International Journal of Advanced Trends in Computer Applications
www.ijatca.com

Enhanced Utilization of GA to limit the Effect of Black hole Attack in MANET

[1]**Harpreet Singh Brar**
M. Tech student Baba Banda Singh Bahadur Engg. College
Fatehgarh Sahib, India
[2]**Harpreet Kaur Mavi**
Asst. Professor Department of Electronics and Communication Engg.
Baba Banda Singh Bahadur Engg. College Fatehgarh Sahib, India

Abstract: *In recent years, MANETs has become a quite interesting research area amongst various researchers because of their flexibility and independence of network infrastructures, such as base stations. At present, numerous efficient routing protocols have been anticipated for MANET. Many protocols take on a reliable & co-operative environment. However, when malicious-nodes are present, the networks are penetrable to numerous kinds of attacks. In MANET, routing-attacks are peculiarly quite serious. It has many potential-applications which are in completely un-predictable as well as dynamic environment. Routing protocol used here is a form of reactive-routing protocol entitled as AODV. This routing protocol routes is based on demand. The most significant benefit of Ad-hoc On Demand Vector protocol is smallest connection-setup-delay & assignment of specific sequence numbers to destination to identify the latest route. In specification based IDS, definite characteristics of vital-objects are investigated as well as any abnormality is detected. So, this paper the proposed work tries to design and implement Mobile Ad-hoc Networks in AODV protocol. It has been observed that black hole attack prevention has been done using genetic algorithm at good rate.*

.

Keywords: *MANET, AODV, Genetic Algorithm, Security.*

I. INTRODUCTION

In recent years, the research-work is done on MANETs has drawn huge interest of scholars as a result of the understanding of the nomadic computing model [1]. A MANET, as per its name proposes, it is a self-configuring network of MANETS as well as mobile devices which usually encompass a network proficient of vigorously varying topology. The network nodes present in a MANET, they not only act as a type of conventional network nodes but then correspondingly as the routers intended for several other sort of peer devices [2]. The dynamic topology had absence of a stable infrastructure in addition to its wireless-nature which make MANET networks more susceptible towards several kind of security attacks. And in addition to that, as a result of the inherent property, huge constraints in storage, power, as well as computational resources in the mobile adhoc network nodes, which are integrating wide-ranging security procedures against such kind of attacks which is correspondingly non-trivial. Consequently, the old-style security procedures as well as rules/protocols – by comprising those intended for the wired networks which are not applicable directly as well as it might need a cautious relook [2].

We also try to reconsidering various kind of routing protocols which could possibly be applicable in MANETs. In this research and investigation work whether it is conceivable to fortify the prevailing attempts on developing much more protected routing protocols intended for MANETs. The routing protocols are mainly vulnerable in mobile adhoc networks as a consequence of the huge dependence on the supportive routing processes which are employed for forming some specific network routes, by means of primary assumptions regarding the purity of that specific peer network node. The network layer in MANET Networks is quite susceptible to numerous attacks as a consequence of snooping by way of using a malevolent intent, spoofing some specific control and data packages handled, malicious alteration of the package matters as well as the Denial-of-service attacks, Wormhole attacks, Sinkhole attacks, Black hole attacks [3].Amongst these, we tried to examine and improving the safety of the AODV routing protocol [4] contrary to any kind of Black hole attacks. Further in literature survey, we have given several past attempts that suggest a secure form of

AODV towards avoiding the Black hole attacks on the network. Though, as per our point of view, not any of the suggested attempts defends AODV from the Blackhole Denial of Service attacks.

The network layer in Mobile Adhoc Networks is vulnerable to several attacks as a result of snooping by way of using a malevolent intent, spoofing some specific control and data packages handled, malicious alteration of the package matters as well as the Denial-of-service attacks, Wormhole attacks, Sinkhole attacks, Black hole attacks. The routing protocols of MANET are unprotected and henceforth come about into the system with the noxious malicious nodes in the system e.g. DSR, OLSR, AODV, etc. Amongst these, we tried to examine and improving the safety of the AODV routing protocol [5].

In this paper, we will focus on the AODV routing protocol to identify black hole attack. In this routing protocol the route discovery mechanism is used to transmit packets from one mobile node to other that will help to find malicious nodes in the black hole attack. In order to avoid such route discovery mechanism each time when the packet is transmitted, the routing technique is used. Then black hole nodes will be optimized using genetic algorithm in AODV environment using parameters like end delay, packet delivery ratio, throughput and error rate.

1.1 Intrusion Detection

Interference finding is intended to monitor the wicked activities occurring in a computer system or network within or outside and analyse them for signs of possible incident, which are violation or approaching threats of violation of computer security policies, satisfactory utilized policies, or paradigm security practices. Interruption incidents to computer systems are growing because of the commercialization of the internet and local networks and new automated hacking tools [6]. Computer systems are turning out to be more and more vulnerable to attack, due to its extensive network connectivity. Nowadays, networked systems play a more and more significant role in our society and its economy. They have become the targets of a wide array of duplicate attacks that invariably turn into actual intrusions. This is the cause computer security has become a necessary concern for network administrators. Too often, intrusion cause havoc inside LANs and the time and cost to restore the damage can grow to extreme scope. Instead of using passive measures to fix and patch security holes once they have been oppressed, it is more effective to adopt a proactive come near to intrusions.

1.2 Black Hole Attack

In a black hole attack, a malicious node sends fake routing data, appealing that it has a most favorable route as well as causes other good nodes to route data packets through the malicious one [7].

