Optimizing the Beacon Exchange Rate for Proactive Autonomic Configuration in Ubiquitous MANETs

#Mr. M. M. Iqbal, Dr. I. Gondal, Prof. L. Dooley
GSCIT, Faculty of IT, MONASH University, Churchill, 3842 Australia
[#Mudasser.Iqbal, Iqbal.Gondal, Laurence.Dooley]@infotech.monash.edu.au

***Abstract*- Proactive self-configuration is indispensable for MANETs like Ubiquitous Sensor Networks (USNs), as component devices of the network are usually exposed to natural or man-made disasters due to the hostile deployment and ad hoc nature of the USNs. *Network State Beacons (NSBs)* are exchanged among the key nodes of the network for crucial and effective monitoring of the network for steady state operation. The *Rate of Beacon Exchange (F_E)* and its *contents*, define the time and nature of the proactive action. Therefore it is very important to optimize these parameters to tune the functional response of the USN. This paper presents a comprehensive model for monitoring and proactively reconfiguring the network by optimizing the F_E. The results confirm the improved throughput while maintaining QoS over longer periods of network operation.**

***Keywords*- Ad-hoc Wireless Sensor Networks, Proactive Self Configuration, Optimization, Quality of Service**

I. INTRODUCTION

Ubiquitous Sensor Network (USN) is a special type of MANETs, comprising mostly of low cost Pervasive Sensor (PS) nodes with low computation, communication, storage and energy resources. Examples of such devices include Smart Dust, Corner-Cube Retroflector and Motes [1]. Networks comprising hundreds of such nodes are deployed to accomplish highly sophisticated and critical biological, chemical and physical sensing tasks [15]. The critical demands of the ubiquitous network based applications are fault tolerance, longer life, maximum throughput and self configuration etc. Also, optimized energy consumption and bandwidth conservation is crucial for QoS in ubiquitous computing.

In order to satisfy these operational requirements, intermediate nodes, called parent nodes, with relatively high resources are used. A Parent Node (PN) is responsible for various tasks including in-network data processing, communication delay minimization and routing the PS nodes data to the Central Commanding Infrastructure (CCI). These building blocks of a USN, the PNs, may fail because of many unprecedented local or non-local factors. In order to maintain the QoS of a USN, (which in our case is defined as the lossless information delivery,) the PNs can be added or removed from the infrastructure on the fly. Also the unattended nature of USNs demands it to be self monitoring and able to take proactive actions to mitigate the malfunctions before they actually occur.

Proactive network monitoring and reconfiguration requires maintaining the network state across the PNs at optimized instants, with sufficient information for the decision to be taken to mitigate the prospective anomaly. This state is maintained through periodic exchange of Network State Beacons (NSBs) at a particular Beacon Exchange Rate (F_E). The contents of NSBs, the value of F_E and the way it is propagated in the network are three important factors that define the extra load that the network has to bear for supporting the reconfiguration activities. Also these factors define the time and the nature of proactive action. Accurate and timely network state information would result in an effective and successful proactive action to mitigate the network impairment. Therefore it is highly important to optimize these factors to maximize throughput and minimize the risk of information loss due to node failures.

Earlier works on the self configuration protocols [11] lack a careful investigation of beacon exchange rate for maintaining network state for supporting QoS for longer term. However, Gupta [2] and Chiasserini [3] have focused on energy-efficient, hierarchical modeling of the sensor network through dynamic configuration of the tree nodes. The success of their dynamic tree models is based on a virtually inappropriate assumption for sensor networks, that a sensor node is capable of connecting to many parent nodes simultaneously. Some researchers like Cerpa [13] emphasized the need for a high degree of synchronization between network components in order to reconfigure correctly. Policy based self managing systems were also considered, but these impose a high computational and storage requirement on the individual sensing units. Extending an already existing network was discussed by Bulusu [7],[9], but this lacked a suitable strategy for self configuration.

Communication models for load balancing were analyzed by Narayanan [4], while energy conservation issues were examined by Jean [5] and Rabaey [6] through tuning the communication ranges of nodes and defining a parameterized physical layer. Their work highlighted the network design issues but did not cover proactive network configuration through optimizing beacon exchange.

