Fault Tolerant Mobile Object Tracking with Sink Hole Detection in Wireless Sensor Network

Madhuri Rao[1], Satya Sovana Patnaik[2], K.Vinod Kumar[3]

[1]*Department of Computer Science & Information Technology*
[2,3]*Department of Computer Science and Engineering, Siksha 'O' Anusandhan University, Jagamara, Khandagiri , Bhubaneswar, Odisha , India 751030*

Abstract: **It is necessary to verify the fault tolerance capabilities of Wireless Sensor Network (WSN) in the object tracking environment before deployment. In the distributed environment, densely collected tiny sensor nodes are equipped with a variety of sensors. These sensors are able to sense events, compute and communicate with end users. They are sometimes required to track moving objects. Such a tracking task has many constraints. Battery power of nodes, link failure, eavesdropping and sinkhole attacks are some of the challenges that the network has to overcome. Tracking a moving object requires regular updating of sensor nodes and therefore may be very power consuming. Finding the shortest paths between the moving object and the sink may be saving energy but may not be reliable. We propose a energy computing model that is designed to detect the moving objects optimally and can also detect a node which may cause a sinkhole attack in the network. The work proposed here addresses the aspects related to energy efficient object tracking and builds a fault tolerant network with sink hole detection.**

Keywords: Wireless Sensor Network, Sink Hole Attack, Fault Tolerant, Object Tracking, Mobile Agent

I. INTRODUCTION

Wireless sensor network is a prominent technology that enables distant surveillance objects and environment. Wireless sensor network (WSN) comprises of a large number of sensor nodes that are placed either inside the phenomenon or very close to it. They presume to serve as a key infrastructure for a wide range of applications which include agriculture, surveillance, intelligent highway systems, emergent disaster response and recovery. The most important application issue for sensor networks is effectively used to track mobile object. Hence, in such an environment, the sensor networks are paced for military (tracking enemy vehicles, detecting illegal border crossings) designs and civilian designs (tracking the movement of wild animals in wildlife protection). To trail an object precisely, two or more of sensors are required concurrently. The collaboration is a significant issue for tracking an object. But the actuated sensors require utilizing power because of communication, sensing, or other factors. Thus, the lowest essential number of sensors is allocated for the job and at the same time other sensors stay in the resting state. While tracking, a large number of sensors take part in the coordination. Such a object tracking sensor network furnish important research option in terms of energy & power management. For satisfying the requirements of saving power as well as improving overall efficiency at the same time, high coordination and other management operations are required. Previously, in object tracking sensor networks, the sensors are assumed to be active. So it causes the sensors to absorb a lot of energy, since a large of sensors assist to determine the location of the moving object as well as transmit the control data simultaneously. Commonly, the object tracking protocols are divided into 2 types i.e , cluster-based and non-cluster-based protocols. When a sensor node detects an object, then it sends forth the information to its cluster head. Then, the cluster head carries all the information and proliferates the information to a sink. This proposal decreases the necessary communication bandwidth and energy is conserved. Therefore, WSNs can lengthen lifespan. In non-cluster-based protocols, the cluster head is not served by any node WSNs. When an object is detected, the sensor node records its information in its local memory. When an user publishes a petition to WSNs when he/ she wants to know the location of tracked object. If the information of the tracked object is with a sensor node, then it responds the information to the user, otherwise it starts to track the object.

II. LITERATURE REVIEW

In [3], it is justified that a source can quickly approach the target in a shortened path. They compare their proposed schemes with 3 flooding based query methods and prove that they achieve better performances. In [23], shortened face track method is proposed which decreases the moving distance of source and hence improves efficiency for chasing. The source can follow short path to chase the target. This method can also avoid track loop problem. In the Fig.1, how the shortest path is selected is shown and Fig 2, depicts efficient object tracking with mobile agents in wireless sensor network. Tracking a mobile object is a complex task. It not only requires nodes to sense and communicate but also requires collaboration in terms of prediction and energy saving.