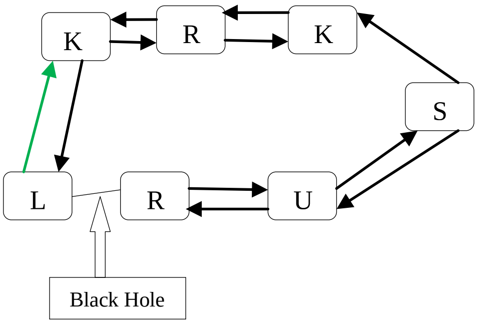

Figure 1: Black Hole Attack

1.3 Genetic Algorithm

Genetic algorithm (GA) is a stochastic seek strategy that will mimics the actual healthy advancement offered by simply Charles Darwin throughout 1858. GA has been effectively given to a variety of combo issues. It truly is patterned typically around the ideas from the advancement via healthy assortment, using an individual of folks that will keep on the choice course of action in terms of variation-inducing operators such as mutation as well as recombination (crossover). An exercise function is utilized to gauge individual, as well as reproductive system achievement ranges with fitness [8].

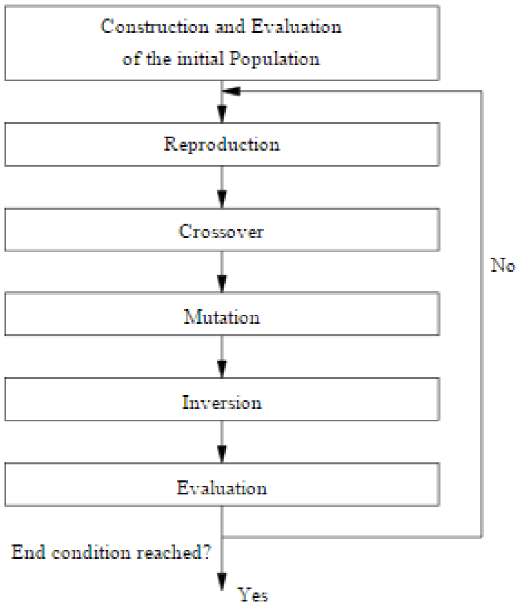

Figure 2: Genetic Algorithm

Initialize random population consists of chromosomes.

Compute fitness function in the population.

Develop new population consists of individuals.

Selection of parent chromosomes to get best fitness function.

Perform crossover to get copy of parents.

Perform mutation to mutate new offspring's.

Place new offspring into population.

Repeat steps to get satisfied solution.

Stop.

II. RELATED WORK

Sunil Taneja et.al, [9]described by Mobile Ad-hoc Network is set of multi-hop wireless mobile nodes that converse with each other without central manage or recognized communications. The wireless relations in this network are very error horizontal and can go down often due to mobility of nodes, intrusion and less transportation. Therefore, routing in MANET is a grave task due to highly active environment. In recent years, some routing protocols have been planned for mobile ad-hoc networks and important among them are DSR, AODV and TORA. This research paper provide a summary of these protocols by present their characteristics, functionality, benefits and borders and then makes their relative analysis so to evaluate their show.

SoufieneDjahel et.al, [10]made a comprehensive survey investigation on the state-of-art counter measures to deal with packet dropping attack. Furthermore, author examine the challenges which will remain to be undertaken by the researchers for purpose of constructing an in-depth defense against such a sophisticated attack.

Fan-Hsu et.al, [11]surveyed the prevailing-solutions and also deliberate the state-of-art of routing-mechanisms. The author not only categorise these proposals into a specific black-hole-attack as well as collaborative-black-hole-attack but then also analyze the categories of these solutions and provide a comparison table. It was expected to furnish more researchers with a detailed work in anticipation.

ShekharTandan et.al,[12]proposed PDRR method to detect the black hole attack in MANET with AODV protocol. An introduction of black hole in MANET with QUALNET 5.0 is done, after applying the detection technique result reflects the performance de-gradation. This paper presented a detection analysis with black hole attack by using AODV routing-protocol in dissimilar-scenario. This examination is performed in wireless ad-hoc network.

Shanmuganathan et.al,[13]described that Mobile Ad-hoc Network is used the majority generally all around the world, because it has the aptitude to converse each other lacking any set network. It has the leaning to take decision on its own that is independent state. MANET is generally known for transportation less. The bridge in the network are usually known as a base station. A united security solution is very a lot needed for networks to protect both route and data forward operation in the network layer. Refuge is an important requirement in MANET. Lacking any proper safety solution, the hateful node in the network will act as a usual node which causes attic is tumbling and choosy forwarding attack normally known as gray whole attack. In this paper we survey about the diverse types of attacks occur in the network layer in MANET. Gray Hole attack is one of the attacks in net layer which comes under security active attacks in MANET.

SapnaGambhir et.al,[14] proposed a routing security issues in MANETs are discussed in general, and in particular the malicious node attack has been described in detail. A security protocol has been proposed that can be utilized to identify malicious nodes in a MANET and thereby identify a secure routing path from a source node to a destination node avoiding the malicious nodes.

EiEiKhin et.al, [15] analyzed the impact of black hole attack on Ad-hocOn-Demand Distance Vector (AODV) protocol. The simulation is carried on NS-2 and the simulation results are analyzed on various network performance metrics such as packet delivery ratio, normalized routing overhead and average end-to-end delay. In this paper, we have analyzed the effect of black hole attack in the performance of AODV protocol.

