# Reliability in Wireless Sensor Networks: A Survey and Challenges Ahead

Muhammad Adeel Mahmood, Winston K.G. Seah and Ian Welch

*School of Engineering and Computer Science, Victoria University of Wellington, Wellington 6140, New Zealand*

**Abstract**

Ensuring energy efficient and reliable transport of data in resource constrained Wireless Sensor Networks (WSNs) is one of the primary concerns to achieve a high degree of efficiency in monitoring and control systems. The two techniques typically used in WSNs to achieve reliability are either retransmission or redundancy.

Most of the existing research focuses on traditional retransmission-based reliability, where reliable transmission of data packets is ensured in terms of recovering the lost packets by retransmitting them. This might result in additional transmission overhead that not only wastes sensors' limited energy resources but also makes the network congested and in turn affects the reliable transmission of data. On the other hand, employing redundancy to achieve reliability in WSNs has received comparatively lesser emphasis by the research community [35] and this area warrants further investigation. In redundancy-based reliability mechanisms, a bit loss within a packet can be recovered by utilizing some form of coding schemes. This ability to correct the lost or corrupted bits within a packet would significantly reduce the transmission overhead caused by the retransmission of the entire packet.

Both retransmission and redundancy can either be performed on a hop-by-hop or an end-to-end basis. Hop-by-hop method allows the intermediate nodes to perform retransmission or redundancy. On the other hand, in the end-to-end approach, retransmission or redundancy is performed only at the source and the destination nodes. However, a hybrid mechanism with an efficient combination of these retransmission and redundancy techniques in order to achieve reliability has so far been neglected by the existing research. Depending on the nature of the application, it is also important to define the amount of data required to ensure reliability. This introduces the concept

of packet or event level reliability. Packet reliability requires all the packets from all the relevant sensor nodes to reach the sink, whereas event reliability ensures that the sink only gets enough information about a certain event happening. Thus retransmission or redundancy techniques using hop-by-hop or end-to-end mechanisms aim to achieve either packet or event level reliability.

This paper presents a survey on reliability protocols in WSNs. We review several reliability schemes based on retransmission and redundancy techniques using different combinations of packet or event reliability in terms of recovering the lost data using hop-by-hop or end-to-end mechanisms. We further analyze these schemes by investigating the most suitable combination of these techniques, methods and required reliability level in order to provide energy efficient reliability mechanism for resource constrained WSNs. This paper also proposes a 3D reference model for classifying research in WSN reliability, which will be used to perform in-depth analysis of the unexplored areas.

*Keywords:* wireless sensor networks, reliability, redundancy, retransmission

## 1. Introduction

Wireless Sensor Networks (WSNs) have been the preferred choice for the design and deployment of next generation monitoring and control systems [1, 2]. It has now become feasible to deploy massive numbers of low-cost sensors to monitor large regions over the ground surface, underwater or in the atmosphere [3]. The most significant benefit of sensor networks is that they extend the computation capability to the physical environment where human beings cannot reach [4]. They can operate for prolonged periods in habitats that are hostile, challenging or ecologically too sensitive for human visitation [5]. Moreover, they have the potential to provide a wealth of data about the environment in which they are deployed and deliver the data across the network to the end-users [6, 7].

At the heart of WSNs are the sensor nodes. A sensor node is a device that possesses sensing, computation and communication capabilities. Depending on their sensing components and the application requirements, sensor nodes can be used to monitor different phenomena like temperature, light, motion, pressure and humidity. The processing module of the sensor node is able to do computation on the sensed data and also on the data received from other sensors. The communication module in sensor nodes is used to send and receive the data packets to and from the neighbouring nodes [8]. Since a single sensor provides only limited information, a network of these sensors is used to provide coverage over large environments.

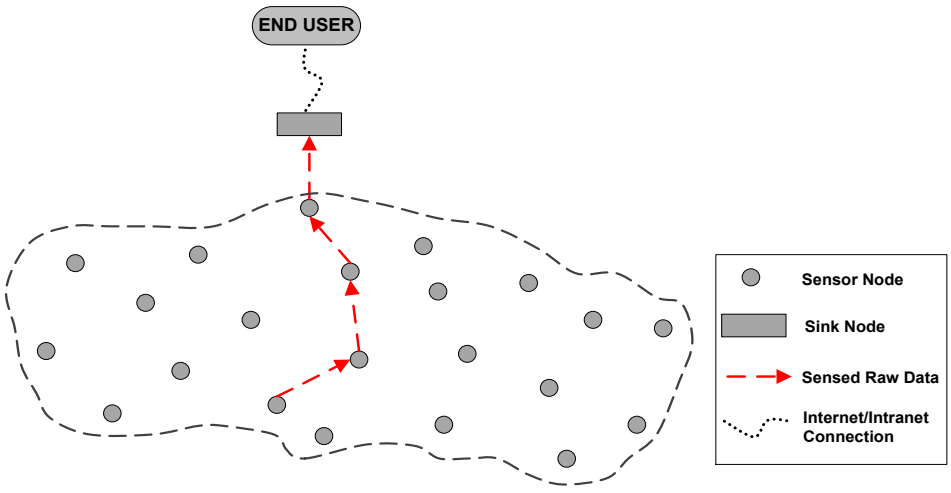


Figure 1: Wireless Sensor Network

Figure 1 shows a typical Wireless Sensor Network (WSN) comprising of several sensor nodes and a sink node. The sensor nodes continually sense data from the environment and send them to the sink node. In most scenarios, tens to as many as thousands of such sensor nodes are distributed throughout a region of interest, where they self-organize into a network through wireless communication and collaborate with one another to accomplish a common task [2]. The sink receives all the sensed data from these sensor nodes, processes them and sends them to the end user.

Due to the nature of traffic in WSNs, where all sensor nodes in the network forward their sensed data towards the sink, the area around the sink becomes more congested with all the traffic flowing towards and converging on the sink. In addition to losing packets through congestion, packets are also lost due to transmission errors, packet collision, interference, node failure (due to energy depletion) or other unforeseeable reasons. Furthermore, due to the short range of the sensor nodes, data might have to travel a large number of hops which, in turn, introduces a lot of entry points for errors that can also become the cause of packet loss. Thus, for successful monitoring of an environment, the critical data collected by the sensor nodes need to be reliably delivered to the sink, requiring the lost data to be recovered. Given the nature of error prone wireless links, ensuring reliable transfer of data from resource constrained sensor nodes to the sink continues to be one of the major challenges in the field of WSNs.

Various protocols have been proposed using different techniques to cope with the challenge of achieving reliability in wireless sensor networks. We investigate the methods involved in creating the overall reliability technique and find the best possible combination of the available options by introducing a three-dimensional (3D) reference model to categorize the work done on providing reliability in WSNs, as shown in Figure 2. In later sections, the 3D reliability reference model will be unfolded to perform in-depth analysis, pointing out the unexplored and efficient combination of the techniques to encounter the challenge of achieving reliability in WSNs. Existing data transmission reliability protocols belong mainly to one of two techniques which are retransmission or redundancy. These techniques ensure reliability by recovering the lost data using a hop-by-hop or an end-to-end method, while adopting either packet or event level reliability based on the application requirements. The terminologies used for these techniques and methods depicted in Figure 2 are defined as follows.

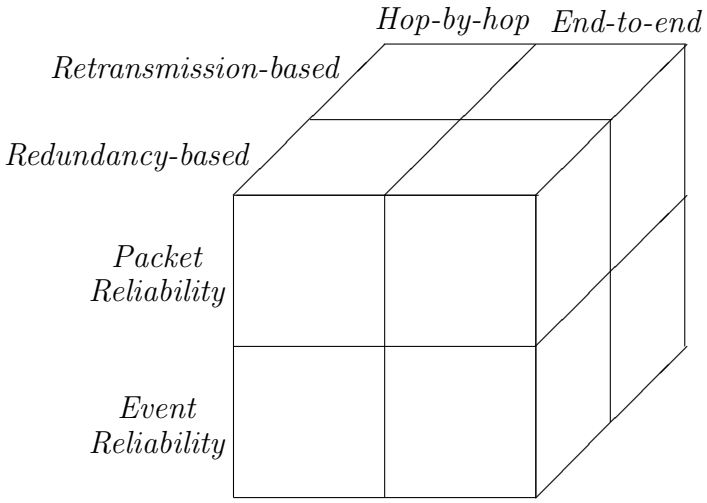


Figure 2: A Three-dimensional(3D) Reference Model for Research in WSN Reliability

### *1.1. Retransmission vs. Redundancy*

Retransmission is the traditional way of ensuring reliability, where the sender node after transmitting its packet, waits for the acknowledgment of its sent packet from the next hop node on the path to the sink. However, in case the sender does not receive any acknowledgments, it deems the sent packet has been lost. Thus, in order to ensure reliability, the lost packet needs to be retransmitted. On the other hand, instead of retransmitting the whole packet, the redundancy approach aims to correct only the lost or corrupted bits within the packet. The sender, adds some extra information to the packet that the receiver can use to reconstruct the packet if some bits are lost or corrupted. This extra information consists of additional redundant set of fragments that are encoded by employing a certain form of coding mechanism such as erasure coding. Further details are given in Section 3.

### *1.2. End-to-end (Connection-oriented) vs. Hop-by-hop (Link-oriented)*

Both retransmission and redundancy-based reliability techniques can be performed using a hop-by-hop or an end-to-end method. We refer to hop-by-hop as a link-oriented mechanism, as reliability needs to be maintained across every single link. In other words, in the hop-by-hop method, every single hop from source to destination is responsible for ensuring the reliable

transmission of the sensed data. Similarly, end-to-end method can be termed as connection-oriented mechanism, where only the two end points (i.e. only the source and destination nodes) are responsible for ensuring reliability, while the intermediate nodes simply relay the packets between the source and the destination.

### *1.3. Packet vs. Event level Reliability*

In a WSN, an event of interest can be described as a meaningful change in the state of the environment that the application users are interested in and require the sensors to observe it.

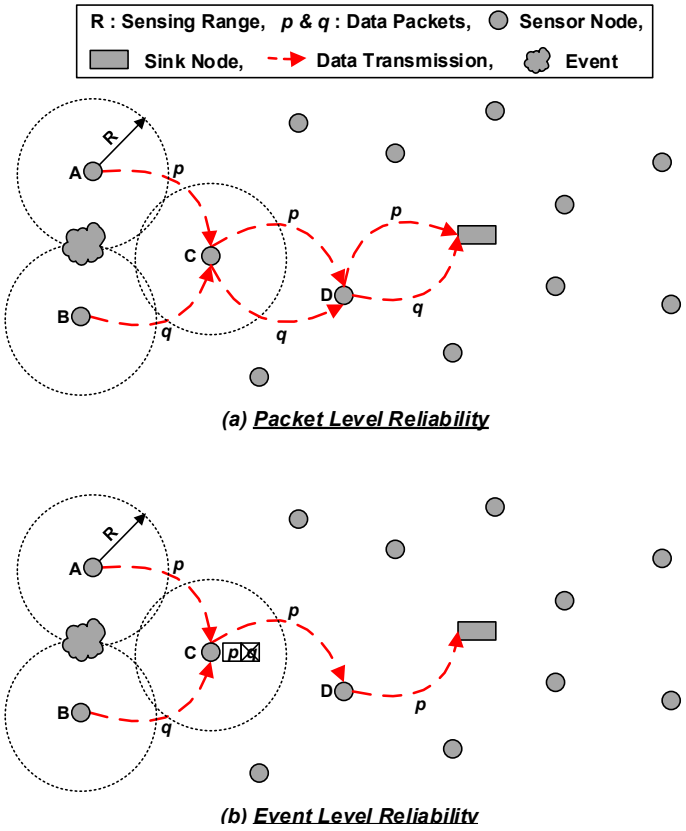


Figure 3: Event and Packet Level Reliability Mechanisms

This introduces the concept of packet and event level reliability, which is concerned with how much sensed data need to be delivered to the sink about the occurrence of an event of interest in the environment as shown in

Figure 3. Packet level reliability aims to ensure that all the packets carrying sensed data from all the related sensor nodes are reliably transported to the sink. On the other hand, event level reliability aims to ensure that the sink only gets enough information about a certain event happening in the network instead of all the sensed packets.