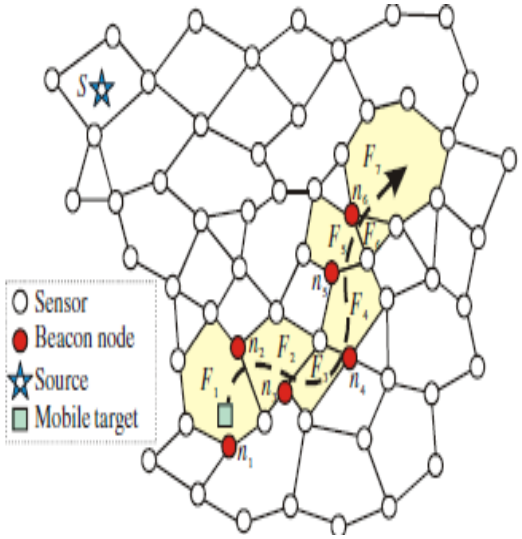


Fig.1 Object tracking in WSN using mobile agent.
Source:

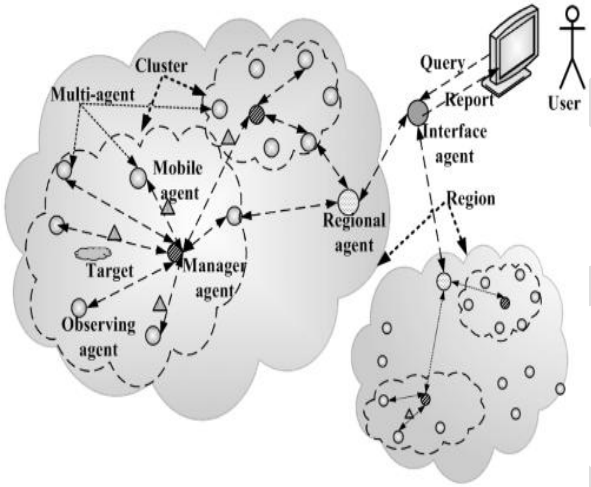


Fig 2 .Mobile agents in a wireless network

In order to optimize the energy usage in sensor nodes, Middleware concept is introduced. The Middleware to provide security for the Wireless Sensor Networks is arranged in the Mobile agent with the capability of optimizing the power usage with the sensor nodes. An energy efficient Mobile agent based algorithm is simulated. It will be established that the Mobile agents provide the security arrangements to the Wireless sensor networks for the reduction of sinkhole and cloning attacks. The tracking phenomenon is vulnerable to sinkhole attack. An attacker in such a case requires a very little effort. Such an attack is usually undetectable. It requires specific detection rules that must be incorporated in the routing protocols itself. In [2], the author propose a better design of routing protocol that is resilient to sinkhole attack and also suggest formal rules in intrusion detection in wireless sensor network.

III. Motivation

WSNs are vulnerable network as they are wireless networks. Like any network, it is also exposed to problems of eaves dropping, error connections. Nodes could be easily possessed by a hacker, who could then, change information, re-route information and ever cause network congestion. All this mishaps could seriously drain the power of the nodes and cause the network to die and it would then be aas good a network not existing in the few places. Hence security in the wireless sensor network is a must. As the nodes are usually put up in the hostile environment, physical interruption may be quite less. It is therefore important to ensure that the wireless medium and wireless communications is secured. Cryptography and key management techniques have been suggested by [3]. However it cannot protect against insider attack and laptop class attacks. An insider attack reduces the effectiveness of the link layer security mechanisms and this is open resource area to be more extensively explored. Wireless sensor networks are small, sometimes as small as dust, large in number with routing techniques that are deployed in physical layer or logical link layer mostly. The advances in wireless sensor networks architecture and communications have been possible with the help of advances in MEMS design. Moreover this has left Wireless sensor network vulnerable to various intrusions, as intrusion has never been considered as a design objective. Energy has always been the most important factor. Besides energy, communication techniques have always been given importance. However reliability of nodes is always compromised. It is found that most of the time, intrusion such as sinkhole attack causes depletion of energy in the sensor nodes. Hence the motivation is to build a fault tolerant mobile system that detects sink hole and also conserves energy.

