International Journal of Advanced Technology in Engineering and Science
Vol. No.3, Special Issue No. 01, November 2015
www.ijates.com
ijates
ISSN 2348 - 7550

EVOLUTIONARY ALGORITHM BASED APPROACH FOR GRAY HOLE ATTACK PREVENTION IN WSN

Jaspreet Kaur [1], Vishal Walia[2]

[1]*Student , RIEIT, Railmajra, Ropar (India)*

[2]*Associate Professor and Dean Academics, RIEIT, Railmajra. Ropar (India)*

ABSTRACT

The deployment of gray hole attack leads to various types of attacks. This paper provides an overview of AODV the most popular routing algorithm of WSN and how AODV will be comprised of gray hole attack. Routing concept along with fitness function of genetic algorithm has been used in this work. The performance of WSN has been checked using genetic algorithm as well as without genetic algorithm. It has been observed that gray hole attack prevention has been done using genetic algorithm at good rate.

Keywords: Gray hole attack, Security, Genetic Algorithm, AODV .

I. INTRODUCTION

1.1 Wireless Sensor Network (WSN)

A Wireless Sensor Network (WSN) [1] consists of a set of nodes of typically low performance. They collaborate with each other to perform sensing tasks in a given environment. A wireless sensor network may contain one or more sink nodes (Base Stations) to collect sensed data and relay it to a central processing and storage system [12]. A sensor node is typically powered by a battery and can be divided into three main functioned units: a sensing unit, a communication unit and a processor unit. Recent advances in micro-electro-mechanical systems technology, wireless communications and digital electronics have boosted the development of sensor nodes. This brings the blooming prospect of WSNs into practical feasibility [2,11].

In WSN network normally packets are sent in forward direction by sensor nodes. A packet can be forwarded via different routes. WSN are usually developed in inimical area that leads to attack. There are two types of attacks that are present in WSN: outside and inside attacks [13].

Outside attacks are easy to handle. One kind of such attack is gray hole attack. This attack arises during the forwarding of the data packet. WSN is useful in various projects so it must be reliable [3].

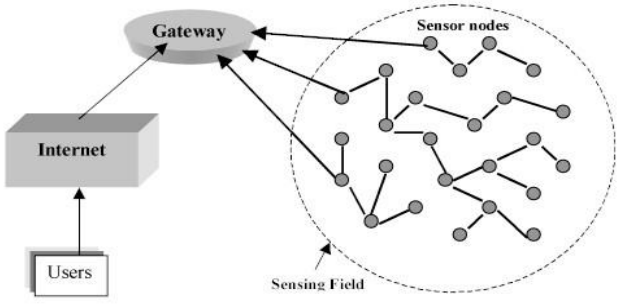

Figure 1. WSN Architecture

1.2 Gray Hole Attack

Gray Hole Attack is one of the network layer attack described in [4] and also called selective forwarding attack . In multi-hop WSN, the nodes send packets to the neighboring nodes thinking that they forward messages to destination faithfully. In Gray Hole attack, a malicious or compromised node legitimately refuses some packets and drops them. A simple form of this attack is when a malicious node acts like a black hole and drops all the packets passing through it. However in such an attack, the nodes can easily detect the attack and can exclude attacker from routing. But, here in selective forwarding attack, malicious nodes selectively drop/forward packet which makes detection of the attack more complicated.

1.3 Ad hoc On Demand Routing (AODV)

Adhoc On Demand Routing (AODV) is the very efficient protocol dsigned mainly for WSN, adhoc networks. Adhoc On Demand Routing(AODV allows network to be self- organizing as well as self- configured [5]. The AODV contains two terms.

- Route Discovery
- Route Maintenance

AODV protocol is an on-demand in which demands are made on requirement. In AODV nodes forwards data packets from one node to another in order to enhance cooperation. AS sequence number is needed at destination, so rich topology is need like mesh, ring etc.There is least routing traffic in the network since routes are built on demand. When two nodes in an ad hoc network wish to establish a connection between each other, it will enable them to build multihop routes. The routing table is updated during each entery.

