International Journal of Applied Engineering Research ISSN 0973-4562 Volume 10, Number 15 (2015) pp 36714-35719

Target Localization and Failure Node Recovery Mechanism in Wireless Sensor Networks

T.Samraj Lawrence
Assistant Professor,
Department of Computer Science and Engineering,
Francis Xavier Engineering College, Tirunelveli.
er.samraj@gmail.com

Dr.V.Seenivasagam
Professor,
Department of Computer Science and Engineering,
National Engineering College, Kovilpatti,Tuticorin.
yespee1094@yahoo.com

Dr.D.C.Joy Winnie Wise
Professor & Head
Department of Computer Science and Engineering,
Francis Xavier Engineering College, Tirunelveli.
joywinniewise@yahoo.com

Abstract- Now a days, low range of communications and low bandwidth usage of sensor networks are unavoidable. The life time and energy harvesting of the sensor nodes is one more main constraints for the developers to make the efficient communication between the nodes. In this aspect, the failure of nodes in the networks always imposed the problem in packet delivery. Hence, to find the suitable target locations to relocate failure nodes to repair holes and dispatching mobile nodes to the target locations while minimizing the power and improving the packet delivery ratio. This paper investigates the node failure detection and reestablishment of network connectivity after node failure without extending the length of data paths. The proposed algorithm of Fault Tolerant Localization and Tracking of Multiple Sources (FTLT) is used to detect the node failure. The recovery scheme is provided by using manager node movement concept and the Destination Sequenced Distance Vector (DSDV) protocol is used for finding the shortest path to improve the life time of the nodes.

Keywords: Recovery mechanism; Fault Tolerant Localization and Tracking of Multiple Sources; Destination Sequenced Distance Vector.

Introduction

A Wireless Sensor Network (WSN) consists of sensor nodes capable of collecting information from the environment and communicating with each other via wireless transceivers. In real world applications of WSNs, sensors often fail and report erroneous observations for various reasons, thus compromising the trust of people towards WSNs technologies [1]. The recent Fault Tolerant Localization and Tracking algorithm (FTLT) used in multiple moving sources for detecting, identifying and tracking which is a low complexity, distributed method suitable for real-time applications in WSNs using binary data. But it can verified by random sensor faults [2]. In the Localization phase, each leader runs dSNAP (distributed Subtract on Negative observation and Add on Positive) to determine the location of the source by only contacting the sensor nodes and approximate the path of the source [3].

Related Work

In the classic coverage model the entire area must be monitor to detect fault targets. From this concept large number of sensor nodes is used. The system not provides recovery schemes [4]. However, since every node in a multihop (or ad hoc) network is responsible for forwarding packets to other nodes, the failure of a critical node can result in a network partition. Hence it is ideal to have an ad hoc network configuration that can tolerate temporary failures while allowing recovery [5]. The biconnectivity algorithms which run in polynomial time transform a connected but non-biconnected network configuration to a biconnected one by hinting certain nodes to move to new positions [6]. The iterative block movement algorithm significantly outperforms the contraction heuristic in the total distance travelled metric but due to the seemingly combinatorial nature of the problem space, finding a exact polynomial time algorithm for the 2D case is extremely hard, if possible at all [7].

The anchor-free locally-centralized localization protocol can determine the position of sensor nodes consistently with low error margins. A major motivation for approach is that believe locally centralized algorithms scale well with increased network size and are robust to network partitioning and node failure. Yet, it can achieve acceptable accuracy compared to a centralized approach [8]. COLA, a COverage and Latency aware Actor placement scheme for WSANs. COLA considers the actor coverage and data gathering latency, when determining the location of the actor nodes. While COLA can improve the coverage in addition to reducing the end-to-end delay, it may make some of the actors inaccessible to others due to their newly designated positions. However, COCOLA restricts the actor's movement to the designated location by considering the transmission range of the neighboring actor nodes [9].

