RESEARCH ARTICLE OPEN ACCESS

PERFORMANCE ANALYSIS OF HYBRID MECHANISM TO IMPROVE RELIABILITY IN WIRELESS SENSOR NETWORK

[1]Ms. Ramya R, [2]Ms. Lavanya S.

[1]M.Phil Research Scholar, Department of Computer Science Auxilium College (Autonomous), Vellore, TamilNadu, India.
[2]Assisant Professor, HOD Department of Computer Science Auxilium College (Autonomous), Vellore, TamilNadu, India.

----------**********----------

Abstract:

A wireless sensor network (WSN) is becoming very popular technology. Wireless networking which is comprised on number of numerous sensors and they are interlinked or connected with each other for performing the same function collectively or cooperatively for the sake of checking and balancing the environmental factors. This type of networking is called as Wireless sensor networking. A wireless sensor network (WSN) consists of a group of self-organizing, lightweight sensor nodes that are used to cooperatively monitor physical or environmental conditions. Each sensor node in a WSN is equipped with a radio transmitter, several sensors, a battery unit and a microcontroller.Because of the size and cost constraints on sensor nodes, they are limited by energy, bandwidth, memory and other resources. Any protocol design for WSNs needs to consider the limitations of sensor nodes carefully. In UWSNs, turbulent conditions of the environments where the sensor nodes are deployed can cause the nodes to die. A contributing effort to explore the reliability issues in multimodal fusion sensor networks. We presented the system reliability for the case of two types of sensors and three types of sensors. WSNs hold the promise of many applications in the area of monitoring and control systems. Many properties of the environment can be observed by the monitoring system with the advent of cheap and tiny sensors. All these applications are meant for the specific purposes, and therefore maintaining data transport reliability is one of the major concern and the most important challenge. To address the reliability, we survey the various existing techniques; each of them has its own unique working to ensure the reliability. Some of the techniques use retransmission mechanism while others use redundant information for insuring the reliability.In the proposed process focus on the routing problem that affects the reliability of WSN. Hereby this problem can be overcome by implementing the Beacon vector routing protocol (BVR) in Hybrid Mechanism. By finding the alternative node in case of any node failure accrues. By this redundancy of information can be reduced and the loss of data can be avoided in Wireless Sensor Network.

Keywords — **wireless sensor network (WSN), UWSNs, lightweight sensor, Beacon vector routing protocol (BVR), Hybrid Mechanism.**

----------**********----------

I. INTRODUCTION

A wireless sensor network (WSN) is becoming very popular technology. Wireless networking which is comprised on number of numerous sensors and they are interlinked or connected with each other for performing the same function collectively or cooperatively for the sake of checking and balancing the environmental factors. This type of networking is called as Wireless sensor networking. A wireless sensor network (WSN) consists of a group of self-organizing, lightweight sensor nodes that are used to cooperatively monitor physical or environmental conditions. Commonly monitored parameters include temperature, sound, humidity, vibration, pressure and motion. Each sensor node in a WSN is equipped with a radio transmitter, several sensors, a battery unit and a microcontroller.

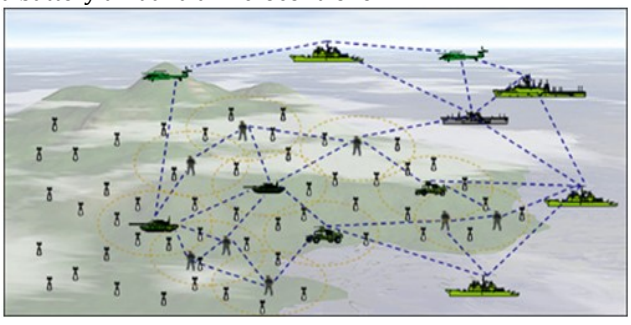

Fig. 1.1 Wireless Sensor Network

1.1 Motivation

The design of a data transport protocol in wireless sensor networks is focused on providing end-to-end reliability, mitigating congestion, and achieving fairness in bandwidth allocation. The reliability issue in the data transport protocol usually involves loss recovery, congestion control, or both.

- Full reliability (100% reliable data delivery) is provided unless there are unavoidable packet drops due to buffer overflow.
- A specified level of robustness can be provided.
- The protocol is robust to node failure and route changes.
- Fresh data has higher priority in the network and is able to be sent as soon as possible.

