Secure Aodv Routing to Prevent Blackhole and Grayhole Attack

Yogendra Singh[1], Farah Shan[2]
[1]M.tech Scholar, Department of Computer Science and Engineering
Kanpur institute of Technology, Kanpur, UP, India
yogimnnit@gmail.com[1]
[2]Assistant professor, Department of Computer Science and Engineering
Kanpur institute of Technology, Kanpur, UP, India

ABSTRACT

The conveyed idea of a MANET endeavors to give repetition by enabling different routes to be shaped, when a route fails because of battery depletion or noxious assault options are promptly accessible. Black hole or Gray hole assault ruins this repetition by detaching the private channel can disengage a dominant part of dynamic courses. These assaults are troublesome in MANET, when it is executed by changing the working of steering conventions like AODV in which routes are chosen based on communicated data, for example, number of hops to base station. Cryptographic security techniques can give security to keep up the privacy and respectability of data messages. The paper proposes a way to deal with adjust the working of AODV keeping in mind the end goal to execute and identify gray hole and black hole nodes in network. AODV routing protocol is utilized as a part of multi hop ad-hoc systems. The AODV convention does not require any sort of system foundation or focal organization. This examination work is altering the working of existing AODV convention as WRP (AODV with wormhole) for usage and discovery of individual black hole, cooperate black hole, gray hole assaults. It finds the faulty nodes in the way based on delay and forwarding ratio.

Keywords - *Wireless sensor network, Network security, Aodv, Grayhole attack, Blackhole*

1. INTRODUCTION

Versatile specially appointed systems are turning out to be more crucial to remote correspondences because of developing notoriety of convenient gadgets [1]. Their capability to act naturally arranged and shapes a versatile lattice system utilizing remote connections which makes them appropriate for various cases that other sort of systems can't satisfy the important necessities. MANETs offer the flexibility to utilize compact gadgets and move autonomously of the position of base stations with the assistance of other system gadgets. The convenient hubs that are in radio scope of each other can straightforwardly banter, while others necessitate the lead of middle of the road hubs to course their bundles. Each of the hubs has a remote interface to banter with each other. These systems are completely disseminated and work anyplace without the aid of any altered topology as access focuses.

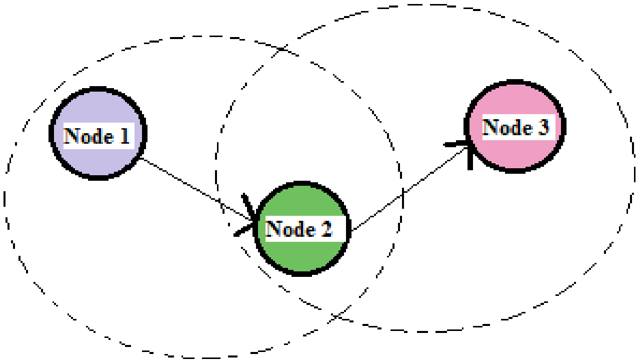


Fig.1 Example of Mobile Ad-Hoc Network [2]

Fig. 1 demonstrates a basic impromptu system having 3 hubs. Hub 1 and hub 3 are not inside scope of each other; however the hub 2 can be utilized to forward bundles between hub 1 and hub 2. The hub 2 will go about as a switch and these three hubs together shape a specially appointed system [2].

2. ATTACKS IN WIRELESS SENSOR NETWORK

There are many attacks that harm or make vulnerable the nodes in WSN. In OSI layer, various attacks are classified according to each layer. These are such as: Application Layer**:** Attacks on Reliability, Malicious code, Repudiation and data. Transport Layer**:** Injects false messages and Energy drain attacks Authentication**.** Network Layer**:** Packet drop, Wormhole, black hole, flooding, Resource consumption, Authentication. Data Link Layer: Jamming and collision Use error correction codes and spread spectrum techniques Physical Layer**:** Jamming, interceptions and Eavesdropping [3].

