Towards Achieving Reliability in Wireless Sensor Networks – A Survey

Sumeet Gupta [#1], Shekhar Verma [*2] and Raj K. Abrol[3]

[#] *School of E&CE, Shri Mata Vaishno Devi University, Kakryal, Katra, India 182 320*
[*] *Indian Institute of Information Technology Allahabad,Jhalwa, Allahabad India 211012*
[1] *sumeet.gupta@smvdu.ac.in,* [2] *sverma@iiita.ac.in,* [3] *rk.abrol@rediffmail.com*

Abstract

Sensor nodes in a WSN are deployed with the intention of collecting information such that the activities and environment in the target area can be faithfully reconstructed at a remote location using the raw data collected and action then may be taken based on same. Reliability of the deployed WSN becomes critical in this context as decision making could be adversely affected in case the reconstruction is incorrect. This becomes a major issue for Wireless Sensor & Actuator Networks where actuation is automated and solely dependent upon the reliability of information collected. The authors present a critical analysis of the various protocols and techniques proposed for ensuring reliability in Wireless Sensor Networks. A categorization of the techniques has been presented with emphasis on identifying the desirable features in a protocol which enables achieving higher degree of reliability. The challenges and critical requirements of reliable data acquisition as applicable to WSNs is also identified. The paper links the concept of reliability in WSNs to the traditional concept of reliability as applicable to devices.

***Keywords:** Wireless Sensor Networks, Reliability, Data Acquisition, Event Detection*

1. Introduction

Wireless Sensor Networks owe their genesis to the concept of ubiquitous computing which was proposed by Marc Weiser [1] in his seminal paper in 1991 and is today widely known as Pervasive Computing. This represents a tight integration of technology with all aspects of human life in a completely non-intrusive manner i.e. without the technology becoming the focus of attention [13].

Wireless Sensor Networks have emerged as an acceptable methodology for sensing events and acquire data spread over a geographic area [2] to satisfy the requirement mentioned in the implementation of Pervasive computing.

Various applications of Wireless Sensor Networks include Building Automation [36], Security & Defense [37], Forest Fire Detection [38], Agriculture [39], Lighting control [40], HVAC [41], Target Tracking [42], Disaster Management [45], Industry [9] and more. As shown in Figure 1, WSNs consist of tiny battery operated, inexpensive, small size computing devices with sensors and radio transceivers on board thus having the capability to sense the events and communicate with each other [3]. The self-organizing sensor nodes communicate with each other to either collaboratively establish the occurrence of an event or simply pass on the sensed data to a centralized sink where the data would be evaluated and the occurrence of the event inferred.

These nodes, energy and resource constrained, are deployed, at times, in harsh environments [37] and rely solely on the unreliable wireless link to communicate among themselves. Factors like network congestion, packet collision, environmental noise, channel characteristics, energy & resource constraint have an adverse impact on the

ability of the network to transfer the collected information to the centralized sink [2] while still maintaining a long working life. This unreliability has a direct impact on the ability of the sink to reconstruct the actual occurrence of the events in the area over which they are deployed. This has a direct bearing on the decisions made at the sink based on the information collected by the sensor network. The effect of some of these factors on the performance of the WSN can be mitigated by use of soft-computing techniques [46] while new hardware and system level design techniques can be utilized for others [47]. Ensuring energy efficient and reliable transport of data in resource constrained Wireless Sensor Networks (WSNs) is hard to achieve but is critical [3] for any practical real-life implementation.
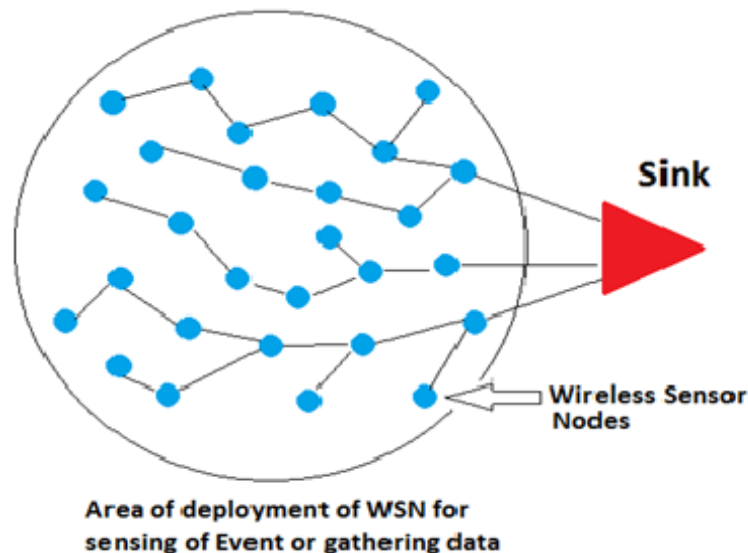
Figure 1. Typical Topology of a Wireless Sensor Network

With the evolution of Wireless Sensor & Actuator Networks (WSAN), the control aspect has been added to the network [3]. The actuator is activated based on the information collected by the sensor nodes and the decision making process is semi-automated or fully-automated [3]. Therefore in context of a WSAN, the reliability of the data acquisition process assumes higher importance, lest the actuation results in catastrophic events.

Many protocols and techniques have been proposed by researchers over the years. Some techniques focus on fault tolerant design where the network is able to deliver the packet in spite of temporary or permanent faults introduced in the network [44] while some techniques focus on maximizing the packet delivery [4]. Such methods prepare multi-path routes between the source nodes and destination nodes and keep changing the route dependent upon parameters like path success rate [43] etc. Some methodologies focus on achieving a balance between energy efficiency and packet delivery [20] while some focus on maximizing a chosen QoS parameter [49]. A host of techniques deliver very good network throughput with the assumption that the nodes are geographically aware i.e. they are aware of their own location as well as the location of other nodes and the sink [50]. Some techniques focus on delivery of packets in multi-sink scenario [5]. Techniques like swarm intelligence have also been adopted by many researchers to demonstrate protocols which offer reliability of data acquisition while using wireless sensor networks [51]. While most of the protocols focus on upstream propagation of collected information, there are some which focus on downstream query dissemination [25]. Some protocols [52] have been simulated using IEEE 802.11 PHY & MAC while others have used IEEE 802.15.4. Some techniques support periodic data acquisition while others support event based data acquisition, query based data acquisition or a combination

of these. Each proposed technique has attempted to optimize certain parameters while balancing others. In some cases, the researchers have validated the simulation results by conducting experiment on a test-bed of MICAz or IRIS motes. Although most of the techniques are based on recovering the lost information by re-transmission of the lost packet, there are some which recover lost or damaged information by using redundancy techniques [16, 30-34]. Authors have surveyed a large number of existing techniques and presented their critical analysis and comparison between them in the subsequent sections. Definition of the concept of reliability in context of WSNs is also discussed.

2. Reliability in Wireless Sensor Networks

The concept of reliability of data acquisition has been defined in different contexts as discovered during the literature survey [14, 53, 54]. The traditional definition of reliability of a system, as mentioned in the theory of reliability [55], is as below:

$$Reliability(t) = \mathrm{e}^{-\lambda t} = \mathrm{e}^{-t/m} \tag{1}$$

where λ is the failure rate, m is MTBF. This indicates that for system under observation, if the failure rate is constant, then the reliability of the system will reduce with time in an exponential manner. This definition is valid in context of a Wireless Sensor Network even though Wireless Sensor Network is a virtual entity composed of widely distributed physical sub-entities called Sensor Nodes. Since these nodes act collaboratively as a single network system, the definition of reliability of a system must be applicable. In view of this definition, various connotation of reliability could actually be defined for WSNs which put together, could provide a definition of reliability in Wireless Sensor Networks (Figure 2).
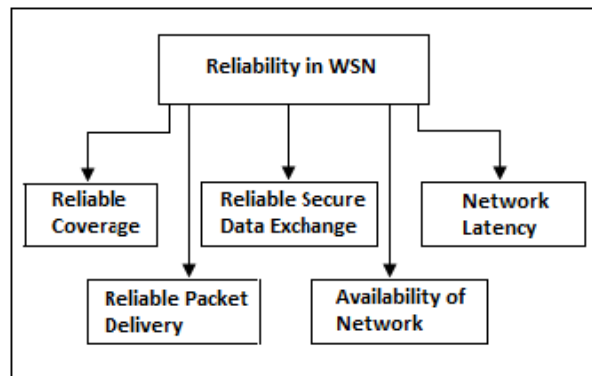

Figure 2. Categorization of Reliability in WSN

2.1 Reliability of Coverage (Sensing)

If the rate of failure of nodes in a Wireless Sensor Network is constant, then the ability of the network to perform the assigned task of collecting information or detecting events will decline exponentially with time. This is because as the nodes in a network die, the ability of the network to acquire information about the environment, in which it is deployed, drops significantly since the number of sensing points reduce and the probability of missing out on the detection of an event increases. Thus the Reliability of Coverage (or Sensing) will reduce exponentially as more nodes keep on failing on a regular basis. The coverage reliability can be improved by deploying redundant nodes and by placing the nodes such that their area of coverage overlaps. This ensures that in spite of failure of nodes, the number

of nodes available and working is more than the minimal required for coverage of the area [3] thus ensuring guaranteed coverage.

2.2 Reliability of Packet Delivery

The un-reliability of the medium of communication as well as the fact that is shared has an obvious impact on the ability of the nodes to communicate. As more and more nodes fail to communicate with each other, the ability of the network to pass on the acquired information to the sink reduces. This lack of ability to pass on the information collected by the nodes to the sink is reflected in a parameter called Packet Delivery Ratio [56] which is measured as:

$$Packet\ Delivery\ Ratio = \frac{Total\ Number\ of\ Packets\ received\ at\ Sink}{Total\ number\ of\ Packets\ sent\ by\ the\ nodes} \quad (2)$$

Thus as the Packet Delivery Ratio of a Wireless Sensor Network drops constantly then the **Reliability of Delivery** of sensed information degrades exponentially.

