An Assured protected interrelated implementation for WSAN

Ashish patil, Mr.jayraj N

M TECH, Asst. professor,

Dept. of ECE, The Oxford College of Engineering,

Bangalore-560068

Abstract- A wireless sensor network (WSAN) is a group of large no of sensors and some actors. Basically these types of networks are placed in a non – protected nature or environment and do the necessary functions. because of this these kind of networks are repeatedly vulnerable to the different kinds of active and passive attacks by harm full nodes . The black hole and gray hole attack is a caused in active attacks this type of attacks reduce the network efficiency and production. In a paper an assurance based protected inter related implementation is suggested to reduce the effect of gray hole and black hole attacks on delay and energy saving routing protocols for sensor – actor networks In the recommended mechanism a every sensor examine the faith level of every sensor based on its participation, suggestion, and understanding. An assured value is forwarded to the actors. The actors inspect these values to find the harm full nodes in a mass region. The suggested (API) is simulated using NS2, the performance is examined with regard to the packet delivery ratio, average energy dissipation in a network and average end to end delay. The given output results of simulation tell that ABPII system do well for the delay and energy saving routing protocols in comparison to the present implemented security system.

KEYWORDS: Gray Hole, Black Hole, Actor, Sensor, Assurance, WSAN.

1. INTRODUCTION

Wireless sensor – actor network (WSAN) is largely distributed to feel the outside physical nature and do appropriate functions to it with using some actors [1] [2]. the wireless sensor network (WSN) only feels the outside physical nature but it cannot do any actions on it. To overcome these disadvantages WSAN uses resource full actors to complete the reliable functions depending upon data received from sensors. An actor is an device which transform electrical signal into a physical action for a purpose and also do a network related task like transmit and receive data. Similar examples of actors are robots, electrical motors and human beings [3]. WSAN plays a crucial role in different applications such as disaster management, battleground, medical field, home intelligence these are the some applications which require sensor and actor which are installed in neglected areas. Thus theses appliances are easily subjected to failures, unprotected various active and passive attacks by harm full nodes.

In passive attacks, aim of harm full node is to acquire information, but it will not change or interfere the data. But this type of attacks may destroy source or destination and on another side, in active attacks harm full nodes either change or leak some data. These active attacks are normally simple to find them then intercepting them because of harm full nodes. These active attacks are more harm full than passive attacks. Sink hole, black hole, gray hole are some of forms of the active attacks in WSAN. A black hole attack is nothing but not allow the packets to move by dropping packets purpose fully. In this the attacker drops all the packets received from source to destination. In selective forward attack the harm full node may drop the packets in discriminative method.

II. RELATED WORK

In this part, the existing techniques to counter the black hole and gray hole attacks in sensor network are examined to find the advantages and disadvantages.

A. Detecting a black hole attack in sensor network

Author *Karakchayov* have proposed a black hole identification system [4]. In this system author has analyzed two methods such as packet purse and packet trade. In packet purse method data sent from source inserts neglects in data packets while sending it. And in packet trade method packet receiver at destination sensor award the transitional sensor for sending the data. Author *sheela* [5] proposed method to counter the black hole reduction method using mobile agent. In a normal way sensor sends its data to near by base station however data packets are transformed to one or more base station in black hole attacks. to check the black hole nodes, mobile agents check all the network and every sensor. Author *ngai* proposed an intruder detection system (IDS) for black hole and gray hole attacks in wireless sensor network[6].in this IDS finds a suspected nodes then it identify invader in list with help of network flow graph. Author *sun* proposed black hole detection technique based on neighbor information [7]. Sensor conserve the resource devices, the overheating process reduce the network life time because of this it is not practical to use neighbor based approaches to find black hole attack in the network. Author *shue* proposed multi cast tree assisted random (MTRP) [8]. In MTRP alternatively finding the one or more paths to transfer data from sensors, it uses random routes some multiple base stations are put at different locations to find a black hole attack in the way of base station.

B. Detecting a gray hole attack in sensor network

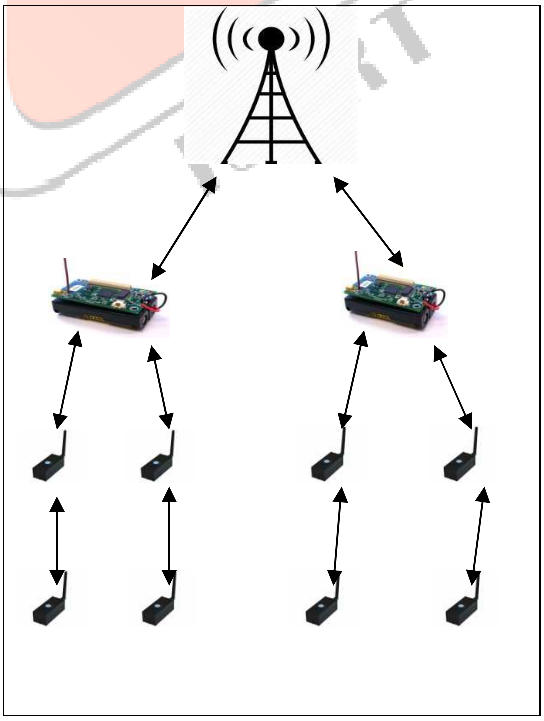
Author *yu* proposed a multi hop acknowledgment scheme [9]. Some of the actors act as in charge for finding harm hull nodes, in between node finds the affected information, it may send an alert packet to the downward or upward node in multi hop fashion. Author *xin* proposed a light weight reduction system for WSN [10]. It uses near by nodes to detect the packet transmission in the network. Author brown proposed a security system to find selective forwarding attack in heterogeneous sensor network (HSN) [11]. Author *jiwan* proposed an adaptive approach to find black and gray hole attack in ad-hoc network depending upon cross layer design. In a network layer a patch based method is used to overhear the next hop action. In a MAC layer collision rate reporting way is used to evaluate dynamic way of finding of threshold to dcrease false positive rate and high traffic condition [12].