This paper describes a proactive fault tolerant and configuration model to deal with the network impairments and also presents optimized bounds for the selection of F_E. The overall objective of the model is to provide the best achievable QoS throughout the network life span.

In the remainder of the paper, Section II describes the underlying USN design and self configuration model, while Section III details F_E optimization aspects. Simulation results highlighting the QoS maintainability and reliability of configuration model for various choices of F_E are presented in Section IV with some conclusions presented in Section V.

#Corresponding Author

0-7803-9019-9/05/$20.00 ©2005 IEEE.

II. Sensor Network Design & Self Configuration Model

A. Network Design

Sensor network design is based on the optimal selection of density and locations of Parent Nodes (PNs) in a virtual hexagonal topology as detailed in our earlier work [10]. The design is optimized to achieve the best QoS by; ensuring the availability of PN to a maximum number of PS nodes, minimizing GR areas (to reduce many-hop routing) and minimizing confusion / conflict zones. The network is arranged as a series of decentralized federations, each headed by a PN. A federation, as shown in Fig. 1, defines critical network characteristics in terms of PN availability areas, where PS nodes have direct connection to a PN, routing areas where an intermediate routing PS node is required due to lack of PN availability and confusion zones where the presence of more than one PNs confuse a PS node for selection between the PNs [10]. As the federation establishes its control over the area in a localized manner, this setup is scaled up to the some major natural disaster sites in Australia.

B. Self Configuration Core Protocol

The proposed network design defines the initial configuration of the sensor network for best QoS with the communication and connectivity model for the PN and PS nodes described in Table I. During active network operation, the model can deal abnormalities including: a) increased traffic load leading to congestion and packet losses causing loss of information, b) decreased energy resources raising the threat of PN failure, c) sudden failure of a PN due to local or non-local disasters and d) addition of new PNs among others.

To address these various scenarios, a *Self-Configuration Protocol* is employed as described by Iqbal et al [11]. The key element of the protocol is continual geographically localized monitoring of the network state and then taking proactive measures to mitigate operational impairments. The following paragraphs describe both the data structure and functions of this protocol.

Data Structure: For continual network monitoring, each federation manages a *Federation Beacon* (FB) shown in Table II. These parameters are locally computed by each federation. In addition, each PS node manages a *PS Beacon* (PSB) shown in Table III, which is used to track parent connectivity and communication sessions.

Network State Management: In order to monitor the network for impairments and malfunctions, it is crucial to maintain the state of the network in some fashion. This state can be managed in both distributed and centralized manner. For this purpose, federation beacons, that we call Network State Beacons (NSBs), are exchanged amongst the PNs throughout the network with periodicity F_E. Section III describes the possibilities and issues in the selection and implementation of F_E, its criticality and its impacts on the overall network performance.

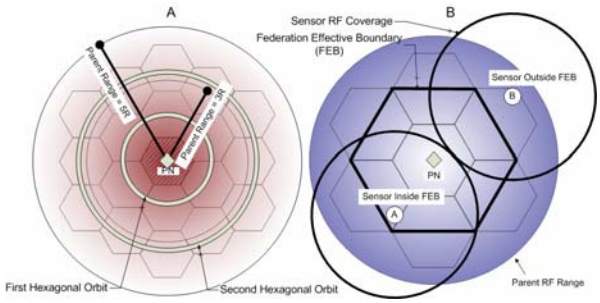

Fig. 1. A: Coverage of a PN in the form of Hexagonal Orbits
B: Federation Structure

TABLE I
PN-PS Communication and Connectivity Model

Communication:

a. All communication between PN and PS nodes is in the form of sessions.
b. Each data transmission activity is given a Session ID (SID).
c. A PN and PS node perform handshaking prior to initiating a data transmission session.
d. Sessions serve two purposes; a) while a session is established there is no need for handshaking except one at the beginning. Also PS nodes implicitly assume the availability of PN, b) the amount of data transmitted can be tracked using check points placed after the termination of each session confirming the data up to the checkpoint has been successfully transmitted.
e. In case of a PS node *Idle* state, PN terminates the session *by force*.

