A Secure Framework for Detecting and Preventing Grayhole Attack (SFAODV)

Asif Uddin Khan[#1], Bikram Kesari Ratha[*2]

[#] *Dept of Computer science, Utkal University*
VaniVihar, Bhubaneswar, India

Abstract *— Mobile Ad-hoc Network (MANET) is a network where nodes cooperate each other to communicate data through multi-hop nodes. It has numerous applications in the current and future networking generations. Due to the popularity of Internet of Things (IOT), where everything can be connected, there is a vital role of MANET in communicating among the IOT devices to exchange information. However providing QOS in terms of security to this network is an important issue. In this paper we investigate grayhole attack in MANET and do analysis with ns2 experimental results and show how the performance degradation of the MANET occurs due to such attack. We then propose a scheme to detect and prevent grayhole attacks in various scenarios. We propose a secure routing framework based on elliptic curve cryptography digital signature algorithm (ECDSA) which can detect and prevent the grayhole attacks with improved performance. We take (Ad-hoc On Demand Distance Vector routing) AODV protocol for implementing our scheme and evaluating performance taking various performance metrics such as packet delivery ratio and throughput to show that our scheme resolve the grayhole attack with better performance.*

Keywords — *quality of service, digital signature, MANET, ECC, IOT, routing protocols, security.*

I. INTRODUCTION

Mobile Ad-hoc Network (MANET) is a self configuring multi-hop radio network in which each node act as source as well as router means node helps each other in forwarding data which is not meant for it. Due to its quick and cheap deployment with no prerequisite of infrastructure, it is useful in many real life situations from military crisis operations and emergency preparedness and response to civilian, such as search and rescue missions, data collection, battle field and virtual classroom and conferences [1] [2].presently MANET and WSN is also integrated in various other networks such as VANET [3] and Internet of Things (IOT) [4]. Due to the salient differentiating features like open medium, limited energy, dynamic changing topology, no centralized Supervision, no strict boundary, and wireless links of MANET it is more vulnerable to attacks than wired network. In the current era of communication security is the prime concern in order to achieve quality of service (QOS). Most of the routing protocols designed such as AODV [5], DSDV [6], OLSR [7], DSR [8], and TORA [9] is with the assumption that all users in network would be trusted and will work in collaborated mode. But the basic function of the network like communication can easily be jeopardized at all layers specially at network layer if counter measures have not been embedded into the early design of the system. This, in turn, led to the current situation where these protocols are vulnerable to a multitude of attacks, including spoofing attacks [10], flooding attacks [11], wormhole attacks [12], replay attacks [13], [11], black-hole and grayhole attacks [14], colluding mis-relay attacks [15], and many others. In this paper we survey and investigate the grayhole attack of MANET using AODV protocol. We analyze the attack using the case study example and ns2 simulation results and propose a secured framework to detect and prevent the attack in order to achieve QOS. In this paper we simulate our proposed framework protocol with grayhole attack and compare with normal AODV protocol without and with blackhole attack .We use ns2.35 simulator for simulating the proposed framework for various scenarios and do extensive analysis and show that the proposed scheme resolves the problem of grayhole attack and achieves better QOS in terms of increased packet delivery ratio and throughput.

The organization of the paper is as follows

In sectin-II we discuss background concepts. In section-III we explain the grayhole attack problem using case study. In section-IV we discuss the related work. In section-V we discuss the mathematical background used in this paper. In section-VI we propose our secure framework for detection and prevention of grayhole attacks. In section-VII we do performance analysis and finally in section-VIII we conclude the paper.

II. BACKGROUND CONCEPTS

In this paper we use AODV routing protocol for showing the grayhole attack, so in this section we discuss the working principle of AODV [5]. This

protocol maintains routing table at each node in the network. This protocol has different phases such as path discovery, reverse path setup, forward path setup, route table management, path maintenance, and local connectivity management. All the phases of our proposed method is same as AODV with some modification in path discovery, reverse path setup, forward path setup. In this section we explain the details of these phases of AODV protocol.

.

A. OVERVIEW OF AODV PROTOCOL

Whenever any source node has some data to communicate with any other node for which it has no routing path information in its routing table, it broadcasts Route Request (RREQ) packet to all its neighbors as shown in fig-1. Each node maintains two counters such as a node sequence number and a broadcast id.

The RREQ contains the following.

<*source_address, source_sequence_no, broadcast_id, destination_address, destination_sequence_no, hop_count* >

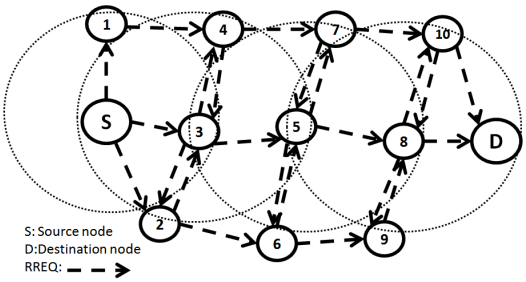

Fig-1: RREQ broadcast of AODV

The pair (source_address, broadcast_id) uniquely differentiates the RREQs from each other.Broadcast_id is incremented each time the source broadcasts a new RREQ.Each neighbor sends Route Reply (RREP) back to the source node if it has a fresh path to that destination otherwise rebroadcasts the RREQ to its neighbors after increasing the hop_count. When an intermediate node receives a redundant RREQ from its neighbors it drops that and does not rebroadcast it.During rebroadcast each intermediate node keeps track of information such as Destination_address, Source_address, Broadcast_id, Expiration time for reverse path route entry and source node's sequence number which are required in the reverse path setup and forward path setup.

