Investigation of Faults, Errors and Failures in Wireless Sensor Network: A Systematical Survey

Karthick Raghunath K.M[1], Rengarajan N[2]

Abstract

This article addresses the behavioral characteristics of faults, errors and failures in wireless sensor network. Viable usage of compact limited resource constrained microsensors for advance deployment tends to face more challenges during the execution of various event handling and this action reflects to obtain deviated result from reaching the targeted goals. Achieving the targeted goals beyond the limitations necessitate special investigation of possible arising faults. Although many fault management approaches are addressed, none has focused on faulty issues at the wireless sensor network protocol stack level and also at sensor nodes' component side. Addressing and exploring various impacts of faults, errors and failures at different layers of wireless sensor network protocol stake and at the level of inter-functional units of sensor node components are concerned to be the main theme of this paper. Moreover, the overall investigation along with three phases (prevention, diagnosis, and recovery) of fault management furnishes generic life-cycle of fault tolerance management with potential basic relevant parameters.

Keywords

Wireless sensor networks, Faults, Errors, Failures, Fault Tolerances, Protocol-Stack, Sensor nodes component, Fault management Lifecycle.

1. Introduction

Recent research exploring advancements in Wireless Sensor Network (WSN) yields many challenges and intends researchers to deal with problem of energy management, difficulties to achieve efficient processing and communication Pattern, Structuring of proper control management for sensor data protocol as well as deploying topology, designing of Fault Tolerance (FT) system, and so on. Since WSN are composed of more compact microsensors, they are more prone to failures. Moreover capability of utilizing the resource by such microsensors also restricted. To make available WSN applications more pervasiveness in the real world, examining WSN with respect to faults/failures is concerned to be the most viable nature of many ideologies.

Vigorous nature of various faults degrades the life-span quality of any WSN oriented applications. A good WSN oriented application offers potential characteristics such as reliability, availability and maintainability. All these three vital fundamental requirements purely depend on fault-tolerance inorder to maintain the system well-being. So, we present maximum exploration of current state-of-the-art for WSN faults. Though there are various applicable fault management [16][17][18][19], a special investigation are to be explored to open up a wide view on these fault oriented research segments. Most of the previous research works are concentrated on fault prevention, fault detection, and fault recovery which are considered to be life cycle process of fault-management in WSN. Many detection techniques are only focused on specified fault nature. None of the previous fault management analysis or suggestion has given entire behavioral nature of faults at different layers of WSN protocol stack, as well as at the nodes' component level. For emerging researcher in WSN especially regarding faults, it's important to know behavioral nature of faults and possible occurrences of faults at different layers of the protocol stack and at nodes' components too.

Further this article exposes casual nature of evolving faults and their associated errors/failures by both layer-wise and nodes' component-wise, which were described in section IV. Followed by section V, we provide life-cycle of WSN fault-tolerance system by analyzing various parametrical based approaches of three phases of FT management (fault prevention, fault diagnosis, and fault recovery). The most

Karthick Raghunath K.M., Department of Computer Scinece, Adhiyamaan College of Engineering, Affiliated to Anna University, Hosur, India.
Rengarajan N, Principal, K.S.R College of Engineering, Affiliated to Anna University, Tiruchengode, India.

required existing fault tolerant methodologies and solutions suggested by researchers are quite specifically presented in section VI. Section VII concludes this paper by brief discussion, which may build future focus for fault tolerant research in WSN.

We first focus on general taxonomy of faults and failures in WSN. **Fault** is an unintended defect that ultimately channelizes to the cause of an error. **Error** is an indication of false (incorrect) state of the system. Imperfection quality of the system state caused by error, ultimately leads to the failure. A **failure** is the condition where the system becomes ineffective to perform the intended regulated functionalities, due to error.

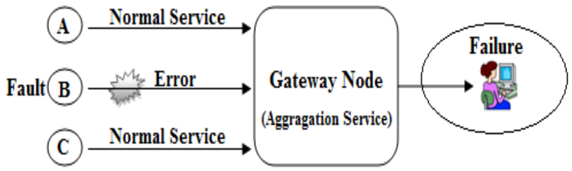

Figure 1: Relationships between Fault, Error and Failure

Figure 1 depicts the basic difference between fault, error, and failure. The principle operation of sensor node A, B and C are reporting periodical sensed data to the gateway node which aggregates different generic sensor data's for future analysis. Each sensor service is normal until node B suffers a fault. Thus, the immediate occurrence of fault (any) causes an error in performing normal service by node B. Due to the occurrence of fault on node B, it provide an errored service to the gateway node. These errored services contain inappropriate information to the analysis of entire application/system. The faulty service provided by node B ultimately causes system failure.

2. Taxonomy of WSN faults

To many budding researchers, a common typical question might springs up - "What will be the most vigorous causes and deep impact factors of faults on WSN?" We have so many different possible answers for this question. From [5], it's conceptually and widely expressed that under any circumstance, entire functionality of WSN should not be disturbed as a whole inorder maintain and ensure high reliability. Thus perpetually "fault" is a direct antagonistic to this word "reliability".

First step to build a WSN fault tolerant system which are closely, relates to dictate various faults, needed to inspect the variety and nature of faults. Fault associated with WSN are categorized into three major sections. They are Sensor reading faults, Software faults and Hardware faults. Each of these three sections has been elaborately depicted in figure 2.