2.3 Reliability of Secure Data Exchange

As wireless medium is used for communication, the possibility of transmitted information being intercepted by unauthorised or rouge-node is high. This may allow these nodes to ingratiate themselves into the network and affect performance adversely. Further these rogue nodes may start feeding false information to the nodes or may even take control of the nodes within the network. If more and more nodes in the WSN get compromised then the **Reliability of Secure Data Exchange** in the network will degrade exponentially.

2.4 Reliability of Availability of Network

Another important parameter defined in the traditional theory of reliability is Availability of the system which is defined as:

$$Availability = \frac{MTBF}{MTBF+MTTR}$$

$$(3)$$

where MTBF is Mean Time Between Failures and MTTR is Mean Time To Repair. Also called Operational Availability, this is an indicator of the overall reliability of the system as it indicates the probability that the system will be available to perform the assigned task at any given time.

On a system level, in context of WSN, availability may be seen in context of the service being provided i.e. sensing information or detecting an event and propagating information to sink. Availability of network could be low because of failure of significant number of nodes or failure of communication. Thus a network with long Network Lifetime would have higher Availability as compared to a network with low network life-time.

2.5 Reliability in terms of Network Latency

Network latency ($T_{NLT)}$) and coherence are important parameters in case of WSANs. Network latency [57] refers to the time taken by the packet to reach sink/actuator while coherence refers to the delivery of the packets at the sink in sequence that they were generated at the nodes. Decision making in WSAN may get adversely affected if information is not received in time-bound and coherent manner. In case the constraints are not met there is a likelihood that the re-construction of the sensed event may not be correct thus leading to incorrect decision making.

Another approach to the concept of reliability is in terms of estimation of the event at sink based on the data received from the deployed sensors as enumerated by Vuran et al [35]. The observed event estimation distortion D at the sink in a decision interval ΔT of has been derived as a function of f which is the reporting frequency. It is assumed that the observed signal is wide-sense stationary as a zero mean Gaussian random process with σ^2. The channel noise is a additive white Gaussian noise, $(0, \sigma_n^2)$. Then, D can be written as [35]

$$D = \sigma^2 + \frac{\sigma^4}{\Delta Tf(\sigma^2+\sigma_n^2)} + \frac{\sigma^6}{\left(\Delta Tf(\sigma^2+\sigma_n^2)\right)^2}\sum_{k=1}^{\Delta Tf}\sum_{l\neq k} e^{-\left(\frac{|k-l|}{f}\right)} - \frac{2\sigma^4\theta}{\Delta T^2f(\sigma^2+\sigma_n^2)}\sum_{k=1}^{\Delta Tf}\left(2 - e^{-\frac{k}{f\theta}} - e^{-\frac{\left(\Delta T - \frac{k}{f}\right)}{\theta}}\right) \tag{3}$$

where the covariance function $e^{-\frac{|m-n|}{\theta}}$ depends on the time difference between signal samples at m and n and the covariance coefficient θ. It can be seen that D depends on f and ΔT. Optimal f will lead to increase in accuracy of estimation and to maximization of the network lifetime. As the number of packets depends on both f and ΔT determine the reliability of the data acquisition mechanism. The expression indicates that the Reliability of Data Acquisition is directly proportional to the packets of information reaching the sink within the given time constraint on the network latency time. Based on the above mentioned methodology the following conclusions can be obtained regarding Reliability in WSN & WSAN:

- Reliability of Data Acquisition & estimation & re-construction at Sink/Actuators will be higher if Effective Packet Delivery Ratio, considering the constraint on Network Latency Time, ΔT, is high and is approaching unity.
- Reliability would be reduced if packets arriving at the sink do not meet the constraint placed on the Network Latency Time, ΔT.
- For achieving a fixed value of reliability, the number of nodes that are required to be ON to detect an event at a given time will be low if the Data Acquisition mechanism can provide high Effective Packet Delivery Ratio i.e. with constraint on ΔT.
- This would also increase the overall Network life-time since more number of nodes can remain in sleep mode for longer period of time.
- Tolerance to faults, within a limit, which does not compromise the ability of the centralized sink to faithfully re-construct the event sensed by it will maintain good reliability

3. Elements of Reliability in Wireless Sensor Networks

The functional task of the WSN is collection of information and propagation to sink in form of data packets. In some applications, estimation of event is not enough, rather exact re-construction of the environment, in which the nodes are deployed, is required. This situation may arise even in an ordinary WSN which has sparse deployment of nodes or where the number of functional nodes has reduced over time. The information collected by each node then becomes critical even for estimation of an event. The objective then is to ensure that each packet transmitted by every node reaches the sink *i.e. Packet Delivery Reliability* [58] becomes critical. As opposed to this, in case a WSN is deployed for the purpose of detection of an event, then the objective of the WSN is to ensure that sufficient number of packets, transmitted by the sensor nodes, reach the sink for it to be able to detect the occurrence of the event *i.e. Reliability of Detecting an Event* becomes important [6]. It is obvious that the performance requirements on the WSN are much more stringent in case of Packet Delivery Reliability as substantial additional effort needs to be made to ensure that every packet reaches the sink.

Confirmation, that a packet transmitted by a node has actually reached the destination node can be obtained by using handshaking technique. This involves receiving an acknowledgement of the fact that the transmitted packet has reached the destination, failing which re-transmission could be initiated. The acknowledgement could be sent on receipt of packet at each hop, in which case it is called *hop-by-hop reliability* [4] or else the acknowledgement could be sent finally by the destination node i.e. *End-to-end reliability* [52].

In case of End-to-End reliability, the fact that a packet has not reached the destination node is detected by the destination node and this message is conveyed via multiple hops to the source node which re-transmits the lost packet. The intermittent nodes do not store the packet that they are relaying thus the memory requirement is not severe. The obvious disadvantage is the latency involved in detecting the loss of a packet and eventually getting the packet after re-transmission by the transmitting node. In case of hop-by-hop reliability each transmission by a source or intermittent relay node is acknowledged by the immediate destination node and re-transmission is done by the preceding transmitting node. This ensures that reliability is maintained at each hop besides ensuring low latency of packet loss detection. However, energy consumption is higher since acknowledgement is to be generated at each hop. End-to-End reliability mechanism is preferred in a network where the packet loss is generally low while Hop-by-hop reliability mechanism is preferred in case of networks where the packet loss is severe.

The acknowledgement itself can be of two types viz *explicit acknowledgement* or *implicit acknowledgement* (Figure 3).
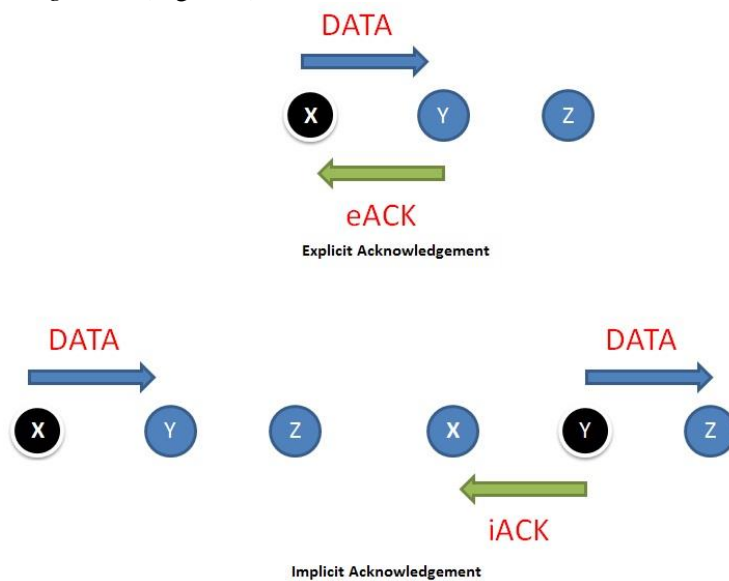

Figure 3. Explicit And Implicit Acknowledgement Mechanism

In former case, acknowledgement packet is generated by the immediate receiver of the packet for each received packet. In case of implicit acknowledgement, the receiver does not generate an acknowledgement for the received packet to its predecessor transmitter node. However when it transmits the packet to its subsequent neighbors, the predecessor node, being in its radio range hears the transmission and confirms receipt of the packet. Implicit acknowledgement is preferable since an additional packet need not be transmitted on receipt of every packet thus theoretically curtaining the number of transmission to half as compared to explicit acknowledgement. The acknowledgement mechanism, though contributing to the enhancement of reliability does create a peculiar situation when the acknowledgement packet itself is lost. This may induce duplicate re-transmissions even though the packet is actually received by the immediate receiver. A combination of

explicit and implicit acknowledgement mechanism is the answer to increasing reliability and simultaneously curtailing the duplication of transmitted packets as demonstrated in [20].

The information lost during the multi-hop propagation to the sink can be recovered either by *re-transmission* of the lost part of the information i.e. re-transmission of lost packet or by using advanced data recovery or redundancy techniques. As is obvious, re-transmission of packet leads to energy loss while data recovery techniques are expected to be computation intensive.

