Scientific
Research

A Survey on Modeling and Enhancing Reliability of Wireless Sensor Network

Latha Venkatesan[1], S. Shanmugavel[2], Chandrasekaran Subramaniam[1]
[1]Velammal Engineering College, Anna University, Chennai, India
[2]Anna University, Chennai, India
Email: lathavenkatesanpnag@gmail.com, ssvel@annauniv.edu.in, chandrasekaran_s@msn.com

ABSTRACT

Design of reliable wireless sensor network (WSN) need to address the failure of single or multiple network components and implementation of the techniques to tolerate the faults occurred at various levels. The issues and requirements of reliability improvement mechanism depend on the available resources and application for which the WSN is deployed. This paper discusses the different modeling approaches to evaluate the reliability and classification of the approaches to improve it. Also the paper analyzes reliability enhancement by existing fault tolerant methods in WSN and compares the performance of these techniques with the technique we developed. From the results of the analysis we highlight the challenges and the characteristics of the sensor network affects the reliability and give some scope of future research directions in order to enhance reliability.

1. Introduction

A wireless sensor network is a collection of large number of sensor nodes deployed over the region or inside the target which is to be detected, monitored or tracked. Each sensor node consists of processing capability, memory, a RF transceiver, a power source, and accommodate various sensors and actuators [1]. These nodes self organize into a cooperative network [2] to communicate in an ad hoc fashion and transmit the sensor measurements to the end user. Such systems can revolutionize the way we live and work. Currently, wireless sensor networks are beginning to be deployed at an accelerated pace. It is not unreasonable to expect that in 10 - 15 years that the world will be covered with wireless sensor networks with access to them via the Internet. Many applications have been proposed including environmental, medical, military, transportation, entertainment, crisis management, homeland defense, and smart spaces [3]. These applications may require reliable network for collecting all data without loss from nodes. But on the other hand the inexpensive sensor nodes may not be highly reliable since they are limited in energy, memory space and processing capabilities, and the onboard sensors have direct contact with the environment. This results in error introduced in some of the sensor measurements while sensing, processing or reporting the data to the sink. So in order to improve data integrity and detection reliability [4],

the faulty sensor data have to be detected and filtered out while data without fault are aggregated and sent. Even when the object or event is reliably detected, error may be introduced in mutihop communication due to poor link quality and to improve the network based reliability can be by suitable routing protocol. Also even if the devices and links are working properly, sometimes the event or targets may not get detected due to limited coverage and connectivity and inefficient placement of sensor nodes.

The first task of reliability improvement is to specify reliability requirements as defined by the network maintenance operator (QoS) and/ or end users in terms of operational performance reliability requirements and the operating environment. Reliability requirements address specifications, testing, assessment of the system and services provided by the system. Without defining the requirements the network will not serve its application reliably and also the resources will be wasted. Some common examples of reliability requirements metrics are [5] MTTF (Mean Life or Mean-Time-To-Failure), MTBF (Mean-Time-Between-Failures), failure rate. Once the requirements have been established determine reliability improvement approaches and apply them and measuring the improvement of the performance is the second task. The next task in the reliability improvement process is reliability modeling and testing, to assess its reliability

level. In the early phase for example during the deployment, reliability modeling can be used to predict the network performance to provide information for suitable position of the sensor nodes. Reliability modeling and analysis are key steps to the design and optimization of sensor network systems. There has been little work done in the reliability modeling and analysis of WSN.

The reliability improvement process is an iterative process that is applied step by step in each stage of implementation of WSN. It can be improved one or multiple components like hardware, software or any service/functions of the network in order to achieve minimum required reliability. One of the approaches to improve the reliability of a system is fault tolerance (FT) defined as tolerating the faults which may occur during node placement, topology control, target or event detection, data aggregation, routing and information processing. Fault tolerance, is achieved by hardware or information redundancy. Usually redundancy can result in increased design complexity and increased costs but redundancy is an inherent property of the sensor network. Nodes in WSNs are prone to be failure due to energy depletion, hardware failure, communication link errors, malicious attack etc [6] can be tolerated by hardware and software redundancy, which in turn improves the inherent reliability, and information redundancy and time redundancy will improve the operational redundancy. In general statistical reliability with level β [8] of WSN is a QoS (Quality of Service) level where during every predetermined time window, a predetermined size of random sensed data are delivered to the sink node from every source, each with a probability of at least β. But studying the characteristics, and considering constraints of WSN, it is understood that the overall reliability depends on many aspects spans from reliable sensing to receiving information in the sink and application underlying.

Most of research works with the objective of reliability improvement addresses network transport protocol and improve end-to-end reliability. Reliability improvement is achieved by improving any one or two aspects with minimal consideration of characteristics of the WSN. In this paper we attempt to examine the existing reliability enhancement techniques which will tolerate some faults and compare them based on their performance. The remainder of the paper is organized as follows: In Section 2 the aspects previous survey works are discussed, in Section 3 methods used for modeling and analyzing the reliability of WSN and its classification are explained. In Section 4 the factors influence the reliability of WSN are investigated, in Section 5 various existing reliability enhancement approaches are compared based on the performance and conclusions are made in Section 6.

2. Previous Work

In WSN a large number of sensor nodes continually sense data from the environment and the critical event data need to be reliably delivered to the sink. The sink receives all the information from these sensor nodes, processes it and sends them to the end user. Therefore, given the nature of error prone wireless links, presence of moving nodes and failing nodes, ensuring reliable transfer of data from resource constrained sensor nodes to the sink is one of the major challenges in WSNs. There is extensive research done on reliable transport protocol and survey on existing data transport reliability protocols in wireless sensor networks is presented in [9,13,14]. The network may be congested and sensor nodes may drop packet when the data packets generated by a large number of sensor nodes exceed the network capacity. In order to achieve reliability, the dropped packets must be retransmitted which in turn leads to wastage of energy and bandwidth, very important stringent factors in WSN. Thus the reliability enhancement is achieved with the trade between reliable data transmission and network resources. In order to mitigate this problem, the reliable transport protocol consists of two essential mechanisms: congestion control (detection and avoidance), and loss detection and recovery with the minimum possible energy consumption. A Comparison between the protocols based on the method by which it recover the losses (End to End recovery, Hop to Hop recovery), messages to detect losses control congestion, type and level of reliability, energy efficiency, packet-driven reliability or event-driven reliability. Also a classification of reliability as Packet or event reliability is concerned with how much of information is required to notify the sink of an occurrence of something happening in the environment.

