Performance analysis and Prevention of Gray Hole and Black Hole Attack in MANET", International Journal of Advanced Research in Computer Science and Software Engineering Volume 4, Issue 7, July 2014.

[17] Chundong She, Ping Yi, Junfeng Wang, Hongshen Yang "Intrusion Detection for Black Hole and Gray Hole in MANETs", KSII Transaction on Internet and Information System VOL.7, NO. 7, Jul. 2013.

[18] Avenash Kumar , Meenu Chawla "Destination based group Gray hole attack detection in MANET through AODV", IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 4, No 1, July 2012.

[19] Sarita Choudhary, Kriti Sachdeva "Discovering a Secure Path in MANET by Avoiding Black/Gray Holes", International Journal of Recent Technology and Engineering (IJRTE), Volume-1, Issue-3, August 2012.

[20] Megha Arya, Yogendra Kumar Jain "Grayhole Attack and Prevention in Mobile Adhoc Network", International Journal of Computer Applications Volume 27– No.10, August 2011.

[21] Onkar V., Chandure,V. T. Gaikwad "A Mechanism for Recognition & Eradication of Gray Hole Attack using AODV routing protocol in MANET", (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 2 (6), 2011.

[22] Vishnu K, Amos J Paul "Detection and Removal of Cooperative Black/Gray hole attack in Mobile AdHoc Networks", International Journal of Computer Applications Volume -1 2010 .

[23] Sukla Banerjee "Detection/Removal of Cooperative Black and Gray Hole Attack in Mobile Ad-Hoc Networks", Proceedings of the World Congress on Engineering and Computer Science 2008.

[24] Robinpreet Kaur, Mritunjay Kumar Rai "A Novel Review on Routing Protocols in MANETs", Undergraduate Academic Research Journal (UARJ), ISSN: 2278 – 1129, Volume-1, Issue-1, 2012.

[25] Jyoti Jain, Mehajabeen Fatima, Dr. Roopam Gupta, Dr. K. Bandhopadhyay "OVERVIEW AND CHALLENGES OF ROUTING PROTOCOL AND MAC LAYER IN MOBILE AD-HOC NETWORK", Journal of Theoretical and Applied Information Technology 2005 - 2009 JATIT.

[26] Harjeet Kaur, VarshaSahni, Manju Bala "A Survey of Reactive, Proactive and Hybrid Routing Protocols in MANET: A Review", (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 4 (3), 2013.

[27] Sudhir Agrawal, Sanjeev Jain, Sanjeev Sharma "A Survey of Routing Attacks and Security Measures in Mobile Ad-Hoc Networks", JOURNAL OF COMPUTING, VOLUME 3, ISSUE 1, JANUARY 2011.

[28] Charles E. Perkins "Ad hoc Networking", Addison-Wedey, 2001.

[29] RatulDey ,HimadriNathSaha "Different Routing Threats and its Mitigations Schemes for Mobile ad-hoc Networks (MANETs) – A Review", (IPASJ) International Journal of Electronics & Communication (IIJEC)Volume 4, Issue 3, March 2016.

[30] S. BanuPriya, C.Theebendra “A Study on Security Challenges in Mobile Adhoc Networks”, International Journal of Research in Computer Applications And Robotics Vol.4 Issue 2, February 2016

[31] Priyanka Goyal, SahilBatra, Ajit Singh “A Literature Review of Security Attack in Mobile Ad-hoc Networks”, International Journal of Applications Volume 9-No. 12 November 2010.

[32] G.V.S. Raju and G. Hernandez, “Routing in Ad hoc networks”, IEEE–SMC International Conference, October 2002.

[33] Xin Yu, "Distributed Cache Updating for the Dynamic Source Routing Protocol," IEEE Transactions on Mobile Computing, vol. 5, Jun.2006.

[34] M. K. Marina, S. R. Das “Routing performance in the Presence of Unidirectional Links in Multi-hop Wireless Networks”, 3rd ACM International Symposium on Mobile Ad Hoc Networking and Computing (MOBIHOC), Jun. 2002.

[35] Sushma B. Akhade, S.M Jagade “Monitoring and Detection of Gray Hole Attacks in Manet to Achive Minimum Packet Drop Rate”, GJRA-GLOBAL JOURNAL FOR RESEARCH ANALYSIS Volume-4, Issue-5, May 2015.

[36] Disha G. Kariya, Atul B. Kathole, Sapna R. Heda “Detecting Black and Gray Hole Attacks in Mobile Ad Hoc Network Using an Adaptive Method”**,** International Journal of Emerging Technology and Advanced Engineering ISSN 2250-2459, Volume 2, Issue 1, January 2012.

[37] N. Drakos and R. Moore, ns2 - The Manual (formerly Notes and Documentation), 1999 [Online]. Available: http://www.isi.edu/nsnam/ns/doc.

[38] NS-2 tutorial, http://www.isi.edu/nsnam/ns/tutorial/index.html