GayatriWahane, Ashok M. Kanthe, Dina Simunic et.al, [16] proposed a work thatused a modified AODV and used a technique for detecting a cooperative black hole attack using crosschecking with the True - Link concept. True-Link is a timing based countermeasure to the cooperative black hole attack.

III. IMPLEMENTATION OF GENETIC ALGORITHM FOR BLACK HOLE ATTACK PREVENTION

Step: 1 Initialize Mobile Ad-hoc Network
Step: 2 Enter height of network.
Step: 3 Enter width of network
Step: 4 Enter nodes of network
Step: 5 Enter number of rounds for the network.
Step: 6 Initialize AODV protocol in network.

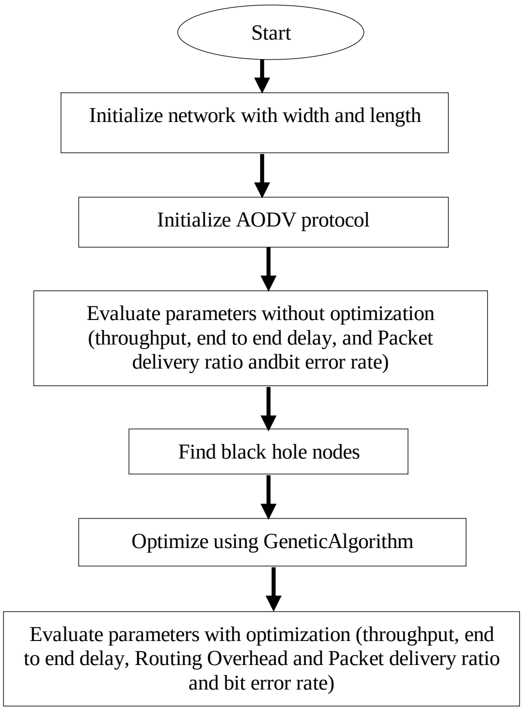
Start
Initialize network with width and length
Initialize AODV protocol
Evaluate parameters without optimization (throughput, end to end delay, and Packet delivery ratio andbit error rate)
Find black hole nodes
Optimize using GeneticAlgorithm
Evaluate parameters with optimization (throughput, end to end delay, Routing Overhead and Packet delivery ratio and bit error rate)

Figure 3: Proposed Work Flowchart

Step: 7 Searching of attack in memory.
Step: 8 Searching in Cache memory.
Step: 9Attack found in network.
Step: 10 Evaluate Parameters.
Step: 11 Apply Genetic Algorithm for optimization using fitness function.
Step: 12 Select best route until best fitness function has not been attained.
Step: 13 Evaluate parameters.
Step:14 Measure Error rate, Throughput, packet delivery ratio and end delay using GA and without GA.

IV. RESULTS AND IMPLEMENTATION

4.1 Computation Parameters

4.1.1 Throughput

The second parameter is throughput; it is the ratio of total amount of data which reaches the receiver from the sender to the time it takes for the receiver to receive the last packet. It is represented in Kbps. In WANETs throughput is affected by various changes in topology, limited bandwidth and limited power. Unreliable communication is also one of the factors which adversely affect the throughput parameter.

4.1.2 Bit Error Rate

The bit error rate (BER) is the number of bit errors per unit time. The bit error ratio (also BER) is the number of bit errors divided by the total number of transferred bits during a studied time interval. BER is measured in Decibel (db).

4.1.3 End-to-End Delay

The packet end-to-end delay is the average time in order to traverse the packet inside the network. This includes the time from generating the packet from sender up till the reception of the packet by receiver or destination and expressed in milli seconds (ms). This includes the overall delay of networks including buffer queues, transmission time and induced delay due to routing activities. Different application needs different packet delay level. Packet Delivery Ratio

The ratio of packets that are successfully delivered to a destination compared to the number of packets that have been sent out by the sender.

Routing Overhead

We know that routing protocol operates on the topology. We simulate a project with 130 nodes, and estimate the routing overhead for least cost path routing between source node and destination node.

4.2 Analysis

Table 1: Simulation Parameters

Property	**Value**
Routing Protocols	AODV
Area Covered(AODV)	1000*1000m
No. of Nodes	130
Observation Parameters	Throughput, Error Rate, End-to-End Delay , Routing Overhead and Packet Delivery Ratio
Network Simulation	MATLAB
Optimization technique	GA
No. Of Data Transfer	5
Population Size	50

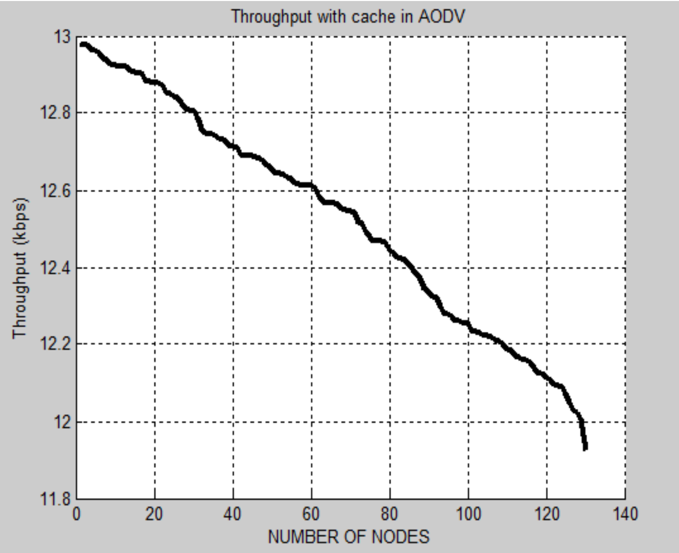

Figure 4: Throughput in AODV

Throughput of AODV routing protocol without optimization is shown in above figure. As we know that high the throughputs better the performance of network. But without any optimization throughput for AODV has found to be very low.