Connectivity:

a. Each PS node broadcasts a PN Availability Request (PNAReq) before establishing a session
b. All PNs that receive the request respond with the PNRep-CID reply where CID is the carrier region ID of the PN.
c. PS nodes upon receiving the replies save the CID coordinates in a ranked order of Euclidian distance from each PN. Communication always commences with the closest PN (first on the list).

The exchange of FBs between neighboring PNs defines the local state of the network at each federation in terms of network load (AL), remaining energy (EL), remaining life of the PN (ETL) and the PN availability. PN availability is inferred from the receipt of FB, so if no FB is received from an adjacent PN within a designated wait window (T_W), the PN is declared to have failed.

PN Failure: If a PN fails, the clients go out of coverage temporarily and are called *Interrupted*. In this case the network is reconfigured in such a way that minimum PS nodes are affected and communication seamlessly continues with minimal interruption. We have investigated two solutions to handle a failed PN based on the cardinality of federations (F_n) and that of the sensors.

In the first solution, the interrupted PS nodes attempt to regain connectivity. If F_n is high enough then most PS nodes can connect to more than one PN at a time. In this case, the descriptor PSD has more than one PN entries against PN-ID attribute. When the PS has waited for time T_W, it tries to

TABLE II
Federation Beacon

Attribute	Value
ID	[x,y]
Neighbor Federations	[x1,y1], [x2,y2],…[xn,yn]
Communication Range	No. of Hex Regions covered
Connected Clients	[x1,y1], [x2,y2],…[xn,yn]
Current Load	Client Requests per Second (RPS)
Average Load (AL)	RPS averaged every 1000 mSec
Energy Level (EL)	Remaining Power Level
Average Energy Degradation (AED)	EL averaged every 1000 mSec
Estimated Time to Live (ETL)	(EL / AED) Seconds
Client Sessions	Client# [Session ID, Check Point]

TABLE III
PS BEACON

Attribute	Value
ID	[x,y]
PN-IDs	[x1,y1], [x2,y2],…[xn,yn]
Current PN-ID	Current PN out of a number of in-range PNs
Session ID	SID of current transmission
Check Point	Last known successful transmission
Buffer	All data after the Check Point which is not yet confirmed by the PN
Associate Parent Node (APN)	ID of a PS node working as router for data forwarding in the absence of a PN
Wait Time	T_W: Time to wait for an acknowledgement from PN regarding data reception

connect to the next available PN. If none of the PNs accepts the connection request, the PS node hangs until the network arranges some other means of connectivity.

In the other solution, the network takes steps to approach the interrupted PS nodes as soon as the failure is detected, in order to keep the connectivity of the nodes in the interrupted federation until the failed PN is replaced. The approach is to assume that PNs are stationary and so a mobile PS node or a PS node close to the failed node is assigned the role of routing the data from the interrupted PS nodes to the nearest PN. The complete solution is given in Table IV.

Proactive Detection of Malfunctions: Since the network is monitored in a localized manner by each PN, it is entirely reasonable that predictable malfunctions, such as overloaded PNs and those running down in power resources, can be detected early and proactive measures can be taken to prevent sudden disconnection of PS nodes from the network. This is done in a localized manner by each federation that keeps monitoring crucial FD parameters such as time to live (ETL) and load (AL) of neighbors. If these parameters approach a threshold, then it can be easily inferred the PN will not be able to complete all its tasks. Having detected the prospective malfunction, an appropriate action depending upon the USN model is taken, as detailed in our earlier work [11].

III. BEACON EXCHANGE RATE (BER[1])

We have investigated the impacts of randomly selecting an F_E on the network performance and state management. The following subsections give a detailed insight into the philosophy, implementation techniques, numerical methods for optimizing the F_E and the network factors that must be taken into consideration. The impacts of different values of F_E on proactive mitigation of prospective node failures are discussed with the simulations in Section IV.

A. Random Rate (F_E)

Beacon exchange rate is kept random in the model. The reason for investigating random rate is to find out the core effects of employing NSB exchange on self configuration in general and proactivity in particular.