Based on these fundamental elements of reliability it is possible to provide a framework for categorizing the techniques proposed by various researchers to improve upon the reliability of the WSN. The proposed framework for categorization is available in Figure 4.
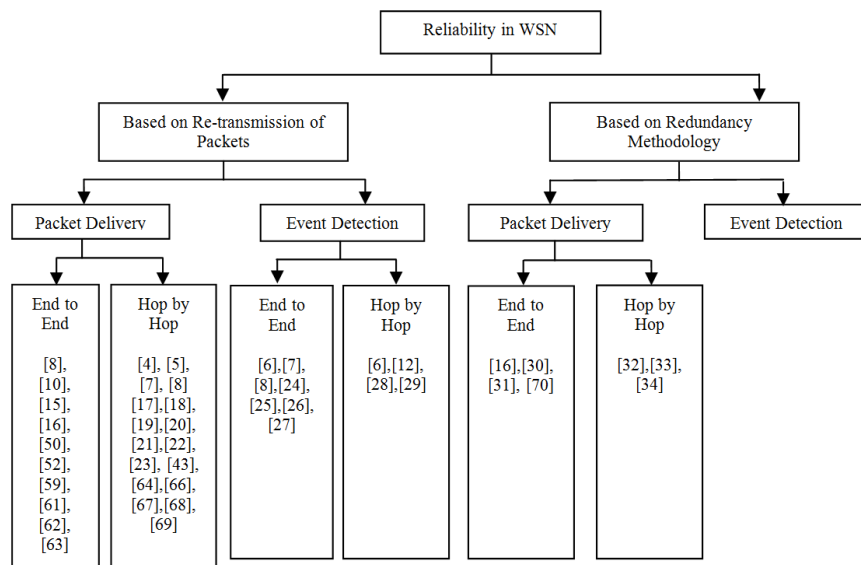
Figure 4. Categorization of Technique for Reliability in WSN

As can be observed, the categorization takes into account the various fundamental elements that go into design of various techniques

3. Retransmission Based Packet Delivery, End to end Reliability Techniques

In case of loss of a packet, during the multi-hop journey from the source node to the sink, the simplest technique for ensuring zero loss of data is to have the source node re-transmit the lost packet. Loh *et al.* [52] proposed EAR, a light-weight protocol requiring low-control overheads to handle a changing topology caused by unreliable RF links and thus maintaining reliability of acquisition. The protocol assumes availability of IEEE 802.11 [48] MAC layer with explicit control messages (RTS, CTS, ACK) to detect loss of messages. Multiple sinks are supported. Routing table is used to store route information for immediate neighbors which may have a route to the sink. Metric called *RouteScore* which depends upon energy level, transmission success rate and weight-age factors is used to remove routes from table to reduce table size. Theoretical proof for guaranteed delivery in connected network is provided assuming no noise and faulty environment. Simulation results and comparison against AODV, DSR & GBR have been shown. It is assumed that each node will have at-least 10 neighbors to choose from. With 50-400 nodes, the protocol demonstrates high PDR of 0.95-1.00, latency of < 0.1 s and low energy consumption. The algorithm has low control overheads and query dissemination

is not supported. Congestion detection is not available and there is no focus on reducing latency. Further energy efficiency is not considered while making routing decisions.

Yuan *et al.* [59] proposed, Energy Efficient Real-Time Routing Protocol for WSN, specifically for reducing the latency time of the network. Effective forwarding ensures that forwarding nodes are always farther from source node and closer to destination nodes thus ensuring proper gradient. Constrained Equivalent Delay (CED) values are calculated at each node and choice of next hop is made based on this value for reducing latency. Thus the decision making at each node, in terms of selecting the next node for forwarding, is done based on the energy requirement for the current hop and not overall energy. Simulations indicate significant reduction in latency due to the methodology of selection of forwarding nodes and the energy consumption is also low as compared to SPEED, GRS & MFR. However, the reliability of the protocol is as low as 20% if the number of participating nodes is less than 100 and reaches values greater than 80% only when the number of deployed nodes is more than 200. Computational complexity is very high, fault tolerance is low and no mechanism for detection of congestion in the network is available.

Soyturk *et al.* [10] proposed, Reliable Real-Time Data Acquisition for Rapidly Deployable Mission-Critical WSN, based on the Stateless Weighted Routing [60] which creates multiple data paths between source and sink to improve upon the reliability of data acquisition. These routes are created on-demand and are not stored in any table beforehand while requiring no knowledge of the neighbor nodes. Weight values are calculated to for each node based on geographical location and specific QoS parameters which serve as gradient for packet propagation towards sink. A QoS parameter field is added as a part of the header which is used to control the number of paths to be created, assign priority of re-transmission to the current packet and for making urgent transmissions. Simulations results show that energy consumption is low, complexity and computational overheads are low since the number of alternate routes created is controlled while reliability is maintained since alternate routes do exist. The methodology does not support multiple sinks and the authors are silent about how duplicate packets arriving from multiple routes are handled by the nodes in-between and the sink.

Karim *et al.* [50] proposed LFCP-MWSN, a protocol which is a location-aware and fault tolerant clustering protocol for mobile WSN, that is not only energy efficient but also reliable. Based on the cluster approach, it incorporates a simple mechanism to localize a node when it enters a cluster or moves into a new one. It assumes that all nodes are mobile and that at-least one node in each cluster, called an Anchor, has a GPS for finding out the location. The authors propose a simplistic methodology for finding the position of each un-localized node provided it is able to hear the beacon from an anchor which is mobile and transmits a beacon broadcasting its position. The localization information is useful since every cluster is aware of joining and leaving of a node and the position of the node within the cluster. The mechanism also detects the failure of a node and thus is fault-tolerant. However, the mechanism does not support multiple-sinks, does not consider network latency, has not network congestion detection mechanism and has high control overheads.

Cross-layer protocols have also been proposed by researchers with the intent to optimize performance of multiple parameters. Di Marco *et al.* [61] proposed, dynamic energy-efficient protocol for reliable and timely communication for WSN in control and automation, a cross layer protocol combining deterministic and random approach to ensure data communication in a WSN. All the relevant characteristics of the physical layer, MAC, routing, duty cycle policy and load balancing are used to ensure guaranteed data communication in a network with adaptation to suit particular application of a WSN. The solution to an optimization problem is sought which takes into account the energy factor and reliability factor. The flexibility is added by varying TDMA cycle for different types of application scenarios. Simulations done on Tmote sky with TinyOS showed that

the protocol achieves approximate reliability factor of 0.95 for different TDMA cycles with timely transmission of packets, ensuring low node duty cycle and a longer network lifetime, with dynamic adaptation to the application requirements.

He, Stankovic, Lu, & Abdelzaher [62] proposed a real-time **cross layer** communication protocol for sensor networks, called SPEED. The protocol provides three types of real-time communication services, one, meant for reporting activity in one part of network to the other (real-time unicast), second, meant for multiple communications from multiple nodes to a base station (real-time area-multicast) and lastly meant for reporting event by any node in case the information has high redundancy (real-time area-anycast). The protocol uses location information of the neighboring nodes to reduce memory requirement. The delay estimation is done by using time stamps on the data rather than sending probes for this purpose. In SPEED, a combined network and MAC layer congestion control scheme is used. The end to end delay reported is approximately 150 ms for network with congestion up to 90%, which is far lesser than AODV and DSR. The SPEED protocol does not use flooding as in AODV or DSR instead it forms the reliable path between nodes for reliable data communication; therefore the energy consumption is also less than the other two techniques. Theoretical analysis, simulation experiments and a real implementation on Berkeley motes are provided by the authors to validate their hypothesis. The protocol can't detect congestion and assumption of nodes being location aware is a big challenge in implementation.

Iyer *et al.* [15] proposed a mechanism for reliability of data acquisition (STCP) where the sink plays a significant role in implementing various functionalities. The methodology assumes synchronization of clocks of all nodes with that at the base station. The reliability is assured by informing the sink about the transmission rate, number of streams and expected reliability flow of the packet to be sent by the node before the data packet is actually sent by sending a special packet called the Session Initiation Packet. The node sends the actual data packet only after receiving an acknowledgement from sink in response to Session Initiation Packet. Since sink knows the data rate and data size it can calculate the Estimated Trip Time for the actual data to arrive from node failing which it generates a NACK to the node which will re-transmit the data thus ensuring **end-to-end reliability**. The protocol provides the application the capability to choose the degree of reliability required. Congestion detection mechanism is also incorporated as each data packet sent forwarded by every node also contains information about the congestion status of the node. The sink, on receiving this, informs the source which can either choose an alternate path or reduce rate of sending packets. Simulation results obtained by the authors over a 2 Mbps radio link with simple CSMA CA MAC and 50-100 nodes located at a distance of 10 m from each other indicate that the chosen degree of reliability can be attained with a latency of less than 2.5 s. Although the latency figure appears good however, in context of a 2 Mbps link it is actually poor. Moreover the control overheads are significantly high in terms of energy spent while meeting the assumption that the clocks of all nodes are synchronized is difficult to attain and requires spending significant amount of energy.

Another technique which focuses on **end to end reliability** was proposed by Kim et al. [63] entitled Flush, a procedure which adapts according to the variable time conditions of the Wireless Sensor Network for transferring bulk data with high end -to- end reliability. The sink coordinates the transfers in the network using control protocol. After the sink sends the request for a data object, the proposed protocol, Flush goes through four stages, namely, topology query stage, data transfer stage, an acknowledgment stage and checking of data integrity stage. To achieve reliability, the end-to-end selective negative acknowledgments and retransmission methods are applied. Using local measurements and an estimation algorithm, Flush computes the available path's bandwidth and notifies this rate to the nodes falling between the bottleneck and the destination. It also computes maximum rate to let the nodes stay away from intra-path obstruction. The packets use

multiple hops to reach to a distant destination. Except for the requirement of stable bidirectional links, Flush doesn't impose any other restriction on chosen path.   The experiment work written in nesC was carried on Tiny OS. Different network scenarios were considered by varying the number of nodes on different topologies to test the adaptability of the protocol to network changes. Simulation results for 48 hop network on MicaZ platform show very low storage overheads in RAM and ROM. The reduction in transfer time is also achieved in the proposed scheme. The algorithm shows a significant improvement in total amount of data collected in lesser amount of time. However, the complexity of Flush seems quite high. Flush can adapt to the change in route found by the routing algorithm but cannot adopt to change in topology altogether.

Alam *et al.* [8], proposed CRRT which is a **cross-layer design** with MAC, Network & Transport layer. It is designed as hop-by-hop and end-to-end upstream reliable and congestion control transport layer protocol for WSN. CRRT provides an efficient MAC layer retransmission method to increase the hop-by-hop reliability. CRRT is based on reservation-based retransmission mechanism, in which the sender reserves the medium to retransmit a packet to the receiver. CRRT makes use of explicit positive and negative acknowledgement and retransmission of packet occurs only when the packet is dropped due to collision or wireless link error and if the sender does not receive the ACK. End-to-end acknowledgment of the sent packets is used to establish 100% reliability of packet delivery. Packet loss is detected at destination based on the sequence number of the packet, in which case the destination sends an NACK to source which retransmits the packet. It uses congestion avoidance technique to avoid unnecessary packet dropping and thus tries to detect the incipient congestion. The level of congestion is measured by using both buffer occupancy and the forwarding rate of the node. Sink node is responsible for controlling the congestion and the rate of every source node based on the Congestion Notification (CN) of the intermediate nodes. The mechanism has high complexity associated with it and implementation is difficult.