Compared with traditional WSN fault detection mechanism, add gateway devices, which can locate and analyze failures. This greatly improves the efficiency of network maintenance and fault repairs. But the topology is not clearly mentioned here [10]. In geographic-based rendezvous mechanisms, geographical locations are used as a rendezvous place for providers and seekers of information. There has been a large amount of non-geographic ad hoc routing protocols proposed in the literature that are either proactive (maintain routes continuously), reactive (create routes on demand). But it does not contain the details of how a real implementation affects the protocol performance [11]. A method using a 2D scan called Scan-based Movement-Assisted sensoR deploymenT method (SMART). Here only consider the integer addition and Boolean AND operations for scan. By using integer addition, the scan operation will return the partial and total sums of the number of sensors. The results show that the proposed method can achieve an even deployment of sensors with modest costs but they have to perform an in-depth simulation on energy consumption of sensor deployment algorithms and design some intra cluster balancing algorithms to achieve high-resolution load balancing [12].

In the recent work DARA, a Distributed Actor Recovery Algorithm, to localize the scope of the recovery process and minimize the movement overhead imposed on the involved actors, although they did not explicitly prove and verify the performances of their algorithms in terms of these metric and significant discrepancies that affect the correctness of the algorithms [13]. The algorithm is completely distributed and requires only the knowledge of have to consider other metrics such as coverage and sensor-to-actor delay in determining the scope of the recovery and in selecting candidates for movement. The proposed algorithm, FTLT (Fault Tolerant Localization and Tracking), mainly used for the identification of faults and target localization in wireless sensor networks.

Proposed System

The main contribution of this paper is the development and analysis of a low- complexity, distributed, real-time algorithm that uses the binary observations of the sensors for identifying, localizing, and tracking multiple targets in a fault tolerant way. This paper solved an important problem by reestablishing network connectivity after node failure without extending the length of data paths. A large percentage of sensor nodes (25 percent) report erroneous observations. Wireless Sensor Networks (WSNs) have been proposed for monitoring large areas against the presence of event sources. The events can be intruders, enemy vehicles, pollutant sources or fires depending on the application.

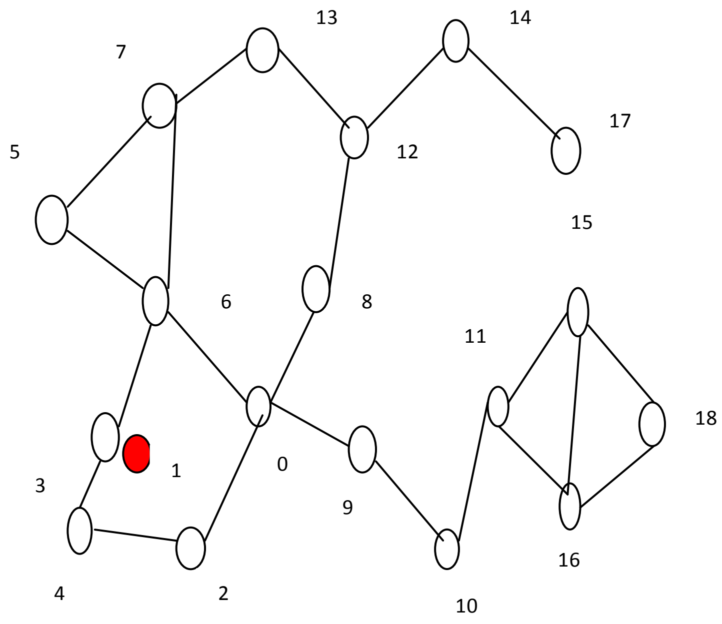


Figure 1. Wireless sensor network with faulty node

Recovery Process

The faulty node is shown in Figure.1. If node 3 and 0 is neighbor of failure node 1, that belongs to smallest block. Node 3 is gateway of remaining nodes in the smallest block and assumed node 3 as 'parent' node. Why we choose smallest block movement means, it has the fewest nodes among all blocks and easy to move during the recovery. When the node 3 moves to replace the faulty node, there is possibility to its children nodes will moves towards its parent's node. The node placement is focused on placement of manager nodes while recovering a failure node in WSNs. Manager node replacement is another approach for restore the network connectivity when failure occurred. The deployment of node is to restore connectivity among the disjoint partitions of a damaged WSN. Introduce manager nodes within the network to provide connectivity so that transmission power of each sensor node can be kept low.