IV. Security Goals

The security aspects of wireless sensor network are as follows:

a. Confidentiality: Data transmitted between the nodes is to be kept safe from eavesdropping. Symmetric key management techniques could help in this case.
b. Integrity: Data while at transit should ensure that it reaches the desired user without being altered by an antagonist.
c. Authentication: It is essential to ensure the identity of the neighboring nodes with which a node has to communicate.
d. Availability: Sensor nodes have limited memory and limited processing abilities, data that is resent should be made available at all time. It must ensure that no old messages are communicated.
e. Non-repudiation: Nodes have to take a responsibility of sending a message in later and must not repudiate a message that it may have sent previously.
f. Authorization: Only authorized nodes should access resources and participate in network services.

Existing traditional cryptographic techniques cannot achieve the above security aspects of Wireless sensor

network. New cryptographic measures are therefore need of the hour.

V. PROPOSED MODEL & ALGORITHM

We propose a model that makes the wireless sensor network more passive to sink home attacks that which is a serious security threat for wireless sensor network applications.

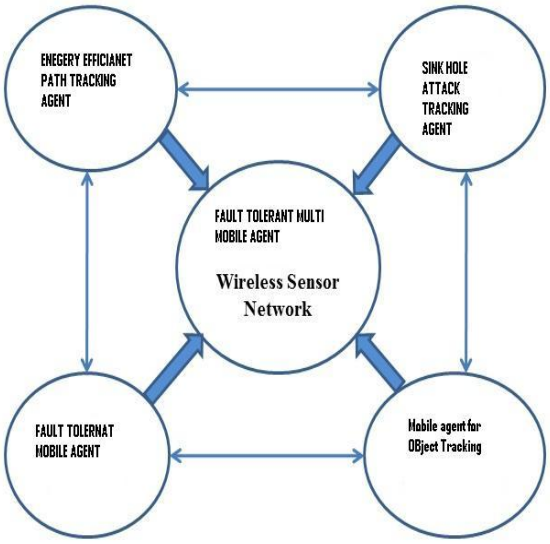


Fig 3: Proposed model

The algorithm proposed uses the approach of Mobile agent paradigm for detecting a possible sink hole attack and thereby taking measures. In this way the model is made fault tolerant .The algorithm find the shortest distance for communication in clusters while tracking objects and thus reduce energy consumption of nodes. The proposed model thus has following objectives, namely to build an fault tolerant energy efficient Path Tracking algorithm using Mobile agents. This makes the model more reliable than as in traditional approach.

The algorithm consists of 2 parts :

(1) The efficient nodes selection and source – destination the shortest distance calculation.
(2) Then the energy calculation of the selected nodes from the first part.

The pseudo code of the proposed algorithm as follows:

BEGIN
1. Specify the number of nodes(n), X & Y coordinates of the sensor nodes.
2. Specify the coordinates of the source node SX & SY.
3. Give the initial energy of ‘n’ number of nodes ‘E(k)’.
4. Transmission Energy ‘E_elect’ of the nodes is set to 0.5 joules arbitrarily.

5.1 DISTANCE CALCULATION:

INITIALIZE i=1 to n
1. Calculate the distance D(M) from source S(x,y) to the three nodes of the first cluster.

   Z=(Y(i)-SY)* (Y(i)-SY)+(X(i)-SX)*(X(i)-S(X).
   D(M)=sqrt(Z).
2. Display D(M).
3. Min1=D(i)
4. If D(i)<=Min 1
5. Display i “the selected mode”

Energy Calculation & Sinkhole detection:
6. Etx1=E_elect*B + Pamp*B*Min1*Min1
7. RE(1)=E(node1)-Etx1
8. Display RE(1)
9 . Max E= E(1)
10.If E(i)>=Max E
11. Display Sinkhole is ‘ i ‘

Again Distance Calculation from selected node to the second cluster:
INITIALIZE j=4 to 6
12. Calculate the distance from the selected node to the nodes in the second cluster.
Z=(Y(j)-Y(node1))*(Y(j)-Y(node1))+ (X(j)-X(node1))*(X(j)-X(node1))
13. D(M)=sqrt(Z)
14. Min 2=D(j)
15. if Min 2 <=D(j)
16. Display ’ j’ as selected node