B. Implementation Method

In the above configuration, NSBs are exchanged by the neighboring PNs in the whole network with randomly selected intervals during the entire course of

1: BER and F_E are used interchangeably in the text

TABLE IV
PARENT FAILURE SOLUTION FOR STATIONARY PNS

a. Find the PN closest to failed PN. This is the first PN that detects the failure of a neighboring PN and is called *Closest PN* (CPN). This will provide an alternative connection to the interrupted federation.
b. IF: life (ETL) of CPN >= the mean life of its neighbors THEN CPN proceeds to reconfigure the network; ELSE: it does not play any reconfiguration role. The mean life of neighbors is known through the respective FDs.
c. IF: CPN permits a connection, it searches for the PS node that is nearest to the failed PN and is served by the CPN, by calculating the respective Euclidian distances of all candidate PS nodes. The closest PS node is called the *Associate Parent Node* (APN).
d. APN then broadcasts its availability and all interrupted PS nodes then connect to this APN.
e. IF: some interrupted PS nodes are unable to connect to an APN. THEN, upon receiving the APN call for connectivity, each PS node broadcasts a message volunteering itself as an intermediate router between *far-off* interrupted PS nodes and the APN. The volunteering broadcast is sent after a sufficient delay that is proportional to the communication ranges of the PS nodes. The larger the range, the longer the delay.

network operation. This NSB exchange strategy requires the propagation of the global-exchange-interval throughout the network of PNs so that each PN can synchronize its NSB transmission and reception cycles with the neighbors. There are four possible ways of propagating F_E to each PN as discussed below.

a. Pre-Programmed: Each PN is programmed with a global F_E before it is put into operation in the network. Though simple, this option works like a hard-coded solution, and therefore is not suitable for USNs which are inherently dynamic in nature and, therefore, their operational requirements vary dynamically too. Also the requirement of programming each PN before deploying into the network limits the types of parents useable in the network and also the efficiency of network deployment.

b. Direct: Under the assumption that each PN is capable of connecting to the CCI by integrating with other communications networks like GPRS, the CCI governs the distribution of F_E to each PN as shown in Fig. 2A. Each PN receives the information regarding the F_E directly from the CCI. The central command also manages policy based synchronization of NSBs' transmission and reception among neighboring PNs.

c. Routing: Option 'b' takes care of the networks that are not connected, i.e. there does not exist a route from every PN to every other PN. For connected networks, it is possible to get rid of a *far-off* central command (like CCI) for maintaining network state, thereby minimizing the dependency of the network on other communications infrastructures and also conserving the overall energy

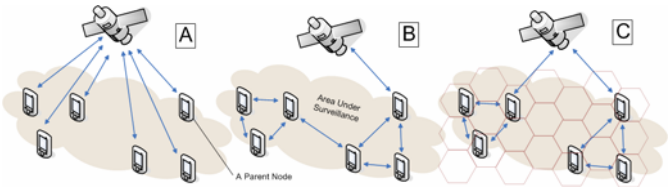

Fig. 2. A: Each PN connects to CCI though GPRS for exchanging F_E
B: For connected networks, in-network routing (GEAR) is employed for F_E propagation with one PN acting as gateway to external world
C: Partially connected networks employ Hybrid interconnectivity

resources. This is achieved by declaring one of the PNs in the network as the head-node. This head-node also works as a gateway of the PN network to external world. The head PN takes one time input from the CCI or is pre-programmed with the initial F_E. This F_E information is routed throughout the network by adopting one of geography-based adhoc routing strategies. For this purpose, GEAR [12] protocol is employed which is a recursive data dissemination protocol for wireless sensor networks. GEAR is selected for F_E propagation because of its proven performance for highly dense wireless sensor networks, while consuming minimum energy. This configuration is illustrated in Fig. 2B.

d. Hybrid: Fig. 2C describes the situation when the network is partially connected and a hybrid approach is adopted by combining options b and c above for interconnectivity of PNs. In this case, the core methodology employed is similar to cluster-based adhoc networks [3]. This technique makes clusters of nodes in the network with each cluster headed by one of the PNs in the cluster. The role of cluster head is randomly rotated among all the nodes in the cluster to ensure that the network energy resources drain evenly thereby protecting the network from experiencing non-uniform impairments. To assign nodes to the cluster heads in an energy efficient way, the usual minimum transmission power criterion is not employed because of its excessive communication and processing overheads. Instead, the node assignment is optimized to maximize the lifetime of entire network [3] given by:

$$L_s = \sum_{i \in S_c} L_i \tag{1}$$

where:

L_s: Network life time defined as the time period from the instant when the network starts functioning to the instant at which all the cluster-heads run out of energy.

