International Journal of Innovative Research in Advanced Engineering (IJIRAE) ISSN: 2349-2163
Volume 1 Issue 4 (May 2014) http://ijirae.com

BLACK HOLE ATTACKS MITIGATION AND PREVENTION IN WIRELESS SENSOR NETWORK

Ms.B.R.Baviskar
Dept. of E&Tc. PES's M.C.O.E
Pune, Maharashtra
Email id-bhagyashri.1424@gmail.com

Mr.V.N.Patil
Dept. of E&Tc, PES's M.C.O.E,
pune, Maharashtra,
email id- vvnnpp2002@yahoo.com

ABSTRACT: ***Wireless Sensor Network consists of nodes which communicate with each other with wireless channel. A general conception of wireless sensor network (WSN) nodes is static and it remains fixed in their position. It has been deployed in dominant manner for a long period of time. Many researches mostly focus on energy consumption in WSN sensor nodes. In WSN The security in wireless sensor networks (WSNs) is a critical issue due to the inherent limitations of computational capacity and power usage The Black hole attacks is one of the attack that challenges the security of WSN. Black hole attacks occur when an adversary cap-tures and re-programs a set of nodes in the network to block/drop the packets they receive/generate instead of forwarding them towards the base station. As a result any information that enters the black hole region is captured. Black hole attacks are easy to constitute, and they are capable of undermining network effectiveness by partitioning the network, such that important event information do not reach the base stations. Several techniques based on secret sharing and multi-path routing have been proposed in the literature to overcome black hole attacks in the network. However, these techniques are not very effective, and as we demonstrate, they may even end up making black hole attacks more effective. Propose an efficient technique that uses multiple base stations deployed in the network to counter the impact of black holes on data transmission, using java simulator and performance compare with multiple base station and without multiple base station to prevent black hole attacks. It implemented using Net bean IDE Java network simulator .***

Keywords: Wireless sensor network, black hole, multiple base station.

I.INTRODUCTION

A WSN is composed of large number of sensor nodes which are distributed in the wireless environment. This feature allows a random distribution of the nodes in the disaster relief operations or inaccessible terrains and several other applications. The other applications of WSN includes environmental control such as fire-fighting or marine ground floor erosion, also installing sensors on bridges or buildings to understand earthquake vibration patterns, surveillance tasks of many kinds like intruder surveillance in premises, etc. Due to the wireless nature and infrastructure-less environment of WSN, they are more vulnerable to many types of security attacks. Generally, the attacks are of two types in WSN- active attacks and the passive attacks. Black-hole attack is one of the harmful active attacks.

II. BLACK HOLE ATTACK

Black hole attacks are one such attacks in WSNs A black hole attack is an attack that is mounted by an external adversary on a subset of the sensor nodes (SNs) in the network. The adversary captures these nodes and re-programs them so that they do not transmit any data packets, namely the packets they generate and the packets from other SNs that they are supposed to forward. These term re-programmed nodes as black hole nodes and the region containing the black hole nodes as a black hole region.

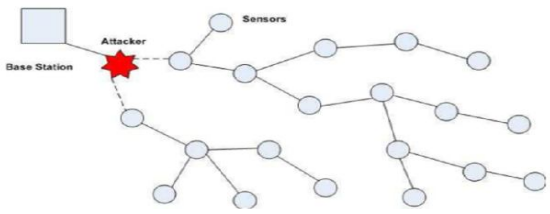

Fig -1 Black hole attack in WSN

Fig. 1 to illustrate these terms. In the figure, the small circles filled in black are black hole nodes and the black hole region is represented by red circle. When the source select the path including the attacker node, the traffic starts passing through the adversary node and this nodes starts dropping the packets selectively or in whole. Here, these re-programmed nodes are termed as black hole nodes and the region containing the black-hole nodes are black hole region. Black hole region is the entry point to a large number of harmful attacks.

III. Multiple Base station

In a WSN, the requirement of successful packet delivery to the BS is more essential than the requirement of prevention of data capture by an adversary. With the use of efficient data encryption algorithms, and data anonymity techniques , the information that an adversary can derive from captured packet(s) can be made inconsequential. Consequently, we concentrate on the objective of delivering the packet(s) to the BS in the presence of black hole nodes. A novel solution that uses the placement of multiple BSs to improve the likelihood of packets from the SNs reaching at least one BS in the network, thus ensuring high packet delivery success Use of multiple base stations to handle the flow of large amounts of ,heterogeneous data from the network and several optimization techniques have been designed for query allocation and base station placement . Here the use of multiple BSs is proposed for improving data delivery in the presence of black hole attacks.

