INTERNATIONAL JOURNAL OF RESEARCH IN COMPUTER APPLICATIONS AND ROBOTICS
ISSN 2320-7345

IMPROVING ROUTING IN INFECTED AREAS OF WSN USING FUZZY CLUSTERING

Mrs Suma S.C[1], Mrs Swathi Y[2]

[1] M.tech (CSE) CMR institute of technology Bangalore, India
sc.suma@gmail.com
[2] Associate prof (CSE), CMR institute of technology Bangalore, India

Abstract: - In Wireless Sensor Networks with infected nodes, identifying infected nodes and deliver data packets are challenging. Infected nodes in Wireless sensor network are the sensor nodes one which exhibits anomaly. Anomalies in sensed data occur due to node failures, malicious attacks or due to dying energy level. Infected nodes can generate and send erroneous data to the base station. When such infected node exists in the WSNs, it causes communication disruption resulting in inaccurate data, misleading packet transmission. It is necessary to identify such infected nodes to ensure and maintain accurate data delivery. In this paper we are bypassing the infected nodes by exploiting uninfected node multi paths. Our approach takes the shorter path to bypass the infected node.

Keywords: Wireless Sensor networks, Routing Protocols, Anomalies Detection, Clustering, Fuzzy clustering

1. Introduction

Wireless sensor networks (WSN) have been and being deployed in remote environment monitoring applications. In Most Wireless Sensor Network applications, the entire network must have the ability to operate in harsh environments regardless of the constraints. The Basic feature of any sensor as shown in fig 1 networks is to monitor and sense the surrounding. Catastrophic conditions can be expected due to the short duration of the battery energy of the sensors and the possibility of damaged nodes during deployment as the large number of sensors is expected.A wireless sensor network consists of huge collections of sensor nodes, each with limited capabilities of sensing, processing and communicating.

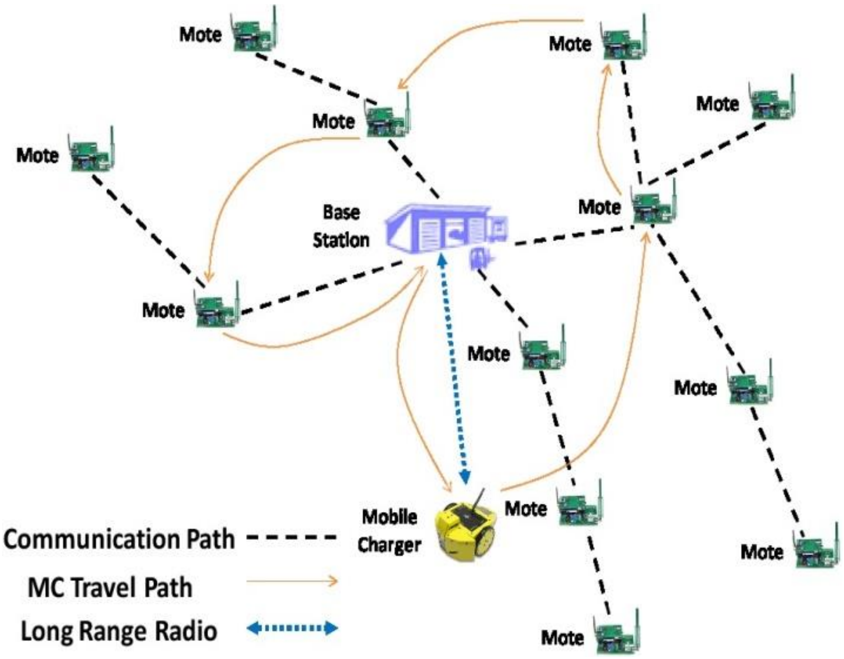


Fig 1.Wireless sensor network

. Due to the limited capabilities of sensor nodes, they are prone to failures. For example, reading errors, malicious attacks, and hardware and software failure. These factors can reduce the node functionality and could affect the WSN operations. Such threats could cause node failure which leads to destructive effects on monitoring applications. Nodes which are malfunctioning due to these factors are classified as infected nodes. Such infected nodes are fails to do their normal sensing and communication tasks. Such sensors which are unable to do their normal sensing tasks are fails to observe timely delivery services that crucial to maintain high Quality of Service (QoS) in WSN. These infected nodes degrade the network reliability unless some provisions are made to bypass them.

