# Mollifying the Effect of Cloning, Sink Hole and Black Hole Attacks in Wireless Sensor Networks using Mobile Agents with Several Base Stations

D Sheela
Associate Professor
Department of CSE Department of CSE
AMC Engineering College

G. Mahadevan, PhD.
Professor and Head of Department
AMC Engineering College

## ABSTRACT

Three dangerous attacks in wireless sensor network is handled in this proposed security solution. This paper proposes a lightweight and fast mobile agent technology based security solution against cloning attack, sinkhole attack and black hole attack for wireless sensor networks (WSNs).Recently mobile agents have been proposed in wireless sensor networks to reduce the communication cost especially over low bandwidth links. The proposed scheme is to defend against cloning attack, sink hole attacks and black hole attacks using mobile agents. In the cloning attack, adversary introduces replicas of compromised node. In the sinkhole attack, an adversary lures traffic through a compromised node. A black hole attack is a type of denial-of-service attack accomplished by dropping packets for a particular network destination in bulk (by dropping all packets).For dealing with black hole attacks more than one base station concept is also added with mobile agent concept to bring the best result. Here we implement a simulation-based model of our solution to recover from cloning attack, sinkhole attack and black hole attack in a Wireless Sensor Network. This mechanism does not require more energy.Comparison of communication overhead and cost were made between the proposed attack detection system using mobile agent against the security system in the absence of mobile agents. Comparison was also done between the proposed security system with the security system handling single attack. The mobile agents were developed using the Aglet.

## General Terms

Security, Algorithms, System.

## Keywords

WSN, mobile agent, cloning attack, sink hole attack, black hole attack, multiple base station.

## 1. INTRODUCTION

The main focus of proposed system is on security in wireless sensor networks against cloning attack, sink hole attack and black hole attack. Here, we describe these three attacks and state the problem to be solved.

### 1.1 Cloning Attack

Clone attack or node replication attack is a severe attack in WSNs. In this attack, an adversary captures only a few of nodes, replicates them and then deploys arbitrary number of replicas throughout the network. It is very hard to distinguish between non compromised node a clone node Since a clone has the same security and code information of original node. Hence cloned nodes can launch a variety of other attacks. The detection of cloning attacks in a wireless sensor network is therefore a fundamental problem. Many existing protocols expose the following limitations: high performance overheads, unreasonable assumptions, necessity of central control, lack of smart attack detection etc. Few existing approaches like [2] solved these problems. But here we present a security model to detect two more attacks along with cloning attack detection with the same communication cost and performance overhead. The part of our proposed system which deals with cloning attack detection is described in section 6. We used the benefit of mobile agent to reduce the communication cost. Also the proposed protocol considers Mobile Wireless Sensor Network environment.

### 1.2 Sinkhole Attack

In a sinkhole attack, the goal of an adversary is to lure nearly all the traffic from a particular area through a compromised node, creating a metaphorical sinkhole with the adversary at the center. Because nodes on, or near, thepath that packets follow have many opportunities to tamper with application data, sinkhole attacks can enable many other attacks (selective forwarding, for example). Sinkhole attacks typically work by making a compromised node look especially attractive to surrounding nodes with respect to the routing algorithm. For instance, an adversary could spoof or replay an advertisement for an extremely high quality route to a base station.One motivation for mounting a sinkhole attack is that it makes selective forwarding trivial. By ensuring that all traffic in the targeted area flows through a compromised node, an adversary can selectively suppress or modify packets originating from any node in the area.

Two examples of sink hole attack are

- Malicious node redirects with modified route sequence numbers. Here malicious node sends greater sequence number to misguide that it is a fresh route.
- Malicious node redirects with modified hop count. Here malicious node sends lesser hop count value to tell that this is shortest path. In fact there is no such path exists.

The proposed security model avoids sink hole attack by 99% along with the detection of cloning and black hole attacks.The part of our proposed system which deals with sink hole attack detection is described in section 7.

### 1.3 Blackhole attack

A Black hole attack of WSN is an attack that is mounted by an external adversary on a subset of the sensor nodes 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 sensor nodes 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*.is 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 [4], [5] or secret sharing and path diversity [6], [7], [8]. Techniques based on neighborhood message interactions and overhearing work under the assumption that the sensor node in the neighborhood of a black hole node are not compromised and hence can monitor and report the black hole node. However, if several sensor nodes that are in close proximity are compromised and collude among themselves, then they can easily make neighborhood overhearing-based techniques ineffective. The path diversity and secret sharing based techniques, although better, are still not very effective.