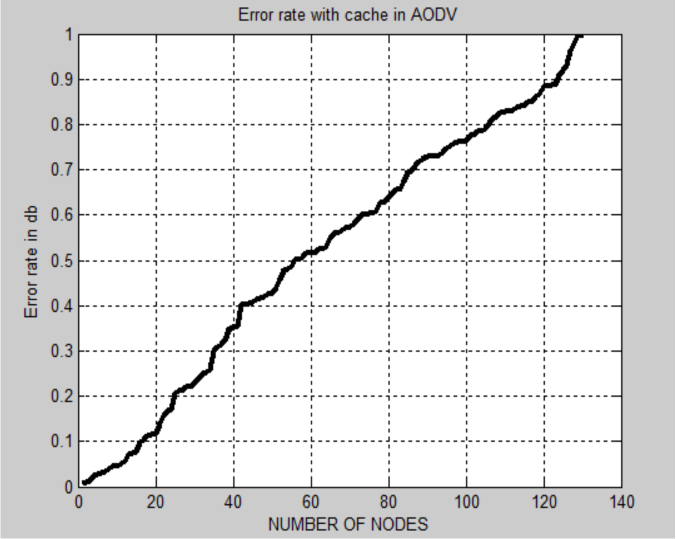

Figure 5: Error Rate in AODV

Bit Error rate of AODV routing protocol without optimization is shown in above figure. As we know that less the bit error rate better the performance of network. But without any optimization technique error rate for AODV has found to be 0.13 db.

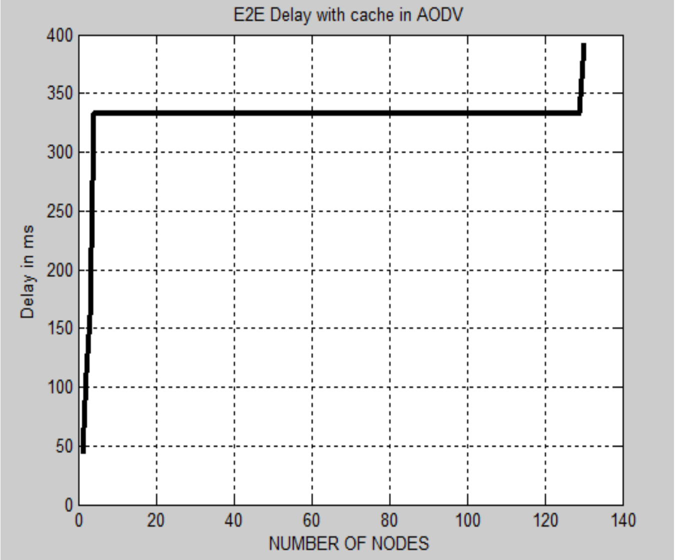

Figure 6: End to end Delay in AODV

End to end delay of AODV routing protocol without optimization is shown in above Figure. As we know that less the end delay better the performance of network. But without any optimization technique end delay for AODV has found to be 7.5 ms.

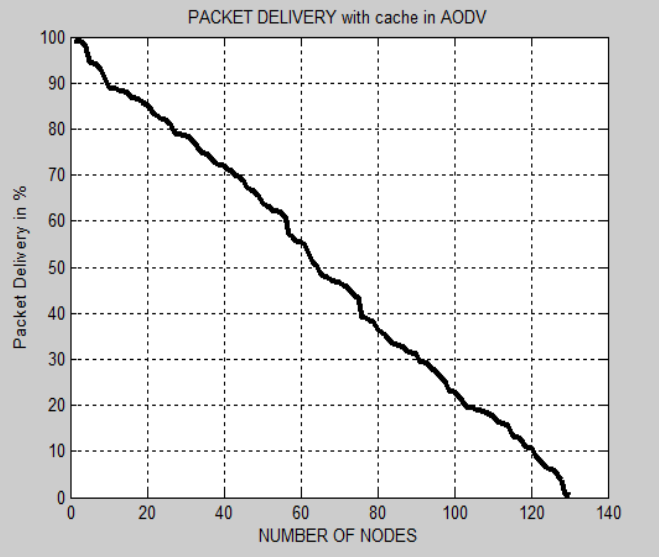

Figure 7: Packet Delivery Ratio in AODV

In above figure it shows packet delivery ratio of the network with AODV protocol. As per above figure it shows that packet delivery ratio degrades/ drops as rounds of data transfer increases. A good network needs a good packet delivery ratio.