1.2 Reliability for Wireless Sensor Network

Packet loss in wireless sensor networks is usually due to the quality of the wireless channel, sensor failure, and congestion. Most of the applications need reliable transmission of each packet, and thus packet-level reliability is required. Almost every transport layer protocol for wireless sensor networks offers unidirectional reliable message delivery, but bidirectional reliability is also required in certain applications.

Reliability Levels:

Packet Reliability

Packet reliability refers to the successful delivery of all the packets to the destination. In case of packet reliability, it is required that all the packets from the sensor nodes reach the sink node that can results in wastage of sensors limited energy resources.

Event Reliability

Event reliability refers to the successful event detection. This requires the reliable transfer of event data from each sensing region in a sensor network.

1.3 Reliability Direction

Upstream Reliability

Upstream reliability refers to the communication between the sensor nodes and sink node, which is mostly unicast/converge cast transmission. All the protocols except PSFQ and GARUDA offer upstream reliability.

Downstream Reliability

Downstream reliability refers to the communication between the sink node and sensor nodes, since there is only a single sender (the sink); the data transmission usually uses broadcasting rather than unicasting. It provides successful delivery of control packets and queries from sink to sources. Only PSFQ and GARUDA offer downstream reliability.

1.4 Reliability

Reliability is the process of sending packets from source to destination without any loss of sensed data. Data or Packet which are sending to the appropriate destination can receives the packet successfully. Reliability is the way of knowing the quality of the data which are sent by the source node. Reliability is the important one in each and everything.

Reliability = the number of packets received by the Sink node / the number of packets sent to the sink node

II. RELATED WORK

1. End-To-End Reliability in Wireless Sensor Networks Survey and Research Challenges

- Wireless Sensor Networks (WSN) is highly distributed self-organized systems.
- Sensor nodes collect measurements of interest over given space, making them available to external systems and networks at special nodes designated sink nodes.
- Moving nodes and failing nodes due to battery power depletion are problems that raise a significant number of routing problems, demanding the use of efficient routing protocols.
- If the sensed information is to be used for active control (e.g. industrial process control) rather than passive monitoring, estimation and detection, the additional design goal of predictable latency appears.
- Many control strategies can compensate for information delay and jitter (delay variations), provided that these can be deterministically bounded or statistically quantified in the design phase.

Disadvantages:

- The whole challenge lies in cost-effective identification and maintenance of these redundant paths in the presence of nodes performing regular sleep periods with coarse time synchronization. Many building blocks are already present in the literature, but to our knowledge no protocol has been proposed that solves the whole problem.
- Although DTC was not developed as a solution to the congestion control problem, it relies on the TCP mechanisms.
- Moving nodes and failing nodes due to battery power depletion are problems that raise a significant number of routing problems, demanding the use of efficient routing protocols.

2. Reliable Transfer on Wireless Sensor Networks

- End-to-end retransmission which is used in Internet for reliable transport layer, does not work well in Wireless Sensor Networks.

- Information redundancy like retransmission, erasure code, and thick path are candidates.
- If loss is not randomly distributed, those methods do not work well. For example, when link fails, but routing table is not updated, all packets through that path will be dropped.
- Route fix, which tries alternative next hop after some failure, reduces correlated consecutive drops, so that information redundancy can perform well.
- Link-level retransmission is effective in most combination of options. Route fix is important to make the loss distribution less bursty.
- Especially elimination of long series of correlated consecutive drops makes erasure code very attractive solution.

Disadvantages

- It's easy for hackers to hack it as we can't control propagation of waves
- Comparatively low speed of communication
- Gets distracted by various elements like Blue-tooth Still Costly at large.

III. LINK-LEVEL RETRANSMISSION

According to the definition of discrete mobility pattern the sink changes its location from time to time. A routing protocol that transfers data towards such a sink should perform the following operations that are not needed for traditional WSNs:

1) Notify a node when it slink with the sink gets broken due to mobility.
2) Inform the whole net work of the topological changes incurred by mobility.
3) Minimize the packet loss during the sink moving period.

3.1 Problems in Network

Hop networks and thus must deal with much more complex collision patterns than in cellular type systems. Cellular type systems were based on hop systems. Achieving a dependable one hop transmission in wireless networks is not an easy mission due to the crashes caused by a singularity known as Hidden Terminal Problem.