In a WSN, the requirement of successful packet delivery to the base station 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 [9], and data anonymity techniques [10], 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 base station in the presence of black hole nodes. Given that in a WSN a base station is a laptop class device, the idea of deploying multiple base stations 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 [11], [12]. Here the use of multiple base stations is proposed only when there is a probability for the presence of black hole nodes in a WSN.

## 1.4 Mobile Agent

A Mobile Agent, namely, is a type of software agent, with the feature of autonomy, social ability, learning, and most importantly, mobility. More specifically, a mobile agent is a process that can transport its state from one environment to another, with its data intact, and be capable of performing appropriately in the new environment. Mobile agents decide when and where to move. Movement is often evolved from remote procedure call methods. Mobile agents have raised considerable interest in the research community (Agent Tcl, Tacoma, and Mole, for example) and in industry (Aglets, Concordia, Jumping Beans, and the like). Mobile agents are not a new concept. It borrows from the Xerox Worm done 30 years ago, from OS process migration work done in the 1980s, from remote evaluations done more than 20 years ago at MIT, and so on. [13].Many advantages which mobile agents have over conventional agents are discussed in [17-19].

Communicating single bit over the wireless sensor network at short ranges consumes more energy than processing that bit. Thus, minimizing the amount and range of communication is very important. Mobile agents were proved to greatly reduce the communication cost especially over low bandwidth links, by moving the processing function to the data rather than bringing the data to a central processor[14-16]. Mobile agent paradigm is proposed here for reducing the communication cost and making the entire detection process easier.

## 2. RELATED WORK

Few prior security proposals for cloning attack, sinkhole attack and black hole attack in wireless sensor network is discussed here.

## 2.1 Survey on cloning attack detection in WSN

In the node replication attack [20], an attacker intentionally puts replicas of a compromised node in many places in the network to incur inconsistency. The node replication attack can enable attackers to subvert data aggregation, misbehavior detection, and voting protocols by injecting false data or suppressing legitimate data [20]. Conventional methods to detect a node replication attack usually include centralized computing based on node locations or the number of simultaneous connections, which is vulnerable to the single-point failure. Distributed detection of the node replication attack was proposed in [20], where each node is assumed to know its location, and it is required to send its location to a set of witness nodes. If a witness node finds a contradiction in the location claims of a suspected node identity, this suspected node identity must be replicated many times. Asymmetric key technology is used here to guarantee the authenticity of location claims. A similar approach is discussed in [21]: each node has a private key corresponding to its location, and the location based key can be used to detect node replicas. RAWL and TRAWL is discussed in [2] presented a non-deterministic and fully distributed replica detection protocol. It greatly reduces the communication and memory overhead when compared to many previous protocols. Still it has a slight communication overhead because of more number of random walks to get an efficient result. Here we tried to develop the detection protocol which deals two more dangerous routing attacks namely, sink hole and black hole attacks along with this cloning attack detection procedure without increasing memory and communication cost.

## 2.2 Comparison between existing and current methods to detect sink hole attacks in WSN

Network overload is very high in many existing methods to detect sink hole attacks in WSN. And many existing approaches to detect sink hole attacks uses encryption and authentication mechanisms, it has encryption, decryption and key overhead. The proposed approach uses mobile agent to defend against sink hole attack to avoid all the above discussed disadvantages.

Packet leashes [22] are based on geographical and temporal packet leashes. The use of geographical leashes assumes knowledge of the node location. The use of temporal leashes requires all nodes to have tightly synchronized clocks and demands computational power, which according to the authors, is beyond the capability of sensors. SECTOR [23] is based on measurement of the time of flight of a message in a challenge–reply scheme. Such a scheme assumes that sensors are able to execute time measurements of nanosecond precision and, hence, this scheme requires very accurate clocks at each sensor. In addition, distance estimates based on the time of flight are sensitive to distance-enlargement errors. Sink hole attack detection [24] finds a list of suspected nodes, and then carries out a network flow graph identifying a sink attack by observing data missing from an attacked area. The method is based on a central processing unit, which is not convenient in a wireless sensor network.

## 2.3 Survey on Black hole attack detection in WSN

Black hole attacks have been studied in the wired, agent based and mobile ad hoc networks. 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 [25], Karakehayov proposed a technique in which transmitting sensor node performs power control to transmit a packet to more than one sensor nodes in the direction of the base station. If a sensor node 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 sensor node 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.

Satyajayant Misra*et al.* Identified [3] couple of serious problems on existing schemes based on secret-sharing and (noded is joint) multi-path routing suffer from a couple of serious problems. [3] listed out these problems : strategic position of the black holes is not considered; a black hole region close 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. Also [3] proposes the use of multiple base stations for improving data delivery in the presence of black hole attacks. Our solution, takes the best part of this and combines this with the detection schemes of cloning and sink hole attacks without increasing the communication and memory cost. Our solution also reduces the overhead of multiple base stations by the detection of abnormal behavior of certain nodes (using mobile agents) is followed upon which the data transmission to multiple base stations is triggered.

