IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Detection and Prevention of Black Hole Attack in Secure-AODV Network Using RSA SECURITY in MANET

Dharmendra Kumar Meena
Dept. of Computer Science & IT
S.B.P.Govt.College , Dungarpur

Dr.vijaykumar M Chavda(M.C.A.,Ph.D)
Principal
N P College of computer studies
and managenetnt , kadi

Article Info

Article history:

ABSTRACT

As mobile ad hoc network (MANETs) is self-organizing scheme for mobile nodes that interconnect with each other by wireless links with no setup such as access point or base station. Mobile nodes can be directly communicated with each other if node comes in transmission range; the relay nodes are forwarding nodes which send packets to the receivers. In this research paper, we concentration on dissecting and enhancing the most commonly used routing protocol Ad hoc On Demand Distance Vector (AODV) based on the security. Our concentration particularly, is on enhancing the Blackhole Attacks security. We modified the AODV protocol based on the Hash function verification algorithm the name of the modified protocol is Secure-AODV routing protocol. The solution of single and Cooperative blackhole attack are verified with the help of implementation and simulation using network simulator (NS-2.35). Here demonstrate the two scenarios of blackhole attacks 1) consider the single blackhole in the network. 2) Cooperative blackhole scenarios.

Our investigation demonstrates the comparison between the single and multiple blackhole in the network. This comparison carried between the Blackhole-AODV-RSA and blackhole-Secure AODV-RSA based the QOS parameter performance of Packet Delivery Ratio (PDR), Average end to end delay and Average throughput in the presence of Blackhole attacks. The packet deliver ratio performances are increased and average delay performance is decreased in Secure-AODV-RSA with respect to blackhole AODV-RSA, its increase the performance of the network. The simulation results show that proposed approach (Secure-AODV-RSA) is better than AODV-RSA.

1. INTRODUCTION

Wireless ad-hoc networks are made out of independent nodes that are self-guided with no foundation. In along these lines, ad-hoc networks have dynamic topology with the end goal that node can simply join or leave the system whenever. They have numerous potential applications, particularly, in military and save ranges, for example, interfacing soldiers on frontline or build up another system setup. Ad-hoc wireless network demonstrates the Route Discovery Process [1]. The wireless networks are appropriate for the area where that is not possible to make a proper connection a fixed infrastructure. The nodes communications happen to each other without presence of infrastructure, whenever it provides connectivity with forwarding packets over themselves. For this node connection, in the network used such routing protocols that are mention, AODV (Ad-hoc On-Demand Distance Vector), DSR (Dynamic Source Routing) and DSDV (Destination Sequenced Distance-Vector).

2. LITERATURE REVIEW

Black hole detection has been a dynamic zone of research since Hongmei Deng modified 'next hop information' [9] based organization in 2002. Researchers have proposed different answers for recognize and handle black hole attack. However, only a couple of researches are identifying collaborative black holes. A review of such strategies is presented here. In [10], L. Tamilselvan et al., proposes the thought of 'Loyalty Table. Here, every node is allotted a specific constancy level, a measure of dependability. At whenever point a source node communicates a RREQ and holds up, the approaching RREPs are assembled in its Response Table. If the average of the dependability level of RREP which sending node (RREPN) and its next hop node (NHN) in this route is found to be over a prearranged threshold, RREPN is measured as responsible.

In this manner, on the receipt of various RREPs, the one with the most noteworthy devotion level is chosen. In any case, if numerous nodes have a similar dedication level, the RREP with the insignificant is picked. At last, directing is refined through the chosen way. Upon information receipt, the goal node sends an affirmation to the source node inside clock. Next, constancy level of the RREPN is augmented as a honor for legit routing else that of both RREPN and its NHN is decremented for being synergistic. Anyway, if constancy level of a node drops to zero, it is considered as a dark opening and the nearness of attacks is implied to all utilizing caution bundles. In spite of the way that this technique handles both single and community dark opening attacks, it includes expanded capacity overhead, directing overhead and deferral.

This is on account of every node ought to keep up a Fidelity Table and a Response Table that must be refreshed and traded among the nodes occasionally. Consequent to routing, the source node needs to sit tight for an affirmation from goal to affirm the wellbeing of course. With a specific end goal to assume that a node is vindictive, we have to hold up until its loyalty level drops to zero. Henceforth information bundles will be dropped to some degree.