It is well accepted that a sensor network should be deployed with high density, in order to prolong the network lifetime. Sensor data collected from such network is likely to be highly correlated and redundant, so a function density control controls the density of the active sensors to certain level. At any instant of time only a subset of sensor nodes will be active, sensed and report to sink while other sensors are inactive must guarantee sufficient sensing coverage and connectivity reliabilities. The performance metrics of interest are 1) the percentage of coverage, i.e. the ratio of the covered area to the total area to be monitored; 2) the number of working nodes required to provide the percentage of coverage in 1); and 3) α-lifetime, defined as the total time during which at least α portion of the total area is covered by at least one node. The ability to report the Sink node is called as connectivity. A network is said to be fully connected if every pair of node can be communicated with each other either directly or via intermediately relay nodes. It is important to find the minimum number of sensors for a

WSN to achieve the connectivity. The connectivity of a graph is minimum number of nodes that must be removed in order to portion the graph in to more than one connected component. Connectivity affects the robustness and throughput of the wireless sensor network. Both the coverage and connectivity are related to each other for improving the performance of Wireless sensor networks. The issues in maintaining sensing coverage and connectivity by keeping a minimum number of sensor nodes in the active mode in wireless sensor networks are presented in [15,17]. Various approaches to model the coverage are compared based on how they address the issues in coverage; some of them are coverage types, deployment strategy, sensing model, sensing area and nature of the algorithm. The system parameters, such as the initial energy of a node, the radio transmission rate, and the energy consumption rate, are assumed to same for all the nodes.

Sensor network is fault prone in the sense that 1) Consists of low cost, less reliable sensor nodes with limited energy, 2) Sensor nodes are deployed in the unattended hostile environment, 3) Erroneous communication through Low quality Wireless links, 4) Multihop communication between node and sink, leads to low performance and reliability. The nature of faults occurred in the WSN is different from other networks. Additionally, manual inspection of faulty sensor nodes after deployment is typically impractical. Nevertheless, many WSN applications are mission-critical, requiring continuous operation. Thus, in order to meet application requirements reliably, WSN must have the ability to detect and recover from faults, the two mechanisms of FT. The objective of fault detection is to provide any countermeasures, the first step a system must perform is to detect that a specific functionality is or will be faulty. Fault Recovery is, after the system has detected a fault, the next step is to prevent or recover from it. Enhancing the service availability and reliability in WSNs through the use of fault tolerance techniques is presented in [20,21]. These papers explains the taxonomy of classification of faults and the corresponding failure are defined and the methodology to detect the faults and how redundancy is used to recover from failure. The other two techniques of FT are identification and isolation of faults are explained in [22] with respect to WSN. The paper [23] present and classify various approaches for redundancy in the area of wireless sensor networks, related to sensing, communication and information processing.

3. Reliability Modelling and Analysis Methods

Reliability is one of the most important performance measures and high level of reliability is a significant requirement for a wireless sensor networks using in Indus-

trial and medical environments. Reliability level of the network can evaluated using the tool called as reliability modeling. Reliability modeling and analysis are key steps to the design and optimization of sensor network systems. The approach generally taken to investigate the reliability of a highly reliable WSN is

1) Develop a mathematical model of the reliability measure of the network;

2) Measure or estimate the parameters of the model;

3) Compute the network reliability based upon the model and the specified parameters.

During the deployment of WSN, reliability modeling can be used to predict the performance of the network elements to provide the information for the design of WSN suitable for an application in hand. For a network already deployed in the field reliability modeling combined with failure data analysis, can be used to identify the critical components, apply Fault tolerance and enhance reliability.

3.1. Reliability Measure

The There exist a number of reliability measures for a wireless network depending on the network and its applications. For a telecommunication network it is obviously communication issues that meet certain connectivity requirements. Whereas for the sensor network the focus is on information gathering, processing and communication issues to meet the coverage and connectivity requirements. Different criteria can be considered in order to express or measure the reliability of a network. The main ones are the following:

- Reliability measure of connectivity falls within any one of the categories, which are 2-terminal reliability, k-terminal reliability, all terminal reliability and many sources to terminal reliability. For example 2-terminal reliability can be computed using computationally efficient source to terminal path sets or cut sets enumeration algorithm;

- Hardware reliability measure are MTTR and MTTF;

- The coverage reliability measure is guaranteed desired level of coverage (at least k-coverage) of event or target at all times formulated by either Boolean sensing model or collaborative sensing model [25];

- Capacity/Max flow measure is defined as the probability that the maximum flow of the network is not less than the given demand.

- QoS reliability measure is guaranteed date transfer timely and guaranteed bandwidth data accuracy timely depends upon user/applications demand [26];

- Information reliability ensures that the nodes transmit to the sink only information concerning significant events or targets.

Each reliability measure is concerned with the ability of a network to be available to provide the desired ser-

vice to the end user.

3.2. Classification of Reliability Modeling and Evaluation

Reliability of WSN, depends on combination of hardware, software and wireless link is modeled in many ways analogous to reliability modeling of hardware system. Reliability modeling aims at using abstract representation of the network as means for assessing their reliability. The basic reliability modeling techniques available in the existing work in WSN field are classified as shown in **Figure 1.**

Two of the most commonly used *Deterministic reliability modeling* and analysis methods are First Order Reliability Method (FORM) and the Second Order Reliability Method (SORM). The advantages of the techniques is less computational effort than *Probabilistic models*, but not suitable for modeling the reliability of real time applications of WSN. In a more restrictive sense, the term reliability is defined to be the probability that a wireless sensor network performs its mission successfully. Because the mission is often specified in terms of time, reliability is often defined as the probability that a system will operate satisfactorily for a given period of time. Thus reliability may be a function of time and can be estimated essentially using probability modeling. When the set of operating components and the set of failed components of a network are specified, it is possible to compute the probability that the system is operating and thus the reliability of the system. In probabilistic modeling, the concepts and methods of probability theory to compute the reliability of a complex system like sensor network.