ENERGY IN SECOND CLUSTER:
17. Etx2=E_elect*B + Pamp*B*Min2*Min2
18. RE(2)=E(node)-Etx2
19. Display RE(2)
20.Repeat steps 12 to 16 for distance third neighborhood.
21. Repeat steps 17 to 20 for energy third neighborhood.
END.
Distance in the third neighborhood cluster is calculated in the above algorithm methods.
Energy of the selected node in the third neighborhood is calculated and the sink hole is detected.

The proposed model implements tracking of a object in a wireless sensor network. It comprises of 9 nodes which are deployed in 3 clusters. The Fig 4 shows the topology of the nodes in the cluster which taken on account.

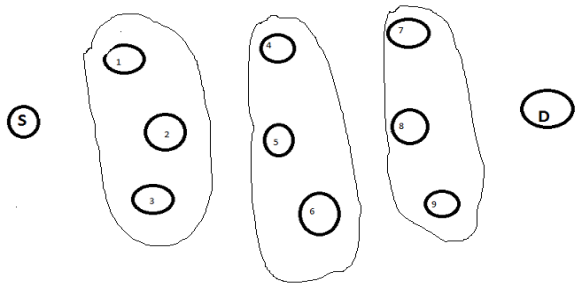


Fig 4: Three-cluster topology with 9 sensor nodes.

The protocol runs a distance vector D(m).This vector calculates the distance between source and the nodes present in the cluster 1. Then the three distances are compared and the shortest distance node is chosen. Thus, the chosen node is selected among the three nodes present in the first cluster is having the shortest distance from the source. Now, in the second round the distance vector D(m) calculates the distance of the previous chosen node to the nodes of cluster 2. Again the three distances are calculated and the shortest distance node is chosen which is shown in the Fig.5

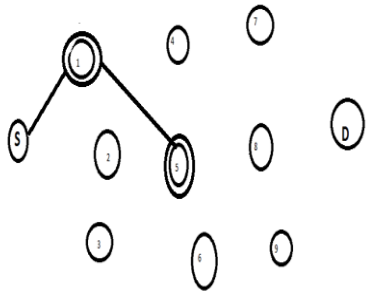


Fig 5: The sensor node selected in the second cluster.

In the third round, the distance vector D(m) gain calculates the distance from the previous chosen node to the nodes of cluster 3 which is shown in the Fig. 6. Again the three distances are calculated and the shortest distance node is selected. Hence the lastly selected node will send the information the destination.

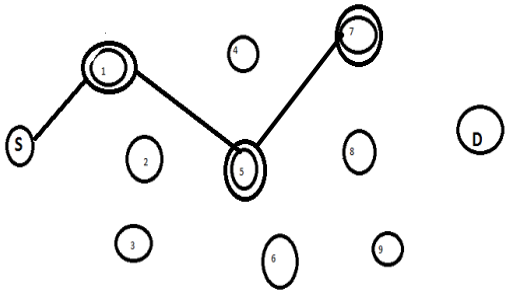


Fig.6: .Node selection in the third cluster.

Thus a path is created from the source to the destination which is depicted in the Fig 7. The approach is to create a shortened path from the source to destination. Hence the distance based approach is an energy conserving object tracking approach.

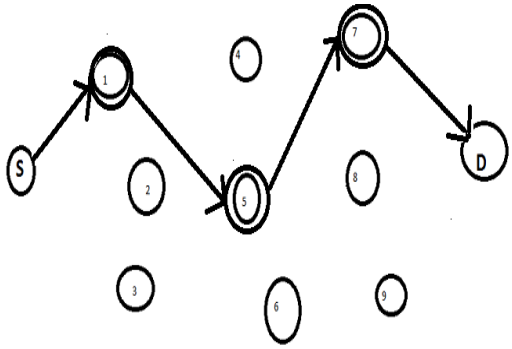


Fig.7.Path created from source to destination.

