

Power Efficient Anomaly Detection Using Pattern at Nodes in Wireless Sensor Network

Gourav Sahni*

Research Scholar

CSE dept., JMIT Radaur Kurukshetra University
India

Sonia Sharma

Assistant Professor

CSE dept., JMIT Radaur Kurukshetra University
India

Abstract—

Wireless Sensor Network (WSN) facilitate today's world by offering large number of application in almost every field. These applications require the WSN to be work effectively even if it is deployed in harsh environment. The proper functioning of the sensor network mainly depends on the sensor nodes as they have power supply which make network alive. As the sensor network are deployed in harsh environment so there is great chance of interference in the communication among nodes. Hence there is a need of anomaly detection method but the key concern is to minimize the communication overhead and energy consumption while detecting anomalies. There is need of energy efficient protocol and recent studies shows that ZRP is energy efficient. To perform anomaly detection this paper proposed a protocol by modifying one of the most popular routing protocol ZRP. This power efficient anomaly detection ZRP (ZRP-PEAD) uses traditional ZRP at base to perform detection in WSN.

Keywords— Wireless Sensor Network, Anomaly Detection, ZRP, ZRP-PEAD, Sensor Node etc.

I. INTRODUCTION

In recent years, Wireless Sensor Networks (WSNs) have gained attention due to development in the wireless and sensing technology. With the advent of the sensor node tasks like sensing, gathering information have become easy to perform. Wireless sensor network is a popular area for research now days, due to vast potential usage of sensor networks in different areas. A Wireless sensor network is composed of a large number of nodes, which are densely deployed and are capable of sensing, data processing and communication. Each Node in WSN is known as sensor or mote. A wireless sensor network can consists of thousand of sensors which are low-cost, small in size and have many capabilities. These nodes can be connected to one or several nodes. Sensors are powered by battery. The position of sensor nodes need not be or pre-determined. So we can easily have a random deployment of nodes in inaccessible terrains. A Wireless Sensor Network is shown in Figure 1.1. [1] [2]

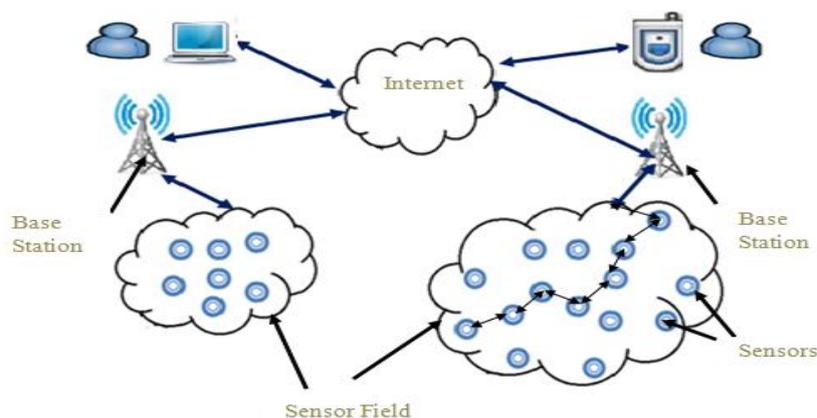


Figure 1.1 Simple Illustration of Wireless Sensor Network

A. Overview of WSN's Anomalies

Anomalies in WSN can be classified as given in [16] based on the nature of anomaly. These can be classified into three main categories as shown below in figure 1.2 [16]. *Network anomalies* are communication related problems that arise in WSNs. Their typical symptoms are an unexpected increase or decrease in amount of packets traversing the network. The network anomaly scope is many or all nodes. We detect these anomalies as if packet deliver rate is zero means there is some problem in network or communication between nodes hence network anomalies. *Node anomalies* are those which occur at a particular node. As WSN is deployed into harsh environments so there is a great chance for the nodes to be damaged hence results in node anomaly. The scope of this type of anomaly is only at a single node. *Data Anomaly* occurs when there are some irregularities are present in the sensed data. Some security breaches can also lead to anomalous data. They can be temporal, spatial and spatial temporal data anomalies.

