



## An Adaptive Energy Efficient Routing and Misbehavior Detection for Wireless Body Area Network

<sup>1</sup>P. Usha, <sup>2</sup>N. Priya

<sup>1</sup>Assistant Professor, <sup>2</sup>M.Phil Research Scholar,

<sup>1,2</sup>Department of Computer Science, Dr. N.G.P Arts and Science College,  
Coimbatore, Tamilnadu, India

**Abstract:** - This research work first investigates the current node placement routing strategy and their problems in wireless body area network. WBAN respond to network events such as energy, computational complexity, centralized operation and congestion in the same manner. This associated with Position aware BNC placement deteriorates the quality of an existing multi hop (k-hop) connection. The poor end to end link connection due to security in the network is invalid for that proposing Secure Position aware BNC routing protocol. SPBP operation range using static routing and long lived BNC flows and show the nodes around the sink always use up security earlier than other nodes. Then to address the problems we purpose to mitigate routing misbehaviour without affecting normal nodes too much when misbehaving nodes do not misreport. To detect the inconsistency caused by misreporting, for each contact record generated and received in a contact, a node selects random nodes as the witness nodes of this record, and transmits the summary of this record to them when it contacts BNC placement. Simulation is done by NS2 and the result improved for Throughput and packet delivery ratio.

**Key word:** - WBAN, BNC, NS2, SPBBP.

### I. INTRODUCTION

A Wireless Sensor Network (WSN) consists of spatially distributed autonomous sensors to cooperatively monitor physical or environmental conditions, such as temperature, sound, vibration, pressure, motion or pollutants. The development of wireless sensor networks was motivated by military applications such as battlefield surveillance. They are now used in many industrial and civilian application areas, including industrial process monitoring and control, machine health monitoring, environment and habitat monitoring, healthcare applications, home automation, and traffic control. One or more sensors, each node in a sensor network is typically equipped with a radio transceiver or other wireless communications device, a small microcontroller, and an energy source, usually a battery.

**Architecture of WSN:** A Wireless Sensor Network (WSN) provides a low-cost and multifunctional means to link communications and computer networks to the physical world. It consists of base stations and a number of wireless sensors. Each sensor is a unit with wireless networking capability that can collect and process data independently. Sensors are used to monitor activities of objects in a specific field and transmit the information to the base station.

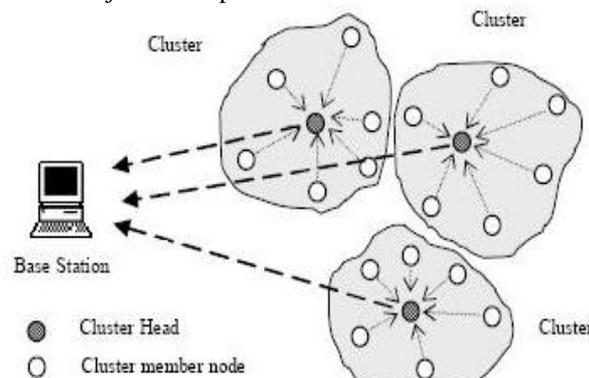


Figure 1.1 Architecture of WSN

### II. LITERATURE SURVEY

This paper [1] most important part of sensor network is deployment and connectivity of nodes where they work alone in un-attended environments. In most cases the WSNs contains hundreds of nodes that operate on small built-in batteries. Low power capacities of sensor node results in limited coverage and communication range for sensor nodes as compare to other mobile devices. In this paper [2], A sensor node stops working when it runs out of energy and thus a WSN may be structurally damaged if many sensors exhaust their onboard energy supply. Because of the limited energy storage capability of sensor nodes, Energy consumption is one of the most challenging aspects of these networks and different

strategies and protocols deals with this area. In power limited wireless network research, the main goal is to achieve minimum communication energy consumption [3]. WSNs consist of many nodes which are deployed closely to each other. A single node has many neighbouring nodes and every node can directly communicate with their neighbour nodes. Due to this, nodes will consume lot of energy. According to Cardei, M. and Wu, J. [4], the coverage of wireless sensor node can be estranged into three classes; area coverage (how to cover an area with the sensors), point coverage (coverage for a set of points of interest) and barrier coverage (decreasing the probability of undetected saturation is the main issue in barrier coverage). Most of the coverage problems in WSNs are due to the following three main reasons; not enough sensors to cover the whole region of interest, limited sensing range and random deployment [5].