Block Diagram

Each and every node always monitors the status of neighbor node, if any node failed in that range is shown in Figure.2. It is indicating and generating the error message to all other sensors. It means in this module we have to find smallest disjoint block. If it is small then it will reduce the recovery overhead in the network. We also consider about that neighbor nodes of that sensor. If that sensor has lot of neighbor nodes it will affect the energy level of that particular sensor. For replacing the faulty node, in that network all the sensors indicating which sensor is near to failure sensor. That is the best candidate to rectify the problem.

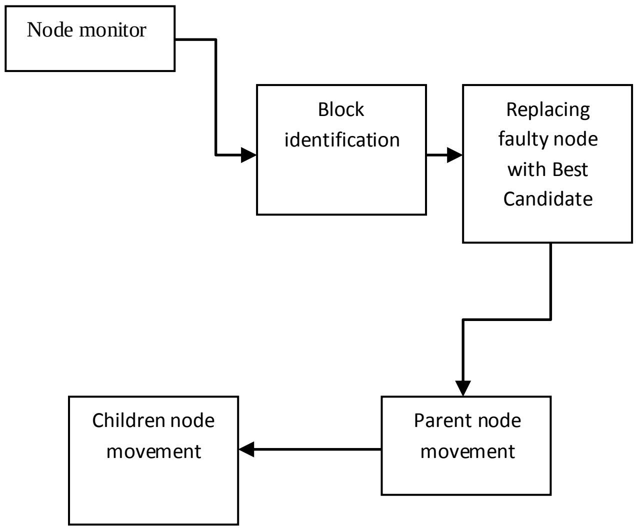


Figure 2. Block Diagram of the proposed design

Parent node moves near to the failure node in Figure 3,. In this block the children node, it means which sensor is near to the failure sensor that sensor moves to that location and replacing the need of that sensor and again formatting the topology. Actors will periodically send heartbeat messages to their neighbors to ensure that they are functional, and also report changes to the one-hop neighbors. Missing heartbeat messages can be used to detect the failure of actors. After that it's just check whether failed node is critical node or not. Critical node means if that node failed it form disjoint block in the network. In this step we have to find smallest disjoint block. If it is small then it will reduce the recovery overhead in the network. The smallest block is the one with the least number of nodes. By finding the reachable set of nodes for every direct neighbor of the failed node and then picking the set with the fewest nodes.

If node J is the neighbor of the failed node that belongs to the smallest block, is consider the BC to replace node. Since node J is considered the gateway node of the block to the failed critical node (and the rest of the network). We refer to it as "parent" node. A node is a "child" if it is two hops away from the failed node, "grandchild" if three hops away from the failed node. In case more than one actor fits the characteristics of a BC (Best Candidate), the closest actor to the faulty node. When node J moves to replace the faulty node, possibly some of its children will lose direct links to it. We do not want this to happen since some data paths may be extended. This algorithm doesn't want to extend the link. if a child receives a message that the parent P is moving, the child then notifies its neighbors (grandchildren of node P) and travels directly toward the new location of P until it reconnects with its parent again. The use case diagram is a graphic depiction of the interaction among the elements of a system. Here planning the overall requirement of the system such as number of nodes involved in the recovery scheme, fault detection and best node selection.