2.1 Wormhole Attack

In wormhole assault, a malignant hub gets parcels at one area in the system and passages them to another area in the system, where these bundles are loathe into the system. This passage between two plotting aggressors is alluded to as a wormhole. It could be set up through wired connection between two conniving assailants or through a solitary long-go remote connection. In this type of assault the assailant may make a wormhole notwithstanding for parcels not routed to itself as a result of communicate nature of the radio channel. For instance in Figure 3.6, X and Y are two noxious hubs that epitomize information bundles and distorted the course lengths [4].

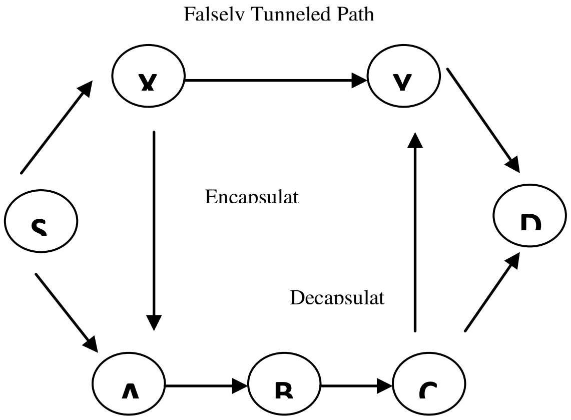


Fig 2: Wormhole assault [4]

Assume hub S wishes to shape a course to D and starts course revelation. At the point when X gets a course ask for from S, X epitomizes the course demand and passages it to Y through a current information course, for this situation {X - > A - > B - > C - >Y}. At the point when Y gets the embodied course ask for D then it will demonstrate that it had just voyage {S - > X - > Y - > D}. Neither X nor Y refresh the parcel header. After course revelation, the goal discovers two courses from S of unequal length: one is of 4 and another is of 3. On the off chance that Y burrows the course answer back to X, S would erroneously consider the way to D through X is superior to the way to D by means of A. Subsequently, burrowing can keep genuine middle of the road hubs from effectively augmenting the metric used to gauge way lengths. Despite the fact that no mischief is done if the wormhole is utilized legitimately for proficient transferring of bundles, it puts the assailant in a capable position contrasted with different hubs in the system, which the aggressor could use in a way that could trade off the security of the system.

The wormhole assault is especially perilous for some specially appointed system steering conventions in which the hubs that hear a parcel transmission straightforwardly from some hub view themselves as in scope of (and in this way a neighbor of) that hub. For instance, when utilized against an on-request steering conventions, for example, DSR [5], a capable use of the wormhole assault can be mounted by burrowing each course ask for parcel specifically to the goal target hub of the demand. At the point when the goal hub's neighbors hear this demand parcel, they will take after typical directing convention handling to rebroadcast that duplicate of the demand and afterward dispose of without preparing all other got course ask for bundles starting from this same course disclosure. This assault in this way keeps any courses other than through the wormhole from being found, and if the assailant is close to the initiator of the course revelation. This assault can even counteract courses more than two bounces in length from being found. Conceivable courses for the aggressor to then endeavor the wormhole incorporate disposing of instead of sending all information bundles, in this manner making a perpetual Denial-of-Service assault or specifically disposing of or changing certain information parcels. In this way, if legitimate components are not utilized to shield the system from wormhole assaults, the vast majority of the current directing conventions for impromptu remote systems may neglect to discover substantial courses.

2.2 Black hole Attack

MANETs confront different securities dangers i.e. assault that are passed out against them to interfere with the ordinary execution of the systems. Black hole assault is one of the security risk in which the activity is divert to such a hub, to the point that really does not exist in the system. In these assaults, dark gap assault is that sort of assault which happens in Mobile Ad-Hoc organizes (MANET). In black hole assault, a pernicious hub utilizes its steering convention so as to embrace itself for having the most limited way to the goal hub or to the bundle it needs to hinder [6]. This ruinous hub promotes its accessibility of new courses independent of checking its steering table. Along these lines assailant hub will dependably have the accessibility in answering to the course demand and in this way block the information bundle and hold it. In convention in light of flooding, the malignant hub answer will be gotten by the asking for hub before the reaction of answer from real hub; consequently a malevolent and manufactured course is made. At the point when this course is set up, now it is up to the hub whether to drop every one of the bundles or elevate it to the obscure address.