We have thus far, presented a background on reliability in WSNs, the challenges involved in achieving reliability and the terminologies that will be used throughout this paper. Following this, an overview of retransmission and redundancy techniques along with the existing reliability protocols based on each of these techniques are investigated in Section 2 and 3, respectively. Each scheme presented in Section 2 and 3 is analyzed based on the categorization of reliability portrayed in the proposed 3D-Reliability reference model. Section 4 discusses the need of having a hybrid mechanism for further improving the reliable transmission of data in WSNs. We compare and analyze the existing schemes using different criterion of comparison by presenting qualitative comparison in Section 5. We conclude the paper in Section 6, followed by Section 7 that highlights some of the challenges to be addressed in the future research.

## 2. Retransmission-based Reliability

In a wireless network, retransmission is the most commonly used technique in order to achieve data transmission reliability. Retransmission is also widely used in a resource constrained WSN for recovering the lost data. Retransmission-based reliability can either be performed using an end-to-end or a hop-by-hop method. End-to-end retransmission requires only the source node that generated the packet to retransmit the lost packet, whereas hop-by-hop retransmission allows the intermediate nodes to perform retransmission of lost packets. In a multi-hop WSN, retransmission-based reliability can be achieved through acknowledgements, where the sender node requires an acknowledgement of its sent data packets from the neighbouring recipient on the path to the sink.

There are generally two kinds of acknowledgement mechanisms, namely, explicit acknowledgement (eACK), which includes negative acknowledgement (NACK), and implicit acknowledgement (iACK) as shown in Figure 4. The eACK mechanism relies on a special control message which the receiving node, after successfully receiving a packet, sends back to the sender as a receipt of the received packet as shown in Figure 4(a). Like eACK, NACK

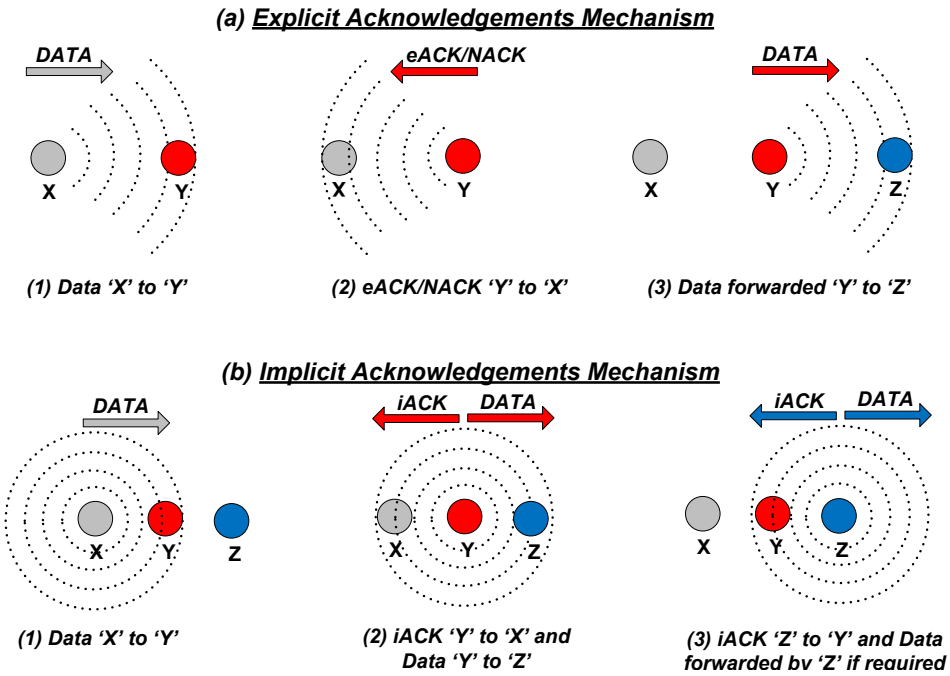


Figure 4: Implicit & Explicit Acknowledgement Mechanisms for Retransmission [9]

also corresponds to a special control message that allows the receiver to notify the sender to retransmit a particular missing sequence of the packet. The special control messages transmitted in eACK and NACK mechanisms result in additional transmission overhead and energy consumption which may not be feasible for most WSN applications [10]. On the other hand, in the iACK mechanism, the sender after transmitting the packet, listens to the channel and interprets the forwarding of its sent packet by the next hop node as a receipt of acknowledgement. In this way, iACK exploits the broadcast nature of wireless channel, avoiding the additional transmission overhead and energy usage caused by the transmission of special control messages (eACK/NACK). A brief overview along with the shortcomings of the major retransmission-based reliability protocols in terms of providing event or packet reliability are presented as follows.

### *2.1. Packet Reliability*

We have divided the retransmission-based reliability protocols in WSNs into two major categories based on the amount of data that needs to be

transmitted in order to maintain reliability. Packet level reliability is one of the categories where the application requires all the packets carrying event information from the relevant sensor nodes to be reliably delivered to the sink. This can be achieved either by using an end-to-end or a hop-by-hop method as described in the following subsections.

*2.1.1. End-to-End (Connection-oriented)*

This section investigates the schemes under the category of retransmission-based packet reliability employing the connection-oriented approach to ensure reliable data transmission. Iyer *et al.* [11] propose sensor transmission control protocol (STCP), a sink-centric end-to-end reliability protocol with congestion control mechanism. One of the key features of STCP is controlled variable reliability mechanism. This allows the data flow to be dynamically controlled by the sink, while adjusting the throughput based on the type of flow (i.e. continuous or event-driven) adapted by the application. Overall reliability is maintained by using ACK/NACK based end-to-end retransmission mechanisms, where each source node keeps the packets in its cache, until it gets an acknowledgement from the sink. On the other hand, congestion control is performed in such a way that the sink after receiving the information about congested paths, directs the downstream congested nodes to opt for the alternative paths. The key issue in STCP relating to reliability is the use of connection-oriented explicit acknowledgments (ACK/NACK), which involves only the end nodes (i.e. source and sink nodes). While STCP is a scalable approach involving large number of nodes with high hop counts from a source node to the sink, it is highly likely for a source node to encounter long waiting time for an acknowledgement from the sink. This may result in high latency and cache overflow, which is not suitable for energy constrained WSNs.

Marchi *et al.* [13] propose distributed transport for sensor networks (DTSN), an energy efficient non-sink centric end-to-end packet reliability protocol that provides a full and a differential reliability mechanism. Full reliability is supported with retransmission-based explicit acknowledgement mechanism; however, differential reliability is performed independently using enhancement flow strategy. In the full reliability mechanism, the source node keeps transmitting the packets until the number of transmitted packets equals the size of the Acknowledgement Window (AW), following which the source node sends an *explicit acknowledgement request* (EAR) to the destination for the confirmation of message delivery (ACK or NACK). An ACK

is sent if the sequence of the packets is in order and these in-sequence packets are removed from the output buffer of the source node. However, if a NACK is received then retransmission of the missing sequence of packets are required. The key contributions of DTSN are the integration of mechanisms involved in achieving reliability such as partial buffering at the source and intermediate nodes and erasure coding. Caching at intermediate nodes minimizes the high communication cost of performing end-to-end retransmissions and acknowledgements, which in turns reduces the energy consumption.

One of the key issues in connection-oriented retransmission-based packet reliability schemes discussed above is the use of explicit acknowledgements that rsults in high message overhead. This becomes worse as the schemes try to achieve packet level reliability, where each and every message needs to be reliably transported to the sink; this is suitable for loss-intolerant environment. On the other hand, in a high loss environment, large number of packets need to be retransmitted and explicitly acknowledged. This affects the overall energy efficiency that is one of the most important factors for a WSN. An overhearing mechanism can be introduced to reduce this message overhead caused by explicit acknowledgements. As compared to other schemes, discussed in Section 2.1.1, DTSN provides a more energy efficient and reliable data transmission using full reliability mechanism, but does not provide details of how the reliability level is maintained in changing network conditions. In addition, DTSN also adopts a distributed approach instead of relying on the sink to control the data flow which reduces the communication overhead and saves energy of the resource-constrained sensor nodes.

#### *2.1.2. Hop-by-Hop(Link-oriented)*

This section discusses the schemes that fall in the category of retransmission-based packet reliability using the hop-by-hop approach. Maróti [14] proposes the directed flood-routing framework (DFRF) using stop-and-wait implicit acknowledgement (SWIA) as a reliable packet recovery mechanism in WSNs. SWIA makes use of the notion of implicit acknowledgement in WSNs, where a sending node, after forwarding a packet, listens to the channel to check whether the receiver has further forwarded the packet towards the destination. The use of implicit acknowledgement is the key advantage of SWIA, as it comes without any additional packet overhead. However, if the sender does not hear anything, the packet is considered as lost and to maintain reliability, every lost packet is retransmitted. This continuous retransmission of packets further aggravates the problem of channel contention and net-

work congestion. Most sensor network applications can afford some degree of packet loss and attempting to retransmit every single lost packet may be both unnecessary and detrimental to the reliability of the network.

Zhou *et al.* [12] propose reliable transport with memory consideration (RTMC), a hop-by-hop packet reliability protocol addressing the challenges of memory and unreliable links in WSNs. The source node transmits data segments until the memory of the relay node is full. To prevent this memory overflow issue, the packet headers are loaded with the memory information which is shared among the neighbours. Reliability is maintained by keeping the forwarded segments at the sender until an acknowledgment is received. RTMC has been validated experimentally using six sensor nodes deployed in a line. One of the major contributions of RTMC is its deployment on real test-beds, which plays an important role when considering real-time WSNs. However, scalability is one of the key issues in RTMC, which may affect the performance of RTMC in case of large number of nodes deployed with dynamic topologies. This is because large number of nodes would require more data segments to be stored at each hop which increases the possibilities of memory overflow, resulting in packet loss and thus affects reliability.

Zhang *et al.* [15, 16] propose the reliable bursty convergecast (RBC) protocol for challenging situations where a large burst of packets from different locations need to be reliably transported to the sink. The main benefits and design considerations for RBC are the need to improve channel utilization and alleviate retransmission incurred channel contention, which is ignored in SWIA [14]. RBC employs a windowless block acknowledgement scheme to improve channel utilization and implements an adaptive timer mechanism for retransmission timeouts to control the channel contention caused by the retransmissions. However, the use of priority schemes to schedule the transmission could make packets having lower priority wait forever in the queue, thus resulting in high latency and unnecessary queue occupancy. While, RBC appears to provide good reliability as compared to SWIA, it also lacks a validation of its energy consumption, which is one of the most important issues of WSNs.

Unlike others, Le *et al.* [17] focus on the energy constraint and propose ERTP, an energy efficient link-oriented packet reliability protocol that performs loss recovery at each hop. ERTP provides statistical reliability determined by the quantity of data packets received at the sink for WSN application involving continuous streaming of the sensed data. It uses the SWIA mechanism [14] to recover the lost packets and utilizes a retransmis-

sion timeout estimation mechanism that dynamically minimizes the number of retransmissions to reduce energy consumption. Unlike RBC [16], ERTP has been validated with a low transmission rate and a negligible amount of congestion, which plays an important role in improving the overall performance of this scheme. Moreover, it uses a low power listening (LPL) MAC protocol for implicit acknowledgements, which results in low overhearing and consequently packet loss. Apart from these issues, ERTP seems to perform better in terms of scalability, energy efficiency and reliability as compared to the other schemes lying under the same category.

Shaikh *et al.* [18] propose tuneable reliability with congestion control for information transport (TRCCIT), aiming to provide reliable data transmission in varying network conditions and application requirements. This is achieved using a 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 neighbour, after receiving the information from the sender, can send an eACK to the sender to stop unnecessary retransmissions. On the other hand, the adaptive retransmission timeout mechanism is based on the buffer occupancy and balancing the number of incoming and outgoing messages at each node. Apart from providing better reliability as compared to RBC [16], TRCCIT also deals with some of the key related issues like timeliness, adaptive timer, hybrid acknowledgements and energy efficiency with dynamic network conditions.

Stann and Heidemann's [19] reliable multi-segment transport (RMST) is a NACK based sink-centric link-oriented packet reliability scheme. It has a caching and non-caching mode which decides whether or not the data segments need to be stored for retransmission purposes. Unlike windowless block acknowledgements and iACK mechanism in RBC, one of the key features of RMST is that it performs loss detection by collectively utilizing selective NACK along with timer based mechanisms. RMST is adequate for WSNs dealing with the transferring of large sized data such as image by performing fragmentation/assembly only at the source and destination without ensuring the delivery of fragments in the same order. This results in increased channel contention, where increasing number of fragments create more issues like in-network congestion. The congestion gets worse as RMST also does not handle the possibility of NACK implosion when the downstream nodes issue a chain of NACK requests in the non-caching mode for the gaps detected within the fragments transmitted.