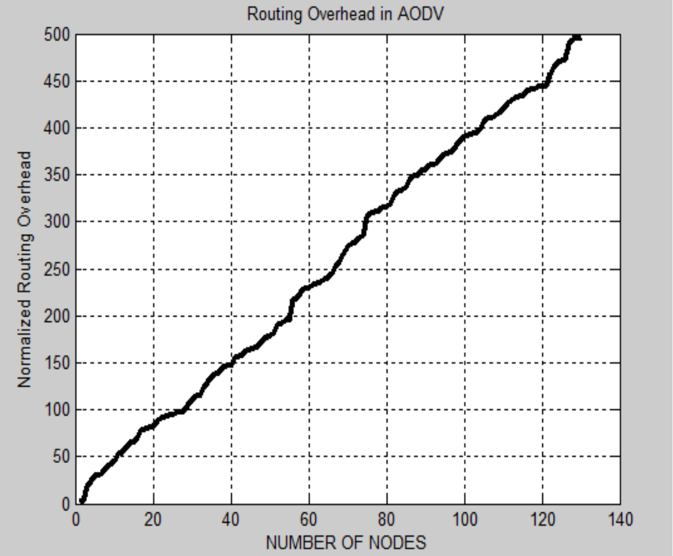

Figure 8: Routing Overhead in AODV

In above figure it shows Normalized Routing Overhead of the network with AODV protocol. As per above figure it shows that Normalized Routing Overhead is less in AODV protocol.

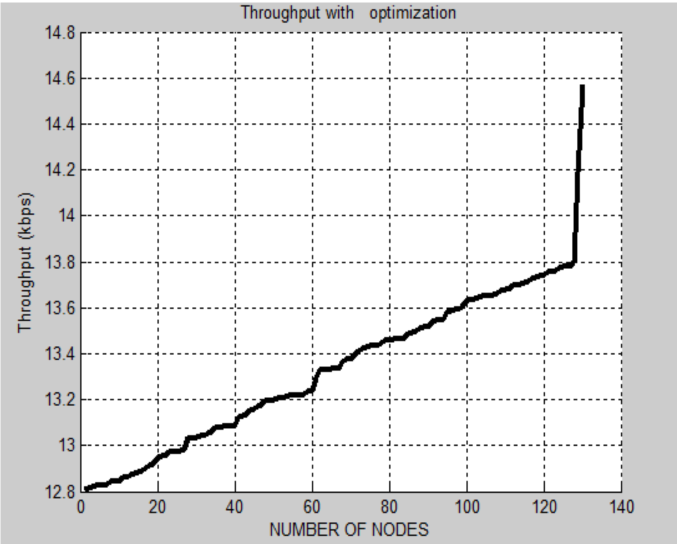

Figure 9: Throughput with GA

In figure above figure, the maximum throughput value is .1 with optimization but after using GA the maximum value is 15. Each iteration percentage value after optimization increases from its previous percentage value. Higher the throughput betters the performance.

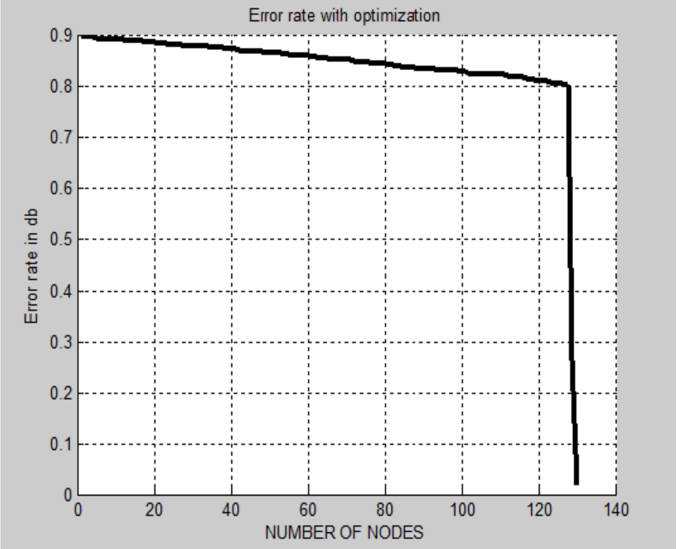

Figure 10: Error Rate with GA

In the above figure, the bit error starts decreasing slowly when an attack occurs that affect the nodes, and we observe that the using GA as optimization method gives better performance in terms of error rate. The maximum BER with attack is 1 db and after optimization the maximum BER value is 0.88db.

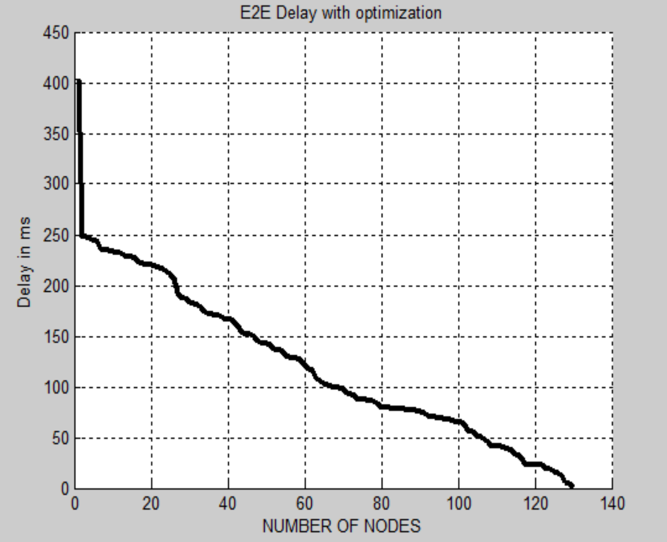

Figure 11: End to End Delay with GA

In above figure, the end-to end delay is very harmful for the performance of nodes during attack but after implementation of GA results are very effective for the network. From the results it has been shown that it is 0.84ms at 5node round that is much better than in the presence of the attack.