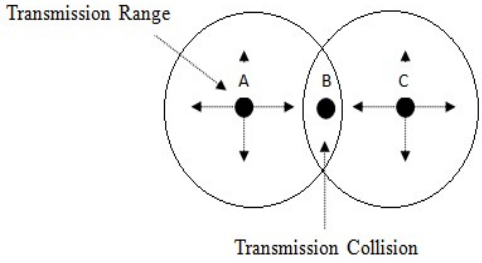

Fig. 3.1 Hidden Terminal Problem

The transmission range is the range, with respect to the transmitting station, within which a transmitted packet can be successfully received. [8]A typical hidden terminal situation is depicted in figure above. The hidden station problem may persist in networks even with the use of the RTS/CTS handshake.

3.2 Reliability in Network

Reliability = the number of packets received by the sink node / the number of packets sent to the sink node

Merits in Networks

- Power Saving due to smaller communication range
- Less number of smashes
- One-hop source routing, attempts to recover from path failures by routing indirectly through a small set of randomly chosen intermediaries.

Demerits in Network

- Reputation of packets, it is hard to complete in wireless networks due to the accidents caused by Hidden Terminal Problem.
- Too much of Packet loss in Hop Network
- Hop network will take long time to reach destination
- Collision occurs during packet transmission

3.3 User Datagram Protocol

On the other hand, when we talk about User Datagram Protocol (UDP), then it does not offer any flow control and congestion control mechanisms. In the case of congestions, UDP simply drops the packets without providing any scope for recovering these lost packets.

- There is no any flow control and congestion control mechanisms.
- Packets are dropped without providing any scope for recovering these lost packets.
- No ACK available in User Datagram Protocol.
- Reliability is lesser than TCP
- Too much of Packet Loss while using the User Datagram Protocol

IV. BEACON VECTOR ROUTING PROTOCOL

This method, called Beacon Vector Routing (BVR), assigns coordinates to nodes based on the vector of hop count distances to a small set of beacons, and then defines a distance metric on these coordinates. BVR routes packets greedily, forwarding to the next hop that is the closest (according to this beacon vector distance metric) to the destination. We evaluate this approach through a combination of high-level simulation to investigate scaling and design tradeoffs, and a prototype implementation over real test beds as a necessary reality check.

4.1 Distributed Hash Table

For some application is it needed to maintain a Distributed Hash Table(DHT). For example Ad-Hoc and sensor-nets needs this kind of structure. The DHT works as follows. Each object in the network has a key and the DHT supports the put and get operations.

4.2 Perimeter know their location

For this approach the paper describes a relaxation procedure for non-perimeter nodes to determine their virtual coordinates The procedure starts with the perimeter knowing their positions and the non-perimeter node starting with a default location, which can be the same or different. In the examples in the paper they use the same default location for all nodes at the beginning of this procedure.

$$x_i = \frac{\sum K \in neighbor_{set\_(i)} xk}{Size\_of(neighbor_{\_set(i)})}$$

$$y_i = \frac{\sum K \in neighbor_{set\_(i)} yk}{Size\_of(neighbor_{\_set(i)})}$$

4.3 Motivation for BVR

First generation sensor nets applications mainly focused on data collection. This limit the routing options using tree based to many-to-one or one-to-many. One-to-one routing is needed for the new applications for sensor nets. Actually no practical point-to-point implementation exists.

For a one-to-one routing protocol be successful some of the design requirements are that the algorithms should be scalable, robust, energy efficient and minimal algorithm complexity.

4.4 The BVR Algorithm

The BVR algorithm defines a set of coordinates and a distance function. The coordinates are defined as a vector of distances (hops count) to a set of beacon nodes. The algorithm uses a reverse path tree construction method to compute these distances.

ALGORITHM 1 BVR forwarding algorithm

BVR FORWARD (node *curr*, packet P)
// **first update packet header**
for (i = 1 to k) **do**
P:δ_i^{min} = min (P: δmin, δi(curr; P:*dst*))

// **try greedy forwarding first**
for (*i* = k to 1) **do**
next ←argmin$x \in NBR(curr)\{\delta_i(x, P{:}dst)\}$
If (δi(*next*; P:*dst*) < P:δ^{min}) **then**
unicast P to *next*

//**greedy failed, use fallback mode**
fallback bcn ←closest beacon to *P:dst*
if (*fallback bcn* != *curr*) **then**
unicast P to PARENT(*fallback bcn*)

//**fallback failed, do scoped flood**
broadcast P with scope P:*P*(*dst*)[*fallback bcn*]

The parameters are r, the total number of beacons, and k≤ r, the number of beacons that dene a destination's position. Forwarding a message starts with a greedy search for a neighbor that improves the minimum distance we have seen so far.