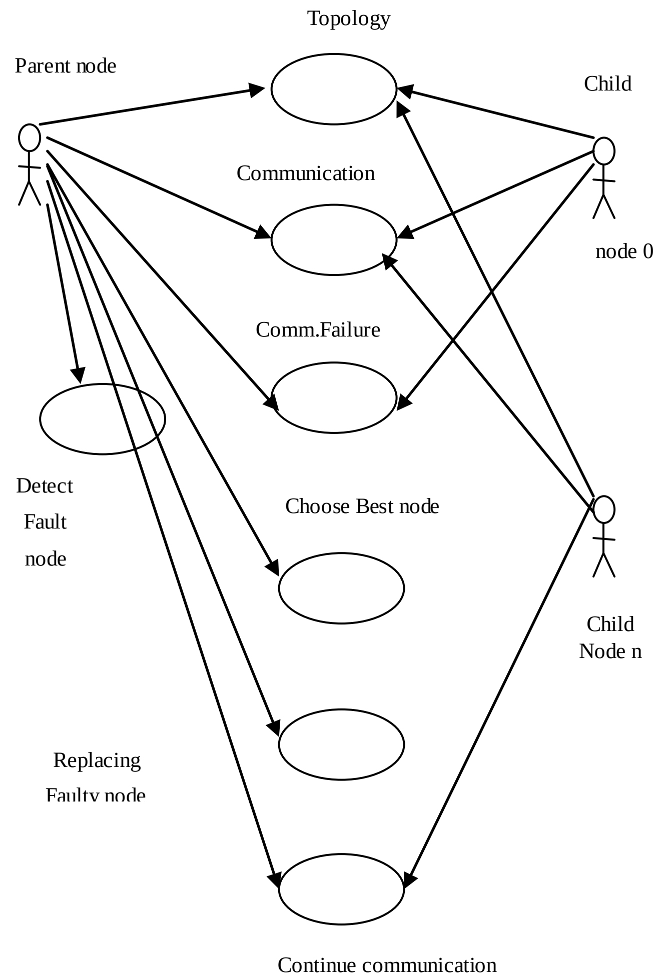


Figure 3. Use Case Diagram

Simulation

The followings steps are followed for the Recovery Mechanism. The most widely used simulator for networking research is the network simulator. NS is a discrete event simulator where the advance of time depends on the timing of events which are maintained by a scheduler.

Step1: Sensor Network

Fault tolerant localization is the process of finding the faulty node in the network is shown in Figure 4. The group of nodes forms the network. In the above scenario nodes are form a network. In that all the nodes are that forms the green color which indicates the active state of the nodes. In this the 0th node is the sender and the 20th node is the receiver. The 15th node is for the replacement the faulty node In the above the circle forms the route discovery process.

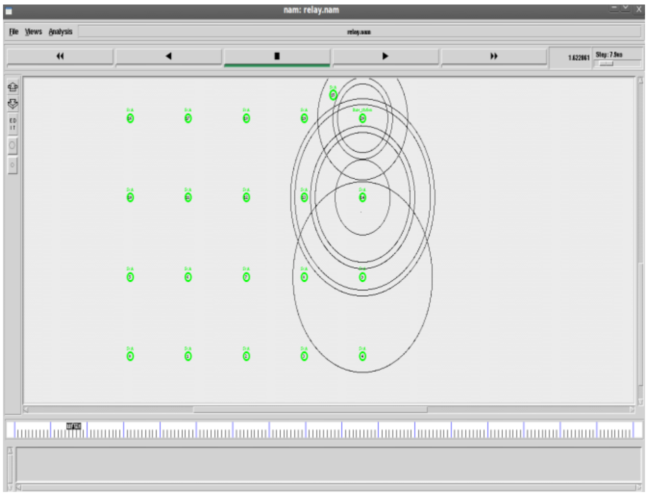
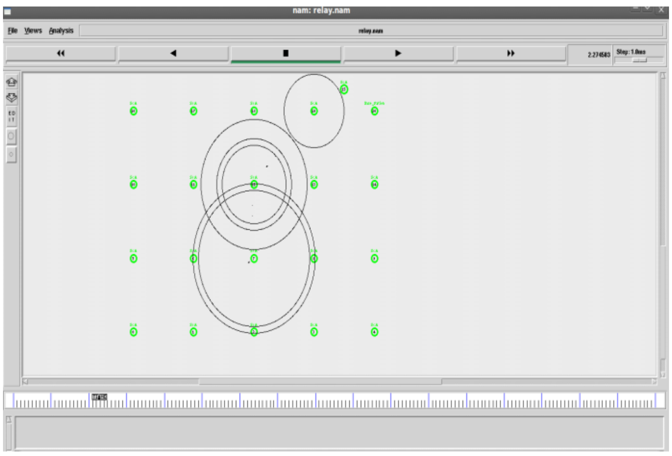


Figure 4. Sensor network model

Step 2: Data transmission

The data transmission model is shown the Figure 5. Normally the data's are sent from source node to base station. The data's are transmit through multiple nodes and finally reaches to the base station. The path for the source and destination is discovered and the data is transmitted to the shortest path in



the network for the source and destination. The shortest path

Figure 5. Data transmission model

is calculated by using Destination Sequenced Distance Vector. The black dotes indicate the data. The nodes discovered the path and send the data to the destination.

