ISSN: 2350-0328

International Journal of Advanced Research in Science, Engineering and Technology

Vol. 3, Issue 2 , February 2016

By-Passing Infected Areas in Wireless Sensor Networks using BPR – A Survey

Mamatha K.R, Ramakrishna M

PG Student, Department of computer science and Engineering, Vemana Institute of Technology, Bangalore
Associate Professor, Department of computer science and engineering, Vemana Institute of Technology, Bangalore

ABSTRACT: Irregularity in sensed data streams reveal the spreading of malignant attacks such as hardware failure, software exploitation among distinct nodes in wireless sensor networks. The above circumstance of node impurity can disturb generated incoming data flow resulting in immense opportunity of incorrect data, false packet translation, erroneous decision making and serious communication interruption. This aforementioned problem is destructive to real time applications having strict quality of services(Qos) requirements, sensed data from disinfected regions also fastened in an corrupted region should make preceding arrangements. Existing methods(BOUNDHOLE and GAR) is used to modify and ease the issues, since the outcome is bound by a few constraints due to huge risk of sliding into routing loops and involvement in irrelevant transmissions. Author presents a solution to by pass the infected nodes dynamically using twin rolling balls technique and redirect the packets that are trapped inside the identified area. Identity of infected nodes is performed by complying a Fuzzy data clustering which classify the nodes on the basis of anomalous data identified in specific data streams. Further the information is used by proposed solution of By-Passed Routing that rotates balls in two directions: clockwise and counter clockwise. The node that hits any ball in any direction first is selected as next hop .it also bothers about the incoming packets that can be affected when problem occurs. To solve afore said problems in existing methods, the proposed technique BPR has enormously upgraded the Qos parameters.

KEYWORDS: Wireless Sensor Networks, Anomalies Detection, Routing Protocols, Fault Tolerance

I. INTRODUCTION

In remote event control applications Wireless sensor networks has been the cutting edge technology, exclusively in areas and adverse environments, for more than a decade. The detection of events is made possible through forwarding from sensor nodes to so called sink node and data sensing for more processing. The occurrence of any accidental action commonly involves communicating data to sink node. Energy constraints, resource limitations are decreased by direct communication between sensor and sink node. The basic feature of any sensor network is to monitor and sense the surrounding. Fig 1

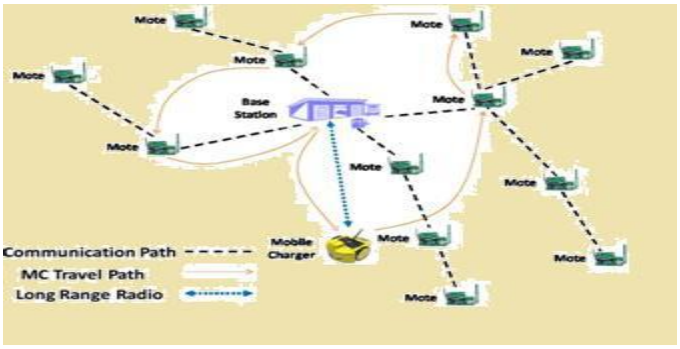

Fig 1 Wireless Sensor Network[WSN]

The two basic components of WSN are cluster head which are also called as aggregations points and base station. Cluster heads are formed to transmit the load energy equally to all sensor nodes. The base station is used to analyse and

ISSN: 2350-0328
International Journal of Advanced Research in Science, Engineering and Technology
Vol. 3, Issue 2 , February 2016

gather data from other sensor nodes. Finite capabilities of sensor nodes are sensitive to various failure such as malware attack, software exploitation, hardware failure. Nodes allowing the above mentioned failures can be classified as infected so performing normal sensing and communication tasks fail hence producing faulty data .An Example of infected nodes and regions on a WSN is shown in Fig2.

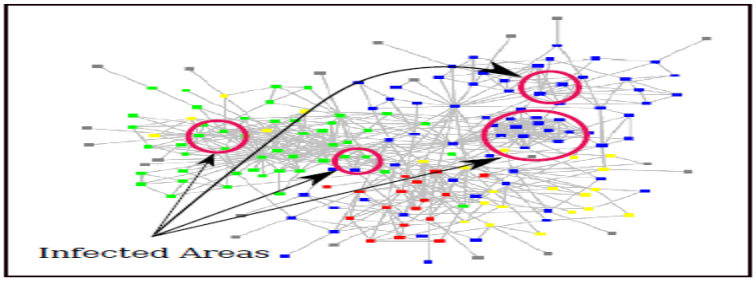

Fig 2 Nodes identified as infected areas.