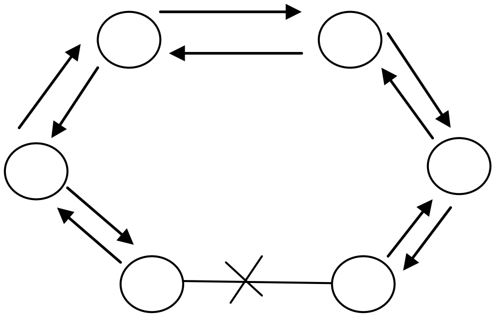


Fig 3: Black Hole Attack [6]

The black hole assault has two properties. To start with, the hub misuses the portable impromptu steering convention, for example, AODV, to advance itself as having a substantial course to an objective hub, despite the fact that the course is false, with the point of catching parcels. Second, the assailant expends the caught parcels with no sending. In any case, the aggressor runs the hazard that neighboring hubs will check and speak to the continuous assaults. There is a more sensitive type of these assaults when an assailant specifically forward parcels. An aggressor stifle or adjusts bundles beginning from a few hubs, while leaving the information from alternate hubs unaltered, which confines the doubt of its wrongdoing [6].

2.3 Gray Hole Attack

Gray Hole assault is an assault in which some specific information parcels are dropped by the malignant hub. Dark gap assault is harder to discover on account of a few information parcels achieved the goal and goal conceives that it is getting the full information.

Gray hole assault in steering convention happen at the season of directing the information parcel. In portable specially appointed system this sort of assault effectively happens because of dynamic nature of MANET. One of the significant issue about the dim opening assaults is that it misleads the source by publicizing that there is a legitimate and briefest way to the goal. In this way the noxious hub could do hurt the system by corrupting the system execution, exasperating course find process etc[7] .

A variety of dark gap assault is the dim opening assault, in which the hubs will drop the bundles specifically. Particular forward assault is of two kinds they are[8]
Dropping all UDP bundles while sending TCP parcels and Dropping half of the bundles or dropping them with a probabilistic conveyance. These are the assaults that try to disturb the system without being identified by the safety efforts.

Dim opening is a hub that can change from carrying on accurately to acting like a dark gap that is it is really an aggressor and it will go about as a typical hub. So we can't distinguish effectively the assailant since it carries on as a typical hub. Each hub keeps up a directing table that stores the following jump hub data which is a course bundle to goal hub. On the off chance that a source hub is in need to highway a parcel to the goal hub it utilizes a particular course and it will be checked in the steering table whether it is accessible or not. On the off chance that a hub starts a course disclosure process by communicating Route Request (RREQ) message to its neighbor, by getting the course ask for message the moderate hubs will refresh their steering tables for turn around course to the source. A course answer message is sent back to the source hub when the RREQ question achieves either to the goal hub or to whatever other hub which has a present course to goal. The dark gap assault has two stages:
Stage 1:A noxious hub misuses the AODV convention to publicize itself as having a legitimate course to goal hub, with the expectation of intruding on parcels of spurious course.
Stage 2: In this stage, the hubs has been dropped the interfered with bundles with a specific likelihood and the recognition of dim gap assault is a troublesome procedure. Typically in the dark gap assaults the assailant acts vindictively for the time until the point when the bundles are dropped and after that change to their ordinary conduct. Both typical hub and assailant are same. Because of this conduct it is elusive out in the system to make sense of such sort of assault. The other name for Gray opening assault is hub acting up assault [9].

