The Implications of Reliable Data Delivery for Performance in Wireless Sensor Networks

Jonathan P. Benson, Cormac J. Sreenan.
Mobile and Internet Systems Laboratory (MISL), Department of Computer Science,
University College Cork (UCC), Ireland

Abstract

Messages transported within a sensor network are subject to losses due to a number of factors. These factors include losses in the wireless channel, MAC layer collisions, node error or failure and losses due to incorrect routing. This paper describes these sources of data loss and discusses the various strategies available to prevent data loss. The effectiveness of each of the strategies to prevent the different types of data loss is discussed. In particular, it is examined how the implementation of any particular scheme affects network performance. Here we define performance as accurate sensing of phenomena, reliable delivery of data, and the timeliness of data delivery. The implementation of reliability mechanisms in a sensor network can adversely effect the timeliness of data delivery thus presenting a design trade off in this area. Our principal contribution is the identification and description of this problem. Furthermore, we discuss the trade offs between reliability and delay and investigate the need for a framework to aid in WSN design in this area. It is our intention to implement and evaluate such a framework in our ongoing research.

I. Introduction

Wireless sensor networks are collections of autonomous devices (sensor nodes) endowed with computational, sensing and wireless communication capabilities. One such example sensor node is the Dsys25 [13], [14] which was developed jointly by the Tyndall National Institute and the Mobile Internet and Systems Laboratory(MISL), UCC. (Fig. 1). A great deal of research is currently ongoing in this field, particularly in the last few years, as the potential applications and benefits of this technology are numerous. Potential application areas include defence, security and asset tracking, industrial monitoring and control, environmental monitoring, and building automation.

While there has been significant work devoted to the development of energy efficient sensor networks and applications there has been a lack of work on implementing performance assurances for sensor network applications. Many application scenarios are mission critical and correct delivery of data in a timely fashion is paramount and therefore may take precedence over energy efficiency, bandwidth utilisation, and other considerations. To be precise we define performance as the following:

1. The ability to accurately and effectively sense the desired data

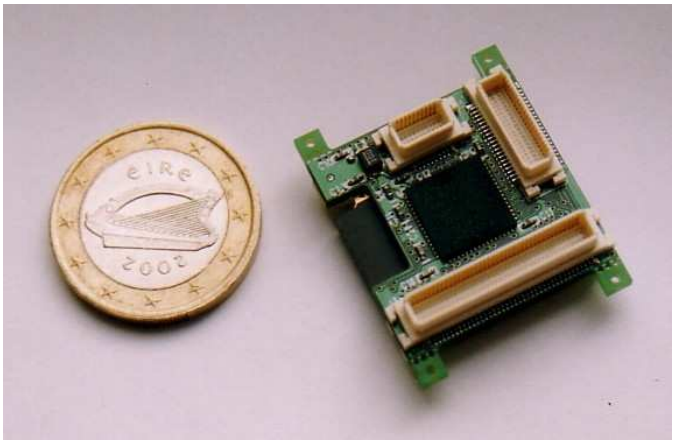

Fig. 1. A Dsys25 sensor node beside a 1 Euro coin

2. The ability to reliably deliver this data to its destination
3. The ability to deliver data within the necessary time bounds

The ability to accurately and effectively sense the desired data is dictated by the abilities of the sensors, their mode of operation and their physical deployment. We will not be discussing these issues. However, we shall discuss the second and third of these requirements and their relationship.

This paper examines the causes of data loss in sensor networks and the strategies used to attain reliable data transmission. Heretofore, the cost of implementing these strategies has been measured primarily in terms of energy consumption. An underlying problem, disregarded by previous research, is that reliability mechanisms can create delays which cause problems for delay intolerant applications. Such a problem area has not previously been defined in WSN research. We investigate the various reliability stratagies employed in wireless sensor networks and discuss their applicability to differing kinds of errors and the amount of delay typically suffered by their use. We also identify several other issues of importance with regard to real time systems including the MAC layer and the use of duty cycles.

The remainder of the document is organised as follows. Section II discusses the motivation for out work. Section III discusses the causes of data loss in sensor networks and Section IV discusses reliability strategies to prevent data loss and the effects of implementing the reliability strategies discussed on data delivery delay. Section V details challenges