Step 3: Node failure

The sensor network node failure model shown in the Figure 6. During the normal data transmission some of the nodes failed. The all nodes can set some threshold value. Whenever a failure occurs the threshold value becomes changed and produce alarm sound based on the threshold value. Thus the node failure is indicated to the base station in the network. The base station receives messages from all nodes. The base station is the head for this network. This base station will sends alternate mobile node to that failed node replacement.

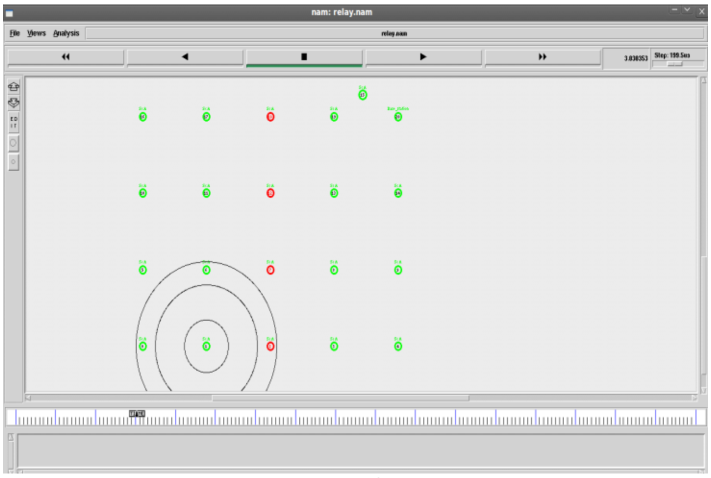


Figure 6. Node failure model

Step 4: Failure detection

The node failure shown in the Figure 7. When a node is detected as failed, then the next step is that, how can it recovered from failure or how to replace the node. When the nodes are failed the neighbor nodes will detect the failure node position and it will update to sink node. In this the node 15 is used for the node replacement. That node is ordered to recover the path by the base station. The base station only sends the 15th node to recover the path. The base station send request to all the nodes if any path is failure.

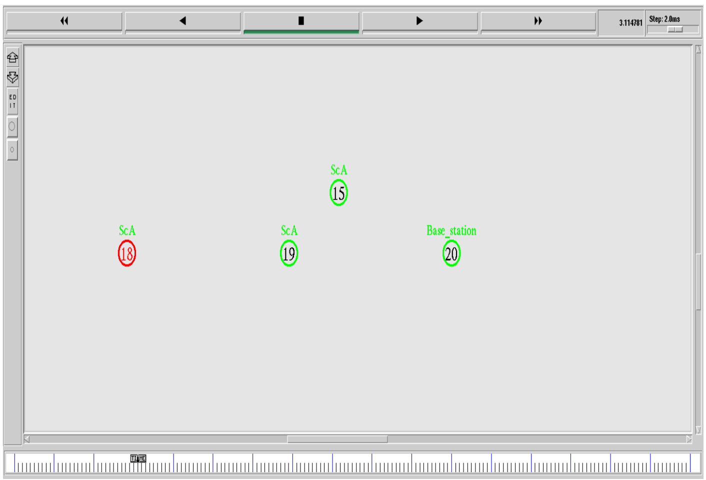


Figure 7.Node failure detection

Step 5: Node replacement

Node replacement is shown in the Figure.8. The node 15 is the sink node. The sink node will send nearby node to recover the node. It will replace the node and finally network will reform the network. Here the 15th node is used for the replacement of the node failure. The base station sends the command to the node 15 to replace the failure node in the path. Node 15 replaces the 18th node failure.