J. Sen et al., presents idea of information routing data (DRI) table [11]. Each node keeps up a DRI table which monitors past steering data. Be that as it may, on the receipt of a RREQ, the RREPN turns upward in its DRI table and sends the DRI passage of its Next Hop Node (NHN) to the source node. A node is dealt with as dependable, if source node has effectively directed information bundles through it. On the off chance that problematic, current NHN turns into the new middle node and the source node needs to send a further demand (FRq) to the following bounce node of this transitional node. At that point NHN sends back a further answer (FRp) that fuses DRI sections of IN and the following jump of current NHN. In the interim, Source node on getting FRp investigates the DRI passages and if DRI section of IN says that it has directed parcels from NHN and that of NHN says that it has not steered any bundle through IN, then every one of the nodes, in the switch way from halfway node to RREPN are considered as dark gap nodes since NHN is a dependable node

In the event that IN is an obliging node, directing can be refined. Despite the fact that this strategy anticipates agreeable dark gap attacks, DRI table expends profitable memory space in scaled down MANET nodes. On the off chance that a node does not perform interest in information exchange action through or from its neighboring nodes, it might prompt bogus arrangement of the trusty node as a malevolent dark gap node. It likewise bombs in the discovery of single or non-agreeable numerous dark openings since they drop FRq itself. In [12], [13] and [14], progressed DRI tables are utilized. As showed by the arrangement indicated in [15], qualities are discretionarily relegated for a few parameters for every node. By taking the result of these parameters to be particular rank (a measure of dependability), soundness consider (alternately comparing to speed of node) and remaining battery constrain, trust estimation of each node is settled. Afterward, normal trust of each course is evaluated by averaging the trust of each and every taking part node in that course and the course with the most elevated normal trust is chosen.

Therefore, the source node needs to sit tight for an affirmation from goal. In the event that the parcel transmission is effective, the goal node sends back an affirmation to the source node. On receipt of assertion from goal, the source node builds the rank and decrements the rest of the battery energy of all nodes in that way. On opposite, if no affirmation, the source node decrements rank of every node in the course. Despite the fact that this strategy handles both single and community oriented dark gap attacks, all RREPs ought to be cushioned and normal trust esteem should be resolved. In addition, the parameters related with every node should be kept up and refreshed as often as possible.

3. RESEARCH METHOD

Black hole Attack is a sort of Denial of Service Attack. Black hole Attack is an error node procedure its routing protocol to promote itself having the shortest path towards the destination node. At the point route is set up, then error node forwards it to the malicious attacks wants address [9].

The Black Hole Attack must make RREP with Destination arrangement more noteworthy than the destination arrangement of the receiver node and sender node trusts that black hole node and additional interconnects with blackhole node in its place of real destination node. This mischievous frequently harm nodes interface and thus waning all asset usage in accumulation to losing packets. Here Blackhole Attacks are categorized into two categories [10].

A. **Single Black Hole Attack:** In this scenario, single blackhole attacks are represent which acts as malicious node within the networks topology shows in (Figure 1).

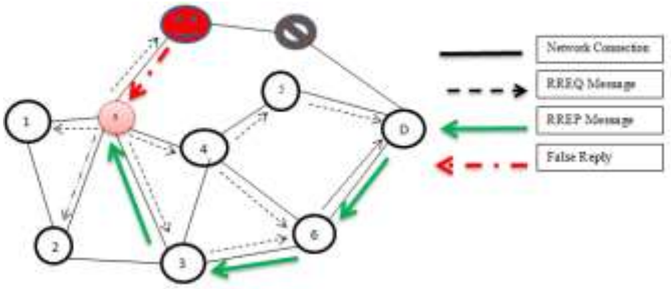


Figure 1: Single blackhole attack topology.

B. **Cooperative Black Hole Attack:** In this scenario, cooperative blackhole attacks are represent which acts as malicious node and provide the false reply to neighbor node within the networks topology shows in (Figure 2).

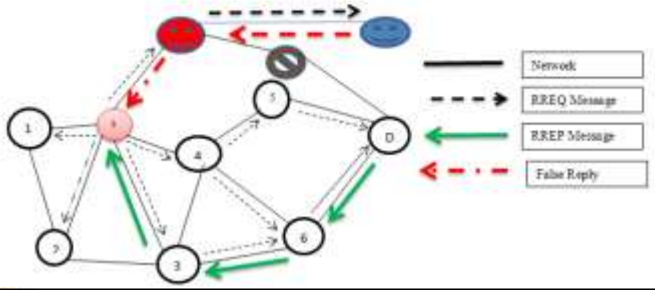


Figure 2: Cooperative blackhole attack topology.

Algorithm-I: Secure-AODV

```
Assumption: RREP header is modified with additional field that is Speed of node.
Step 1:   Source S broadcasts RREQ message to the network.
Step 2:   If Destination D replies RREP then S will start transmission.
          END
Step 3:   If intermediate node (say B) replies with RREP and when packet reaches node Y's preceding node@ (say A), it checks the following:
if (Speed of Node** > speed_threshold or SequenceNo**  > seq_no_threshold)
GOTO Step 4.
else
GOTO Step 5.
Step 4:   If (hopcount** >= 2)
Node X will send a Modified Hello signal (MHELLO) with
HopCount equal to 2 (in case hopcount** = 2)
                    or
HopCount equal to 3 (in case hopcount** > 2) to a Node@@ (say Z) which is few hops (equal to hopcount**) away from A.
If A receives acknowledgment from Z successfully then
A forwards RREP to S and S will transmit the data.
          Else
Node next to B is Blackhole and an alert signal will be transmitted by A to S.
Else
Node B is Blackhole node and an alert signal will be transmitted by A   to S.
Step 5:   A forwards RREP to S and S will transmit the data.
Note:-  1.          MHELLO is same as HELLO packet with hop count = hopcount**.
2.        Threshold value is updated every time intermediate node receives a RREQ packet.
3.        Threshold value of sequence no is calculated as
sequence_number_threshold = sequence_number(of RREQ packet) * hop count
4.        Threshold value of node speed is taken as
speed_threshold = 100 m/s
** all the values have to be taken from the RREP received from intermediate node B.
@ preceding node A is in the direction in which RREP is traversing from B towards S.
@@ Z node is in the path through which RREP packet has reached B.
```

Algorithm-II: RSA Algorithm

RSA algorithm is public key cryptographic algorithm that makes use of 2 keys namely public key and private key [5].