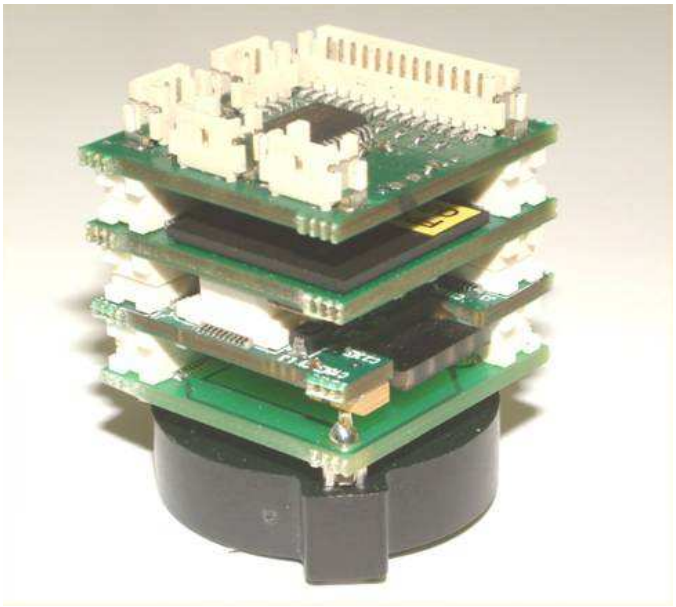

Fig. 2. Dsys25 node with stackable sensor modules and FPGA layer

in this area and also discusses our proposed framework.

II. Motivation

There are a great number of potential sensor network application that could be successfully implemented but are dependent on performance related guarantees, principally concerning the reliability and timeliness of data delivery. Such applications may have hard real-time or soft real-time requirements in addition to limited tolerance to data loss. Medical applications where remedial or emergency actions may be initiated as a result of incoming data would have demands as described above. For instance, a patient can be attached to a number of devices which monitor blood pressure, heart rate, breathing rate, temperature and muscle activity. Data can be collected from the patient and relayed to a collection point for analysis. In this scenario abnormal data from one or more sensors can trigger an action; erratic heartbeat coupled with rapidly falling blood pressure may signal a heart attack and emergency services may be summoned. In a more advanced scenario remedial drugs can automatically be released into the bloodstream of the patient. Several other application scenarios exist with potential applications in factory automation, security and real-time data collection.

While the potential applications for wireless sensor networks are numerous their introduction is hampered by some fundamental problems. In particular the issue of the reliability of data transport through a multihop network is crucial. Wireless communication is subject to interference from a number of sources ranging from interference from other wireless devices to interference from physical objects in the environment. In addition collisions and node failures can add to the perceived lack of reliability experienced. Thus, wireless communications are far less reliable that wired communications and remedial actions must be taken to ameliorate this problem.

In order to increase the level of data transfer reliability experienced by the end user, or, indeed by application itself, it is necessary to employ a number of methods and techniques. Almost all these of methods use some redundancy to achieve their goal thus imposing a cost. Heretofore, the cost of employing such methods has been measured in terms of how much extra energy is consumed within the network, thus presenting the well known design trade off of energy vs reliability. However, it has not been considered in any great detail how these methods effect the timeliness of data delivery particularly for application with real-time constraints. All of the methods to increase the reliability of data delivery have an effect on the time taken to successfully deliver a message to its destination. Also, note that in a multihop wireless network that the delays imposed by reliability methods are very often cumulative. Thus sensor networks of varying sizes and topologies may experience dramatically different delays to each other.

III. Causes of Data Loss

A strategy to ensure reliability in a sensor network has a number of obstacles to overcome. These sources of data loss include:

1. Losses in the wireless channel due to interference and physical effects
2. MAC layer losses due to collisions
3. Losses due to node related errors or failures
4. Losses due to routing failure

The wireless channel is inherently lossy and experiences both bit and burst errors caused by interference from other wireless devices, and multipath effects caused by the environment. In addition the wireless signal may be absorbed or blocked by certain objects. This problem is compounded by the fact that the wireless channel is not constant over time [3], [4]. It is often assumed that errors in the wireless channel occur as a statistical distribution of bit errors. However, in wireless networks it has been observed that errors can be bursty in nature and can effect significant areas of the network for a period of time before disappearing [5]. During these periods it is often impossible to send or receive from any of the affected nodes.

Accessing the MAC layer may lead to errors in some particular cases. It is often assumed, incorrectly, that node connectivity is bi-directional and this is sometimes not the case. In these particular instances MAC layer errors can potentially occur. Contention based MAC protocols, whether using collision avoidance or not, fall foul of this condition via the hidden terminal problem. Typically, collision avoidance schemes assume bi-directional connectivity while CSMA schemes explicitly ignore the problem. Results from [3], [4] suggest that bi-directional connectivity assumptions are unrealistic. Other MAC protocols which coordinate with other nodes in order to automatically configure themselves may also be susceptible to errors caused by asymmetrical connectivity. This is particularly true where automatic clustering and synchronisation is involved.