Combinatorial model: It can be used to analyze transient or steady state network. These model types are similar in that they capture conditions that make a system fail in terms of the structural relationships between the system components. Various categories exists under combinatorial Model, some of them that are commonly used for WSN are reliability block diagrams, reliability graphs and fault trees. *Reliability block diagrams* (RBD) model has been widely used as one of the most practical reliability modeling tools due to its simplicity. RBD model consists of an input point, an output point, and set of components are combined into blocks in series, in parallel or in k-out-of-n configurations. Each block represents a physical component that functions correctly. The blocks in the RBD are arranged in a proper combination of series and parallel or k-out-of-n such a way that illustrates working components that keep the entire system operational. RBD for data transport in the WSN is discussed in [33] the reliability of data transport is modeled. The Fault tree is a pictorial representation of the combination of events that can cause the occurrence of an undesirable event. It represents all the sequences of individual component failures that cause the system to stop functioning, in a treelike structure. Traditional fault trees can only express the system failure in terms of the combination of component failures through the use of AND, OR, and n-out-of-m logic gates. The occurrence of each event is denoted by a logical 1 at that node; otherwise the logic value of a node is 0. The process of building a fault tree is performed deductively and starts by defining the TOP event, which represents the system failure condition. From this event, and by proceeding backwards, the possible root causes are identified. The events at the bottom of the tree are referred as basic events. If a basic event occurs two or more times in a fault tree it is called a repeated event. Some of the reduction algorithms of Series-parallel formula, VT algorithm the factoring/conditioning algorithms allow to resolve reliability problem in linear time for repeated event fault tree. A three-level hierarchical model for the reliability analysis of a sensor network is given in [34] as top model for the sensor network, the middle level model for sensor node are the fault tree and the bottom level models are Markov chains for individual sensor node components such as the power, sensor, ADC, microcontroller, external memory), tiny OS and channel model. The work in [35] focus on the approach called as sum of disjoint products (SDP) efficiently in fault trees consists of repeated events and it is easily automated in sensor network. The expressive power of the fault tree can be expanded by defining some dynamic gates for describing the modular imperfect coverage behaviour and common-cause failure behaviour of WSN [36]. Basically, a fault tree can be used to model a system with only permanent faults (no transient or intermittent faults) and reconfiguration is not possible. Also assume component failure is independent and state-dependent behaviour
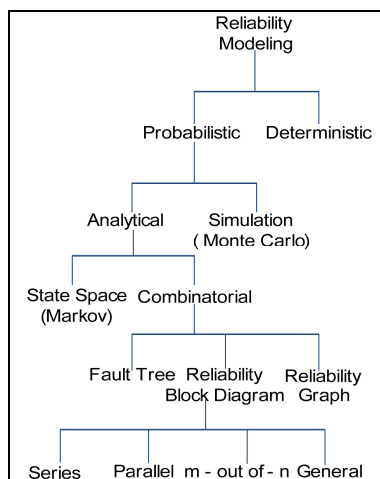

Figure 1. Classification of reliability models.

cannot be modelled. Because fault trees are easier to solve than Markov models, fault trees should be used wherever these fundamental assumptions are not violated. Fault tree and reliability block diagram are called as non state space models.

Path Enumeration methods: A reliability graph is equivalent to a non-series-parallel reliability block diagram and directly analyzed by many algorithms to resolve the reliability problem. Any communication network can be considered as directed graph G = (V, E), where V—vertices represents the sensor nodes and sinks, Eedges represents the link between the two nodes. Graphical modeling is the exact method in which there are two classes for the computation of the network reliability, which are path or cut enumeration methods and network reduction methods. In path enumeration method, first step is the enumeration of all the minimum paths for a working network to provide a Boolean expression called as Structure function. These minimal paths are different for each reliability problem. For example two terminal reliability of the network is the probability that there exist atleast one or more successful paths from the target sensor node to the sink. The second step is computation of this Boolean expression probability. The computational problem to determine the complete set of minimal paths or cuts and to construct and evaluate the structure and reliability functions is difficult. In general, if there are k cuts or paths, the corresponding reliability equation will have $(2^k - 1)$ terms. Several techniques available to reduce the structure function and compute the reliability in polynomial time. WSN application for structure health monitoring can represented by a propositional directed acyclic graph (PDAG) through which the reliability is evaluated in three steps [49]. In first step the connectivity information of the network is represented in the matrix form and using LDF algorithm, the structure function is determined. The structure function consists of connectivity to node and link connected using logical AND, OR operators. In the second step the complex network structure function is reduced by introducing the context sensitive information of sensor network. The context of a wireless sensor network may be expressed in terms of the network elements or the conditions in which the sensor nodes are deployed. The third step is computation of network reliability for the reduced context aware structure function is obtained by assigning the probabilities of connectivity to the nodes and the edges. The reduced expression consists of minpaths from source to sink, connected by logical operators and the reliability of the WS network is the reliability of that min path which has the maximum reliability out of many min paths.

In the network reduction algorithms are based on graph topology, reduce the size of the graph by removing some structures. Then it is possible to compute the reli-ability in linear time and the reduction will result in a single edge. The Binary Decision Diagram (BDD) structure provides compact representation of Boolean expressions and is used to work out the terminal reliability of the links. Set of algorithms for efficient construction and manipulation of BDD structure. An enhanced ordered binary decision diagram (OBDD) algorithm is proposed in [37] to evaluate the reliability of wireless sensor networks (WSNs), based on the considerations of the common cause failure (CCF) and a large number of nodes in WSNs. It is also shown that OBDD can decrease the cost of OBDD constructions and storage. Decomposition algorithms compute k-terminal reliability in linear time by decomposing the graph into sub graphs. k-coverage and k-connectivity reliability can be computed as the product of coverage or connectivity probability of all nodes and links in the path [27,28]. The performance metrics of WSN-Packet delivery ratio [29], message delay [30] with a reasonable overhead (in terms of retransmissions, acknowledgement messages, and control messages) is also measured. For computation of reliability the probability of link existence and failure rate of node are not only considered but also reliability of a node depends on various environmental parameters such as noise, temperature, pressure and magnetic effects are also considered. The development of reliability model needs to take in account all of these parameters [31].