If RSA keys do not exist, they need to be generated. The key generation process is usually slow but it is performed seldom. It involves three steps: Key Generation, Encryption and Decryption [5].

Key Generation: Prime integers are used for key generation.

1. n =p*q(n is used as modulus for both public key and private key)

2. Compute ij(p*q) = (p í 1)*(q í 1).

3. Choose an integer e such that 1 < e <ij(p*q), and GCD of e and ij(p*q) must be 1.

➢ e is released as the public key exponent.
➢ e having a short bit.

4. Determine d (using modular arithmetic) which satisfies congruence relation.

- d*e =1(mod(ij(p*q))

d is kept as the private key exponent

Encryption:

Destination node transmits its public key (n, ,e) to Source node and keeps the private key secret then source wants to send message M to Destination

It first turns M into an integer 0 < m < n by using an agreed-upon reversible protocol known as a padding scheme. It then computes the cipher text c corresponding to:

$$\mathbf{C= m^{2}\ (mod\ n)}$$

Decryption:

Destination node can recover m from c by using its private key exponent d by the following

Computation:

Given m, Destination can recover the original message M by reversing the padding scheme.
===

4. RESULTS AND ANALYSIS

After the mathematics, integration and algorithms simulated the performance of blackhole-AODV-RSA and proposed-work (blackhole-Secure AODV-RSA) with the help of network simulator 2 (NS-2.35). Here used a real node network topology. The scenario consists of 50, 100, 150, 225 and 315 numbers of nodes which is showing in figure. The movement of presented nodes was generated with MANET network simulator [5]. For the evaluation considered two protocols of the MANET networks- AODV, Secure-AODV Protocol using RSA algorithm which is used for more and higher security purpose with blackhole attack is develop and design for comparative study on the basic of QOS performance parameter. Secure-AODV using RSA algorithm is modified and improved work to make the protocol more secure and increased the performance of the system. Here two types of blackhole scenario (Single Blackhole in (figure 3& 4) and Cooperative Black Hole Attack in (figure 5 & 6)) results are presented.

Table 1: Simulation parameter

Parameters	**Values**
Operating System	Linux (Ubuntu 12.04)
NS-2 version	NS-2.35
No. of Node	50, 100, 150, 225, 315
Packet Size	512
Traffic Type	UDP/CBR
Simulation Time	100 Second
Antenna Type	Omni-Antenna
Transmission Range	1000*1000 m
Routing Protocol	AODV, Secure-AODV, RSA-Algorithm

A. Performance Metrics

a) ***Average end-to-end delay:*** Average end-to-end delay expressed the average time which data packets passed to transmission from source nodes to destination however since all delays initiated by buffering, queuing and propagation delays. Thus, average end–to-end delay somewhat depends on packet delivery ratio. When distance increased between source and destination, probability of the packet drop is also increased. The mathematically formula of average end-to-end delay (D) and total number of packets delivery successfully (n) in this scenario shown in equation (1).

$$Average\ end2end\ delay = \frac{\sum_{i=1}^{n}(Received\ Packet\ Time - Send\ Packet\ Time)*1000(ms)}{Total\ Number\ of\ Packets\ Delivery\ Successfully} \quad (1)$$

b) ***Average network throughput:***The average network throughput expressed the total amount of data packets which successfully arrived at final destination as per given simulation time. The mathematical calculation of throughput shows, here PacketSize is size of packet of ith packet reaching to destination, PacketArrival is the time when last packet arrived and PacketStart is the time when first packet arrived to destination.

$$Throughput = \frac{PacketSize}{(PacketArrival - PacketStart)} \qquad (2)$$

c) ***Packet Delivery Ratio (PDR):***Packet Delivery Ratio expressed the ratio of total packets positively reached at the destination nodes source nodes. The network performance is high, when packet delivery ratio is high in the network. The mathematically calculation of packet delivery ratio shown in equation (3)

$$\text{Packet Delivery Ratio} = \frac{\sum \text{Total packets received by all destination node}}{\sum \text{Total packets send by all source node}} \,(3)$$

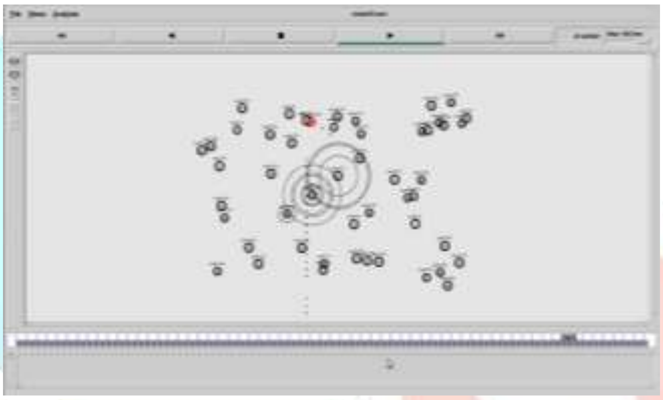


Figure 3: Network topology for single blackhole in network simulator 2.35.