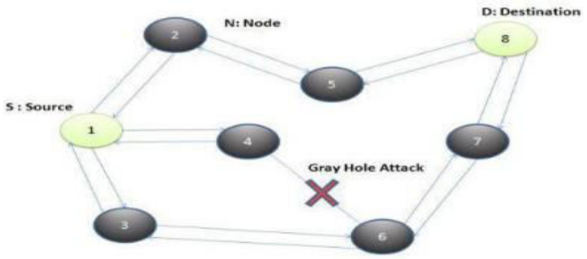


Fig 4: Gray Hole Attack

3. AODV ROUTING PROTOCOL

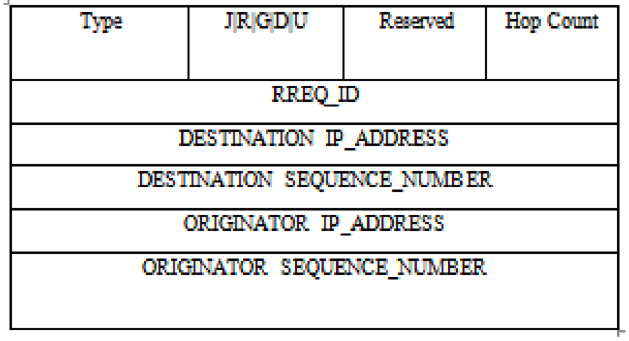
In Er. G. Singh et al. [10] presented two kinds of directing conventions receptive and proactive. AODV directing convention is a table driven steering convention that deals with the directing table to discover a course. It is intended for versatile impromptu systems with tens to thousands number of portable hubs .It is a responsive steering convention that sits tight for demands before endeavoring to locate the most ideal course from one node(source hub) to send messages to another hub (goal). The most ideal course is dictated by the separation or the quantity of bounces between hubs. Arrangement numbers at goal is utilized for circle opportunity.

3.1 Message Types in AODV

The AODV convention utilizes 4 sorts of messages to find, set up and keep up the courses. Route Request (RREQ), Route Reply (RREP), Route Error (RERR) and HELLO messages.

3.1.1 Route Request (RREQ): The source hub communicates a RREQ bundle to discover a course to the goal. Course ask for parcel (RREQ) organize is given in table.

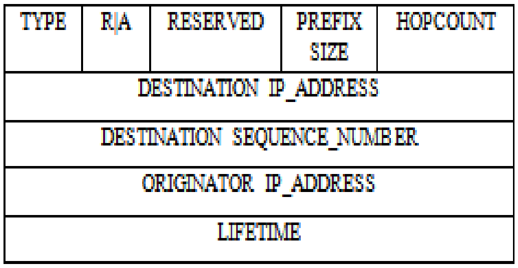
Table1: RREQ packet format



Type	J|R|G|D|U	Reserved	Hop Count
RREQ_ID			
DESTINATION IP_ADDRESS			
DESTINATION SEQUENCE_NUMBER			
ORIGINATOR IP_ADDRESS			
ORIGINATOR SEQUENCE_NUMBER			

3.1.2 Route Reply (RREP): Any hub having a new course jars unicast the RREP to the RREQ originator hub. The parcel arrangement of RREP is given in table:

Table 2: RREP packet format

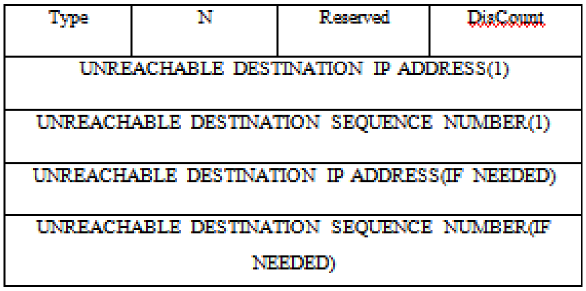


TYPE	R|A	RESERVED	PREFIX SIZE	HOPCOUNT
DESTINATION IP_ADDRESS				
DESTINATION SEQUENCE_NUMBER				
ORIGINATOR IP_ADDRESS				
LIFETIME				

3.1.3 Hello Messages Hubs keep up the course by checking the connection status of next jumps in dynamic courses by occasionally sending the HELLO messages. Hi message are not communicated to the system in light of the fact that these messages has TTL esteem 1.