S_c: Set of cluster heads

L_i: Life time of a single cluster head, defined by

$$L_i = \frac{E_i}{\alpha c_i + f(n_i)} \tag{2}$$

where E_i is the initial amount of energy available at cluster head i and the two terms at the denominator represent the contribution to power consumption due to the output transmit power and the cluster-head transmitting/receiving activity, respectively.

C. Calculation and Optimization

Calculation of random F_E is not complex, but there are bounds within which this randomly picked rate must lie. The lower bound of this range defines the minimum rate with which the NSBs must be exchanged to maintain the network state even in case of significantly less load on network. On the other side the upper bound of rate puts a limit on the maximum value of F_E, exceeding which would put exceedingly extra load on the network due to very frequent NSB exchanges and, in fact, may result in redundant NSBs being observed and propagated. This randomly selected rate expressed in seconds is distributed throughout the network by adopting one of the four methodologies described earlier.

Mathematically:

$$F_E = RND(F_{E\min}, F_{E\max}) \tag{3}$$

Where:

F_E is the Beacon Exchange Rate in seconds. Its value states the time interval after which the NSBs will be exchanged. The two other terms $F_{E\min}$ and $F_{E\max}$ are the Lower and Upper bounds of F_E respectively. Fixing the lower and upper bounds of FEB is greatly influenced by two parameters of network design-policy:

Extra Load (U_x): Network overhead load caused by proactivity activities must not exceed *k%* of the total actual load on the network.

Update Resolution (T_R): The minimum resolution of time by which the updated network state is required should be T_R.

Keeping these parameters in consideration, the upper bound is given by:

$$\eta = U_{Total} + \left[\frac{T_f - T_i}{F_{E\max}}\right]\bar{U} \tag{4}$$

Where:

$$U_{Total} = \int_{t=T_i}^{T_f} \sum_{i=0}^{F_n} U_{it}$$

U_{it} : Load on PN i at time t.

$\bar{U}$: Extra load caused by proactivity in a unit time.

η : Total load on the network, including the load caused by proactivity, after time T_f. U_{Total} in above equation gives total load on the network within the given time interval $\{T_i, T_f\}$. The second term in (4) is the load caused in this interval by proactive activities. Given the extra load (U_x) policy factor k, η defines the upper bound of F_E given by:

$$\eta \le (1 + \frac{k}{100})U_{Total} \tag{5}$$

i.e. $F_{E\max}$ must keep η within the allowed extra *k%* load.

The lower bound, defined by the required update resolution (T_R), is given by:

$$F_{E\min} \le T_R \tag{6}$$

I.e. as long as lower bound $F_{E\min}$ is less than T_R, the state of the network is observed at higher resolution than required and therefore this network state will be available in any critical situation. However, if $F_{E\min} << T_R$, it is highly possible that redundant NSBs are propagated, resulting in exceedingly overhead proactivity actions. On the other hand, if $F_{E\min}$ gets greater than the T_R, the NSB propagation will be less frequent than the required and so there is probability that at times the network will be *under-stated*, a state where actual picture of current network state is not available. In order to avoid these two extreme conditions of *redundancy* and *under-stateness*, it is required to optimize $F_{E\min}$. Consider the following relationship:

$$d = T_R - F_{E\min} \tag{7}$$

The optimal lower bound of F_E should be as close to T_R as possible such that $F_{E\min}$ minimizes $|d|$, the lower bound optimization factor. Fig. 3 illustrates the relationship between $F_{E\min}$ and the two extreme network conditions.