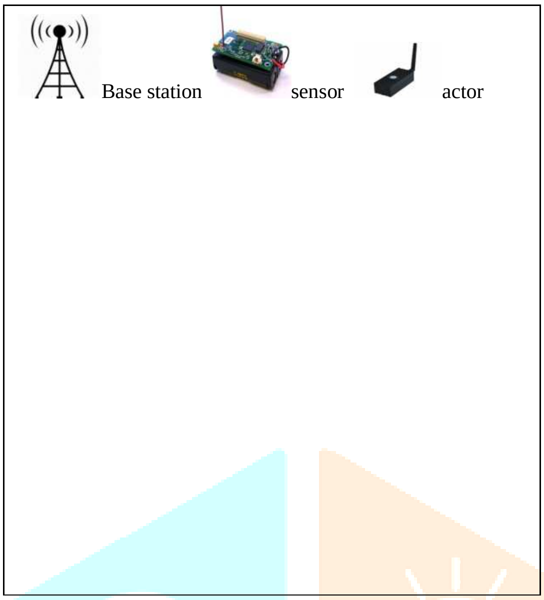
All the current black hole and gray hole attacks recognition system for sensor network may be able to not perform good in WSAN. As per our knowledge still there is no good secured coordinated system in WSAN to overcome the black hole and gray hole attacks. hence assured protected interrelated implementation for delay an low energy consumption technique in WSAN.

III. ANASSURED PROTECTED INTERRELATED IMPLEMENTATION METHOD

An assured protected interrelated implementation method is proposed to control a black hole and gray hole attack for our earlier proposed energy efficient and delay protected technique in WSAN. This technique consists of fast processing, communication capabilities and very few constrained actors. A multi level hierarchical system is designed for WSAN as shown in fig. 1 in a first top level act as base station and next level as actors and next lower level as sensors. Sensor sends information to actors and actor foreword this information to base station. This actor implements action in an event area depending up on sensor sending information.

Fig. 1.Interconnected architecture for WSAN





A. Gray hole attack countering

In gray hole attacks the harm full node which attacks may refuse to send few packets and drop some of them because of which they don't reach destinations. In our model every single sensor node move the trusted value of its near by to the actor. The actor node decides over all credibility of its all cluster nodes and whenever a harm full node projects itself as a good neighbor then all the sensor node recommends increases . the near by sensor node of harm full node provides a high endorsement. In this the near by node is chosen based on a distance.

B. Black hole attack countering

In a black hole node, it will not send all the data packets received from source but it merely drops all the packets instead of sending them to destination. Since black hole nodes easily drops all the packets instead of sending them to destination it is very easy to find the black hole attack in comparison with gray hole attack. An assured protection model can find and remove black hole sensor node, if any one of the sensor node drops data packets without sending them to actor node then we reduce credibility of that particular sensor. If any sensor node want to be in routing process it need to send packets honestly in the future.

IV. Output and simulations

For small size wireless networks with few nodes still it is difficult to show analytically the relation between the nodes. For this NS2 network simulator is used to get our output and compare it with others. the parameters used in this experiments are given below in table 1. Sensors are placed randomly in the 500*500 network area some of the nodes are considered as harm full nodes.

Table 1. Simulation Parameters

Parameters	Values
Network Area	500*500
Simulation time	48
MAC Layer	802_11
No of sensors	44
No of Actors	2
Packet size	500
Sensor energy	50j

Packet delivery ratio: it is defined as the number of packets transferred from source to destination successfully. Due to the harm full nodes packet delivery ratio decreases in the network compare to normal time and it even decreases more in black hole attack compare to gray hole attack. To control the decrease in packet loss assured protective interrelated implementation method is adopted, if sensor node drops the packets it decreases the trust level based on its assurance a sensor selects a neighbor node to transfer the data hence this method reduces the packet loss in network.