A node may experience a failure or may simply fail to forward a message for a number of reasons. Hardware failure, battery failure, destruction of the node, etc., is not uncommon among sensor nodes and this can result in lost messages. Aside from this, constraints on memory and buffer space can cause a packet to be dropped. For example, certain radios have a single buffer space and if an incoming packet is not handled before the next packet arrives one of the packets must be dropped. In general, nodes with a heavy routing load may be able to hold a finite queue of messages in memory awaiting transmission. Problems arise when traffic loads within the network and on a particular node, are heavy and/or the node experiences difficulty accessing the transmission media. Thus dropped packets can occur.

A route may fail for any of the reasons described above. Link errors, periods of congestion and node errors can cause a designated route to become disconnected. Should a node find itself unable to forward a message towards its destination it will very likely drop the packet after a period of time has expired. In this case an alternative route is necessary and if a message is to be successfully delivered, one must either already be formed or created as needed.

IV. Reliability Strategies

There are at present a number of different reliability strategies that can be used in combination or individually. These can be classified by the particular problem area that they attempt to address.

A. Link Layer

A number of techniques exist which address the need for reliability at the link layer. Link layer reliability mechanisms can be effective in increasing the reliability of a single link but fail to eliminate the effects of route failure and only partially remove the effects of node error and failure. In this regard additional mechanisms are needed.

Forward error correction (FEC) relies on redundant data being appended onto the existing data. Bit errors that occur can be detected and corrected [5], [9]. Various types of codes exist with various properties. In general the stronger the code that an FEC uses the more bit errors it can successfully detect and correct. In general, the stronger the FEC the more redundant bits are needed thus increasing transmission time. The use of variable FEC strength depending on packet importance was investigated in [9]. Recent research has shown that the use of error correcting codes is of limited use in sensor networks [5] since errors are typically bursty in nature. In essence [5] describes that where burst errors occur the number of redundant bits necessary for correction is prohibitively expensive. Since, burst errors are common in wireless sensor networks it is reasonable to conclude that FECs are of limited value.

If FECs are used the additional redundant data takes additional time to encode, transmit and additional time to decode. In general, the stronger the FEC the more redundant bits are needed thus increasing transmission time. However this time is usually relatively small. The time taken to encode and decode FEC codes depend on the abilities of the sensor node and the complexity of the FEC code used. Since processing power on sensor nodes is relatively low this may take quite a long time. However, on the Dsys25 it is possible to add stackable hardware layers, one of which is an FPGA which can be used to greatly speed the encoding and decoding of FEC codes, Fig. 2 . The time taken to encode, transmit, receive and decode an FEC can be described as follows:

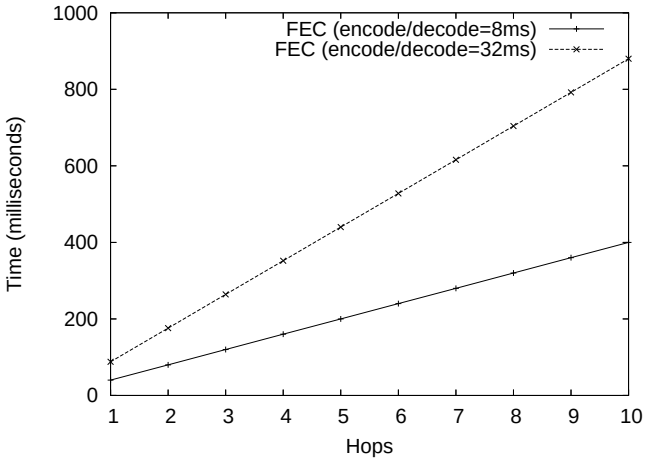

Fig. 3. FEC delay summed over a number of hops

$$Encode_{FEC} + Tx/Rx_{data+header+FEC} + Decode_{FEC} + [MAC_{access}] \quad (1)$$

where $Encode_{FEC}$ and $Decode_{FEC}$is the time taken to encode and decode respectively, and $Tx/Rx_{data+header+FEC}$ is the time taken to transmit the data, the header and the additional bits for the FEC respectively to the receiver.

Consider Fig. 3. We evaluate the total transmission time for a message over a variable number of hops using Equation 1. The time taken to transmit and receive a packet without addition FEC codes is 4 milliseconds (typical transmission time on Dsys25 node). The additional time take to transmit and receive the FEC is 4 ms. MAC access is considered constant and take 16 ms (typical MAC access time on Dsys25 node using contention based MAC protocol under medium traffic). The times taken to encode and decode the are described in Fig.3 and are 8ms and 32ms respectively. Note that in the following figures (Fig. 3 to 7) the value for the MAC access time is considered to be constant and thefore the resultant graphs appear linear whereas in a real network they will be more random and affected by changes in traffic cause by longer packet size and retransmission etc..