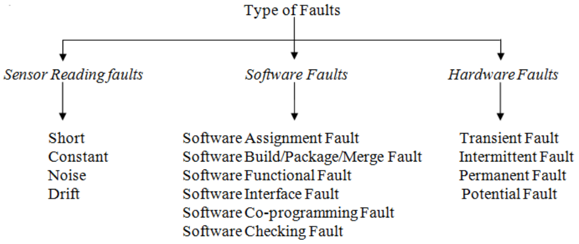

Figure 2: Faults variegation and classification

2.1. Classes of Sensor reading faults

To examine the common effects of sensor reading faults in WSN, firmly it's better to understand their classifications on different case-by-case basis. They are classified as short, constant, noise and drift. Short-lived oscillation on the input signal indicates the presence of *short* type sensor reading faults. This type of fault reflects very small impact till the presence of spike. *Constant* sensor reading faults are perceived as a flat signal, which produce an invariant repetition of random/arbitrary values whereas *noise* likes to be appeared as unstable vacillating signals. The impact of constant and noise turned-out to be the effect of losing sensor input values and degrading signal-to-noise ratio respectively. In case of *drift*, error persist when the observed value are found to be deviated from a standard or pre-defined specification (from the ground truth).Consequential activities of drift type of faults distorts the sensor reading. Perhaps, considering sensor reading validity service for signal processing techniques may reduce the effect of sensor reading faults.

2.2. Associated Software faults of WSN

Indeed to fulfill the desired complete service of WSN, contribution of software's makes a worthy concern. Hence unconventional nature of any software functionality service may not attain saturated status in terms of completing the desired task. So it is highly necessitate to analysis software faults that are associated with WSN. From [6], very few distinctive and appropriate software faults, associated with WSN are chartered and classified. They are Software Assignment Fault, Software Build/Package/Merge Fault, Software Functional

Fault, Software Interface Fault, Software Co-programming Fault and Software Checking Fault.

- ***Assignment Faults:*** Source code posses such a type of fault only on occasion of faulty initialization.
- ***Build/Package/MergeFaults:*** Accumulation of error due to mistakes in library system, direction of changes and version control.
- ***Functional Fault:*** Error in formal design causes wrong functionality and requires formal design change.
- ***Interface Fault:*** Occurrence of communication error between sensor node and sink node.
- ***Co-Programming Faults:*** This type of fault is an outcome of concurrency error/race condition/deadlock which happens during concurrent operation.
- ***Checking Faults:*** Existences of faulty or missing validation of data/values in the source code; leads to checking faults. Some other causes are software math bugs.

2.3. Categories of Hardware faults of WSN

On several aspects hardware faults can be classified, but regarding on their duration, following three faults are concerned to be open research issues on WSN. They are transient, intermittent, permanent [7] and potential faults [19].

Transient faults: Transient faults are induced by environmental conditions such as humidity, vibrations, cosmic rays, etc. The impressions of this type of fault are usually very less intense since occurs once and then disappears. For example, a signal from source end system may not reach its destination system but probably reach when transmitted again. Thus it was also known as *soft* faults.

*Intermittent faults**:*** This type of faults follows the looping mannerism that the fault occurring then vanishing, then reappears, and so on. Intermittent fault are caused by non environmental conditions such as loose connection, senescent components, etc. Dealing with intermittent fault causes great exasperation as they are hard to diagnose. For example, unstable repeated false state of any system is corresponding representation of this type of fault occurrence.

Permanent faults: The effect of permanent fault is stable and continues to exist until the faulty component is fixed or substituted. Examples of permanent fault are chip with manufacturing defects, burned-out light bulb, etc.

*Potential Faults**:*** Diminution of node hardware resource usually results in potential fault [19] for example: battery energy. Depletion of battery energy halts the entire functionality of WSN application.

3. WSN Failure Classification

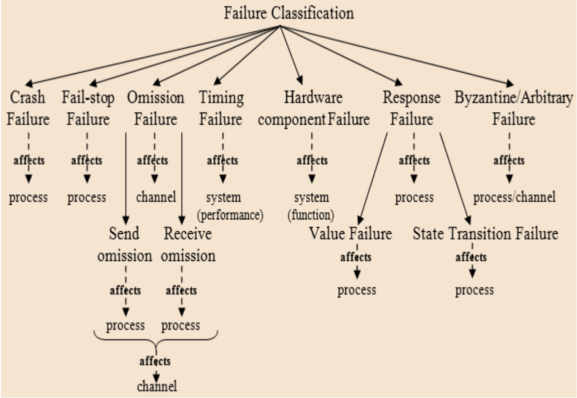

Figure 3: Failure Classification

Figure 3 depicts the exploration of different types of failures to get a better grasp in the world of failure era. Specific uninterrupted activity effects of fault leads to crash-stop failures. *Crash-stop* affects the process or functional unit and makes it to remain at halting state, at which no further defective output are produced. Fail-stop failures are also referred as fail-silent failures. Fail-stop failure is similar to that of crash-failure but can be easily detected by other processes while the former cannot be. The major causes of omission failure are network transmission error or insufficiency of buffer space. Due to *omission failure*, system fails to respond to the incoming queries. Both *receive* and *send* omission confirms the failing stage, to respond to processed incoming messages as well as to processed outgoing massages respectively. The combined effect of receive and send omission are notified as channel omission. Most of the *hardware failures* are associated with generic hardware components of sensor nodes. Liable reflection of environmental disasters causes hardware failures. Another important class of failure is timing failure, related to periodic operational scheme of WSN system. *Timing failure* is one which directs the synchronous distributed WSN system or real-time WSN system to respond outside the specified time interval. Since there is no standard assurance are provided for response time in asynchronous WSN system, timing failures said to have null effects on those. Next class of failure is *response failure*, is majorly due to the outcome of incorrect response by the system. There is possibilities of two kinds of response failure may happen, namely value failure and state transition failure. *Value failure* causes the system to provide faulty reply to the requested queries. For example some group of sensor nodes respond with wrong sensory data to the sink node.