## 3. PROPOSED APPROACH

This system is designed to make every node aware of location and identity of many nodes (Say n) so that each neighbor of node A verifies the signature and checks the plausibility of Location of A. When a node finds a collision (2 different location claims with the same ID), it broadcasts the two conflicting claims as evidence to revoke the replicas. And this system also makes every node aware of the entire network so that a valid node will not listen the cheating information from malicious or compromised node which leads to sink hole attack. The role of mobile agent in this part is to prepare and update the global information table at every sensor node. This system is also designed to defend against black hole attack using multiple base stations deployed in network by using mobile agents. Routing through multiple base station algorithms 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. Data routing algorithm tells how a node uses the global network information to route data packets.

Thus the proposed security solution has three parts. Part-I: CA (Cloning Attack detection) is to detect clones and any malicious nodes. Part-II: SA (Sink hole Attack avoidance) algorithm is to tell how a node uses the global network information to route data packets by avoiding sink hole attack. Part-III : BA ( Black hole Attack avoidance) is to find the probability of the presence of black hole nodes and to trigger the routing process through multiple base station accordingly. Note that the above said three parts run parallel all the time. The proposed system also has an Agent Routing Algorithm to route mobile agents which tells how does a mobile agent gives location and network information to nodes and visits every node.. The proposed security solution can also be applied to Mobile WSN.

## 4. BASIC DEFINITION

Definition 1 : $D_{AB}$ → Distance between two neighboring nodes ( Say A & B).

$D_{AB}$ = (R-d) / V ; Where R → Transmission range; d → Distance between Node A and Node B ; V → 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.)

Definition 3: Table details in every Node

The structure of every nodej ie., sensor node information list is shown in the table1.Counter of every node tells how many times this node has been visited by an agent (frequency of the visits by agents).

**TABLE 1 SENSOR NODE (J )INFORMATION LIST**

| Node | 1 | 2 | .<br>.<br>. | i | .<br>.<br>. | N | counter | History |
|---|---|---|---|---|---|---|---|---|
| 1 | | | | | | | | |
| 2 | | | | | | | | |
| ... | | | | | | | | |
| j | | | | | | | | |
| ... | | | | | | | | |
| N | | | | | | | | |

History information of recent 3 visits

This cell has Four information. (If it is a non-zero value) Among this, two are global information, and other two are local to that sensor node (here, node j):

Global information: This information is filled for every cell x*y where x and y are any node from 1,2,….,N.

- Agent packet counter information tells how many times agent visited j after i . i.e., how many times agent found j as a one hop neighbor of i. (This is helpful for finding sink hole nodes.)
- Location claim of node i. (**Note** : There will be no updating a value if this entry is same as the location claim of node i carried by mobile agent. Here more than one entry may be made only when mobile agent carries a different latest location claim for the same node i). (Here maximum three entries, i.e., latest three location claim for mobile nodes can be made.)

Local information: This information is filled only for $j^{th}$ row (j is the current sensor node)and $NN_1$,$NN_2$,$NN_3$,….$NN_n$ columns where $NN_1$ to $NN_n$ are one hop neighboring nodes of j.(Note : neighboring nodes list may be changed since nodes are mobile. So one hop neighboring nodes list should be updated often. )

- $D_{ji}$ (**Note :**$D_{ij}$ should not be more than the transmission range.If $D_{ji}$ is more than the transmission range, there is a chance of a cloning attack).
- The value fp (Frequency of packets) , which tells the number of packets received so far (for the last time period t1 ) by sensor node j from sensor node i.(This is helpful for finding black hole nodes.)

Definition 4: Key information of every node

Every node A is given a private key , $PR_A$ and the public key , $PU_A$ during the deployment. More powerful key managing techniques can be adopted in future.

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.

## 5. AGENT ROUTING ALGORITHM

The primary goal of agent is to deliver information of one node to others 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. Each node has an information cache that agents can update with more recent values. Nodes access this shared cache whenever they require information about the network.

When the agent reaches a node ifrom node k, agent program performs the following steps.