Reverse path setup

The source node knows source sequence number and the destination's last sequence number included in the RREQ.Source_sequence number is used to maintain the freshness of the reverse route to the source and destination sequence number is used to maintain the freshness of the route to the destination node.When the RREQ travels to different destination nodes, it automatically sets up the reverse path back to the source as shown in the fig-2.To setup the reverse path nodes record the address of their neighbors from which they receive the first copy of the RREQ packet. The reverse path route entries are maintained in the table for enough time which is required for the RREQ to traverse the network and produce a reply back to the sender.

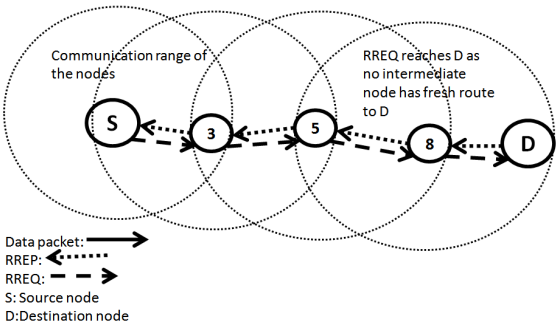

Fig-2: Reverse path formation of AODV

Forward path setup

When the RREQ packet reaches the destination node or the node which has the route information to the destination, checks that the RREQ received through a bidirectional link or not. If an intermediate node has route information for the desired destination, it checks whether the route is fresh or not by comparing the destination sequence number in its own record and the destination sequence number in the RREQ packet. If the destination's sequence number of RREQ is greater than the intermediate node's stored sequence number then it is assumed that the saved route information to the desired destination is not fresh and the intermediate node rebroadcasts the RREQ packet. If the destination sequence number of the RREQ packet is less than or equal to the saved one, it is considered that the intermediate node has fresh route to the desired destination. If the RREQ has not processed previously the intermediate node sends back the route information as RREP to the neighbor node from which it has received the RREQ. The RREP packet contains following information.

< source_address, destination_address, destination_sequence_no, hop_count, lifetime >

When the RREP travels back to the source node, each node along the path sets up a forward pointer to the node from which RREP came, updates its timeout information for the route to the source and destination and stores the latest destination sequence number for the requested destination.Fig-3 shows how RREP is unicasted by the intermediate node to

the source node which generated RREQ packet and forward path setup from source node to the destination.

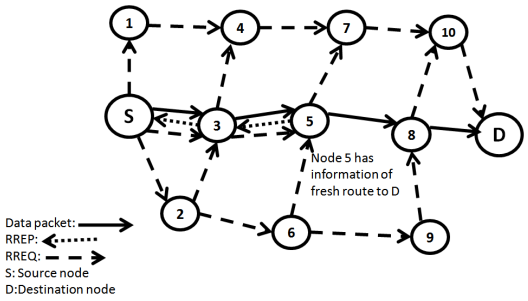

Fig-3: Forward path formation from intermediate node

If there no intermediate node has a fresh route information to the desired destination, the RREQ packet ultimately reaches the destination node. The destination node increments its sequence number and unicasts the RREP back to the source node through the node from which it has received the RREQ packet and same process is repeated as intermediate node. Fig-4 illustrates the forward path setup as RREP is traversed from destination node D to source node S.

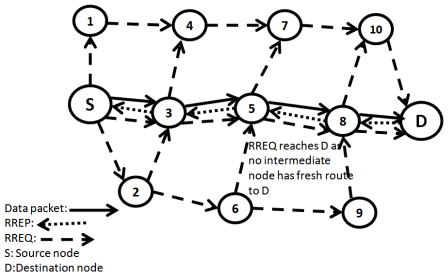

Fig-4: Forward path formation from destination node D

A node receiving RREP propagates the first RREP for a given source towards that source. If it receives further RREPs, it updates its routing information and propagates the RREP only if the RREP contains either greater or same sequence number as the previous RREP with smaller hop count. It drops all other RREPs propagating towards the source node while also ensuring the most updated and quickest routing information. The source node can begin data transmission as soon as the first RREP is received and can later update its routing information if it learns a better route.

III. Grayhole Attack Problem Description

Grayhole attack is another form of Blackhole attack [14] in which the nature of malicious node is highly unpredictable. The malicious node behaves as a genuine and legitimate node for some time and behaves as a malicious node for other times. We can say that the grayhole attack acts as a slow poison because the probability of packet loss cannot be determined perfectly as the malicious node drops the packets secretly for some period of time and acts as a legitimate node for all other time [16].