4.5 Beacon Maintenance

Sensor network nodes are prone to failure and we must provide a mechanism to maintain the set of beacons when they fail. We first note that the algorithm we described can function with fewer than r beacons, and even when there is inconsistency in the beacon sets nodes are aware of, by routing only based on the beacons they have in common. Thus, the beacon maintenance need not be perfect, it only needs to guide the system towards a state where there are r globally recognized beacons. We now sketch such an algorithm. For convenience, we describe the simplest algorithm we've used; we've also experimented with more advanced algorithms but describing them would take us too far afield

ALGORITHM 2 BVR beacon maintenance algorithm

BEACON ELECT MYSELF(r, B)
// **invoked periodically;** B **is the current set of beacons**
if (|B| > r) **then**

Set timer T = *log(myID)/ log(maxID(B))* * T_{max} + *jitter*

TIMER T EXPIRES(r, B)

if (|B| < r) **then**

Announce myself as a beacon

BEACON SUPPRESS MYSELF(r, B)

If (*my*ID $\in$ B)&(|B| > r)&(*my*ID >r^{th} guested(B))

Then

Stop announcing myself as a beacon

4.6 The Distance Function

The distance function defined by this algorithm takes two arguments, a node p and a particular destination d. This metric measures how good node p would be as the next hop to reach node d. The metric favor neighbors whose coordinates are more similar to the destination,

and always moves toward beacons if the beacons are closer to the destination. The metric is the following:

$$\delta^{+}_{k}(p,d) = \sum_{i \epsilon Ck(d)} max(p_i - d_i, 0)$$

$$\delta^{-}_{k}(p,d) = \sum_{i \epsilon Ck(d)} max(d_i - p_i, 0)$$

Here C_k (d) is the set of k closest beacons to d. δ_k+ is the sum of the differences for the beacons that are closer to the destination d than to the current routing node p, while δ_k- measures the sum of the distances to the farthest beacons. The algorithms chooses the next hop that minimizes δ+k and if there is a tie then is broken by minimizing δ^{-}_{k}. Actually what they do is to implement $\delta_k = A\delta^{+}_{k} + \delta^{-}_{k}$ for some large constant A.

4.7 BVR Implementation (key issues)

When implementing the algorithms in real nodes, they indentified four key issues that must be addressed: Link estimation, link/neighbor selection, distance estimation and route selection. They come up with the following conclusions for each of these issues. For Link estimation they noticed that the nodes always selects a high quality neighbor, for Routing performance the found out success rate about 97% when the network load is low. In terms of Dynamics BVR sustains high performance under high node failure rate and in Coordinate Stability they noticed this one varies little in magnitude and over time. In other words changes to the overall topology are minimum. The next section gives a high level description of the last paper for this topic, the GLIDER approach.

V. PERFORMANCE EVALUATIONS AND ANALYSIS

5.1 An Introduction to Cygwin

Cygwin is free software that provides a Unix-like environment and software tool set to users of any modern x86 32-bit and 64-bit versions of MS-Windows (XP with SP3/Server 20xx/Vista/7/8) and (using older versions of Cygwin) some obsolete versions (95/98/ME/NT/2000/XP without SP3) as well. Cygwin consists of a Unix system call emulation library, cygwin1.dll. With Cygwin installed, users have access to many standard UNIX utilities. They can be used from one of the provided shells such as bash or from the Windows Command Prompt.