ARQ protocols may use multiple repeat transmissions to ensure correct data delivery between two nodes. Obviously this will have a significant effect on the delay incurred. However note that ARQ protocols are inherently resilient to burst errors since the repeat messages are temporally displaced from each

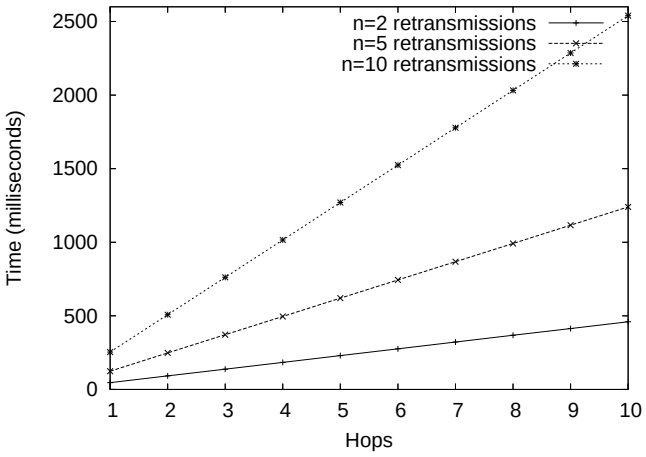

Fig. 4. Delay caused by ARQ retransmissions

other. Repeating a message can also help to ameliorate the effects of both node errors and, in some cases, MAC errors. The time taken to successfully send a packet when using repeat link layer transmissions is as the following probability:

$$(1 - p_{drop}^{n}) \cdot (n \cdot (Tx/Rx + [MAC_{access}]) + (n-1)TimeOut) \quad (2)$$

where p_{drop} is the probability that a packet is lost on the wireless link, n is the n^{th}transmission sent, and $TimeOut$ is the time a node waits for an ACK to be recieved.

Consider Fig. 2. The same values for Tx/Rx and $[MAC_{access}]$ as used in Fig. 3 are used (4 and 16ms). The timeout takes 6ms. The delay for a varying number of retransmissions is considered.

B. Routing/Network Layer

There are three main strategies for establishing error free routing in wireless sensor networks: Avoidance [8], [1], Reaction, and Redundancy [6], [7], [8]. In terms of avoidance, choosing a route that avoids areas prone to packet loss can help to increase the overall reliability. For example when choosing a neighbour to route through, a node may pick the one with the least errors experienced or the strongest recieved signal strength. Better still, a reactive system that can rebuild a route to avoid problems as they occur can be especially beneficial in a WSN where conditions may often change due to node failure, unpredictable traffic and physical effects. An alternative to reactive rerouting is to regularly update the routing structure thereby routing around problem areas as or shortly after they occur. Redundant routes can be used to send duplicate data thus increasing overall reliability. Multiple disjoint routes [6], [7], [8], in particular, can help to ameliorate the effects of node failure and fluctuations in link quality. These methods are costly since they involve an increase in control messages in order to set up the routes and all the data is duplicated as it is sent across them, reducing the overall bandwidth of the network and causing increased congestion at the MAC layer.

Directed diffusion [1] is one particular method that makes use of multiple routes with one important difference. While multiple routes are maintained only one is reinforced and used to carry most of the data. Some redundant data is sent along the alternative routes and also serves the purpose of acting as a route testing and probing mechanism. Should an alternative route prove better than the existing one it can then be reinforced and used instead. A more primitive method of using redundancy at the routing layer is to use flooding or limited flooding [8], [7]. This method reduces the amount of control messages needed to set up routes but increases the amount of messages sent and recieved by participating nodes. Flooding often makes use of the broadcast nature of a WSN. A message maybe sent once but may be recieved by any listening node within range. Typically, if a receiving node is not closer to the sink than the sender it will drop the incoming packet. In some cases nodes that are the same number of hops away may keep and rebroadcast the message as this aids the fanning out of messages and helps to create non-overlapping routes.

The various strategies for ensuring reliable high quality routes can be used in combination or individually. Again each approach has both strengths and weaknesses. Strategies involving multiple paths dramatically reduce the likelihood of route failure and, providing that there is a reasonable degree of fanning out between the paths, reduce the venerability to localised bursty errors and localised areas of channel contention. Using multiple paths incur the following additional delay compared to using the shortest path only:

$$(Tx/Rx + [MAC_{access}]) \cdot (h_{actual} - h_{min}) \quad (3)$$

where Tx/Rx is the transmission time from each sender to sink and $h_{actual}$and $h_{min}$is the number of hops the data has traversed when recieved at the sink and the minimum number of hops between source and sink respectively. Note that when using multiple routes the delay may vary depending upon the particular route a message arrives by. In some cases this may indeed be the shortest possible route. Fig. 5 shows the delay incurred by choosing a route longer than the shortest available. Values forTx/Rx and $[MAC_{access}]$ are as before, 4ms and 16ms.

