ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

A Mechanism of Prevention of Gray Hole Attack in WSN using Genetic Algorithm

Jaspreet Kaur, Vishal Walia, Dr.Rahul Malhotra

M.E Student, Dept. of ECE, RIEIT, GTBKIET, Railmajra, Ropar, India

Associate Professor & Dean Academics, Dept. of ECE, RIEIT, Railmajra, Ropar, India

Professor & Director, Dept. of ECE, RIEIT, Railmajra, Ropar, India

ABSTRACT: This paper presented that the Wireless Sensor Networks (WSNs) are inclined to different attacks in which gray hole attack is extremely hard to recognize and guard. In this attack, the intruder catches and re-programs an arrangement of hubs in the system to obstruct the data they get as opposed to sending them towards the base station. Accordingly any data that enters the gray hole locale is caught and not ready to achieve destination bringing on top of the line to-end postpone and low throughput. Beforehand little measure of work is done only for identification and counteractive action of the gray hole attack in the WSN making its discovery and avoidance extremely essential according to network execution is concerned. In this paper at first the influence of gray attack was measured on the system parameters took after by the proposition of a novel method for the recognition and counteractive action of gray hole attack in WSN using genetic algorithm (GA).

KEYWORDS: Gray hole attack, WSN, Genetic Algorithm, Security.

I. INTRODUCTION

A Wireless Sensor Network (WSN) consists of a set of nodes of typically low performance. They collaborate with each other to perform sensing tasks in a given environment [1]. 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. 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 [2]. 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 [3].

Wireless sensor networks may consist of many different types of sensors such as seismic, thermal, visual, infrared, and acoustic and radar etc., which enables wireless sensor networks to be projected into a broad range of applications [4]. The concept of micro-sensing and wireless communication of these nodes promises many new application areas. The understanding of these different application areas and their requirements is crucial to the design of a wireless sensor network [5].

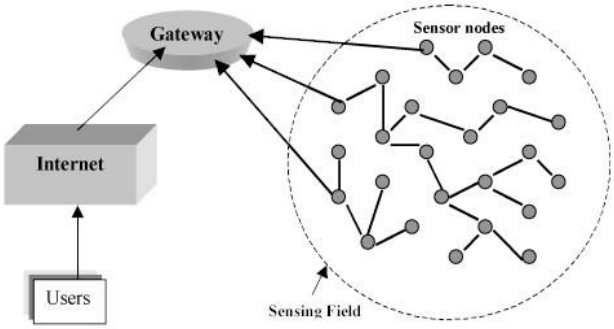


Fig.1 WSN Network

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

Simplicity in Wireless Sensor Network with resource constrained nodes makes them extremely vulnerable to variety of attacks. Attackers can eavesdrop on our radio transmissions, inject bits in the channel, replay previously heard packets and many more. Securing the Wireless Sensor Network needs to make the network support all security properties: confidentiality, integrity, authenticity and availability. Attackers may deploy a few malicious nodes with similar hardware capabilities as the legitimate nodes that might collude to attack the system cooperatively [6, 7]. The attacker may come upon these malicious nodes by purchasing them separately, or by "turning" a few legitimate nodes by capturing them and physically overwriting their memory [8]. Also, in some cases colluding nodes might have high-quality communications links available for coordinating their attack. Sensor nodes may not be tamper resistant and if an adversary compromises a node, she can extract all key material, data, and code stored on that node. While tamper resistance might be a viable defense for physical node compromise for some networks, we do not see it as a general purpose solution based on genetic algorithm [9].

II. RELATED WORK

In proposed work Adhoc On-Demand Distance Vector (AODV) protocol is used as communication protocol over wireless system. As AODV is vulnerable to many attacks like black hole, gray hole attack etc. However, Gray hole attack is very crucial attack. In gray hole attack, malicious node changes its behaviour from normal to attacker node by changing its personality. So, work is done on detection of such crucial Gray hole attack using Genetic Algorithm with AODV protocol. AODV is an on –Demand routing protocol which is confluence of DSDV and DSR. Route is calculated on demand, just as it is in DSR via route discovery process. That is why it is called reactive protocol [10]. However, AODV maintains a routing table where it maintains one entry per destination unlike the DSR that maintains multiple route cache entries for each destination. AODV provides loop free routes while repairing link breakages but unlike DSDV, it doesn't require global periodic routing advertisements [11]. AODV has three types of control messages for route maintenance as mentioned following:

- RREQ
- RREP
- RRER

So, in proposed work gray hole detection and prevention is done using genetic algorithm. Genetic algorithm is the type of algorithm that is used to solve both constrained and non-constraint problems based on selection criteria. Genetic algorithm modifies the new population and generates new solutions until best solution has not been reached. From large set of population, genetic algorithm uses the random chromosomes to make it parent then make it to produce children. In proposed work, firstly network deployment is done then parameter evaluation will be done in presence of attack like BER, PDR, Throughput and Delay. After that optimization of network will be done using Genetic algorithm and then again parameter evaluation will be done. In the end comparison will be done without or with genetic algorithm. The whole simulation is done using MATLAB 2010 an environment.