State transition failure directs the system to deal with collapsed set of control flow, which ultimately triggers unintended default action at wrong time and produce irrelevant set of information as response. In any system dealing with byzantine failure are simply "messy" because *byzantine/arbitrary failure* makes the system to produce random values at arbitrary time. During processing, this type of failures tend to omit intended processing assessments but prefers unintended processing measures lead to message corruption and responding with multiple delivery in communication medium.

4. Wide Perspective on WSN faulty world

The required functionality services of wireless sensor network applications are affected by faults that may occur in different layers of the system. WSNs are commonly prone to failure in harsh environment, due to occurrence of faults at various levels. Inorder to deal with different levels of faults that occur in real application scenarios, we performed a systematical research and observed several trial reports at different layers of sensor network protocol stack. These observed trail reports can be used as steering for future research trials to prevent the occurrence of same type of errors and also to provide refinement methods at critical faulty situations. The sources of faults are discussed at following categories.

4.1 Components of Sensor node

Based on the generic architecture of sensor node, components are subdivided into six units. They are power unit, sensing unit, processing unit, transmission unit, storage unit and application dependent additional component. In this section, we discuss regarding possible failures/faults dealt with all of the early mentioned six units.

The sensor unit is composed of sensors and analog to digital converter (ADC). Sensor is a kind of transducer that involves transformation of signals/physical variables into required forms. Thus categorizations of sensors are also based on stimulus/physical variable (such as mechanical, electrical, thermal, radiation, magnetic, chemical) for which they are needed to measure. The required informative signals obtained through the analog sensors are converted into digital signal by ADC. During this process of conversion, some prominent quantization procedure takes place which necessarily directed to quantization errors [8] by quantization faults. So this quantization fault may be the destructive-starter of any WSN application. Other possible faults that may occur in ADC are circuit noise, aperture uncertainty and comparator ambiguity, all of these ultimately leads to unavoidable signal reconstruction errors [8]. Circuit noises such as device noise, conducted noise, radiated noise are the violations that have been raised via ADC input devices. The originator of device noise, conducted noise, and radiated noise are from ineffective amplifiers/resistors, power-supply devices and external electromagnetic interference signals respectively. Aperture uncertainties are caused by fluctuation in time difference between sampling events. Inorder to incorporate/enhance fault-free WSN applications, some of special procedures or methodologies are considered for research to tackle sensing unit fault issues.

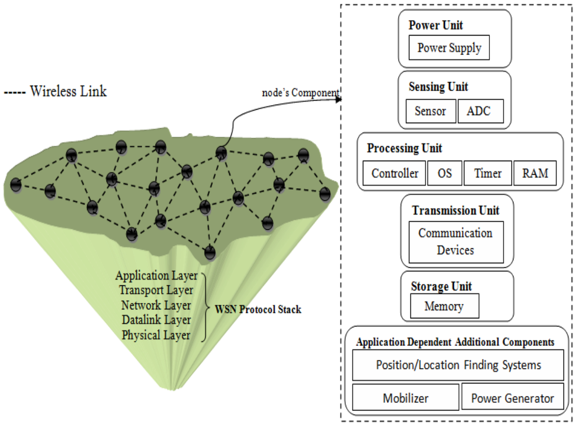

Figure 4: Sensor Node Components

One of the powerful and vital among sensor node components is central processing unit. To process the gathered data obtained from sensing unit and to communicate with other nodes in the network, each sensor node must pose processing unit which is responsible for prominent operations such as processing of data, controlling of other components in the node, execution of communication protocols, performing the required task. Apart from those operations, processing unit determines the [9] computation capabilities and energy consumption of node. Although plenty of controllers (microcontrollers, microprocessors, digital signal processors, Field-programmable array gate and Application-specific integrated circuit) are available, they are chosen according to the deployment and motivation of the application. Processing unit also comprises of RAM, timer, Operating System (OS) [9]. Modern controllers of WSNs are prone to hardware transient faults as well as permanent faults. Major reasons behind such hardware transient faults are minimizing noise levels and chip voltage, maximizing the usage of number of transistors and processors. Simultaneously the causes behind permanent faults are majorly based on deployed network area changes and direct or indirect impact of environmental disasters. Enormous power consumption of FPGAs makes it ill-suited for WSN, since FPGAs based WSN declines efficient management of power unit [9]. Self-involvement of operating system on each sensor nodes fulfils the completeness of WSN by wrapping low-level abstract information of sensor nodes and provide efficient interface to external gadgets [20]. OS offers appropriate API (Application Programming Interface) to underlying hardware and enforce proper process management. Some basic quality jobs performed by OS are device management, scheduling policies, multi-threading, multitasking, maintain strict concurrency mechanisms and also support for dynamic loading/unloading of modules [20]. Crash of OS leads to various failures, few among them are synchronization failures among sensor nodes, memory manipulation failure, freeze of triggering activities for prioritized task inducing task management failures, makes the entire senor node isolated from the network and so on. The impact of crashed OS produces infinite abnormal negative result.

