International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

Initial Fault Detection by Using RAEED Protocol in Face Tracking Technique

Anuradha M. Joshi[1], Jagruti J. Shah[2]

[1, 2]G.H.Raisoni College of Engineering, Nagpur, Digdoh Hill Hingana Road Nagpur 16, India

Abstract: ***One of the type of wireless sensor network is object tracking sensor network, which is used to track the object moving in the dedicated area. It reports the latest location of the object to base station. There is new framework for object tracking, which is also called as face track. In face tracking technique the nodes are deployed in spatial region surrounding a target, which is known as face. This framework estimate the target's moving toward another face instead of predicting the target location separately. A new framework for secure objet tracking is introduced, In which it detects the faulty node and malicious node initially, to prevent from attack and loss of tracking. It also increase the energy efficiency by preventing from reconstruction of polygon, during the tracking of object.***

Keywords: OTSN, tracking the target , selection of sensor , edge detection, face tracking, fault tolerance, attack on sensor node, RAEED.

1. Introduction

One of the type of wireless sensor network is object tracking sensor network, which is used to track the object moving in the dedicated area. It reports the latest location of the object to base station. It is used for many real time applications for monitoring the dedicated area for e.g. . Wild life monitoring, security applications for buildings and monitoring for illegal border crossings etc. There is new framework for object tracking, which is also called as face track. In face tracking technique the nodes are deployed in spatial region surrounding a target, which is known as face. This framework estimate the target's moving toward another face instead of predicting the target location separately. In face tracking framework edge detection algorithm is used to generate each face further in a way so that the nodes can prepare ahead of the target's moving path. Due to which the tracking of target is done on time. So that the recovery from special is done before, e.g., sensor fault. Optimal node selection is another algorithm which is used in this framework, which is used to choose the sensor nodes in the face. So that only the selected nodes will become active for query and for forwarding the tracked data [1]

A protocol called RAEED (Robust Formally Analyzed protocol for Wireless Sensor Network Deploymeny) is used in this paper. This protocol is used to detect the faulty or malicious node initially during the polygon formation to prevent it from DOS (Denial of Service) attack and loss of tracking [2]

This protocol uses the approach of observing the performance of their neighbor, in which every nodes watch the performance of their neighbor [2]. Using this approach every node detects whether their adjacent node forwarding the vigilance message or data to their 1-hop node or not. Based on their performance; the neighbor nodes are ranked. The nodes will report their predecessor if it is not able to forward data further, and also report if it is not able to participate in tracking due to low power of battery. The node will consider as the faulty or malicious node if it will not report their predecessor and it is discarded from network by notification broadcasting to all nodes in network by using DDB (Dymanic Broadcast Protocol).

Another node get selected for forming the polygon or face further to track the object of object tracking sensor network by sending the vigilance message to their neighbor nodes after discarding it from the network.

2. Related Work

A. Face Tracking [1]

In face tracking technique the nodes are deployed in spatial region surrounding a target, which is known as face. This framework estimate the target's moving toward another face instead of predicting the target location separately. In face tracking framework edge detection algorithm is used to generate each face further in a way so that the nodes can prepare ahead of the target's moving path. Due to which the tracking of target is done on time. So that the recovery from special is done before, e.g., sensor faults. Optimal node selection is another algorithm which is used in this framework, which is used to choose the sensor nodes in the face. So that only the selected nodes will become active for query and for forwarding the tracked data [1]

B. RAEED Protocol [2]

To detect the Black Hole attack RAEED (Robust Formally Analyzed protocol for WSN Deployment) is used. Neighbor watching approach is used in this protocol in which each nodes observes the performance of their adjacent node, it checks whether it forwarding the data to their 2-hop legitimate node or not.
Depending on the performance of their adjacent node they are ranked, if it is not doing well, the that nodes are ignored. If any node in network are not able to forward the data due to some reason, they will report their predecessor about by sending the message.

It is having an advantage that, the virtual links get removed by communicating to their 2-hop nodes. Due to which black hole attack by any virtual link is not possible.

C. Tracking with Unreliable Node Sequences [3]

An ordered list is extracted from the unreliable node sequences for which a tracking technique is used which is robust. In this technique original problem of tracking is converted to finding the shortest in the graph, rather than separately predicting the each position in movement of track. It develop multidimensional smoothing techinique in adition to above scheme, to increase the tracking accuracy.

Certain forms of physical signals which is emitted from target is detected when any target mobile node enters in the surveillance area . Sensing result of every node in the network is different due to vary in geographic distance between target and sensor node. Ex. different strength of signal and arrival of time. Sensor nodes natural ordering is given which is also called as detection sequence or detection node sequence.