2. Related work

The issues related to sensor localization, fault-resilience, network lifetime, security and also routing in WSN have been addressed by researchers with different approaches. Among these routing issues are significant.
Due to the limitation of the transmission range in WSN most of the routing algorithms uses multi hop transmission. One of the issues in traditional GF algorithm is congestion causing traffic overflow. This scenario will cause packet loss and reduce the packet delivery ratio. Our paper focusing on diverts the incoming traffic to the uninfected nodes if the packets are being transmitted to the infected nodes. Bypassing the infected nodes or holes found in BOUNDHOLE algorithm. This algorithm identifies the boundary of holes and forwards the packets by GF algorithm. The major drawback of this algorithm is false boundary nodes that will fall into a loop. This leads to longer routing which degrades the performance.

3. Proposed work

3.1 Problem Description

The main problem in WSN limited capabilities of sensor node, due to which they prone to various failures (malware attacks, software and hardware failures) that impact the wireless network operations. When a node malfunctions, that node can be referred as infected; such infected node will fail to do normal sensing and communication tasks. There are real challenges in ensuring timely and maintain accurate data delivery in emergency conditions. Therefore the problem needs to be considered in such scenario is to bypass infected nodes and retour the incoming traffic towards uninfected region. This paper focuses on detecting the infected node/infected region in WSN and avoids such infected nodes in further transmission and communication processes. We addressed the problem that will be caused if the packets are transmitted into an infected region and we are also concerned with avoiding any infected regions which is crucial to prevent packets from being trapped and lost during transmission.

3.2 Proposed method

In this paper, the problem that will cause if the packets being trapped into the infected nodes and the way of bypassing such infected nodes to ensure successful data delivery. Infected nodes are identified by adapting fuzzy based clustering which groups the nodes. Infected nodes are detected based on the anomalous data that are identified in each node. Once these infected nodes are identified, those nodes information are used by the BPR method to bypass those infected nodes. We are also addressing diverting the incoming to the uninfected nodes to further transmission in order to send the information towards the destination.
The Proposed By-Passed Routing (BPR) technique comprises two parts.

- Infected area detection
- By-passed routing.

First part identifies the occurrence of infected nodes by Fuzzy Data Clustering approach to detect anomalies. Fuzzy clustering is suitable while evaluating whether a node is infected or not, and is it through a hardware malfunction, malware attack or software corruption.
The second part uses the information obtained on infected nodes/areas and diverts the incoming traffic to unaffected areas and by-passed the routing

i. Fuzzy Data Clustering: Infected nodes in communication space identified via Fuzzy Data Clustering method. This approach uses Fuzzy C algorithm to detect anomalies in sensor measurements.
ii. By-Passed Routing (BPR)

This technique aims at two things .First, getting the stuck packets out of infected region and forwards these packets to their destination on time. Secondly, we are concerned about divert the incoming traffic away from such infected region to avoid packets from being sent to the infected region.

The Twin Rolling Balls: Once the infected packets are detected and the nodes that are holding such infected packets are also identified, it needs to identify the boundaries of such infected nodes to avoid sending packets to these nodes. The idea detection of boundary nodes is inspired by the Existing solution (GAR) Rolling ball technique. However, in the proposed Twin Rolling Ball technique roll the ball in both the directions simultaneously; clockwise and counter-clockwise. So this is done in order to find the next closer node quickly to continue with the routing process.

Definition (The Twin Rolling Balls) The Twin Rolling Balls is defined as two identical balls RB1Ni(Si;R/2) and RB2Ni(Si;R/2) with radius R/2 that are attached at NLocal, rotate in two directions simultaneously. Each ball has the same characteristics. An illustration of twin rolling balls can be seen in Figure which shows the rotation in both directions.