The techniques discussed so far have focussed only on ensuring the delivery of packets and end to end reliability. The detection of loss of packets is done at the destination and retransmission is affected by the source node. In most cases there is no overt focus on reducing the network latency and many times the protocol design is so computationally complex that implementation is not practical. Some techniques have used cross layer design to achieve better cooperation among the layers and obtain better results; however, this does create the problem of not adhering to a particular, globally accepted protocol. Some techniques have prerequisites like knowledge of topology, knowledge of location etc. which make implementation difficult. The obvious disadvantage of using end to end reliability in noise prone environment is also a factor in not focussing on reduction of network latency since achieving this is highly unlikely if detection of lost packet is done at destination and recovery maintained with source re-transmission.

4. Retransmission Based Packet Delivery, Hop by Hop Reliability Techniques

Another approach to ensuring a high packet delivery ratio is by achieving reliable delivery at every hop *i.e.* hop-by-hop reliability where confirmation of receipt of packet at every hop is ensured. Wan, Campbell & Krishnamurthy [4] approached the issue of reliability of Data Acquisition in Wireless Sensor Networks by proposing "PSFQ – Pump Slow Fetch Quickly" a transport mechanism which focuses on ensuring best case delivery of every packet of information generated by each node to its destination. Authors assume that packet may be lost only because of lossy wireless environment. Source nodes insert information into the network at a slow rate but in case any intermediate node detects a loss of packet, based on receipt on unique sequence number of packets, then it fetches the lost packet by communicating at a fast rate with its neighbour nodes who may have

received a copy of the lost packet and may not have transmitted the same. PSFQ focuses on **hop-by-hop reliability** and not on end to end reliability between the source and destination nodes with no focus on network latency. Negative acknowledgement along with fast Fetch and Report mechanism enables it to detect loss of packet and initiate the fetch sequence from its neighbours. Simulation results obtained by the authors over a 2 Mbps radio link indicates good packet delivery but network latency is in range of 5 – 10 s even with such high bandwidth. Memory, communication & control overheads are high.

Dai *et al.* [5] proposed a soft QoS based high reliability multi-path routing scheme primarily for ad hoc wireless networks entitled Proactive Route Maintenance Protocol [PRM]. PRM depends upon the concept of *communication locality* in ad-hoc networks which is used to conclude that most of the communication occurs on a small set of routes called Active Routes which are optimal in nature while the sub-optimal routes are called Passive routes. Active Routes are refreshed frequently to maintain freshness while the Passive Routes are used only when the Active routes have failed. The protocol uses the watermarks at each node to indicate gradient along the path to the destination with frequent updated for active nodes. PRM guarantees conditional loop freedom and supports multi-sink operation. Simulation using 50 nodes with IEEE 802.11 PHY & MAC with limited mobility of nodes indicates slight improvement in packet delivery ratio and significant reduction in network latency with low route discovery overheads viz z viz AODV. Control and maintenance overheads are quite high.

Le *et al.* [20] proposed Energy Efficient Reliable Transport Protocol (ERTP), a mechanism for significantly improving **end-to-end reliability** while simultaneously achieving significant reduction in energy consumption at the nodes. ERTP assumes low sampling rate and low power listening mechanism support by MAC. ERTP consists of two components viz hop-by-hop reliability, and hop-by-hop retransmission timeout (RTO). End-to-end reliability is maintained by hop-to-hop reliability at each node which controls dynamically the number of re-transmissions at each node. The balance between energy efficiency and reliability is maintained by optimizing the number of re-transmissions. ERTP uses Implicit Acknowledgement and assumes that congestion does not exist. The RTO is adjusted to optimize balance between ensuring network latency and energy consumption by the nodes. Simulation using 200 nodes shows that ERTP achieves an end-to-end reliability of 0.92-0.95; which declines rapidly with increasing sampling rate. Network congestion is observed when sampling rate is better than 1 sample per 5 s in lossy environment and better reliability is observed with explicit acknowledgement rather than with implicit acknowledgement. Implementation using Tmote nodes in TinyOS environment supports the theoretical analysis. The assumption made by ERTP regarding no congestions becomes invalid in such scenarios and the resultant degradation is clearly observed. Further network latency is not a core issue in ERTP.

Shaikh *et al.* [64] proposed Adaptive Reliable Information Transport Protocol (AReIT), for classification of services being offered by WSN. AReIT exploits the spatial and temporal redundancies in the network to achieve higher reliability. "Convergcast Reliability model" is proposed which calculates the number of transmissions required to achieve a specific degree of reliability based on issues like desired degree of reliability and number of hops assuming that probability of success across a single path is constant. Simulation results show that AReIT outperforms RBC (Reliable Bursty Convergcast) mechanism [65] on multiple counts including information transport reliability and network latency. However, the control overheads are high, number of re-transmissions is high and support for multiple-sinks does not exist.

Park *et al.* [66] propose a graphical routing concept based on virtual circuit which is used to ensure guaranteed transfer from source to destination with minimum energy consumption and delay between the nodes. The algorithm assumes that all nodes in network know their location priori and each node has location information about its

neighbor as well as the destination where data is to be sent. Further authors assume that data packet loss is more because of poor signal rather than data congestion. Three functional mechanisms of the proposed scheme guarantee data routing from source to destination. First, is virtual circuit construction which constructs fixed routing path using the routing table. Second, hop-by-hop control does the task of error detection and retransmission to guarantee the data transmission between nodes. Lastly to overcome the node failure in a virtual circuit due to any reason, the virtual circuit management reconstructs another route avoiding route with failed nodes. The simulation of the proposed protocol in 802.11b standard shows approximately 100% data delivery to destination up to 20 hops away from source. The energy consumption is also limited due to the fact that the protocol is not a multipath protocol as, therefore when compared to similar techniques, the factors like error rate in the nodes and number of hops in a network has limited effect on the energy consumption. The error rate of one hop transmission is varied from 0.1 to 0.2. However congestion control mechanism does not exist and there is no focus on reducing network latency.

Moustafa *et al.* [67] have proposed, MSR (Multipath Secure Reliable Protocol), a mechanism which not only improves the reliability of delivery but also simultaneously improves the reliability of secure data transfer. MSR improves security by dividing a packet into sub-packets, by using method called erasure-coding, and sends these multiple fragments via multiple paths which it has established beforehand. The re-construction of original message is done at the sink after receipt of the fragments. It uses On-demand Routing mechanism to establish multiple paths between the node and the sink. It further uses Passive acknowledgement mechanism which is based on passively listening to traffic with the objective of analyzing the security behavior of neighbors. The authors have analyzed the various types of security attacks observed in a Network and have shown that MSR can actually withstand most of them without compromising on the integrity of the data and performance of the network. Simulation results using 50-200 nodes in IEEE 802.11 environment have been presented by the authors who demonstrate that Average end-to-end delay varies between 0.5-3.5 s and reduces significantly with increase in size of the packet especially if packet length is more than 32 bytes. The average packet delivery ratio is between 0.85-1 in absence of any hostile attacks but reduces to about 0.8 in face of security threats. However, it outperforms against AOMDV which has been used for comparisons. The mechanism has been designed to work for a single-sink approach and does not detect congestion.

Sahu *et al.* [68] present a multipath routing protocol for Ad-hoc networks using the Leaf Routing mechanism with the objective of improving the reliability of delivery in ad-hoc networks. The proposed Multi Path Routing with Re-coil (MRRecoil) mechanism identifies a main routing path for normal transmission of information and falls back on alternate routes only in case of failure of this route. A leaf is formed of all the nodes falling between a source and destination node. When the delivery of packet fails on the primary route then the nodes which are a part of the leaf are intimated and store the packet. However, they back-off for some time and then decide to either transmit the packet or re-coil.

Chipara *et al.* [69] present a Real-time Power-Aware Routing (RPAR) protocol based on dynamic power adaptation and selection of appropriate neighbor. Authors through experiment observed that for a fixed distance, increasing the power increases the packet velocity. It happens because number of retransmission required will be less if link quality is increased as a result of increase in the power of transmission. A tradeoff between the communication delay, energy consumption, and network capacity is achieved by modulating the transmission power based on required communication delays. In case of high priority data, RPAR increases power to have shorter communication delay while transmission power is reduced in case of normal priority data. A neighbourhood manager dynamically discovers the eligible neighbour for data forwarding and uses two strategies

for desired reliability in a WSN. First is power optimization, in which power is modulated to increase data velocity if it is not achievable using current power level. Second is when power adaption cannot achieve required data velocity, neighbour discovery is done, where the neighbours are discovered and the ones which satisfy the current data velocity requirement are selected. Simulation done in MATLAB based simulator show that RPAR achieves a miss ratio of approximately 0.2 in a network with deadline of 150 ms. The miss ratio close to 0 is achieved when deadline is increased to 350 ms. Energy overhead is also very small *i.e.* about 5 mj/packet and remains constant with respect to deadline indicating uniform energy depletion. The method has high computing overheads, does not consider congestion and has low energy efficiency.

Shaikh *et al.* [21], propose TRCCIT, a transport mechanism which provides the ability to tune the reliability depending upon the congestion in the network under different network conditions. It makes use of localized hybrid acknowledgement (HACK) mechanism and a timer management system, where HACK is a combination of implicit and explicit acknowledgement. Implicit acknowledgements are used as the main source of acknowledgement; however, the next hop neighbor, after receiving the information from the sender, can send an eACK to the sender to stop unnecessary retransmissions. The adaptive retransmission timeout mechanism is based on the buffer occupancy and balancing the number of incoming and outgoing messages at each node. TRCCIT efficiently monitors the information flow and adapts between single path and multiple paths in order to alleviate congestion such that desired application reliability is maintained. TRCCIT provides reasonable reliability and also addresses issues like hybrid acknowledgement, time bounds and energy efficiency with dynamic network conditions. Simulation results indicate that the mechanism is able to adapt its performance based on the changing network conditions as hypothesized by the authors.