It is loop free protocol which uses Destination Sequence Numbers (DSN) to avoid counting to infinity which is the distinguishing feature of this protocol. Requesting nodes in a network send Destination Sequence Numbers (DSNs) together with all routing information to the destination. It selects the optimal route based on the sequence number. Some assumptions are made in DSR protocol as discussed follows:

- All nodes are willing to participate in the network for communication.
- Each willing node is ready to forward the data packets.
- Minimum number of nodes to transfer data from source to destination are itself Source and Destination.
- Packets may be lost in network.
- Nodes placement can be takes place at any time.
- AODV nodes cannot move continuously.
- Nodes can enable their continuous receive mode.
- Wireless strength may not be equal in both directions of nodes.
- AODV can work well in unicast also.
- Each node selects random IP address by which it can be known in the whole network.

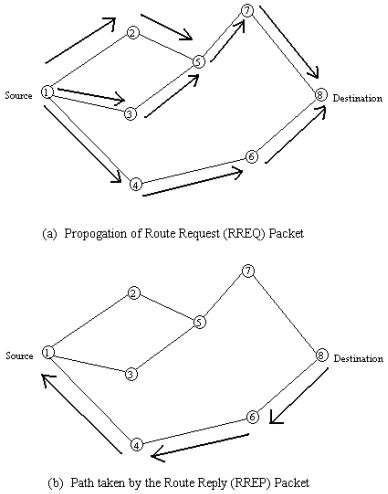

Figure 2. AODV Architecture

1.4 Genetic Algorithm (GA)

Genetic Algorithms (GAs) are the biological search algorithm based on selection and genes. They optimise the searching problem using intelligent exploitation method. It is the main technique to simulate the processes for evolution. They work on the fitness function. Each generation consists of the population as we can see in our DNA. Each individual of population represents the search space or possible solution. Each individual in population leads to the evolution [6].

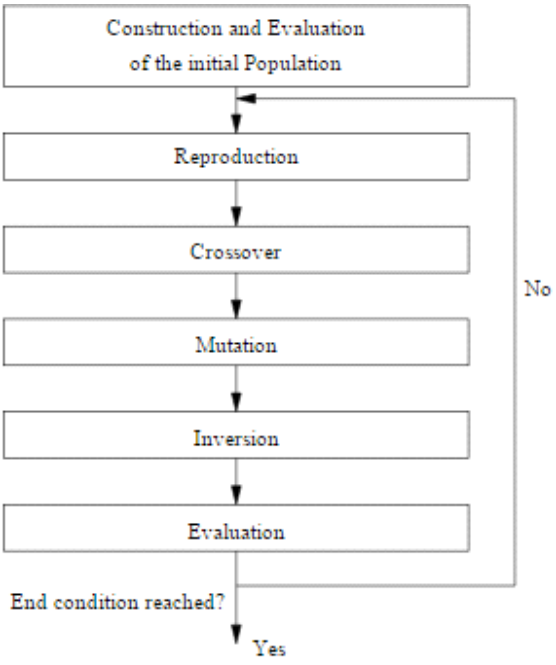

Figure 3. Genetic algorithm Process

1.5 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

Ahmed Shariff (et.al) [7] demonstrated that Mobile Ad-Hoc Networks (MANETs) are portrayed by the absence of framework, element topology, and their utilization of the open wireless medium. Black hole attack speaks to a noteworthy risk for such sort of systems. Firstly, it exhibit a broad study of the known black hole discovery and the prevention approaches and another by assessed new measurements for their characterization. S.K Sujhatah (et. al) [8] propose a strategy for dissecting the introduction attacks in AODV, and build up a particular based Intrusion Detection System (IDS) utilizing Genetic Algorithm approach. The proposed framework is in view of Genetic Algorithm, which examined the practices of each hub and gives insights about the attack. Manvi(et. al) [9] proposed a productive system that uses various base stations to be conveyed haphazardly in the system to counter the effect of black holes on information transmission. The proposed plan can be utilized to recognize 100% black hole attacks with almost negligible false positives.Preeti(et.al) [10] proposed new protocol, named BFAODV by applying BFOA system on AODV. The proposed convention enhances the execution measurements in correlations to DSDV and AODV conventions. This paper identifies and keeps from black hole attack utilizing proposed BFAODV calculation.

