Optimized Positioning Of Multiple Base Station for Black Hole Attack

Anurag Singh Tomar, Gaurav Kumar Tak

Abstract— **Wireless sensor network (WSN) consists of distributed autonomous sensors to monitor physical or environmental conditions, such as sound, temperature, pressure, etc. and to pass their data through the network to a main location. The modern networks are bi-directional. They also enable the control of sensor activity, so security is major issue as number of attacks are present in the network for capturing the information. One of the attacks is black hole. That attack is mounted by an external adversary on a subset of the sensor nodes (SNs) in the network. The adversary captures these nodes and reprograms them so that they do not transmit any data packets, or start to drop the packets. In this paper we have proposed the algorithm that will help to successfully deliver the packets in the presence of black hole attack by using multiple base stations with optimized position using genetic algorithm (GA).**

Index Terms—**Base station, Genetic Algorithm, Wireless Network, .**

I. INTRODUCTION

Wireless sensor networks were motivated by military applications such as battlefield; today such networks are used in many industrial and consumer applications, such as industrial process control and monitoring, e-commerce, and so on. As the sensor networks can also operate in an ad-hoc manner the security goals cover both those of the traditional networks and goals suited to the unique constraints of ad-hoc sensor networks. Security goals are classified as primary and secondary. Primary goals are known as standard security goals such as Integrity, Confidentiality, Authentication and Availability. Secondary goals are Self- Organization, Data Freshness, Time Synchronization and Secure Localization. Such kind of networks can be used in emergency conditions but security is major issue in these networks. If any node is compromised by attacker then it will affect the whole communication so we need to monitor the behavior of node like packet drop rate, packet delivery rate etc in regular way.

Rest of the paper is organized as follows. The related work described in section II. Proposed scheme explained in section III. Security analysis of the proposed scheme has been discussed is in section IV. Section V concludes the paper.

Manuscript received Aug, 2014.
Anurag Singh Tomar, *Lovely Professional University,Phagwara,Punjab,India,*
Gaurav Kumar Tak, *Lovely Professional University,Phagwara,Punjab,India, ,*

II. RELATED WORK

Various Algorithms have been proposed to prevent from black hole attack in network.

Base Station is a natural target for an adversary that desires to achieve the most impactful attack possible against a WSN with the least amount of effort. An adversary may employ traffic analysis techniques to identify the BS based on network traffic flow even when the WSN implements conventional security mechanisms. This motivates a significant need for improved BS anonymity [5] to protect the identity, role, and location of the BS. So, they proposed a strategy to increase BS anonymity in a WSN by utilizing multiple relays at each hop. Each relay retransmits received messages at an increased power level to increase the number of candidate receivers included in the adversary's analysis. They examine the effect of the distributed relay technique on improving BS anonymity using evidence theory and demonstrate the effectiveness of this approach through simulation. This paper considered the effectiveness of distributed relays for improving BS anonymity and did not consider how relays affect the underlying target network performance. Increasing transmission power not only expends sensor energy more quickly, but also increases the overall RF noise floor within the WSN

. Author proposed the algorithm to defend against black hole attack by deploying multiple base stations in network. A packet drop attack or black hole attack [1,2,4] is a type of denial-of-service attack accomplished by dropping packets. The attack can be accomplished either selectively (e.g. by dropping packets for a particular network destination, a packet every n packets or every t seconds, or a randomly selected portion of the packets, which is called "Gray hole attack") or in bulk (by dropping all packets). Mobile agent is a program segment [8] which is self-controlling. They navigate from node to node not only transmitting data but also doing computation. They are effective paradigm for distributed applications, and especially attractive in a dynamic network environment.