In choosing a high quality route it is important to note that a longer route may be chosen than the shortest route possible. As a result the delay incurred once the route is established is similar to Equation 3. Reactive rerouting incurs the delay of forming the new route and of course the route length may change for better or worse as a result. The mechanisms for rerouting are varied but typically this operation involves a control message being sent and returned along the reverse path. Therefore the additional delay is in the order of:

$$Timeout + (2Tx/Rx + [MAC_{access}]) \cdot h_{reroute} + ((h_{old} - h_{new}) \cdot (Tx/Rx + [MAC_{access}])) \quad (4)$$

where Tx/Rx is as before, $h_{reroute}$ is the number of hops needed to reroute and $(h_{old} - h_{new})$ is the difference in hops

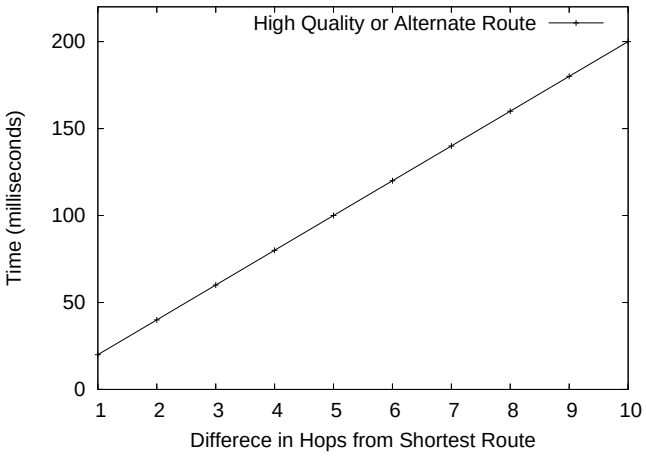

Fig. 5. High Quality or Alternate route delay

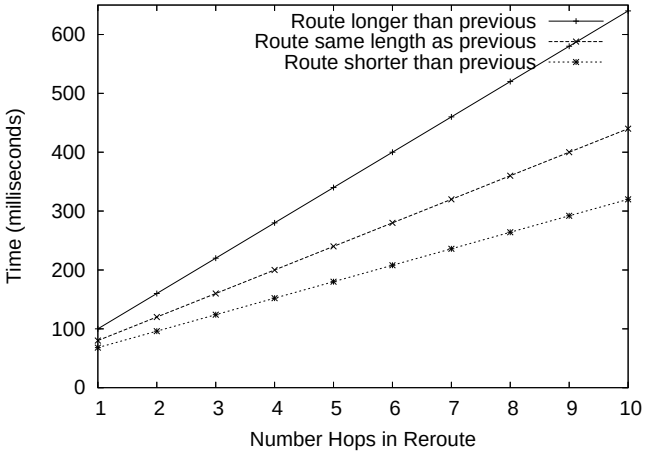

Fig. 6. Delay due to Rerouting

between the old and the new route. Wide scale duplication of messages can have adverse effects on MAC layer protocol performance as can large amounts of control messages. Increasing traffic within the network can increase errors due to congestion of the wireless channel and prevent nodes sending their data. It is therefore important to ensure that sufficient capacity and redundancy is present in order to support the traffic load generated. Fig. 6 shows the delay imposed by a forced rerouting due to an error found. Tx/Rx=4ms and $[MAC_{access}]$=16ms as previous. $Timeout$=40ms. Note that this delay only occurs when a reroute is necessary. Obviously frequent rerouting can cause considerable delays. In cases where rerouting occurs very frequently alternative methods such as limited flooding may have superior performance in terms of delay.

C. Transport Layer

Transport Layer mechanisms include the use of multiple duplicate transmissions and end-to-end acknowledgments such as TCP. The use of end-to-end acknowledgments differs from link layer ACKs. Transport layer systems making use of ACKs endeavor to ensure correct delivery has occurred at the transmission endpoint whereas link layers ACKs merely ensure that the message has reached the next hop. End-to-end ACK systems have the advantage that all errors become apparent at the sender and successive attempts can then be made to resend the lost packet. Note that while the errors are apparent the exact cause may not be. TCP itself must be drastically modified to operate in a WSN environment as its original design assumes that packet loss is due to the transmission rate increasing to a level where a router on the path is forced to drop packets due to congestion. Such assumption do not often hold in WSNs where packet loss may be caused by any number of factors. Note that the transmission of end-to-end ACKs are also subject to packet loss themselves. Split TCP and Mobile TCP attempt to address this problem for wireless networks but are nor tailored to the needs of WSNs.