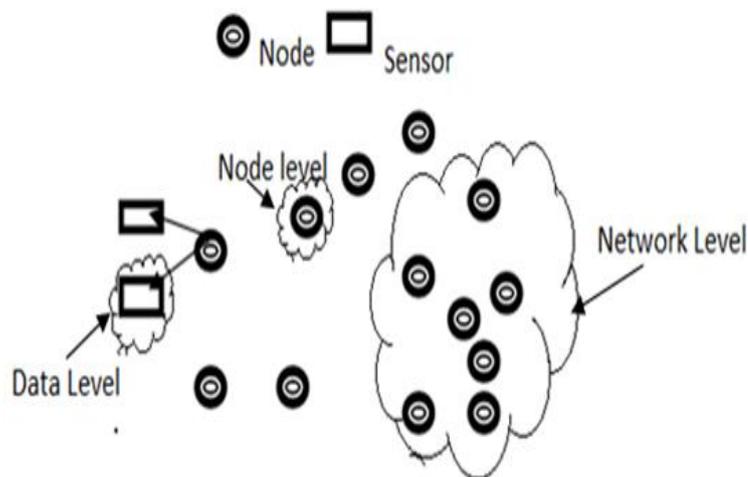


Figure 1.2 Basic Types of Anomalies in WSN

The design of any anomaly detection approach for WSNs should consider two main issues which are the effectiveness in detecting anomalies and efficiency in utilizing the network resources.

II. PROBLEM FORMULATION

Wireless Sensor Network consists of the many autonomous sensors nodes that communicate with each other using wireless communication. The sensor nodes also known as motes communicate with each other for transmitting and processing the data. The data gathered by the nodes is often unreliable due to many resource constraints like low power, less memory and low computational capability. All the nodes while communication sends the gathered raw data to its neighboring nodes which further send that data to sink. A large amount of energy is consumed during the communication of the nodes. If the data collected is inaccurate or anomalous then power consumed during communication is simply wasted. The main motive or challenge for a sensor network is to have larger lifetime as it has such application which requires this condition to be fulfilled.

The data gathered by the nodes are usually anomalous due to stringent constraints imposed on the sensor network. So here the main issue of concern is that we need to remove inaccuracy or we can say anomaly in the data gathered by the nodes. Till today many techniques are present there to detect and correct these anomalies. Each of the techniques uses different method and model for this purpose. Initially the centralized method was used to detect the anomalies in which all the nodes send data to the sink node or base station. This technique of detection was not energy efficient. As a large amount of power is needed for transferring the raw data from all the nodes of sensor network to the base node and if network is large the problem is severe. Another technique was distributed detection in which detection is done locally. In this we can cluster the data at each level in normal or abnormal cluster and can perform the detection at internal level if we are using hierarchical architecture of sensor node. In the end the hybrid technique was used which combine features of both centralized detection and distributed detection. Some of the technique detect the anomalies at the sink which somehow detect anomalies but does not improve network lifetime as the communication overhead is same as in collection of data. So there should be a method which reduces the communication overhead and hence energy as we considering it the major factor. Also a method must be developed to drop those packets which have anomalous data at each node so that number of packets send is less. Our main purpose is to analyze various anomaly detection techniques which can be used to detect the anomalies in the data at node level. The technique proposed must consider the concept of energy means the anomaly detection should be power efficient.

III. PROPOSED ALGORITHM FOR ANOMALY DETECTION

Anomaly detection can be done by using various techniques as proposed in [15] [12] [22]. Each of the technique has its own advantage and disadvantage. The algorithm proposed here used the ZRP as its base protocol due to its energy efficiency. The proposed algorithm is ZRP-PEAD i.e Power Efficient Anomaly Detection using Zonal Routing Protocol. The proposed algorithm is as followed.

Algorithm: ZRP-PEAD

1. Create sensor nodes and wireless network between them.
2. Start the Network and consider one of the nodes as sink in a zone. Sink node will collect the packets for a limited time period i.e. simulation time (T).
3. Each node within the zone will have packet of Normal pattern stored on it (used for detection).