**Step1:** Update the information table of node iwith any newer information available in its own briefcase.

As a whole of this step, when an agent reaches a node i from node k, the following information is to be updated in the current sensor node i , if it is not existing or old information.

i) $D_{ik}$

ii) Agent packet counter information: It tells how many times agent finds this particular nodei as a one hop neighbor to the previous node. Otherwise it means that how many times agent finds this particular node as a child node of the previous node.(To describe more of this: The counter of all nodes stored in the information cache of node i is compared with the corresponding counter carried in the briefcase of this agent. If the counter of some nodes, say j , in the host node's information cache happens to be less than that in the agent's briefcase, obviously, the agent is carrying more recent information about node j. In that case, the entire information about node *j* in the host node's cache is overwritten by information in the agent's briefcase.)

iii) Available location claims from agent's brief case.

**Step2:** Mobile agent checks the fp value (frequency of receiving packets for every neighboring nodes) in the sensor node 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. And it triggers routing process algorithm through multiple base stations for time t2.

**Step3:** Agent gets the signed location claim= {IDi, Li, EP PRi {H(Idi || Li)} of node i. It is compared with the location claim of node i in the agent's briefcase. If it is similar, there is no updation for that field in agent's briefcase. Otherwise that field is updated with the latest location claim of node i. The entire step is done after checking the location plausibility of location Li. ie.,$D_{ik}$ should not be more than the transmission range. Here k is any one hop neighbor of node i which was previously visited by an agent.

**Step4:** Determine which neighboring node has the least counter. It is the least visited neighbor.

**Step 5:** If this neighbor of *i*hasn't been visited in recent 3 times, the agent selects this neighbor as its next destination. History information about the last 3 visits can be found in the node's information cache. In case node selected has been visited in the recent past, the agent selects the second least visited neighbor, and so on.

**Step 6:** After choosing the next destination, the agent updates its next destination's ID with the chosen destination node ID, and changes the history variables in the host node's information cache with the next destination node.

## 6. PART I OF SECURITY SOLUTION: CA (CLONE ATTACK DETECTION)

The important steps of CA are

- Every node A prepares a signed location claim. Signed location claim = $ID_A$, $L_A$, $EP_{PRA}$ {H($Id_A$ || $L_A$)} Preparation of location claim is explained in the Figure 1. Here, EP $_{PRA}$( M ) means encrypting M using private key of node A.

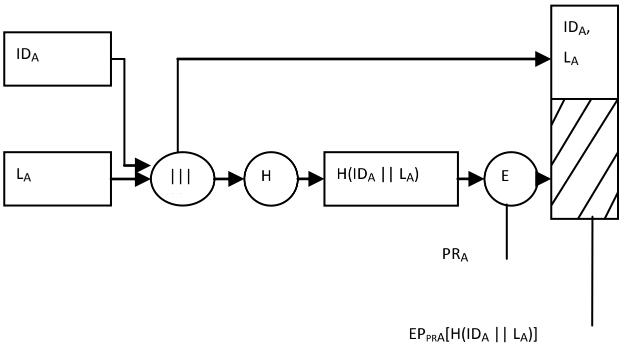

**Figure 1: Preparation of location claim**

- Mobile agent gets the signed location claim of node which is visited by it. The node's information matrix can be acquired through mobile agent routing algorithm.
- Each node A gets the information matrix (Table 1), verifies the signature and checks the plausibility of $D_{AB}$(e.g. the distance between the neighbors cannot be bigger than the transmission range.)
- Signature verification is explained in the Figure 2.
- Here, more than one entry for signed location claim may be made in a single cell of an information matrix of one node. It happens only when mobile agent carries a different latest location claim for the same node i. (Because nodes can also be mobile.)

When a node finds a collision (2 different claims with the same ID),It broadcasts the two conflicting claims as evidence to revoke the replicas. Each node receiving the two claims independently verifies two signatures. If two signatures are valid, it terminates links with replicas.

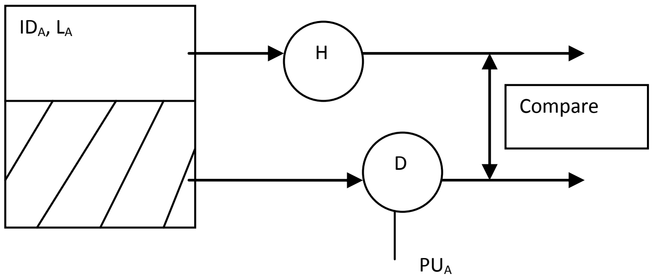

**Fig 2: Signature verification**

## 7. PART II OF SECURITY SOLUTION: SA (SINK HOLE ATTACK AVOIDANCE)

This algorithm is used for routing the data by avoiding the sink hole attack. The node's information matrix can be acquired through mobile agent routing algorithm. When the data packets wanted to be sent to node *B*, it can be transmitted by this methodaccording to node *A*'s information matrix.