While end-to-end ACKs can be very effective it is important to realise that this comes at the cost of increased latency with respect to transmitting lost packets. A full round trip time (RTT) must expire before the lack of an acknowledgement triggers the retransmission of missing packets. This leads to a relatively large amount of time before retransmission occurs and this problem is further compounded by the fact that, in a WSN where route length and channel access time may be highly variable, a highly conservative RTT must be chosen. Therefore, it would greatly improve performance if channel access time and route length are bounded. The time taken for a packet to be sent successfully is the following probability:

$$(1 - p_{loss}^{n}) \cdot ((n \cdot Tx/Rx_{end-to-end} + (n-1) \cdot (RTT - Tx/Rx_{end-to-end}))) \quad (5)$$

where p_{loss} is the probability that a packet is lost, n is the n^{th}transmission sent, and RTT is the time a node waits for an ACK to be recieved before resending. Fig. 7 shown the effects of using an end-to-end retransmission scheme for varying amounts of retransmissions. Tx/Rx=4ms and $[MAC_{access}]$=16ms as previous. The RTT is chosen to be a constant 500ms. The time taken for successive retransmissions grows quite sharply when the network become large. This indicates that basic end-to-end retransmissions are not suitable for large sensor networks.

Another strategy, that seeks to lessen this problem, is to subdivide the route into stages and have a caching point at each stage. In this manner the responsiveness of repeated transmissions can be improved as well as the energy efficiency.

A more simple approach is to simply send redundant messages or repeat transmissions. The use of duplicate transmissions can be used to reduce the probability of packet loss [2], [6], [7]. The number of transmissions sent can be based on the recieved signal strength and the distance in hops away from the sink. As discussed previously strategies involving repeated transmissions are very resilient to bursty errors. Multiple retransmission systems suffer similar delays

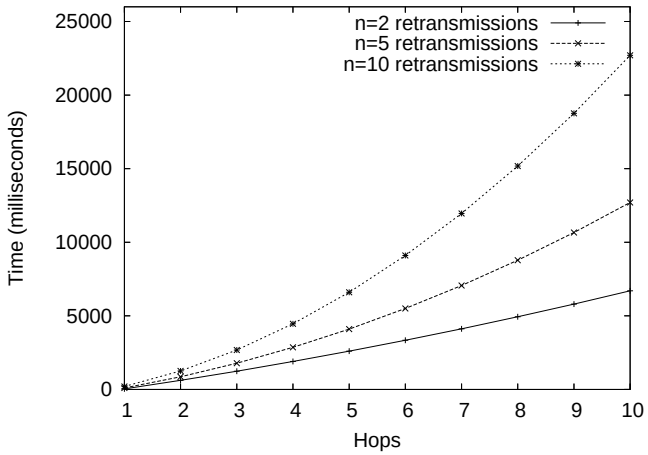

Fig. 7. Delay incurred by End to End Methods using RTT

to their link layer counterparts as in Equation 2.

V. Agenda

A. Mac Layer

Special attention must be given to the choice of MAC protocol in WSN deployments that need delay assurances. Essentially, the predictability of delays during node-to-node communications is fundamentally defined by the MAC layer protocol used and its behaviour under varying conditions. Note that in the previous graphs in section IV a fixed value was used for the MAC access times. In reality this is not the case as MAC access times can be highly variable. Therefore an essential component of building the frame work discussed below is to quantify MAC layer performace with respect to delay under a variety of traffic conditions (since most MAC layer are not traffic invariant).

In general, there are two types of MAC systems: contention based and schedule based. Both of these types of systems differ in their implementation requirements and the type of behaviour they deliver.

Contention based MAC layers are widely used since they have far fewer requirements than their schedule based counterparts and are therefore easier to implement. Contention based MAC protocols have a particular disadvantage compared to their rivals. It is impossible to predict exactly how long it will take for a node to successfully access the channel and send a packet. This leads to non-deterministic behaviour and also has an indirect effect on reliability strategies that use retransmissions since it becomes impossible to gauge the time it will take for a retransmission to occur. Strategies that increase local traffic also cause increases in contention for the channel thus changing the properties of the MAC protocol itself making predictable behaviour extremely difficult.

A schedule based MAC protocol is more difficult to implement because accurate time synchronization among neighbouring is required. Each node uses a dedicated time slot to transmit messages. As fixed time slots are used the maximum message delay bounds can be easily be given. The principal problem of schedule based MAC protocols is the complexity introduced by time synchronization. First, it is difficult to synchronize clocks in a distributed wireless multihop environment. Second, the amount of synchronization messages that must be passed between nodes at regular intervals to combat clock drift can be significant. This has the effect of decreasing the amount of time allocated to data transfer and therefore increases the maximum delay bound for sending packets.