III. PROPOSED ALGORITHM

- *Design Considerations:*
- Initialize the network.
- Plot the number of nodes in x and y locations where x location has the width and y location has height.
- Discover the path in that vary network only.
- Initialize the source and destination to find the shortest path, which is a simple process.
- Initialize the Gray hole attack to discover the path.
- Implement the process by using Genetic Algorithm with new fitness function.
- Evaluate the parameters that are Throughput, Bit Error rate, end to end delay, packet overhead, packet delivery ratio.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

B. *Description of the Proposed Algorithm*

The *Genetic Algorithm (GA)* is a method for solving both constrained and unconstrained optimization problems that is based on natural selection, the process that drives biological evolution. The genetic algorithm repeatedly modifies a population of individual solutions.
Step 1: Create Initial population of individuals
Step 2: Evaluate fitness of individuals
Step 3: Select the individuals
Step 4: Apply Genetic Operators
Step 5: Finished generations in genetic algorithm

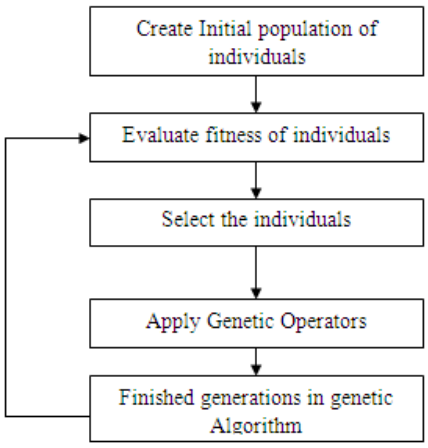


Fig.2 Genetic Algorithm

IV. PSEUDO CODE

```
 Function [f] = fitness_fn (e, Fs, Ft)
% Fs= each feature
% Ft = total number of features
% e is classification error rate (optimization parameter (unknown))
   Fs=rand; Ft=rand;

%f= (1-e)*((1-Fs)/Ft);
f= (Fs/Ft)*100;
```

V. SIMULATION RESULTS

In Simulation Environment the AODV protocol is used with area covered (AODV) 1000*1000m, coverage set is 250 m. The number of nodes taken is 25. The parameters to be observed are Throughput, End to end delay and Bit error rate. The Optimization technique used is Genetic Algorithm. First the value of parameters are measured without GA and then after applying Optimization, the values of parameters are measured with GA. That shows the optimized and improved values of the parameters and hence resulting in better performance of the system.
Network simulation is MATLAB. Number of data transfer is 5and the population size is 50. The result of the simulation on parameters Throughput, End to end delay and Bit error rate with GA and without GA is shown as follows.

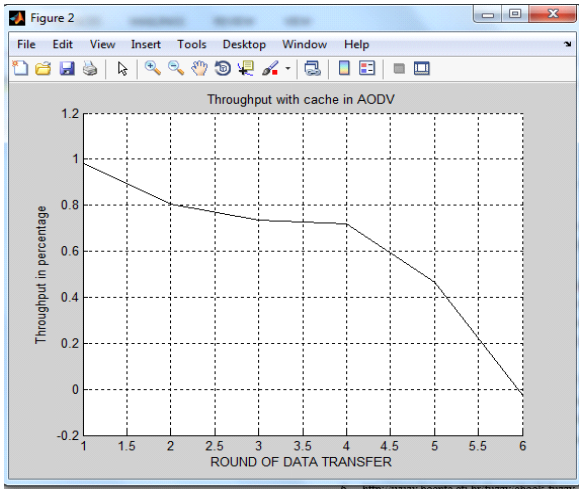
ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

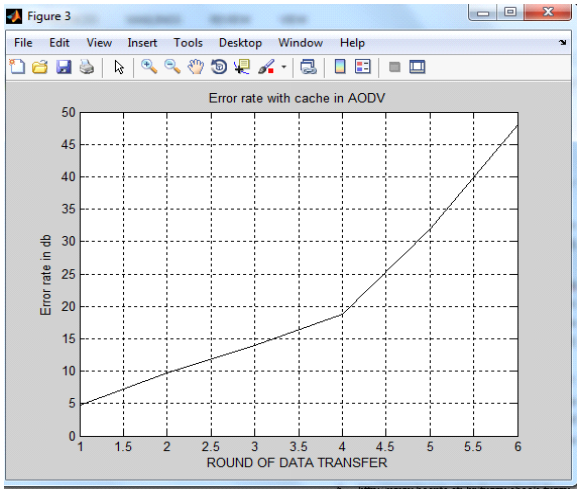
International Journal of Innovative Research in Computer and Communication Engineering