State enumeration methods: A very basic method of *Markov modeling* to compute the sensor network reliability involve enumerating all possible states of the network based on the states of its components, all possible transition between those state and rate parameters of those transitions. In reliability modeling the possible states are healthy and failed. The reliability of fault tolerant WSN is modeled and analyzed in [38-40] using Markov modeling technique A network with "n" number of elements there are 2^n possible states termed as state space explosion. Thus it becomes computational unfeasible for a network with large number of elements since the network reliability problem is NP-hard. So the states that results in successful network operations are identified in Hidden Markov model and the probability of occurrence of each successful state is calculated. The reliability of the network is the sum of all successful state probabilities. Markov reward modeling is more powerful techniques suitable for reconfigurable and fault tolerant networks with redundancies and failure dependencies. A Generalized Stochastic Petri nets (GSPN) model is designed to evaluate the reliability of a parallel-redundant fault tolerant WSN. Unlike Markov model, GSPN is more observable, scalable and portable. The enumeration methods provides an exact solution of reliability problems, yet the method becomes computationally expensive for the analysis of large networks since the number of

possible configurations increases exponentially with the number of mobile nodes. So the enumeration methods can be employed for networks of relatively small size and there is a need of faster computational procedures that can provide an accurate approximation of complex WSN. In [43] paper, the author present a hexagon tessellation sensor network model with role assignment scheme and estimate the reliability and lifetime distribution by employing a new improved *Monte Carlo scheme* which incorporates both simulation and analytic methods and is suitable for the WSN. Also it is shown that the node sub-roles and node density have important effects on the network reliability and lifetime. A new concept known as event reliability is defined in [44] and the author propose Event Reliability Protocol (ERP), an event-to-sink reliability protocol that serves to improve the scalability of event detection in a WSN by minimizing the unnecessary retransmission of data packets coming from multiple nodes in an event's locality. The performance of the protocol is simulated and Event reliability is analysed using a network simulator GloMoSim.

Characteristic aspects of sensor networks such as limited accessibility and dynamic topology changes complicate the usage of traditional reliability evaluation methods. The limitations of the traditional models overcome by presenting [45] a model-based approach to assess the reliability of redundant sensor networks.

Weibull failure model can be used in reliability theory to model the time to failure or life time modelling presented in [46] to examine the coverage and reliability of distributed sensor networks that are designed for surveillance applications. In Weibull distribution the failure rate is proportional to a power of time and it can be used to model life time of WSN defined as the time to first failure. In the reliability modeling field, we sometimes encounter systems with uncertain structures, and the use of fault trees and reliability diagrams is not possible. To overcome this problem, Bayesian approaches offer a considerable efficiency in this context. The paper [47] introduces recent contributions in the field of reliability modeling with the Bayesian network approach. Bayesian reliability models are applied to systems with Weibull distribution of failure. The advantages of this modeling approach are presented in the case of systems with an unknown reliability structure, those with a common cause of failures and redundant ones.

4. Factors Affecting Reliability in WSN

A basic way to improve the reliability is to have redundant components; it may be hardware, software or information. Reliability analysis of the WSN provides a measure of the performance of the WSN. As the importance of reliability in WSN is discussed in the previous section, this section it is appropriate to investigate the

factors affecting reliability so that the reliability can be improved by improving these parameters. In order to ensure that the network supports the application's requirements, it is important to understand how each of the categories of wireless sensor networking affects reliability. Challenges to achieving reliability on Wireless Sensor Networks can be divided to four main categories which are network elements, networking characteristics, conditions in which WSN is deployed and strategies used to design the network for an application are represented in **Figure 2**.

The first kind of problems comes from the limited resources of Wireless Sensor Networks nodes. A sensor node has a limited power without recharging capability affects the hardware reliability. The node is able to sense the environment using sensors and ADC used to convert to digital signal has low accuracy and low resolution will affect the information reliability. Similarly the processor with low computational power and memory space affects the Quality of Information (QoI).

Next kind of problems comes from software engineering point of view adds more challenges to achieve reliability of sensor network. In general, sensor networks software can be layered into levels: sensor node software, middleware and sensor network software. The sensor node software is the bottom layer contains sensor software and node software. The sensor software (Operating System) has full access to the sensor hardware, execute the process by which events occurred in the real world is sampled and converted into machine-readable signals. Malfunction or bucks in the software or programs will affect the QoS and information reliability. The node software process the raw data, receive and process the query and transmit the data to toe next node includes system software for network maintenance and application specific software related with packet reliability.
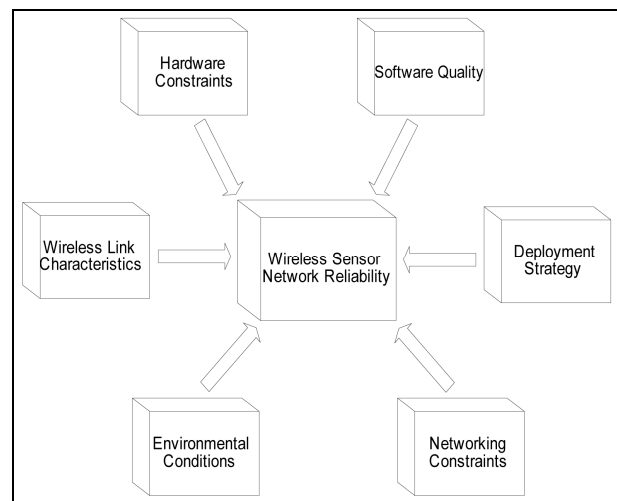

Figure 2. Factors Influence the reliability in WSN.

Next level, a collection of common services for application development, called middleware; reside over the operating system related with service reliability. Application programs use this middleware according to their own specific requirements; these programs often access the individual node resources and local services. Finally, the sensor network software specifies the main tasks and required services of transporting the data and query through the network, maintain the performance and achieve network reliability.

Third sort of problems are related to the networking characteristics and nature of wireless communication link. The asymmetry of links makes link quality estimation hard and invalidates many assumptions made in other environments. Correlated losses due to obstacles, mobility and interference can lead to consecutive losses, decreasing the effectiveness of erasure code. Weak correlation between quality and distance, hidden terminal problems, and dynamic change of connectivity complicates the situation further [48]. In addition, as its communication bandwidth is narrow, overhead due to the error correcting coding cannot be added with the data packet. All these features of wireless communication link degrade the transport or packet reliability.