Suppose node Ais the source node, node Bis the destination node. Communicating with node B, node Aperforms as follows:

**Step1:** Examine $TabVal_{AB}$of A's matrix. If $TabVal_{AB}$is not equal to 0 (has a non zero value), there is a connection between A and B. The data packets are sent to Bdirectly . End routing. Otherwise, go to step2.

**Step2:** check the column, *B* , in the cache of node B, and find out all the items which are not equal to zero in *B* , these items are the child nodes of node B;

If TabVal$_{B}$ != 0 for node$_{1}$ to node $_{n}$ where n can be 1 to max number of nodes present in the network. So, node1 to node $_{n}$ are child nodes of B.

If all the items in *B* are equal to zero, then, there is no valid route between node A and nod B, and the routing ends.

**Step3:** Set the maximum number of hops to reach the destination as n.

**Step4:** Initialize k =1. Where k = current number of hops.

(After finding child nodes of node$_{1}$ to node $_{n}$ , will be incremented by one. k can reach upto n.)

This process continues till it reaches to A.

Here maximum repeated hop with less weight is selected every time. i.e., Maximum agent counter value with less TabVal$_{AB}$ For every neighboring nodes A & B. It limits the chance of paths containing sink hole.

*A. Illustration*

Consider a very small network in figure 3. Links in this figure shows that the nodes are in the transmission range. The sample information matrix prepared by our proposed method for this network is shown in the table 2. To simplify the explanation here, only agent counter information is considered in this part.

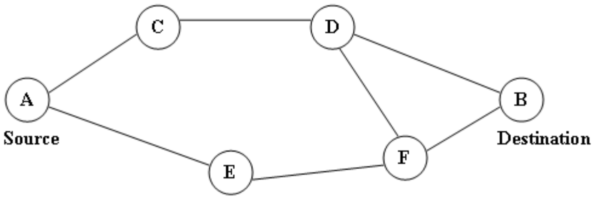

**Fig 3: Sample Network**

TABLE 2 SAMPLE INFORMATION MATRIX

| TabVal | A | B | C | D | E | F |
|---|---|---|---|---|---|---|
| **A** | | 0 | *** | 0 | *** | 0 |
| **B** | 0 | | 0 | *** | 0 | *** |
| **C** | *** | 0 | | *** | *** | 0 |
| **D** | 0 | *** | *** | | 0 | *** |
| **E** | *** | 0 | 0 | 0 | | *** |
| **F** | 0 | *** | 0 | *** | *** | |

In the table 2,

*** has 3 information. (Non-zero value). The following is explained for **** by assuming X as row and Y as column.

i) D$_{XY}$ -Distance between X node & Y node =(R-d)/v

ii) Agent packet counter information tells How many times Agent visited X after Y.i.e., How many times agent found Y as a one hop neighbor of X.

iii)fp – Number of packets received for the last time period time t1 by node X from node Y.

iv) Location claim of node Y. (**Note**: There will be no updation if this entry is same as the location claim of node i carried by mobile agent. Here more than one entry may be made only when mobile agent carries a different latest location claim for the same node Y).

To send a packet from Node A to Node B,

- TabVal$_{AB}$ = 0 → No one hop route.
- Check TabVal$_{B}$ in the cache of B to get child nodes of B.
  TabVal$_{B}$ != 0 for D & F.
  So, D & F are child nodes of B.
- Set the maximum number of hops to reach the destination as n.
- Initialize k =1. Where k = current number of hops.
  (After finding child nodes of D or/and F , k will be incremented by one. k can reach upto n.)
  This process continues till it reaches to A.
- For n=3
  - B → D ; B → F
  - B → D → C
    B → D → F
    B → F → D
    B → F → E
  - B → D → C → A (One Route)
  B → D → F → E
  B → F → D → C
  B → F → D → F
  B → F → E → A
→
(Another route)

Maximum repeated hop with less weight is selected every time. i.e., Maximum agent counter value with less TAB For every neighboring nodes A & B. It limits the chance of paths containing sink hole.

## 8. PART III OF SECURITY SOLUTION: BA (BLACK HOLE ATTACK AVOIDANCE)

Neighboring nods list is maintained by each node as shown in table 1. 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 visitsevery node according to agent routing algorithm which was explained in section V.
- 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 blackhole node.
    - it triggers routing process algorithm through multiple base stations (explained in section 9 ) for time period t2.
    - Within time t2,
      - 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 in this part is to detect the black hole nodes . This is done by giving information of one node to its neighboring nodes in the network.

## 9. 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 8..

Assume that the packets from the sensor node*u* to the nearest base station is captured by the black hole 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. The base concept of using multiple base stations is derived from [3].

## 10. 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 built 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 3.