Although significantly more focus has been given to upstream (sensor to sink) reliability, there is also a need to ensure that control messages and/or sensor software updates are reliably delivered from the sink to the sensors (downstream). Notably, Wan *et al.* [20] and Park *et al.* [21] propose hop-by-hop downstream reliability mechanisms called Pump Slowly Fetch Quickly (PSFQ) and GARUDA respectively, which aim to achieve reliability in order to disseminate the control messages or software code segments towards downstream sensor nodes, while performing loss detection and data recovery using retransmission.

PSFQ is based on three key operations, namely pump, fetch and report. The pump operation regularly broadcasts the code segments to the downstream nodes. The fetch operation starts as the sequence number gap is found by any intermediate nodes. The nodes stop forwarding new packets when there are missing packets and send the NACKs to their neighbours to ask for retransmission of the missing packets. It resumes the forwarding process when the missing packet has been retrieved from its neighbours. Finally, the report operation provides the status report to the user when a report message is sent from the farthest node in the network by aggregating messages from each node till it reaches the user. PSFQ requires all the nodes to cache all the packets received in order to reprogram the sensor nodes successfully, which is not suitable for memory constrained sensor nodes. If the sink has already received the information (such as temporal and spatial information) about a particular area, extra information about that area would be just an incentive but not a necessity. PSFQ is more suited for nodes reprogramming which typically do not happen frequently.

Park *et al.* [21] propose GARUDA, another downstream reliability protocol aims to reliably deliver the query-metadata and the control codes to the downstream nodes. GARUDA appoints the nodes in the network as core nodes for retransmission of the lost packets using an Availability Map (A-map) to prevent unnecessary retransmission requests; this requires an extra core construction stage for GARUDA, where the loss recovery and the core creation may cause high latency in the case of large sensor networks and the reliability guarantee is provided only for the transfer of the first packet. If GARUDA is used to accomplish the main functions of environmental sensing, it would be an overkill, the reason being similar to that for PSFQ.

This section covered some of the schemes aiming to achieve packet level reliability using link-oriented method of recovering the lost packet. These link-oriented schemes have been shown to be more reliable and, time and

energy efficient than the connection-oriented schemes, as the loss recovery is performed at each hop instead of the end nodes. One of the key issues in both the categories aiming to achieve packet level reliability is the requirement to ensure that every packet is safely delivered to its destination. Every scheme has accomplished the requirement in its unique way based on what is required by the application. However, most if not all the WSN applications have the tolerance to bear some degree of packet loss instead of restricting the nodes to reliably deliver every single packet. This would not only save sensor's limited energy, but also improve reliability.

### *2.2. Event Reliability*

Apart from packet reliability, event reliability is the other category that is based on the amount of data required to ensure the reliable transmission using the retransmission technique. In WSNs, event reliability as opposed to packet reliability should be sufficient for most of the event driven applications. Reliability in this way aims to ensure that at least one of the many packets from the sensors that detected an event is delivered to the sink, instead of all the packets from all the sensors as shown in Figure 3. The following discussion covers the major event reliability schemes that fall within the category of end-to-end or hop-by-hop retransmission-based event reliability.

#### *2.2.1. End-to-End (Connection-oriented)*

This section covers the retransmission-based event reliability schemes achieving reliable data transmission using the connection-oriented approach. Akan *et al.* [22, 23] are the first to introduce the concept of event reliability by proposing the event-to-sink reliability protocol (ESRT), where reliability is measured by the number of packets carrying information about a particular event that are delivered to the sink. ESRT is a sink-centric protocol, where flow of data is centrally controlled by the sink in such a way that when the required reliability is not achieved, the sink will increase the event reporting frequency, $f$, of the nodes. Conversely, it will reduce $f$ when there is congestion in order to restore the reliability required at the sink. A key assumption of ESRT is that the sink has a high power radio that can transmit the latest value of $f$ to all the sensor nodes in a single broadcast message, and each node will adjust its $f$ accordingly. This is a serious limitation because conventionally the sink is not one hop away from all the sensor nodes and ESRT also does not provide any downstream reliability guarantee for this broadcasting. Furthermore, ESRT increases the source sending rate in order to guarantee

event reliability. However, this central rate control method is not as energy efficient as non sink-centric approach by using hop-by-hop retransmission-based loss recovery mechanism. This would further deteriorate the overall bandwidth utilization and introduce high energy wastage as different parts of the network having different network conditions.

Gungor and Akan [24] propose delay sensitive transport (DST), an extended version of ESRT by adding application specific delay bounds with a Time Critical Event First (TCEF) scheduling policy. The key issue focused by DST in addition to reliability is timely delivery of event information to the sink. This introduces the idea of TCEF, where the data packets within each node's queue with lower remaining time to the deadline are given a high priority for transmission. The remaining time to deadline is calculated by piggybacking the elapsed time information of that event with the data packets, which eliminates the need for global time synchronization. Like ESRT, one of the major criticisms of DST is that the whole functionality is totally dependent on the one point that is the sink in order to regulate the flow of data. All the traffic first needs to be transmitted to the sink, where the sink takes control of the traffic flow by adjusting the data rate for the downstream nodes which then transmit the data accordingly. This not only increases the traffic overhead, but also significantly impact on energy efficiency and reliability. Moreover, DST works around a predefined single event with known location which is not practically sound, as in a WSN, multiple concurrent events may happen in close proximity or across the network.

Tezcan and Wang [25] propose asymmetric and reliable transport (ART) by choosing some essential nodes (E-nodes) within the sensor network that work together as cluster heads to provide upstream end-to-end reliability and downstream query reliability. Thus, ART is one of the few protocols to provide bidirectional reliability. Most of the work is done by the E-nodes; thus, all the other non-e-nodes do not incur end-to-end communication overhead. The E-nodes are selected based on the remaining battery power of the nodes and picking the ones with the highest remaining energy. To achieve upstream reliability, ART uses the ACK mechanism between the E-nodes and the sink, while reliable downstream query propagation is performed using the NACK mechanism. E-nodes also regulate the data flow by restricting the neighbouring non-essential nodes from sending their data until the congestion is cleared. As the congestion control and event reliability is performed by the E-nodes, packet loss due to congestion at non-essential nodes cannot be recovered by this protocol. ART assumes that there is congestion when an ACK

is not received within a timeout period. This is not a reasonable assumption, as it is not necessary that the ACK is lost due to congestion; it might also be lost due to the poor link quality or some other form of transmission errors. E-nodes work on the principal of clustering which improves the network scalability, but requires significant communications and energy resources for cluster formation and maintenance. This includes the cost of communication involved in advertisement, joining, global data acquisitions and scheduling messages from the sensor nodes in changing network conditions. 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.

Following ART, Xue *et al.* [26] propose a loss-tolerant reliable event sensing (LTRES), an end-to-end event reliability protocol designed for applications with heterogeneous sensing fidelity requirements over different event areas within a WSN. It aims to provide source rate adaption based on network capacity awareness which is calculated by measuring the event goodput at the sink. In addition, it also employs a lightweight congestion control mechanism, where instead of relying on the nodes to report congestion, the sink itself suppresses the transmission of the aggressive nodes based on the data it receives. This protocol is totally dependent on the sink, where the sink sends the updated source rates to the downstream E-nodes, but it does not employ any downstream reliability or congestion control mechanism. E-nodes are the set of nodes covering the event area, which are dynamically detected by the sink. Lack of loss recovery mechanism and reliability considerations for the non-essential nodes are critical issues that have not been addressed.

Unlike the existing quantity-based event reliability protocols, Park [27] propose quality-based event reliability protocol (QERP), which emphasize on the quality of event data reported to the sink. The authors claim that other existing quantity-based event reliability protocols are not suitable for the resource-constrained WSNs, as they aim to achieve reliability by increasing or decreasing the frequency of data reporting rates. These varying frequencies sometimes increase the overall data rate more than the desired rate, which could aggravate the network conditions. QERP as an end-to-end event reliability protocol claims to provide better reliability than ESRT by using the concept of Contribution Degree (CD). This means that the difference of sensor data in CD for event detection is due to the different environmental conditions like varying distance of nodes from the events. The data packets

are marked with a CD value, where those originating from the nodes located closer to the event's location are assigned with higher CD values and assumed to be more critical and are transmitted on higher priority. The node closest to the event is selected as a leader node, while the rest of the nodes in the event's region report their data to the sink through the leader nodes. If the node density is high near the event's location, then the process of selecting the leader node would be longer, resulting in energy wastage. There is no packet loss detection mechanism and the data flow mechanism is based on the event's location; however, there is no mention of the mechanism used to find the event's location, which is used to define the CD values.

*2.2.2. Hop-by-Hop (Link-oriented)*

This section discusses the existing schemes under the category of retransmission-based event reliability, focusing on link-oriented schemes. The price-oriented reliable transport protocol (PORT) proposed by Zhou *et al.* [28] aims to provide finer fidelity in event reliability as compared to ESRT, while minimizing the energy consumption. Unlike ESRT [23], PORT performs the adjustment of reporting rate frequency by adjusting the different reporting rates of source nodes in different regions accordingly. In addition, PORT also provides energy efficient congestion control mechanism by avoiding the nodes along the paths that have high loss rates based on the node price. The node price is the number of transmission attempts made before the packet is successfully delivered. The energy cost for the communication is also evaluated with the help of the node price. The sink regulates the reporting rate of a particular source based on the communication cost information according to the changing network conditions. The sink decreases the reporting rates of sources having higher communication cost and vice versa, while maintaining reliability.

PORT has been shown to be more energy efficient as compared to ESRT and it works well for the networks having diversified reporting rates at different parts of the network. However, if the reporting rates of different areas of the network are similar, then PORT will also give similar results to the other schemes. Like the other event reliability schemes, PORT also requires a high powered sink to regulate the flow of data and does not provide any packet loss recovery mechanism which may be vital in high loss environments.

Most recently Mahmood and Seah [29] propose the Event Reliability Protocol (ERP), an upstream hop-by-hop event reliability protocol which aims to reliably deliver the information about event occurrences to the sink. It sup-

presses the transmission of redundant packets containing information about similar events based on spatio-temporal correlation. 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 further reduces the traffic by exploiting the broadcast nature of the wireless channel through the use of implicit acknowledgements (iACK). Instead of relying on the sink to control the data flow, ERP performs in-network data processing that saves the overall network cost in terms of energy, data flow and congestion. The proposed approach highlights the importance of in-node data processing while minimizing the dependability on the sink. A more robust event identification mechanism would further strengthen its performance. However, the use of eACKs might also be a suitable option, since eACKs do not force the sender to listen the channel for a long period before it can overhear the packet transmission.

### *2.3. Open Issues*

In a WSN, sensor nodes collectively sense the environment and deliver the data through wireless channels. The limited constraints of the sensor nodes such as low power (i.e. limited batteries), short transmission range and small memory make the reliable delivery of the data one of the biggest challenges in the area of WSNs. In view of this, several reliability protocols (e.g. [23],[26] and [25]) has been proposed in the existing literature.

The retransmission-based reliability protocols discussed in Sections 2.1 and 2.2 aim to ensure the reliable transfer of data. Each protocol is discussed based on different methods of loss recovery such as hop-by-hop or end-to-end and packet or event level reliability (see 3D reliability reference model in Section 1).

One of the key challenges faced by most of the schemes is the need of being energy efficient while achieving reliability. This necessitates the use of distributed approach to achieve reliability as compared to the traditional centralized approaches (i.e. sink-centric approach). Most of the protocols discussed in Sections 2.1 and 2.2 use sink-centric approaches where the centralized collection point, that is the sink node, controls the data flow to maintain certain level of reliability. This approach is not energy efficient as it requires all the sensor nodes to first deliver the sensed data to the sink. The sink then broadcast the data rate to the sensor nodes to achieve the reliability required by the application. In addition, the network conditions change all the time,

which require the sink to repeatedly perform rate adjustments. Therefore, even the most efficient of the schemes using the sink-centric approach would require a lot of communication, which in turn affects the energy efficiency. Alternatively, it would be more energy efficient to use in-network processing (i.e. distributed approach), where sensor nodes take the responsibility of maintaining packet or event level reliability required by the application. This is an open issue, as majority of the reliability schemes relies on the sink to control the data flow to achieve reliability.