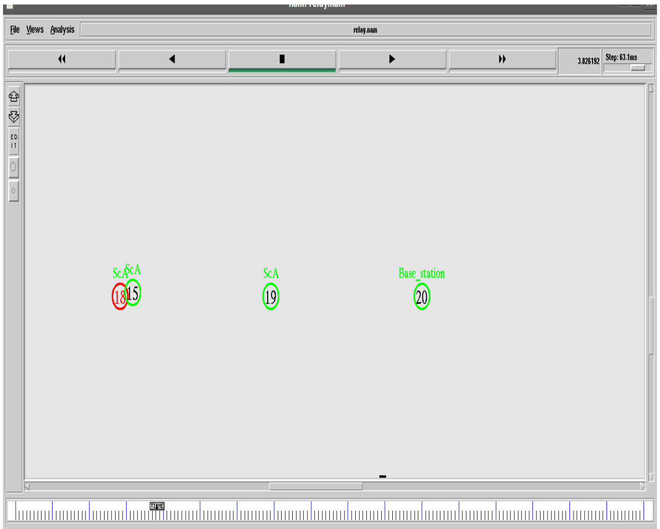


Figure 8. Node replacement model

Step 6: Continue data transmission

Then replacing the 18th node by 15th node the losses path is overcome is shown the Figure.9. The data transmission is continued by this process if the node failure occurs. By this method have to find the failure node and using node replacement we continue the data transmission.

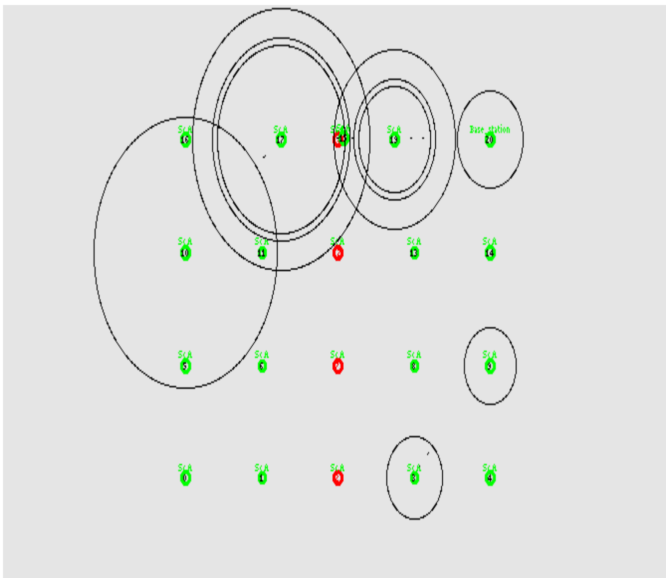


Figure 9. Continue Data Transmission

The overhead comparison graph is shown the Figure 10, in which the overhead is higher in the node failure case and lower in recovery mechanism. The data bits added to user transmitted data, for carrying routing information and error correcting and operational instructions. Overhead is undesired and must be avoided.