A. Case study: Grayhole Attack

As shown in Fig-5, the malicious node M behaves as a legitimate genuine node and forwards all the control as well as data packets that are destined for the destination. In fig-6 the node M is behaving maliciously. It behaves as a genuine node during the route discovery phase and starts to drop the data packets. Thus the behavior of the malicious node i.e. the grayhole node cannot be predicted. In some cases, the grayhole node may forward the packets from some node while it may drop packets of some other nodes [17]. Thus such type of attack is very vulnerable for the network and may affect the performance of the network.

In the following example in fig-5 and fig-6, there are 12 nodes, one source node represented by 'S', one destination node represented by 'D', grayhole node represented by 'G' and rest are normal nodes. All the nodes use AODV protocol for routing packets. The grayhole node is in the path from S to D. In fig-5 'G' forwards the data packets to the next node 5 in the path from S to D from time T1 to Ti as a normal node. In fig-6, we can see that the grayhole node G drops data packets from time T_i to T_{i+k}.

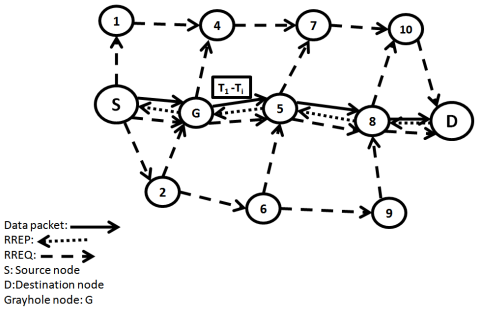

Fig-5: grayhole attacker forwarding packets from time *T1* to *Ti*

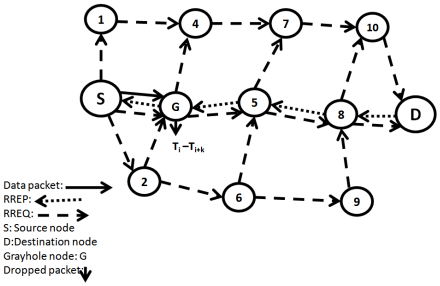

Fig-6: Grayhole attacker *'G'* dropping packets at times from *Ti* to *Ti+k*

IV. Related Work

In [18][19] Rutvi Jhavery proposed a scheme in which the nodes receiving RREP calculates a peak value. This peak value is the maximum value that a sequence number can have. The node receiving the RREP compares the sequence number in the RREP packet with the calculated peak value. If the sequence number is greater than the peak value than the RREP is considered to be fraudulent and is marked as Do Not Consider RREP and the node sending that RREP packet is considered to be malicious. The intermediate node then sends all the RREP's to source node. The source node then discards all Do Not Consider RREP's and selects any one genuine RREP. In this approach, it is observed that if a malicious node sends the sequence number within the range of peak value than it becomes difficult to detect the grayhole node.

In [20] Authors gave a scheme which use a table known as extended data routing information table which is maintained by every node. This table contains the history of all the packets sent and received to or from any neighboring nodes. The EDRI entries of both neighboring nodes and neighbour of neighbour are compared by the source node. If both table entries match then it is confirmed that there is no malicious node otherwise malicious node is present. This approach requires extra control packets to communicate with neighbors of neighbor node, every node has to frequently check EDRI tables which results more delay and also extra control packets as overhead.

In [21] [22] Authors propose a method which uses three different algorithms which are interrelated. Creating proof algorithm, Check up algorithm and Diagnosis algorithm. This method uses a hash function for detecting malicious node. In this method it is observed that all malicious nodes are not detected.

In [23] Authors use a correspondent node and probe packet such that when Intermediate node(IN) wants to detect malicious node, it first appoints the node known as correspondent node(CN) which is found to be most loyal on the basis of the DRI entry. Then RREQ is sent to all neighbors requesting route to CN. This node will receive many RREPs. Then it sends a probe packet .If CN replies affirmatively then it is confirmed that there is no malicious node, but if CN replies negatively then the node which did not forward the probe packet is considered as malicious and its suspicious value is increased. In this method the transmission overhead increases because of more probe packets between neighbors.

In [24] authors proposed a scheme which uses Restricted IP where source node sends a request to Backbone network for unused Restricted IP. When source node receives the Restricted IP ,it sends the control message to all nodes in the route for entering into promiscuous mode. In promiscuous mode all nodes monitor their neighbors for the packets sent or received from Restricted IP. By using help from monitoring nodes the malicious node is detected. In this approach it is difficult to detect malicious nodes which do not use restricted nodes.

In [25] authors proposed a method named as destination based detection method where a node receiving the RREP packet sends the Request FREQ to common neighbors of the suspected node and the previous node. When source node receives FREP it sends the FREQ to the destination through the route where there is no one hot nodes of suspected node. If the destination node has a path to intermediate node then RREP is generated otherwise FREP and RREP are discarded and alarm signal is generated. In this method requirement of common neighbor is mandatory for detecting malicious nodes.