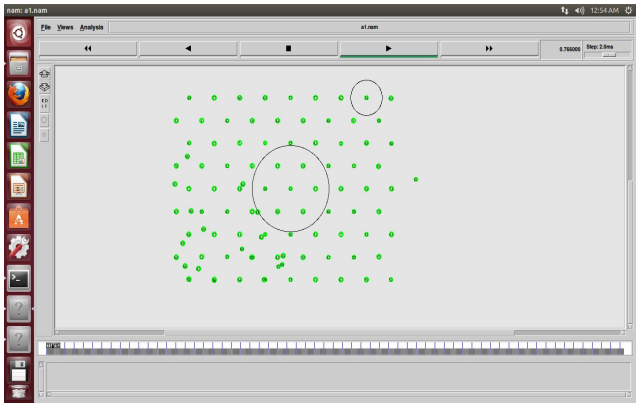

Fig 5.1 : NAM Creation for WSN

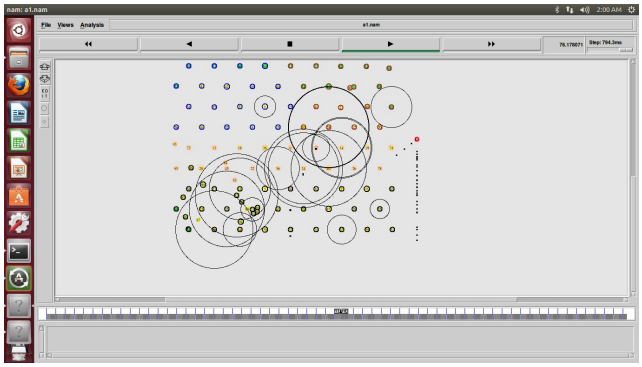

Fig 5.2: Collision Identification

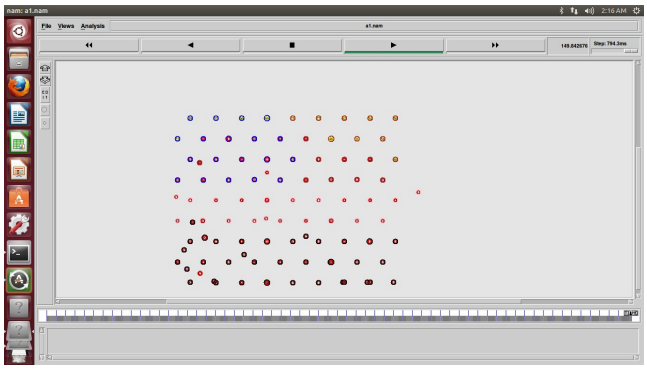

Figure 5.3 Multi Hop reliability Model

VI. PERFORMANCE EVALUATION

Following Graph will prove that Three-Hops Selection will provide the better performance comparing to the One and Two-Hop models. With the Help of the NS-2 Simulator tool to prove the Metrics like.

- Packet Delivery Ratio
- Packet Drop
- Throughput

6.1 Packet Delivery Ratio

Many protocols in wireless sensor networks use packet delivery ratio (PDR) as a metric to select the best route, transmission rate or power. PDR is normally

estimated either by counting the number of received hello/data messages in a small period of time, i.e., less than 1 second, or by taking the history of PDR into account.

A Sensor Network consists of multiple detection stations called sensor nodes, each of which is small, lightweight and portable. Every sensor node is equipped with a transducer, microcomputer, transceiver and power source.

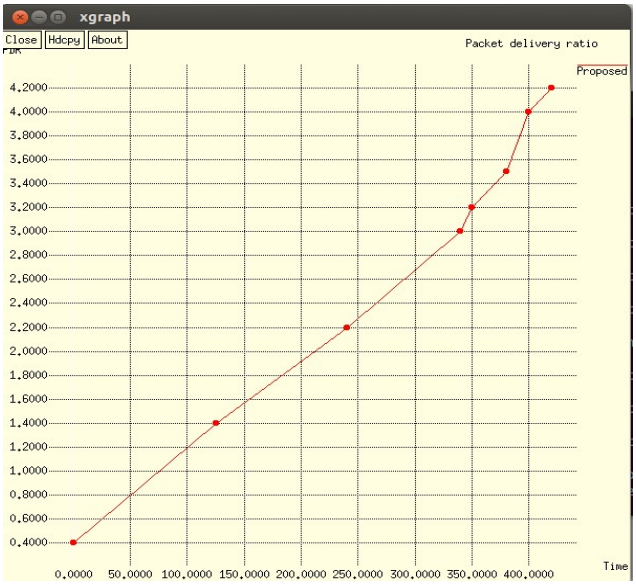

Fig 6.1: Packet Delivery Ratio

6.2 Packet Drop

A Wireless Sensor Network (WSN) is a collection of nodes organized into a cooperative network. Each node consists of processing capability which acts as transceiver. Packet dropping is a compromised node which drops all or some of the packets that is supposed to forward. Packet modification is a compromised node which modifies all or some of the packets that is supposed to forward. Packet dropping and modification are common attacks that can be launched by an adversary to disrupt communication in Wireless Sensor Network