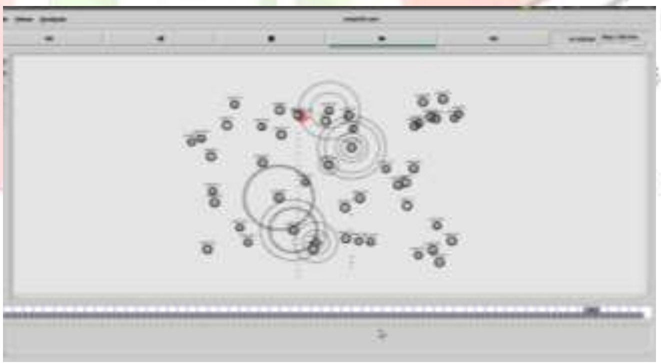


Figure 4: Network topology for single blackhole after 50 seconds in network simulator 2.35.

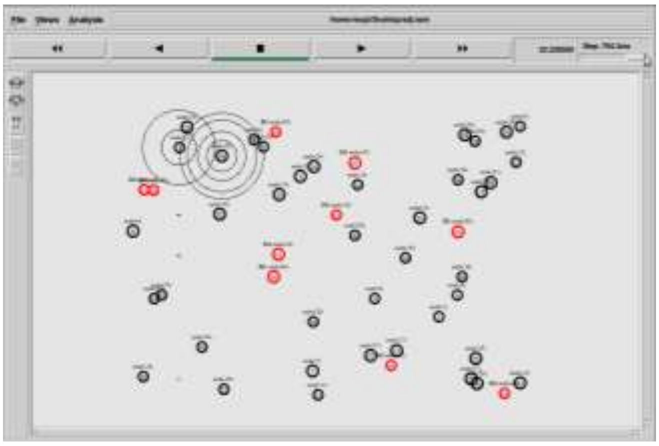


Figure 5: Network topology for Cooperative Black Hole Attack in network simulator 2.35

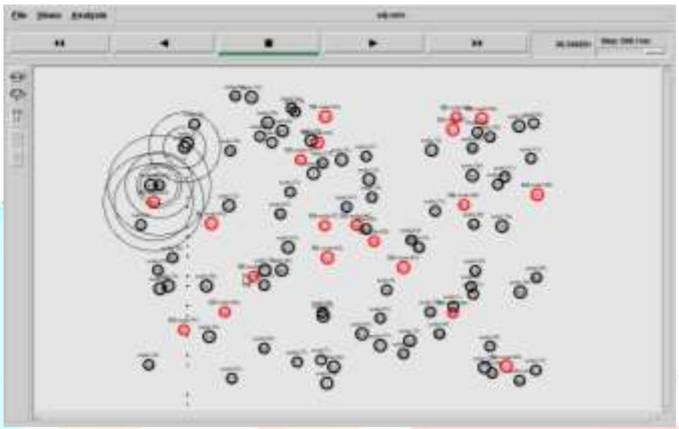
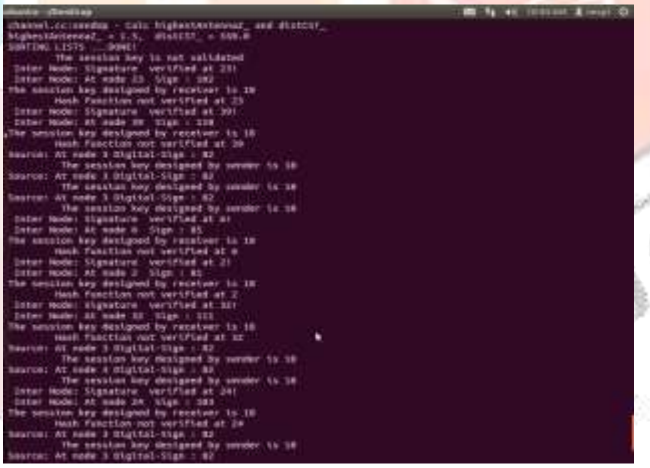