It is having a drawback as follows i.e. the searching path of shortest graph is too big, when the target stays in the surveillance area for more time. Another drawback is tracking multiple target at a time is not possible with this technique. It is robust to various noise model and the only constraint is, it impose more speed , is one of the advantage of this technique.

D. Localization of Event Based Intensity [4]

The fully distributed localization technique, which consist of two algorithm: 1] DENA (Distributed Election Winner notification algorithm), 2] ILA (Intensity based Localization algorithm). The first algorithm determines the node closest to an event, and sends the notification to all other nodes about the winner node. It provides the signal independent position estimation. Another protocol the use is DDB (Dynamic Broadcast Protocol), which is used for dynamically te localization is impossible.3] Performing and maintaining the operation in timely fashion is difficult i.e. turning the switches on and off most of the time.

E. INSENS [5]

In this paper for wireless Sensor Networks an Intrusion-tolerant routing protocol (INSENS) is described. At each node it constructs the table to provide communication between base station and the sensor node

3. Methodology

Face tracking technique is a technique which is used to track the target in the monitoring area. The nodes on the border of the monitoring area are always in the wake up state, and the remaining nodes are in the sleep state. Hence detecting the target in the monitoring area, the border nodes send the vigilance message to their adjacent nodes which are on the expected path of the target where it is moving towards.

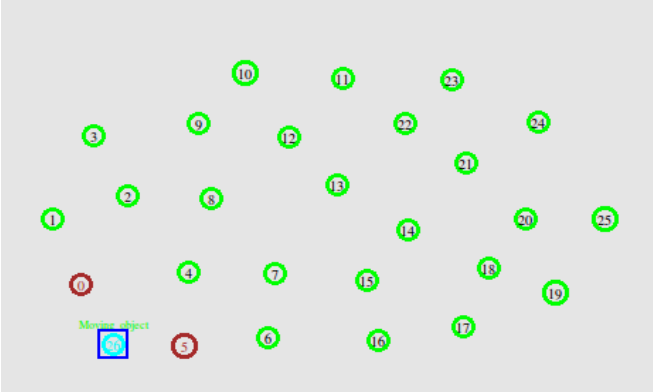

Figure 1: Target Discovery

As shown in figure 1. the target is detected by the border nodes in the surveillance area.

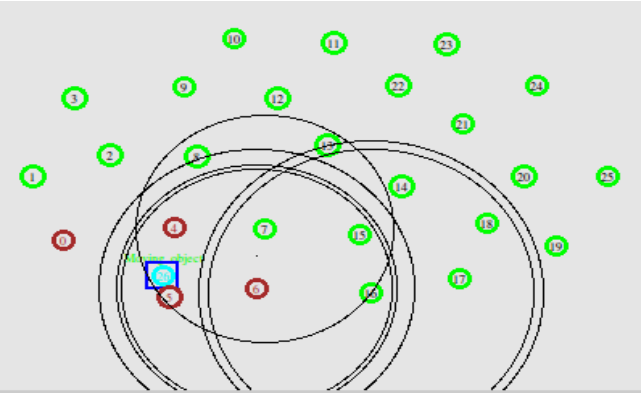

Figure 2: Polygon Formation

In figure 2 the couple nodes 0 and 5 sends the vigilance message to their adjacent nodes about the target discovery, so has to wake them up to track the target. The nodes which are on the targets moving path will remain active and form the polygon, to track the target. The nodes which participate on the polygon formation, on that nodes will remain active and participate in tracking. Other nodes in the network will remain in sleep state.

While sending the vigilance message to the adjacent nodes, it will detect the following conditions using the RAEED protocol [2].

1) First condition is it will check whether the node is sending the vigilance message to their adjacent node or not. If it will not send the vigilance message to their adjacent node then that node will consider as the faulty node or malicious node
2) Another condition is it will check whether the battery power is in the threshold value or not. If the power of node is below threshold value then it will not participate in the tracking

This conditions are necessary to increase the energy efficiency. In the face tracking technique if any fault will occur during the target tracking then reconstruction of polygon is required [1]. Which may cause loss of tracking. Hence to overcome this drawback, the proposed system is using RAEED protocol to detect the fault initially. So has to avoid the fault occurrence during the tracking of target. Generally the fault is occur because of the low battery power or the malicious node. If any of the in the network is

malicious it will not send the wake up message to their adjacent node, due to which it will affect the polygon formation which will cause the loss of tracking. This drawback will overcome by using the above conditions. If the faulty node and malicious node is detected initially then it will prevent from reconstruction of polygon. Due to which the energy efficiency will be increase.