### III. PROPOSED WORK

Energy aware routing, one of the most used performance assessor metrics is the Depletion Time, which is defined as the time until the first node (or a fixed percentage of nodes) of a network depletes its available energy. So, a network with a higher depletion time has a higher lifetime, which shows its energy efficiency. Here, we considered the death of the first node of a WBAN, as the depletion time, to evaluate the performance of our proposed algorithms. Commonly, the routing protocols, used in WBANs, can be classified (based on their data transmission manner) as multi hop routing protocol and cluster-based routing protocol. In order to depict the performance of our proposed algorithms, here considered recent, relevant, and available form of both of these routing protocols: PER and EAR-BAN, with security based routing. There are two types of nodes: misbehaving nodes and normal nodes. A misbehaving node drops the received packets even if it has available buffers but it does not drop its own packets. It may also drop the control messages of our detection scheme. A small number of misbehaving nodes may collude to avoid being detected, and they may synchronize their actions via out-band communication channels.

A normal node may drop packets when its buffer overflows, but it follows our protocol. Each packet has a certain lifetime, and then expired packets should be dropped whether or not there is buffer space. Such dropping can be identified if the expiration time of the packet is signed by the source. Such dropping is not misbehaviour, and will not be considered in the following Presentations our approach consists of a packet dropping detection scheme and a routing misbehaviour mitigation scheme.

The basic approach for misbehaviour detection of node is required to generate a contact record during each contact and report its previous contact records to the contacted node. Based on the reported contact records, the contacted node detects if the misbehaving node has dropped packets. The misbehaving node may misreport (i.e., report forged contact records) to hide its misbehaviour, but forged records cause inconsistencies which make misreporting detectable.

To detect misreporting, the contacted node also randomly selects a certain number of witness nodes for the reported records and sends a summary of each reported record to them when it contacts them. The witness node that collects two inconsistent contact records can detect the misreporting node. The approach for routing misbehaviour mitigation reduces the data traffic that flows into misbehaving nodes in two ways:

1) If a misbehaving node misreports, it will be blacklisted (after the misreporting is detected) and will not receive any packet from other nodes;

2) if it reports its contact records honestly, its dropping behaviour can be monitored by its contacted nodes, and it will receive much less packets from them. Two nodes contact, they generate a contact record which shows when this contact happens, which packets are in their buffers before data exchange, and what packets they send or receive during the data exchange. The record also includes the unique sequence number that each of them assigns for this contact. The record is signed by both nodes for integrity protection.

A node is required to carry the record of its previous contact, and report the record to its next contacted node, which will detect if it has dropped packets since the previous contact. Buffers Packet before the contact with node and it receives from in the contact. Such information is included in the contact record that reports to its next contacted node. From the record can deduce that should still buffer and at the current time. If has dropped after the contact with will detect the dropping when it exchanges the buffer state with A misbehaving node may report a false record to hide the dropping from being detected. Misreporting will result in inconsistent contact records generated by the misbehaving node.

### IV. SYSTEM ARCHITECTURE

This work starts from Network setup as nodes are connected & packets are sending through router. The router identifies the path & send the nodes to particular router and if the path is identified correctly receiver will send the request to the sender and contact record the ID, then SPBP technique will check the maximum or minimum cost of path access of an router. A SPBP technique report ,if any misbehaviour or attacks happen, then it make sure that the SPBP authenticate is corrector or not .If it is not again it send back the node to the particular router & it receiver the packet of a particular router.

#### Methodology

**User interface design:-**User interface design is to make the user's interaction as simple and efficient as possible, in terms of accomplishing user goals—what is often called user-centered design. Good user interface design facilitates finishing the task at hand without drawing unnecessary attention to it. Graphic design may be utilized to support its usability. The design process must balance technical functionality and visual elements to create a system that is not only operational but also usable and adaptable to changing user needs.

**Contact records:**-The two nodes also exchange their current vector of buffered packets. One node knows the two sets of packets the other node buffers at the beginning of the previous contact and the beginning of the current contact, which are denoted by  $\mathbf{b}_i$  and  $\mathbf{b}_j$ , respectively. It also knows the two sets of packets the other node sends and receives in the previous contact, which are denoted by  $\mathbf{r}_i$  and  $\mathbf{r}_j$  and a misbehaving node may drop a packet but keep the packet ID, pretending that it still buffers the packet.