Alimohammadi *et al.* [43] proposed a Multipath Routing mechanism for MANETS with focus on improving reliability of Data Delivery, in face of frequent change of topology and high probability of communication and node failure, thus reducing routing overheads. The mechanism introduces two parameters namely Node Reliability (NR) and Path Reliability (PR). Node reliability is an indicator of the connectivity of a node in upstream and downstream direction with a high NR indicating better connectivity and therefore higher reliability. Similarly Path Reliability is an indicator of the reliability of a specific path out of the multiple-paths that may exist between a node and a sink and is also dependent upon the NR of the nodes in the path. A table containing the multiple-paths is maintained and the selection of a route at any time is done based on the ratio Path Reliability / Number of hops with the objective of improving reliability of delivery while simultaneously reducing the network latency time. Simulation using 50 mobile nodes in an IEEE 802.11 PHY-MAC layer environment is done and comparisons are made against the performance of AOMDV. It is observed that proposed algorithm outperforms AOMDV in terms of Packet Delivery Ratio and network latency time. However, high control overheads, computational complexity, storage overheads and significant energy consumptions are the trade-off against improvement in reliability and latency.

Chen *et al.* [73] proposed a performance guaranteed routing protocol for asymmetric networks where the focus is on reliable delivery of packet from node to sink or vice-versa in asymmetric networks i.e. where the routes in both the directions may not be same. The authors introduce the concept of Reverse Path, a mechanism which finds the reverse paths for asymmetric networks. The authors use the concept of dividing the deployed nodes into layers and provide algorithm for calculating the optimized number of layers. Packet Delivery Rate of 99% is deemed to be achieved by the authors based on simulations, however significant focus is not available on reducing network latency.

5. Retransmission Based Event Detection, Hop by Hop Reliability Techniques

Ensuring that each packet transmitted by the source nodes reaches the sink is one way of establishing reliability of reconstruction of the event. However, this requires a significant amount of wastage of time and energy in the form of re-transmissions whenever a packet is lost. Reliable event detection does not put such a stringent packet delivery requirement on the network. In case an event has been sensed by a set of nodes then all the packets transmitted by these nodes need not mandatorily reach the sink; a specified number of delivered packets may be enough for the sink to re-construct the event.

Zhou *et al.* [28], proposed a mechanism entitled PORT (Price-Oriented Reliable Transport Protocol) and argued that the rate of incoming packets was not the correct measure of the reliability of the network and the contribution of a node's data towards the estimation of an event at the sink must also be considered. Therefore the reliability would depend upon the incoming data rate as well as the application related information. PORT is specifically designed for event-driven data flow and the main focus is on reducing the energy consumption at the nodes. Authors define *Node Price* as a factor for measuring the energy cost, including re-transmissions, for sending information from a node to sink. PORT targets congestion as the single most important factor leading to low reliability and provides two mechanisms to counter congestion. The first method, in-network-congestion-avoidance-method, suggests that each node makes use of information about *Node Price* factor of each of its neighbours to choose neighbours with least likelihood of getting congested. The second mechanism, end-to-end-rate-adjustment-mechanism, suggests that as the sink gets information about congestion at a particular node, it asks the node to reduce its reporting rate to avoid congestion. Simulation results for a deployment of 100 nodes in an IEEE 802.11 PHY & MAC layer environment indicated about 10-30% reduction in energy consumption at the nodes for a varying rate of un-certainty, as against a mechanism where above mentioned adjustments are not done. PORT does not factor in issues like Latency of the Network, multi-sink applications etc.

Mahmood *et al.* [29], proposed Event Reliability Protocol (ERP), whose objective is to provide reliable delivery of information regarding event occurrence to the sink. Authors have proposed a spatio-temporal correlation mechanism to ensure that packets containing information about same event are not transmitted thus reducing traffic. This reliable transmission of unique events to the sink is performed with the help an intelligent region-based selective retransmission mechanism. Apart from minimizing the transmission of unnecessary duplicate packets containing similar event data, ERP uses implicit acknowledgement to reduce traffic. ERP is not sink centric and performs in-network data processing to reduce congestion & energy consumption. The mechanism has no focus on reducing network latency, is computationally intensive and has low fault tolerance.

6. Retransmission Based Event Detection, End to End Reliability Techniques

Akan *et al.* [6] proposed, Event to Sink Price Reliable Transport (ESRT), a methodology to achieve reliable event detection, with congestion resolution capability, while incurring minimum energy. The focus is on achieving reliable event detection using overall information gathered by nodes. The authors model the reliability problem by defining the rate of reporting frequency of nodes and the actual number of packets received at the sink within a specific time interval. Based on this the reliability of event detection is calculated. It is observed that as the reporting frequency increases the reliability of event detection increases too; however, after a specific reporting frequency the reliability drops since network is unable to handle the large injection of packets. ESRT uses a congestion detection mechanism based on local buffer level monitoring in

sensor nodes. A CN bit in the header is used by the node to intimate the sink about buffer overflow congestion faced by a node. The sink then changes the reporting frequency to achieve the reliability required. Analytical results show improvement in reliability based on the reporting frequency and the congestion mechanism. However, the mechanism is not designed for multiple-sink applications, does not focus on network latency and has high control overheads.

Gungor *et al.* [24] presented Delay Sensitive Transport (DST), a transport mechanism whose focus is on ensuring that the information sensed by the deployed nodes reaches the sink reliably and within specified time-constraint with minimum energy constraint. Major focus is on ensuring time bound delivery of event action to the sink. The authors identify buffer delay as the main contributor towards network congestion and also the most easily controllable parameter since this can be controlled to an extent by reducing reporting frequency. Assumption is made that propagation time per hop is constant. The protocol introduces the *Time Critical Event First* scheduling policy which assigns higher priority to packets with lower time to deadline values thus ensuring that such packets are transmitted first from the buffer. Congestion detection at each node can be done by checking its average delay and buffer overflow count. On detecting congestion, sink is intimated by setting the Congestion Notification bit in the packet header, which on receipt of this information and other factors, reduces the reporting frequency of the nodes. Simulation results for a deployment of 200 nodes in an IEEE 802.11 PHY & MAC layer environment show that the end-to-end delay is reduced significantly till a critical reporting rate is reached after which the delay-constrained reliability reduces significantly and the end-to-end delay increase significantly. Mechanism proposed does not focus on event reliability, is not energy-aware and does not support multiple-sinks.

Tezcan *et al.* [25] proposed an asymmetric and reliable transport (ART) mechanism for wireless sensor networks. Specific nodes are identified as E-nodes and function as cluster heads. These cluster heads work in a collaborative manner to provide reliable data acquisition as well as query dissemination. Nodes with high balance battery energy are chosen as E-nodes. ART uses explicit acknowledgement techniques (eACK & NACK) for data collection and query dissemination reliability. Congestion and traffic control is implemented by the E-nodes for improving reliability which makes it untenable to recover lost packets for other nodes. In case the ACK packet is not received within the time-limit, ART assumes that the delay is because of congestion. However, the ACK packet may have got lost because of other reason as well, thus congestion detection mechanism is not accurate. As with other clustering mechanisms, the cluster formation, maintenance and inter-communication between the E-nodes is energy intensive. Therefore, sacrificing energy efficiency in the trade-off between network scalability and energy consumption might not be a suitable choice for a resource constrained WSN.

Gungor *et al.* [7] proposed Real Time Reliable Transport protocol for WSAN (RT)^2 a methodology for simultaneously addressing congestion control and timely event transport reliability objectives in WSANs. The stated objective is to reliably deliver the detected event to the sink within a specific time constraint so that WSAN can take correct decision. The authors have defined delay constrained reliability indicator for data transfer between sensor nodes and Actors and a separate reliability indicator for communication between Actors. The protocol proposes a *combined congestion detection* mechanism which checks the average node delay and buffer overflow to detect congestion. The protocol is similar to [24] and has been suggested by the same set of authors. Like [24] it uses the *Time Critical Event First* scheduling policy which assigns higher priority to packets with lower time to deadline values thus ensuring that such packets are transmitted first from the buffer. Also each node can detect its congestion level by checking its average delay and buffer overflow count. On detecting congestion it informs the sink by setting the Congestion Notification bit in the packet header which on receipt of this information and

other factors reduces the reporting frequency of the nodes. For Actor-Actor communication Actor mobility is assumed.

Simulated results indicate good reliability and low network latency as in [24] and low latency for Actor-Actor communication. However, the protocol has high control overheads although the network latency is low.

Xue *et al.* [26] proposed Loss-tolerant reliable event sensing protocol (LTRES), an end-to-end event reliability protocol which is optimized for applications which have varying reliability requirements over multiple event areas in a WSN. It is sink centric and uses a simple congestion control mechanism controlled by the sink. The mechanism can't however recover lost packets and reliability for general nodes is low.

7. Redundancy Based Packet Delivery, Hop by Hop Reliability Techniques

Wen *et al.* [32], proposed transmission reliability in sensor networks (TRSN), a redundancy based protocol which improves packet delivery reliability. TRSN checks the packet arrival probability and compares it against the required reliability to arrive at the reliability figure. The Gilbert model, which was originally designed for a single-hop channel, is utilized for modeling the loss behavior with the assumption that the two-state Gilbert model can be utilized at each hop. The successful packet arrival probability through multiple (n) hops and average energy consumption for a successful packet arrival is theoretically calculated and analyzed for simple transmissions, retransmissions and erasure coding mechanisms. The authors define a parameter called ULP which indicates the probability that a packet will be lost as the previous packet was also lost. The probability of successful arrival of a packet is compared against this parameter. The authors prove that the energy efficiency of erasure coding is better than the link-oriented retransmission mechanism as long as ULP value is below a certain threshold. However, in lossy environments, the performance of erasure codes is degraded significantly. The mechanism is highly computationally amd memory intensive.

Srouji *et al.* [33] proposed reliable erasure-coding based data transfer scheme (RDTS) for achieving hop by hop reliability. As erasure coding is computationally intensive, partial coding is also done to at each node as it also reduces erasure coding process overheads. This ensures that the receiver has received and transmitted enough data fragments required at the next hop for the reconstruction of the original message. Therefore, the encoding/decoding process is performed only when one or more original fragments are lost during the transmission. Thus, the overall cost of transmission is reduced due to lower processing overheads and reduced delays. RDTS shows good performance in terms of energy consumption, traffic overhead, load-balancing and network lifetime. RDTS calculates the number of fragments required at the next hop on the basis of probability of successful data arrival, which is assumed to be a random value predefined from 0.7 to 0.95. However, the overall performance of RDTS could be improved by calculating this probability dynamically, according to the varying network conditions.