Data brought by this kind of nodes contain abnormalities that does not mirror exact data .For eg temperature fluctuations observed from normal readings taken. If there are flaws in the node the sensing process will be disorganized, causing serious periodic connection over the whole network, packets may not be forwarded to the destinations by trapping in the infected areas. It introduces the problem of packet loss rate and high consumption of energy in WSNs. Packets carrying important information about occurrence of emergency situation this type of loss of packet could result in severe consequences which affect the whole nation using the network. Anomalous data resulting in incorrect decision making and bad data collected systems in the network need to timely detect corrupted nodes and avoid them which require alternative routes to be reconstructed making incoming packets to detour packets to its destinations by avoiding infected areas.

II. OBJECTIVE

The research is driven by a concern to address the following issues:

- To find a solution that can mitigate the above said problems and get stuck packets out
- To design a method that can By-Pass the infected areas
- To minimize the effects of infected nodes.

III. RELATED WORK

WSN research community is considered with a few issues including network lifetime[1] which propose Hybrid Multihop routing HYMN algorithm which is a hybrid of two contemporary multi-hop routing algorithm architectures namely Flat multi-hop routing that utilizes efficient transmission distances and hierarchical multi-hop routing algorithm that capitalizes on data aggregation.
In [2] detecting anomalies in sensed data in a WSN is essential to identify malfunctioning nodes in order to minimize communication overhead and energy consumption.
In [3] sensor localization by distributed angle estimation propose to estimate the angle of departure (AOD) of the emitted waves at each receiving node via frequency measurement of the local received signal strength indication(RSSI) signal.
In [4] Wireless Sensor and Actuator networks(WSANs). Using the mobile sink as an example of the actuator to control the movement of a sink has been adopted by researchers in the past to achieve high efficiency in terms of gathering data from the sensors so proposes a novel method based on set packing algorithm and travelling salesman problem.
In [5] MANETs have attracted due to mobility and ease of deployment major challenge is to guarantee secure network, certificate revocation is important, issue of certificate revocation to isolate attackers from further participating in network activity.
Most of the routing protocols developed for sensor networks employ greedy forwarding algorithm which forwards a packet to a destination node via one hop neighbor[6].It repeats the process until the packet reaches destination and also efficient in reducing energy consumption.

ISSN: 2350-0328

International Journal of Advanced Research in Science, Engineering and Technology

Vol. 3, Issue 2 , February 2016

Local minima generally refers to situation in which packet cannot be forwarded to the next hop since no other node has shorter distance to destination. A graph based technique is employed which require the entire network to be stored leading to poor scalability, non graph based technique will result in long routing paths and high energy expenditure. Here holes can be inferred as hot spots caused by traffic congestion.
Routing technique to divert traffic away from holes or infected regions and by passing them introduces BOUNDHOLE to discover holes and establish adaptive routes to bypass identified nodes. Another issue is false boundary detection that presents a high risk of falling into loops.
To tackle the problem of false boundary GAR is designed which employs a rolling ball method which is attached or hinged at the node having local minima problem and rotate counter clockwise with R/2 radius and visits unnecessary nodes.

IV. EXISTING SYSTEM

A. Local minima problem: Routing protocols in wireless sensor network adopt greedy forwarding algorithm which forwards the packet via one hop neighbour to the destination node. A Local minimum problem refers to situation in which packet cannot be forwarded to the next hop since there exist no other node that has shorter distance than itself.
The neighboring table contains closest one hop neighbors the node that has largest distance to destination could not be choosed
.
B. Boundhole: It is a distributed algorithm that builds routes and holes, which are connected regions of the network with boundaries consisting of all stuck nodes. These hole- surrounding routes can be used in many applications such as geographic routing, path migration, information storage mechanisms and identification of regions of interest. It route the packets based on GF algorithm.

C.GAR(Greedy Anti Void Routing): To handle the issue of false boundary detection in Boundhole method GAR is designed. The protocol of greedy anti void routing protocol is based on Unit Disk Graph(UDG) which is proposed to guarantee packet delivery to the specified destination by resolving the void problem and to increase routing efficiency.
GAR employs a rolling ball method which is attached at the node having local minima problem and rotate counter clockwise with R/2 radius. The first node that intersects with the rolling ball and which is closer to the destination node is selected as next hop. It repeats the process until the packet safely arrives at the destination node.

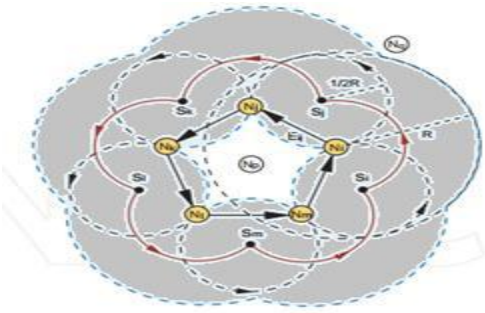

Fig 3 Rolling ball

Rolling ball for given S_i and N_i the method turns the rolling ball $RB_{Ni}(S_i,R/2)$ counter clockwise and builds the easy closed curve(i,e flower like solid curve in the above figure).The boundary Set $B=\{N_i,N_j,N_k,N_l,N_m\}$ is recognized as a easy unidirectional ring.