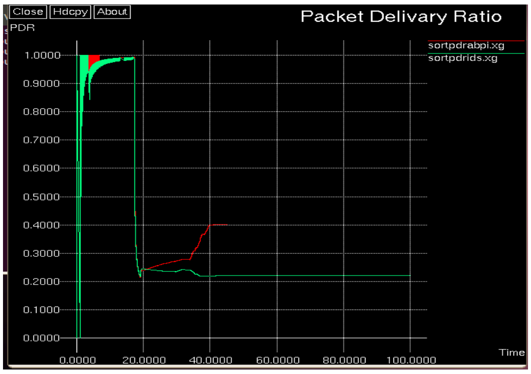


Fig. 2. Packet delivery ratio

Delay time: it is given as the average time taken for transferring a data packets from source to destination. Because of selective forward and black hole attacks average delay increases in network. As the no of sensors increases the average delay also increases. The given method performs better than existing mechanisms. As shown in fig3.

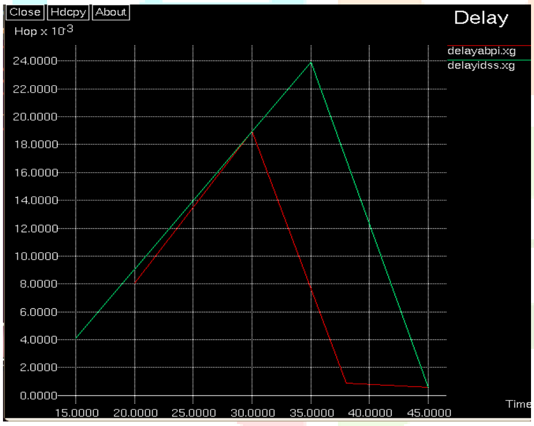


Fig. 3. Delay time

Energy consumption: it is given as the total amount of energy it consumed to establish the network and send the information from source sensor to actor in destination. Due to some packet loss in network while transferring the sensor has to retransmit the data. Because of this it consumes more energy in the network.

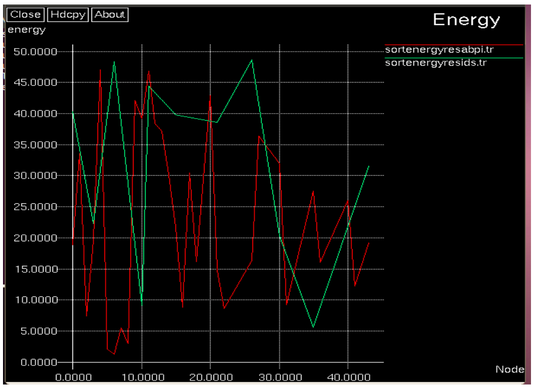


Fig. 4. Energy consumption

In our proposed method it consumes less energy compared to other mechanisms. As shown in above fig. 4.

V. Conclusion

WSAN is placed in open environment to feel the physical environment and take a reliable actions on it. Because of this these actors are always vulnerable to numerous kinds of passive and active attacks by harm full nodes. These type of attacks decrease the network productivity and effectiveness. In one of earlier work a delay and low energy consumption method is given for WSAN. In this paper an efficient assured reduction method is presented to control black hole and gray hole attacks. For delay and low energy consumption method in proposed technique every sensor examines its belief on its neighbor sensor depending upon the experience, advice and knowledge. The examined amount of trust is moved to the actors and it checks these values to find the harm full nodes in its cluster region. To estimate the performance of recommended method it is simulated in NS2 and examines Qos parameters like packet delivery ratio, avg energy dissipation in the network .The simulation output reveal that assured reduction technique executed well for the delay and it consumes less energy compared to the existing security techniques.

References

[1]. I. F Akyidiz and I.H. kasimoglu, “wireless sensor and actor network: research challenges” 2004.

[2] Y. Akkaya, Kemal and Mohamed, “Coverage and latency aware actor placement mechanisms in wsans,” 2008.

[3] S. G. A, H. Bozyigit, and F. B., “Cluster-based coordination and routing framework for wireless sensor and actor networks,” 2011.

[4] Z. Karakehayov, “Using reward to detect team black-hole attacks in wireless sensor networks,” 2005.

[5] A. B. A. Sheela.D, Srividhya.V.R and C. G.M., “Detecting black hole attacks in wireless sensor networks using mobile agent,” 2012.

[6] E.-H. Ngai, J. Liu, and M. R. Lyu, “On the intruder detection for sinkhole attack in wireless sensor networks,” 2006

[7] S. Kaplantzis, A. Shilton, N. Mani, and Y. A. Sekercioglu, “Detecting selective forwarding attacks in wireless sensor networks using support vector machines,” 2007

[8] W. Lou and Y. Kwon, “H-spread: a hybrid multipath scheme for secure and reliable data collection in wireless sensor networks,” 2006.

[9] B. Yu and B. Xiao, “Detecting selective forwarding attacks in wireless sensor networks,” 2006

[10] W. Xin-Sheng, Z. Yong-zhao, X. Shu-ming, and W. Liangmin, “Lightweight defense scheme against selective forwarding attacks in wireless sensor networks,” 2009

[11] J. Brown and X. Du, “Detection of selective forwarding attacks in heterogeneous sensor networks,” 2008.

[12] J. Cai, P. Yi, J. Chen, Z. Wang, and N. Liu, “An adaptive approach to detecting black and gray hole attacks in ad hoc
network,” 2010.