Given the short transmission range of the sensor nodes, data may have to travel several hops before it reaches the destination. Each hop introduces entry points for errors resulting in data loss which needs to be recovered to maintain required reliability. Adopting the most efficient method (e.g. type of acknowledgements) of recovering the lost data is another key issue. For the multi-hop nature of transmission in WSNs, it is beneficial to perform hop-by-hop recovery as compared to end-to-end. In addition, intelligently choosing the right acknowledgement mechanism is also required. Most of the schemes use explicit acknowledgement mechanism, which requires extra communication and memory. Alternatively, it is much better to use implicit acknowledgements by exploiting the broadcast nature of the wireless channel. This reduces the extra message overhead caused by the transmission of acknowledgement messages, which in turn reduces the channel contention and network congestion.

Some of the applications require guaranteed delivery of each and every packet from source to destination while others may tolerate some degree of packet loss. A WSN is deemed to be working well as long as the sensor nodes from a certain area reliably delivers the data back to the sink. Mostly, a monitoring system requires information about an area and not the individual report from each node in the network. Therefore, event level reliability as opposed to packet level reliability is sufficient for most of the applications. In addition, event level reliability introduces another key issue of accurate event identification which is overlooked by the existing research. Most, if not all, of the existing schemes assume that location of the events is already known or fixed. However, in a WSN, events can randomly happen anywhere. The event reliability protocols should be able to accurately calculate the location of the event, using some appropriate methods before ensuring their reliable transmission.

Most of the schemes discussed have been validated using a small number of sensor nodes and ignored the scalability of the network. Typically, a sensor

network comprises of hundreds of sensor nodes; therefore, in order to test the robustness and reliability of any scheme, it is important to validate it with a large number of nodes. Large deployments introduce increased interference due to the overlapping regions, high traffic overhead and congestion which are the important factors to be tested for a scalable WSN. In Section 5, we further provide a qualitative analysis and comparison of all the retransmission based reliability schemes discussed in Sections 2.1 and 2.2 based on criteria, such as, energy efficiency, complexity and scalability.

## 3. Redundancy-based Reliability

In retransmission-based reliability, a bit loss within a packet is treated as a loss of the entire packet and requires the retransmission of that packet in order to achieve reliable data transmission. This motivates the concept of redundancy-based reliability where the lost or corrupted bits within the packet can be recovered through the use of coding techniques [30, 31]. This significantly reduces the transmission overhead caused by the retransmission of the entire packet [32]. Keeping in view the resource-constrained nature of WSNs, employing redundancy techniques will not only strengthen the overall reliability but also conserve the limited energy resources of the sensor nodes.

Among the coding techniques, Forward Error Correction (FEC) techniques are used for error detection and correction at the lower layers of the protocol stack for telecommunication and computer communication (e.g. CRC in computer communication) systems [33]. However, when it comes to the upper layers (e.g. link, transport and application layers), erasure codes are needed to deal with the missing bits of the packets, since it is easier to determine the exact position of the lost bits. Rizzo [34] implemented and evaluated erasure coding for a desktop computer network. By carefully choosing the optimization parameters, erasure coding can also be implemented in a resource constrained WSN.

In erasure coding, the sender divides the packet into $m$ fragments, which are encoded by adding another $k$ fragments. These $m+k$ fragments are transmitted to the sink which is able to reconstruct the original data packet out of it. The receiver is able to reconstruct the original data packet if the number of fragments it has received (i.e. $m$') is equal to or greater than the number of original fragments (i.e. $m$) as shown in Figure 5. Like retransmission, redundancy-based reliability can also be achieved on an end-to-end (connection-oriented) or a hop-by-hop (link-oriented) level. In end-to-end

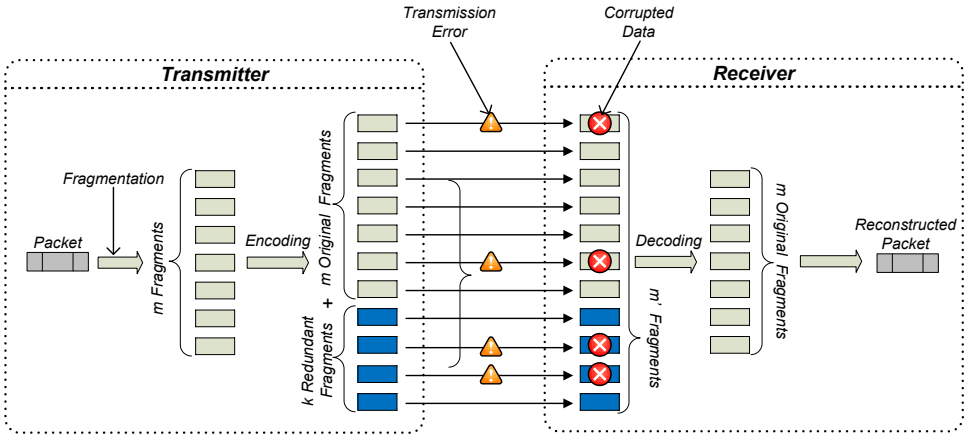


Figure 5: Redundancy Mechanism using Erasure Coding (adapted from [35])

erasure coding, the encoding/decoding of data is only performed at the source and the sink nodes, where the intermediate nodes simply relay the packets. However, in hop-by-hop erasure coding, encoding/decoding of data is performed at every intermediate node through to the sink. Thus, unlike end-to-end erasure coding, hop-by-hop erasure coding refreshes the data at each hop, reducing the chance of losing more than the desired amount of fragments on the way to the sink. Therefore, end-to-end erasure coding is not as reliable as hop-by-hop erasure coding in lossy environments when the number of hops from the source node to the sink is large. The existing research employing information redundancy in order to achieve reliability in WSNs is discussed below.

### *3.1. Packet Reliability*

Packet reliability refers to the process of ensuring the delivery of every data packet that contains the event information observed by the relevant sensor nodes to the sink. In redundancy-based reliability schemes, this is achieved by performing encoding/decoding either at the source and the destination node (end-to-end) or each pair of communicating sensor nodes (i.e. each hop) from the source to the destination (hop-by-hop).

#### *3.1.1. End-to-End (Connection-oriented)*

The schemes explained in this section fall under the category of redundancy-based packet reliability employing the connection-oriented approach to ensure reliable transmission of data from the source to destination. Ali *et al.*

[36] propose Optimum Reed-Solomon Erasure Coding (OREC) to achieve connection-oriented redundancy based packet reliability in a WSN. The source node creates and transmits the fragments of a packet using Reed-Solomon codes, a class of erasure codes, along multiple paths towards the sink where they are reconstructed. The cost of transmitting these fragments under different network conditions is computed and Genetic Algorithms (GAs) are used to determine the optimized number of fragments to be transmitted accordingly. This scheme assumed a query-based WSN where the sink sends the query to the "prongs" which are nodes one hop from the sink. The prongs further broadcast the queries throughout the network and the relay nodes keep track of the path through which they received the queries. This helps the relay nodes to forward the response of the queries back to the sink through the prongs, while selecting the path with short hop counts or high reliability.

Theoretical analysis of OREC shows that by increasing the number of parity fragments (additional redundant fragments), reliability is increased at the cost of traffic overhead. Therefore, intelligent selection of the number of redundant bits become the optimization factor in Reed-Solomon codes. However, the use of genetic algorithms requires intensive processing and might not be suitable for a resource-constrained WSN. 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, specially 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. The idea of introducing prongs does not seem to be suitable, as it will create an extra processing overhead on the nodes acting as prongs, while wasting the enhanced processing abilities of the sink.

Distributed transport for sensor networks (DTSN) by Marchi *et al.* [13] provides an energy efficient non sink-centric end-to-end packet reliability protocol with a full and a differential reliability mechanism; the full reliability mechanism has already been discussed in Section 2 under the retransmission category. However, in cases where full reliability is not required, a differential

reliability mechanism is used separately with an addition of a Forward Error Correction (FEC) technique using erasure coding. Differential reliability is supported by their proposed Enhancement Flow strategy. This is used to transfer a block of data, say an image, where the basic image (i.e. image with minimum resolution) is reliably transferred using FEC; however, FEC support is not provided to the rest of the image (i.e. image with maximum resolution). Enhancement Flow along with the FEC technique is implemented separately that is independent of retransmission-based full reliability mechanism. This results in high reliability and improved throughput as compared to full reliability strategy with the complete block transfer. DTSN employs 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 (i.e. image with minimum resolution), but does not provide details of how the size of the core data is determined or the reliability level is maintained under changing network conditions.

Unlike other redundancy-based reliability schemes in WSNs, Kim *et al.* [37] propose reliable transfer on sensor networks (RTSN) by experimentally validating the use of erasure codes on sensor test-beds. RTSN is a packet-level reliability mechanism using systematic codes, where the node does not need to perform a great deal of computation for the reconstruction of the original message. Systematic codes are implemented by labelling the transmitted packets either as an original or a redundant packet. This is because, if a part of the encoded message is the original message itself, then the receiving node can reconstruct it without performing any decoding operation. This will not only reduce the processing cost and memory usage of the nodes, but also improve reliability and energy efficiency. The processing cost is reduced as the node does not need to perform encoding/decoding if it finds the original message. The RTSN reliability mechanism has been compared with simple retransmission-based reliability where retransmission results in high latency and buffer overflow, which was alleviated by introducing erasure coding at the cost of traffic overhead. The performance of erasure coding deteriorates in lossy environments; therefore, finding alternative routes using the route fix mechanism when there is continuous packet loss at the current path is one of the major contributions of this scheme.

*3.1.2. Hop-by-Hop (Link-oriented)*

This section investigates redundancy-based packet reliability schemes, where encoding/decoding is performed by employing the link-oriented approach. Wen *et al.* [38] propose transmission reliability in sensor networks (TRSN), an energy efficient link-oriented redundancy based packet reliability mechanism. TRSN evaluates reliable data transmission in terms of packet arrival probability by checking it against the required reliability, while energy efficiency is evaluated in terms of energy consumed in successful delivery of a packet. The authors modelled the loss behaviour using the Gilbert model [39], which is basically designed for a single-hop channel. However, for a multi-hop network, it is assumed that the two-state Gilbert model can be adopted independently 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 analysed for simple transmissions, retransmissions and erasure coding mechanisms. The packet arrival probability and energy consumption are mainly compared against the unconditional loss probability (*ulp*). *Ulp* is the probability that the next packet will be lost based on the condition that the previous packet was lost. Finally, erasure coding is evaluated to be better than the link-oriented retransmission mechanism in terms of energy efficiency only on the condition that the *ulp* value is below a certain threshold. However, it is pertinent to mention that the performance of erasure codes might degrade in an environment with high loss rate and have a negative effect on both reliability and energy efficiency. Therefore, it is important to evaluate the performance of these mechanisms with varying loss rates to make a robust network that is capable of performing well in lossy environments.

Srouji *et al.* [35] propose the reliable erasure-coding based data transfer scheme (RDTS), an efficient hop-by-hop packet reliability mechanism that uses erasure coding. Unlike end-to-end redundancy-based schemes, RDTS uses erasure coding at each hop to attain hop-by-hop reliability. In addition to erasure coding, RDTS applies partial coding to reduce the computational overhead caused by performing erasure coding at each hop. The partial coding mechanism further reduces the cost of performing complete erasure coding process at each intermediate node. 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 dur-

ing the transmission. Thus, the overall cost of transmission is reduced due to lower processing overheads and reduced delays. RDTS is compared with simple hop-by-hop erasure coding without partial coding and end-to-end erasure coding, where it shows better 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.

Most recently, Awami and Hassanein [41] propose 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 [42]. One of the main contributions of the DS-DEC is that it specifically calculates the energy required to perform encoding/decoding process.

Most of the schemes discussed so far focus on upstream reliability guarantees implemented using erasure codes; however, Kumar *et al.* [40] propose a schemes to provide redundancy-based downstream data transmission reliability in a large WSN. The context for Kumar's work was pushing out software updates to WSN nodes. When the software codes need to be updated for the downstream nodes, the sink is required to broadcast the software updates throughout the sensor network. This broadcast results in excessive overhead which may become the cause of data loss and affect overall relia-

bility. Unfortunately, a partial software update is unacceptable as all nodes must be updated in order for the whole network to function correctly. To provide complete reliability, Kumar *et al.* [40] propose FBcast that uses FEC techniques.