Fourth kind of problems raised by the environmental conditions affects the sensing unit and wireless transceiver components of a sensor node since they directly interact with the environment, which is subject to variety of physical, chemical, and biological factors. The probability that a sensor suffers a physical attack in such an environment is therefore much higher. It results in low reliability of performance of sensor nodes. Even if condition of the hardware is good, the communication between sensor nodes is affected by many factors, such as signal Strength, antenna angle, obstacles, weather conditions, and interference [50].

Fifth set of problems related to strategies used to build the application which includes deployment, scalability, security and responsiveness. Deployment strategy is an important issue to place the sensor nodes, relay nodes, base station and sink in the proper position to maximize coverage, connectivity, detection and communication reliability and thus improve the life time of the sensor network. Given the area to be covered, energy, range of sensing and transmission radius of the node, many techniques are available for calculating the number and position of the nodes. Many aspects of WSN like topology management, power management, and routing requires suitable placing of the nodes deployment problem can be stated in many ways and there is no one systematic methodology for solving the deployment problem. But improper deployment may hamper the service provided by the sensor network which leads decrement the overall network reliability. In typical wireless ad hoc networks, reliability and scalability are always inversely coupled. In other words, it becomes more difficult to build a reliable ad hoc network as the number of nodes increases. This is due to the network overhead that comes with the increased size of the network.

Because of the nature of wireless communications, resource limitation on sensor nodes, size and density of the networks, unknown topology prior to deployment, and high risk of physical attacks to unattended sensors, it is a challenge to provide security in WSNs. Security attacks modify the information by packet damage and render the information unavailable by dropping the packets affects the information and packet reliability. Wireless networks are vulnerable to security attacks due to nature of wireless communications, resource limitation on sensor nodes, size and density of the networks, dynamic topology and the attackers may device different types of security threats to make the WSN system unstable. Typical treats and adequate defense techniques in WSNs are summarized in [51]. The security mechanisms are actually used to detect, prevent and recover from the security attacks. A wide variety of security schemes to counter malicious attacks and these can be categorized and listed in [52]. But the question is how much the security mechanisms are secure? The reliability of security systems is connected with proper implementation of software and hardware components of security systems. When security of information systems is considered it is needed to analyze three attributes: confidentiality, availability and integrity. If these goals are not met then no proper routing, clustering, aggregation process carried over in a WSN and the reliability will certainly decreases. Responsiveness is the ability of the network to quickly adapt itself to changes in topology. To achieve high responsiveness, an ad hoc network should issue and exchange more control packets, which will naturally result in less scalability and less reliability.

5. Reliability Improvement in WSN

The approaches proposed to reinforce the network reliability, provide a method for maximizing reliability under certain given constraints and WSN has sensor node constraints like battery power, transmission range, sensing range and processor capability. In addition network constraints are ad hoc nature, data rate, packet size, wireless link, scalability, security, dynamic topology and cost constraints. For WSN the focus is on sensing, processing and communication issues that meet some reliability measures and requirements. The communication issue has to meet the connectivity requirements so that the end user is able to access the network and receive the information sensed and processed by the sensor nodes. Achieving the overall network reliability of the communication process is to construct a network the minimum

number of reliable links and each link must be economically feasible. The transport layer of WSN provides mechanisms for establishing a connection between sensor network and end users, while supporting Quality of Service (QoS) mechanisms to ensure the properties of the link lives up to a required quality of connection and reliability. In general, there are several approaches to achieve reliability against unreliable link, e.g., automatic repeat request, multi-path routing and source coding. On the other side the overhead increases and network become overloaded. That is, these traditional approaches are not suitable for WSN, many research works concentrate in improving the existing transport layer protocols or developing new efficient reliable data transfer scheme that satisfy the constraints and improve the performance. To cope with the above issues, many works has been proposed for efficient reliable data transfer scheme, some of them are network coding [53], cross-layer strategy that considers physical layer (*i.e.*, power control), MAC layer (*i.e.*, retransmission control) and network layer (*i.e.*, routing protocol) jointly [54], hybrid method based on multipath data sending [55] and behavior-based trust mechanism [56].

Scalability is networking constraint and can be meet

out in WSN through efficient clustering. The cluster head node is used to receive data from other nodes in the cluster, aggregate it and then transmitting the processed information. Data aggregation is a process whereby data from sensors in an area is gathered for performing fusion to eliminate redundant data to provide the useful fused information to the base station and improve reliability and life time of the network. The clustering and cluster head selection process involves many issues of power efficiency [57], traffic distribution, link quality distance to sink etc to guarantee reliability. Aggregated values when transmitted to sink, aggregated values from other clusters can be fused using in the intermediate nodes to reduce traffic in WSN. Rule based Fuzzy logic, trust based, weight based, rough set theory are some of the secure and reliable techniques to tolerate faulty nodes and improve the credibility of the fused content in the presence malicious nodes.

Sensors deployed in the real world senses the physical parameters include temperature, acoustics, light and pollution. Sensor network in the war field need to detect, classify and track the objects in the vicinity. The reliability can be defines as the successful detection by a node to correctly estimate a target's presence while avoiding

Table 1. Comparison of reliability improvement techniques.