To improvise data processing department with special feature, such as deletion of unwanted records, indexing, querying, updating data aggregation records and updating information of neighbourhood nodes in the network, integration of storage unit to sensor node are vital procedure, and it needfully concerned during design development of WSN. Storage unit are generally associated with controller unit. Though along with RAM (internal memory), flash memory also contribute some memory space, especially for storing programming codes. Selection of memory size is purely application dependant. Process of handling queries by storage unit may also contain several sub-processing events, like parsing the queries, data indexing and optimized execution plan. Each of these sub-processing events has so many challenges to deal with. Unavailability of stored sensor data happens often by random byzantine failures and data pollution attacks [15]. During data pollution attack, the adversaries take advantage by injecting polluted data, making it unrecoverable by the users.

Communication unit for WSN can be focussed and overviewed on three different ways: using RF (Radio Frequency), Infrared and Optical media. RF based communication suits to most of the WSN applications. Though RF based communication provides high data rate and efficient range of communication, consumption of energy at various operating modes (idle, sleep, transmit, receive) are concern to be serious problem. Moreover, the fragile nature of antenna from node and its size are also concerned as vital challenging factors. Such antenna's permanent faults tend the user for new replacement. Common restrictive parameters such as distance and power consumption are other notable factors of any RF technologies. Effects of multipath fading [12] may deteriorate radio system if proper efforts were not taken. Various RF based technologies [11] are listed in table 1 along with unfavoured possible factors that have tendency to emerge as critical fault/error/failure in WSN.

Table I: Radio-Frequency Technologies for WSNs

RF technologies	Standards	Unfavoured facts
Bluetooth Technology	IEEE 802.15.1	▪ During active mode drains more battery energy. ▪ Lacks security ▪ Short range
Wi-Fi Technology	IEEE 802.11. a/b/h/g	▪ Security risk ▪ Interference ▪ Short range
Ultra Wide Band (UWB) Technology	IEEE 802.15.3	▪ Standardization Incomplete. ▪ No proper frequency sharing (with existing user). ▪ High energy needed
WAVENIS Technology	EN 300-220 and FCC 15.247 (Coronis system)	▪ Possible risk of data collision.
Wibree	IEEE	▪ Not suitable for

Technology (Nokia)	802.15.4	high bandwidth required applications. ▪ Short range
Zigbee Technology	IEEE 802.15.4	▪ Security risk

Infrared technology provides short range of communication through omni-directional manner. Both radio and infrared communication system faces inband interference [12] by undesired transmission from various communications. This interference weakens/corrupts the signal, if its amplitude is larger than desired signal. Wireless optical communication (WOC) is a combination of optical fiber and radio frequency communication, which carries information via light beam at extremely high data rate. WOC system consists of three prominent blocks namely transmitter, propagation channel and receiver. Since WOC always expect line of sight communication setup, atmospheric effect such as [13] fog, rain, aberrations of the optical elements, atmospheric attenuation, and atmospheric turbulence affects the optical communication based WSN system. Potential processing of atmospheric effects are absorption, dispersion and refractive index variations [13]. As a result, WOC faces pointing errors [14] which diverts the propagation of optical signal.

Power unit handles the task of powering entire node. These unit manage to take additional responsibilities, since it provide energy for the execution of all activities within the node and support for reliable continuous function of the network. Either by using batteries or ambient energy harvesting, any wireless sensor node can be energized. Batteries are of two types namely rechargeable (primary) or non-rechargeable (secondary), depending on the application they were integrated along with sensor nodes. Most of the WSN applications are battery powered while some applications are power by ambient energy harvesting system (such as solar, vibration, etc.). Continuous uninterrupted supply of power to the node ensures high reliability and prevent from planned failures. Major cause of planned failures is degradation/depletion of power unit resources. Overcharging or over discharging capabilities of batteries may lead to the battery faults. Battery faults also directs to the degradation of solar charging. On the otherside, while investigating electrochemical world of batteries, it is noted that they depends largely on availability of active response sites throughout the cathode [10]. During intervals, due to low discharge currents, inactive reaction sites get uniformly disseminated throughout the volume of the cathode. Impact of such action covers the outer surface of the cathode with inactive sites. Such rate capacity [10] (measure of available capacity of battery) effects contribute to the reduction of battery capacity at higher rates of discharge. Improper battery delivery capacity also fails the working condition of active node. The variations in battery terminal voltage result in increased battery terminal voltage degradation errors. Many quantitative analyses are suggested by investigating on the cause of battery faults, errors and failures to enhance the efficiency of battery usage.

4.2. Overview of faults, errors, failures at different layer of WSN protocol stack

Any faults/errors/failures have the possibility to propagate to the next sequence level. Hence, it has become ultimate moral to focus on different layers of WSN protocol stack with respect faulty issues for forthcoming research issues.

Physical Layer: In WSN, physical layer is responsible for active communication among the sensor nodes via given medium and it also address the necessity of robust modulation, type of transmission (simplex, half duplex, full duplex), frequency selection, regulation of transmission and receiving techniques. Physical layer influence the mode that streams of bits are translated into signals for transmission. The most formidable gainsays of physical layers are fixed bandwidth, limited transmission range and poor packet delivery due to interference, attenuation, etc. According to [1], transmitter faults, receiver faults, the upper layer faults and noise are primarily considered as the sorted out fault occurrence at physical layer. The performance of both transmitter and receiver are commonly quantified by error vector magnitude. Here, performance degradation/ encounter of malfunctions at transmitter or receiver lead to transmitter or receiver faults respectively. Sensors in WSN are densely deployed, hence signal interferences is inevitable among the sensors. Unwanted variations in signal such as noise could also lead to a fault. The major causes of this noise are cross-talk, impulse noise, thermal noise. Such faults degrade the signal to noise ratio. Thus interference, multicasting and synchronization are most notable categories of physical layer design management. Interface error between host and network interface unit are referred to as upper layer faults. Common interface error that occurs in the network is intermittent. To obtain reliable WSN-physical layer, efficient error control strategies to be implemented according to the parametric schema of specified wireless medium. Inorder to ensure a FT in WSN system, several aspect of physical layer designing has to be considered, since it has potential to block the failure of node that may happen due to planned failures such as energy depletion. Optimizing the energy consumption in WSN requires low power operations which begin at physical layer. Thus most of the research works are concentrated on optimizing transmission energy and circuitry energy.