Al Awami *et al.* [34] proposed data survivability decentralized erasure codes (DS-DEC) framework to estimate the amount of redundancy required for the data transmitted among the nodes in order to keep the network operational even in case of node failures. Underlying this framework, energy efficiency is maintained by proposing two coding mechanisms, DEC-Encode-and-Forward (DEC-EaF) and DEC-Encode-and-Disseminate (DEC-EaD) that utilizes Random Linear Network Coding (RLNC) mechanism. Data survivability is one of the key challenges addressed by DS-DEC, which intends to ensure the reliable transmission of data even if the node failure happens. DEC-EaF and DEC-EaD are implemented on the relay nodes in order for them to participate in the coding process while the data is transmitted towards the destination. In DEC-EaF, the source

node randomly chooses a storage node to forward the packet, where each relay node before forwarding the packet combines it with the encoded packet it stores locally. DEC-EaF works on the assumption that the source node has multiple routes to the destination. On the other hand, DEC-EaD eliminates the need of maintaining a routing table, as it works on the principal that source node transmits the packet using random walk mechanism. One of the main contributions of the DS-DEC is that it specifically calculates the energy required to perform encoding/decoding process.

8. Redundancy Based Packet Delivery, End to End Reliability Techniques

Ali *et al.* [30] proposed Optimum Reed-Solomon erasure coding (OREC) mechanism to achieve redundancy based packet reliability in a WSN. The source node creates and transmits the fragments of a packet using Reed-Solomon codes along multiple paths towards the sink where they are reconstructed. Genetic Algorithms are used to calculate the effort required to transmit the packet fragments under different network conditions. This information is used to optimize the number of fragments to be transmitted. This scheme assumes a situation where a query is to be disseminated in the WSN. The sink sends the query to its one hop neighbors termed prongs which further broadcast the queries throughout the network. Each receiving node in-between maintains information about the path through which it receives the query and later uses the same while sending information back in response to the query. The path chosen may be with shortest hops or higher reliability.

Authors indicate that reliability is increased with an increase in the number of additional redundant parity fragments; however, this does lead to an increase in the traffic. Thus optimization of the number of redundant bits is critical. The mechanism puts high computational overheads on the nodes as Genetic Algorithms being recursive in nature, require high degree of fast computations. Another important factor ignored in OREC is the consideration of a large-scale network with high hop count between the source and the destination. This may affect the overall performance of OREC, as the encoding/decoding is performed only at the source node and the sink, introducing a lot of entry points for errors. The need for relay nodes to keep track of the path to forward the response back to the sink, which raises memory concerns for the sensor node, especially if applied to large networks. The prong selection process seems to be pretty straight forward, but there is no backup process if a particular prong node fails. Moreover, the proposed scheme uses downstream query processing without introducing any downstream reliability mechanism.

Marchi *et al.* [16] proposed DTSN: distributed transport for sensor networks which provides an energy efficient non-sink centric end-to-end packet reliability protocol with a full and a differential reliability mechanism. Differential reliability mechanism can be used with an addition of a Forward Error Correction (FEC) technique. Differential reliability is supported by Enhancement Flow strategy as mentioned by authors. This technique can be used to transfer large block of data. Enhancement Flow along with the FEC technique is implemented separately that is independent of retransmission-based full reliability mechanism. Therefore, a higher degree of throughput and reliability is achieved as compared to full reliability strategy with the complete block transfer. DTSN utilizes FEC on an end-to-end basis, where a high hop count from source to destination increases the loss probability of data fragments, and consequently the destination will not be able to perform error correction completely. DTSN provides a mechanism to transfer the core part of data, but no information is available about the technique for determining the size of the core data or maintaining the high degree of reliability when the network conditions change. DTSN, however, does not have ample security for its reliability mechanism.

Dvir *et al.* [70] have proposed SDTP+: Securing a distributed transport protocol for WSNs using Merkle trees and Hash chains, where strong security mechanism has been

provided to ensure that reliability does not suffer because of security breach. The paper presents the objectives and challenges faced in achieving reliability in Wireless Sensor Networks and presents different perspectives to categorize the Reliability definitions and reliability enhancement techniques. The pros and cons of these techniques are also discussed. Table 1 indicates the categorization of various mechanisms proposed by researchers in the last decade for achieving reliability in Wireless Sensor Networks. It is observed that both retransmission and redundancy techniques aiming to achieve either packet or event level reliability perform better when using hop-by-hop method as compared to end-to-end method. It is believed that a hybrid combination of retransmission and redundancy based techniques using a combination of explicit and implicit acknowledgement

Table 1(a). Comparison & Categorization of Existing Protocols for Reliability in WSN

Loss Recovery Mechanism : *Retransmission Based* Objective : *Reliable Packet Delivery* Reliability : *End to End*								
Protocol / Mechanism	Congestion Detection	Network Latency	ACK	Complexity	Overall Reliability	Security	Fault Tolerance	Validati on *
CRRT [8]	Yes	Low	Implicit /Explicit	High	High	No focus	Good	S
RRTD [10]	No	Low	Explicit	Low	High	No focus	Good	S
STCP [15]	Yes	High	Explicit	High	High	No focus	Good	S
DTSN [16]	No focus	Average	Explicit	High	High	No focus	Good	S
LFCP MWSN [50]	No	High	-	High	High	No focus	Good	S
EAR [52]	No focus	Low	Implicit	High	High	No focus	Average	S
EERTRP [59]	No focus	Low	-	High	High	No focus	Poor	S
Di Marco [61]	No focus	High	-	High	High	No focus	Average	TB
SPEED [62]	Yes	Average	Explicit	High	High	No focus	Poor	S
Flush [63]	Yes	Low	Explicit	High	High	No focus	Average	S
Loss Recovery Mechanism : *Retransmission Based* Objective : *Reliable Packet Delivery* Reliability : *Hop by Hop*								
Protocol / Mechanism	Congestion Detection	Network Latency	ACK	Complexity	Overall Reliability	Security	Fault Tolerance	Validati on *
PSFQ [4]	No focus	High	Explicit	Low	High	No focus	High	S
PRM [5]	No focus	Average	-	High	High	No focus	High	S
RT^2 [7]	Yes	Low	Selective ACK	High	High	No focus	High	TB
CRRT [8]	Yes	Low	Implicit /Explicit	High	High	No focus	Good	S
DFRF [17]	No focus	High	-	Low	Average	No focus	Average	S
RTMC [18]	Yes	Low	-	Low	High	No focus	Good	TB
RBC [19]	Yes	Low	Implicit	High	High	No focus	Good	TB
ERTP [20]	No focus	High	Implicit /Explicit	High	High	No focus	Good	S
TRCCIT [21]	Yes	High	Implicit /Explicit	High	High	No focus	Good	S
RMST [22]	No focus	High	Explicit	High	High	No focus	Good	S
GARUDA [23]	No focus	Low	Explicit	High	High	No focus	Good	S
Park, Kim [43]	Yes	Low	-	High	High	No focus	Good	S
AReIT [64]	Yes	Low	Implicit	High	High	No focus	Average	S
HHCR [66]	No focus	High	-	High	High	No focus	Good	S
MSR [67]	No focus	Average	Passive ACK	High	Average	Yes	Average	S
RPAR [69]	No focus	Average	-	High	Average	No focus	Average	S
Chen [73]	Yes	Average	Explicit	High	High	No focus	Average	S

* S: Validation by Simulation, TB: Validation on Test-Bed

Table 1(b). Comparison & Categorization of Existing Protocols for Reliability in WSN

Loss Recovery Mechanism : *Retransmission Based* **Objective :** *Reliable Event Detection* **Reliability :** *End to End*								
Protocol / Mechanism	**Congestion Detection**	**Network Latency**	**ACK**	**Complexity**	**Overall Reliability**	**Security**	**Fault Tolerance**	**Validation***
ESRT [6]	Yes	High	-	High	High	No focus	Good	S
RT² [7]	Yes	Low	Selective ACK	High	High	No focus	High	TB
DST [24]	Yes	Low	-	High	High	No focus	High	
ART [25]	Yes	Low	Explicit	High	High	No focus	High	S
LTRES [26]	Yes	Low	Explicit	High	Low	No focus	Good	S
QERP [27]	No focus	-	-	Low	High	No focus	Good	S
Loss Recovery Mechanism : *Retransmission Based* **Objective :** *Reliable Event Detection* **Reliability :** *Hop by Hop*								
Protocol / Mechanism	**Congestion Detection**	**Network Latency**	**ACK**	**Complexity**	**Overall Reliability**	**Security**	**Fault Tolerance**	**Validation***
ESRT [6]	Yes	High	-	High	High	No focus	Good	S
LTCRDM [12]	Yes	Low	Explicit / Implicit	Low	High	No focus	Good	TB
PORT [28]	Yes	High	-	High	High	No focus	Good	S
ERP [29]	Yes	Low	Implicit	Low	High	No focus	Poor	S
ESRT [6]	Yes	High	-	High	High	No focus	Good	S

* S: Validation by Simulation, TB: Validation on Test-Bed

9. Conclusion

Any practical implementation of WSN or WSNA requires that the reliability of the network be high. Reliability and timeliness in the delivery of packets is imperative for ensuring practical initiating control action in response to an event being reported by a sensor network. However, the lossy nature of shared wireless medium results in excessive message loss and introduces delay. Congestion in the network also adds to the decrease in reliability. Any attempt to increase the reliability through end to end or hop by hop acknowledgments increases the delay inordinately. This mechanism also energy intensive and reduces the network lifetime.

Extensive literature survey shows that various techniques have been attempted to improve the reliability of sensor networks and these can be categorized as shown in Figure 4. A comparison of these techniques has been made and is available in Table 1.