5.2. ENERGY CALCULATION:

Then the energy of the nodes is calculated. In this approach, energy is calculated by the formula and is compared between the three nodes in the first cluster. Then, the node having the highest energy is considered to be the sink hole in the first cluster. Then again the energies of second and third cluster nodes are calculated. The three selected nodes are again compared and then the highest energy node is found out.The highest energy node is considered to be the sink hole. The residual energy of the nodes is also calculated

VI. SIMULATION AND RESULTS

The proposed model is simulated in MATLAB R2013a. The algorithm is implemented using a distance vector and energy vector. Total numbers of 9 nodes are set up in a homogenous network of 500m X 500m field. The X & Y coordinate of each node is taken as input. Then the source node is placed at (4, 19).

The initial energy of the nodes are taken randomly. Power the amplifier 'Pamp' is set to 1.0 to transmit 1 bit of data. The data rate of a node is taken as 4 bit/sec.

At first the distance calculation is done taking the Euclidean distance formula. Then, the distance to each node in the clusters are compared. The least distance is calculated.

The formula for distance calculation is given by:

$$Z=(Y(i)-SY)* (Y(i)-SY)+(X(i)-SX)*(X(i)-S(X)) \quad \text{(i)}$$

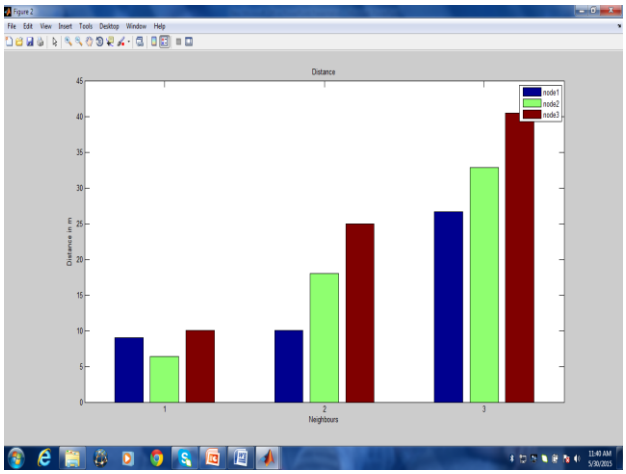
$$D(M)=\text{Sqrt}(Z) \quad \text{(ii)}$$

The equations (i) and (ii) calculates the distance vector D(m) . The equations calculate the shortest distance between the source and the first cluster.

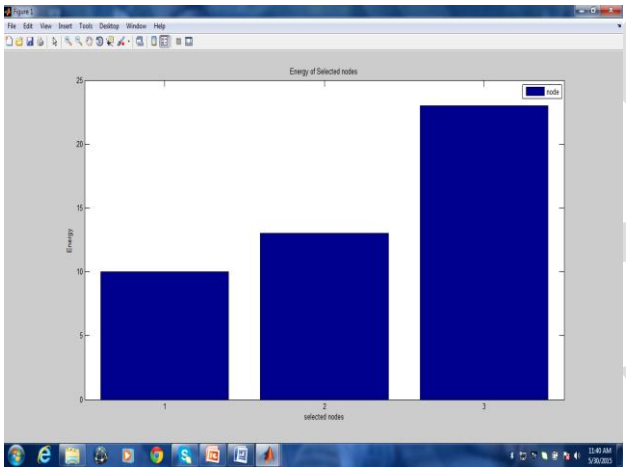
$$Z=(Y(j)-Y(node1))*(Y(j)-Y(node1))+(X(j)-X(node1))*(X(j)-X(node1)) \quad \text{(iii)}$$

In equation (iii), the distance is calculated between the first selected nodes to the nodes in the second cluster. Then the least distance node is taken on account and is selected. The least distances is taken on account to find the shortened route from source to destination. Hence the shortest path is discovered saving energy. Then the energy of the nodes three clusters are compared and node with high energy from each cluster is selected. Then the nodes with higher energy are detected to be the sink holes. The X and Y co-ordinates of the nodes are given as input. Then the X and Y coordinate of the Source Node is given as input. The Energy of the nodes are also given as input.Then the distance is calculated and then compared. Thus, the shortest path is discovered from source to destination i.e, (2-4-7) .The energy of the nodes are compared and the possibility of sinkhole node is determined i.e nodes (3-6-7). The graph 1, below shows the comparison of least distance