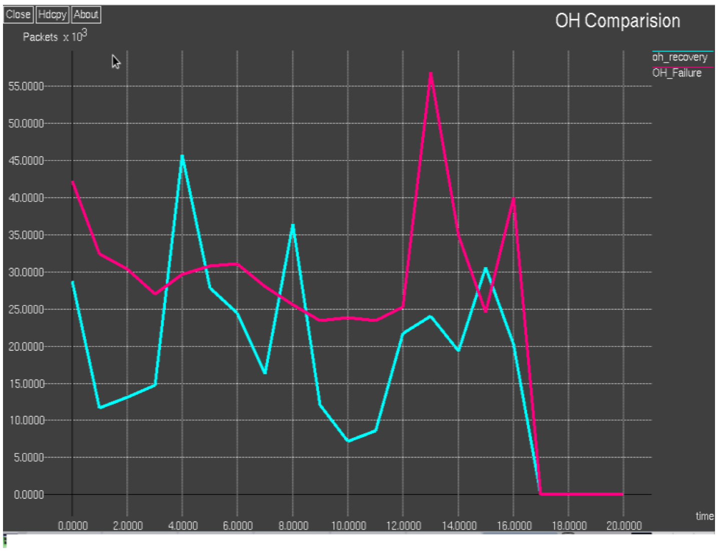


Figure 10. Overhead Comparison

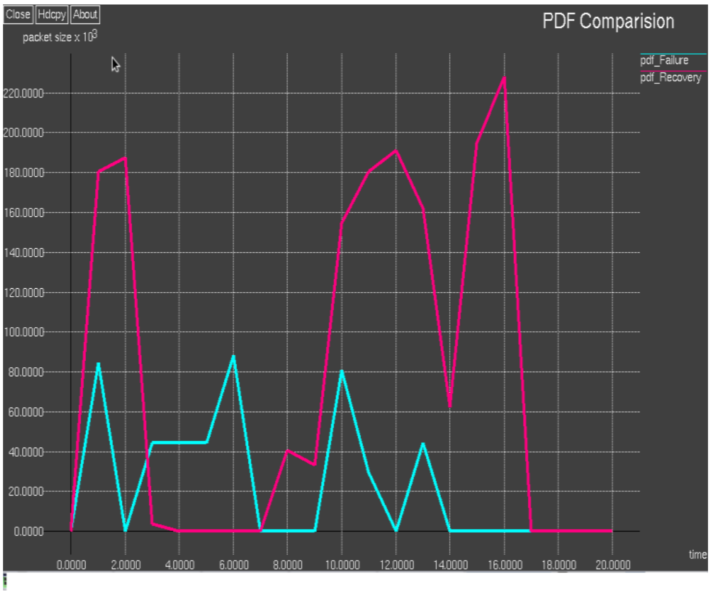


Figure 11 PDF comparison

The packet delivery fraction comparison is shown the Figure 11. The PDF is higher in the recovery schemes and lower in the failure case. It is defined as the ratio of packets that are successfully delivered to the destination compared to the number of packets that has been send out by the sender. The delay comparison is shown in The Figure 12. The delay is higher in failure case and lower in recovery mechanism. It is defined as the ratio of packets that are successfully delivered to the destination compared to the number of packets that has been send out by the sender.

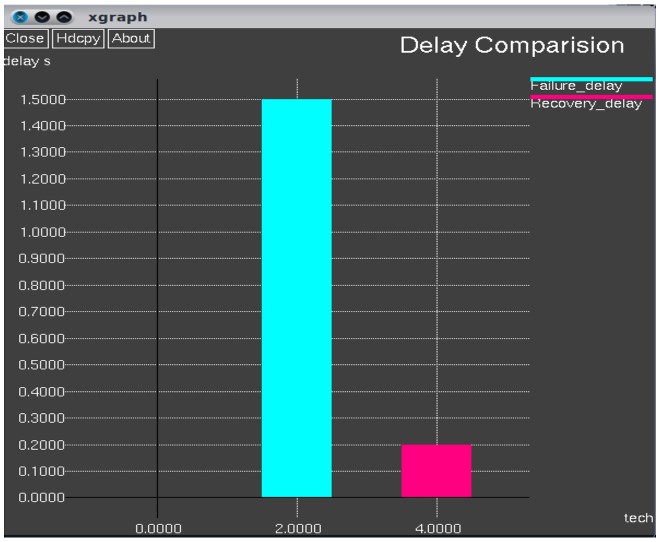


Figure 12. No. of Nodes Moved

TABLE.1. Parameter comparison

Parameters considered	**FTLT Mechanism**	**Recovery Mechanism**
Overhead	60%	20%
Packet delivery fraction	250pkts	460pkts
Number of nodes moved	30%	23%
Delay	0.55s	0.40s

In Table.1, the overhead is the data bits added to user transmitted data, for carrying routing information and error correcting and operational instructions. Overhead is undesired and must be avoided. It is higher in FTLT mechanism compared to that of recovery mechanism. The packet delivery fraction is defined as the ratio of packets that are successfully delivered to the destination compared to the number of packets that has been send out by the sender. It is higher than in recovery scheme. The sensor node movement alters the overall network performance, and it is comparatively high in the FTLT scheme than recovery scheme. Delay is defined as the ratio of packets that are successfully delivered to the destination compared to the number of packets that has been send out by the sender, it's is less in recovery scheme.

