Detecting Black Hole Attacks in Wireless Sensor Networks using Mobile Agent

Sheela.D, Srividhya.V.R, Asma Begam, Anjali and Chidanand G.M.

Abstract— Wireless sensor network (WSN) have diverse field of application, but it is very much prone to the security threats. This paper proposes a lightweight, fast, efficient and mobile agent technology based security solution against black attack for wireless sensor networks (WSNs). WSN has a dynamic topology, intermittent connectivity, and resource constrained device nodes. The proposed scheme is to defend against black hole attack using multiple base stations deployed in network by using mobile agents. A packet drop attack or black hole attack 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 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. This mechanism does not require more energy. Here we implement a simulation-based model of our solution to recover from black hole attack in a Wireless Sensor Network. Comparison of communication overhead and cost were made between the system without using multiple base stations and the system with multiple base stations to prevent black hole attacks. Comparison was also made between the proposed attack detection system using mobile agent against the security system in the absence of mobile agents. The mobile agents were developed using the Aglet.

Keywords – WSN, multiple base stations, mobile agent, black hole attack.

I. INTRODUCTION

A. Black hole Attack

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. In this paper, we term these re-programmed nodes as black hole nodes and the region containing the black hole nodes as a black hole region. The entry point to a large span of insidious attacks. The techniques proposed in the literature for black hole attacks either use neighborhood interactions and message overhearing or secret sharing and path diversity.

B. 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, such as AES, 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. We propose 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. Given that in a WSN a BS is a laptop class device, the idea of deploying multiple BSs is inexpensive. Use of multiple base stations have been proposed in the literature 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.

C. Mobile Agent

Mobile Agent is defined as a software component which is either a thread or a code carrying its execution state to perform the network function or an application. Mobile agent methods have lot of advantages over traditional distributed computing method under circumstances of limitations on network.

II. RELATED WORK

Application of mobile agent computing model in WSN carries many advantages especially following ones:

1. Decrease in energy consumption. Instead of data to be processed, agent is transmitted through network which can dramatically decrease quantity of data transmitted;
2. Scalability. System performance without direct relationship with network scale, is supportive of balanced load;
3. Reliability, which means the capability of overcoming the influence by unreliable network links through reaching the
nodes accessed at time of establishing network links and Returning result after link recovered; (iv) Gradual computing accuracy. With the migration of mobile agent in network, computing result is required to become a gradually accurate. Once the requirement is met, mobile agent can return half-way with effect of energy saving.

A. Survey on black hole attack detection in WSN

Black hole attacks have been studied in the wired networks [2], [3], agent based networks, mobile ad hoc networks (MANETs) and wireless sensor networks [7], [11]. Most of the techniques proposed in non-WSNs do not apply to the black hole problem in WSNs, because of the high computation and storage requirements.

In [7], Karakehayov 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, for each original message, O(n) extra messages are required, which is very expensive.

In [11], the proposed an extension for WSNs, which addressed the combined objectives of security and reliability. In [13], Shuet al. proposed enhanced techniques based on the multi-path routing design proposed by Lou et al. in [11] and [10] to mitigate black hole attacks in the network. They consider the black hole region as illustrated by us in Section I. 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, Shuet 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.

We compare our technique with this algorithm as it is the best in the literature. We note that schemes based on secret-sharing and (node disjoint) multi-path routing suffer from a couple of serious problems. This approach does not consider the strategic position of the black holes. 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 may be prone to black hole attacks. Here we propose the use of multiple BSs for improving data delivery in the presence of black hole attacks. Our solution, despite being simple, outperforms the state of the art algorithms by more than 90%.

III. PROPOSED APPROACH

This system is designed to defend against black hole attack using multiple base stations deployed in network by using mobile agents. Routing through multiple base station algorithm is activated only when there is a chance of black hole attack. The probability of the presence of black hole nodes is found by mobile agents.

IV. BASIC DEFINITION

Definition 1: \( D_{AB} \rightarrow \text{Distance between two neighboring nodes (Say A & B).} \)

\[ D_{AB} = \frac{(R-d)}{V} \]

Where \( R \rightarrow \text{Transmission range} \); \( d \rightarrow \text{Distance between Node A and Node B.} \)

\( V \rightarrow \text{Average speed of the node.} \)

Definition 2: Counter of agent

It tells how many times the agent finds the particular Node as a one hop neighbor or as a child node to the previous Node. One mobile agent has agent ID, agent Program, agent briefcase (It contains some condition parameters such as \( D_{AB} \); Counter, Latest location Claim of node it visited.)