In that Algorithm, AODV has been used for simulating few attacks using NS3. Black hole attack [3,6] is one of the security threat in which the traffic is redirected to such a node that drops all the packets or the node actually does not exist in the network. Black holes refer to places in the network where incoming traffic is silently discarded or dropped. Jellyfish (JF) attack is a type of selective black hole attack. When JF node gets hold of forwarding packet [7], it starts

delaying/dropping data packets for certain amount of time before forwarding normally. Since packet loss is common in mobile wireless networks, the attacker can exploit this fact by hiding its malicious intents using compliant packet losses that appear to be caused by environmental reasons. They have provided a quantification of the damage they can inflict. It showed that, perhaps surprisingly, such attacks can actually increase the capacity of ad hoc networks as they will starve all multi hop flows and provide all resources to one-hop flows that cannot be intercepted by Jellyfish or Black Holes. As such a partitioned system is clearly undesirable; they also considered fairness measures and the mean number of hops for a received packet, as critical performance measures for a system under attack.

III. PROPOSED ALGORITHM

In this paper, Black hole attack prevention by deploying multiple base stations Scheme has been proposed. We have used Genetic algorithm to find out suitable position of multiple base stations. Genetic Algorithms are the heuristic search and optimization techniques that mimic the process of natural evolution. This is very efficient algorithm to find the optimization position. It has following steps to calculate the optimization position as shown below

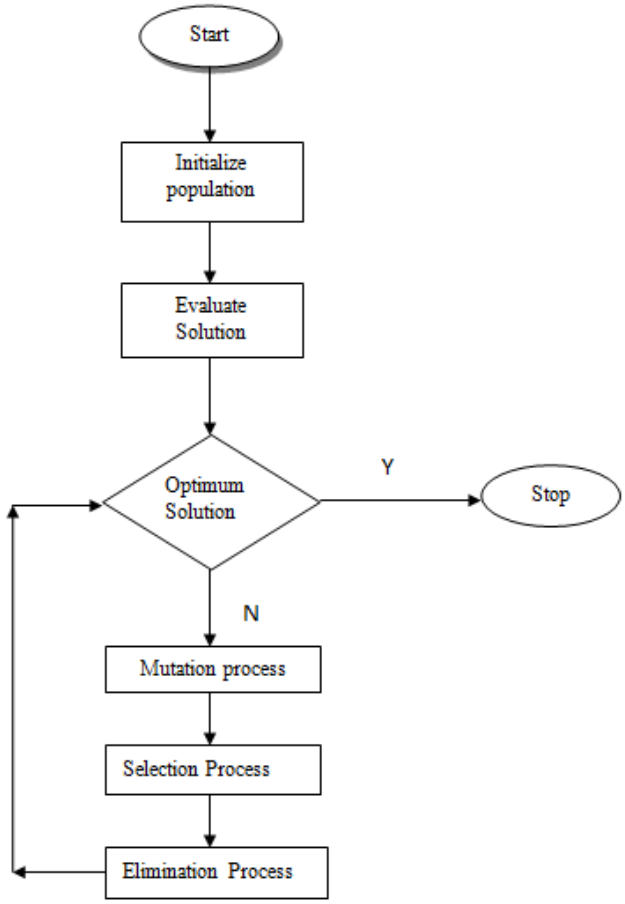

Fig 1: Process of Genetic Algorithm

It works in 3 steps which are mentioned below

A. Mutation Process: In this step populations are divided into two parts and child part mutate to another location by a predefined step size.

B. Selection Process: Primary objective of the selection process is to select the best solution from the child and parent population by calculating the fitness value.

C. Elimination Process: Eliminate the bad solutions in a population while keeping the population size constant.

Proposed algorithm is divided into three parts.

A. In first part we deploy the sensor nodes, base stations and create the black hole regions.

B. In Second parts we find the optimized position of our BS(s) using GA (Genetic Algorithm) and repositioned it to that position.

C. In last part we start routing from fifty randomly transmitting nodes and calculate the results

Steps of the proposed algorithm are as follows

1. Deploy randomly the given sensors nodes into the given area so that they are deployed uniformly throughout the area.
2. Randomly deploy the BS at the corner of the area.
3. Randomly place two black hole region into the area by taking the radius given and the nodes come into that region consider them as a black hole nodes.
4. Now apply Genetic Algorithm to the Number of BS to calculate the optimized position of the BS after dividing the area into parts equal to the number of BS. Below are the steps to calculate the optimized position of each BS using GA：

   Randomly set the value of chromosomes and calculate the (X, Y) positions of all chromosomes within that co-ordinates.