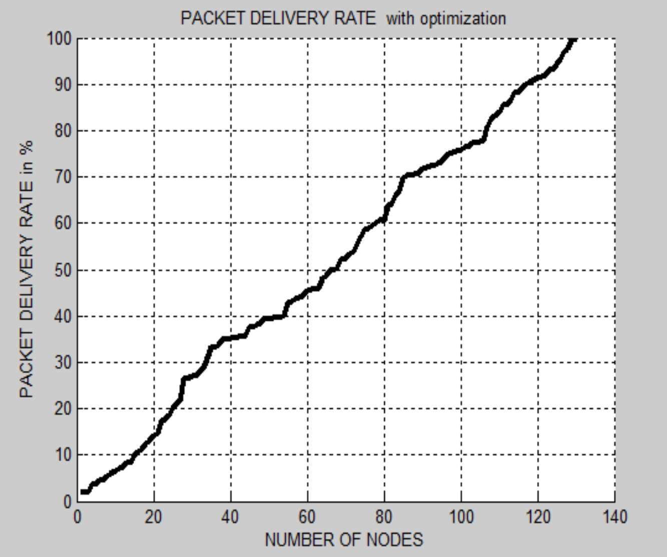

Figure 12: Packet Delivery Ratio with optimization

In above figure, the packet delivery ratio is very beneficial for the performance of nodes during attack but after implementation of GA results are very effective for the network. The packet dropping ratio decreases and packet delivery ratio increases simultaneously. From the results it has been shown that 87% of packet delivery ratio at round 5that is much better than in the presence of the attack.

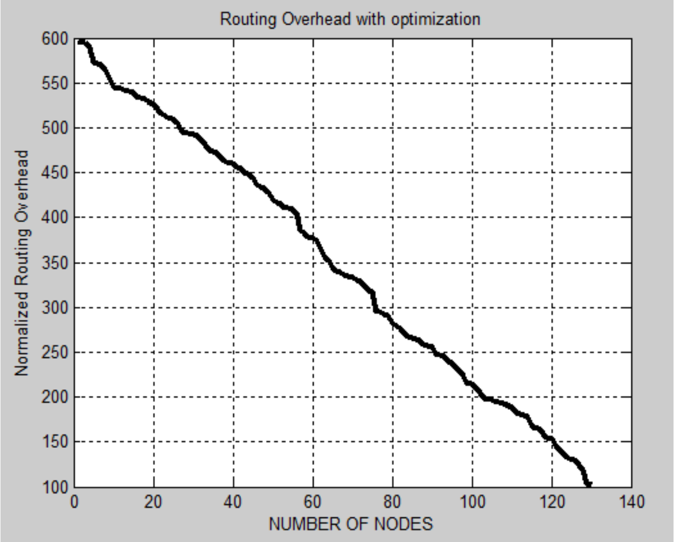

Figure 13: Routing Overhead with GA

In above figure it shows Normalized Routing Overhead of the network with GA protocol. As per above figure it shows thatNormalized Routing Overhead is more in GA protocol according to the Nodes.

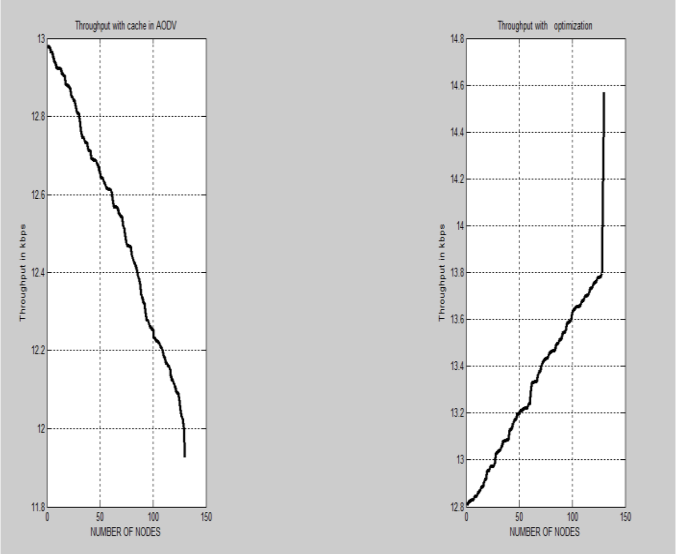

Figure 14: Comparison graph of throughput without and with optimization

In above graph, we have shown the comparison between throughput result parameter with cache in AODV and throughput with optimization. In this as we can see result value of Throughput parameter improves after applying GA optimization algorithm on the network even after facing the attack.

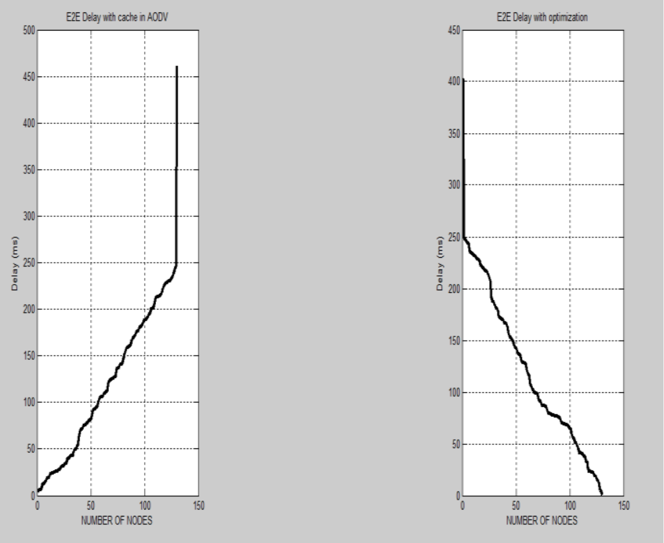

Figure 15: Comparison graph of End to end Delay without and with optimization

In above graph, we have shown the comparison between End to End Delay result parameter with cache in AODV and End to End Delay with optimization. In this as we can see result value of End to End Delay parameter improves after applying GA optimization algorithm on the network even after facing the attack.