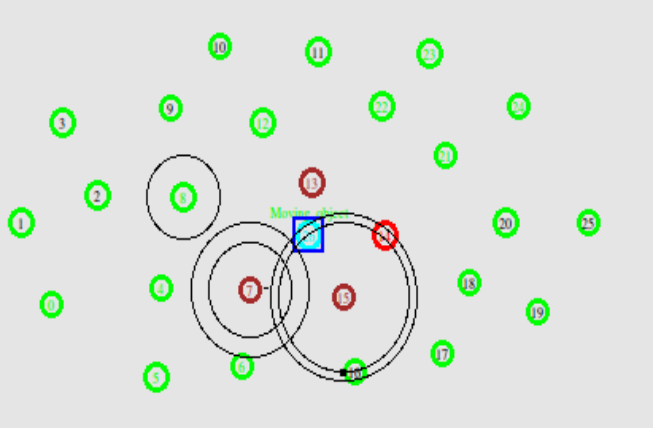

Figure 3: Fault Detection

Above figure shows the fault occurrence in the network, so that the faulty node will not participate in polygon formation and tracking.

4. FlowChart

Firstly after the discovery of target in the respected area, the edge near the target is moving get activated and send the message to their neighbor node about the target discovery. And that neighbor node will send the vigilance message to their neighbor node, as shown in figure 1 After sending the message to their neighbor it also checks whether it forwarding to their neighbor or not using RAEED protocol. And form the polygon, shown in figure 2.

When the object enters in polygon, it will track that object and other nodes remain in sleep state. When the object move toward the border of that polygon then depends on the distance and weight of polygon from every edge the brink will be detected using brink detection algorithm. Again after that the couple nodes will be selected using brink detection algorithm. And when the target nears the couple node it will send the message to their neighbor node about the target. It also checks whether it is forwarding to their neighbor or not. Because of this the Denial of Service attack gets detected and also node failure during the polygon formation. figure 3 shows the fault occurance. Due to which it minimizes the reconstruction overhead during object tracking hence energy consumption will decrease and prevent it from loss of tracking.