3.1.4 Route Error Message (RERR): At the point when interface soften up a dynamic course is identified, a RERR message is sent to different hubs. The RERR has sign about every one of the courses that are utilizing that broken connection. RERR message contains:

Table 3: RERR packet format



Type	N	Reserved	DisCount
UNREACHABLE DESTINATION IP ADDRESS(1)			
UNREACHABLE DESTINATION SEQUENCE NUMBER(1)			
UNREACHABLE DESTINATION IP ADDRESS(IF NEEDED)			
UNREACHABLE DESTINATION SEQUENCE NUMBER(IF NEEDED)			

Every hub in arrange keeps a forerunner list which contains the IP address for every it neighbors that are probably going to utilize it as next bounce towards every goal.

3.1.5 Sequence Numbers

Arrangement numbers are utilized as a part of AODV to guarantee the course freshness. In AODV succession numbers are refreshed by the source hub when it produces another course demand to a goal or by the goal hub while it sends a course answer. On the off chance that the source hub gets more than one course answer messages for an asked for goal, the course to the goal hub with most noteworthy succession number is chosen .It guarantees the freshness of chose course. On the off chance that there are numerous course answer messages with same arrangement number at that point source hub will choose the course where jump tally is less.

3.2 Routing Table Management

Each hub in AODV keeps up a directing table. AODV does not keep up the whole course to the goal. Every hub just keeps up the following jump data, this lessens handling and capacity overhead to maintain courses. A hub refresh the directing table when it gets a control bundle, the steering table will be checked for presence of passage for that goal. On the off chance that no coordinating section for that goal is discovered, another table passage will be made. on the off chance that the steering table passage for the goal is available ,at that point the arrangement number for that goal will be refreshed if the control bundle refreshes the succession number for that goal if the parcel has grouping number higher than the goal succession number in the directing table. Directing table has nine fields as takes after:

i. Destination IP Address
ii. Destination Sequence number
iii. Valid Destination Sequence Number banner

iv. State and directing banners like legitimate, invalid, repairable, under repair
v. Network interface
vi. Hop Count (Source to Destination)
vii. Next Hop
viii. Precursor list
ix. Lifetime (course termination/cancellation time)

Alongside the source and goal grouping numbers the Route Request Expiration Timer and Route Caching Timeout are utilized to decide a course is as yet dynamic or not . The sections for hubs that are not on the source to goal course are viewed as invalid. A course remains substantial just for course reserving timeout all sections for courses not utilized for course storing timeout are negated. Rundown of antecedents is kept up keeping in mind the end goal to send the blunder nearby repair notices when next jump connect misfortune is found in a course. Antecedent rundown contains the rundown neighbor hubs to which a hub produces the course answer messages.

3.3 Route discovery

While correspondence courses between hubs are substantial, AODV does not assume any part. At the point when a source hub does not have sufficiently crisp course to the goal, it starts a course revelation process for the goal hub by communicating a RREQ message. A new course to goal is discovered when the RREQ achieves either to the goal or any middle of the road hub has sufficiently new course to the goal. Each middle of the road hub increases the bounces include esteem RREQ message by one.Any hub which has a course with more prominent succession number when contrasted with the arrangement number in the RREQ message is considered as new course .Reverse course is kept up to send back the RREP to the originator of RREQ by keeping up the antecedent rundown for the following jump from which a hub gets a RREQ message. Each middle hub when gets a RREQ message refreshes it goal grouping number if required. it peruses the address of hub from which it gets the RREQ from the RREQ message and refresh it with its own before sending it towards the goal. RREP message is unicasted to the source hub over the turn around course. The source to goal course is built up when the source hub get the RREP message. In the event that the source got more than one RREP messages then the RREP message with more noteworthy grouping number is considered.

3.4 Maintaining local connectivity

To keep up the nearby network among neighbor hubs Hello Messages are sent with TTL esteem set to 1. Each hub that is a piece of dynamic course ought to send HELLO messages to guarantee nearby network. On the off chance that a hub does not send Hello message or some other bundle for ALLOWED_HELLO_LOSS * HELLO_INTERVAL milliseconds, the neighboring hub will consider the connection to that hub is lost . Hi bundles are sent just when the neighboring hubs are not sending any parcels.