[26] Proposed a scheme where the messages known as prelude and postlude are used to detect malicious nodes. In this approach total data is divided into blocks. Before sending data packets source node sends prelude message which is used to alert the destination about the transmission of data blocks. A timer is started by destination and it receives the data packets until timer expires. After the expiration of the times it sends postlude message to the source node about the number of packets received. If the received packets and sent packets are same or their difference is under a tolerable threshold then it transmits the next block otherwise grayhole detection mechanism is used where all the monitoring nodes work together and detect malicious node in the network. In this method there is delay between because of prelude and postlude messages.

In [27] authors proposed a method of storing all the RREP's received in the Request Reply table. Then investigating all the entries in the table. If the Destination Sequence number is much higher than the Source Sequence number then remove that entry form the table and note down the node entry of that node. Sort all the entries in the table according to the destination sequence number and select the node which is on the top of the list. In this way all the malicious nodes are removed and only genuine nodes are left in the request reply table. In this approach it is observed that the average end to end delay increases as node has to wait for multiple RREP's to arrive until a particular timeout.

In [28] authors gave a method known as Course Based Detection Method in which the node keeps its entire focus on the neighboring node that is involved in the route. It does not monitor all the neighbors. Source node forwards the packet to the neighboring node in the route and also maintains copy of packet in a buffer named FwdPacketBuffer. It then overhears the neighboring node. When the neighboring node forwards the packet forward, it deletes the copy from the FwdPacketBuffer. Source node computes the Overhear rate which is the percentage of data packets actually received by the

destination. If the overhear rate goes beyond threshold then that node is considered malicious. In this method, if constant threshold is used for high overload network, then it produces a very high false positive probability.

In [29] authors proposed a method of peak value calculation where the intermediate node, on receiving the RREP packet compares the destination sequence number and the calculated peak value. If the destination sequence number is greater than the peak value then that RREP is discarded by the intermediate node. In this approach, the source node will receive all the genuine RREP's because all the RREP's from malicious nodes will be discarded by the intermediate nodes.

In [30] Schweitzer, Nadav, et al, proposed a method for minimizing the grayhole DoS attack. They used OLSR protocol for analysis of grayhole attack. Their solution assumes no explicit node collaboration, with each node using only internal knowledge gained by routine routing information. The technique was evaluated using 5 different threat models (different attacker capabilities), allowing for a better understanding of the attack surface and its prevention.

V. Mathematical Background

To solve the problem of grayhole attack in MANET in this section we propose a secure framework to detect and prevent the above attack in an efficient way. We use modified Elliptic curve cryptographic digital signature (ECC) [31], [32], [33] algorithm in our security framework.

Basics of Elliptic curve cryptography (ECC)

A. Elliptic curve over finite field

Let a and b $\in Z_p$ where $Z_p = \{0,1,2,..., P-1\}$; and P > 3 is a large prime such that $4a^3+27b^2 \neq 0 \ (mod\ p)$.A non singular elliptic curve $y^2 = x^3+ax+b$ over finite field *GF(p)* is the set $E_p(a, b)$ of solutions $(x, y) \in Z_p \times Z_p$ to the congruence $y^2 = x^3+ax+b \ (mod\ p)$ where *a* and *b* $\in Z_p$ are constants such that $4a^3+27b^2 \neq 0 \ (mod\ p)$, together with a special point O called the point at infinity or zero point. The condition $4a3+27b^2 \neq 0 \ (mod\ p)$ is the necessary and sufficient condition to ensure that the equation $y^2 = x^3+ax+b$ has a non-singular solution [34]. If $4a^3+27b^2 = 0 \ (mod\ p)$, then the corresponding elliptic curve is a singular elliptic curve.

If $P = (x_P, y_P)$ and $Q = (x_Q, y_Q)$ be points in *E(a,b)*, then $P+Q = O$ implies that $x_Q = x_P$, and $y_Q = -x_Q$. Also elliptic curve *Ep(a,b)* over *Zp* has roughly p points on it. More precisely a well known theorem due to Hasse asserts that the number of points on $E_p(a,b)$, which is denoted by *#E*, satisfies the following inequality[35]:

$$P + 1 - 2\sqrt{P} \leq \#E \leq P + 1 + 2\sqrt{P}$$

In addition, $E_p(a,b)$ forms an abelian group or commutative group under *P* operation.

B. *Addition of points on Elliptic curve over finite field*

The following parameters about the proposed scheme over the elliptic curve domain are required.

We take an elliptic curve over a finite field GF (p) as $E_p(a,b) : y2 = x^3+ax+b \ (mod\ p)$, where *a* and *b* ε *GF (p)*. The field size p is considered as a large prime. We take G as the base point on $E_p(a,b)$ whose order is n, that is $nG = G + G + \ldots + G$ *(n times) = O (mod p).*

The elliptic curve addition differs from the general addition. Let $P = (x1, y1)$ and $Q = (x2, y2)$ be two points on elliptic curve $y^2 = x^3 + ax + b \ (mod\ p)$, with $P \neq -Q$, then $R = (x3, y3) = P + Q$ is computed as follows:

$x3 = (\lambda 2 - x1 - x2)(mod\ p)$, $y3 = (\lambda (x1 - x3) - y1) (mod\ p)$,

$$Where \quad \lambda = \begin{cases} \frac{y2-y1}{x2-x1} \ (mod\ p), & if\ P \neq Q \\ \frac{3x1^2+a}{2y1} \ (mod\ p), & if\ P = Q \end{cases}$$

In elliptic curve cryptography, multiplication is defined as repeated additions. For example,

if $P \in E_p(a, b)$ then, *5P is computed as P + P + p + P + P (mod p).*

C. *Elliptic Curve discrete logarithm problem*

Let $E_p(a, b)$ be an elliptic curve modulo prime p. Given two points $P \in E_p(a, b)$ and $Q = KP \in E_p(a, b)$, for some positive integer *K*. *Q = KP* represents the point P on elliptic curve $E_p(a, b)$ is added to itself K times. The elliptic curve discrete logarithm problem *(ECDLP)* is to determine *K*, given *P* and *Q*. It is reltively easy to calculate *Q* given *K* and *P*, but it is computationally infeasible to determine *K* given *Q* and *P*, when the prime *P* is very large.

VI. Security Framework for Detection and Prevention of Grayhole Attack

Grayhole attack is more harmful than blackhole attack [14], because detection of grayhole attack is difficult as the malicious node does not always drop the packets rather it drops the packets sometimes secretly and acts as normal legitimate

node other times. In order to detect and prevent grayhole attack we use acknowledgement packet 'm_ack' with modified ECDSA algorithm.

While sending data packets source node sends a dummy acknowledgement packet that is m_ack as piggybacking with data to the destination node. After receiving data packets along with m_ack packet the destination node signs the m_ack using our modified ECDSA algorithm and sends it back to the source node along the same path through which data packet has come. Source node verifies the signature on m_ack packet. If signature is verified then S confirms that the data packet is successfully received by the destination node else it is concluded that there is a malicious node in the current path. After detection of malicious path the source node S stops sending data packets in that path broadcasts the node id of the node from which it had received RREP packet as malicious node and restarts the route discovery process again.

A. **Algorithm at the Destination 'D' for sending signed '*m_ack*':**

1. *select a random or pseudorandom integer t in the interval [1… n-1]*
2. *compute $Q_D = t \times G$, D's public key is Q_D and private key is t*
3. *For each data packets receive m_ack*
4. *find e = h (m_ack)*
5. *Let Z be the Ln left most bits of e , where Ln is the bit length of the group of order n*
6. *select random integer K in [,1…, n-1]*
7. *Find curve point $(x1,y1) = K \times G$*
8. *Find $r_m = x1 \bmod n$*

   if $r_m == 0$ go to step-6
9. *Find $s_m = K^{-1}(Z+r_m t) \bmod n$*

   if $s_m == 0$ go to step-6
10. *Signature on m_ack is $\sigma = (r_m, s_m)$.For each data packets di send signature σ_i to the source node through the path from which it received di.*

B. **Grayhole Detection and Prevention algorithm**

For the source node *S* to authenticate destination node *D*, *S* must have the copy of *D*'s public key curve point Q_D. *After receiving the σi, the source node S does following for each σi and m_ack_i*

1. *For each σi received, check Q_D is not equal to identity element O.*
2. *Check Q_D lies on the curve*
3. *check that $n \times Q_D = O$*
4. *verify that r_m and s_m are integers in [1,… n-1]*
5. *if not verified*

   (a) There is a malicious node in the current path

   (b) Stop sending data packets in the current path and restart route discovery process again.

   Else go to step-6
6. *calculate e = h(m_ack)*
7. *Let Z be the Ln left most bits of e*
8. *find $Wm = s_m^{-1} \bmod n$*
9. *find $u1 = ZWm \bmod n$ and $u2 = r_m W_m \bmod n$*
10. *Calculate the curve point $(x1,y1) = u1 \times G + u2 \times Q_D$*
11. *if $r_m \equiv x1 \bmod n$ then authenticated and data sent successfully*

    else do following

    (a) stop sending data packets because there is a grayhole node in the current path

    (b) Restart route discovery process for a new route

VII. PERFORMANCE EVALUATION

Simulation Setup

For simulation, we have used ns2 (v-2.35) network simulator. The mobility scenarios are generated randomly varying 30 to 70 nodes randomly moving in an area of 1200m x 1200m.The simulation parameters are summarized in Table 1.

TABLE I

SIMULATION PARAMETERS

Simulation Parameters	*Values*
Simulator	*Ns-2.35*
Simulation time	*100 s*
Number of Nodes	*Varies from 30 to 70*
Routing Protocol	*AODV*
Traffic model	*CBR*
Pause time	*0*
Mobility	*Varies from 10 to 40 m/s*
No of Source Nodes	*4*
Simulation Area	*1200m × 1200m Flat grid*
Packet Size	*Varies from 500 bytes to 2500 bytes*
Data rate	*0.1 MB*
No of Malicious Nodes	*1*

We have done simulation to analyze the performance of the network under various scenarios with and without grayhole attack using normal AODV and our proposed framework. The metrics used to evaluate the performance are listed below:

Performance Metrics:

- Packet Delivery Ratio: The ratio of the data delivered to the destination to the data sent out by the source.
- Throughput: Throughput of network is the rate of successful message delivery over a communication channel. It is usually measured in bits per second (bit/s or bps).