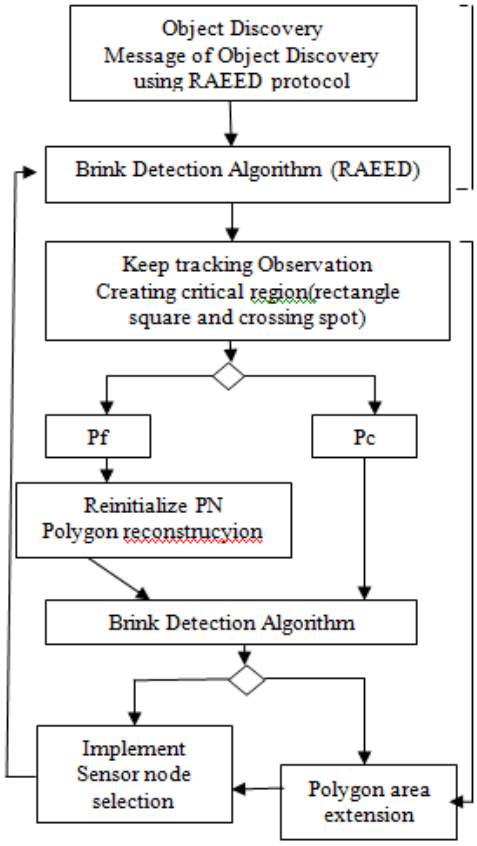

Figure 4: Flow Chart

5. Simulation Results

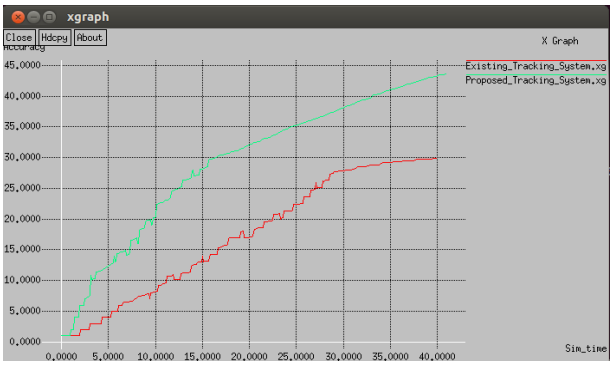

Figure 5: Accuracy Graph

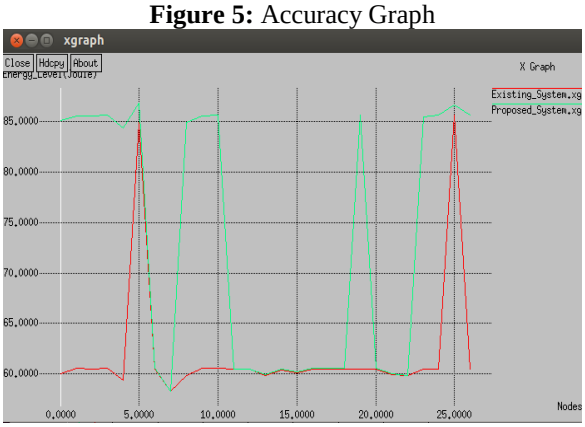

Figure 6: Energy Graph

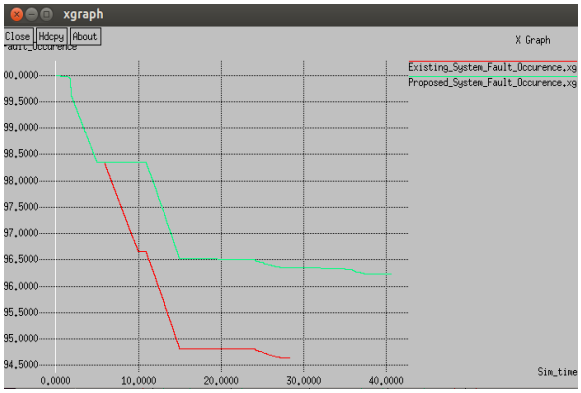

Figure 7: Fault Occurance Graph

Above graph shows the results of the proposed system. The first graph shown in figure 5 is the accuracy graph which shows the increase in accuracy compare to existing technique. The second graph shown in figure 6 is the energy graph, which shows that the energy consumption will be decrease due to this technique. And last graph shown in figure 7 is the fault occurance graph, which shows that the fault occurance during the tracking of the object will get minimized

6. Acknowledgement

I am currently pursuing M.E in Wireless Communication and Computing and the work in this paper is under process. A technique called Face tracking for tracking of object and RAEED protocol is using for fault detection during the construction of polygon is used. So that the reconstruction of polygon due to faulty node or malicious node during tracking is prevented.

7. Conclusion

A system to detect the fault and malicious node initially is proposed. In this technique a protocol called RAEED is used for fault detection and malicious node detection. To detect the fault initially, every node after sending the vigilance message will check whether their adjacent node is sending the message to their adjacent node or not. If any node is not able to send the message to their adjacent node then it will report to their predecessor. If it will not report then that node is considered as the faulty or malicious node. Another condition it checks is whether the battery power is above threshold value or not. If it is below the threshold value then it will not participate in the tracking of object. Due to this it will prevent from fault occurance, loss of tracking and reconstruction of polygon during the tracking. Due to which the energy efficiency will also increase.

References

[1] G. Wang, Md.Z.A.Bhuiyan, Jiannong,J.Wu, "Detecting Movements of a Target Using Face Tracking in WSN", IEEE Transaction on Parallel and Distributed Systems, Vol.25, No 4,April 2014

[2] K. Saghar, D. Kendall, A. Bouridane, "Application of Formal Modalling to Detect Black Hole Attack in WSN",Proceeding of 11 International Conference on Applied Sciences and Technology (IBCAST), 978-1-4799-2319-9, January 2014

[3] Z. Zhong, T. Zhu, D. Wang, and T. He, "Tracking with Unreliable Node Sequence," Proc. IEEE INFOCOM, pp. 1215-1223, 2009.

[4] M.Waelchli, M. Scheidegger and T. Braun, " Intensity-based Event Localization in Wireless Sensor Networks," IEEE transaction 2006 .

[5] J. Deng, R. Han, S. Mishra," INSENS: Intrusion-Tolerant Routing in Wireless Sensor Networks" University of Colorado, Department of Computer Science Technical Report CU-CS-939-02

[6] L. KAPLAN," Global Node Selection for Localization in a Distributed Sensor Network", IEEE TRANSACTIONS ON AEROSPACE AND ELECTRONIC SYSTEMS VOL. 42, NO. 1 JANUARY 2006

[7] L. Tobarra, D.Cazorla, F. Cuartero," Formal Analysis of Sensor Network Encryption Protocol (SNEP)", 1-4244-1455-5/07/ 2007 IEEE.

[8] Y. Hanna, H. Rajan, "Slede: Framework for Automatic Verification of Sensor Network Security Protocol Implementations", *ICSE'09*, May 16-24, 2009, Vancouver, Canada 978-1-4244-3494-7/09 2009 IEEE

Author Profile

Anuradha Joshi received the B.E degree from RTMNU and currently pursuing ME in Wireless Communication and Computing from G.H.Raisoni College of Engineering. Recently student in G. H. Raisoni College of Engineering