Name of the protocol/ technique	Reliability enhanced	Constraints satisfied	Performance improved	Techniques used
E²SRT [32]	Event-to-sink reliability	Dynamic topology, unreliable link	Energy efficiency	Including congestion control and reducing convergence time
GARUDA [10]	Multiple reliability semantics	Packet size, retransmission overhead	Latency, energy efficiency	Loss recovery through minimum dominating set
RCRT [11]	End-to-end reliability	Asymmetric link, hardware constraints	Network efficiency and flexibility	Implementing NACK based end-to-end loss recovery scheme
ZARB [12]	Packet reliability	More broadcast coverage time	Network efficiency	Active & passive ACK packets broadcasting
HERO [19]	Bi-directional packet delivery	Node and network constraints	Energy efficiency and life time	Efficient clustering technique
Data fusion with [41] desired reliability	Transmission and information reliability	Unreliable data fusion structure	Energy efficiency	Fusion depends upon amount of information weight
Improved CICADA [28]	End-to-end	Mobility	Throughput, reduced retransmission, delay, energy efficiency	Randomization and overhearing
Simple CRT based packet forwarding [18]	Packet forwarding	Unreliable channels, dynamic topology changes and MAC overhead	Power saving, simplicity, and fair distribution of energy consumption	Packet-splitting algorithm based on the Chinese Remainder Theorem (CRT)
EIRDA [24]	Clustering	Security	Energy efficiency, life time, fault tolerance	Functional reputations for sensing, aggregation and routing implemented using beta-distribution function to evaluate trustworthiness
CAP [7]	Event reporting	Node constraint	Fault tolerance	Collaborative aggregation
Collaborative distributed detection [16]	Information reliability	Faulty nodes	Energy efficiency, life time, fault tolerance	Coefficients of a regression Polynomial, aggregation the median information, and judges the final state of the event-region

false detections in which no target is present. Hence to increase the accuracy of the detection algorithm it becomes necessary to fuse the measurements of a group of sensors while discard the faulty nodes. Faults are encountered at any stage of WSN development, from the high-level design of embedded software down to hardware faults, energy failures, or harsh environmental conditions. This makes it necessary to add fault tolerance capability to tolerate the faulty hardware/software/functions, so that the overall reliability of the surveillance system can be improved. A fault diagnostic model using case based reasoning technique in a Wireless Sensor Network (WSN) for Wildlife Preservation application is proposed in [42]. In the case based reasoning, semantic tracking is applied to detect the various faults in the hardware and software modules utilized in the sensors over different zones, network and service levels. The correctness and context of the data is checked using the semantic engine with verification rules. The fault detection in WSN can be improvised using the algorithms proposed in this work. The first part of the algorithm decides the occurrence of fault based on a Fault Ontology for REpetitive Semantic Tracking (FOREST) and the second part using the Weak Inactive Link Data (WILD) method to locate the fault in the corresponding cluster or the device. Some of the approaches/protocol/techniques used in WSN to enhance its reliability are compared in **Table 1.**

6. Conclusion

Various design, deployment and functional aspects of a reliable WSN are analyzed in this paper. Also the necessity and requirements of reliability in WSN applications are discussed in detail. The existing research works with the notion of improving reliability are studied elaborately, compared based on their performance and reliability measures. Many of the works are available to improve the communication reliability of WSN by modifying the existing MAC, routing and transport protocols. Many methodologies to improve the sensing and coverage reliability are developed exceptionally for WSN by improving the aggregation and deployment techniques. On analyzing the works, it is shown that the reliability can efficiently improved by adopting fault tolerance in the design of various functions especially event/target detection and data aggregation/fusion techniques. It is understood that all reliability techniques concentrate in energy efficiency and are aimed to improve the life time of the network. At the same time less number of works are available to satisfy the other node and network constraints of WSN and improve QoS parameters. Also need to develop the concept to define the relation between security and reliability, quantify information security, design and testing methodologies based on the application and services provided by WSN.

REFERENCES

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam and E. Cayirci, "Wireless Sensor Network: A Survey," *IEEE Communications Magazine*, Vol. 40, No. 8, 2002, pp. 102-114. doi:10.1109/MCOM.2002.1024422

[2] J. Agre and L. Clare, "An Integrated Architecture for Co-operative Sensing Networks," *IEEE Journal Computer*, Vol. 33, No. 5, 2000, pp. 106-108. doi:10.1109/2.841788

[3] J. A. Stankovic, "Wireless Sensor Networks," *IEEE Computer*, Vol. 41, No. 10, 2008, pp. 92-95. doi:10.1109/MC.2008.441

[4] R. Kim, J. Song and B. F. Spencer, Jr., "Reliability Analysis of Wireless Sensor Networks," *Proceedings of the Workshop on Advanced Smart Materials and Smart Structures Technology*, Dalian, July 2011, pp. 1-12.

[5] D. Bein, V. Jolly, B. Kumar and S. Latifi, "Reliability Modeling in Wireless Sensor Networks," *International Journal of Information Technology*, Vol. 11, No. 2, 2005, pp. 1-9.

[6] H. Liu, A. Nayak and I. Stojmenović, "Fault Tolerant Algorithms/Protocols in Wireless Sensor Networks" In: S. C. Misra, I. Woungang and S. Misra, Eds., *Guide to Wireless Sensor Networks*, Springer Veglag, London, 2009, pp. 261-291. doi:10.1007/978-1-84882-218-4_10

[7] W. Yuan, S. V. Krishnamurthy and S. K. Tripathi, "Improving the Reliability of Event Reports in Wireless Sensor Networks," *Proceedings of the* 9*th International Symposium on Computers and Communications*, Vol. 1, 2004, pp. 220-225.

[8] Z. Rosberg, R. P. Liu, T. L. D. Yi, F. Dong and S. Jha, "Statistical Reliability for Energy Efficient Data Transport in Wireless Sensor Networks," *Springer Journal Wireless Networks*, Vol. 16, No. 7, 2010, pp. 1913-1927. doi:10.1007/s11276-009-0235-5

[9] A. Ayadi, "Energy-Efficient and Reliable Transport Pro- -tocols for Wireless Sensor Networks: State-of-Art," *Journal Wireless Sensor Network*, Vol. 3, No. 3, 2011, pp. 106-113. doi:10.4236/wsn.2011.33011

[10] S.-J. Park, R. Vedantham, R. Sivakumar and I. F. Akyildiz, "GARUDA: Achieving Effective Reliability for Downstream Communication in Wireless Sensor Networks," *IEEE Transactions On Mobile Computing*, Vol. 7, No. 2, 2008, pp. 214-230. doi:10.1109/TMC.2007.70707

[11] J. Paek and R. Govindan, "RCRT: Rate-Controlled Reliable Transport for Wireless Sensor Networks," *ACM Transactions on Sensor Networks*, Vol. 7, No. 3, 2010, pp. 305-317. doi:10.1145/1807048.1807049

[12] T.-W. Sung, T.-T. Wu, C.-S. Yang and Y.-M. Huang, "Reliable Data Broadcast for Zigbee Wireless Sensor Networks," *International Journal On Smart Sensing And Intelligent Systems*, Vol. 3, No. 3, 2010, pp. 504-520.

