Black hole Attacks Prevention in Wireless Sensor Network by Multiple Base Station Using of Efficient Data Encryption Algorithms

Ms.B.R.Baviskar¹, Mr.V.N.Patil¹
PES’s Modern College of Engineering Pune, India
Electronics and Telecommunications Engineering Department
bhagyashri.1424@gmail.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 captures and reprograms 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(Net Beans) and performance compare with multiple base station and without multiple base station to prevent black hole attacks.

Key word- Wireless sensor network, black hole, multiple base station.

1. INTRODUCTION

Large scale distributed wireless sensor networks (WSNs) have become popular in both the military and civilian domains [1]. However, several fundamental problems need to be addressed in these networks, especially in the area of security [4]. 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 reprograms 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 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.

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. Novel solution that uses the placement of multiple BSs to improve the of packets from the SNs reaching at least one BS in the network. Use of multiple base stations to handle the flow of large amounts of heterogeneous data from the network and several optimization techniques, 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.

2. RELATED WORK

Application of multiple base station in WSN carries many advantages especially following one (i) Decrease in energy consumption. Instead of data to be processed, agent is transmitted through network which can dramatically decrease quantity of data transmitted; (ii) Scalability. System performance without direct (iii) Gradual computing accuracy with effect of energy saving.

A. Security in WSN

The security in wireless sensor networks (WSNs) is a critical issue due to the inherent limitations of computational capacity and power usage. While a variety of security
techniques are being developed and a lot of research is going on in security field at a brisk pace but the field lacks a common integrated platform which provides a comprehensive comparison of the seemingly unconnected but linked issue user we attempt to comparatively analyse the various available security approaches highlighting their advantages and weaknesses. This will surely ease the implementers’ burden of choosing between various available modes of defence.

Wireless sensor networks (WSN’s) are quite useful in many applications since they provide a cost effective solution to many real life problems. But it appears that they are more prone to attacks than wired networks .They are susceptible to a variety of attacks, including node capture, physical tampering, and denial of service, prompting a range of fundamental research challenges, an attacker can easily eavesdrop on, inject or alter the data transmitted between sensor nodes.

Security allows WSNs to be used with confidence and maintains integrity of data. Without security, the use of WSN is any application domain would result in undesirable consequences. Particularly in military based projects where a compromise in security can lead to disastrous consequences. Thus security must be addressed in such critical sensor applications. It turns out that providing security in wireless sensor networks is pivotal due to the fact that sensor nodes are inherently limited by resources such as power, bandwidth, computation, and storage.

B. Security requirements :

1 Availability: Sensors are strongly constrained by many factors, e.g., limited computation and communication capabilities. Additional computations or communications consumes additional energy and if there is no more energy, data will not be available. Energy is another extremely limited resource in large scale wireless sensor networks.

A single point failure will be introduced while using the central point scheme. This greatly threatens the availability of the network. The requirement of security not only affects the operation of the network, but also is highly important in maintaining the availability of the whole network

2 Confidentiality: Data confidentiality is the most important issue in network security. Confidentiality, integrity and authentication security services are required to thwart the attacks from adversaries mentioned in the above section. These security services are achieved by cryptographic primitives as the building blocks. Confidentiality means that unauthorized third parties can not read information between two communicating parties. Especially in a military application, the data stored in the sensor node may be highly sensitive. Generally, encryption is the most widely used mechanism to provide confidentiality.

3 Integrity and authenticity: Confidentiality only ensures that data can not be read by the third party, but it does not guarantee that data is unaltered or unchanged. Integrity means the message one receives is exactly what was sent and it was unaltered by unauthorized third parties or damaged during transmission.

4 Data freshness: Data freshness means that the data is recent and any old data has not been replayed. Data freshness criteria are a must in case of shared-key cryptography where the key needs to be refreshed over a period of time. An attacker may replay an old message to compromise the key.

5 Self organization: Due to the ad-hoc nature of WSNs it should be flexible, resilient, adaptive and corrective in regards to security measures.