Figure 6: Network topology for Cooperative Black Hole Attack after 50 seconds in network simulator 2.35



```
channel.cc:sendUp - Calc highestAntennaZ_ and distCST_
highestAntennaZ_ = 1.5,  distCST_ = 550.0
SORTING LISTS ...DONE!
        The session key is not validated
 Inter Node: Signature  verified at 23!
 Inter Node: At node 23  Sign : 102
The session key designed by receiver is 18
        Hash Function not verified at 23
 Inter Node: Signature  verified at 39!
 Inter Node: At node 39  Sign : 118
The session key designed by receiver is 18
        Hash Function not verified at 39
Source: At node 3 Digital-Sign : 82
         The session key designed by sender is 18
Source: At node 3 Digital-Sign : 82
         The session key designed by sender is 18
Source: At node 3 Digital-Sign : 82
         The session key designed by sender is 18
 Inter Node: Signature  verified at 6!
 Inter Node: At node 6  Sign : 85
The session key designed by receiver is 18
        Hash Function not verified at 6
 Inter Node: Signature  verified at 2!
 Inter Node: At node 2  Sign : 81
The session key designed by receiver is 18
        Hash Function not verified at 2
 Inter Node: Signature  verified at 32!
 Inter Node: At node 32  Sign : 111
The session key designed by receiver is 18
        Hash Function not verified at 32
Source: At node 3 Digital-Sign : 82
         The session key designed by sender is 18
Source: At node 4 Digital-Sign : 83
         The session key designed by sender is 18
 Inter Node: Signature  verified at 24!
 Inter Node: At node 24  Sign : 103
The session key designed by receiver is 18
        Hash Function not verified at 24
Source: At node 3 Digital-Sign : 82
         The session key designed by sender is 18
Source: At node 3 Digital-Sign : 82
```

Figure 7: Verification output of Secure-AODV Network topology in network simulator 2.35.

B.   Simulation Results

Several simulations scenarios on the different approaches were done. Here represent two different comparison scenarios of the present work

Table 2: Delay comparison for single and Cooperative blackhole attacks using RSA-AODV.

Blackhole-RSA-AODV Delay		
Delay	**SBH-AODV-RSA**	**CBH-AODV-RSA**
50-NODES	389.45	373.82
100-NODES	744.97	473.45
150-NODES	393.48	248.4
225-NODES	499.48	359.55
315-NODES	675.81	616.1

Table 3: PDR comparison for single and Cooperative blackhole attacks using RSA- AODV

Blackhole-RSA-AODV PDR		
PDR	**SBH-AODV-RSA**	**CBH-AODV-RSA**
50-NODES	81.8197	82.0419
100-NODES	76.6302	78.0872
150-NODES	82.3547	82.9127
225-NODES	88.4411	81.9704
315-NODES	85.1583	88.3678

Table 4: Throughput comparison for single and Cooperative blackhole attacks using RSA-AODV

Blackhole-RSA-AODV Throughput		
Throughput	**SBH-AODV-RSA**	**CBH-AODV-RSA**
50-NODES	1405.99	1425.34
100-NODES	1090.45	949.33
150-NODES	936.1	897.76
225-NODES	1473.54	1434.96
315-NODES	1673.48	1461.59

Table 5: Delay comparison for single and Cooperative blackhole attacks using Secure-RSA-AODV.

Blackhole-Secure RSA-AODV Delay		
Delay	**SBH-SAODV-RSA**	**CBH-SAODV-RSA**
50-NODES	465.57	57.34
100-NODES	515.78	0
150-NODES	442.22	0
225-NODES	694.14	119.93
315-NODES	537.6	653.68

Table 6: PDR comparison for single and Cooperative blackhole attacks using Secure- RSA-AODV.

Blackhole-Secure RSA-AODV PDR		
PDR	**SBH-SAODV-RSA**	**CBH-SAODV-RSA**
50-NODES	79.2301	85.1202
100-NODES	79.8012	85.6662
150-NODES	87.2691	83.0904
225-NODES	85.7013	76.5388
315-NODES	90.044	89.5886

Table 7: Throughput comparison for single and Cooperative blackhole attacks using Secure-RSA-AODV

Blackhole-Secure RSA-Aodv Throughput		
Throughput	**SBH-SAODV-RSA**	**CBH-SAODV-RSA**
50-NODES	1379.3	1152.24
100-NODES	989.09	473.11
150-NODES	889.44	473.11
225-NODES	1463.04	1771.68
315-NODES	1375.36	1381.06

The simulation result shows x-axis denotes the simulation node and y-axis is shows the performance metrics parameter

Average end-to-end delay: The average delay of AODV is increased with number of nodes but after a 150-node delay is increased smoothly. The overall performance of average delay for single and cooperative blackhole attack with respect to number of nodes are showing in (Figure 8), where single black hole AODV-RSA having increased delay value as compare to the cooperative blackhole AODV-RSA

Packet Delivery Ratio: The Performance of packet delivery ratio of single black hole-AODV-RSA is increased with 150 nodes. With the variation of number of node AODV-RSA routing protocol packet delivery ratio is low for the single black hole attack till 150 nodes after 225 nodes it's slightly increased as compare to the Cooperative (Figure 9).

Throughput: The performance of throughput for blackhole-AODV-RSA for single and cooperative blackhole almost same for nodes 50, 100, 150 and 225 but throughput after 225 nodes is showing the different performance and single blackhole-AODV-RSA increased (Figure 10).