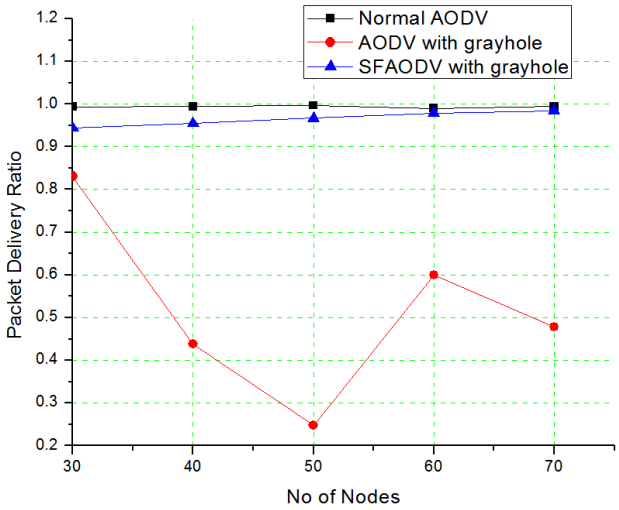

Fig-7 : Packet Delivery Ratio with varying number of nodes

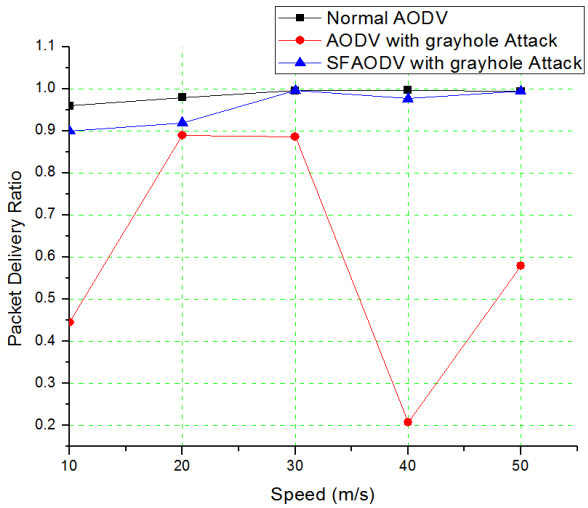

Fig-8 : Packet Delivery Ratio with varying node speed

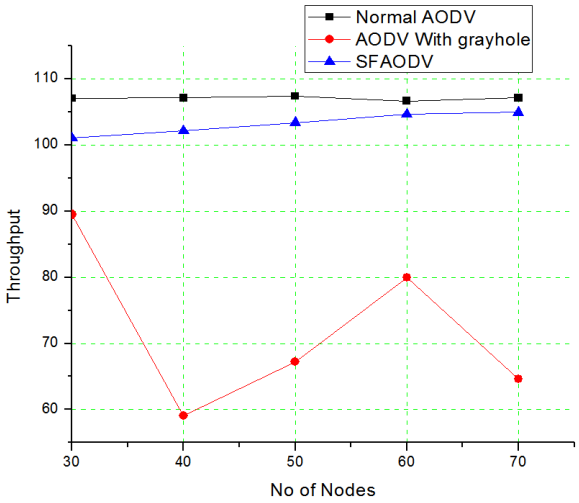

Fig-9: Throughput with varying number of nodes

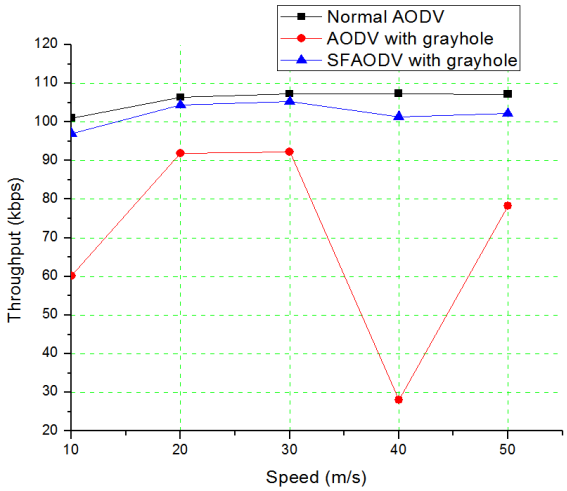

Fig-10: Throughput with varying node speed

In fig-7 we have plotted packet delivery ratio in Y axis and varying no of nodes in X axis.In this figure we obsorve that packet delivery ratio of normal aodv protocol is close to 98% and aodv with grayhole attack is from 20% to less than 90%.The packet delivery ratio of our our proposed framework is close to normal aodv protocol.In this figure at the beginning i.e at node 30 and 40 packet delevery ratio of SFAODV is less than 95% but when number of nodes increase packet delivery ratio increse close to normal aodv this is because when number of nodes is more there are more alternative paths despite the grayhole attack with our secure framework.