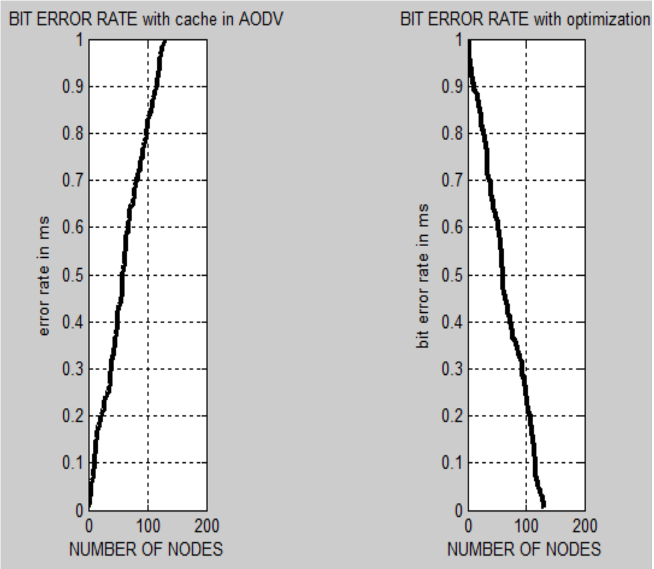

Figure 16: Comparison graph of Bit Error Rate without and with optimization

In above graph, we have shown the comparison between Bit Error Rate result parameter with cache in AODV and Bit Error Rate with optimization. In this as we can see result value of Bit Error Rate parameter improves after applying GA optimization algorithm on the network even after facing the attack.

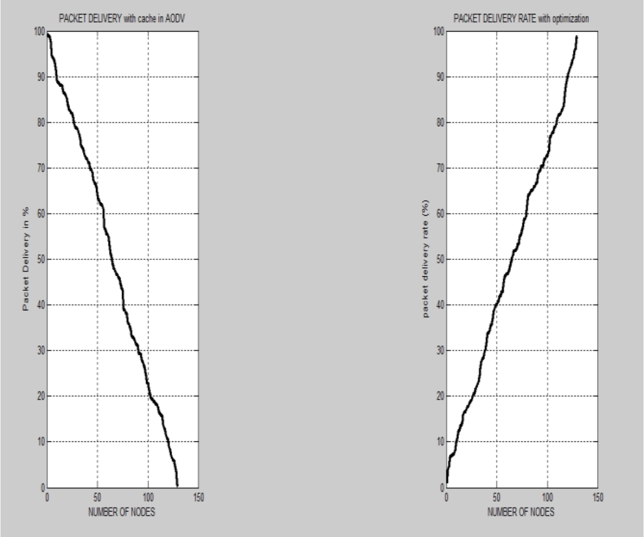

Figure 17: Comparison graph of Packet Delivery Rate without and with optimization

In above graph, we have shown the comparison between Packet Delivery Rate result parameter with cache in AODV and Packet Delivery Rate with optimization. In this as we can see result value of Packet Delivery Rate parameter improves after applying GA optimization algorithm on the network even after facing the attack.

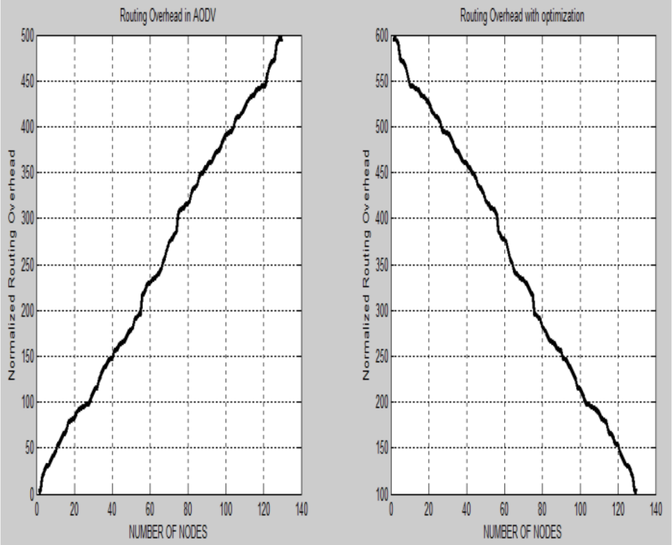

Figure 18: Comparison graph of Normalized routing overhead without and with optimization

In above graph, we have shown the comparison between Routing Overhead result parameter with cache in AODV and Routing Overhead with optimization.