[13] A. G. Bagadi, S. Sarode and J. W. Bakal, "A Survey of Reliable Transport Layer Protocols for Wireless Sensor Network," *International Journal of Computer Applications*, Vol. 33, No. 1, 2011, pp. 44-50.

[14] K. K. Sharma, R. B. Patel and H. Singh, "A Reliable and Energy Efficient Transport Protocol for Wireless Sensor Networks," *International Journal of Computer Networks & Communications*, Vol. 2, No. 5, 2010, pp. 92-103. doi:10.5121/ijcnc.2010.2506

[15] J. J. Winston and B. Paramasivan, "A Survey on Connectivity Maintenance and Preserving Coverage for Wireless Sensor Networks," *International Journal of Research and Reviews in Wireless Sensor Networks*, 2011, Vol. 1, No. 2, pp. 11-18.

[16] Z. ShuKui, G. ShengRong, C. ZhiMing and F. J. Xi , "A Reliable Collaborative Detection Scheme of Event-Region in Wireless Sensor Networks," *Proceedings of the International Symposium on Information Processing*, 2009, pp. 021-024.

[17] G. J. Fan and S. Y. Jin, "Coverage Problem in Wireless Sensor Network: A Survey," *Journal of Networks*, Vol. 5, No. 9, 2010, pp. 1033-1040.

[18] G. Campobello, A. Leonardi and S. Palazzo, "Improving Energy Saving and Reliability in Wireless Sensor Networks Using a Simple CRT-Based Packet-Forwarding Solution," *EEE/ACM Transactions on Networking*, Vol. 20, No. 1, 2012, pp. 191-205.

[19] E. Cañete, M. Díaz, L. Llopis and B. Rubio, "HERO: A Hierarchical, Efficient and Reliable Routing Protocol for Wireless Sensor and Actor Networks," *Computer Communications* Vol. 35, No. 11, 2012, pp. 1392-1409. doi:10.1016/j.comcom.2012.04.003

[20] R. V. Kshirsagar and B. Jirapure, "A Survey on Fault Detection and Fault Tolerance in Wireless Sensor Networks," *International Journal of Computer Applications*, Vol. 3, No. 1, 2011, pp. 130-138.

[21] S. Mishra, L. Jena and A. Pradhan, "Fault Tolerance in Wireless Sensor Networks," *International Journal of Advanced Research in Computer Science and Software Engineering*, Vol. 2, No. 10, 2012, pp. 146-153.

[22] L. Paradis and Q. Han, "A Survey of Fault Management in Wireless Sensor Networks," *Journal of Network and Systems Management*, Vol. 15, No. 2, 2007, pp. 171-190. doi:10.1007/s10922-007-9062-0

[23] F. Koushanfar, M. Potkonjak, A. Sangiovanni-Vincentelli, "Fault Tolerance Techniques for Wireless Ad Hoc Sensor Networks," *Proceedings of the IEEE Conference Sensors*, Vol. 2, 2002, pp. 1491-1496. doi:10.1109/ICSENS.2002.1037343

[24] H. Sethi, D. Prasad and R. B. Patel, "EIRDA: An Energy Efficient Interest based Reliable Data Aggregation Protocol for Wireless Sensor Networks," *International Journal of Computer Applications*, Vol. 22, No. 7, 2011, pp. 20-25.

[25] X. Chen, "On Fault Tolerance, Performance, and Reliability for Wireless and Sensor Networks," Ph.D. Thesis, The Chinese University of Hong Kong, Hong Kong, 2005.

[26] E. Felemban, C.-G. Lee and E. Ekici, "MMSPEED: Multipath Multi-SPEED Protocol for QoS Guarantee of Reliability and Timeliness in Wireless Sensor Networks," *IEEE Transactions on Mobile Computing*, Vol. 5, No. 6, 2006, pp. 738-754.

[27] Y.-L. Jin, H.-J. Lin, Z.-M. Zhang, Z. Zhang and X.-Y. Zhang, "Estimating the Reliability and Lifetime of Wireless Sensor Network," *Proceedings of the 4th International Conference on Wireless Communications, Networking and Mobile Computing*, October 2008, pp. 1-4.

[28] B. L. Braem, B. Blondia, C. Moerman and I. Demeester, "Improving Reliability in Multi-Hop Body Sensor Networks," *Second International Conference on Sensor Technologies and Applications*, August 2008, pp. 342-347.

[29] J. Shin, U. Ramachandran and M. Ammar, "On Improving the Reliability of Packet Delivery in Dense Wireless Sensor Networks," *Proceedings of the 16th International Conference on Computer Communications and Networks*, August 2007, pp. 718-723.

[30] H. M. F. AboElFotoh, S. S. Iyengar and K. Chakrabarty, "Computing Reliability and Message Delay for Cooperative Wireless Distributed Sensor Networks Subject to Random Failures," *IEEE Transactions on Reliability*, Vol. 54, No. 1, 2005, pp. 145-156. doi:10.1109/TR.2004.842540

[31] N. V. Doohan, D. K. Mishra and S. Tokekar, "Reliability Analysis for Wireless Sensor Networks Considering Environmental Parameters Using MATLAB," *Proceedings of the 3rd International Conference on CICSN*, 2011, pp. 99-102.

[32] S. Kumar, Z. Feng, F. Hu and Y. Xiao, "E2SRT: Enhanced Event-to-Sink Reliable Transport for Wireless Sensor Networks," *Journal of Wireless Communications and Mobile Computing*, Vol. 9, No. 10, 2009, pp. 1301-1311. doi:10.1002/wcm.705

[33] F. K. Shaikh, A. Khelil and N. Suri, "On Modeling the Reliability of Data Transport in Wireless Sensor Networks," *Proceedings of 15th EUROMICRO International Conference on Parallel, Distributed and Network-Based Processing*, Feburary 2007, pp. 395-402.