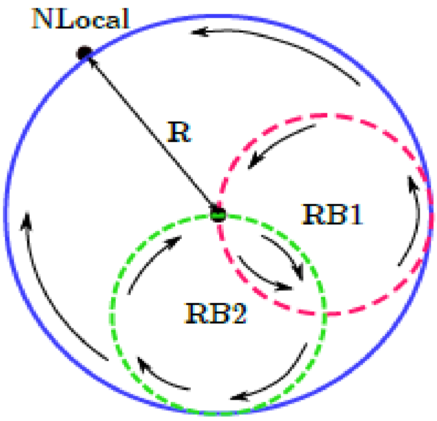


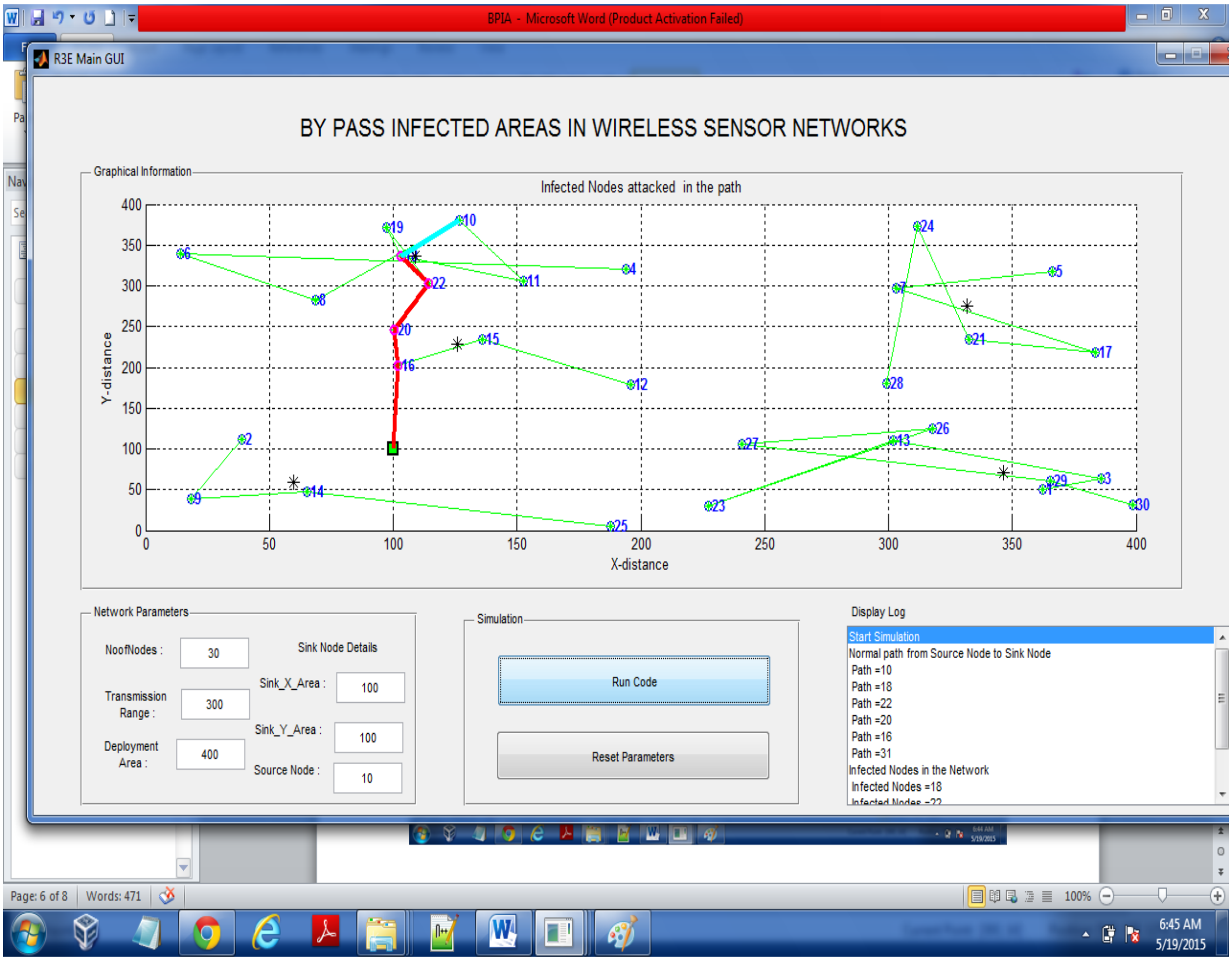
Fig 5.Two rolling operation

The Twin Rolling Balls Technique selects Exit gate node once the same node is about to visit again. In fig 6 as the ball will attach at Ne, it will roll and hit N10. This process continues till the packet is reached its destination node ND. This method unnecessary visits to other nodes (Ne;N10;N11;N12) while there is another shorter route to the destination. In contrast, the proposed method will choose N8 as an exit gate node. The selection of this exit node is based on the transmission range covered by NLocal. Ne node is excludes as exit gate node avoiding taking longer routes. From Node 8 it will proceed with normal forwarding using GF algorithm. The moment packet reaches exit gate node we stop the rolling process and forward the packet using GF algorithm.

By-Passing Infected Areas: This is to provide alternative route to detour the affected packets. The initial phase of the proposed BPR technique is based on the GF algorithm. Neighbours' location and distance to other neighbours are obtained through frequent beacon updates and kept in each node's routing table. Once each node aware of their infection status, the corresponding node quickly send a flag notification to source, so that it will not receive the further packets. Upon receiving flag notification, source node will sending packet towards infected nodes.

4. Experimentation, Result and Interpretation

Scenario 1:



Network Parameters

NoofNodes : 30

Transmission Range : 300

Deployment Area : 400

Sink Node Details

Sink_X_Area : 100

Sink_Y_Area : 100

Source Node : 10

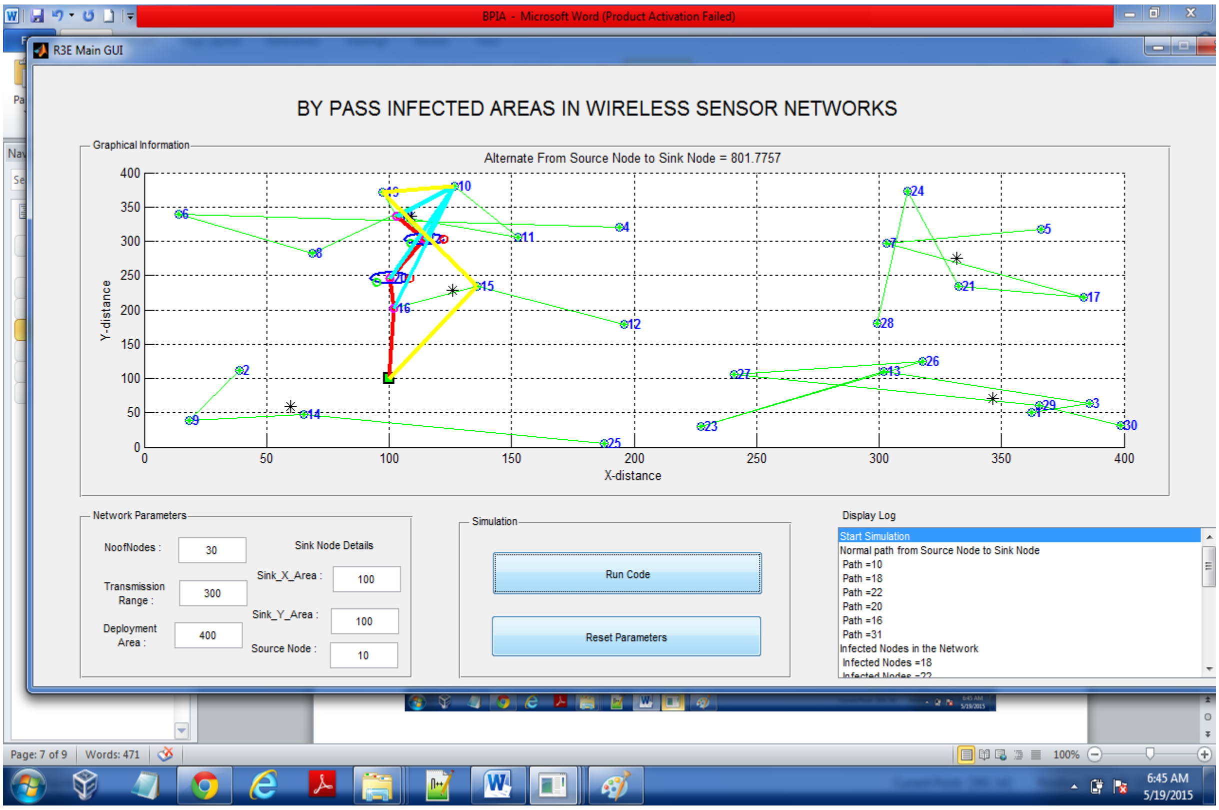
Simulation

Display Log

```
Start Simulation
Normal path from Source Node to Sink Node
 Path =10
 Path =18
 Path =22
 Path =20
 Path =16
 Path =31
Infected Nodes in the Network
 Infected Nodes =18
 Infected Nodes =22
```

In this first scenario we have set of wireless sensor nodes communicating each other with an infected area.

Scenario 2:


BPIA - Microsoft Word (Product Activation Failed)

R3E Main GUI

BY PASS INFECTED AREAS IN WIRELESS SENSOR NETWORKS

Graphical Information

Alternate From Source Node to Sink Node = 801.7757

Network Parameters

NoofNodes : 30

Transmission Range : 300

Deployment Area : 400

Sink Node Details

Sink_X_Area : 100

Sink_Y_Area : 100

Source Node : 10

Simulation

Display Log

```
Start Simulation
Normal path from Source Node to Sink Node
 Path =10
 Path =18
 Path =22
 Path =20
 Path =16
 Path =31
Infected Nodes in the Network