In figure-8 we have plotted packet delevery ratio in Y axis and node speed in X axis.In this figure we obsorve that packet delevery ratio of normal aodv is close to 95% at the beginning and approaches to 98% when incleasing number of nodes.packet delivery ratio for aodv with grayhole attack is between 20% to less than 90%. When attack is more packet delivery ratio is close to 20% and when grayhole attack is less packet delivery ratio is close to 90%.In this figure we can see that using our proposed framework packet delivery ratio is increased and it is close to normal aodv.In simulation we have taken some nodes fixed and some nodes mobile.In this figure we can see that when speed is 10 and 20 m/s the packet delivery ratio of our proposed framework is less than 95% and when node speed incleases to 30m/s packet delivery ratio increase and approaches to normal aodv and again when node speed is 40m/s packet delivery ratio again decreases.This is because at the beginning there are less path from source to destination because of less traffic density and when speed increases nodes come in the range of each other which increases traffic density and more alternative path become available which increases packet delivery ratio and again when speed further increases link failure occors and packet delivery ratio decreases.

In fig-9 we plotted throughput in Y axis and number of nodes in X axis.In this figure we obsorve that throughput of normal aodv is more than 105 and that of aodv with grayhole attack is between 60 to 90 kbps.In this figure we can see that by using our proposed framework throughput in improved and it is close to normal aodv.

In fig-10 we have plotted throughput in Y axis and node speed in X axis.In this case we have taken 70 number of nodes.In this figure we obsorve that throughput of normal aodv is more than 100 and aodv with grayhole attack is in between 30 to 90 and by using our propsed framework with grayhole attack, it is close to normal aodv.In this figure we also see that at the beginning when node speed is less throughput is less but when speed increase throughput increases, and after some time again it decreases at speed 40 and again increase at speed 50 this is because of increased node speed the nodes comes in the range of each other at speed 20 and 30 and go away at speed 40 which results link failure and again when speed further increased some other node comes in the range which rebuilds another link as we have taken some nodes mobile and some nodes fixed.When mobile nodes come to the source node or nearer to the path from source to destination, link is established between the nodes and when nodes go away from nodes along the path link fails.

VIII. CONCLUSION

In this paper we survey and do experimental analysis of grayhole attack in MANET for various scenarios. We observe how performance of MANET degrades because of grayhole attack. We then proposed a secure framework "*SFAODV*" which is based on modified *ECDSA*. We did extensive simulation of our proposed framework and normal aodv with and without grayhole attacks and observe that our proposed framework gives better result with grayhole attack and which can remedy the grayhole attack problem in MANET.

ACKNOWLEDGMENT

We would like to thank the anonymous reviewers for their valuable comments and suggestions which helped us to improve the contents and presentation of the paper significantly.

REFERENCES

[1] S. S. Anjum, R. M. Noor and M. H. Anisi, "Survey on MANET Based Communication Scenarios for Search and Rescue Operations," 2015 5th International Conference on IT Convergence and Security (ICITCS), Kuala Lumpur, 2015, pp. 1-5. doi: 10.1109/ICITCS.2015.7293023.

[2] M. Rath and B. K. Pattanayak, "A methodical survey on real time applications in MANETS: Focussing on key issues," 2014 International Conference on High Performance Computing and Applications (ICHPCA), Bhubaneswar, 2014, pp. 1-5. doi: 10.1109/ICHPCA.2014.7045301.

[3] G. Karagiannis et al., "Vehicular Networking: A Survey and Tutorial on Requirements, Architectures, Challenges, Standards and Solutions," in IEEE Communications Surveys & Tutorials, vol. 13, no. 4, pp. 584-616, Fourth Quarter 2011. doi: 10.1109/SURV.2011. 061411.00019

[4] P. Bellavista, G. Cardone, A. Corradi and L. Foschini, "Convergence of MANET and WSN in IoT Urban Scenarios," in IEEE Sensors Journal, vol. 13, no. 10, pp. 3558-3567, Oct. 2013. doi: 10.1109/JSEN.2013.2272099.

[5] Perkins, Charles, Elizabeth Belding-Royer, and Samir Das. Ad hoc on-demand distance vector (AODV) routing. No. RFC 3561. 2003.

[6] Perkins, Charles E., and Pravin Bhagwat. "Highly dynamic destination-sequenced distance-vector routing (DSDV) for mobile computers." ACM SIGCOMM