TABLE 3 SIMULATION PARAMETER SETTING

| Parameter | Value |
|---|---|
| Network scale | 200m x 200m |
| No.of sensor nodes | 25~400 |
| Energy level | 0~64 |
| Mobile Agent code size | 500 bytes |
| Bytes accumulated by the mobile agent at each sensor node | 100 bytes |
| Mobile agent execution time at each node | 50 ms |
| Mobile agent instantiation delay | 10 ms |

TABLE 4. COMPARISION OF METHODS TO DETECT CLONING , SINK HOLE AND BLACK HOLE ATTACKS WITH / WITHOUT MOBILE AGENTS

| Sample Executions | 1 | 2 | 3 |
|---|---|---|---|
| Simulation details: | | | |
| No. of nodes | 100 | 200 | 300 |
| No. of cloned nodes | 10 | 20 | 15 |
| No. of sink hole nodes | 10 | 20 | 20 |
| No. of black hole nodes | 10 | 20 | 25 |
| Cloning attack detection without using mobile agent [2] | | | |
| Cloned nodes found | 4 | 8 | 6 |
| Cloned nodes missed | 6 | 12 | 9 |
| Communication overhead | 14000 | 30799 | 46200 |
| Memory overhead | 14600 | 30800 | 46800 |
| Cloning attack detection by using mobile agent (only part –I of our proposed protocol) | | | |
| Cloned nodes found | 7 | 14 | 12 |
| Cloned nodes missed | 3 | 6 | 3 |
| Communication overhead | 11000 | 22000 | 33000 |
| Memory overhead | 11700 | 23000 | 34000 |
| Sink hole attack detection without using mobile agent [5] | | | |
| Sink hole nodes found | 5 | 7 | 8 |
| Sink hole nodes missed | 5 | 13 | 12 |
| Communication overhead | 18200 | 36400 | 54600 |
| Memory overhead | 19300 | 37500 | 57600 |
| Sink hole attack detection by using mobile agent (only part II of our proposed protocol) | | | |
| Sink hole nodes found | 6 | 12 | 16 |
| Sink hole nodes missed | 4 | 8 | 4 |
| Communication overhead | 13000 | 26000 | 39000 |
| Memory overhead | 12200 | 24520 | 40100 |
| Black hole attack detection with multiple base stations and without using mobile agent [3] | | | |
| Black hole nodes found | 4 | 8 | 10 |
| Black hole nodes missed | 6 | 12 | 15 |
| Communication overhead | 14000 | 27000 | 42000 |
| Memory overhead | 15000 | 28000 | 43000 |
| Black hole attack detection with optional multiple base stations by using mobile agent(only part II of our proposed protocol) | | | |
| Black hole nodes found | 6 | 14 | 20 |
| Black hole nodes missed | 4 | 6 | 5 |
| Communication overhead | 10000 | 20000 | 30000 |
| Memory overhead | 11000 | 22000 | 31000 |
| Our proposed protocol of cloning, sink hole and black hole attacks by using mobile agent (part I, II and III of our proposed protocol parallelly) | | | |
| Cloned nodes found | 7 | 16 | 13 |
| Sink hole nodes found | 8 | 17 | 22 |
| Black hole nodes found | 7 | 17 | 18 |
| Cloned nodes missed | 3 | 4 | 2 |
| Sink hole nodes missed | 2 | 3 | 3 |
| Black hole nodes missed | 3 | 3 | 2 |
| Communication overhead | 11345 | 22670 | 34000 |
| Memory overhead | 11640 | 23180 | 35033 |