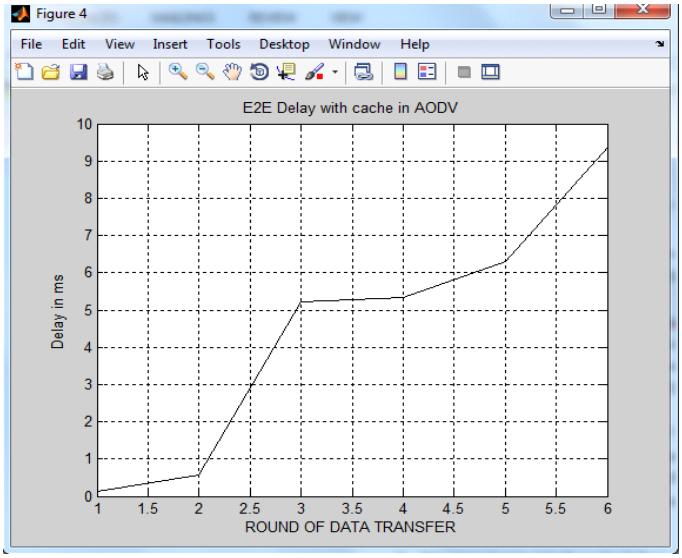
(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

Results without GA:







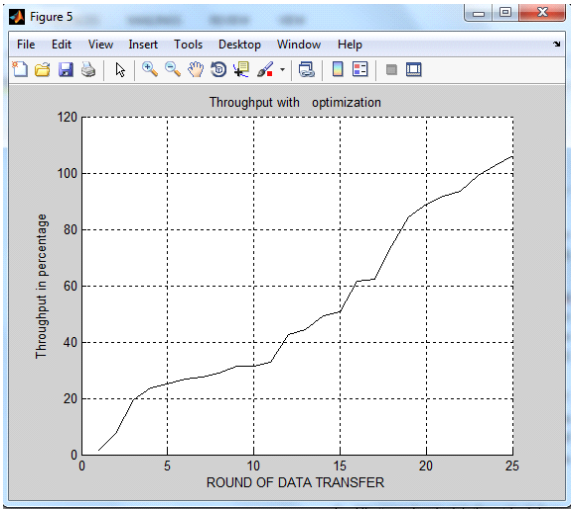
ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

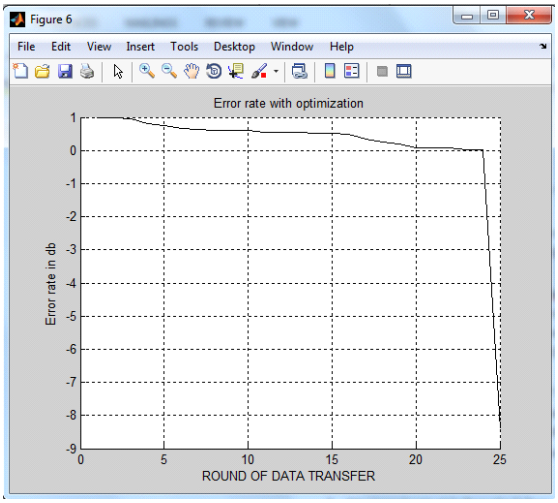
International Journal of Innovative Research in Computer and Communication Engineering

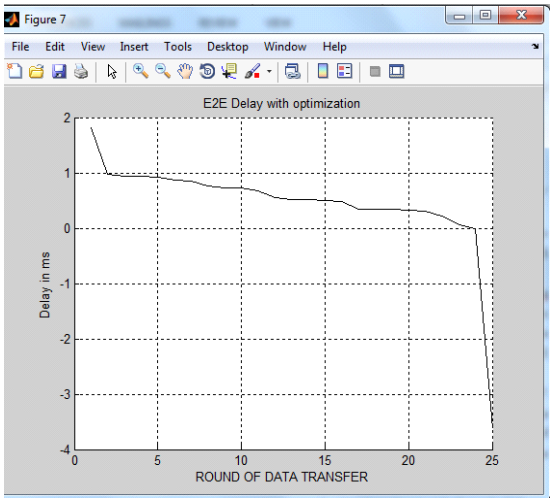
(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

Results with GA:







Comparison between parameters

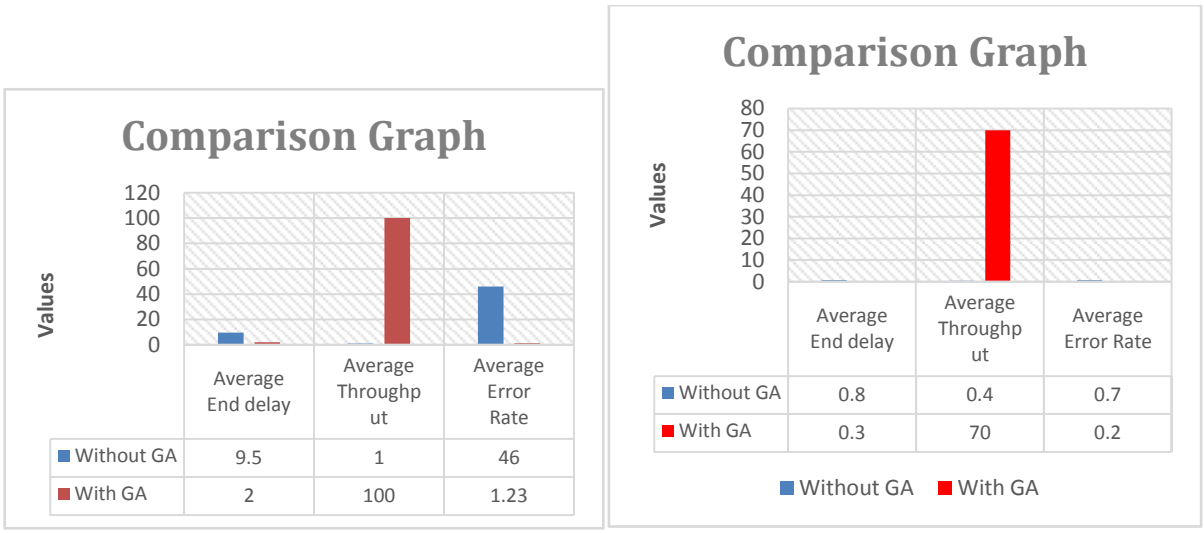
Parameters	Without GA	With GA
Average End delay	9.5	2
Average Throughput	1	100
Average Error Rate	46	1.23

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

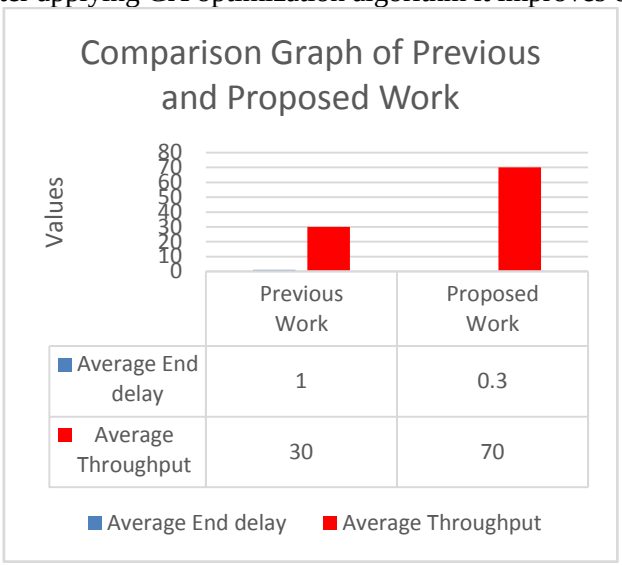
(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015



Comparison with and without Genetic algorithm

In above graphs, 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.



Comparison between previous work and Proposed Work

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

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

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. Haithem Ben Chikha, Amira Makhlouf and Wiem Ghazel, "Performance Analysis of AODV and DSR Routing Protocols for IEEE 802.15.4/ZigBee", IEEE, 2011.
11. Kwashie A. Anang, Lawal Bello, Titus. I. Eneh, Panos Bakalis and Predrag B. Rpajic, "The Performance of Dynamic Source Routing Protocol to Path Loss Models At Carrier Frequencies Above 2 GHz", Communication Technology (ICCT), IEEE, , pp151-155, 2011.
12. Pengfei Guo Xuezhi Wang, "The Enhanced Genetic Algorithms for the Optimization Design," 978-1-4244-6498-2/10/$26.00 ©2010 IEEE.
13. Yong-Feng Dong, Jun-Hua Gu, " Combination Of Genetic Algorithm And Ant Colony Algorithm For Distribution Network Planning," -4244-0973-x/07/$25.00 ©2007 IEEE.
14. Chang Wook, R. S. Ramakrishna, "A Genetic Algorithm for Shortest Path Routing Problem and the Sizing of Populations," 1089-778X/02$17.00 © 2002 IEEE.
15. 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.