computer communication review. Vol. 24. No. 4. ACM, 1994.
[7] Clausen, Thomas, and Philippe Jacquet. Optimized link state routing protocol (OLSR). No. RFC 3626. 2003.
[8] Johnson, David B., David A. Maltz, and Josh Broch. "DSR: The dynamic source routing protocol for multi-hop wireless ad hoc networks." Ad hoc networking 5 (2001): 139-172.
[9] Park, Vincent, and M. Scott Corson. Temporally-ordered routing algorithm (TORA) version 1 functional specification. Internet-Draft, draft-ietf-manet-tora-spec-00. txt, 1997.
[10] Raffo, Daniele, et al. "An advanced signature system for OLSR." Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks. ACM, 2004.
[11] Adjih, Cédric, Daniele Raffo, and Paul Mühlethaler. "Attacks against OLSR: Distributed key management for security." 2nd OLSR Interop/Workshop, Palaiseau, France. 2005.
[12] Hu, Yih-Chun, Adrian Perrig, and David B. Johnson. "Wormhole attacks in wireless networks." IEEE journal on selected areas in communications24.2 (2006): 370-380.
[13] Adjih, Cedric, et al. "Securing the OLSR protocol." Proceedings of Med-Hoc-Net. 2003.
[14] Patel, Ankit D., and Kartik Chawda. "Blackhole and grayhole attacks in MANET." Information Communication and Embedded Systems (ICICES), 2014 International Conference on. IEEE, 2014..
[15] Kannhavong, Bounpadith, et al. "NIS01-2: A collusion attack against olsr-based mobile Ad Hoc networks." IEEE Globecom 2006. IEEE, 2006.
[16] Patel, Meenakshi, and Sanjay Sharma. "Detection of malicious attack in MANET a behavioral approach." Advance Computing Conference (IACC), 2013 IEEE 3rd International. IEEE, 2013.
[17] Sen, Jaydip, et al. "A mechanism for detection of grayhole attack in mobile Ad Hoc networks." Information, Communications & Signal Processing, 2007 6th International Conference on. IEEE, 2007.
[18] Rutvij H. Jhaveri, Sankita J. Patel, Devesh C. Jinwala, " A novel approach for Grayhole and Blackhole Attack in Mobile Adhoc Networks." , Second International Conference on Advanced Computing & Communication Technologies, IEEE, 2012.
[19] Rutvij H. Jhaveri, Sankita J. Patel, Devesh C. Jinwala, " Improving Route Discovery for AODV to prevent Blackhole and Grayhole Attacks in MANETs." , INFOCOMP, Version 11, No. 1, p. 01-02, March 2012.
[20] Gundeep Singh Bindra, Ashish Kapoor, Ashish Narang, Arjun Agarwal, "Detection and Removal of Co-operative Blackhole and Grayhole attacks in MANET's ", International Conference on System Engineering and Technology, IEEE, 2012.
[21] Chen Wei, Long Xiang, Bai Yubein, Gao Xiaopeng, " A new solution for resisting Grayhole Attack in Mobile Adhoc Networks." , IEEE, 2007.
[22] Gao Xaiopeng, Chen Wei, " A novel Gray Hole Detection Scheme for Mobile Adhoc Networks.", IFIP International Conference on Networking and Parallel Computing –Workshops, IEEE, 2007.
[23] Jaydip Sen, M. Girish Chandra, Harihara S.G. , Harish Reddy, P. Balamuralidhar, " A mechanism for Detection of Grayhole Attack in Mobile Adhoc Networks.", IEEE, 2007.
[24] Vishnu K, Amos J. Paul , "Detection and Removal of Cooperative Black/Gray hole attack in mobile adhoc networks." , International Journal of Computer Applications,Vol.1,No.22, 2010.
[25] Avenash Kumar and Meenu Chawla, "Destination based group Grayhole attack detection in MANET through AODV", International Journal of Computer Sciences , Vol 9 issue 4, No 1, July 2012.
[26] 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, WCECS 2008, October 22 - 24, 2008, San Francisco, USA.
[27] Chetan S. Dhamade, Prof. H. R. Deshmukh, "An Efficient way to minimize the impact of the Grayhole attack in Adhoc network", International Journal of Emerging Technology and Advanced Engineering Volume 2, Issue 2, February 2012.
[28] Disha G. Kariya, Atul B. Kathole, Sapna R. Heda, "Detecting Black and Gray Hole Attacks in Mobile Adhoc Network Using an Adaptive Method,", International Journal of Emerging Technology and Advanced Engineering, Volume 2, Issue 1, January 2012.
[29] Rutvij H. Jhaveri, "MR-AODV: A Solution to Mitigate Blackhole and Grayhole Attacks in AODV Based MANETs ", Third International Conference on Advanced Computing & Communication Technologies, IEEE, 2013.
[30] Schweitzer, Nadav, et al. "Contradiction Based Gray-Hole Attack Minimization for Ad-Hoc Networks." IEEE Transactions on Mobile Computing (2016).
[31] Hankerson, Darrel, Alfred J. Menezes, and Scott Vanstone. Guide to elliptic curve cryptography. Springer Science & Business Media, 2006.
[32] Koblitz, Neal, Alfred Menezes, and Scott Vanstone. "The state of elliptic curve cryptography." Towards a quarter-century of public key cryptography. Springer US, 2000. 103-123.
[33] Kar, Binayak, et al. "Ecc Based Self Proxy Signature Scheme." International Conference on Instrumentation, Measurement, Circuits and Systems (ICIMCS 2011). ASME Press, 2011.
[34] Nickalls, R. W. D. "A new approach to solving the cubic: Cardan's solution revealed." The Mathematical Gazette 77.480 (1993): 354-359.
[35] Stallings, William. Cryptography and network security: principles and practices. Pearson Education India, 2006.