FBcast uses fountain codes [49], a class of erasure codes, producing an encoded block of data on-the-fly without any dependence on the limited buffer space. The encoded data is broadcasted to the neighbours, which is further rebroadcasted, when new fragments are received. This protocol is based on the assumption that all the nodes in the network are one hop away from the sink, which broadcasts the updated codes in a single broadcast message. This is not a feasible solution for a network where the sink is multiple hops away from the downstream nodes, thus Kumar *et al.* propose an extended version of FBcast protocol with the concept of repeaters. The repeater functionality is applied on the sensor nodes, where the sensor nodes, after receiving enough data fragments, reconstruct the original data. This reconstructed data is further re-encoded and rebroadcasted to these sensors' neighbours and so on. In another variation of the scheme, a probabilistic broadcast scheme is used; however, this does not provide good reliability. The idea of implementing erasure codes for ensuring downstream reliability might be new, but performing encoding/decoding at each and every downstream node of the network to successfully broadcast the data throughout the network is an expensive choice to achieve reliability in a dense network.

In Section 3.1, we have so far investigated the schemes that fall under the category of redundancy-based packet reliability by utilizing either end-to-end (connection-oriented) or hop-by-hop (link-oriented) approach to perform encoding/decoding. We have categorized these schemes based on their use of certain coding techniques that require the sender to add some additional redundant set of fragments to the packet so that the receiver will be able to reconstruct the packet if some bits are lost or corrupted. In contrast to this, some of the existing research uses the term redundancy in a completely different perspective that is ensuring reliability without using any form of coding techniques. Based on our proposed 3D reliability structure, these schemes fall under the packet reliability category using either end-to-end or hop-by-hop approach.

Yang *et al.* [43] propose Packet-based Cooperative Diversity (CP-diversity) by introducing the concept of redundancy-based packet reliability in WSNs from a different but interesting perspective. Yang *et al.* [43] interpret redundancy based on the cooperative diversity concept used by RAID (Redundant

Array of Independent Disks), a data storage virtualization technology. Therefore, instead using coding schemes to divide a packet into multiple segments and add addition redundant bits, CP-diversity simultaneously distributes multiple redundant copies of the original packet over multiple links towards the destination. The destination recovers the lost packet based on the message IDs of the redundant copies received. Unlike the traditional process of combining signals in diversity techniques, CP-diversity sends multiple copies of a packet through multiple but independent links. Prior to this, Seah and Tan [44] propose a similar approach in their Multipath Virtual Sink Architecture (MVSA) for wireless sensor networks in harsh environments. In the MVSA approach, multiple copies of a packet are sent via independent disjoint paths to different sinks deployed over diverse locations in order to overcome extremely poor and fluctuating channel conditions prevalent in harsh environments, e.g. underwater sensor networks, and all the sink are connected by high-speed (wired or wireless) links to form a virtual sink. This is indeed a reliable and non-complex idea in terms of implementation, as it avoids the channel estimation or time synchronization. However, it ignores the resource constrained nature of WSN and incurs high communication cost by transmitting multiple copies of a packet via multiple links which results in high energy cost. However, this energy cost can be minimized by improving the cooperation mechanism among the nodes.

Wu *et al.* [45] propose an adaptive redundancy-based mechanism (ARM), a connection-oriented packet reliability protocol independent of any routing or underlying layered architecture. Unlike the traditional redundancy-based reliability mechanisms, they use the term "redundancy" to refer to the same packet being transmitted twice based on pre-assumed link quality of the next hop node. To avoid unnecessary transmission of redundant packets, ARM takes the redundant transmission decision based on average packet reception ratio of the link and expected delay to the sink. The packet is transmitted twice when the link quality is lower than the predefined threshold and delay is high. ARM does not make use of any coding scheme and simply transmits a packet twice without employing any form of acknowledgement mechanism. ARM claims to be scalable; however, it is evaluated with only eight nodes with maximum two hops from the source node to the sink. The transmission of the same packet twice without employing any acknowledgement mechanism results in the wastage of sensors' limited energy resources which is one of the most important factors to be considered for a WSN.

Unlike CP-diversity [43], MVSA [44] and ARM [45], Damuut and Gu

[46] present another viewpoint of redundancy in randomly deployed WSNs by proposing M-LEACH, a modified version of the LEACH [47] algorithm, referred here as M-LEACH. M-LEACH interprets redundancy in terms of multiple nodes with completely overlapping sensing regions, which usually occurs when the nodes are deployed in a random fashion. M-LEACH focuses on dynamically identifying these redundant nodes by exploiting their topology information. Out of the redundant nodes, the one with the minimum distance to the sink is selected as a resident node and the rest are considered as redundant. In order to maximize the overall network lifetime and energy efficiency, the redundant nodes could be turned to sleep mode. This would also reduce the number of nodes transmitting, as a result packet collision and network congestion can be significantly reduced.

Tang and Wang [48] propose CoDyMAC (Cross-layer and Dynamic balance energy-consumption MAC), an energy efficient redundancy-based packet reliability protocol by exploiting the carrier listening functionality of the MAC layer and routing information from routing layer. CoDyMAC takes advantage of the listen/sleep cycle where the nodes are waken up at each cycle. The nodes that need to be involved in the communication are selected based on the highest energy available at the node, while filtering out rest of the low power redundant nodes. The successfully selected nodes perform adaptive wake-ups periodically where they efficiently perform listening in the request and response windows. CoDyMAC is compared with SMAC, ASMAC and ELMAC where it performs better in terms of energy efficiency and latency. Like M-LEACH [46], CoDyMAC also interprets redundancy as having more than one node transmitting the same data. Reliability is increased by increasing the number of redundant nodes, which becomes the cause of communication overhead and high energy consumption; however, CoDyMAC controls redundancy after measuring energy consumption and percentage of packets received by the sink.

### *3.2. Event Reliability*

To the best of our knowledge, there has been no published work on redundancy-based event reliability. The interdependent nature of different techniques and methods has led us to the development of the 3D reliability reference model as presented in Section 1, which when unfolded as shown in Figure 6, discloses the existence of an unexplored area in the existing research on redundancy-based reliability. This unexplored area, shown as a blank square in Figure 6 reveals that the existing research on reliability does

not exploit redundancy-based event reliability by using either an end-to-end (i.e. connection oriented) or a hop-by-hop (link-oriented) method. This area seems to be promising in improving the energy efficient reliable transmission of the packets carrying an event's information from the relevant sensor nodes towards the sink.

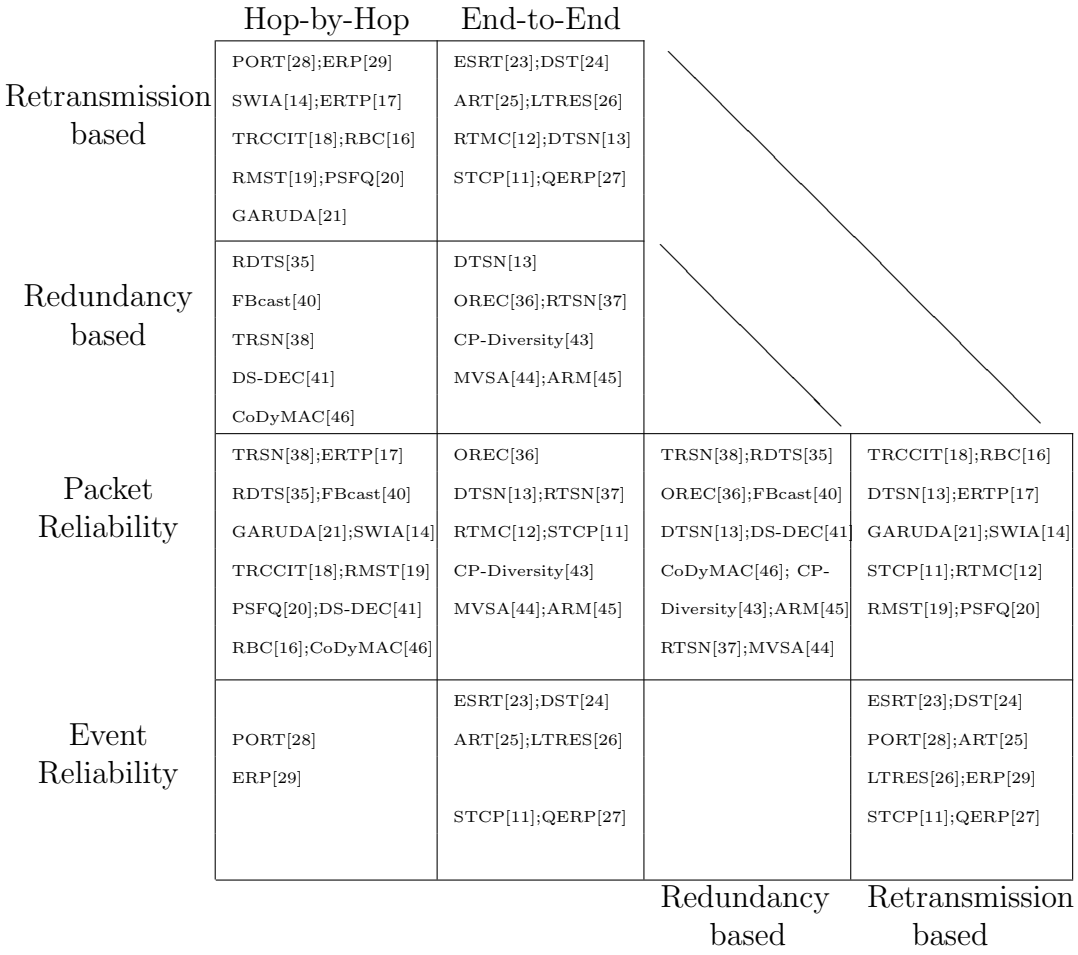


Figure 6: Unfolded 3D Reference Model for Research in WSN Reliability

In a WSN, achieving event level reliability as opposed to packet level reliability should be sufficient for most of the event-driven applications. This requires the efficient utilization of event reliability approach in redundancy-based technique using either end-to-end or hop-by-hop methods. Redundancy-based event reliability in this way aims to perform encoding/decoding for at

least one of the many packets carrying information about the same event, instead of all the packets from the related sensor nodes. This not only scales down the communication among the sensor nodes, but also reduces the processing cost at the sensor nodes. It is due to the fact that event level reliability requires only the transmission and processing of the most significant packets instead of all the packets sensed by the relevant sensor nodes. This improves the overall reliability and energy efficiency in a WSN by minimizing the traffic overhead which causes network congestion thereby resulting in the packet loss. Finally, employing hop-by-hop or end-to-end approaches also plays an important role in redundancy-based event reliability depending on the application requirement, such as end-to-end may perform better in low hop-count from source to destination as compared to hop-by-hop. Therefore an intelligent selection of these techniques is required to achieve redundancy-based event reliability in an energy efficient manner.

### *3.3. Open Issues*

Several protocols have been proposed (e.g. [37], [35] and [41]) in the existing literature to achieve reliable transmission of data in a resource constrained WSN. Like retransmission-based protocols, redundancy-based protocols aim to ensure the reliable transmission of data as discussed in Section 3.1. Each protocol is investigated based on the common taxonomy (e.g. hop-by-hop or end-to-end and packet or event level reliability) proposed in the 3D reference model presented in Section 1.

One of the major issues encountered by most of the redundancy-based reliability protocols is that the performance of these protocols degrades in high loss environments. This is due to the fact that the coding techniques are only able to reconstruct a limited number of lost or corrupted bits. This limit depends on the amount of redundant fragments added to the original set of fragments of a packet. Large numbers of additional redundant fragments are able to tolerate higher degree of loss as compared to small number of additional fragments. This large number of redundant fragments also increases the traffic overhead that may result in congestion and affect overall reliability. It is therefore required to investigate a mechanism that dynamically selects the number of additional fragments to reconstruct the lost or corrupted bits in changing network conditions, such as high to low loss environments and vice versa.

Another important issue that needs attention is that most of the existing protocols have ignored scalability and assessed the respective protocols by de-

ploying small number of sensor nodes. A typical WSN consists of hundreds of sensor nodes [3], which increases the number of hops from the source node to the destination node. Each hop introduces entry points for errors, such as packet collision or interference. This issue can be handled by performing encoding/decoding in a hop-by-hop manner as compared to end-to-end basis. Encoding/decoding at each hop provides reliability at the cost of high processing overhead at the sensor nodes. However, this processing overhead can be reduced by introducing an energy-efficient mechanism. For example, if a node receives enough number of fragments to reconstruct the original packet then it simply forwards the fragments to the next hop without performing encoding/decoding. In this way, scalability can be efficiently achieved by avoiding the extra processing at the sensor node.

Finally, a major gap in this research area as highlighted in Section 3.2 is to further investigate redundancy-based event reliability mechanism to improve overall reliability. Redundancy-based event reliability also involves the challenge of accurate event identification in order to achieve high degree of efficiency in monitoring and control systems. This is because the event data from closely located sensor nodes in a network tends to be highly correlated. Therefore, transmitting as few as a single packet carrying information about the event instead of multiple copies of the same packet would reduce the transmission overhead, thereby resulting in extended network lifetime.