The next contacted node may be a better relay for the dropped packet according to the routing protocol, which can be determined when the two exchange the destination included in packet ID of the buffered packets. The misbehaving node should forward the packet to the next contacted node, but it cannot since it has dropped the packet. Thus, the next contacted node can easily detect this misbehaviour and will not forward packets to this misbehaving node.

**Witness node:**

**Detection:** To detect the inconsistency caused by misreporting, for each contact record generated and received in a contact, a node selects random nodes as the witness nodes of this record, and transmits the summary of this record to them when it contacts them. It selects the witness nodes from the nodes that it has directly contacted. Here, the nodes contacted a long time ago are not used since they may have left the network.

**Alarm:** After detection, the witness node floods an alarm to all other nodes. The alarm includes the two inconsistent summaries. When a node receives this alarm, it verifies the inconsistency between the included summaries and the signature of the summaries. If the verification succeeds, this node adds the appropriate misreporting node into a blacklist and will not send any packets to it. If the verification fails, the alarm is discarded and will not be further propagated. A misreporting node will be kept in the blacklist for a certain time before being deleted.

A node deletes the record that it generates in a contact after the contact has been purged out of its report window, probably after a few contacts. It deletes the records received from the contacted node right after this contact, since these received records are only used to check if the contacted node has dropped packets recently. The witness node should keep its collected record summaries for a long enough time to detect misreporting. For simplicity, our scheme uses a time-to-live parameter, which denotes the time for the collected summaries to be stored before being deleted.

**Black list:**-To mitigate routing misbehaviour, we try to reduce the number of packets sent to the misbehaving nodes. If a node is detected to be misreporting, it should be blacklisted and should not receive packets from others. We cannot simply blacklist it because it is dropping packets, since a normal node may also drop packets due to buffer overflow.

Our basic idea is to maintain a metric forwarding probability (FP) for each node based on if the node has dropped, received and forwarded packets in recent contacts, which can be derived from its reported contact records. The nodes that frequently drop packets but seldom forward packets will have a small FP and will receive few packets from others. Our scheme borrows ideas from congestion control to update FP. More specifically, it combines additive increase, additive decrease, and multiplicative decrease to differentiate misbehaving nodes from normal nodes.

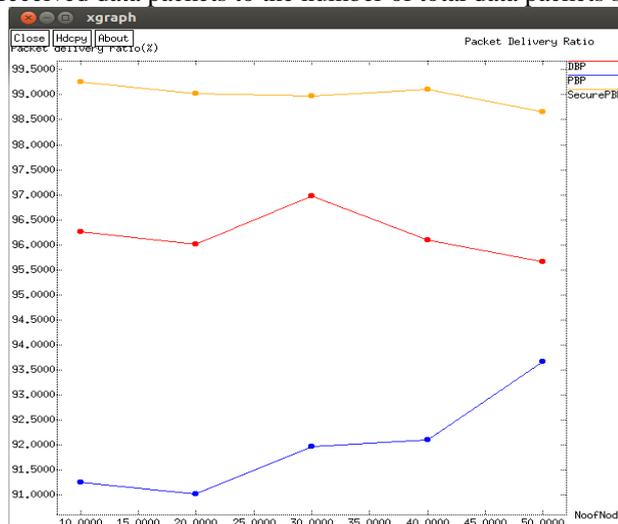
**Input configuration:**-The design phase is a multi-step process. It focuses on system creation with the help of user specifications and information gathered in phases. It is the phase the system requirements are translated to operational details. System has to be designed for various aspects of the input and output. Based upon edge calculation the nodes are placed. According to this proposed protocol we configure some input parameters some are simulation time, Mac protocol, radio type, number of nodes.

**V. RESULT AND ANALYSIS**

The proposed method addresses the congestion issues considering delay, packet loss and routing overhead. In order to evaluate the performance to measure the lifetime expectancy of a node, the below parameters are configured in the network simulator.