III. PROPOSED WORK

- **Methodology**
- Initialize WSN Network
- Enter height of network.
- Enter width of network
- Enter nodes of network
- Searching of attack in memory
- Searching in Cache memory
- Attack found in network
- Apply Genetic Algorithm for optimization using fitness function.
- Select best route until best fitness function has not been attained.
- Evaluate parameters.

Measure Error rate, Throughput and end delay using GA and without GA

IV. RESULTS AND IMPLEMENTATION

4.1 Parameters

4.1.1 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.

4.1.2 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 Percentage (%). 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.

4.1.3 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).

4.2 Analysis

Simulation of grey hole attack prevention has been done using genetic algorithm in MATLAB 7.10 environment. Below graphs shows the simulation results.

Table: 1 Simulation Environment

Property	**Value**
Routing Protocols	AODV
Area Covered(AODV)	1000*1000m
Coverage Set	250m
No. of Nodes	25
Observation Parameters	Throughput, End-to-End Delay and Bit Error Rate
Network Simulation	MATLAB
Optimization technique	GA
No. Of Data Transfer	5
Population Size	50

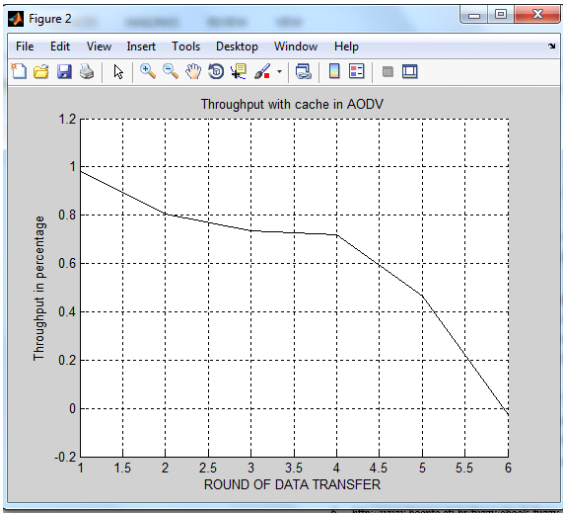

Figure 5. Throughput without GA

Throughput of AODV routing protocol without optimization is shown in Figure 5. As we know that high the throughput better the performance of network. But without any optimization throughput for AODV has found to be 1.

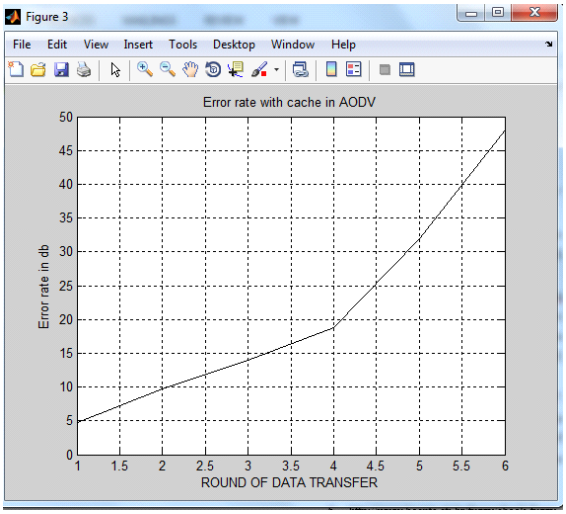

Figure 6. Error Rate without GA

Bit Error rate of AODV routing protocol without optimization is shown in Figure 6.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`46 db.