Data-Link Layer**:** Next to physical layer, its data-link layer which equally contributes its role for the successful function availability of any WSN. Data-link layer consist two sublayer namely logical link control sublayer which identifies the operational protocol of higher-level layer inorder to frame the received information and Medium Access control (MAC) sublayer addresses the frame and provide channel access control. While receiving and transmitting information from lower-level to higher-level layers two vital processing are performed by data-link layer. Raw bit streams received from physical layer are structured into frames similarly packets from network layer are also encapsulated into frames. When these frames involves in communication, consumes more energy. In wireless communication, data-link layer is prone to face high error rate. Moreover there is possibility for fault propagation from physical layer to data-link layer. In contrast to physical layer, several problems dealt by data-link layer are [2] single bit error, multiple bit error, collision, idle listening, overhead of control packets. Single bit error is an individual bit error in an entire data unit, example in a specified byte, change of bit 1 to bit 0 or bit 0 to bit 1. Multiple bit error or burst error is the change of two or more bits in an entire data unit. Persistence of both single and multiple bit errors causes loss of data during transmission. The most common event in WSN is concurrent transmission of data which leads to collision. Large amount of sensor node's energy are wasted for the purpose of false retransmission as well as for sensing channels. Here, both the collision and idle-listening heads to the battery depletion of sensor node. Thus, designation of MAC protocol in Data-link layer is always concerned to be energy saving systematical mandatory approach for entire WSN.

Network Layer: As WSNs deals with forwarding data packets, establishing efficient communication, maintaining coordination among the nodes; network layer performs logical network addressing and service addressing to enable end-systems to be connected to different networks. In case of network layer, routing and link between the nodes are considered to be building block and backbone of the network respectively. Most crucial faults that happen in network layer are link faults (radio interference, data rate distortion between the nodes) and faults that encountered on the established communication path (software bugs) [3]. Software bugs may divert appropriate message to incorrect destination on a well established communication path. Based on number of broken links, link failures are categorized into single link failure and multiple link failure. With respect to recovery time, link failure can be classified into permanent link failure and transient link failure. For a given short period of time if the link failure flunks to recover, then it refers to permanent else it falls under transient type of failures. In WSN , transient link failure are more frequent then permanent failures especially in presence of high dynamic of low-power wireless link. Effect of link faults channelizes to route oscillation, emergent link utilization of links on surrogate paths, inconsistent data flow over intercede router buffers. For a stable constant high reliability, these failure effects are observable manifestation of network layer in wireless sensor technology.

Transport Layer: To maintain the end-end reliability and congestion free connectivity throughout WSN, transport layer's complete standard functions are unavoidable. Most of the unknown/unsolved failures propagated from lower-level layer to higher-level layer impose overloaded work on transport layer. Regarding directions, transport layer organize and manage data flow in two ways namely upstream and downstream [4]. Upstream are flows of data from sensor node to base station, which can also be mentioned as many-to-one, sensor to sink, converge-cast. Unlike upstream, downstream involves flow of data from base station to sensor node, and can be referred as one-to-many, sink to sensor, multicasting. The most concerned issuing factor of transport layer on reliable communication is congestion, which is caused by numerous sources dissipating/transmitting more data too fast for network to handle. Congestion can be categorized into link-level congestion (happens when link carries too much data) and retransmission congestion (happens when repeated transmissions are handled to compensate for packet loss). Faults related with both upstream and downstream are purely link-level congestion oriented while retransmission congestions are associated with node level faults. Congestion faults deteriorates QoS which may cause total failure for entire network and can impact WSN by degrading the network performance, loss of packets, consuming node's energy by several retransmissions, increasing end-to-end packet delay. So to realize fault free communication in WSN, transport layer should concern [4] upstream reliability, downstream reliability, packet reliability, hop-by-hop reliability, event reliability and end-to-end reliability.

Application/Monitoring Layer: Depending on the required sensing task various applications can be carried and utilized on WSN application layer. From [5] points of view, the fundamental procedural functions of application layer are sensor management, task assignment, data advertisement and sensor querying. The layer is also responsible for providing required software that makes the hardware and software's of the lower layers transparent to the sensor network management applications. Imperfection designing and coding of application software leads to software fault. Moreover application layer is the only perfect interfacing point to any user; may face malicious threatening activities from external intruder which may crash core function process of the software. So the faults that are caused by external activities are referred as external application software faults and those found internally are internal application software faults. The main design goal of application layer is to provide high quality consistent service by ensuring fault-free information flow to lower layers.