COMPARISON GRAPH

Table 2: Comparison between parameters

Parameters	Without GA	With GA
Average End delay	340	85
Average Throughput	12	13.3
Average Error Rate	0.9	0.1
Average Packet Delivery Rate	82	87
Normalized Routing Overhead	500	400

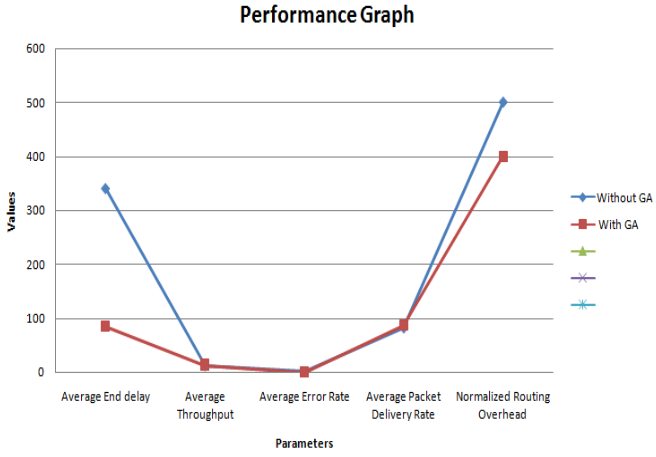

Figure 19: Comparison with and without Genetic algorithm

In above graph, we have shown the comparison using result parameters such as End delay, throughput, and error rate. As, we can see after applying GA optimization algorithm it improves overall results of the system.

V. CONCLUSION AND FUTURE SCOPE

In this work, the issues related to security and the loopholes of AODV protocol, has been studied specific to the network layer attacks such as packet drop Attack. An Intrusion Detection System (IDS) is implemented using Genetic Algorithm and tested with networks of varied node configurations. The proposed work gives an approach for secure routing algorithm AODV in black-hole attack in MANETs. Delivering data to the base station is very important in real time applications. By having so much base stations it must be very important to have delivery of data from source to destination in the presence of blackhole attack. So this work has concluded that utilization of genetic algorithm leads to high rate of throughput. The performance of the system has been analysed via various parameters using GA and without GA. In the end it has been concluded that using genetic algorithm optimization has been achieved at good rate.

Future scope lies in the use of the hybridisation of Genetic algorithm with other routing protocols like DSR or DSDV. As they are also vulnerable to this type of attacks.

REFERENCES

[1] Mani Arya, “BFO Based Optimized Positioning For Black Hole Attack Mitigation in WSN”, International Journal of Engineering Trends and Technology (IJETT) – Volume 14 Number 1 – Aug 2014.

[2] Mohammad Wazid, AvitaKatal, Roshan Singh Sachan, R H Goudar and D P Singh, “Detection and Prevention Mechanism for Blackhole Attack in Wireless

Sensor Network", International conference on Communication and Signal Processing, IEEE, pp. 576- 581, 2013.

[3] K.S.Sujatha1, Vydeki Dharmar2, R.S.Bhuvaneswaran3, "Design of Genetic Algorithm based IDS for MANET", IEEE, pp. 28-35, 2012.

[4] MeenakshiTripathi,M.S.Gaur,V.Laxmi, "Comparing the Impact of Black Hole and Gray Hole Attack on LEACH in WSN", The 8th International Symposium on Intelligent Systems Techniq, Procedia Computer Science, pp.1101 – 1107, 2013.

[5] Adnan Nadeem and Michael Howarth, A Generalized Intrusion Detection &Prevention Mechanism for Securing MANETs, International Conference on Current Trends in Engineering and Technology, pp. 35-40, 2009 .

[6] Zhao Min, Zhou Jiliu, "Cooperative Black Hole Attack Prevention for Mobile Ad-hoc Networks", International Symposium on Information Engineering and Electronic Commerce, pp. 26-30, 2009.

[7] Noor M. Asraf, Raja N. Ainon, PhangKeatKeong, " QOS parameter Optimization using Multi-Objective Genetic Algorithm in MANET", 2010 Fourth Asia International Conference on Mathematical/Analytical Modelling and Computer Simulation, pp. 138-143, 2010.

[8] Sunil Taneja and Ashwani Kush," A Survey of Routing Protocols in Mobile Ad-hoc Networks", International Journal of Innovation, Management and Technology, vol. 1, no. 3, pp. 279-285, 2010.

[9] SoufieneDjahel, FaridNaıt-abdesselam , and Zonghua Zhang, Mitigating Packet Dropping Problem in Mobile Ad-hoc Networks", IEEE communications surveys & tutorials, vol. 13, no. 4, pp. 658-672, 2011.

[10] Fan-Hsu n Tseng1 , Li-Der Chou1 and Han-Chieh Chao et. al (2011), A survey of black hole attacks in wireless mobile ad-hoc networks , IEEE Interntional conference, pp. 25-30, 2011.

[11] ShekharTandan and PraneetSaurabh, A PDRR based detection technique for blackhole attack in MANET, (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 2 (4) , pp. 1513-1516, 2011.

[12] Shanmuganathan And Mr.T.Anand ," A Survey on Gray Hole Attack in MANET", IRACST – International Journal of Computer Networks and Wireless Communications (IJCNWC),vol.2, no. 6, December 2012, pp. 647-650, 2012.

[13] SapnaGambhirSaurabh Sharma, "PPN: Prime Product Number based Malicious Node Detection Scheme for MANETs", 3rd IEEE International Advance Computing Conference (IACC), pp. 335-340, 2013.

[14] EiEi Khin1 and ThandarPhyu (2014), Impact of black hole attack on aodv routing protocol, IEEE Conference on Computers and electronics applications, pp. 66-70, 2014.

[15] Sandeep Kumar Arora, MubashirYaqoobMantoo, MahnazChishti, NehaChaudhary, 5th International Conference- Confluence The Next Generation Information Technology Summit, pp. 406-410, 2014.

[16] G. D. Wahane, A. M. Kanthe, D. Simunic," Technique for detection of cooperative black hole attack using truelink in mobile adhoc networks", MIPRO 2014, IEEE Conference,Opatija,Croatia.