There are a number of other deterministic MAC protocols available that are CDMA, or FDMA based. These have desirable properties since they can give bounded times for channel access delays thus facilitating the calculation of data delivery delay bounds. However, several of these schemes are difficult to implement and have scalability issues. For example FDMA require more complex radios, and all of these systems require clustering when the network become too large to facilitate efficient multiple access. The issue of self configuration is also pertinent here. It is by no means certain that self configuration and clustering will result in correct collisionless operation. In mission critical cases advancements in automatic configuration are needed otherwise manual configuration and verification is the only method to ensure correct functioning.

TABLE I

Effectiveness of reliability methods

	Bit	Burst	MAC	Node	Route
FEC	good	poor	-	-	-
ACK	v.good	good	good	poor	-
Quality Route	medium	medium	medium	poor	-
Re-routing	poor	poor	medium	good	good
Multi-Routes	good	medium	good	good	good
End-to-end	v.good	v.good	v.good	v.good	v.good

B. Decision framework and verification

The decision space in this area is extremely complex and it is difficult to capture the behaviour, effects and dynamics of the numerous reliability techniques available and their effects on delay. It is clear that in order to design a WSN with performance assurance more sophisticated tools and methodologies are needed than currently available at present. A framework that would serve as a design tool and guide to WSN designers is needed. Given the size, shape and density of the network, characteristic errors, traffic pattern, delay constraints and power constraints, such a design tool could help resolve the design trade offs inherent in this area.

We propose a two phase approach. First a generic framework must be developed which can serve as a guide to WSN designers. Using the frame work a number of appropriate methodologies, a stand alone or combinatorial approaches, can be selected. However, due to the complexity of the problem at hand we feel that the framework itself cannot fully capture the dynamics and interrelationships of the problem and as a result cannot guarantee correct operation. Therefore we suggest the use of in-depth simulation to further test and verify proposed WSN behaviour, thus creating a two step approach that can be further refined by repeated iterations.

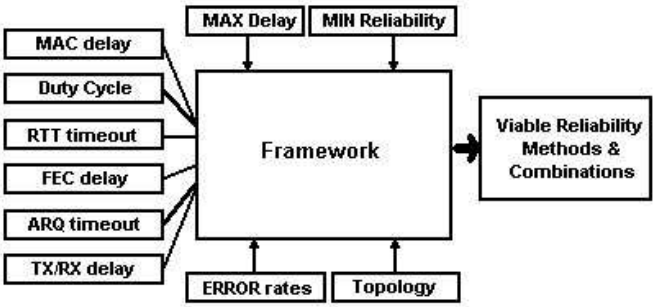

Fig. 8. Framework

In order to provide this framework it is necessary to quantify the effect of each type of reliability mechanism for a range of generic scenarios. For example using multiple redundant routes may be an effective technique in large unstable networks but would be inappropriate in smaller networks consisting of a handful of nodes. Likewise multiple redundant routes may not be appropriate in networks where traffic is already high. The effects of the various reliability techniques when used in conjunction must also be considered where appropriate. In depth characterisation of these reliability methods and their applicability to given topologies and network conditions shall be conducted in our future work. Table I gives an overview of the effectiveness of various strategies (FEC, Link Layer ACK, etc.) against the various possible errors (Bit, Burst, MAC etc.). Further quantifiable research needs to be conducted in this area and the results generalised and reduced into mathematical equations. This, along with delay metrics and the quantification of MAC layer behaviour, will from the back bone of our proposed framework.

As previously stated, while this framework can serve as a general guide it may not be possible verify that the chosen solutions are able to meet the constraints imposed using the framework alone. Given that there are a large number of variables which may interact in unexpected ways, that certain aspects of the network may have indeterministic qualities (MAC and routing protocols, traffic), and, finally, that errors may be random, it appears that this is indeed the case. To this end we propose a detailed simulation model capable of simulating all typical errors found on a WSN and the methods used to prevent them along with the energy expenditure and delay incurred. Using this simulation model, it will be possible to stress test a proposed WSN deployment in order to ascertain when and if it should fail to meet design constraints, especially with regard to reliability achieved, delay.

The benefits of such a two-phase system include better and more precise dimensioning of sensor networks, and correct protocol choices for any given target environment and set of application demands.