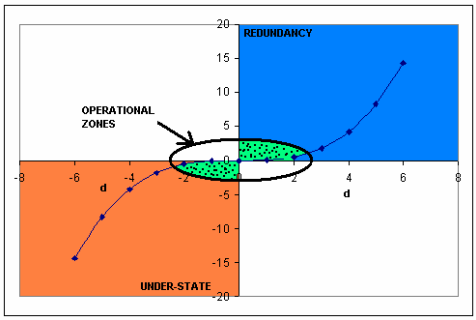

Fig. 3. Optimizing the lower bound of F_E. Dotted areas show the acceptable operational regions within which the two extreme conditions are safely avoided. Lower bound $F_{E\min}$ must be selected to keep d in these regions

The operational zones shown in the figure describe the optimal range for the selection of lower bound that would keep network state safely around the horizontal axis thereby avoiding the two extreme conditions. This relationship that ties the network state (λ) to the lower bound optimization factor (d) is given by:

$$\lambda \simeq \frac{d^3}{p} \tag{8}$$

where p is a tuning factor and its value depends upon the resolution of updation (T_R). The operational zone is given by:

$$-2d \le \lambda \le 2d \tag{9}$$

IV. Simulation Results

Simulations were carried out to find out the impacts of complex combinations of F_E, its method of implementation and PS and PN nodes densities on the overall QoS. TABLE V illustrates the simulation environment parameters. Performance metrics of percentage packet loss, energy consumption and throughput were used for 10 and 40 seconds F_E, implemented by all the techniques discussed in Subsection III-B.

A. Packet Loss

Fig. 4 illustrates packet losses due to randomly failing nodes in the network for the three methods of F_E implementation and no-F_E strategy. The results indicate that there is a savings of up to 70% in the packet losses due to failing nodes in case of incorporating beacon exchange for network state management as compared to without F_E strategy. Out of the three methods of F_E implementation, Routing and Hybrid techniques performed better than the Direct technique at the latter stages of network operational, where the Direct technique seems to trace the packet loss profile of No-beacon-exchange curve. This is due to the direct connectivity of nodes with the CCI which drains their energy more quickly. Comparing the two graphs (Fig. 4: A & B) reveal that as the F_E value increases, the network state is maintained less frequently which leads to a serious degradation in performance of the Routing as well as Hybrid techniques. This phenomenon testifies our arguments for optimizing the bounds of F_E presented in Fig. 3. The smooth transition of the curves of Routing and Hybrid techniques illustrates the proactive action of the self configuration model that protects the network from facing unprecedented losses and arranges a solution to the malfunctions beforehand. The graphs also show a very important impact of F_E on the life time of the network; the network life is reduced in all cases of F_E implementation as compared with the No-BER. The result is as expected, but the point to be focused is the trade-off of life with the reliability of data transmission. In case of Routing and Hybrid techniques, the network life is reduced from 15 to 13 and 14 minutes respectively, but the confidence of data transmission is leveraged up to 70%, which is definitely, a worth trade with the life of the network.

TABLE V
Simulation Environment Parameters

Attribute	Value
Area under Surveillance	Open irregular Terrains of near 25000m² dimensions
Deployment Topology	Random for both PS & PN nodes
PS Comm. Range	3m
PN Comm. Range	3m-13m
Density of PS nodes	125-143 Randomly Deployed
Density of PN nodes	25-30
Mobility	Stationary PNs & Mobile PS nodes
F_E	10sec, 40sec
F_E **Implementation**	None, Direct, Routing, Hybrid
QoS Metrics	Packet Loss, Energy Consumption, Throughput Parent Availability
Network Activity Time	15 min