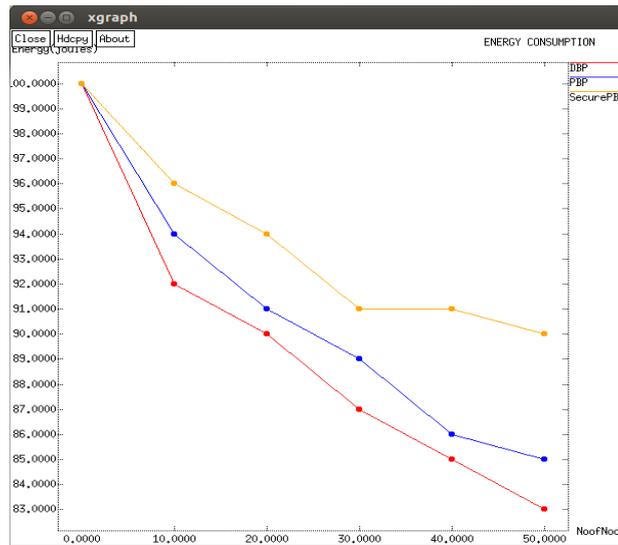
**A) PACKET ARRIVAL RATE:**

The ratio of the number of received data packets to the number of total data packets sent by the source.

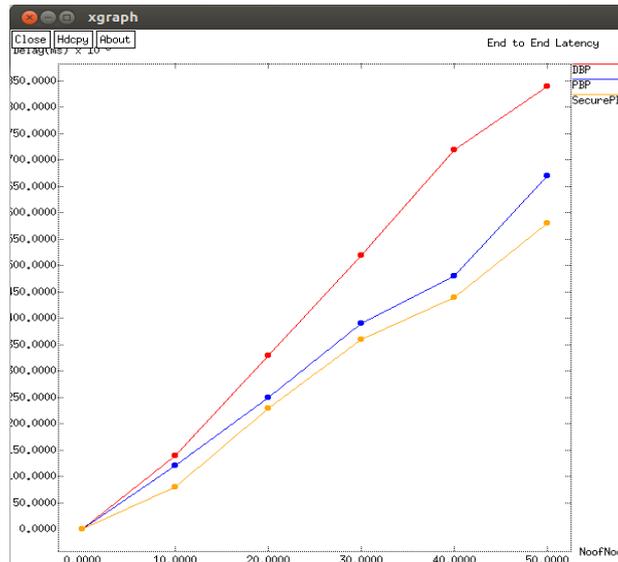


**B) ENERGY CONSUMPTION:**

The energy consumption for the entire network, including transmission energy consumption for both the data and control packets.

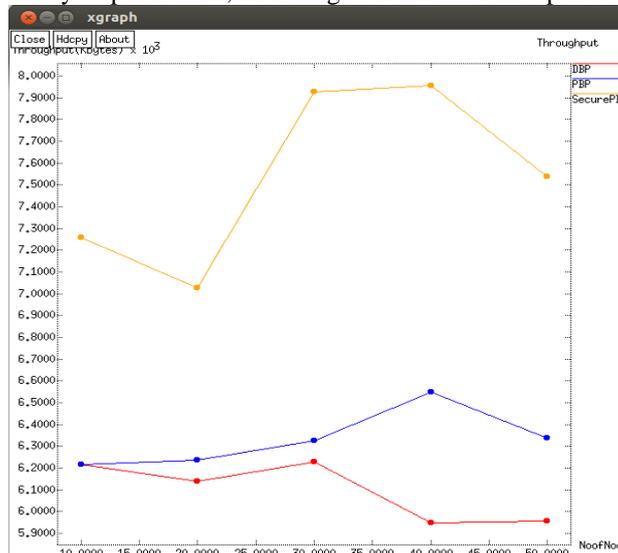


**C) AVERAGE END-TO-END DELAY:** The average time elapsed for delivering a data packet within a successful transmission



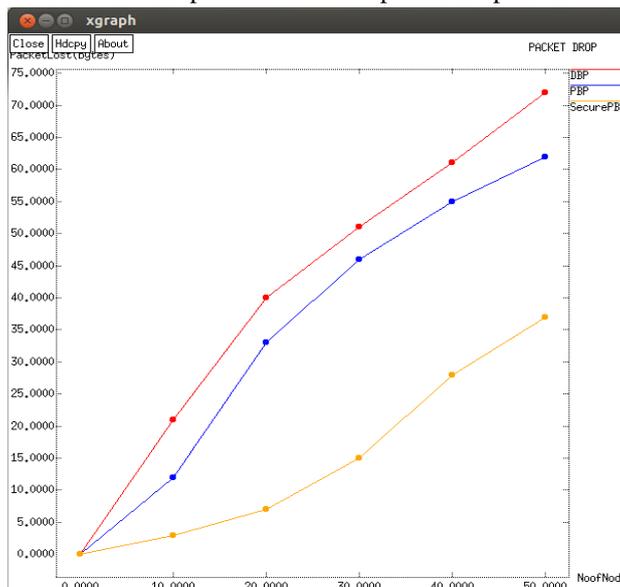
**D) THROUGHPUT:**

The average number of transmitted bytes per second, including both the total data packet received on time.