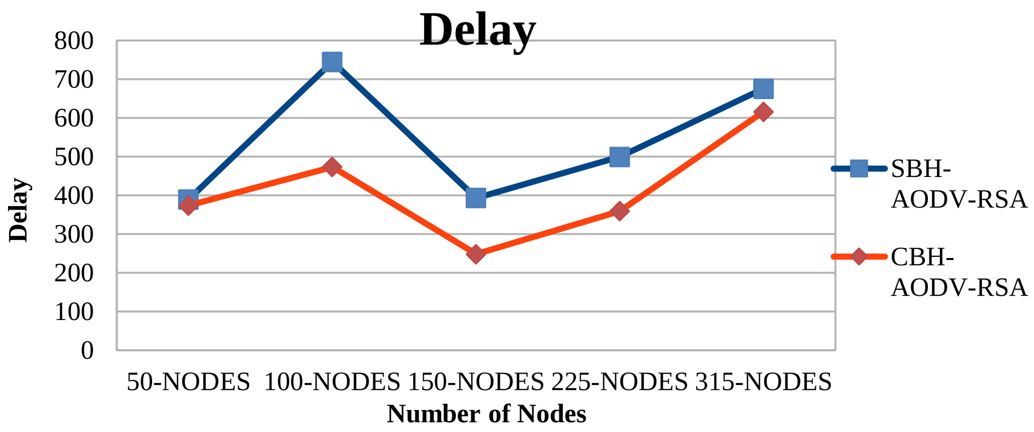


Figure-8 Delay comparison for single and Cooperative blackhole attacks with respect to number of node variation using RSA-AODV.

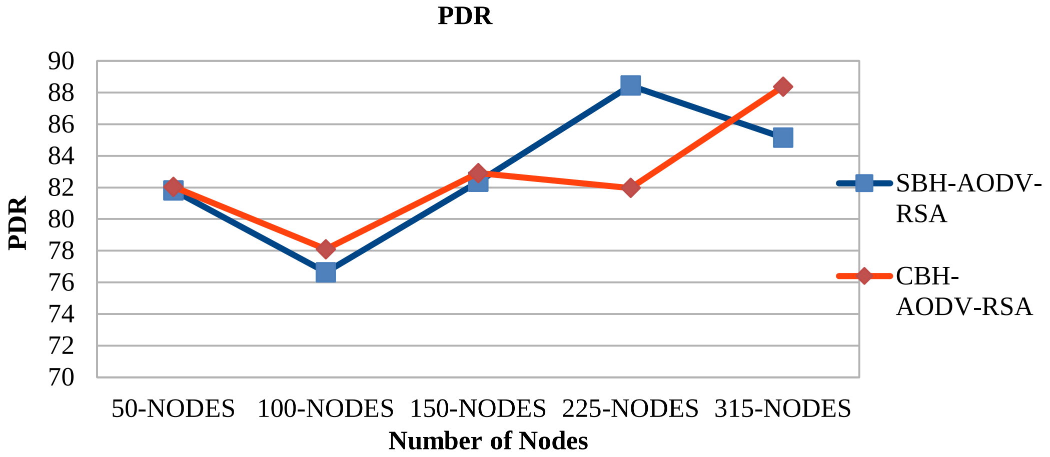


Figure-9 Packet Delivery Ratio comparison for single and Cooperative blackhole attacks with respect to number of node variation using RSA- AODV.

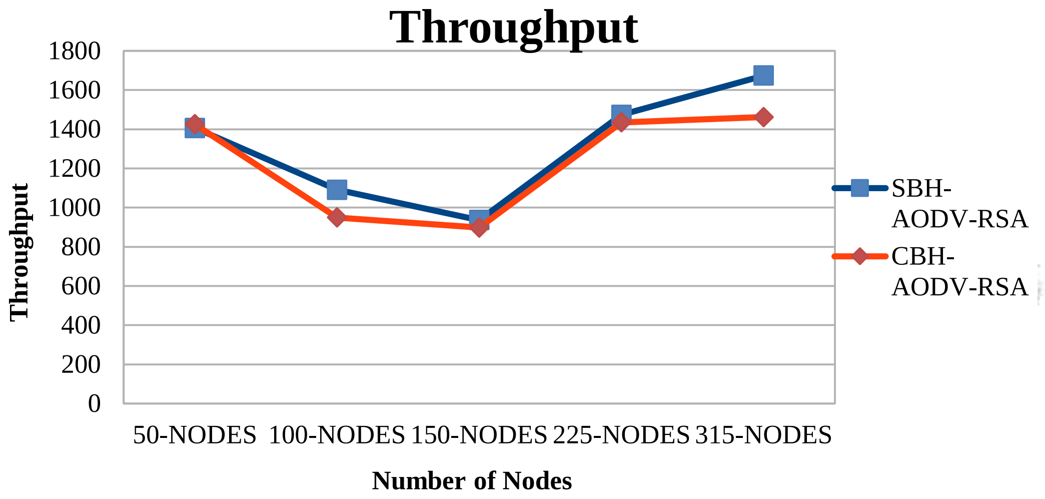


Figure-10 Throughput comparison for single and Cooperative blackhole attacks with respect to number of node variation using RSA- AODV.