Disadvantages:
GAR visits unnecessary nodes thus resulting in higher energy consumption.
BOUNDHOLE approach is subjected to routing loops due to false boundary detections. other effects are high delay, higher communication overhead, higher energy consumption.

ISSN: 2350-0328
International Journal of Advanced Research in Science, Engineering and Technology
Vol. 3, Issue 2 , February 2016

V. PROPOSED SYSTEM

By-Passed Routing System: The By-Passed Routing(BPR) technique comprises two parts

- Infected area detection
- By-Passed Routing

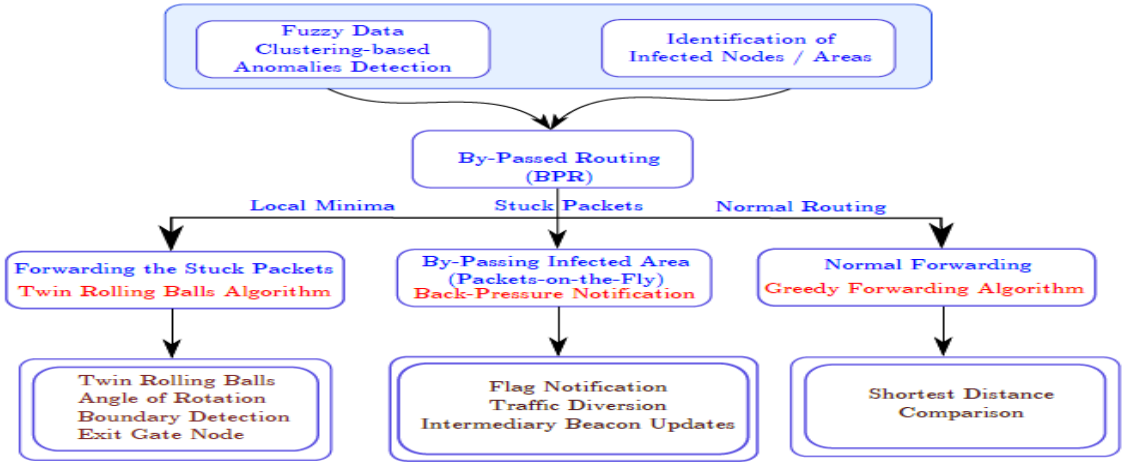

Fig 4 The proposed architecture view[BPR technique]

First part identifies the infected nodes by Fuzzy Data Clustering to detect anomalies. This method is chosen as it evaluates anomalous data over various sensor nodes. A centric data point view with fuzzy cluster is correct when evaluating a node is infected or not whether through malware attack, hardware malfunction or software corruption.
Infected node information is then used for traffic diversion in the proposed BPR technique. The innovation of BPR approach relies on introduction of twin rolling ball technique that recognize the next one hop neighbours immediately than the GAR approach. Getting the trapped packets out of infected region is other contribute of BPR.

- **Fuzzy Data Clustering:** Infected nodes in communication space identified via Fuzzy data clustering method uses Fuzzy C algorithm to detect anomalies in sensors. In this algorithm an attempt is made to partition a finite collection of 'n' elements X={X1,X2,X3,X4,…..Xn} into collection of 'C' fuzzy cluster. In a given finite set of data the FCM will return us a set of 'C' cluster centre C={C1,C2,C3,…Cc} and also partition matrix $W=W_{ij}$ €[0,1] with i=1,2,3,4..j=1 in which W_{ij} tells the degree to which elements X_i belongs to cluster C_j. To determine the shortest route between nodes Dijikstra algorithm is used .In the given network for any provided source node, the shortest route is detected by taking x and y coordinate along with threshold value of that node and process continues till the destination is reached.
- **By Passed Routing[BPR]:**This technique is aimed at two things. First getting the stuck packets out of infected region and forward the packets to destination, Secondly divert the incoming traffic away from infected region.

Given a set of sensor nodes $N=[N_1,N_2,N_3,\ldots N_n]$on a WSN, a particular node N_i is considered as infected if it satisfies threshold value based on energy value. If the value is above threshold which is random is considered as infected node. Infected nodes are those which violate normal function of the network so it is detected and by passed
When nodes are infected some packets are trapped inside the region and cannot be forwarded to the next hop simply because there is no available node to do so, such that these packets have a high possibility of being dropped if no alternative paths are made to get out of it. So the method called twin rolling ball came into exists. Stuck

ISSN: 2350-0328
International Journal of Advanced Research in Science, Engineering and Technology
Vol. 3, Issue 2 , February 2016

packets are identified if the node is out of transmission range to send the packet to next node due to local minima problem, hence this concept of twin rolling ball is used.