Conclusion

In real world applications of WSNs, sensors often fail and report erroneous observations for various reasons, thus compromising the trust of people towards WSNs technologies. A large percentage (25 percent) of the nodes report erroneous observations due to various reasons, such as random sensor faults. This paper investigated the node failure detection and reestablishment of network connectivity after node failure without extending the length of data paths. FTLT algorithm is used in Fault Tolerant Localization and Tracking of Multiple Sources in WSNs systems to detect the node failure. In this paper the recovery scheme is provided by using manager node movement concept. It also incorporates with the shortest path calculation mechanism by using Destination Sequenced Distance Vector (DSDV) protocol. The future enhancement of this paper can be done by using Reliable Event Transmission Protocol (RETP) in a wireless sensor network for real time event detection and reliable packet forwarding in wireless sensor networks.

.

References

[1] Michaelides and Panayiotou C.G,(2014) “Fault Tolerant Maximum Likelihood Event Localization in Sensor Networks Using Binary Data,” IEEE Signal Processing Letters, vol. 16, No. 5, pp. 406-40.

[2] Abdel, Hamid Hossam and Hassanein Glen Takahara,(2011), “Routing for Wireless Multi Hop Networks – Unifying and Distinguishing Features ,” Vol. 17, No.8, pp.1454-1465.

[3] Agreenberg and Winograd.S , (2006), “A lower bound on the time needed in the worst case to resolve conflicts deterministically in multiple access channels ,” Vol. 32.No.3,pp.589-596.

[4]Charles.E.Perkins and Elizabeth. M.Royer, (2007),“Ad_hoc On_Demand Distance Vector Routing ,” Vol 5. No.14,pp.153-181.

[5] Fenye Bao, Ing-Ray Chen, Moon Jeong Chang, and Jin-Hee Cho,(2012), “Hierarchial Trust Management For Wireless Sensor Networks And Its Applications To Trust Based Routing And Intrusion,”IEEE Trans Commun.,Vol. 9. No.2,pp 169-183.

[6]GuoyouHe,(2011),“Destination-Sequenced Distance Vector (DSDV) Protocol,”IEEE Trans Commun.,Vol.10.No.8,pp.1178-1186.

[7] Gottie and W.J. Kaiser, (2002)“Information Processing in Microsensor Networks,” IEEE Signal Processing Magazine, Vol. 19, No. 2, pp. 13-14.

[8] Junqi Zhang, Rajan Shankaran, Mehmet A. Orgun, Vijay Varadharajan and Abdul Sattar,(2010), “A Trust Management Architecture For Hierarchial Wireless Sensor Network,” IEEE Conference on Local Computer Networks, Vol. 22.No.24, pp. 115-120.

[9] Martin Schutte, (2006), “ Detecting Selfish And Malacious Nodes In Manets,”Vol. 18.No.13,pp.1-7.

[10] Michaelides, F. Liu, A. Thaeler, D. Chen, and X. Cheng, “Fault-Tolerant Target Localization in Sensor Networks,”(2007), EURASIP J. Wireless Comm. and Networking, vol.17,No.1, pp. 1-9.

[11] Pedro B. Velloso, Rafael P. Laufer, Daniel de O. Cunha, Otto Carlos M. B. Duarte, and Guy Pujolle,(2010), ” Trust Management In Mobile Adhoc Network Using Scalable Maturity Based Model,”IEEE Trans,Vol. 7.No.3,pp. 172-185.

[12] Riaz Ahmed Shaikh, Hassan Jameel, Brian J. d’Auriol, Heejo Lee, Sungyoung Lee and Young-Jae Song,(2009), “Group Based Trust Management Scheme For Clustered Wsn,” IEEE Trans, Vol. 20.No.11,pp. 1698-1712.

[13] Rony Niu and P. Varshney,(2004), “Target Location Estimation in Wireless Sensor Networks Using Binary Data,”Vol.9,No.3,pp.24-33.

[14] Sagar D. Padiya, Rakesh Pandit, Sachin Patel,(2012), “A System For Manet to Detect Selfish Nodes,”Vol. 1.No.2,pp. 25-35.

[15] Sedgewick Chen, Kia Makki, Kang Yen, and Niki Pissinou,(2009), “Sensor Network Security:A Survey,”Vol.11,No.2,pp. 52-73.