It is observed that traditionally there has been more focus on improving the packet delivery mechanism such that more information is received at the sink. However, this generally requires re-transmission of the lost packets thus increasing energy consumption which is a great concern in WSN. Another issue related with re-transmissions is that of duplication of packets in the network as the previously sent packet may not actually have been lost. It is observed that including congestion control mechanism has a direct favorable impact on the packet delivery ratio and combination of this with retransmission mechanism helps significantly in reducing packet loss which further results in energy efficient operation of the network. It is further observed that using a combination of explicit and implicit acknowledgement may provide better reliability and energy efficiency in the network. It can be concluded that although redundancy based techniques are energy efficient, create less traffic and offer good reliability however, their computational complexity is a major deterrent to proper implementation as the nodes have low computational and memory capabilities.

Further Cross layer design has distinct advantages in maintaining reliability even when used with standard routing protocols. However, a cross layer design finds difficult acceptance since the lower layers tend to be non-standard layers.

Tufail *et al.* [72] have also demonstrated mathematically that backbone-assisted routing gives noticeably better reliability in comparison to traditional all wireless ad hoc routing. Thus a WSNA with wired Actuators serving as backbone, communicating wirelessly with the nodes, is likely to offer better reliability viz a viz the traditional all wireless adhoc routing. Future reliable, practical implementation of WSAN may take this into consideration.

It is also observed that a common algorithm set, providing high reliability for both upstream and downstream movement of information, are very few. A common algorithm set which can perform both the functions is highly desirable.

References

[1] M. Weiser, "The Computer for the 21st Century.", Scientific American, vol. 265, no. 3, (**1991**), pp**.** 94-104.

[2] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam and E. Cayirci, " Wireless Sensor Networks: A Survey", Computer Networks, vol. 38, (**2002**), pp. 393-422.

[3] I.F. Akyildiz and I.H. Kasimoglu, "Wireless sensor and actor networks: research challenges", Ad Hoc Networks, vol. 2, no. 4, (**2004**) October, pp. 351–367.

[4] C.-Y. Wan, A.T. Campbell and L. Krishnamurthy "Pump-slowly, fetch-quickly (PSFQ): a reliable transport protocol for sensor networks," IEEE Journal on Selected Areas in Communications, vol. 23, no. 4, April (**2005**)**,** pp. 862- 872.

[5] F. Dai & J. Wu, "A highly reliable multi-path routing scheme for ad hoc wireless networks.*",* International Journal of Parallel, Emergent and Distributed Systems, 20(3-4), 205-219, 2005.

[6] O.B. Akan & I.F. Akyildiz, "Event-to-sink reliable transport in wireless sensor networks,"IEEE/AM Transactions on Networking", vol.13, no.5, pp. 1003- 1016, Oct. 2005

[7] Gungor, V.C.; Akan, O.B.; Akyildiz, I.F., "A Real-Time and Reliable Transport (RT)2 Protocol for Wireless Sensor and Actor Networks," *Networking, IEEE/ACM Transactions on* , vol.16, no.2, pp.359-370, April 2008

[8] M.M. Alam & C.S. Hong, "CRRT: congestion-aware and rate-controlled reliable transport in wireless sensor networks." IEICE Transactions on Communications, 92(1), 184-199, 2009

[9] S. Gupta, S. Verma, R.K. Abrol & G.S. Tomar, "Intelligent industrial data acquisition and energy monitoring using wireless sensor networks.", International Journal of Grid and High Performance Computing (IJGHPC), 2(3), 44-59, 2010.

[10] M. Soyturk & D.T. Altilar, " Reliable real-time data acquisition for rapidly deployable mission-critical wireless sensor networks" In Proceedings of IEEE INFOCOM Workshops 2008"(pp. 1-6). IEEE.

[11] T. Bernard, H. Fouchal, S. Linck and E. Perrin, " Impact of routing protocols on packet retransmission over wireless networks.", Proceedings of IEEE International Conference on Communications 2013 , pp.2979,2983.

[12] S. Gupta, S. Verma and R.K. Abrol, "Layer Based Time Constrained Reliable Data Acquisition Mechanism for Wireless Sensor & Actuator Networks.", International Journal of Communication systems & Networks(IJCSN), 3(1), 9-20, 2014

[13] F. Adelstein, S.K. Gupta, G. Richard and L. Schwiebert, "Fundamentals of mobile and pervasive computing (pp. 1-2). McGraw-Hill.

[14] M.A. Mahmood, K.G. Seah Winston and I. Welch, "Reliability in wireless sensor networks: A survey and challenges Ahead", Computer Networks 79 (2015) 166–187

[15] Y. Iyer, S. Gandham,S. and S. Venkatesan, "STCP: a generic transport layer protocol for wireless sensor networks", Proceedings of 14th International Conference on Computer Communications and Networks (ICCCN), San Diego, California, USA, 17–19 October 2005,pp. 449–454.

[16] B. Marchi, A. Grilo and M. Nunes, " DTSN: distributed transport for sensor networks", Proceedings of the 12th IEEE Symposium on Computers and Communications (ISCC), Aveiro, Portugal, 01–04 July 2007, pp. 165–172.

[17] M. Maróti," Directed flood-routing framework for wireless sensor networks", Proceedings of the 5th ACM/IFIP/USENIX International Conference on Middleware (Middleware), Toronto, Canada, 18–22 October 2004, pp. 99–114.

[18] H. Zhou, X. Guan and C. Wu, " RTMC: Reliable transport with memory consideration in wireless sensor networks", in Proceedings of the IEEE International Conference on Communications (ICC), Beijing, China, 19–23 May 2008, pp. 2819–2824.

[19] H. Zhang, A. Arora, Y.R. Choi and M.G. Gouda, "RBC: reliable bursty convergecast in wireless sensor networks", in proceedings of the 6th ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc), Urbana-Champaign, Illinois, USA, 25–28 May 2005, pp. 266–276.

[20] T. Le, W. Hu, P. Corke and S. Jha, "ERTP: energy-efficient and reliable transport protocol for data streaming in wireless sensor networks", Computer Communication 32 (7–10) (2009) 1154–1171.

[21] F. Shaikh, A. Khelil, A. Ali and V. Suri, "TRCCIT: tunable reliability with congestion control for information transport in wireless sensor networks", in proceedings of the 5th Annual International ICST Wireless Internet Conference (WICON), Singapore, 01–03 March 2010, pp. 1–9.

[22] F. Stann and J. Heidemann, "RMST: reliable data transport in sensor networks", in proceedings of the First IEEE International Workshop on Sensor Network Protocols and Applications (SNPA), Anchorage, Alaska, USA, 11 May 2003, pp. 102–112.

[23] S.J. Park, R. Sivakumar, I.F. Akyildiz and R. Vedantham, "GARUDA: achieving effective reliability for downstream communication in wireless sensor networks", IEEE Tranactions on Mobile Computing,. 07 (02) (2008) 214–230.

[24] V.C. Gungor and O.B. Akan, "DST: delay sensitive transport in wireless sensor networks", in proceedings of the 7th International Symposium on Computer Networks (ISCN), Istanbul, Turkey, 16–18 June 2006, pp. 116–122.

[25] N. Tezcan and W. Wang, "ART: an asymmetric and reliable transport mechanism for wireless sensor networks", International Journal of Sensor Networks 02 (3–4) (2007) 188–200.

[26] Y. Xue, B. Ramamurthy and Y. Wang, "LTRES: a loss-tolerant reliable event sensing protocol for wireless sensor networks", Computer Communication, 32 (15) (2009) 1666–1676.

[27] H. Park, J. Lee, S. Oh, Y. Yim, S. Kim and K. Nam, "QERP: Quality-based event reliability protocol in wireless sensor networks", in proceedings of the IEEE Consumer Communications and Networking Conference (CCNC), Las Vegas, Nevada, USA, 09–12 January 2011, pp. 730–734.

[28] Zhou,Y.; Lyu,M.; Liu,J.,; Wang,H., "PORT: a price-oriented reliable transport protocol for wireless sensor networks", *in: Proceedings of the 16th IEEE International Symposium on Software Reliability Engineering (ISSRE)*, Chicago, Illinois, USA, 08–11 November 2005, pp. 10–126.

[29] M.A. Mahmood and W.K.G. Seah, " Event reliability in wireless sensor networks.", In 7th International Conference on Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP), *pp. 01–06.*

[30] 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, 16–19 October 2007, pp. 6–10.

[31] Kim,S.; Fonseca, R.; Culler,D.,"Reliable transfer on wireless sensor networks", in: Proceedings of the 1st Annual IEEE Communications Society Conference on Sensor and Ad Hoc Communications and Networks (IEEE SECON), Santa Clara, California, USA, 04–07 October 2004, pp. 449–459.

[32] Wen,H.; Lin, C.; Ren,F.; Yue,Y.; Huang,X., "Retransmission or redundancy: transmission reliability in wireless sensor networks", *in: Proceedings of the IEEE 4th International Conference on Mobile Adhoc and Sensor Systems (MASS),* Pisa, Italy, 08–11 October 2007, pp. 1–7.

[33] M.S. Srouji, Z. Wang and J. Henkel, "RDTS: a reliable erasure-coding based data transfer scheme for wireless sensor networks", in proceedings of the 17th International Conference on Parallel and Distributed Systems (ICPADS), Tainan, Taiwan, 07–09 December 2011, pp. 481–488.

[34] L. Al-Awami and H. Hassanein, "Energy efficient data survivability for WSNs via decentralized erasure codes", in proceedings of the IEEE 37th International Conference on Local Computer Networks (LCN), Clearwater Beach, FL, USA, 22–25 October 2012, pp. 577–584.

[35] M.C. Vuran, M.C.; Ô . B. Akan and I.F. Akyildiz, "Spatio-temporal correlation: theory and applications for wireless sensor networks.", Computer Networks 45, 3, 2004

[36] F. Osterlind, E. Pramsten, D. Roberthson, J. Eriksson, N. Finne and T. Voigt, "Integrating building automation systems and wireless sensor networks," in proceedings of IEEE Conference on Emerging Technologies and Factory Automation, 2007. ETFA., pp.1376,1379, 25-28 Sept. 2007

[37] M.P. Durisic, Z. Tafa, G. Dimic and V. Milutinovic, "A survey of military applications of wireless sensor networks," in proceedings of 2012 Mediterranean Conference on Embedded Computing (MECO), pp.196,199, 19-21 June 2012

[38] J. Lloret, M. Garcia, D. Bri and S. Sendra, "A wireless sensor network deployment for rural and forest fire detection and verification.", Sensors Journal, IEEE , 9(11), 8722-8747.