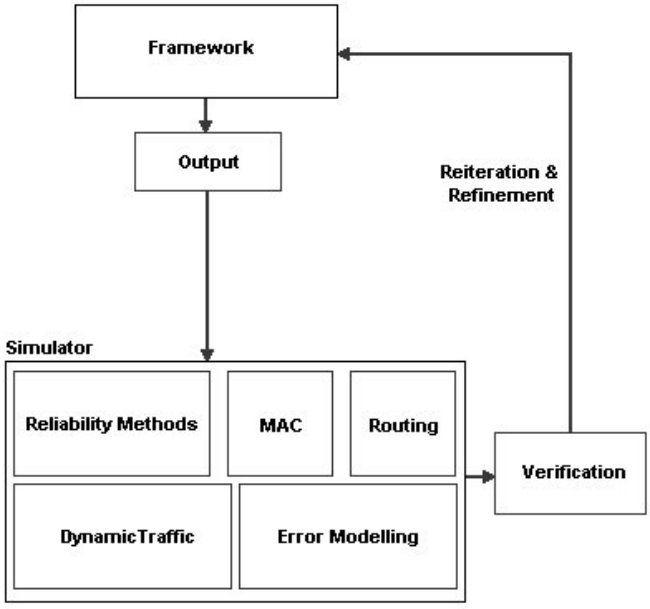

Fig. 9. Simulation and Verification

VI. Conclusions and Future Work

It has been clearly shown that the needs of sensor network applications with real-time constraints and demands are not considered by current methodologies. Previous research has considered energy the primary cost and de facto unit of currency in sensor networks research. We believe that if applications with real-time constraints are to be developed a radical shift of focus is needed that encompasses the demands of these applications, namely reliability of data delivery and the timeliness of data delivery. It has also been clearly shown that there are a great number of variables, attributes and dynamic behaviours that must be considered which necessitate the use of more sophisticated tools such as the framework and simulation tools we have described. In addition a great deal of work needs to be undertaken to quantify various aspects of network behaviour. In particular MAC layer performance and error modelling for realistic application scenarios must be properly evaluated and quantified and this will be conducted in our future work. Our proposed framework and methodology is an important step towards the important goal of providing reliable wireless sensor network applications with real time requirements.

VII. Acknowledgments

The support of the Informatics Research Initiative of Enterprise Ireland is gratefully acknowledged.

REFERENCES

[1] C. Intanagonwiwat, R. Govindan, D. Estrin. Directed Diffusion: A Scalable and Robust Communication Paradigm for Sensor Networks. Proc. of the 6th Annual Conference on Mobile Computing and Networks, 2000.

[2] F. Stann and J. Heidemann. RMST: Reliable Data Transport in Sensor Networks. Proc. of the IEEE Internationatl Workshop on Sensor Net Protocols and Applications, 2003.

[3] A. Woo, T. Tong, D. Culler. Taming the underlying challenges of reliable multihop routing in sensor networks. Proc. of ACM Sensys03, Los Angeles, CA, USA, 2003.

[4] D. Ganesan,B. Krishnamachari, A. Woo, D. Culler, D. Estrin, S. Wicker. Complex behaviour at scale: An experimental study of low power wireless sensor networks. Tech. Report UCLA/CSD-TR 02-0013, Computer Science Dept., UCLA, 2002

[5] A. Willig and R. Mitschke. Results of Bit Error Measurements with Sensor Nodes and Casuistic Consequences for Design of Energy-Efficient Error Control Schemes. Proc. of the IEEE European Workshop on Wireless Sensor Networks, 2006.

[6] Sudeept Bhatnagar, Budhaditya Deb and Badri Nath. Service Differentiation in Sensor Networks. Proc. of the 4th International Symposium on Wireless Personal Multimedia Communications, 2001.

[7] B. Deb, S. Bhatnagar, B. Nath. Information assurance in sensor networks. Proc. of the 2nd ACM International Conference on Wireless Sensor Networks and Applications, 2003.

[8] B. Deb, S. Bhatnagar and B. Nath. ReInForM: Reliable Information Forwarding using Multiple Paths in Sensor Networks. Proc. of the 28th Annual IEEE Conference on Local Computer Networks, 2003.

[9] A. Kopke, H. Karl and M. Lobbers. Using energy where it counts: Protecting important messages in the link layer. Proc. of the IEEE European Workshop on Wireless Sensor Network, 2005.

[10] I. F. Akyildiz, W. Su, Y Sankarasubramaniam, E. Cayicri. Wireless sensor networks: a survey. Computer Networks 38 (2002) 393-422.

[11] S. Hedetniemi, A. Liestma. A survey of gossiping and broadcasting in communications networks, Networks 18 (4) 1988, 319-349.

[12] K. Akkaya, M. Younis. A Survey on Routing Protocols for Wireless Sensor Networks. Elsevier Ad Hoc Network Journal, Vol. 3/3 pp. 325-349, 2005.

[13] D-Systems. http://www.cs.ucc.ie/misl/dsystems/

[14] B. O'Flynn, A. Barroso, S. Bellis, J. Benson, U. Roedig, K. Delaney, J. Barton, C. Sreenan, and C. O'Mathuna. The Development of a Novel Miniaturized Modular Platform for Wireless Sensor Networks. In Proceedings of the IPSN Track on Sensor Platform, Tools and Design Methods for Networked Embedded Systems (IPSN2005/SPOTS2005), Los Angeles, USA, April 2005.