Average end-to-end delay: The average delay of Secure-AODV-RSA single blackhole is almost same for node 50, 100 and after 150 nodes its increase and slightly decrease at node 315. The cooperative black holes are showing less delay as compare to single black hole. It's having very less dealy as compare to single black hole, so that our proposed Secure-AODV is more secure and highly aware to the network (Figure 11).

Packet Delivery Ratio: The Performance of packet delivery ratio of single and cooperative black hole in Secure-AODV-RSA network is continuously increased as compare to AODV-Blackhole-RSA; it's increased the packet delivery ratio (Figure 12).

Throughput: The performance of throughput for blackhole-AODV-RSA for single and cooperative blackhole almost same for nodes 50, 100, 150 and 225 but as compare to the normal blackhole AODV-RSA is better, all results in secure-AODV-RSA is high (Figure 13).

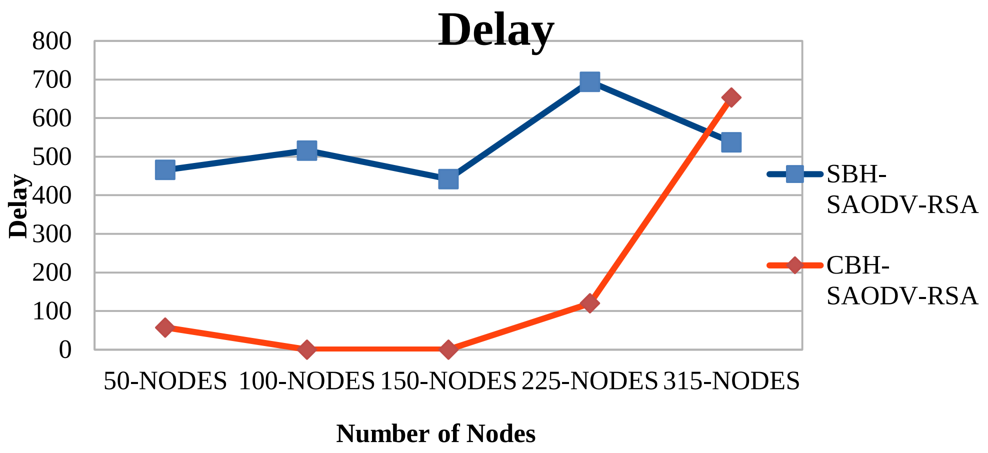


Figure-11 Average Delay comparison for single and Cooperative blackhole attacks with respect to number of node variation using Secure-RSA-AODV.

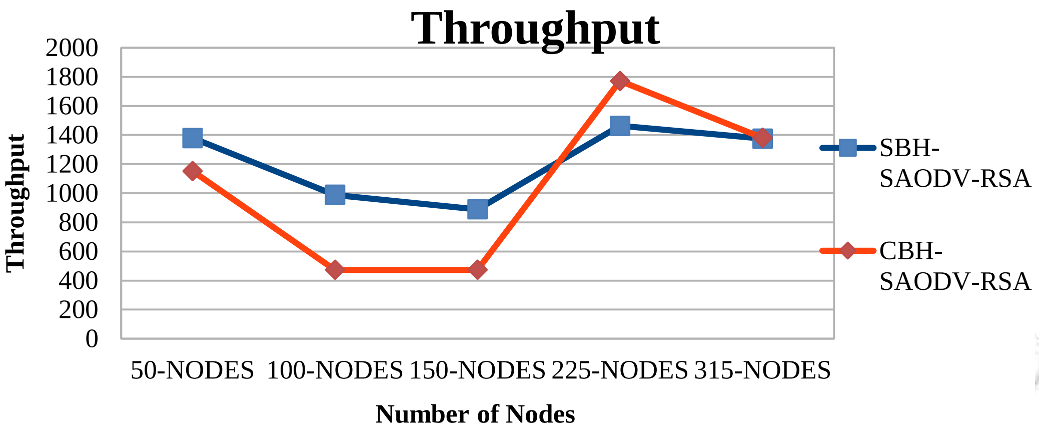


Figure-12 Packet Delivery Ratio comparison for single and Cooperative blackhole attacks with respect to number of node variation using Secure-RSA-AODV.