   Calculate the fitness value of each Parent chromosomes as

   Active Sensor Nodes position=(R, C)

   Fitness_value= w1*(no_of_active) + w2* (tx_range-(averageof($\sum_{i=1nodes}$(sqrt((R_i-X)^2+(C_i-Y)^2))).

   (Where tx_range is transmission range in term of distance, R, C are coordinates of active sensor node, w1 & w2 are constants and are used for give weightage)

   After calculating the fitness value mutation process will start it means randomly move each chromosome to one of the following position if the current position is (X, Y) then the possible moves for child chromosomes are

{X-1 , Y-1}	{X , Y-1}	{X+1 , Y-1}
{X-1 , Y}	{X , Y}	{X+1 , Y}
{X-1 , Y+1}	{X , Y+1}	{X+1 , Y+1}

Table:1 possible positions for child chromosome

Now calculate the fitness value of child as well as Compares the fitness value of parent chromosomes with the child fitness value and discard the one with least value. After that out of all chromosomes' fitness

values the one which has highest value is selected as the optimized position of BS for that generation.

5. Now our BS is optimized after this routing will begin from Sensor nodes to number of BS as follows Repeat steps while remaining distance< maximum transmitting distance

Step1. Take pedestal distances for each node form current elected source node.

Step2. Discard the nodes whose pedestal distances are out of range from source node.

Step3. Compute pedestal distances for remaining nodes from sink.

Step4. Rearrange nodes according to pedestal distances.

Step5.Send data to the node which is having minimum pedestal distance.

(check for all nodes)
if(negative acknowledged)
data trapped by black hole or channel loss
if(positive acknowledged)
data send successfully to next node

IV. RESULTS

The proposed Multi Base Station optimized position against Black hole attack based methodology is implemented in MATLAB R2011b. MATLAB (Matrix Laboratory) environment is one such facility which lends a high performance language for technical computing. In our technique we have taken multiple BS and multiple black hole regions as 20 m, 30m and 40m out of total area that is 100 m. With 20 m radius almost 20% nodes are come into black hole region, with 30 m radius 38 % and with 40 m 57 % nodes as shown in figure below.

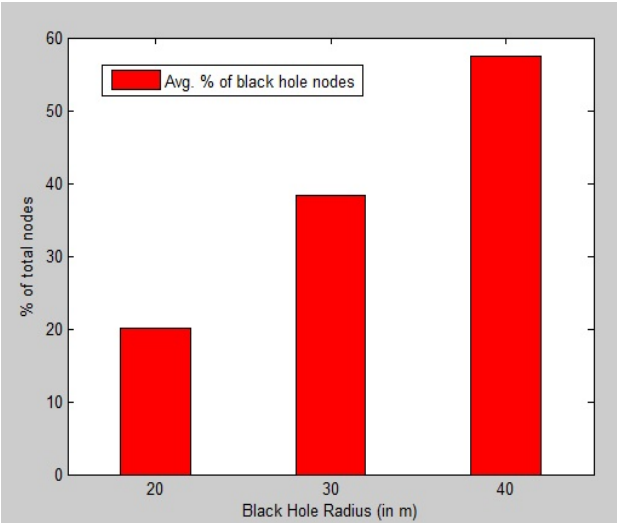

Fig:2 Average % of nodes comes into Black hole region

This implies that as the radius of Black hole region will increased the average number of nodes in Black hole region are also increased and packet lose in also increased but with our technique the successful delivery of packet is almost 100 % by using 3 and 4 BS and with 1 or 2 BS the successful rate is also high. In our approach we are using multiple BS for transmitting the data and we calculate the results for 1, 2, 3 and 4 BS so in case of more than 1 BS if the data reach to one of the BS than we consider it as successful deliver of packet. The results are given here.