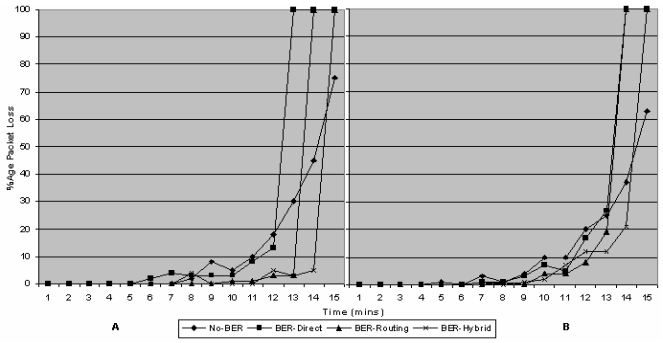

Fig. 4. Average Packet Loss for (A): 10 Sec F_E, (B): 40 Sec F_E

B. Energy Consumption & Throughput

An analysis of the energy consumption profile was done for the network configuration described in TABLE V. Fig. 5 shows the aggregate energy drainage profile of the PNs. It is quite promising to see a minimum increase of up to 10-15% in the energy consumption for Hybrid technique over the No-BER technique. In order to appreciate the benefit of proactivity at the cost of extra energy consumption due to proactivity, a key QoS parameter, *Throughput*, is calculated as:

$$Throughput = \frac{EnergyConsumed}{PacketLoss + c} \tag{10}$$

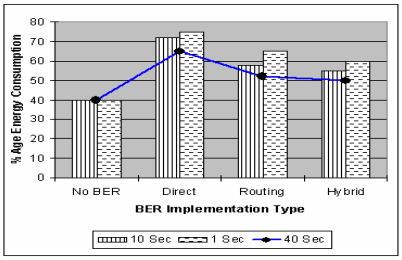

Fig. 5. Energy consumption profile for implementation methods of F_E

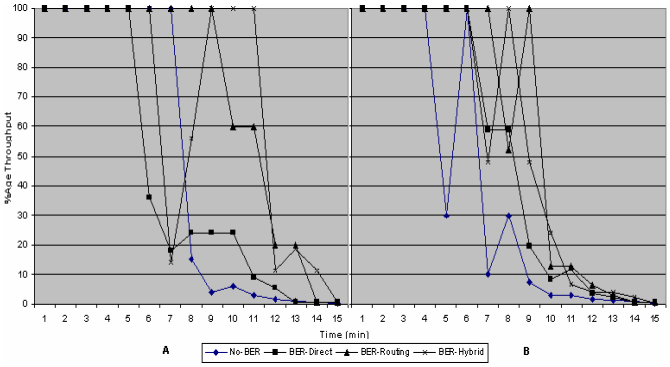

Fig. 6. Comparison of throughput for various implementation methods of F_E for (A): 10 Sec F_E, (B): 40 Sec F_E

where 'c' is a constant to avoid division by zero, and is taken to be equal to .001. Graphs of Fig. 6 illustrate that proactivity has improved overall throughout with all types of beacon exchanges, with Hybrid method maintaining the best QoS for an additional 25% of the network operation time compared to the No-beacon-exchange scenario. Comparing graphs A and B, it becomes evident that a larger value of F_E leads to less energy consumption but bears less confidence in maintaining the QoS for longer time. This evidence leads to the need of proper selection of F_E within the bounds of the operational zone shown in Fig. 3. Also the unstable throughput in case of larger F_E value (graph 5B) shows the understate situation when the improper value of F_E fails to keep the network state updated and so the proactive action of the model fails to figure out the possible impairments well in time.

C. *Parent Node Availability*

Fig. 7 shows the effects of PN failure on overall connectivity of PS nodes in the network. The PNs were triggered to die randomly one after the other. The effect on sensor-parent connectivity was analyzed for both situations when self-configuration was active and inactive. The graph confirms that network could capture more than 80% of network traffic through proactively reconfiguring connections through routing nodes, even when half of the PNs failed.

V. CONCLUSIONS

This paper has presented beacon exchange rate optimization technique for Direct, Routing and Hybrid methods of beacon propagation. The numerical as well as simulation results have shown that the optimization of F_E is a significant improvement over the proactive self configuration protocol to deal with various malfunctions and abnormalities in USNs including node failure and node overloading. Results and analysis indicate that the most critical aspect of network design based on such proactive self-configuration model is the selection of F_E. For this purpose, numerical bounds on the maximum and minimum values of F_E were presented. This operational zone for the selection of F_E, eliminates/reduces the risk of getting into *Redundancy* or *Understate* situations. The simulations for packet loss, energy consumption and throughout have confirmed the increased energy consumption in case of *Redundancy* while *Understate* situation has lead to unstable network throughput.