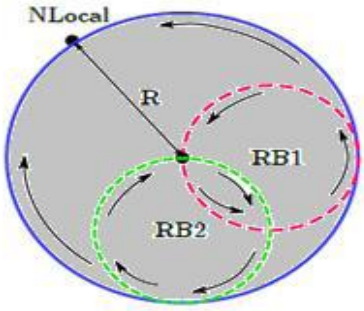

Fig 5 Two Rolling ball operation

The two identical balls RB1 $N_i(S_i,R/2)$ and RB2 $N_i(S_i,R/2)$ each with radius R/2 hinged at N local and turn around in two directions at once until the first node is hit. Instead of rotating in one direction may take a longer time if node is located far away from the ball, so two balls which are different is attached to same point(Nlocal) and rotate balls in different directions. The intersection between the rolling ball [RB $N_i(S_i,R/2)$] and node as the next corresponding boundary node.

After infected node and twin rolling ball is done, the back trace message must be send to source node to inform its infected and stop sending the packet to the node, To bypass the node and take alternative route. This alternate path again depends upon the parameter taken for the other nodes to satisfy the condition and taken in the loop with normal forwarding algorithm.

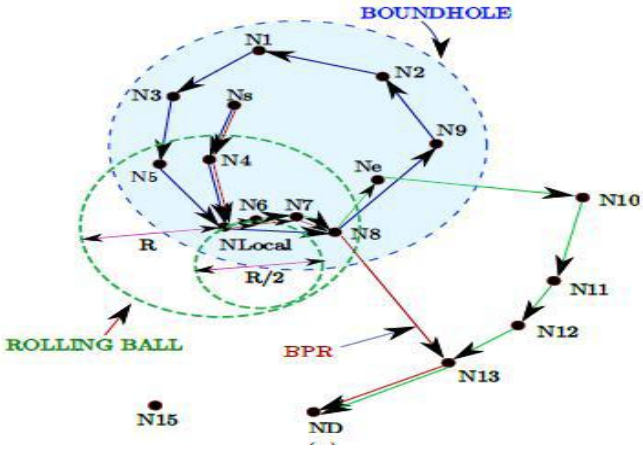

Fig 6 Example of constructing path using Rolling ball technique

In fig the ball will attach at N_e, it will roll and hit N_{10}.This process continues till the packet reaches destination node (N_D).This method unnecessary visits to other nodes(N_e,N_{10},N_{11},N_{12}) While there is another shortest route to destination. In contrast the BPR method will choose N_8 as an exit gate node. The selection of this exit gate node is based on transmission range covered by Nlocal. N_e node excludes as exit gate node avoiding taking longer routes. From node 8 it will proceed with normal forwarding using GF algorithm.

VI. CONCLUSION

In this work, the efficiency of BPR technique which avoids the infected nodes in the network is seen by improving overall performance of network. The infected nodes are detected by Fuzzy data clustering technique in which clustering is performed and infected node is calculated based on threshold value in energy model. This information is used by BPR to find alternate path to transfer packets from source to destination node with the help of twin rolling balls which

ISSN: 2350-0328

International Journal of Advanced Research in Science, Engineering and Technology

Vol. 3, Issue 2 , February 2016

defines the next forwarding node and reduces the false boundary detection.BPR has good performance in energy consumption, Hence BPR has regarded the best technique when compared to existing BOUNDHOLE,GAR methods in solving the problem.

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] W. Zhang, Q. Yin, H. Chen, F. Gao, and N. Ansari, "Distributed angle estimation for localization in wireless sensor networks," IEEE Transactions on Wireless Communications, vol. 12, no. 2, pp. 527–537, February 2013.
[4] H. Nakayama, Z. Fadlullah, N. Ansari, and N. Kato, "A novel scheme for WSAN sink mobility based on clustering and set packing techniques," IEEE Transactions on Automatic Control, vol. 56, no. 10, pp. 2381–2389, Oct 2011.
[5] 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.
[6] 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.
[7] 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.
[8] 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.
[9] 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.
.[10] 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.
[11] 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.
[12] R. Di Pietro, L. Mancini, C. Soriente, A. Spognardi, andG. Tsudik, "Data security in unattended wireless sensor networks,"IEEE Transactions on Computers, vol. 58, no. 11, pp. 1500–1511, Nov 2009.