4. Parameters on each sensor node defined are
 - No of packets(NP)
 - Node ID
 - Zone ID
5. Parameters considered during anomaly detection are
 - Data pattern of sending packets (DP_SNP),
 - Normal pattern of stored packet (NP_SOP),
 - No of packets (NP).
6. Run the following steps 7 and 8 for total simulation time T and for two different zone radius
7. At each sensor node check buffer to send undelivered packets stored at node.
8. Remove all the abnormal packets using procedure `purgeAbnormalPacket()` which works as follows


```

      If (NP == 0) then
        Nothing to do
      else
        If (DP_SNP) does not match (NP_SOP) then
          Skip or Drop Anomalous Packets using ZRP-PEAD
        else
          Send ZRP packet (normal packet)
        End if
      End if
      
```

IV. SIMULATION AND RESULTS

A. The Simulation Environment:

A wireless network consists of 30 nodes with a simulation time of 10 seconds. The Zone radius is taken as 1.5. The reference network of our simulations consists of 30 nodes distributed randomly in an area of 800×800 flat grid. In simulation environment, Zone routing protocol (ZRP) is used as the routing protocols. These 30 different nodes are involved in the communication. Some of the nodes are considered as sink nodes.

B. Simulation Parameters

The summary of various simulation parameters used are given below in Table 4.1.

Table 4.1: Summary of Simulation Parameters.

S.No	PARAMETERS	DESCRIPTION or VALUE
1	Network Size	800x800
2	No. of Nodes	30
3	Zone radius	1.5
4	Simulation Time	10s
5	Traffic Type	Constant Bit Rate (CBR)
6	Queue Type	Drop Tail
7	Max packets in Queue	50
8	Routing Protocol	ZRP
9	MAC Protocol	802.11
10	X dimension of the topography	800
11	y dimension of the topography	800
12	Observation Parameters	Energy, packet received, amount of energy saved

C. Simulation Metrics

- 1) *Energy Consumed*: Compare the amount of energy consumed at different simulation time. Simulation to compare Energy in both protocols was run for 10 seconds. The comparison of both the algorithm is shown below in tabular and graph form. Here, we consider the zone radiuses 1.5.

Table: Energy Consumed At zone radius =1.5

Simulation Time	Energy_Consumed_ZRP (With Anomaly)	Energy_Consumed_ZRP-PEAD(Without Anomaly)
1	0	0
2	87.5	0
3	125	11
4	167.5	13
5	200	20
6	230	35
7	325	39
8	360	42
9	375	48
10	399	50

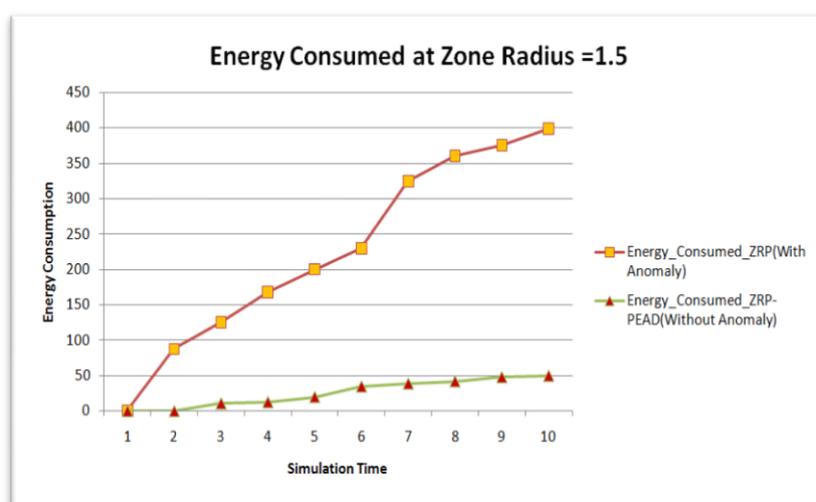


Fig 4.1: Comparison of Energy Consumed in ZRP and ZRP-PEAD ZR=1.5

The graph shows that the amount of energy consumed in ZRP-PEAD is very less as compared to ZRP.

- 2) *Percentage Amount of Energy Saved:* This can be calculated as follows:
 Assume total amount of energy consumed = Energy Consumed by ZRP
 Energy Consumed in ZRP= 399
 Energy Consumed in ZRP-PEAD= 50

Formula Used:

% of Energy Saved = (Energy Consumed in ZRP - Energy Consumed in ZRP-PEAD) / (Energy Consumed in ZRP) *100

Energy Saved = 399-50 = 349

% of energy Saved = 349/399 *100 = 87 % (approximate)

- 3) *Packet Received:* Here the packets received by sink in both the algorithms are compared at a given Zone Radius.