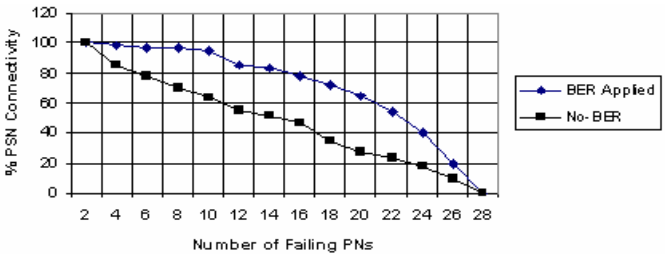

Fig. 7 Effect of Parent Node Failure on % Connectivity

The results have demonstrated that incorporation of beacon exchange has provided a trade off between the network life and reliable data transmission. Out of three F_E implementation methods, Hybrid and Routing have shown promising results while consuming nearly 15% more energy and providing over 65% savings in packet losses. Also the results have confirmed the continuing stability of the model in terms of maintaining the QoS (throughput) for another 25% of network operation time. The proposed model is found robust as more than 80% of component devices are observed connected through development of multi hop routes in the USN even when half of the PNs failed to work. This implies that the model keeps maximum components connected to the network in case of node failures and failovers with smooth degradation of performance.

REFERENCES

[1] "Wireless Sensor Networks for Emergency Medical Care" *www.eecs.harvard.edu/~mdw/talks/ge-codeblue.pdf*

[2] H. Gupta, S. Das, Q. Gu, "Connected Sensor Cover: Self-Organization of Sensor Networks for Efficient Query Execution", *ACM,MobiHoc 03.*

[3] C.F. Chiasserini, I.Chlamtac, P. Monti, A. Nucci "An Energy efficient method for nodes assignment in cluster-based ad hoc networks", *ACM/Kluwer Wireless Networks Journal, 2003*

[4] N. Sadagopan and B. Krishnamachari, "Decentralized Utility-based Design of Sensor Networks," *WiOpt'04*, Cambridge Uni, UK.

[5] J. Carle, David, S. Ryl, "Energy-Efficient Area Monitoring for Sensor Networks", *IEEE Computer Society 2004*

[6] J. Rabaey, J. Ammer, J. L. da Silva Jr., and D. Patel, "PicoRadio: Ad-hoc wireless networking for ubiquitous low-energy sensor/monitor nodes*", IEEE VLSI, pp. 9-12, 2000.*

[7] N. Bulusu, J. Heidemann, and D. Estrin. "Adaptive Beacon Placement". *21st International Conference on Distributed Computing Systems, pp. 489-498. Phoenix, AZ, April, 2001.*

[8] H. Zhang and A. Arora,"GS^3: scalable self configuration and self-healing in wireless sensor networks", *Computer Networks, Vol. 43, 2003*

[9] N. Bulusu, J. Heidemann, and D. Estrin. "Scalable Coordination for Wireless Sensor Networks: Self Configuring Localization Systems". *ISCTA-01 UK*

[10] M. Iqbal, I. Gondal, L. Dooley. "Investigating the Dynamics of Pervasive Sensor Networks through Parent Localization", *ATNAC 04*

[11] M. Iqbal, I. Gondal, L. Dooley. "LACON: Localized Autonomic Configuration in Pervasive Sensor Networks", *ISSNIP 04*

[12] Y. Yu, R. Govindan, D. Estrin. "Geographical and Energy Aware Routing: A Recursive Data Dissemination Protocol for Wireless Sensor Networks", *UCLA Computer Science Department Technical Report UCLA/CSD-TR-01-0023, May 2001*

[13] A. Cerpa, D. Estrin, "ASCENT: adaptive self-configuring sensor networks topologies", *IEEE INFOCOM 02.*

[14] C. Schurgers, V. Tsiatsis, M. B. Srivastava. "STEM: Topology Management for Energy Efficient Sensor Networks", *IEEEAC 2002*

[15] J. Kahn, R. Katz, and K. Pister, "Next Century Challenges: Mobile Networking for Smart Dust," *ACM MOBICOM'99.*