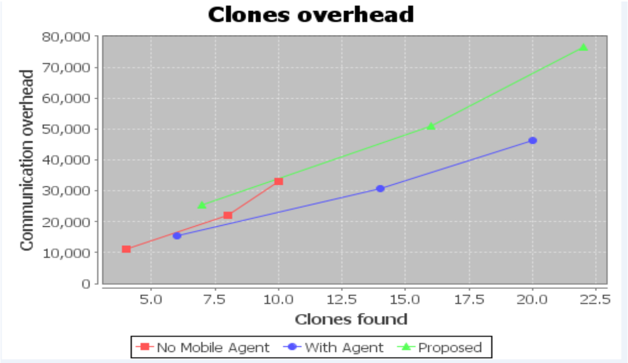

**Fig 4: Cloning attack detection overhead**

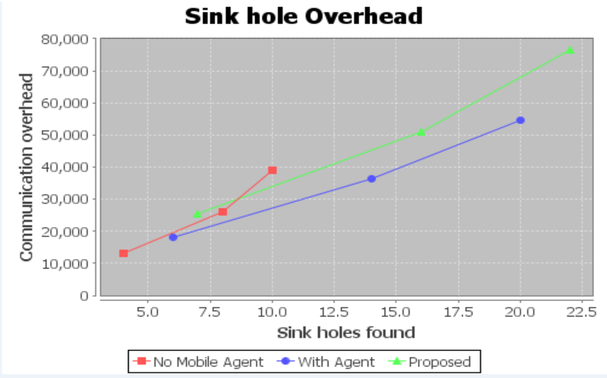

**Fig 5: Sinkhole attack detection overhead**

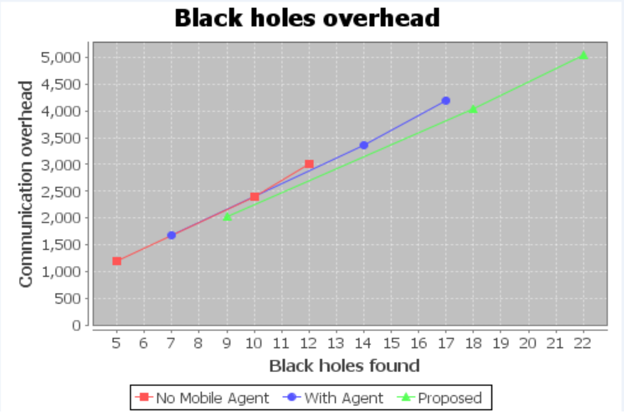

**Fig 6: Black hole attack detection overhead**

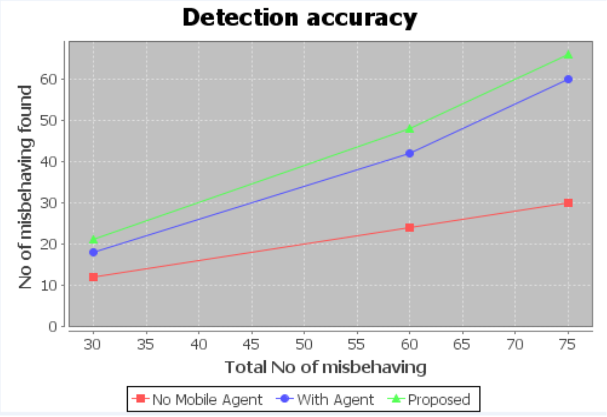

**Fig 7: Detection accuracy**

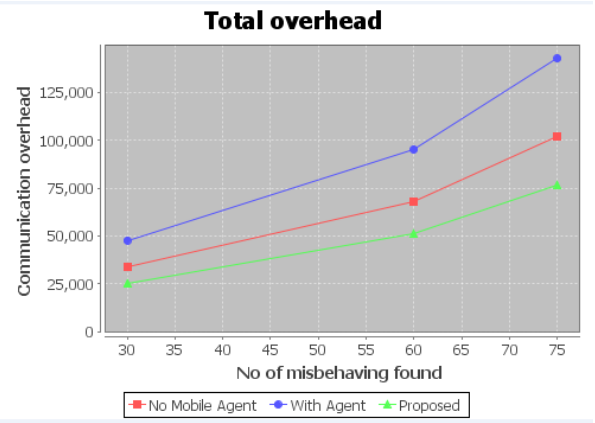

**Fig 8: Total overhead**

The above simulation results (Fig.4 to Fig.8) show the comparison between the communication overhead with average probability of detection method (cloning/ sink hole/ black hole) using mobile agent with the existing detection methods without using mobile agent. It shows that the communication overhead is very less for the method which uses mobile agent.It also shows the total communication overhead for our proposed protocol to detect cloning, sink hole and black hole attacks is same as the communication overhead of a protocol which detects a single attack. It also proves that the detection accuracy is higher than the existing protocol.

## 11. CONCLUSION

In this paper a mobile agent based security solution is proposed for wireless sensor network to detect clone attack, black hole attack and to avoid sink hole attack with the communication overhead of finding a single attack.The performance of the proposed approach has been examined through simulations.

## 12. REFERENCES

[1] Yun zhou and Yuguang fang, university of florida, Yanchaozhang, new jersey institute of technology, “Securing Wireless Sensor Networks : A survey”,IEEE Communications, 3rd quarter 2008, volume 10, no. 3.

[2] YingpeiZeng, Jiannong Cao, *Senior Member, IEEE*, Shigeng Zhang, ShanqingGuo and Li Xie, “Random walk based approach to detect clone attacks in wireless sensor networks”, IEEE Journal of selected areas in communication, vol 28,No.5, June 2010.

[3] SatyajayantMisra, KabiBhattarai, and GuoliangXue, “BAMBi: Blackhole Attacks Mitigation with Multiple Base Stations in Wireless Sensor Networks”, IEEE ICC 2011 proceedings.