[34] D. S. Kim, R. Ghosh and K. S. Trivedi, "A Hierarchical Model for Reliability Analysis of Sensor Networks," *Proceedings of the 16th IEEE Pacific Rim International Symposium on Dependable Computing*, December 2010, pp. 247-248.

[35] I. Silva, L. A. Guedes, P. Portugal and F. Vasques, "Reliability and Availability Evaluation of Wireless Sensor Networks for Industrial Applications," *Sensors*, Vol. 12, No. 1, 2012, pp. 806-838. doi:10.3390/s120100806

[36] L. Xing and H. E. Michel, "Integrated Modeling for Wireless Sensor Networks Reliability and Security," *Proceedings of the Annual Conference on Reliability and Maintainability Symposium*, January 2006, pp. 594-600.

[37] Y.-F. Xiao, S.-Z. Chen, X. Li and Y.-H. Li, "Reliability Evaluation of Wireless Sensor Networks Using an Enhanced OBDD Algorithm," *Proceedings of the IEEE International Conference on Communications*, 2009, pp. 453-457.

[38] W. W. Bein, D. Bein and S. Malladi, "Reliability and Fault Tolerance of Coverage Models for Sensor Networks," *International Journal of Sensor Networks*, Vol. 5, No. 4, 2009, pp. 199-209. doi:10.1504/IJSNET.2009.027628

[39] V. Kumar, R. B. Patel, M. Singh and R. Vaid, "Reliability

Analysis in Wireless Sensor Networks," *International Journal of Engineering and Technology*, Vol. 3, No. 2, 2011, pp. 74-79.

[40] A. Munir and A. Gordon-Ross, "Markov Modeling of Fault-Tolerant Wireless Sensor Networks," *Proceedings of* 20*th International Conference on Computer Communications and Networks*, August 2011, pp. 1-6.

[41] H. Luo, H. Tao, H. Ma and S. K. Das, "Data Fusion with Desired Reliability in Wireless Sensor Networks," *IEEE Transactions on Parallel and Distributed Systems*, Vol. 22, No. 3, 2011, pp. 501-512. doi:10.1109/TPDS.2010.93

[42] V. Latha, C. Subramaniam and S. Shanmugavel, "Fault Tolerant Wireless Sensor Network Using Case Based Reasoning with Semantic Tracking," *Proceedings of the WSEAS International Conference on Communications*, July 2011, pp. 240-246.

[43] M. A. Mahmood and W. K. G. Seah, "Event Reliability in Wireless Sensor Networks," *Proceedings of* 7*th International Conference on Intelligent Sensors*, *Sensor Networks and Information Processing*, 2011, pp. 377-382.

[44] K. El-Darymli, F. Khan and M. H. Ahmed, "Reliability Modeling of Wireless Sensor Network for Oil and Gas Pipelines Monitoring," *Sensors* & *Transducers Journal*, Vol. 106, No. 7, 2009, pp. 16-26.

[45] E. G. Rowe and T. A. Wettergren, "Coverage and Reliability of Randomly Distributed Sensor Systems with Heterogeneous Detection Range," *International Journal of Distributed Sensor Networks*, Vol. 5, No. 4, 2009, pp. 303-320. doi:10.1080/15501320802299853

[46] A. Taherkordi, M. A. Taleghan and M. Sharifi, "Achieving Availability and Reliability in Wireless Sensor Networks Applications," *Proceedings of the* 1*st International Conference on Availability, Reliability and Security*, 2006, pp. 529-535. doi:10.1109/ARES.2006.21

[47] A. Zaidi, B. O. Bouamama and M. Tagina, "Bayesian Reliability Models of Weibull Systems: State of Art," *International Journal of Applied Mathematics and Computer Science*, Vol. 22, No. 3, 2012, pp. 585-600.

[48] P. S. Patheja, A. Waoo and P. Shrivastava, "Fault Tolerant, Energy Saving Method for Reliable Information Propaga- tion in Sensor Network," *International Journal of Smart Sensors and Ad Hoc Networks*, Vol. 1, No. 4, 2012, pp. 34-38.

[49] L. Venkatesan, C. Subramaniam and S. Shanmugavel, "Reliability Modeling of Context Aware Wireless Sensor Network," *International Journal of Information and Electronics Engineering*, Vol. 2, No. 5, 2012, pp. 710-715.

[50] S. Kim and R. Fonseca, "Reliable Transfer on Wireless Sensor Networks," *Proceedings of the* 1*st Annual IEEE Communications Society Conference on Sensor and Ad Hoc Communications and Networks*, October 2004, pp. 449-459.

[51] Z. S. Bojkovic, B. M. Bakmaz and M. R. Bakmaz, "Security Issues in Wireless Sensor Networks," *International Journal of Communications*, Vol. 2, No. 1, 2008, pp. 106-115.

[52] H. C. Chaudhari and L. U. Kadam, "Wireless Sensor Networks: Security, Attacks and Challenges," *International Journal of Networking*, Vol. 1, No. 1, 2011, pp. 04-16.

[53] T.-G. Li, C.-C. Hsu and C.-F. Chou, "On Reliable Transmission by Adaptive Network Coding in Wireless Sensor Networks," *Proceedings of the IEEE International Conference on Communications*, June 2009, pp. 1-5.

[54] H. Kwon, T. H. Kim and S. Choi, "A Cross-Layer Strategy for Energy-Efficient Reliable Delivery in Wireless Sensor Networks," *IEEE Transactions on Wireless Communications*, Vol. 5, No. 12, 2006, pp. 1-11. doi:10.1109/TWC.2006.256992

[55] S. Saqaeeyan and M. Roshanzadeh, "Improved Multi-Path and Multi-Speed Routing Protocol in Wireless Sensor Networks," *International Journal of Computer Network and Information Security*, Vol. 4, No. 2, 2012, pp. 8-14. doi:10.5815/ijcnis.2012.02.02

[56] T. Ryutov and C. Neuman, "Trust based Approach for Improving Data Reliability in Industrial Sensor Networks," ftp://ftp.isi.edu/isi-pubs/tr-631.pdf

[57] K. Maraiya, K. Kant and N. Gupta, "Efficient Cluster Head Selection Scheme for Data Aggregation in Wireless Sensor Network," *International Journal of Computer Applications*, Vol. 23, No. 9, 2011, pp. 10-18.