5. Generic Life Cycle of Fault Tolerances Management

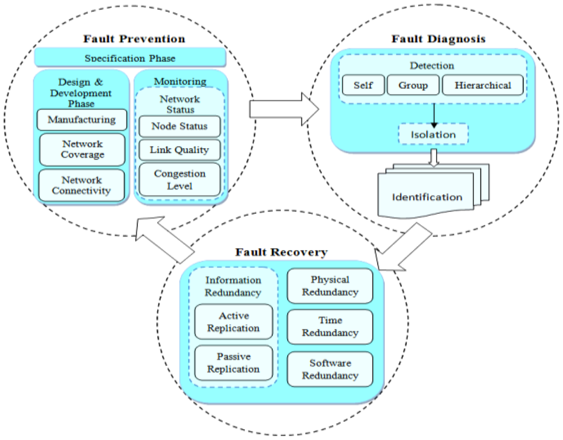

Figure 5: Generic Fault Tolerance Management Life cycle

Increasing fault tolerance potentiality of WSN depends on continuous well organized multi-operational procedures of three phases (prevention, diagnosis and recovery), that are involved in FT management. On following analysis with three phases, a generic lifecycle has been furnished, which is depicted in figure 5.

5.1. Fault Prevention

Fault prevention is an act of pre-propounding to an abnormal fault implying activities that usually takes place in WSN applications. So, prevention role can be incorporated along with main concerned phases of WSN application design, they are i) Specification phase ii) design and development phase and iii) monitoring phase. During specification phase, it avoids incomplete specifications and equivocal specifications. By adopting suitable standard of quality for hardware components and certain definition of flow along with controlled structures at network coverage and connectivity level, ensures the involvement of prevention act in design and development phase. Generation of fault may happen by incorrect usage/handling of resources/events or functional degradation due to several factors. Therefore viable monitoring phase are always concerned to watchout on node status, link quality and congestion level.

5.2. Fault Diagnosis

Since WSN experiences perpetual changes, stringent fault prevention enrolment may not ensure 100% prevention of fault invasion. A primary fault diagnosis system is always needed to detect and isolate the generated faults. Such a procedures can be handled in any of the following three ways i) self, ii) group and iii) hierarchical diagnosis at centralized-oriented or distributed-oriented networks. After the fault detection and isolation procedures, each isolated faults are to be identified, to study the characteristics and behavioral nature of that fault.

5.3. Fault Recovery

Following thorough investigation of detected faults, it has to be normalized to minimize/eliminate the effects. Fault recovery phase is the primary in-charge to evacuate the effects of faults through all the phases. This can be done using appropriate redundancy techniques. Some of the common redundancies applied at several levels are information, physical, time and software redundancies. Information redundancy provides FT by active/passive replication of required information.

In case of active replication, all request are processed by multiple instance (all replicas) while in the case of passive, single instance process the request, only when it fails to do so, other instance takes the charge of processing the request. Physical redundancy ensures FT by providing additional equips, hence also be called as hardware redundancy. Similarly software redundancy seeks to provide required redundant software code. Time redundancy attains FT capability by performing certain needed operations at several times.

6. Evaluation

As discussed in section IV and V, this survey deals with the behavioral nature of faults and its various impact in WSNs is quite coherent. Better understanding of various FT techniques and their shortcoming or build-in efficiencies helps to develop fault-free WSN system. Therefore overviews of different existing FT technique are necessary for future research advancement. This section further extended via Appendix I, which present the short overview on different aspects of FT techniques.

7. Summary and Conclusion

In this article, taking advantages of generic workflow nature of various WSN applications, some of the vital facts relevant to faults and its associated impacts on WSN are broadly discussed as an eagle-view. We identified that proper function of WSN protocol stack and sensor nodes' components ensure the high '*success rate'* of any WSN applications, since each and every layers as well as components contribute their part of work to WSN. As soon as possible, on the commencements of applications, several applicable restrictions and limitations of WSN tend to return the network to failure conditions. Based on the diverse needs, design of any generic fault management approaches have to consider every operation that take place in any WSN applications.

References

[1] Jae Min Lee, Wook Hyun Kwon, Young Shin Kim, Hong-Ju Moon. Physical Layer Redundancy Method for Fault Tolerant Networks, proceedings of International Workshop on Factory Communication Systems, DOI: 10.1109/WFCS.2000.882546, pages 157–163, 2002.

[2] Sidra Aslam, Farrah Farooq, Shahzad Sarwar. Power Consumption in Wireless Sensor Networks, Proceedings of the 7th International Conference on Frontiers of Information Technology, ISBN: 978-1-60558-642-7, DOI: 10.1145/1838002.1838017, 2009.

[3] Ulka Ranadive, Deep Medhi. Some Observations on the Effect of Route Fluctuation and Network Link Failure on TCP, Proceedings of IEEE International Conference on Computer Communication and Networks. DOI: 10.1109/ICCCN.2001.956305, pages 460–467, 2001.

[4] Md.Abdur Rahman, Abdulmotaleb El Saddik, Wail Gueaieb. Sensors Lecture Notes Electrical Engineering © Springer-Verlag Berlin Heidelberg, volume 21, pages 221–245, 2008.

[5] Akyildiz, I.F., Su, W., Sankarasubramaniam. Y., Cayirci, E. Wireless Sensor Networks: A Survey. Computer Networks, International Journal of Computer and Telecommunications Networking, volume 38, pages 393–422, 2002.

[6] Jan Ploski, Matthias Rohr, Peter Schwenkenberg, Wilhelm Hasselbring. Research Issues in Software Fault Categorization, ACM SIGSOFT Software Engineering Notes, volume 32, pages 1–8, 2007.

[7] Israel Koren, Mani Krishna, C. Fault-Tolerant Systems, Morgan-Kaufman Publishers, San Francisco, CA, 2007.