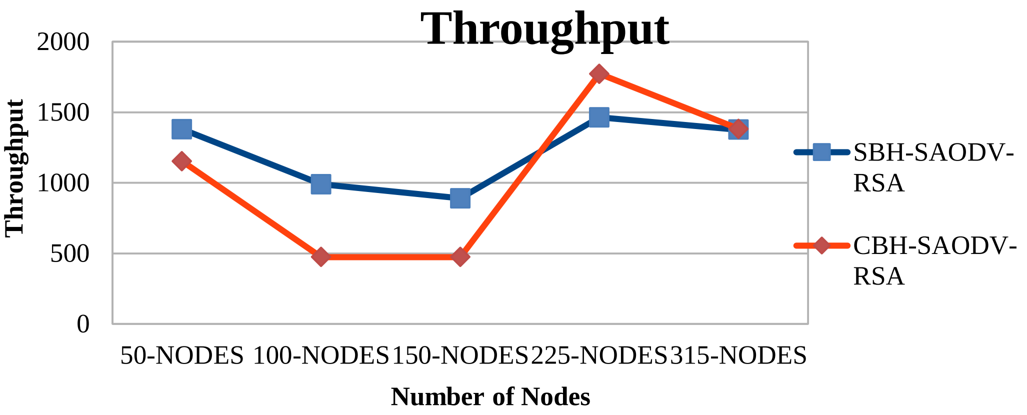


Figure-13 Throughput comparison for single and Cooperative blackhole attacks with respect to number of node variation using Secure-RSA-AODV.

5. CONCLUSION

A Black Hole attacks is one of the genuine security issues in MANETs. It is an attack where a vindictive hub imitates a goal hub by sending fashioned RREP to a source hub that starts course disclosure, and therefore denies information movement from the source hub. In this paper a review on various existing strategies for identification of dark opening attacks in MANETs with their deformities is displayed. The identification procedures which make utilization of proactive steering convention have better bundle conveyance proportion and right recognition likelihood, yet have higher overheads. The discovery methods which make utilization of responsive directing conventions have low overheads, yet have high parcel misfortune issue. In light of the above execution correlations, it can be presumed that black Hole attacks influences organize adversely. Subsequently, there is requirement for flawless recognition and end instruments. The recognition of Black Holes in impromptu systems is as yet considered to be a testing errand. Future work is expected to an productive Black Hole attacks discovery and disposal calculation with least postponement and overheads that can be adjusted for impromptu systems helpless to Black Hole attacks. The overall performance of average end to end delay, packet delivery ration, and throughput for single and cooperative blackhole attack with respect to number of nodes variation are Secure-AODV with hash function using RSA verification performance better to AODV –RSA protocols.

REFERENCES

[1] Pandya, Morli, and Ashish Kr Shrivastava. "Improvising the performance with security of AODV routing protocol in MANETs." Engineering (NUiCONE), 2013 Nirma University International Conference on. IEEE, 2013.

[2] Ghouti, Lahouari, Tarek R. Sheltami, and Khaled S. Alutaibi. "Mobility prediction in mobile ad hoc networks using extreme learning machines." Procedia Computer Science 19 (2013): 305-312.

[3] Taneja, Sunil, and Ashwani Kush. "A survey of routing protocols in mobile ad hoc networks." International Journal of innovation, Management and technology 1.3 (2010): 279.

[4] Tseng, Fan-Hsun, Li-Der Chou, and Han-Chieh Chao. "A survey of black hole attacks in wireless mobile ad hoc networks." Human-centric Computing and Information Sciences 1.1 (2011): 4.

[5] Ponsam, J. Godwin, and R. Srinivasan. "A survey on MANET security challenges, attacks and its countermeasures." International Journal of Emerging Trends & Technology in Computer Science (IJETTCS) 3.1 (2014).

[6] Gurung, Shashi, and Krishan Kumar Saluja. "Mitigating impact of blackhole attack in MANET." Int. Conf. on Recent Trends in Information, Telecommunication and Computing, ITC. 2014.

[7] J.Sen, S. Koilakonda, A. Ukil, "A Mechanism for Detection of Cooperative Black Hole Attack in Mobile Adhoc Networks" IEEE Second International Conference on Intelligent Systems, Modeling and Simulation, 2011

[8] G.S Bindra, A. Kapoor, A. Narang, and A. Agrawal, "Detection and Removal of Co-operative Blackhole and Grayhole Attacks in MANETs," in Proceeding of InternationalConference on System Engineering and Technology, Bandung, 2012.

[9] V.A. Hiremani and M. M Jadhao, “Eliminating Cooperative Black hole and Gray Hole using Modified EDRI Table in MANET,” IEEE,2013.

[10] G. Wahane and S. Lonare, “Technique For Detection of Cooperative Black Hole Attack In MANET,” 4th ICCCNT 2013, July 4-6,2013, Tiruchengode, India.

[11] S. Biswas, T.Nag and S. Neogy, “Trust Based Energy EfficientDetection and Avoidance of Black Hole Attack to Ensure Secure Routing in MANET”,in IEEEXplore International Conference on Applications and Innovations in Mobile Computing (AIMoC 2014),India,pp. 157.

[12] Nishukalia, KundanMunjal,“Multiple Black Hole NodeAttack DetectionScheme in MANET by Modifying AODV Protocol” International Journal of Engineering and Advanced Technology (IJEAT), Vol. 2, Issue-3, February 2013.

[13] Thachil, F., and Shet, K.C.: 'A Trust Based Approach for AODV Protocol to Mitigate Black Hole Attack in MANET'. Proc. International Conference on Computing Sciences, 14-15 Sept 2012.