## 4. Hybrid Mechanism

We have thus far investigated various protocols in wireless sensor networks that aim to achieve reliable transmission of data. The most common techniques involved in achieving reliability in WSNs are retransmission and redundancy. To the best of our knowledge, no existing research has so far considered the use of a hybrid approach that involves an efficient combination of both retransmission and redundancy techniques to achieve reliability, and thus provides a motivation to investigate a hybrid mechanism.

A hybrid mechanism combines the features of both retransmission and redundancy techniques. One of the limitations of redundancy techniques is that the reconstruction of the original packet at the receiving node will only be successful when the number of received fragments are equal to or more than the original set of fragments, otherwise, the packet is considered as lost. This introduces the need for a hybrid mechanism, where the retransmission technique can be applied when the receiver is not able to receive the

minimum number of fragments required to reconstruct the packet. In this scenario, the hybrid mechanism will only retransmit enough lost fragments in order to make up the minimum number of fragments needed to reconstruct the original packet. This would not only minimize the unnecessary retransmissions of the packets but also reduces the overall network load by requiring only retransmission of the small sized fragments instead of the whole packet. This results in conserving the sensors' limited energy and improves the overall reliability. However, such an approach would introduce latency due to the in-node processing at each hop in the sensor network.

WSN applications can be classified into three broad categories such as environmental monitoring, health-care and surveillance [52]. A hybrid mechanism best suits the needs of environmental monitoring applications (such as vineyard and water quality monitoring) based on their characteristics as discussed above. This is because the environmental monitoring applications require the sensor networks to operate for longer periods in unattended areas, while delaying the data transmission to improve the overall network lifetime.

## 5. Analysis

We now present a qualitative analysis of the reliability schemes discussed in Sections 2 and 3. We have divided the overall analysis into feature analysis and performance analysis. The feature analysis (see Section 5.1) compares and evaluates all the schemes based on the common taxonomy proposed in the 3D reference model (see Figure 2), while the performance analysis (see Section 5.2) focuses on comparing the reliability schemes qualitatively based on several key performance criteria, such as, energy consumption, complexity and reliability.

### *5.1. Feature Analysis*

This section presents the comparison of the reliability schemes (discussed in Sections 2 and 3) based on the 3D reference model. Sections 5.1.1 and 5.1.2 present the comparison of the schemes that fall under the retransmission and redundancy based reliability, respectively. This comparison is mainly based on the features such as reliability level, loss recovery mechanism and type of acknowledgements adopted by each scheme.

### *5.1.1. Retransmission-based Reliability Schemes*

Table 1 presents the retransmission-based reliability schemes discussed in Section 2 and 3. It can be seen that majority of the research focus on achieving reliable transmission of data from the sensor nodes to the sink node (i.e. up-stream traffic) as compared to downstream traffic. However, except ART [25], all the existing schemes make the assumption that a reliable downstream communication mechanism is already available. ART has an advantage over the other schemes in terms of having an additional downstream reliability mechanism along with the upstream reliability. This enables the network to perform accurately under changing application requirements by allowing the sink to reliably disseminate the information (such as control messages, software codes segments or updates) to the sensor nodes.

***Retransmission-based Schemes***

| ***Protocol*** | ***Traffic Flow*** | ***Reliability Level*** | ***Loss Recovery*** | ***ACK Mechanism*** | ***Sink Centric*** | ***Evaluation Method*** | ***Key Feature*** |
|---|---|---|---|---|---|---|---|
| ERP [29] | Up | Event | Hop-by-hop | iACK | No | Simulations | Region-based Selective Retransmission |
| ESRT [23] | Up | Event | End-to-end | – | Yes | Simulations | Reporting Frequency Rate |
| DST [24] | Up | Event | End-to-end | – | Yes | Simulations | Reporting Frequency Rate |
| PORT [28] | Up | Event | Hop-by-hop | – | Yes | Simulations | Reporting Frequency Rate |
| ART [25] | Up/ Down | Event | End-to-end | ACK/ NACK | Yes | Simulations | E-Node/Non-E-Node |
| LTRES [26] | Up | Event | End-to-end | ACK/ NACK | Yes | Simulations | Distributed Source Rate Adaption |
| QERP [27] | Up | Event | End-to-end | – | Yes | Simulations | Contribution Degree |
| STCP [11] | Up | Event/ Packet | End-to-end | ACK/ NACK | Yes | Simulations | Controlled Variable Reliability |
| SWIA [14] | Up | Packet | Hop-by-hop | iACK | No | Real Test-beds | DFRF Engine |
| RBC [16] | Up | Packet | Hop-by-hop | iACK | Yes | Real Test-beds | Windowless Block Acknowledgement |

**Table 1: Comparison of Retransmission-based Reliability Schemes (continued on next page)**

**Table 1 – continued from previous page**

| *Protocol* | *Traffic Flow* | *Reliability Level* | *Loss Recovery* | *ACK Mechanism* | *Sink Centric* | *Evaluation* | *Key Feature* |
|---|---|---|---|---|---|---|---|
| ERTP [17] | Up | Packet | Hop-by-hop | iACK/ ACK | Yes | Simulations | Statistical Reliability |
| TRCCIT [18] | Up | Packet | Hop-by-hop | iACK/ ACK | Yes | Simulations | HACK/Adaptive Retransmission |
| RTMC [12] | Up | Packet | Hop-by-hop | – | Yes | Real Test-beds | Memory Management |
| RMST [19] | Up | Packet | Hop-by-hop | NACK | Yes | Simulations | Selective ARQ |
| DTSN [13] | Up | Packet | End-to-end | ACK/ SACK | No | Simulations | Full/Differentiated Reliability |
| PSFQ [20] | Down | Packet | Hop-by-hop | NACK | Yes | Simulations | Operations under High Error Rate |
| GARUDA [21] | Down | Packet | Hop-by-hop | NACK | Yes | Simulations | Loss Recovery Infrastructure |

Table 1: Comparison of retransmission-based reliability schemes

Maintaining packet or event level reliability depends on the amount of sensed data required by the application to ensure the reliable transmission of data. Event reliability not only fulfils the needs of most of the event-driven applications, but also reduces the overall message overhead in the network. However, most of the event reliability schemes such as ESRT, DST, PORT, LTRES and ART rely on the sink to control the flow of data in the network to maintain the required reliability level. This sink-centric approach results in increased message overhead, as the sink and the sensor nodes have to frequently communicate to maintain certain reliability level. Only ERP and DTSN are the exceptions in this regard, as they use in-node data processing instead of a sink-centric approach. This reduces unnecessary transmission of the packets from the sink and improves the network lifetime. Among the schemes analysed, STCP is the most flexible in terms of dynamically providing both event and packet reliability depending on the application requirement.

The type of acknowledgement mechanisms selected by any of the reliability protocols also plays an important role in the efficient recovery the lost packets in a WSN. Among the existing schemes, majority of them recover

the lost packets using explicit acknowledgments; however, only a few exploit the broadcast characteristics of a wireless channel by using implicit acknowledgments. Some of the protocols, such as ESRT, DST, PORT and QERP, do not explicitly mention any loss detection and notification mechanism. In comparison, ERP, SWIA, RBC, ERTP and TRCCIT perform better than the other schemes in terms of the selection of acknowledgement mechanism, as they are based on implicit acknowledgements. This saves the transmission of additional control packets that are required by explicit acknowledgement mechanisms.

Loss recovery is the essential part for every reliability protocol, which can either be performed on a hop-by-hop (link-oriented) or end-to-end (connection-oriented) basis. ESRT, DST, STCP, ART, LTRES, PORT, QERP, DTSN, GARUDA and PSFQ aim to achieve reliability while recovering the lost packets based on the end-to-end retransmissions, whereas the rest of the schemes use the hop-by-hop method. The end-to-end method in comparison to hop-by-hop introduces high delay and high energy consumption in a large-scale sensor network. Overall, in large WSNs, schemes employing hop-by-hop methods tend to be more scalable and energy efficient as compared to schemes based on end-to-end method, at the cost of higher local (node level) computational overheads.

*5.1.2. Redundancy-based Reliability Schemes*

Table 2 presents the comparison of redundancy-based reliability schemes surveyed in Section 3. Rizzo *et al.* [34] first validated the erasure codes in computer communication which motivated the idea of implementing redundancy-based reliability in resource constrained WSNs. Among all the redundancy-based reliability protocols, only FbCast [40] achieves downstream data transmission reliability, whereas others only focus on upstream reliability. Majority of the existing protocols perform either upstream or downstream reliability, whereas none of them provide a combination of both upstream and downstream reliable transmission.

As far as maintaining the packet or event level reliability is concerned, all the redundancy-based schemes ignore the use of event level reliability, focusing only the packet level reliability. Event level reliability in redundancy-based schemes is a promising approach for resource-constrained WSNs. This is due to the fact that fewer packets need to be transmitted in event level reliability as compared to packet level reliability. This reduces of overall transmission overhead and hence minimizes the overall energy consumption

| ***Redundancy-based Schemes*** | | | | | | |
|---|---|---|---|---|---|---|
| ***Protocol*** | ***Traffic Flow*** | ***Reliability Level*** | ***Hop-by-hop/ End-to-end*** | ***Coding Scheme*** | ***Evaluation*** | ***Key Feature*** |
| OREC[36] | Up | Packet | End-to-end | RS-Codes | Theoretical Analysis | Genetic Algorithms |
| DTSN[13] | Up | Packet | End-to-end | Erasure Codes(EC) | Simulations | Enhancement Flow |
| RTSN[37] | Up | Packet | End-to-end | Systematic & EC | Real Test-beds | Route Fix Mechanism |
| TRSN[38] | Up | Packet | Hop-by-hop | Erasure Codes | Theoretical Analysis | ULP |
| RDTS[35] | Up | Packet | Hop-by-hop | Erasure Codes | Simulations | Partial Coding |
| DS-DEC[41] | Up | Packet | Hop-by-hop | Erasure Codes | Simulations | DEC-EaF /DEC-EaD |
| FBcast[40] | Down | Packet | Hop-by-hop | Erasure Codes | Simulations | FB Cast |
| CP-diversity[43] | Up | Packet; multiple copies | End-to-end; multiple paths | – | Simulations | Diversity Techniques |
| MVSA[44] | Up | Packet; multiple copies | End-to-end; multiple disjoint paths | – | Theoretical Analysis | Multiple sinks forming a virtual sink |
| ARM[45] | Up | Packet; 2 copies | End-to-end | – | Real Test-beds | Routing protocol independent |
| MLEACH[46] | Up | Packet | *Not Applicable* | – | Simulations | LEACH; overlapping coverage |
| CoDyMAC[48] | Up | Packet | Hop-by-hop | – | Simulations | Cross Layering |

Table 2: Comparison of Redundancy-based Reliability Schemes

in WSNs.

Among the existing redundancy-based packet reliability protocols, TRSN [40], RDTS [35], DS-DEC [41] and CoDyMAC [48] performs better as compared to the other protocols by adopting hop-by-hop approach over the end-to-end approach for loss recovery. The better performance is reflected in the increased network lifetime. However, these protocols may incur higher processing overheads at each node, as it is expected to perform the encoding/decoding process. In addition, RDTS proposes partial coding mechanism in a hop-by-hop fashion which results in reduced coding overhead and increased network lifetime. In contrast, RTSN seems to be promising among the schemes using end-to-end method, as it achieves highest reliability.

CP-diversity [43], MVSA [44], ARM [45], M-LEACH [46] and CoDyMAC [48] present a completely different perspective without employing any coding

technique. For example, CP-diversity, MVSA and ARM interpret the term redundancy by transmitting multiple redundant copies of the same packet, whereas M-LEACH and CoDyMAC define redundancy as multiple redundant nodes with overlapping regions. CP-diversity, MVSA and ARM employs end-to-end loss recovery, whereas CoDyMAC uses hop-by-hop approach which performs better than CP-diversity and ARM. All these schemes (such as CP-diversity, ARM, M-LEACH and CoDyMAC) also aim to achieve packet level reliability.

*5.1.3. Findings and Recommendations*

Based on the feature analysis presented in Sections 5.1.1 and 5.1.2, we believe that event level reliability tends to be more energy efficient than packet level reliability in both retransmission and redundancy based mechanisms. On the other hand, retransmission and redundancy based schemes using hop-by-hop approach are more reliable as compared to end-to-end in high loss environments, especially when there is a high hop count from the source to the destination. This motivates the need to investigate the possibilities of loss-tolerant and scalable mechanisms for reliability protocols.