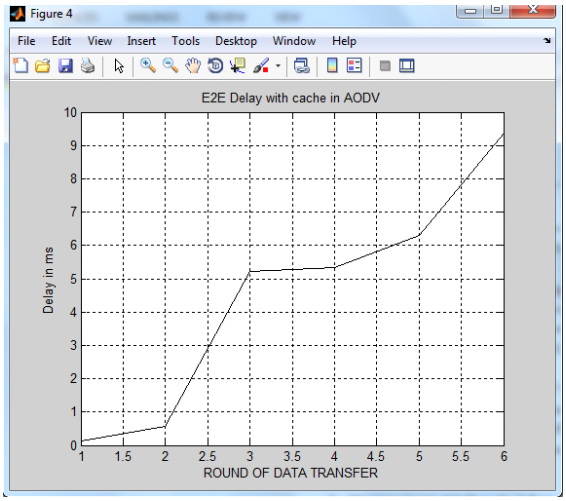

Figure 7: End Delay without GA

End delay of AODV routing protocol without optimization is shown in Figure 7. 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 9.5 ms.

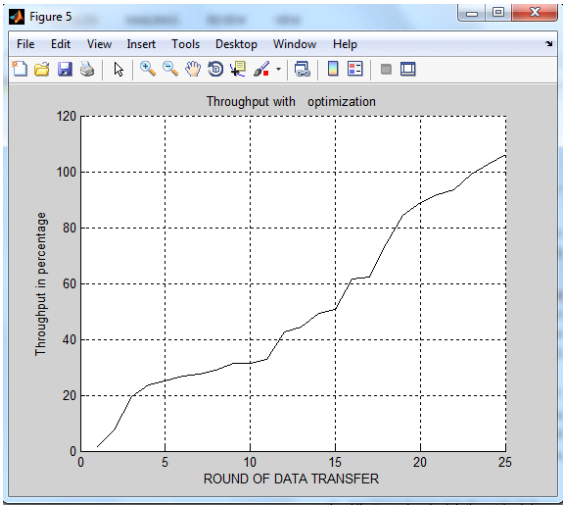

Figure 8. Throughput with GA

In figure 5.The maximum throughput value is 1 without optimization but after using GA the maximum value is 100. Each iteration percentage value after optimization increases from its previous percentage value. Higher the throughput betters the performance

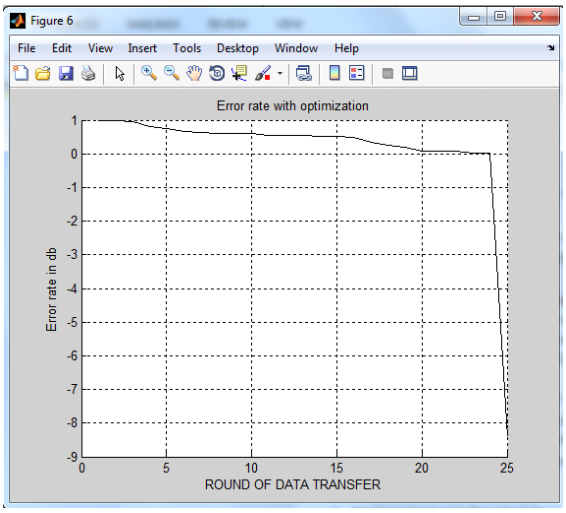

Figure 9. Error Rate with GA

In the figure 6. The bit error starts increasing 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 46db and after optimization the maximum BER value is 1.23 db.