C. Various Types Attacks In Different Layers:-

In WSN there are different types of threats form in different layers in sensor networks can be broadly classified into Passive attacks and Active attacks. Passive attacks are in the nature of eavesdropping on, or monitoring of, range transmissions. The motive of the attacker is to obtain information that is being transmitted. Two types of passive attacks are release of message contents and traffic analysis.

Basicall in WSN mainly looking at two types of protection: protection from denial-of-service (DoS) attacks, and protection of the secrecy of information.

In physical layer jamming and tampering attacks are found due to this attacks spread spectrum. In link layer collision, exhaustion attacks are found. Black hole attacks are found in network layer. when black hole attacks accrued in network layer it, s act as sensor node due to attacks packet loss in network layer.

3. SURVEY OF TECHNIQUE USE TO BLACK HOLE ATTACK DETECTION IN WSN

There are several technique used to detect black hole attacks in MANET this technique not applied for WSN because of the high computation and storage requirements. For WSN proposed a technique in which transmitting SN performs power control to transmit a packet to more than one SNs in the direction of the BS. If an SN that is on the forwarding path does not forward a packet, then its next hop neighbor on the forwarding path will identify this event and report the SN as a black hole. This scheme is very expensive for a network with n black hole nodes.

The best technique was called the Multicast Tree Assisted Random Propagation (MTRP). In MTRP, instead of using deterministic multi-path routes to the BS to transmit data from the SNs, Shu et al. proposed the use of randomized routes. A share is routed in the direction of the BS on a randomized path until it traverses a pre-specified number of hops to a forwarding node. Subsequently, the share is routed deterministically to the BS from the forwarding node.

By using multiple base station placed multiple base station in different end and detect black hole attack in path of different base station.

Compare technique for WSN to detect the black holes. In multipart base station technique ,a black hole region close
(may also hold if it is far) to the Base Station can capture all packets with high probability. Also all the routes directed towards a single base station. In the use of multiple BSs for improving data delivery in the presence of black hole attacks.

4. 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.

B. 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 replenishable 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.

C. DESIGN AND IMPLEMENTATION

Let, B is the set of Base Stations available in the network, which are more powerful than SNs, B={B1,....,Bm}.

Let, \( B = \sum_{i=1}^{m} B_i \)

The Sensor network represented as a graph where, \( V = N \cup B \) where N represent the Sensor Node and B represents the Base Stations.

The Euclidean distance between two nodes i and j by \( d_{ij} \) is the line segment connecting them (ij). In Cartesian Coordinates, if \( i = (i_1, i_2, i_3,......, i_n) \) and \( j = (j_1, j_2, j_3,......, j_n) \) are two points in Euclidean n-space, then the distance from i to j or from j to i is given by,

\[
d_{ij} = d_{ji} = \sqrt{(i_1 - j_1)^2 + (i_2 - j_2)^2 + \cdots + (i_n - j_n)^2}
\]

distance between points i and j may have a direction, so it may be represented by another vector given by, \( i - j = \{i_1 - j_1, i_2 - j_2, \ldots, i_n - j_n\} \).

Identification of the Black Hole Nodes:- \( S_i \) denote the set of SNs identified by \( B_i \) as a black hole nodes, Routing tree routed at \( B_i \) will be given by, \( \{u, v, w, x, y, z, B_i\} \) \( S = \{ \text{Black Hole Nodes}\} \). Initially all SNs in the network are added to the set \( S_i \), \( N = \{1,\ldots,n\} \). All the BSs in B get together and create the global black hole set as,

\[ S = \bigcap_{i} S_i \]

Which are the SNs from whom none of the BSs got any data packet. This procedure performs in the network by regular time interval. Black hole node does not forward any packet to the BSs. As a result no black hole node is going to be a part of the path from any non-black hole SN to a BS. Consequently, these nodes will not be removed from the set \( S_i \).

So all the black hole nodes will be present in the set S. This proves that our scheme will be able to identify all the black hole node

5. RESULT

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.
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.

6. 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.