Simulation Time	Packet Received_ZRP	Packet Received_ZRP-PEAD
1	0	0
2	15	6
3	16	16
4	30	30
5	60	50

6	140	100
7	160	110
8	170	130
9	180	150
10	280	182

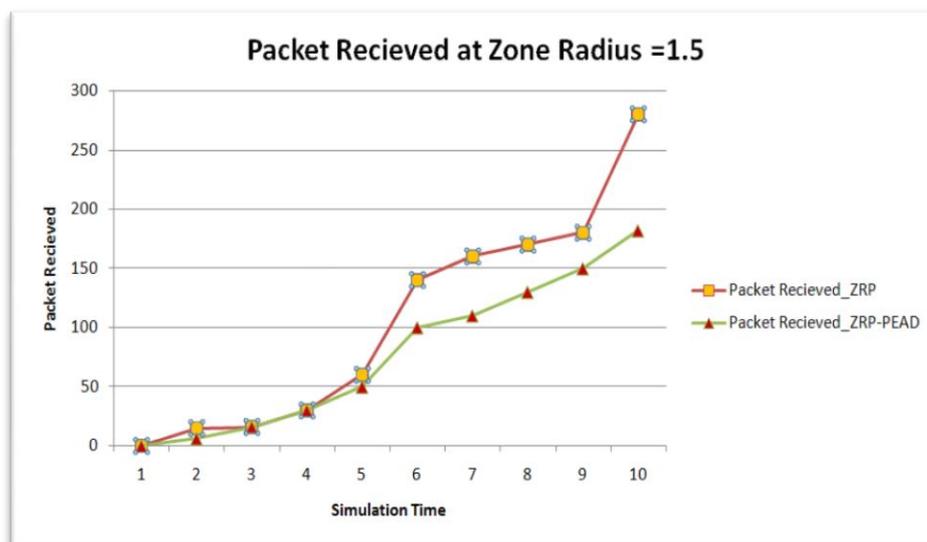


Fig 4.2 Comparison of Packet Recieved in ZRP and ZRP-PEAD ZR=1.5

V. CONCLUSION

The proposed protocol “Power Efficient Anomaly Detection Zone routing Protocol” introduces power awareness into Anomaly detection in wireless sensor network.

- This shows that the large amount of energy is saved by using the proposed algorithm which reduce the communication overhead of the sensor network.
- Proposed algorithm also shows that the number of packets received at sink is less in case of using new proposed algorithm as this using the anomaly detection which discards some of the packets having abnormal patterns.

So we conclude that after considering the different scenarios the ZRP-PEAD is energy efficient.

VI. FUTURE SCOPE

Future perspective of this research is to include the different zonal radius to check what effect it makes on the network life time. The concept of radius should also consider in case of packet received by nodes. At different zones radius, packets received at sink are affected or not should also check. More over here only the small number of nodes are considered. It would be is interesting to see the performance of ZRP in large network with many number of nodes and the performance comparison of ZRP with other protocols. Also in future, work can be done of other parameters like throughput, scalability and load balancing.

REFERENCES

- [1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci “A survey on sensor networks”, IEEE Communications Magazine, 40(8):102–114, August 2002.
- [2] Jennifer Yick, Biswanath Mukherjee and Dipak Ghosal “Wireless sensor network survey”, ELSEVIER 2008, pp 2292-2330.
- [3] Jalil Jabari Lotf, Seyed Hossein Hosseini, Nazhad Ghazani, “A Survey of Wireless Sensor Networks”, Australian Journal of Basic and Applied Sciences, 5(8): 1496-1503, 2011.
- [4] Wikipedia Free multi language on-line encyclopedia, Retrieve on 28th January 2013 from the World Wide Web
1. http://en.wikipedia.org/wiki/Sensor_node
2. http://en.wikipedia.org/wiki/Wireless_sensor_network
- [5] Yazeed Al-Obaisat, Robin Braun, "On Wireless Sensor Networks: Architectures, Protocols, Applications, and Management", Institute of Information and Communication Technologies, University of Technology, Sydney, 2007.
- [6] Raquel A. F. Mini, Antonio Alfredo Ferreira Loureiro, Badri Nath, "The distinctive design characteristic of a wireless sensor network: the energy map", ELSEVIER, Computer Communications 27(10): 935-945 (2004).