4. Proposed Algorithm

Here, a network with n nodes is given. Route[] is an array contains the nodes in the path from source node to destination node. There c[] is the array denotes number of packets received at particular node in the network and similarly send[] represents number of packets forwarded to the other nodes. h is the number of hops in the route from the source to destination. S is the source and D is the destination.

```
For I =1 to h
    If route[i]==S || route[i]==D
        Forwardingratio[i]=0
    else
        Forwardingratio[i]= send[route[i]/ rec[route[i]
    End if
end
Max=forwarding ratio[1]
Min=forwarding ratio[1]
Nodepostion=1
Nodepostion1=1
For i=2:h
    If forwardingratio[i]>Max
        NodePosition=i
    If forwardingratio[i]<Min
        NodePosition1=i
    If(f[NodePosition]==NRTE)
        Max=forwardingratio[i]
    End if
    If(f[NodePosition1]==NRTE)
        Min=forwardingratio[i]
    End if
If Max >th
    Attacked_node=max[Nodeposition]
End if
if min <th
    Attacked_node=max[Nodeposition1]
end if
End
```

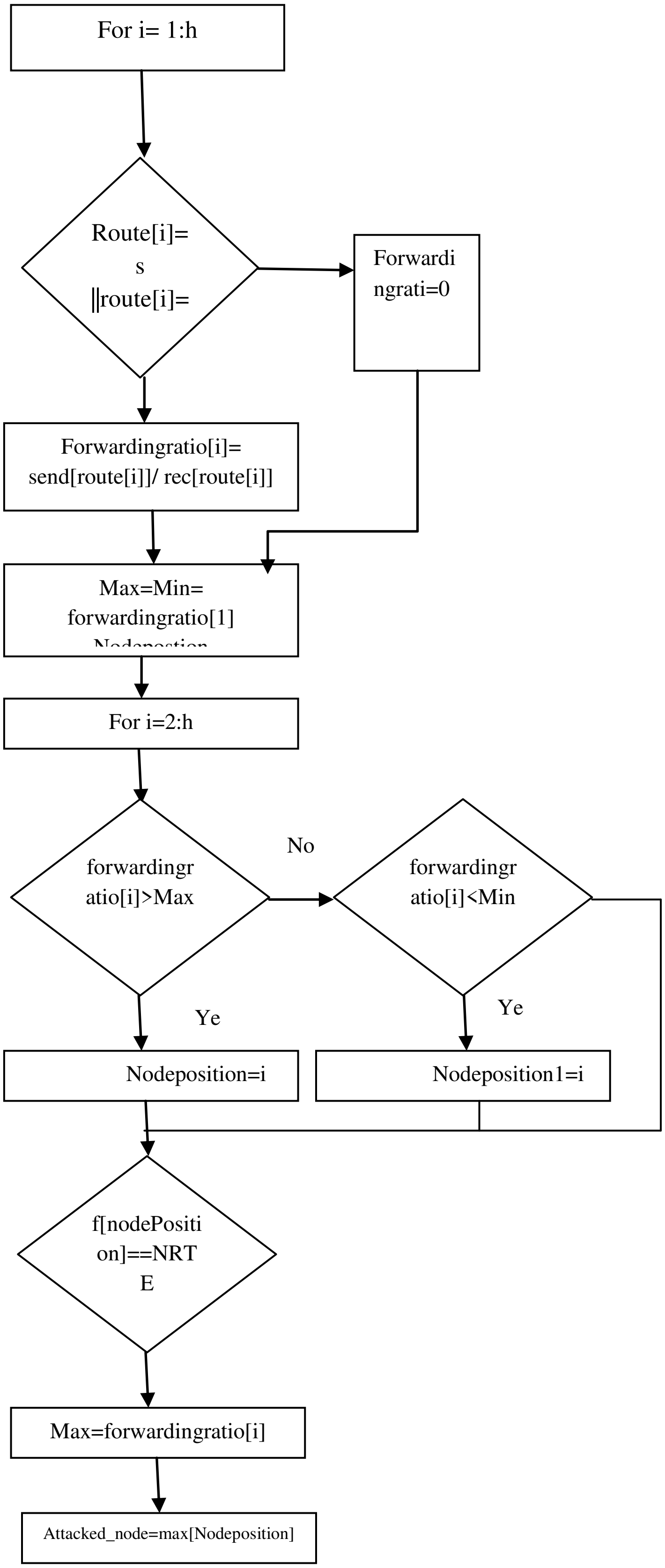


Fig 5: Flow chart of proposed work

The flowchart for the algorithm described above. This algorithm is implemented using the NS2.