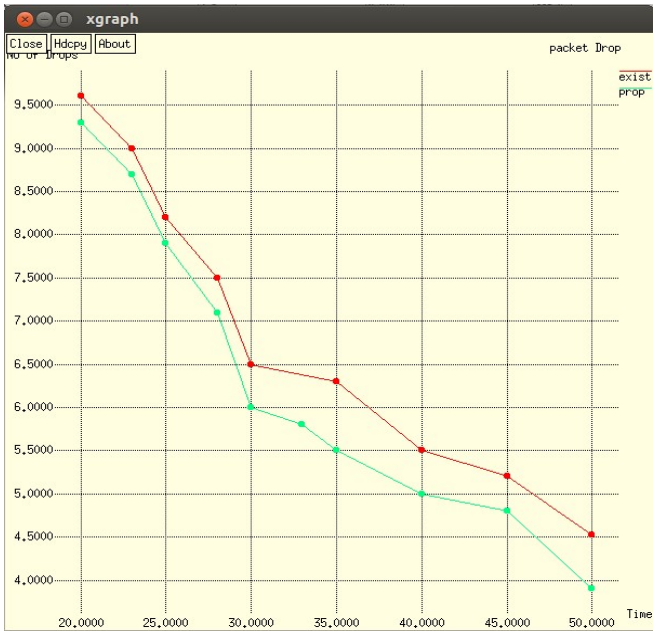

Fig 6.2: Packet Drop

6.3 Throughput

Most of studies only consider that wireless sensor networks are equipped with only Omni-directional antennas, which can cause high collisions. It is shown that the per node throughput in such networks is decreased with the increased number of nodes. Thus, the transmission with multiple short - range hops is preferred to reduce the interference. However, other studies show that the transmission delay increases with the increased number of hops. Found that using directional antennas not only can increase the throughput capacity but also can decrease the delay by reducing the number of hops.

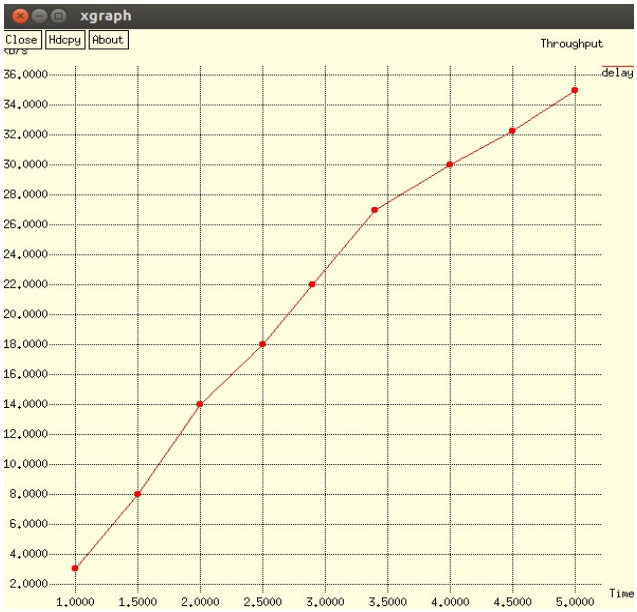

Fig 6.3: Throughput

CONCLUSION

In UWSNs, turbulent conditions of the environments where the sensor nodes are deployed can cause the nodes to die. A contributing effort to explore the reliability issues in multimodal fusion sensor networks. We presented the system reliability for the case of two types of sensors and three types of sensors. WSNs hold the promise of many applications in the area of monitoring and control systems. Many properties of the environment can be observed by the monitoring system with the advent of cheap and tiny sensors. All these applications are meant for the specific purposes, and therefore maintaining data transport reliability is one of the major concern and the most important challenge. To address the reliability, we survey the various existing techniques; each of them has its own unique working to ensure the reliability. Some of the techniques use retransmission mechanism while others use redundant information for insuring the reliability. Few of the above objectives may be considered in the future by the researchers.