*5.2. Qualitative Analysis and Comparison*

We also analyzed and compared the reliability protocols qualitatively based on various performance criteria, viz. degree of reliability, energy consumption, complexity, latency and scalability. Table 3 and Table 4 summarize the findings of this qualitative analysis of the two classes of reliability protocols discussed in Sections 2 and 3 respectively. These schemes have been developed to support a wide range of applications: e.g., TRCCIT and STCP may be suitable for heterogeneous and continuous flow applications; ESRT, LTRES and QERP for event detection applications such as object tracking; ART, DST and PORT may be useful for mission critical applications like border security and intrusion detection; and ERTP for environmental monitoring applications such as water quality management. Moreover, ERP is good for event-driven applications; RBC for high-volume busty traffic applications; and RMST and DTSN for multimedia applications. Therefore, it is worth mentioning that all the schemes can be used for a wide range of applications based on their functionalities. We stress that these findings are not quantitative results obtained via simulations or experimental studies; the conclusions are drawn from the results presented by the individual papers.

Due to the diverse assumptions made in the designs and different target applications, we decided on the use of only "High" or "Low" values in most of the criteria being compared. In the case of scalability, our classification of "High", "Med(ium)" or "Low", is based mainly on the size of the networks used by the authors in the performance evaluation of their respective schemes. Schemes which have only been validated using networks of less than 100 nodes are deemed to be of "Low" scalability. Typically, we would expect schemes for wireless sensor networks to be able to scale up to 1000s of nodes in order to be deemed as having "High" scalability. However, among the reliability schemes that we have studied, none have been validated in 1000-node networks or larger. There is clear gap between 200 and 500 nodes used in the various performance studies. Besides this observation, we also noted that FBcast [40] has been experimentally validated using 441 motes in a 21×21 grid network; being the only scheme in the 400-500 region, and since it has been experimentally studied, unlike the rest which have only been studied using simulations, we classified it as having "High" scalability. Hence, we classified schemes to be of "Med(ium)" scalability if they have been validated in networks from 100 nodes up to but less than 400 nodes, and any scheme that has been validated using networks of 400 nodes or more is deemed to be of "High" scalability.

Energy constraint is the most important issue of WSNs as the sensor nodes have limited battery-power. This constraint requires the protocols to operate in an energy efficient manner in order to prolong the network lifetime. It can be seen that majority of the protocols (such as ERP, ERST and DST) report low energy consumption while achieving high reliability. While some of the protocols (such as STCP, RBC and OREC) need high energy consumption in order to achieve high reliability, the high energy consumption in such reliability protocols can be the consequence of the underlying routing mechanism, and not necessarily due to the reliability mechanism itself.

It can also be observed that some of the protocols (such as DST, ART and RDTS) produce low latency as compared to the other reliability protocols (such as ESRT, STCP, and SWIA). This is also evident from the proposed use of such low-latency protocols in the delay-sensitive applications, e.g., surveillance and emergency/rescue applications. On the other hand, protocols (such as ESRT, STCP, and SWIA) that have high latency are most suitable for environmental monitoring applications, like water monitoring, as these applications do not have strict latency bounds for reporting the events occurring in an environment.

| *Retransmission-based Schemes* | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| ***Scheme*** | ***Reliability High/Low*** | ***Energy Consumption High/Low*** | ***Complexity High/Low*** | ***Latency High/Low*** | ***Scalability High/Med/Low (no. of nodes)*** | ***Deployment Strategy*** | ***Suitable Application(s)*** | ***Routing*** |
| ERP [29] | High | Low | Low | — | High (500) | Multi-hop /Random | Event-driven Applications | Shortest Path |
| ESRT [23] | High | Low | High | High | Med (200) | Multi-hop /Random | Event-driven Applications | DSR |
| DST [24] | High | Low | High | Low | Med (200) | Multi-hop /Random | Event-driven Applications | DSR |
| PORT [28] | High | Low | High | — | Med (100) | Multi-hop /Grid | Border Surveillance /Intrusion detection | Directed Diffusion |
| ART [25] | High | Low | High | Low | Med (100) | Multi-hop /Clustered /Random | Mission Critical Applications | AODV |
| LTRES [26] | High | Low | High | Low | Med (100) | Multi-hop /Grid | Event-driven /Surveillance | Static Proactive Routing |
| QERP [27] | High | Low | Low | — | High (500) | Multi-hop /Clustered /Random | Event-driven Applications | Geographic Routing/GPSR) |
| STCP [11] | High | High | High | High | Med (100) | Multi-hop /Random | Event-Driven /Continuous Flow | Shortest Path |
| SWIA [14] | Low | High | Low | High | Low (60) | Multi-hop | — | Directed Flood Routing) |
| RBC [16] | High | High | High | Low | Low (49) | Multi-hop /Grid | Event-driven Busty Traffic | Logical Grid Routing (LGR) |
| ERTP [17] | High | Low | High | High | Med (200) | Multi-hop /Uniform | Environmental (Water) Monitoring | DSDV |
| TRCCIT [18] | High | Low | High | High | Med (100) | Multi-hop /Grid | Event-driven /Continuous Flow | LGR |
| RTMC [12] | High | Low | Low | Low | Low (6) | Multi-hop /Linear | — | — |
| RMST [19] | High | — | Low | High | Low (21) | Multi-hop /Grid | Event-driven Applications | Directed Diffusion |
| DTSN [13] | High | Low | High | High | — | Multi-hop | Surveillance Applications | Omniscient Routing |
| PSFQ [20] | High | High | Low | High | Low (13) | Multi-hop /Linear | Disaster Recovery Applications | Broadcasting Mechanism |
| GARUDA [21] | High | Low | High | Low | High (800) | Multi-hop /Grid and Random | Security Applications | Flooding Mechanism |

Table 3: Qualitative analysis of retransmission-based reliability schemes

| *Redundancy-based Schemes* | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| ***Scheme*** | ***Reliability High/Low*** | ***Energy Consumption High/Low*** | ***Complexity High/Low*** | ***Latency High/Low*** | ***Scalability High/Med/Low (no. of nodes)*** | ***Deployment Strategy*** | ***Suitable Application(s)*** | ***Routing*** |
| OREC [36] | High | High | High | High | Low | Multi-hop | Loss Sensitive Applications | Multi-path Routing |
| DTSN [13] | High | Low | High | High | — | Multi-hop | Multimedia Applications | Omniscient Routing |
| RTSN [37] | High | — | Low | Low | Low (78) | Multi-hop | Structural Monitoring Applications | Beacon Vector Routing (BVR) |
| TRSN [38] | High | Low | Low | — | Low | Static | Loss Sensitive Applications | — |
| RDTS [35] | High | Low | High | Low | Low (60) | Multi-hop | Loss Sensitive Applications | Multi-path Routing |
| DS-DEC [41] | High | Low | Low | — | Low | Multi-hop | — | Shortest Path |
| FBcast [40] | High | — | High | High | High (441) | Multi-hop /Grid | — | Probabilistic Broadcasting |
| CP-diversity [43] | High | High | Low | Low | Med (100) | Multi-hop /Grid | Emergeny / Rescue Applications | AODV / Multi-path |
| MVSA [44] | High | High | Low | Low | — | Multi-hop | Harsh (e.g. Underwater) Environments | Multi-path Multi-sink Routing |
| ARM [45] | High | — | Low | Low | Low (8) | Single/ Two-hop | — | — |
| M-LEACH [46] | — | Low | Low | — | Med (100) | Clustered /Grid | — | — |
| CoDyMAC [48] | High | Low | High | Low | Low | Multi-hop /Random | — | — |

Table 4: Qualitative analysis of redundancy-based reliability schemes

Scalability is another important aspect in WSNs due to deployment in large monitoring areas, where a large number of sensor nodes are required to monitor the desired area in order to collect meaningful information. The analysis of the reliability protocols show that some of the protocols (such as ERP, GRAUDA, and FBcast) provide high scalability, while other protocols (such as PORT, LTRES, and M-LEACH) are more suitable for medium-sized WSNs. Moreover, due to the limited transmission range of the sensor nodes, nodes have to rely on the other nodes (en-route to the sink node) to relay their packets to the sink. All of the analyzed protocols use some form of multi-hop transmission of collected sensor data from the source to the sink nodes. Some of the major underlying protocols used in the analyzed reliability schemes are shortest-path-first, dynamic source routing and adaptive on-demand distance vector routing protocols.

It is also worth mentioning that most of the protocols are evaluated using simulations. Examples of such protocols are ERP using GlomoSim, DST using NS-2 and STCP using the TOSSIM simulator. There are very few protocols that have been experimentally evaluated and tested in real-world test-beds, such as, SWIA based on Mica2 motes and ARM based on IRIS motes.

*5.2.1. Findings and Recommendations*

The qualitative analysis presented in this section compared the performance and effectiveness of the reliability protocols. It identifies protocols that perform significantly better in terms of energy consumption and low transmission overhead in WSNs, and also assesses the protocols using other performance criteria such as scalability, and latency bounds. As energy constraint is the major limiting factor in WSNs, it is critical for the design of the protocols to explicitly account for the limited energy resources of the sensor nodes.

## 6. Conclusion

WSNs hold the promise of many new applications in the field of monitoring and control systems. With the advent of cheap and small sensors, monitoring systems can make use of them to monitor numerous characteristics of the environment. All these applications are built for specific purposes, where maintaining reliable transmission of data from source to destination is one of the most important challenges. To address this issue, we surveyed

the research and state-of-art in reliability schemes and protocols for WSNs. These are analyzed based on our proposed 3D reference model that establishes a common taxonomy to evaluate the research in WSN reliability. This involves different combinations of either retransmission or redundancy techniques that aim to ensure event or packet level reliability by using either end-to-end (connection-oriented) or hop-by-hop (link-oriented) methods.

Retransmission and redundancy are classified as the two main approaches to achieve data transmission reliability in WSNs. Retransmission is the traditional way of ensuring reliability which performs well under high loss environments at the cost of high communication overhead, energy consumption and memory occupancy. Comparatively, redundancy-based mechanisms achieve high reliability with reduced communication, energy and memory requirements, but require high processing overhead. However, the performance of redundancy-based reliability mechanisms degrade under high loss environments.

Packet or event level reliability is concerned with how much sensed data is required by the WSN application to be delivered to the sink in order to achieve the required reliability. Event level reliability as opposed to packet level reliability is sufficient for most event-driven WSNs, where a certain level of packet loss is acceptable as long as sufficient information is delivered to the sink. However, packet level reliability is preferred for the WSN applications (e.g. surveillance) that require the delivery of all the sensed packets at the cost of high energy consumption and possible network congestion.

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. The high hop count in large-scale WSNs introduces more entry points for errors which become the cause of packet loss, thus affecting the reliability. This can be avoided to some extent by using a hop-by-hop method, as it ensures reliability at each intermediate hop from the source to the destination. However, this introduces in-node processing overhead and incurs high overall latency in reporting event information to the sink.

Lastly, the existing literature reflect a lack of research on the use a hybrid mechanism involving both retransmission and redundancy based techniques to provide reliability in WSNs. In view of this, we believe that introducing a hybrid mechanism would play a significant role to further strengthen data transmission reliability. In addition, it would also address the challenge of minimizing the overall energy consumption in a resource constrained WSN.

## 7. Challenges Ahead

There are a number of promising research areas that could be pursued to address the limitations in the existing protocols and extend it further. We conclude this paper with a discussion of the directions in which the existing reliability protocols can be extended.

***Accurate Event Identification:*** Majority of the surveyed protocols aiming to achieve event level reliability ignores the importance of an accurate event identification mechanism by assuming that the event of interest has been accurately identified by the sensor node(s). Thus, one of the major challenges for event reliability protocols is an accurate event identification mechanism, which is an essential characteristic of an event-driven wireless sensor network. Once the events are accurately identified, then only a single packet carrying information about the event would be enough for the sink instead of receiving all the packets from the involved sensor nodes. This approach requires the sensor nodes to suppress the transmission of packets that carry duplicate information about an event, typically those that have been generated by sensors in the same sensing region, by exploiting spatio-temporal correlation [42] among the closely located sensor nodes.