[8] Sinem Coleri Ergen, Pravin Varaiya. (2006). Effects of A-D Conversion Non-Idealities on Distributed Sampling in Dense Sensor Networks, proceedings of international conference on information processing in sensor networks, DOI: 10.1145/1127777.1127811, pages 202–209, 2006.

[9] Ajay Jangra, Swati, Richa, Priyanka. Wireless Sensor Network (WSN): Architectural Design issues and Challenges, International Journal on Computer Science and Engineering, volume 2, pages 3089–3094, 2010.

[10] Chulsung Park, Lahiri, K., Raghunathan,A. Battery Discharge Characteristics of Wireless Sensor Nodes: An Experimental Analysis, Sensor and Ad Hoc Communications and Networks, Digital Object Identifier: 10.11.1109/SAHCN.2005.1557096, pages 430–440, 2005.

[11] Ana-Belan Gracia-Hernado, Jose-Fernan Martinez-Ortega, Juan-Manuel Lopez-Navarro, Aggeliki Prayati, Luis Redondo-Lopez. Problem Solving for Wireless Sensor Networks, Digital Object Identifier: 10.1007/978-1-84800-203-6_2 © springer-verlag london limited. pages 1–13, 2008.

[12] Barry, J.R. Wireless Infrared Communications (Third Edition). Boston: Kluwer Academic Publishers, 1994.

[13] Mutamed Khatib. Trends of the Optical Wireless Communications (Second Edition), InTech publishers, 2011.

[14] Debbie Kedar, Shlomi Arnon. Optical Wireless Communication through Fog in the Presence of Pointing Errors, Applied Optics, volume 42, pages 4946–4954, 2004.

[15] Qian Wang, Kui Ren, Wenjing Lou, Yanchao Zhang. Dependable and Secure Sensor Data Storage with Dynamic Integrity Assurance, INFOCOM 2009, Digital Object Identifier: 10.1109/INFCOM.2009.5062006, pages 954–962. 2009.

[16] Iman Saleh, Mohamed Eltoweissy, Adnan Agbaria, Hesham El-Sayed. A Fault Tolerance Management Framework for Wireless Sensor Networks, Journal of Communications, volume 2, pages 38–48, 2007.

[17] Muhammad Zahid Khan, Madjid Merabti, Bob Askwith, Faycal Bouhafs. A Fault Tolerant Network Management Architecture for Wireless Sensor Networks, 11th Annual postgraduate Symposium on the Convergence of Telecommunication, Networking and Broadcasting, ISBN: 978-1-902560-24-3 © 2010 PGNet, 2010.

[18] Muhammad Zahid Khan, Muhammad Asim, Ijaz Muhammad Khan. Centralized schemes of Fault Management in Wireless Sensor Networks, Georgian Electronic Scientific Journals (GESJ), volume 36, Issue 4, pages 66-74, 2012.

[19] Muhammad Asim, Hala Mokhtar, Madjid Merabti. A self-managing fault management mechanism for wireless sensor networks, International Journal of Wireless & Mobile Networks (IJWMN), volume 2, pages 184–197, 2010.

[20] Anil Kumar Sharma, Surendra Kumar Patel, Gupteshwar Gupta. Design issues and classification of WSNs Operating Systems, International Journal of Smart Sensors and Ad Hoc Networks (IJSSAN), volume 2, pages 71–75, 2012.

[21] Jin Mu-jing, QU Zhao-wei. Efficient neighbor collaboration fault detection in WSN, Journal of China Universities of Posts and Telecommunications, volume 18, pages 118-121, 2011.

[22] Arunanshu Mahapatroa, Pabitra Mohan Khilar. Transient Fault Tolerant Wireless Sensor Networks, Procedia Technology, volume 4, pages 97-101, 2012.

[23] Bijun Li, Ki-Il Kim. An (m, k)-FirmReal-Time Aware Fault-Tolerant Mechanism in Wireless Sensor Networks, International Journal of Distributed Sensor Networks (IJDSN), volume 2012, pages 1-12, 2012.

[24] Meikang Qiu, Zhong Ming, Jiayin Li, Jianning Liu, Gang Quan, Yongxin Zhu. Informer homed routing fault tolerance mechanism for wireless sensor networks, Journal of Systems Architecture (JSA), volume 59, pages 260-270, 2013.

[25] Peng Jiang. A New Method for Node Fault Detection in Wireless Sensor Networks, Sensors journal, volume 9, issue 2, pages 1282-1294, 2009.

[26] Edward Chan, Song Han. Energy Efficient Residual Energy Monitoring in Wireless Sensor Networks, International Journal of Distributed Sensor Networks (IJDSN), volume 5, issue 6, pages 748-770, 2009.

[27] Benahmed Khelifa, Haffaf, H., Merabti Madjid, David Llewellyn-Jones, Monitoring Connectivity in Wireless Sensor Network. International Journal of Future Generation Communication and Networking (IJFGCN), volume 2, pages 1-10, 2009.

[28] Ayasha Siddiqua, Shikha Swaroop, Prashant Krishan, Sandip Mandal. Distance Based Fault detection in wireless sensor network, International Journal on Computer Science and Engineering (IJCSE), volume 5, pages 368-375, 2013.

[29] Kuo-Feng Ssu, Chih-Hsun Chou, Hewijin Christine Jiau, Wei-Te Hu. Detection and diagnosis of data inconsistency failures in wireless sensor networks, International Journal of Computer and Telecommunications Networking, volume 50, issues 9, pages 1247-1260, 2006.