5. RESULTS

AODV, EAODV and IAODV(proposed) are compared using a ad-hoc network scenarios with varying the number of nodes on the basis of various parameters like PDR, delay and throughput. Performance degradation because of the attack is shown in the given tables:

Table 4: Performance of AODV routing protocol with different number of nodes

No of nodes	PDR	Delay(ms)	Throughput(kbps)
10	42.510	6.351	63.45
20	42.702	6.313	63.51
30	27.455	6.204	33.55
40	28.187	6.184	34.15

Table 4 shows the analysis results of performance of AODV routing protocol. The performance is measured with pdr, Delay and Throughput.

Table 5: Performance of EAODV routing protocol for different number of node.

No of nodes	PDR	Delay(ms)	Throughput(kbps)
10	42.520	6.348	63.49
20	42.398	6.366	63.29
30	29.856	6.049	37.83
40	28.956	6.084	35.43

In Table 5 the analysis results of performance of EAODV protocol with the same parameters used to analyze the performance of AODV protocol is shown. The minute improvement is observed as the existing protocol is able to handle the black hole attack only.

Table 6: Performance of IAODV routing protocol with different number of nodes

No of nodes	PDR	Delay(ms)	Throughput (kbps)
10	49.919	4.99	86.58
20	49.98	5.26	80.67
30	49.955	5.249	80.67
40	49.90	5.216	79.36

Table 6 show the analysis of the IAODV protocol on the same network and same parameters as of the previous

protocols. The performance improvement can be analyzed as the protocol is able to handle the two type of blackhole as well as gray hole attack. The analysis can be graphically as follow:
Packet Delivery Ratio: It is the ratio of number of packet delivered to the number of packet generated.

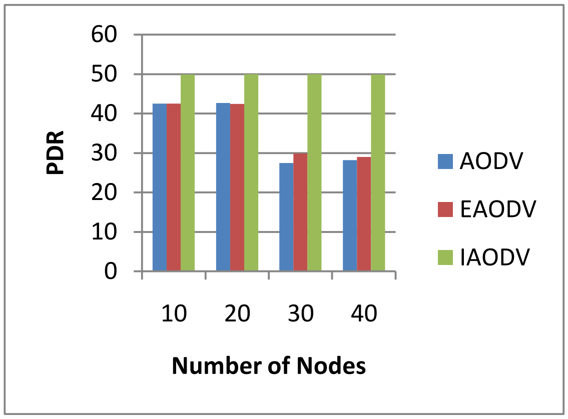


Fig 6: Comparison Graph for PDR between IAODV, EAODV and AODV

The fig. 6 shows the performance difference between AODV, EAODV and IAODV based on the PDR parameter. In this figure the PDR is low in the case of with attack for AODV, EAODV while IAODV shows the proper performance.

a) Average End to End Delay

The average time taken by a data packet to arrive in the destination and it also includes the delay caused by route discovery process and the queue in data packet transmission.

∑ (arrive time – send time) / ∑ Number of connections

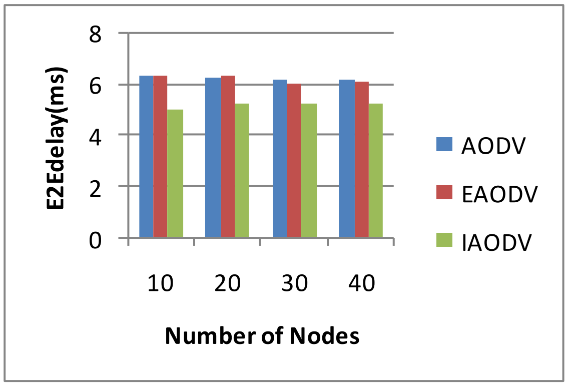


Fig 7: Comparison Graph for average end to end delay (ms) between WRP and AODV

The given fig 7 shows the performance degradation in case of Wormhole attack based on the end-to-end delay Ratio matric. The result of end to end delay ratio is high with attack as compared to normal AODV communication.