Black hole radius	No. of BS	success	failure	false +ve	No. of nodes in black hole
20 m	1	80.9	19.1	0.05	20.12
20 m	2	95.14	4.86	0	
20 m	3	99.3	0.7	0.27	
20 m	4	99.54	0.46	0.2	
30 m	1	77.18	22.82	0.12	38.336250
30 m	2	96.52	3.48	0.57	
30 m	3	99.48	0.52	0.34	
30 m	4	99.64	0.36	0.18	
40 m	1	74.9	25.1	0.36	57.43625
40 m	2	97.92	2.08	0.57	
40 m	3	99.8	0.2	1.38	
40 m	4	99.82	0.18	0.86	

Table:2 Tabular representations of results

V. CONCLUSION

In this paper we showed an approach to prevent the black hole attack and successfully delivery of data by optimizing the position of base station using genetic algorithm (GA). The results have improved greatly for less number of BS and a little for large number of BS with a very little false positive. In large number of BS the successful data delivery results are above 99%. As we are using multiple BS for sending the same data so it requires more energy to send the data so In future we will look to minimize the energy consumption of the sensor nodes.

REFERENCES

[1] Ali Modirkhazeni, Norafida Ithnin, and Othman Ibrahim "Secure Multipath Routing Protocols in Wireless Sensor Networks: A Security Survey Analysis," *Second International Conference on Network Applications, Protocols and Services*, pp. 228-233, 2010.

[2] Dr. G. Padmavathi, Mrs. D. Shanmugapriya, "A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks," *International Journal of Computer Science and Information Security*, vol. 4, pp. 1-9, 2009.

[3] Feilong Tang, Minyi Guo, Minglu Li, Zhijun Wang and Zixue Cheng, "Scalable and Secure Routing for Large-Scale Sensor Networks," *International Conference on Embedded and Ubiquitous Computing.*, pp. 300-305, 2008.

[4] Jian Yin and Sanjay Kumar Madria "A Hierarchical Secure Routing Protocol against Black Hole Attacks in Sensor Networks," *International Conference on Sensor Networks, Ubiquitous and Trust worthy computing.*, vol. 1, 2006.

[5] Jon R. Ward and Mohamed Younis "On the Use of Distributed Relays to Increase Base Station Anonymity in Wireless Sensor Networks," *Military Communications Conference"*, pp. 1-6, 2012.

[6] Younis Leela Krishna Bysani , Ashok Kumar Turuk, "A Survey On Selective Forwarding Attack in Wireless Sensor Networks,"

International conference on devices and communications", pp. 1-5, 2011.

[7] Mariam Ahmed Moustafa, Moustafa A. Youssef, Mohamed Nazih El-Derini, "MSR: A Multipath Secure Reliable Routing Protocol for WSNs," 9th IEEE *International conference on computers systems and applications"*, pp. 54-59, 2011.

[8] Mukesh Tiwari, Karm Veer Arya, Rahul Choudhari, Kumar Sidharth Choudhary "Designing Intrusion Detection to Detect Black hole and Selective Forwarding Attack in WSN based on local Information," 4th *International conference on computers sciences and convergences information technology"*, pp. 824-828, 2009.

Anurag Singh Tomar is currently working as Assistant Professor at Lovely Professional University,Phagwara,India.He received Master of Technology from ABV-Indian Institute of Information Technology, Gwalior.His area of research are Network Security,Cloud Computing,,Mobile Ad Hoc Networks.
.

Gaurav Kumar Tak is currently Assistant Professor in Lovely Professional University,Phagwara,India. He received Master of Technology Degree and Bachelor of Technology Degree from ABV-Indian Institute of Information Technology,Gwalior He had published 20+ international publications in reputed international journals and conferences including IEEE,springer, ACM, Science-Direct. He also guided several master thesis.His area of research are Network Security,Cyber Crime and Security,Mobile Ad Hoc Networks.