[4] Z. Karakehayov. Using REWARD to detect team black-hole attacks in wireless sensor networks.In *ACM Workshop on Real-World Wireless Sensor Networks*, 2005.

[5] S. Roy, S. Singh, S. Choudhary, and N. Debnath. Countering sinkhole and black hole attacks on sensor networks using dynamic trust management. In *IEEE Symposium on Computers and Communications*, pages 537–542, 2008.

[6] W. Lou, W. Liu, Y. Zhang, and Y. Fang.SPREAD: enhancing data confidentiality in mobile ad hoc networks. In *IEEE FOCOM*, volume 4, pages 2404–2413, 2004.

[7] W. Lou and Y. Kwon. H-SPREAD: A hybrid multipath scheme for secure and reliable data collection in wireless sensor networks. *IEEE Transactions on Vehicular Technology*, 55(4):1320–1330, 2006.

[8] M. Ketel, N. Dogan, A. Homaifar. Distributed Sensor Networks Based on Mobile Agents Paradigm. Proc. 37th Southeastern Symposium on System Theory, Tuskegee, AL, USA, 2005: 411-414.

[9] S. Didla, A. Ault, and S. Bagchi.Optimizing AES for embedded devices and wireless sensor networks. In *Proceedings of the 4th International Conference on Testbeds and research infrastructures for the development of networks & communities (Trident)*, pages 1–10, 2008.

[10] S. Misra and G. Xue. Efficient anonymity schemes for clustered wireless sensor networks. *Intl. Journal of Sensor Networks*, 1(1):50–63, 2006.

[11] S. Kim, J.-G. Ko, J. Yoon, and H. Lee. Multiple-objective metric for placing multiple base stations in wireless sensor networks. In *Proceedings of the International Symposium on Wireless Pervasive Computing*, pages 627–631, February 2007.

[12] B. Xiao, B. Yu, and C. Gao. CHEMAS:Identify suspect nodes in selective forwarding attacks. *Journal of Parallel and Distributed Computing*,.

[13] DejanMilojicic,Charles Petrie, Chris Rygaard“ Mobile agent applications” IEEE concurrency.,July1999.

[14] Zhang Yuyong, Jingde. Mobile Agent Technology. Beijing, Tsinghua University Press, 2003.

[15] Zhu Miaoliang, Qiuyu. Mobile Agent System. Journal of Computer Research and Development, 2001, 38(1): 16-25.

[16] G. Sladic , M. Vidakovic and Z. Konjovic Agent based system for network availability and vulnerability monitoring 2011 IEEE 9th International Symposium on Intelligent Systems and Informatics • September 8-10, 2011, Subotica, Serbia.

[17] L. Tong, Q. Zhao, S. Adireddy. Sensor Networks with Mobile Agents.IEEE Military Communications Conference, Boston, MA, USA, 2003:688-693.

[18] M. Ketel, N. Dogan, A. Homaifar. Distributed Sensor Networks Based on Mobile Agents Paradigm. Proc. 37th Southeastern Symposium on System Theory, Tuskegee, AL, USA, 2005: 411-414.

[19] H. Qi, Y. Xu, X. Wang. Mobile-Agent-based Collaborative Signal and Information Processing in Sensor Networks. Proc. IEEE, 2003, 91(8):1172-1183

[20] B. Parno, A. Perrig, and V. Gligor, “Distributed Detection ofNode Replication Attacks in Sensor Networks,” *Proc. 2005 IEEESymp. Security and Privacy (SP’05)*, Oakland, CA, May 2005.

[21] Y. Zhang *et al.*, “Location-Based Compromise-Tolerant Security Mechanisms for Wireless Sensor Networks,” *IEEE JSAC*, special issue on Security in Wireless Ad Hoc Networks, vol. 24, no.2, Feb. 2006, pp. 247–60.

[22] Y. Hu, A. Perrig, and D. Johnson, Packet Leashes: A Defense Against Wormhole Attacks in Wireless Ad Hoc Networks, in: Proc. Of Infocom 2003. San Francisco, CA, USA, April 2003.

[23] S. Capkun, L. Buttyan, J. Hubaux, SECTOR: Secure Traking of Node Encounters in Muti-hop Wireless Networks, in: proc. Of SASN 2003. Fairfax, Virginia, October 2003.

[24]E. C. H Ngai, J. Liu and M R. Lyu, “On the intruder Detection for Sinkhole Attack in Wireless Sensor Networks,” Proc. IEEE ICC, 2006.

[25] Z. Karakehayov. Using REWARD to detect team black-hole attacks in wireless sensor networks.In *ACM Workshop on Real-World Wireless Sensor Networks*, 2005.