b) Throughput

The amount of data transferred in a specified amount of time i.e. average number of bits delivered per second(Kbps)

Throughput =(Packet Size/(stopTime-startTime))*(8/1000)

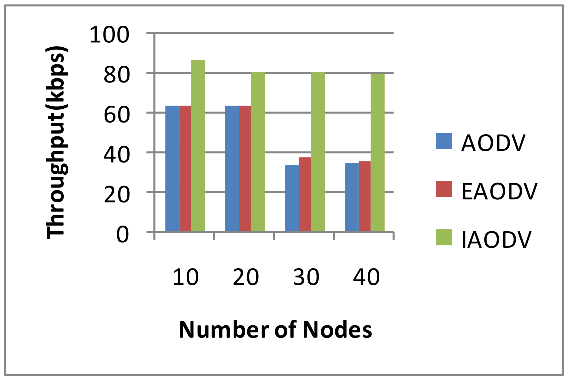


Fig 8: Comparison Graph for throughput (kbps) between WRP and AODV

The figure 8 shows the performance degradation in case of EAODV in comparison with IAODV on the basis of throughput metric. In this figure the throughput is high in the case of IAODV in the comparison of EAODV with wormhole attack.

6. CONCLUSION

The black hole and gray hole attack degrades the performance of the network. This degradation is analyzed in this work. The attack is implemented in the network over AODV routing protocol. The comparison between the performance of network for protocol AODV, EAODV and IAODV is done using the parameters throughput, delay and pdr by varying number of nodes. The algorithm developed for the detection of attack doesn't need any hardware and detects the attacked node only by trace file. The performance of IAODV protocol is better as compared to the existing protocols. In future following work can be done. The proposed algorithm can be extended for the prevention process. It extended for the sinkhole and other network layer attacks. It can be implemented for the wireless mesh network.

REFERENCES

[1] Yang, Hao, et al. "Security in mobile ad hoc networks: challenges and solutions." Wireless Communications, IEEE 11.1 (2004): 38-47.

[2] Ghonge, Mangesh, and S. U. Nimbhorkar. "Simulation of AODV under Blackhole Attack in MANET." International Journal 2, no. 2 (2012).

[3] V. Shanmuganathan, "A Survey on Gray Hole Attack in MANET", Vol.2, No6, December 2012.

[4] Rai, Abhay Kumar, Rajiv RanjanTewari, and Saurabh Kant Upadhyay. "Different types of attacks on integrated MANET-Internet communication." International Journal of Computer Science and Security 4.3 (2010): 265-274.

[5] David B. Johnson and David A. Maltz. "Dynamic Source Routing in Ad Hoc Wireless Networks". In Mobile Computing, edited by Tomasz Imielinski and Hank Korth, chapter 5, pages 153–181. Kluwer Academic Publishers, 1996

[6] Revathi, B., and D. Geetha. "A Survey of Cooperative Black and Gray hole Attack in MANET." International Journal of Computer Science and Management Research 1.2 (2012).

[7] 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: 1-16

[8] V. Shanmuganathan, "A Survey on Gray Hole Attack in MANET", International Journal of Computer Networks and Wireless Communications (IJCNWC), ISSN: 2250-3501 Vol.2, No6, December 2012

[9] V. Solomon Abel, "Survey of Attacks on Mobile Ad-Hoc Network" IJCSE, Vol.3, No.2, Feb 2011

[10] Er.GurjotSingh,Er.GurpreetKaur"Analyzing the Impact of Wormhole Attack on Routing Protocol in Wireless Sensor Network on Behalf of packet tunnel, dropped and intercepted" pp.42-48 ,IJEDR 2013.