***Non Sink-Centric Data Flow:*** The existing reliability protocols lack the use of in-node data processing [43] as they rely on the sink to regulate the flow of data in order to achieve reliability. This increases the communication overhead which is the highest power consumer in a wireless sensor network. It is worthwhile to note that sensor nodes receiving packets from the sink to control the data flow consumes more energy as transmitting packets themselves [45]. This necessitates the use of a non sink-centric approach that allows each sensor node to make in-node decisions on the need to forward the data to the destination. This reduces the unnecessary packet transmissions at the cost of higher in-node processing, which is becoming increasing feasible with the rapid advances in semiconductor technology.

***Reliability at Medium Access Control (MAC) Layer:*** Cross layer design, a well established research area, can be further exploited to achieve reliability, where closer interaction with the MAC layer would help in solving the channel contention problems while the network layer

helps to find the best route or alternative routes in case of congestion. The existing research on reliability covers the selection of routing algorithms to some extent; however, it lacks an intelligent selection of MAC protocols that needs further attention in order to improve reliability in WSNs. Most WSN reliability mechanisms proposed have simply adopted one of the many existing WSN MACs schemes without specific consideration of how greater interaction with the MAC can enhance reliability.

***Security and Privacy Considerations:*** The deployment of WSNs in unattended areas over a large region (such as in environmental and habitat monitoring applications) and the wireless communication channel of WSNs present an easy target for various security and privacy attacks. The existing reliability protocols suffer from a narrow focus on the technical issues as they are confined only to the reliable transmission of event information to the sink nodes. Existing work ignore the reliability of shared information (i.e. events) in cases of information manipulation (e.g., injecting false information) or corruption of sensor nodes for collection of unauthorized information (e.g., misrouting packets). It is thus desirable to consider the reliability of the collected information by addressing the security and privacy risks in WSNs. Reliability can also be measured from the perspective of how securely the data has been delivered to the sink without being eavesdropped or tampered with.

## References


[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam and E. Cayirci, "Wireless sensor networks: a survey," *Computer Networks*, vol. 38, no. 4, pp. 393-422, 2002.

[2] J. Yick, B. Mukherjee and D. Ghosal, "Wireless sensor network survey," *Computer Networks*, vol. 52, no. 12, pp. 2292-2330, 2008.

[3] S. Nikoletseas, "Models and Algorithms for Wireless Sensor Networks (Smart Dust)," *invited paper in the Proceedings of the 32nd SOFSEM Conference on Current Trends in Theory and Practice of Computer Science*, ser. Lecture Notes in Computer Science (LNCS), Eds. Springer Verlag, vol. 3831, pp. 64-83, 2006.

[4] S. Nikoletseas and J. D. P. Rolim, *Theoretical Aspects of Distributed Computing in Sensor Networks,* Springer Verlag, 2011.

[5] R. Szewczyk, A. Mainwaring, J. Polastre, J. Anderson and D. Culler, "An analysis of a large scale habitat monitoring application," in *Proceedings of the 2nd International Conference on Embedded Networked Sensor Systems* (SenSys), Baltimore, Maryland, pp. 214–226, 03-05 November 2004.

[6] A. Boukerche and S. Nikoletseas, "Protocols for Data Propagation in Wireless Sensor Networks: A Survey," in *Handbook of Wireless Communications Systems and Networks*, Mohsen Guizani (Ed), Kluwer Academic Publishers, pp. 23–51, 2004.

[7] Y. Chen, H. V. Leong, M. Xu, J. Cao, K. Chan and A. Chan, "In-Network Data Processing for Wireless Sensor Networks," in *Proceedings of the 7th International Conference on Mobile Data Management* (MDM), Nara, Japan, pp. 26, 10-12 May 2006.

[8] X. Tang and J. Xu "Extending Network Lifetime for Precision-Constrained Data Aggregation in Wireless Sensor Networks," in *Proceedings of the 25th IEEE International Conference on Computer Communications* (INFOCOM), Barcelona, Catalunya, Spain, pp. 01–12, 23-29 April 2006.

[9] R. Gonzalez and M. Acosta, "Evaluating the impact of acknowledgment strategies on message delivery rate in wireless sensor networks," in *Proceedings of the IEEE Latin-American Conference on Communications* (LATINCOM), Bogota, Colombia, pp. 1 –6, 15-17 September 2010.

[10] S. -J. Park, R. Vedantham, R. Sivakumar, and I. Akyildiz , "A scalable approach for reliable downstream data delivery in wireless sensor networks," in *Proceedings of the 5th ACM International Symposium on Mobile Ad Hoc Networking and Computing* (MobiHoc), Tokyo, Japan, pp. 78–89, 24-26 May 2004.

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

[12] 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, pp. 2819 –2824, 19-23 May 2008.

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

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

[15] 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, pp. 266–276, 25-28 May 2005.

[16] H. Zhang, A. Arora, Y-ri. Choi and M. G. Gouda, "RBC: Reliable bursty convergecast in wireless sensor networks," *Computer Communications*, vol. 30, no. 13, pp. 2560-2576, 2007.

[17] T. Le, W. Hu, P. Corke and S. Jha, "ERTP: Energy-efficient and reliable transport protocol for data streaming in wireless sensor networks," *Computer Communications*, vol. 32, no. 7-10, pp. 1154 – 1171, 2009.

[18] 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, pp. 1 – 9, 01-03 March 2010.

[19] 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, pp. 102 – 112, 11 May 2003.

[20] C.-Y. Wan, A. 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. 04, pp. 862 – 872, 2005.

[21] S.-J. Park, R. Sivakumar, I. Akyildiz and R. Vedantham, "GARUDA: Achieving effective reliability for downstream communication in wireless sensor networks," *IEEE Transactions on Mobile Computing*, vol. 07, no. 02, pp. 214 –230, 2008.

[22] Y. Sankarasubramaniam, O. B. Akan and I. F. Akyildiz, "ESRT: event-to-sink reliable transport in wireless sensor networks," in *Proceedings of the 4th ACM international symposium on Mobile ad hoc networking & computing* (MobiHoc), Annapolis, Maryland, USA, pp. 177–188, 1-3 June 2003,

[23] O. B. Akan and I. F. Akyildiz, "ESRT: Event-to-sink reliable transport in wireless sensor networks," *IEEE/ACM Transactions on Networking*, vol. 13, no. 05, pp. 1003–1016, 2005.

[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, pp. 116-122, 16-18 June 2006.

[25] N. Tezcan and W. Wang, "ART: an asymmetric and reliable transport mechanism for wireless sensor networks," *International Journal of Sensor Networks*, vol. 02, no. 3-4, pp. 188–200, 2007.

[26] Y. Xue, B. Ramamurthy and Y. Wang, "LTRES: A loss-tolerant reliable event sensing protocol for wireless sensor networks," *Computer Communications*, vol. 32, no. 15, pp. 1666 – 1676, 2009.

[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, pp. 730–734, 09-12 January 2011.

[28] Y. Zhou, M. Lyu, J. Liu and H. Wang, "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, pp. 10 pp. –126, 08-11 November 2005.

[29] M. A. Mahmood and W. K. G. Seah, "Event Reliability in Wireless Sensor Networks," in *Proceedings of the 7th International Conference on Intelligent Sensors, Sensor Networks and Information Processing* (ISSNIP), Adelaide, Australia, pp. 01– 06, 06-09 December 2011.

[30] G. Clark, *Error-Correction Coding for Digital Communications*, Plenum Press, 1981.

[31] B. Sklar, *Digital Communications: Fundamentals and Applications*, 2nd Edition, Prentice Hall, 2001.

[32] J. Jeong and C. Ee, "Forward Error Correction in Sensor Networks," in *Proceedings of the First International Workshop on Wireless Sensor Networks* (WWSN), Marrakesh, Morocco, pp. 1–6, 4-8 June, 2007.

[33] S. B. Wicker, *Error Control Systems for Digital Communication and Storage*, Prentice Hall, 1995.

[34] L. Rizzo, "Effective erasure codes for reliable computer communication protocols," *ACM Computer Communication Review*, vol. 27, no. 02, pp. 24 – 36, 1997.

[35] 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, pp. 481–488, 07-09 December 2011.

[36] S. Ali, A. Fakoorian and H. Taheri, "Optimum Reed-Solomon erasure coding in fault tolerant sensor networks," in *Proceedings of the 4th International Symposium on Wireless Communication Systems* (ISWCS), Trondheim, Norway, pp. 6–10, 16-19 October 2007.

[37] S. Kim, R. Fonseca and D. Culler, "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, pp. 449–459, 04-07 October 2004.

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

[39] J. C. Bolot, "End-to-end packet delay and loss behavior in the internet," in *Proceedings of the ACM SIGCOMM Conference on Communications Architectures, Protocols and Applications* (SIGCOMM), San Francisco, California, USA, pp. 289–298, 13-17 September 2005.

[40] R. Kumar, A. Paul, U. Ramachandran and D. Kotz, "On improving wireless broadcast reliability of sensor networks using erasure codes," in *Mobile Ad-hoc and Sensor Networks* (MSN), ser. Lecture Notes in Computer Science, J. Cao, I. Stojmenovic, X. Jia and S. K. Das, Eds. Springer Berlin Heidelberg, vol. 4325, pp. 155-170, 2006.

[41] L. Al-Awami and H. Hassanein, "Energy efficient data survivability for WSNs via Decentralized Erasure Codes," *Proceedings of the IEEE 37th Internatonal Conference on Local Computer Networks* (LCN), Clearwater Beach, FL, USA, pp. 577–584, 22-25 October 2012.

[42] V. B. Priezzhev, D. Dhar, A. Dhar and S. Krishnamurthy, "Eulerian Walkers as a Model of Self-Organized Criticality," in *Physical Review Letters*, vol. 77, pp. 5079–5082, 1996.

[43] Y. Yang, M. Wahlisch, Y. Zhao and M. Kyas, "RAID the WSN: Packet-based reliable cooperative diversity," in *Proceedings of the IEEE International Conference on Communications* (ICC), Ottawa, ON, Canada, pp. 371–375, 10-15 Jun 2012.

[44] W. K. G. Seah and H. P. Tan, "Multipath Virtual Sink Architecture for Wireless Sensor Networks in Harsh Environments," in *Proceedings of the 1st International Conference on Integrated internet ad hoc and Sensor networks* (InterSense), Nice, France, 30-31 May 2006.

[45] C. Wu, S. Ohzahata and T. Kato, "An Adaptive Redundancy-Based Mechanism for Fast and Reliable Data Collection in WSNs," in *Proceedings of the IEEE 8th International Conference on Distributed Computing in Sensor Systems* (DCOSS), Hangzhou, China, pp. 347–352, 16-18 May 2012.

[46] L. P. Damuut and D. Gu, "On redundancy identification in randomly deployed WSNs, another perspective," in *Proceedings of the IEEE Sensors Applications Symposium* (SAS), Texas, USA, pp. 27–32, 19–21 Feb 2013.

[47] M. J. Handy, M. Haase and D. Timmermann, "Cross-layer energy efficiency design in wireless sensor networks," in *Proceedings of the IEEE 4th International Workshop on Mobile and Wireless Communications Network* (MWCN), Stockholm, Sweden, pp. 68–372, 9–11 Sep 2002.

[48] X. Tang and Y. Wang, "Low energy adaptive clustering hierarchy with deterministic cluster-head selection," in *Proceedings of the IEEE 10th World Congress on Intelligent Control and Automation* (WCICA), Beijing, China, pp. 2312–2317, 6–8 Jul 2012.

[49] M. Luby, "LT Codes," in *Proceedings of the 43rd Symposium on Foundations of Computer Science* (FOCS), Vancouver, BC, Canada, pp. 271-280, 16-19 November 2002.

[50] M. C. Vuran, O. B. Akan and I. F. Akyildiz, "Spatio-temporal correlation: theory and applications for wireless sensor networks," in *Computer Networks*, vol. 45, no. 03, pp. 245–259, 2004.

[51] M. K. Kasi and A. M. Hinze, "Cost analysis for complex in-network event processing in heterogeneous wireless sensor networks," in *Proceedings*

*of the 5th ACM International Conference on Distributed Event-Based Systems* (DEBS), New York, USA, pp. 385-386, 11-14 Jul 2011.

[52] Th. Arampatzis, J. Lygeros and S. Manesis, "A Survey of Applications of Wireless Sensors and Wireless Sensor Networks," in *Proceedings of the IEEE International Symposium on Intelligent Control & 13th Mediterranean Conference on Control and Automation* (WCICA), Limassol, Cyprus, pp. 719–724, 27–29 Jun 2005.

[53] Q. Wang and W. Yang, "Energy Consumption Model for Power Management in Wireless Sensor Networks," in *Proceedings of the 4th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks* (SECON), San Diego, California, USA, 18-21 June 2007.