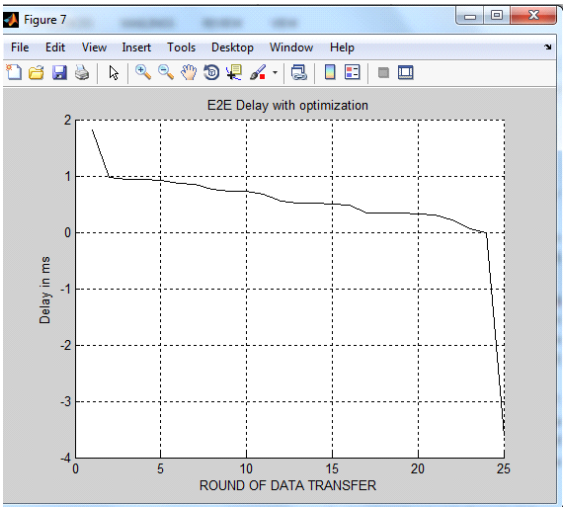

Figure 10. Delay with GA

In figure 7 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 2 ms that is much better than in the presence of the attack.

Parameters	Without GA	With GA
Average End delay	9.5	2
Average Throughput	1	100
Average Error Rate	46	1.23

Figure 11. Comparison with and without Genetic algorithm

V. COMPARISON GRAPH

Parameters	Without GA	With GA
Average End delay	0.8	0.3
Average Throughput	0.4	70
Average Error Rate	0.7	0.2

Figure 12 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.

In above graph, we have shown comparison between previous work and proposed work done using parameters end to end delay and throughput.

VI. CONCLUSION AND FUTURE SCOPE

The proposed work gives an approach for secure routing algorithm in gray hole attack in WSN. 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 gray hole attack. So this paper has concluded that utilization of genetic algorithm leads to high rate of throughput. The performance of the system has been analyzed 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.

REFERENCES

[1]. C. Siva Ram Murthy, B.S. Manoj, "Ad Hoc Wireless Networks : Architectures and Protocols", Prentice Hall PTR, May 2004, New Jersey, USA

[2]. K. Biswas and Md. Liaqat Ali, "Security threats in Mobile Ad-Hoc Network", Master Thesis, Blekinge Institute of Technology" Sweden, 22nd March 2007.

[3]. P.V.Jani, "Security within Ad-Hoc Networks," Position Paper, PAMPAS Workshop, Sept. 16/17 2002.

[4]. HaiyunLuo,FanYe,SongwuLu,LixiaZhang,"Security in mobile ad hoc networks:challenges and solutions ",Volume :11,Issues:1,PP:38-47,IEEE Journals & Magazines,2004.

[5]. Hongmei Deng & Wei Li, Dharma P. Agarwal (2002) "Routing security in wireless ad hoc networks", University of Cincinnati, IEEE Communications magazine, Vol. 40, No. 10.

[6]. http://www.boente.eti.br/fuzzy/ebook-fuzzy-mitchell.pdf

[7]. YinghuiGuo, "Detecting Blackhole and Greyhole Attacks in Vehicular Delay Tolerant Networks", COMSNETS 2013.

[8]. Vimal, "Performance Analysis of Black Hole Attack in Vanet", I. J. Computer Network and Information Security, 2012, 11, 47-54.

[9]. Ram Shringar Raw1, Manish Kumar1, Nanhay Singh, "Security Challenges, Issues And Their Solutions For Vanet", International Journal Of Network Security & Its Applications (Ijnsa), Vol.5, No.5, September 2013.

[10]. Priyanka Sirola(et.al), "An Analytical Study of Routing Attacks in Vehicular Ad-hoc Networks (VANETs)", International Journal of Computer Science Engineering (IJCSE), Vol. 3 No.04 .pp210-218,July 2014.

[11]. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks: a survey," Computer Networks, vol. 38, 2002.

[12]. L. Tong, Q. Zhao, S. Adireddy. Sensor Networks with Mobile Agents.IEEE Military Communications Conference, Boston, MA, USA, 2003:688-693.

[13]. M. Ketel, N. Dogan, A. Homaifar. Distributed Sensor Networks Based on Mobile Agents Paradigm.