 Infected Nodes =18
 Infected Nodes =22
```

Page: 7 of 9 | Words: 471 | 100%

6:45 AM
5/19/2015

In the second scenario by passing the affected area for transmission by providing the alternate route towards to the destination through uninfected nodes.

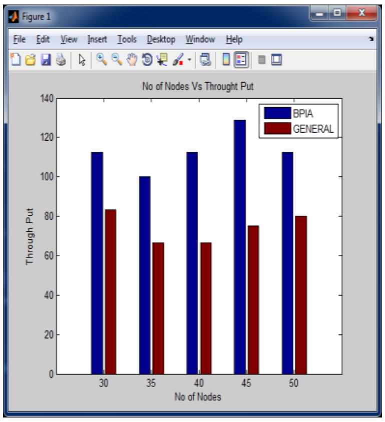


Figure 1

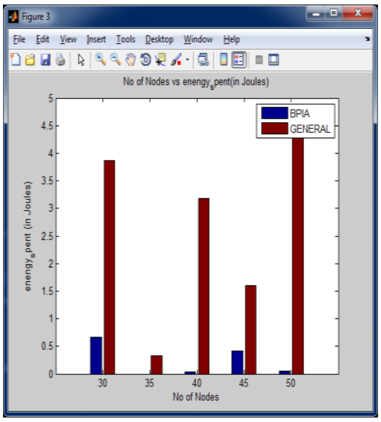


Figure 3

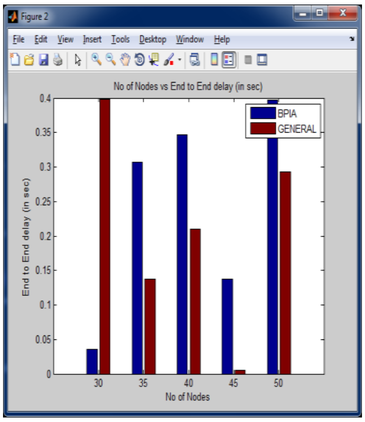


Figure 2

The results are calculated by the below parameters

- Throughput
- End2Enddelay
- Energy Spent

From the graph it is clearly observed that By passed Routing Technique using fuzzy clustering is better than general technique for transmission in wireless sensor networks

5. Conclusion

In the proposed work, we tried to improve the routing in infected areas of WSN by bypassing the infected areas. This bypassing mechanism is used to provide high energy efficient routing in wireless sensor networks. We have studied the effectiveness of our proposed By-Passed routing (BPR) in avoiding infected areas and its efficiency in improving the overall performance.