An agent is capable of sharing its briefcase with other agents and nodes. The state variables may be updated if necessary when an agent leaves a node.

Definition 3: Table details in every Node

Counter of every node tells how many times this node has been visited by an agent. i.e., it represents frequency of the visits by agents.

V. BLACK HOLE ATTACK DETECTION ALGORITHM

Neighboring nodes list is maintained by each node. Routing path is established using AODV Protocol. Initially routing is done through nearest base station i.e., without using multiple base stations. Routing through multiple base station algorithm is activated only when there is a chance of black hole attack. This is needed to save the energy in WSN.

To check the probability of the presence of black hole nodes,

- Mobile agent randomly visits very node.
- When mobile agent visits a node i,
  - it checks the frequency of receiving packets for every neighboring nodes in the list.
  - if it finds '0' (No packet from node j to node i) for neighboring node j.
    - it doubts node j is a black hole node.
    - it triggers routing process algorithm through multiple base stations for time t.
    - Within time t,
      - it confirms whether node j is a blackhole node or not.
      - if node j is a black hole node, it revokes node j.
    - After time t, it triggers routing process algorithm through nearest base station (without using multiple base stations)

The primary goal of agent is to detect the black hole nodes. This is done by giving information of one node to its neighboring nodes in the network. In order to achieve this goal with the least overload, we put forward a least visited neighbor first algorithm to control the navigation of mobile agent. An agent applies the algorithm to the information of node on which it currently resides, and decides its next destination.
VI. ROUTING USING MULTIPLE BASE STATIONS

In this section, we present the details of our technique which uses multiple Base Stations placed in the network to help mitigate the effect of black holes on data delivery in a WSN. Here, instead of only one BS at the top right corner of the network, four BSs are deployed at the four corners. This is one of the many possible ways of placing a set of BSs.

To reduce the extra computation and message exchange overheads on the sensor nodes in the network, this method is activated only when there is a chance of black hole attack. This is found using black hole detection algorithm which is explained in section V.

Assume that the packets from the SN \( u \) to the nearest Base Station is captured by the blackhole region. However, since \( u \) can route to the other Base Stations, its packets can still reach the remaining three Base Stations. We use this concept to provide a robust solution, with very little extra computation and message exchange overheads on the SNs in the WSN. Our technique requires transmission of redundant copies of a packet from each SN, but we note that this is no different from transmitting several shares. In fact, we use much fewer redundant communications.

VII. SIMULATION RESULTS

The proposed work was simulated using a open source simulator called JProwler. Prowler (ISIS 2006) is a probabilistic sensor simulator written in Matlab, and has a version build in java (JProwler). JProwler is build for MICA Mote hardware platform, which is running on Tiny OS. It also has a very efficient throughput, but it provides only one MAC protocol of TinyOS. Simulation parameter setting is given in table 1.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network scale</td>
<td>200m x 200m</td>
</tr>
<tr>
<td>No.of sensor nodes</td>
<td>25–400</td>
</tr>
<tr>
<td>No.of Base Stations</td>
<td>4</td>
</tr>
<tr>
<td>Energy level</td>
<td>0–64</td>
</tr>
<tr>
<td>Mobile Agent code size</td>
<td>500 bytes</td>
</tr>
<tr>
<td>Bytes accumulated by the mobile</td>
<td>100 bytes</td>
</tr>
<tr>
<td>agent at each sensor node</td>
<td></td>
</tr>
<tr>
<td>Mobile agent execution time at</td>
<td>50 ms</td>
</tr>
<tr>
<td>each node</td>
<td></td>
</tr>
<tr>
<td>Mobile agent instantiation delay</td>
<td>10 ms</td>
</tr>
</tbody>
</table>

Figure 1 shows how is average energy at nodes decreased for increased time because of storage of neighboring nodes information matrix at every node.

Figure 2 shows the relationship between probability of black hole detection with number of nodes. Figure 3 shows the average probability of black hole attack detection in the presence and the absence of mobile agents.

VIII. CONCLUSION

The proposed approach gives an approach for secure routing algorithm against black hole attacks for wireless sensor networks. Delivering data to the base station is more important especially in the case of real time applications for which it is designed. By having several base stations we make
sure that data is being delivered to the destination base station despite the presence of black hole regions near the neighborhood of the sensor nodes near the base station. This ensures data delivery and the security of the data delivered can be taken care of by using encryption algorithms. Further to avoid unnecessary transmission of packets to multiple base stations, 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 mobile agents which keep visiting the stationary nodes to detect any abnormality in the presence of black holes. The performance of the proposed approach has been examined through simulations.

REFERENCES