#### E) PACKET DROP:

The number of packet receive minus the number packet sent is the packet drop ratio.



### VI. CONCLUSION

Effective BNC placement within a WBAN to maximize the network longevity. Besides, to measure the lifetime expectancy of a node, which are different in their requirements, formations, and result in different level of energy efficient and computational performance, each BNC node detects packet dropping locally based on the collected information. Moreover, the detection scheme can effectively detect misreporting even when some nodes collude on detection probability and detection delays were also presented. Based on packet dropping detection scheme, mitigate routing misbehaviour in WBAN. The simulation result shows the consistency of PBP, over DBP-I&DBP-F, in term of energy efficient and computationally efficient performances.

### VII. FUTURE WORK

Proactive wake up: when a node detects a target, it broadcasts an alarm message to proactively awaken its neighbour nodes to prepare for the approaching target. To enhance energy efficiency, we modify this basic proactive wake-up method to sleep schedule nodes precisely. Select some of the neighbour nodes that are likely to detect the target to awaken. On receiving an alarm message, each candidate may individually make the decision on whether or not to be an Awakened node, and if yes, when and how long to wake up. We utilize two approaches to reduce the energy consumption during this proactive wake-up process: 1) Reduce the number of awakened nodes. 2) Schedule their sleep pattern to shorten the active time.

### REFERENCES

- [1] A. Roy and N. Sarma, "Energy Saving in MAC Layer of Wireless Sensor Networks: A Survey," National Workshop in Design and Analysis of Algorithm (NWDA), Tezpur University, Assam, 2010, pp. 961-994
- [2] M. Younis and K. Akkaya, "Strategies and Techniques for Node Placement in Wireless Sensor Networks: A Survey," *Ad Hoc Networks*, Vol. 6, No. 4, 2008, pp. 621-655. doi:10.1016/j.adhoc.2007.05.003
- [3] C. Suh, Y.-B. Ko, C.-H. Lee and H.-J. Kim "Numerical Analysis of the Idle Listening Problem in IEEE 802.15.4 Beacon-Enable Mode," 1st International Conference on Communications and Networking in China, Beijing, 25-27 October 2006, pp. 1-5.
- [4] M. Cardei and J. Wu, "Coverage in Wireless Sensor Networks," In: M. Ilyas and I. Mahgoub, *Handbook of Sensor Networks: Compact Wireless and Wired Sensing Systems*, CRC Press, Leiden, 2005.
- [5] N. A. Ab. Aziz, K. Ab. Aziz and W. Z. W. Ismail, "Coverage Strategies for Wireless Sensor Networks," *World Academy of Science, Engineering and Technology*, Vol. 50, 2009, pp. 145-150.
- [6] P. Santi, "Topology Control in Wireless Ad Hoc and Sensor Networks," John Wiley & Sons, Hoboken, 2005, pp. 27-95. doi:10.1002/0470094559.ch3
- [7] H. Karl and A. Willig, "Protocols and Architectures for Wireless Sensor Networks," John Wiley & Sons, Hoboken, 2005. doi:10.1002/0470095121
- [8] J. Beutel, K. Romer, M. Ringwald and M. Woehrle, "Deployment Techniques for Sensor Networks," *Signals and Communication Technology*, 2009, pp. 219-248. doi:10.1007/978-3-642-01341-6
- [9] G. N. Purohit and U. Sharma, "Topology Control for Energy Conservation in Wireless Sensor Network," *International Journal of Contemporary Mathematical Sciences*, Vol. 7, No. 5, 2012, pp. 227-239.
- [10] Md. Tanvir Ishtaique ul Huque, Kumudu S. Munasinghe and Abbas Jamalipour "Body Node Coordinator Placement Algorithms for Wireless Body Area Networks" VOL.2,NO.1, FEBRUARY 2015,pp.94-104.

**BIOGRAPHY**



**Mrs. P. Usha** working as a Assistant professor, Department of Computer Science, Dr N.G.P Arts and Science College, Coimbatore, Tamilnadu, India



**Miss. N. Priya** Pursuing M Phil Resource Scholar, Department of Computer Science, Dr N.G.P Arts and Science College, Coimbatore, Tamilnadu, India