REFERENCES

[1] A. Abdulla, H. Nishiyama, J. Yang, N. Ansari, and N. Kato,“HYMN: A novel hybrid multi-hop routing algorithm to improve the longevity of wsns,” IEEE Transactions on Wireless Communications, vol. 11, no. 7, pp. 2531–2541, July 2012.

[2] M. Ahmadi Livani and M. Abadi, “An energy-efficient anomaly detection approach for wireless sensor networks,” in IST: 5th International Symposium on Telecommunications, 2010, pp. 243–248.

[3] N. Ahmed, S. S. Kanhere, and S. Jha, “The holes problem in wireless sensor networks: a survey,” SIGMOBILE Mob. Comput. Commun. Rev., vol. 9, no. 2, pp. 4–18, Apr. 2005.

[4] I. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, “A survey on sensor networks,” IEEE Communications Magazine, vol. 40, no. 8, pp. 102–114, 2002.

[5] N. Arad and Y. Shavitt, “Minimizing recovery state in geographic ad hoc routing,” IEEE Transactions on Mobile Computing, vol. 8, no. 2, pp. 203–217, 2009.

[6] Ashwini and P. A. S, “Information dissemination between nodes of different intersections intersection in city environment using hop greedy routing protocol (BAHG),” International Journal of Ethics in Engineering and Management Education, vol. 1, no. 4, pp. 232–236, April 2014.

[7] D. Chen and P. K. Varshney, “On-demand geographic forwarding for data delivery in wireless sensor networks,” Computer Communications, vol. 30, no. 1415, pp. 2954 – 2967, 2007.

[8] S. Chen, G. Fan, and J. hong Cui, “Avoid ”void” in geographic routing for data aggregation in sensor networks,” International Journal of Ad Hoc and Ubiquitous Computing, vol. 1, pp. 169–178, 2006.

[9] R. Di Pietro, L. Mancini, C. Soriente, A. Spognardi, and G. Tsudik, “Data security in unattended wireless sensor networks,” IEEE Transactions on Computers, vol. 58, no. 11, pp. 1500–1511, Nov 2009.

[10] Q. Fang, J. Gao, and L. Guibas, “Locating and bypassing holes in sensor networks,” Mobile Networks and Applications, vol. 11, no. 2, pp. 187–200, 2006.

[11] K.-I. Kim, M.-J. Baek, and T.-E. Sung, “Load balancing for greedy forwarding of geographic routing in wireless networks,” IEICE Transactions, vol. 93-B, no. 8, pp. 2184–2187, 2010.

[12] H. Kumarage, I. Khalil, Z. Tari, and A. Zomaya, “Distributed anomaly detection for industrial wireless sensor networks based on fuzzy data modeling,” Journal on Parallel and Distributed Computing, vol. 73, no. 6, pp. 790–806, Jun. 2013.

[13] S. Lai and B. Ravindran, “Least-latency routing over time dependent wireless sensor networks,” IEEE Transactions on Computers, vol. 62, no. 5, pp. 969–983, 2013.

[14] W. Liu, H. Nishiyama, N. Ansari, J. Yang, and N. Kato,“Cluster-based certificate revocation with vindication capability for mobile ad hoc networks,” IEEE Transaction on Parallel Distributed System, vol. 24,no. 2, pp. 239–249, Feb. 2013.

[15] J. Na, D. Soroker, and C.-K. Kim, “Greedy geographic routing using dynamic potential field for wireless ad hoc networks,”IEEE Communications Letters, vol. 11, no. 3, pp. 243–245, 2007.