- [7] Daniele Puccinelli and Martin Haenggi, "Wireless Sensor Networks: Applications and Challenges of Ubiquitous Sensing", IEEE CIRCUITS AND SYSTEMS MAGAZINE-(2005).
- [8] Nandini. S. Patil, Prof. P. R. Patil and B.V. Bhoomaraddi, "Data Aggregation in Wireless Sensor Network", College of Engineering and Technology, Hubli, IEEE International Conference on Computational Intelligence and Computing Research (2010).
- [9] John A. Stankovic, "Research Challenges for Wireless Sensor Networks", Department of Computer Science, University of Virginia, ACM-DL (July 2004).
- [10] Chee-Yee Chong, Member, IEEE and Srikanta P. Kumar, Senior Member, IEEE, "Sensor Networks: Evolution, Opportunities, and Challenges", Proceedings of the IEEE, Aug 2003.
- [11] Zoran S. Bojkovic, Bojan M. Bakmaz and Miodrag R. Bakmaz, "Security Issues in Wireless Sensor Networks", International Journal of Communications (2008).
- [12] Yang Zhang, Nirvana Meratnia, and Paul Havinga, "Outlier Detection Techniques for Wireless Sensor Networks: A Survey", IEEE COMMUNICATIONS SURVEYS & TUTORIALS, 2010.
- [13] T. Arampatzis, J. Lygeros, and S. Manesis, "A Survey of Applications of Wireless Sensors and Wireless Sensor Networks," Proc. of the IEEE International Symposium on Intelligent Control, Mediterranean Conference on Control and Automation, pp. 719–724, Limassol, Cyprus, 2005.
- [14] Kiran Maraiya, Kamal Kant and Nitin Gupta, "Application based Study on Wireless Sensor Network", International Journal of Computer Applications (0975 – 8887) Volume 21– No.8, May 2011
- [15] Sutharshan Rajasegarar, Christopher Leckie, and Marimuthu Palaniswami, "Anomaly Detection In Wireless Sensor Networks", University Of Melbourne, Australia, IEEE Wireless Communications, August 2008
- [16] Varun Chandola, Arindam Banerjee, Vipin Kumar, "Anomaly detection: A survey", ACM Comput. Surv. 41(3) (2009)
- [17] Raja Jurdak, Rosalind Wang, Oliver Obst, Philip Valencia, "Wireless Sensor Network Anomalies: Diagnosis and Detection Strategies," Springer-Intelligence-Based System Engineering. Vol.10, No.1, pp. 309-325, 2011
- [18] Jinran Chen, Shubha Kher, and Arun Somani "Distributed fault detection of wireless sensor networks ," ACM Proceedings of the 2006
- [19] Nicklas Beijar, " Zone Routing Protocol (ZRP)", Networking laboratory, Helsinki University of Technology P.O. Box 3000, FIN-02015 HUT, Finland
- [20] Sree Ranga Raju and Dr. Jitendranath Mungara, "ZRP versus AODV and DSR: A Comprehensive Study on ZRP Performance", IJCA (0975-8887), Volume 1 – No. 12, 2010.
- [21] Kamal Beydoun, Violeta Felea, "Wireless Sensor Networks Routing over Zones", Telecommunications and Computer Networks, Croatia (2010)
- [22] Gourav Sahni and Sonia Sharma "Study of Various Anomalies and Anomaly Detection Methodologies in Wireless Sensor Network" International Journal of Advanced Research in Computer Science and Software Engineering Volume 3, Issue 5, May 2013
- [23] S. Rajasegarar, C. Leckie, M. Palaniswami, and J. C. Bezdek, "Distributed Anomaly Detection in Wireless Sensor Network," in IEEE International Conference on Communications Systems. (Singapore), October 2006
- [24] Nithya Ramanathan, Kevin K. Chang, Rahul Kapur, Lewis Girod, Eddie Kohler, Deborah Estrin, "Sympathy for the sensor network debugger", SenSys 2005: 255-267
- [25] Sutharshan Rajasegarar, Christopher Leckie, Marimuthu Palaniswami, James C. Bezdek, "Quarter Sphere Based Distributed Anomaly Detection in Wireless Sensor Networks", ICC 2007: 3864-386.