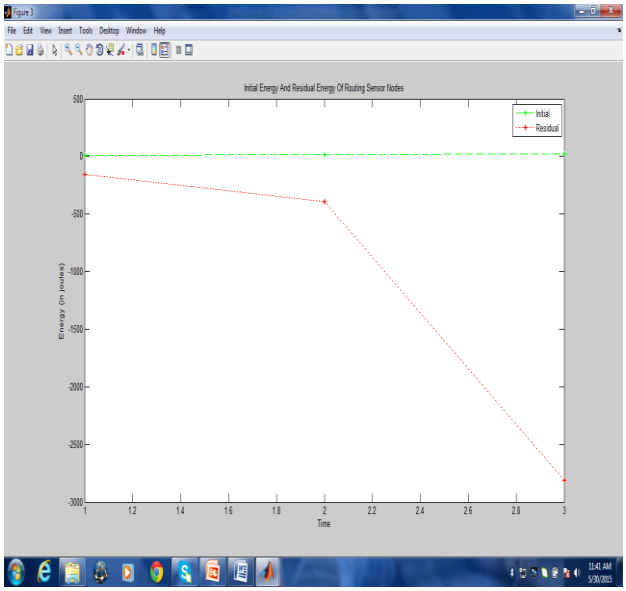
nodes found. Graph 2, depicts the highest energy selected nodes are shown.



Graph 1: Comparison of least distances



Graph 2: Comparison of highest energy nodes is shown.



Graph 3: energy dissipation of the elected nodes.

VII. CONCLUSION

The work proposed here is to find a shortest path for tracking objects in wireless sensor networks, in addition to it, the energy of the nodes are calculated. On the basis of the energy, the proposed model also detects the probable nodes that may cause a sinkhole attack. A mobile agent here discovers a shortened path to reach the destination. By detecting and avoiding a Sink hole attack scenario the proposed algorithm makes the system more reliable and more fault tolerant. By choosing paths with nodes with optimal energy , the system ensures that less fault occurs in communication. A motivation for a better architecture of routing protocols in wireless sensor network that can make them more passive to attacks is yet needed. There are many general as well as formal rules in intrusion detection systems, but customizing it for wireless sensor networks with their inherent constraints is the need of the hour.

REFERENCES

[1]. Hua-Wen Tsai, Chih-Ping Chu, Tzung-Shi Chen, "Mobile object tracking in wireless sensor networks", *Computer Communication*, vol. 30, pp. 1811-1825, 2007.

[2]. Ioannis Krontiris, Thanassis Giannetsos, Tassos Dimitriou, "Launching a Sinkhole Attack in Wireless Sensor Networks; the Intruder Side", Athens Information Technology, 19002 Peania, Athens, Greece.

[3]. Stefan Pleisch, Andre Schiper, "Fault-Tolerant Mobile Agent Execution", *IEEE Transactions on Computers*, vol. 52, no. 2, pp. 209-222, 2003.

[4]. A. Vijayalakshmi, T. Shrimathy, T.G. Palanivelu, "Mobile Agent Middleware Security for Wireless Sensor Networks", *International Conference on Communication and Signal Processing*, pp. 1669-1673, 2014.

[5]. Sania Bhatti, Jie Xu, Mohsin Memon, "Model checking of a Target Tracking Protocol for Wireless Sensor Networks", *2010 10th IEEE International Conference on Computer* Information Technology, pp.16-21, 2010 .

[6]. Mohini Gawande, Veena Gulhane, "Cluster-based Target Tracking and Recovery Algorithm in Wireless Sensor Network" IJASCSE, vol. 1, issue. 4,2012.

[7]. Stefan Pleisch, Andre Schiper, "Fault Tolerant Mobile Agent Execution"IEEE TRANSACTIONS ON COMPUTERS, vol. 52, no. 2, Feb 2003.