IV TECHNICAL DESCRIPTION

The system model and assumptions for our technique are as follows. The network consists of a set of randomly deployed SNs, N={1...n}. The network consists of a set of BSs, B={B1,....., Bm}, which are more powerful than SNs and are connected to a replenish able power source. The density of the WSN is high enough to ensure adequate connectivity so that each SN can route data packets to all the BSs in the network. The BSs are assumed to be connected to each other over a wired network. We assume that the SNs in the network can be compromised by an external adversary and programmed to analyze the packets they receive and drop them instead of forwarding them to the BSs. We refer to a compromised SN as a black hole node. The adversary is capable of compromising more than one SN in the network, thus creating one or more black hole regions. In addition, the compromised nodes are capable of colluding with other compromised nodes in their neighborhood or in other black hole regions to analyze the captured packets. We assume that the SNs in the black hole region do not perform their environment sensing tasks as they are compromised.

V. RESULT AND DISCUSSION

The AODV protocols are simulated using Net Beans java network simulator software to activate network . The performance of using AODV protocols are compared with and without multiple based station on various network parameters.

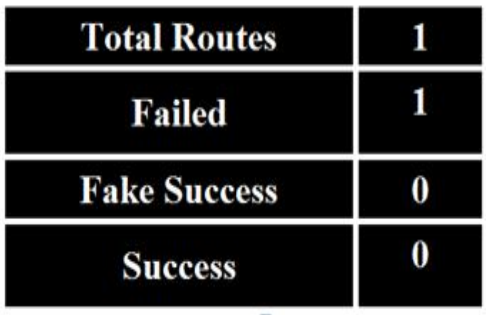

Fig 2 Output False & success Black Hole Attack by using one base station

For needed to save energy in WSN, initially routing path done through nearest base station i.e without using multiple base station .Routing through multiple base station is activated only when there is chance of black hole attack. By using encryption algorithm. To check presence of black hole nodes.

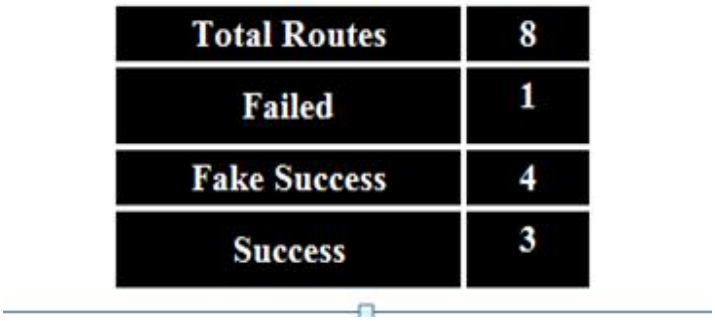

Fig 3 Output False & success Black Hole Attack by using multiple base station.

VI.CONCLUSION

Multiple base station technique to effectively mitigate the adverse effect of black hole attack in WSN. The detection of abnormal behavior of certain nodes is followed upon which the data transmission to multiple base stations is triggered. For this purpose we make use of encryption algorithm, which keep visiting the stationary nodes to detect any abnormality in the presence of black holes. These solution is highly effective and require little computation and message exchanges in network, thus saving energy of the SN.

REFERENCES

1 satyajayant Misr,Kabi Bhattarai.“*Hole attack mitigation with Multiple base station in Wireless sensor network* ”. 2011
2. “Detecting Black Hole attacks in Wireless sensor network using Mobile agent.”by Sheel D,Asma Begam 2012
3. Thamil salvi C.P “ *Novel method to detect black hole inWSN*” .“ International Journal of Computer Applications (0975 – 8887) Volume 45– No.17, May 2012 .
4. Pooja Kumari,Mukesh Kumar, Rahul Rishi, .“*Study of Security in Wireless Sensor Networ* International Journal of Computer Science and Information Technologies, Vol. 1 (5) , 2010.
5. Parul Kansal ,depali kansal“ compression of various routing protocol in wireless sensor network ”, International Journal of Computer Technologies, Vol. 1 (5) no-11, 2010.
6. Muazzam A. Khan, Ghalib A. Shah, Muhammad Sher “Challenges for Security in Wireless sensor network” International Journal of Computer Science and Information Technologies. vol.2,s5 2011
7. Z. Karakehayov. Using REWARD to detect team black-hole attacks in wireless sensor networks.In ACM Workshop on Real-World Wireless Sensor Networks , 2005.
8. W. Lou and Y. Kwon. H-SPREAD: A hybrid multipath scheme for secure and reliable data collecti on in wireless sensor networks. IEEE Transactions on Vehicular Technology , 55(4):1320–1330, 2006.