These objectives may be achieved as under:

- By developing a Markov based model with additional mobile sensors to replace the faulty sensors in case failure occurs.
- By developing the efficient mechanism for clustering the sensor nodes in heterogeneous WSNs to minimize the number of additional sensors required during the deployment based on artificial neural network models.
- By developing a model for reliable and quick packet delivery in WSNs to enhance the performance of the network using appropriate application dependent communication schemes.
- By developing a model for reliable and fault tolerant transmission by introducing biologically inspired sensor nodes which can be trained to memorize the possible events to be observed by the network.
- The proposed model will overcome the problems coming from limited memory and error prone wireless communication medium as the network can recall the lost memory (information of interest) from the biologically inspired sensor nodes based on chain of mental (already memorized system) associations despite of the corrupted signal sensed at the destination.

FUTURE WORK:

Generally, for networks that are multi-hop, hop-by-hop is thought to be superior in regards to reliability. On the other hand, sensor nodes in UWSNs are more likely to die because of energy loss which causes a tremendous number of packets to be lost. Our conclusions have been clarified and supported by simulation results that were achieved using a variety of parameters.

REFERENCES:

1. M. Maroti, \Directed ood-routing framework for wireless sensor net- works," in Proceedings of the 5th ACM/IFIP/USENIX International Conference on Middleware (Middleware), Toronto, Canada, pp. 99{114, 18-22 October 2004.
2. L. Rizzo, \E_ective erasure codes for reliable computer communication protocols," ACM Computer Communication Review, vol. 27, no. 02, pp. 24 { 36, 1997.
3. J. Postel, \Transmission Control Protocol," IETF RFC 793, September 1981.
4. S.-J. Park, R. Sivakumar, I. Akyildiz and R. Vedantham, \GARUDA: Achieving e ective reliability for downstream communication in wireless sensor networks," IEEE Transactions on Mobile Computing, vol. 07, no. 02, pp. 214 {230, 2008.
5. G. Clark, Error-Correction Coding for Digital Communications, Plenum Press, 1981.
6. H. Wen, C. Lin, F. Ren, Y. Yue and X. Huang, \Retransmission or Redundancy: transmission reliability in wireless sensor networks," in IEEE 4th International Conference on Mobile Adhoc and Sensor Systems (MASS), Pisa, Italy, pp. 1 { 7, 08-11 October 2007.
7. J. C. Bolot, \End-to-end packet delay and loss behavior in the internet," in Proceedings of the ACM SIGCOMM Conference on Communications Architectures, Protocols and Applications (SIGCOMM), San Francisco, California, USA, pp. 289{298, 13-17 September 2005.
8. S. Ali, A. Fakoorian and H. Taheri, \Optimum Reed-Solomon erasure coding in fault tolerant sensor networks," in Proceedings of the 4th International Symposium on Wireless Communication Systems (ISWCS), Trondheim, Norway, pp. 6{10, 16-19 October 2007.
9. B. Marchi, A. Grilo and M. Nunes, \DTSN: Distributed transport for sensor networks," in Proceedings of the 12th IEEE Symposium on Computers and Communications (ISCC), Aveiro, Portugal, pp. 165{172, 01-04 July 2007.
10. T. Le, W. Hu, P. Corke and S. Jha, \ERTP: Energy-efficient and reli- able transport protocol for data streaming in wireless sensor networks," Computer Communications, vol. 32, no. 7-10, pp. 1154 { 1171, 2009.
11. F. Shaikh, A. Khelil, A. Ali and V. Suri, \Trccit: Tunable reliability with congestion control for information transport in wireless sensor networks," in 5th Annual International ICST Wireless Internet Conference (WICON), Singapore, pp. 1 9, 01-03 March 2010.

12. H. Zhou, X. Guan and C. Wu, \RTMC: Reliable transport with memory consideration in wireless sensor networks," in IEEE International Conference on Communications (ICC), Beijing, China, pp. 2819 2824, 19-23 May 2008.

BIOGRAPHIES

Ms. Lavanya S. M.Sc., M.Phil., (Ph.D)., Asst. Prof HOD I/C Department of Computer Science Auxilium College (Autonomous), Vellore, TamilNadu, India.

Ms. Ramya R., M.Phil Research Scholar, Department of Computer Science Auxilium College (Autonomous), Vellore, TamilNadu, India.