[39] L. Ruiz-Garcia, L. Lunadei, P. Barreiro and I. Robla, "A review of wireless sensor technologies and applications in agriculture and food industry: state of the art and current trends.", Sensors Journal, IEEE , 9(6), 4728-4750.

[40] Meng-Shiuan Pan; Lun-Wu Yeh; Yen-Ann Chen; Yu-Hsuan Lin; Yu-Chee Tseng, "A WSN-Based Intelligent Light Control System Considering User Activities and Profiles," Sensors Journal, IEEE , vol.8, no.10, pp.1710,1721, Oct. 2008

[41] V.L. Erickson, M.A. Carreira-Perpinan and A.E. Cerpa, "OBSERVE: Occupancy-based system for efficient reduction of HVAC energy*,"* in proceedings of 2011 10th International Conference on Information Processing in Sensor Networks (IPSN), pp.258,269, 12-14 April 2011

[42] A. Oka and L. Lampe, "Distributed target tracking using signal strength measurements by a wireless sensor network," IEEE Journal on Selected Areas in Communications*,* vol.28, no.7, pp.1006,1015, September 2010

[43] H. Alimohammadi and S.J. Jassbi, "A Fault Tolerant Multipath Routing Protocol for Mobile Ad Hoc Networks.", European Journal of Scientific Research, *85*(2), 317-326.

[44] M. Cardei, S. Yang, and J. Wu, "Algorithms for fault-tolerant topology in heterogeneous wireless sensor networks.", IEEE Transactions on Parallel and Distributed Systems, 19(4), 545-558.

[45] I. Maza, F. Caballero, J. Capitán, J.R. Martínez-de-Dios and A. Ollero, "Experimental results in multi-UAV coordination for disaster management and civil security applications." Journal of intelligent & robotic systems, 61(1-4), 563-585.

[46] A.N. Averkin, A.G. Belenki and G. Zubkov, "Soft Computing in Wireless Sensors Networks.", In EUSFLAT Conference (1) (pp. 387-390).

[47] Z. Ang, H. Jin, Z. Fan and Y. Duan, "WSN Node Design and Communication Realization Based on ZigBee Protocol", Journal of Modern Electronics Technique, *10*, 47-50.

[48] IEEE Standard for Information technology-- Local and metropolitan area networks-- Specific requirements-- Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications Amendment 8: IEEE 802.11 Wireless Network Management," IEEE Std 802.11v-2011 (Amendment to IEEE Std 802.11-2007 as amended by IEEE Std 802.11k-2008, IEEE Std 802.11r-2008, IEEE Std 802.11y-2008, IEEE Std 802.11w-2009, IEEE Std 802.11n-2009, IEEE Std 802.11p-2010, and IEEE Std 802.11z-2010) , vol., no., pp.1,433, Feb. 9 2011. doi: 10.1109/IEEESTD.2011.5716530

[49] F. Xia , "QoS challenges and opportunities in wireless sensor/actuator networks.", Sensors, 8(2), 1099-1110.

[50] L. Karim and N. Nasser, "Reliable location-aware routing protocol for mobile wireless sensor network.", Communications, IET, 6(14), 2149-2158.

[51] T. Camilo, C. Carreto, J. Silva and F. Boavida, "An energy-efficient ant-based routing algorithm for wireless sensor networks.", Ant Colony Optimization and Swarm Intelligence, 49-59.

[52] P.K.K. Loh, W.J. Hsu and Y. Pan, "Reliable and efficient communications in sensor networks.", Journal of Parallel and Distributed Computing, 67(8), 922-934.

[53] D. Bein, V. Jolly, B. Kumar and S. Latifi, " Reliability Modeling in Wireless Sensor Networks.", International Journal of Information Technology, Vol. 11 No. 2

[54] M. Katiyar, H.P. Sinha and D. Gupta, " On Reliability Modeling in Wireless Sensor Networks-A Review.", IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 6, No 3, November 2012

[55] R.F. Stapelberg, "Handbook of Reliability, Availability, Maintainability and Safety in Engineering Design." Springer-Verlag London

[56] S. Yan-qiang and W. Xiao-dong, "Jamming Attacks and Countermeasures in Wireless Sensor Networks.", In H. Jin, & W. Jiang (Eds.) Handbook of Research on Developments and Trends in Wireless Sensor Networks: From Principle to Practice (pp. 334-352). Hershey, PA: Information Science Reference. doi:10.4018/978-1-61520-701-5.ch015

[57] G. Lu, B. Krishnamachari and C.S. Raghavendra, "An adaptive energy-efficient and low-latency MAC for data gathering in wireless sensor networks," in proceedings of 18th International Parallel and Distributed Processing Symposium, 2004., pp.224,, 26-30 April 2004

[58] S. Dulman, T. Nieberg, Wu Jian and P. Havinga, "Trade-off between traffic overhead and reliability in multipath routing for wireless sensor networks," Wireless Communications and Networking, 2003. WCNC 2003. 2003 IEEE , vol.3, no., pp.1918,1922 vol.3, 20-20 March 2003

[59] L. Yuan, W. Cheng and X. Du, "An energy-efficient real-time routing protocol for sensor networks.", Computer communications, 30(10), 2274-2283

[60] M. Soyturk and T. Altilar, " Source-initiated geographical data flow for wireless ad hoc and sensor networks. In proceedings of IEEE Annual Wireless and Microwave Technology Conference, 2006. WAMICON'06. (pp. 1-5). IEEE

[61] P. Di Marco, P. Park, C. Fischione and K.H. Johansson, "A dynamic energy-efficient protocol for reliable and timely communications for wireless sensor networks in control and automation.", In Sensor, Mesh and Ad Hoc Communications and Networks Workshops, 2009. SECON Workshops' 09. 6th Annual IEEE Communications Society Conference on (pp. 1-3)

[62] T. He, J.A. Stankovic, C. Lu and T. Abdelzaher, "SPEED: A stateless protocol for real-time communication in sensor networks.", in proceedings of 23rd International Conference on Distributed Computing Systems, 2003. Proceedings. (pp. 46-55). IEEE.

[63] S. Kim, R. Fonseca, P. Dutta, A. Tavakoli, D. Culler, P. Levis and I. Stoica, " Flush: a reliable bulk transport protocol for multihop wireless networks.", in Proceedings of the 5th international conference on Embedded networked sensor systems (pp. 351-365).

[64] F.K. Shaikh, A. Khelil and N. Suri, "AReIT: adaptive reliable information transport protocol for wireless sensor networks.", in proceedings of ICWN 2009, pp-75-81

[65] H. Zhang, A. Arora, Y.R. Choi and M.G. Gouda, "Reliable bursty convergecast in wireless sensor networks.", Computer Communications, *30*(13), 2560-2576.

[66] H. Park, T. Kim, J. Lee, M.S. Jin and S.H. Kim, "Hop-by-hop control for reliable data dissemination in wireless sensor networks.", in proceedings of International Symposium on Autonomous Decentralized Systems, 2009. ISADS'09. (pp. 1-6). IEEE.

[67] M.A. Moustafa, M. A. Youssef and M.N. El-Derini, "MSR: A multipath secure reliable routing protocol for WSNs.", in proceedings of 9th IEEE/ACS International Conference on Computer Systems and Applications (AICCSA), 2011 (pp. 54-59). IEEE.

[68] R.K. Sahu, R. Saha and N.S. Chaudhari, " Fault Tolerant Reliable Multipath Routing Protocol for Ad Hoc Network.", in proceedings of Fourth IEEE International Conference on Computational Intelligence and Communication Networks (CICN), 2012 (pp. 117-121).

[69] O. Chipara, Z. He, G. Xing, Q. Chen, X. Wang, C. Lu and T. Abdelzaher, "Real-time power-aware routing in sensor networks.", in proceedings of 14th IEEE International Workshop on Quality of Service, 2006. IWQoS 2006. (pp. 83-92). IEEE.

[70] A. Dvir, L. Buttyan and Ta Vinh Thong, "SDTP+: Securing a distributed transport protocol for WSNs using Merkle trees and Hash chains.", in proceedings of International Conference on Communications, pp.2073,2078.

[71] F. Yunus, N.-S.N. Ismail, S.H.S. Ariffin, A.A. Shahidan, N. Fisal and S.K. Syed-Yusof, "Proposed transport protocol for reliable data transfer in wireless sensor network (WSN).", in proceedings of International conference on Modeling, Simulation and Applied Optimization (ICMSAO), pp.1,7, 19-21 April 2011

[72] A. Tufail, S.A. Khayam, A. Ali, W.A. Baig, F.M. Anwar, Ki-Hyung Kim and Seung-wha Yoo, " On the reliability of backbone-assisted end-to-end transmissions in WSNs.", First International Conference on Ubiquitous and Future Networks, pp.22,27

Authors

Sumeet Gupta, he received his B.E. in Electronics from University of Pune in 1993. He is currently working as an Assistant Professor at School of Electronics & Communication Engineering at Shri Mata Vaishno Devi University, Katra, India. He has extensive experience in product development in process industry. His area of research includes Wireless Sensor Networks & Embedded System Design and is currently pursuing

Ph.D. in Electronics & Communication Engineering at Shri Mata Vaishno Devi University.

Raj K. Abrol, he received his B.E. in Electrical Engineering from REC Srinagar, M.Tech from IIT Kanpur and Ph.D. from Indian Institute of Science, Bangalore. He has had a very long academic career and has also served as the founding Director of Center for Electronics Design Technology of India, J&K under DOT, GOI. His research areas include Power Electronics, Power Systems & Wireless Sensor Networks.

Shekhar Verma, he has received his PhD in Computer Sc. & Engg. from Banaras Hindu University, Varanasi, UP, India. Currently he is working as Associate Professor at Indian Institute of Information Technology, Allahabad, UP, India. His different research areas are, QoS provisioning for Service Level Agreements in IP networks, Development of QoS aware algorithms and Routing techniques for Multimedia transmission over the Internet and wireless networks.