[30] Abolfazl Akbari, Arash Dana, Ahmad Khademzadeh, Neda Beikmahdavi. Fault Detection and Recovery in Wireless Sensor Network Using Clustering, International Journal of Wireless & Mobile Networks (IJWMN), volume 3, pages 130-138, 2011.

[31] Song Jia, Wang Bailing, Peng Xiyuan, Li Jianfeng, Zhong Cheng. A Recovery Algorithm based on Minimum Distance Redundant Nodes in Fault Management in WSNs, International Journal of Control and Automation (IJCA), volume 6, pages 175-183, 2013.

[32] Chessa, S., Maestrini, P. Fault recovery mechanism in single-hop sensor networks, Computer Communications, volume 28, issue 17, pages 1877–1886, 2005.

[33] Ramesh, S., Gobinathan, S. Railway Faults Tolerance Techniques using Wireless Sensor Networks, International Journal on Electronics & Communication Technology (IJECT), volume 3, issue 1, pages 204-208, 2012.

[34] Joa-Hyoung Lee, In-Bum Jung. Speedy Routing Recovery Protocol for Large Failure Tolerance in Wireless Sensor Networks, Sensors journal, volume 10, issue 4, pages 3389-3410, 2010.

[35] Faisal B. Hussain, Yalcin Cebi, Ghalib A. Shah. A Multievent Congestion Control Protocol for Wireless Sensor Networks, EURASIP Journal on

Wireless Communications and Networking, volume 2008, pages 1-12, 2008.

Appendix I

Ref	*Focused on*			*Remarks*
	Prevention	**Detection**	**Recovery**	
[23]			✓	● Used an (*m*, *k*)-firm-based real-time fault-tolerant mechanism. ● Ensures acceptable worthy QoS performance. ● Maintains desired reliability and timeliness.
[33]	✓	✓		● Proposed system avoids collisions on the railway track. ● Also detects the railway track for cracks using IR rays.
[29]	✓	✓		● Focused on data inconsistency failures. ● By constructing node-disjoint paths and utilizing automated diagnosis schemes, errors that evolved due to data inconsistencies are detected (99.9%) by sink node.
[24]	✓	✓	✓	● Proposed Informer Homed Routing (IHR) Mechanism. ● Checks the aliveness of nodes inorder to prevent network failures. ● Certain constraints are fixed and detected to prevent failure. ● Recovery measures have been framed incase of failure of cluster heads. Routing protocol consumes very less energy.
[16]		✓		● The proposed model detects fail-stop failures.
[26]	✓			● Constructed a hierarchical approach for a continuous energy mapping to a sensor network. ● Two phases are involved: Topological discovery, clustering phase. The efficient usage of these two phases reduces the monitoring scheme impacts on the lifetime of the network.
[22]		✓		● A distributed detection algorithm is used. ● Concerned regarding transient, intermittent, and permanent faults.

[30]			✓	● Used cluster-based recovery algorithm. ● Recovers the connectivity of the cluster. ● Faster response time.
[27]	✓	✓		● Proposed a novel monitoring mechanism for a strong and reliable connectivity (links) in wireless sensors networks. ● The new mechanism also has the ability of anticipating disconnections, before they occur.
[25]		✓		● An improved Distributed Fault Detection (DFD) Technique is proposed to detect failed nodes. ● Addresses the major issues of existing DFD by introducing modification to detection criteria.
[35]	✓			● Multi-event congestion control protocol (MCCP) is proposed. ● Avoids packet collisions ● Increases the packet delivery ratio by using schedule-based scheme.
[34]			✓	● **A**daptive routing protocol for fast **R**ecovery from large-scale **F**ailure (ARF) has been proposed. ● ARF performs immediate recovery of the network from the failures over large area. ● Very less energy is consumed.
[32]			✓	● Introduced a redundancy scheme for single-hop sensor networks. ● By this schema the sensors maintain redundant information and dissipate the information during failures.
[31]			✓	● Proposed a recovery algorithm to recover “coverage holes”. ● Supports energy balancing and optimization.
[21]		✓		● Self-monitoring of Wireless Sensor Networks (SM-WSN) algorithm is used. ● Has lower energy consumption. ● Has higher fault detection accuracy.
[28]		✓		● Distance Based Fault Detection (DBFD) algorithm is proposed. ● Using spatial data’s and timing information DBFD method identifies the sensor faults.

K.M. Karthick Raghunath has received his B Tech. in Information Technology from Anna University in 2008 and M.E. in Pervasive Computing Technology from Anna University (BIT Campus) in 2011. Since January 2012, he has been pursuing his Ph.D. degree in the Anna University, Chennai. His research interests include Wireless Sensor Networks, Pervasive/Ubiquitous Computing, and Embedded Systems. He is lifetime member of IAENG and IACSIT.

Dr. N. Rengarajan has more than 30 years of Experience consisting 25 years of Teaching / Research / Administrative experience in engineering colleges and 5 years Industrial experience. Presently, he is working as principal in K.S.R College of Engineering, Tiruchengode. Received his Ph.D. in Electrical and Electronics Engineering at India in 2004 and his M.E. in Power System from National Institute of Technology, Tiruchirapalli in 1993. He received his B Tech in Electrical and Electronics Engineering from Anna University (MIT campus), Chennai in 1983 and his B.Sc in Physics from Madras University, Chennai in 1980. His areas of specialization are Power System Control, Power Electronics, ANN, Fuzzy and Control System. He published numerous Journals under his specialization.