
Kamaldeen Ayodele Raji1, *, Kazeem Alagbe Gbolagade2

1Department of Computer Science, Kwara State Polytechnic, Ilorin, Nigeria
2Department of Computer Science, Kwara State University, Malete, Nigeria

Email address:
Kamal2004@gmail.com (K. A. Raji), kazeem.gbolagade@kwasu.edu.ng (K. A. Gbolagade)
*Corresponding author

To cite this article:
doi: 10.11648/j.wcmc.20190701.13

Received: January 26, 2019; Accepted: March 30, 2019; Published: April 18, 2019

Abstract: Wireless Sensor Network (WSN) consists numerous sensor hubs which containing a preparing unit, at least one sensor, a radio for information correspondence and power unit generally outfitted with a low limit energy distributed over a geographic area for monitoring our environment and physical conditions. It has been established that vitality is the most obliging element on the functionality of such systems as they are controlled with constrained vitality and replacement of vitality resources might be difficult. While sending the data in sensor network, there might be loss of information or miscalculation could occur in receiving data during transferring. The correctness of information has incredible impact on the performance of the network. To enhance the exactness of sensor information, minimizing vitality utilization and adaptation to internal failure is vital for some WSN’s applications as they operate in unpredictable conditions and ought to stay operational regardless of whether a network failure happen. This paper surveys the available energy efficient, reliability and fault tolerant in WSNs. It focuses on Residue Number System (RNS) and Agent technologies for energy-efficient and fault tolerant in WSNs respectively. However, performance evaluation was also conducted based on the energy consumption, reliability, delay in receiving the sent data and efficiency.

Keywords: Wireless Sensor Networks, Fault Tolerant, Multi-agent, Redundant Residue Number System, Power Efficiency

1. Introduction

Wireless sensor networks (WSNs) comprise of a vast quantities of remote sensor hubs scattered in a region of enthusiasm with at least one base station, where information is gathered. They are mainly used in monitoring our environment and also for physical conditions. They are also small devices which enable the measurements of physical and environmental conditions [1]. WSNs are very useful in many areas such as patient monitoring in hospital, battle field surveillance and other areas where wireless nodes may operate in highly dynamic environments [2]. WSNs are also self-sorted out systems that comprise of considerable amount of distributed sensor devices that are disperse over a wide environment to monitor physical phenomena, including temperature, humidity, vibrations, etc [3]. WSNs consist of scattered network of enormous quantity of arbitrarily organised sensor hubs, which have inherent computational, storage and transmission proficiencies that operate in an unfriendly mode and gather information of enthusiasm from its surrounding [4].

The principle errand of remote sensor systems is to gather the detected information from condition and send them back to the sink hub to be handled. Figure 1 shows a Wireless Sensor Networks containing wireless nodes and the sink. A sensor hub is a little gadget that incorporates three parts: a processing unit used to process local data, a sensing unit used to obtain information from the physical environment, and a wireless transceiver that transfers the sensing information to the base station. These sensor nodes perform data sensing and
processing tasks and also communicate with each other. In WSNs, sensor node batteries cannot be replaced or recharged, hence, applications and services should be designed in an energy efficient manner [3]. Adaptation to non-critical failure is imperative for some WSNs applications as they work in unstable situations and ought to stay operational regardless of whether a few disappointments happen.

![Figure 1. A Typical Wireless Sensor Network.](image)

However, it was observed that the reliability and availability of WSNs can be affected by faults, including those from radio interference, battery exhaustion, hardware and software failures, communication link errors, malicious attacks, etc [3]. Since nodes are prone to error, failure detection and fault recovery techniques are essential requirements in WSNs. However, a base station that collects and identifies information from each of the sensor nodes to provide fault tolerance can be very expensive. To enhance the exactness of sensor information, the errors are recognized in light of the order of errors. Commotion expulsion in sensor information additionally enhances it unwavering quality [1]. The term agent is ending up exceptionally prominent in the registering press as it is inside the computerized reasoning and the software engineering networks. Agent software has continued to attract significant research attention due to their intelligence, mobility and collaborative nature. Agent-based systems play variety of roles in the development of various essential industrial applications [5]. However, there is high need of agents in processing as a result of quick advancement in computing and information organizing innovation to help those requirements, and blast in the assortment of hardware and systems. A multi-agent system (MAS) usually consists of many cooperative agents that can solve problem impossible for single agent [6]. MAS have a rule that can be effortlessly adjusted and coordinated in complex frameworks due to their completely decentralized and "intelligent" approach.

Residue Number System (RNS) is a non-weighted number system that gives convey free, parallel, rapid, secure and fault tolerant arithmetic tasks. In the past decades, residue number system has gotten extraordinary consideration. In this system, residues of the original number with respect to moduli set are represented instead of the original number itself. Along these lines the number will be part into some littler numbers which are autonomous and tasks can be refined on them independently and simultaneously which makes the calculations less complex and substantially speedier [7]. It offers extraordinary capacity for rapid computer arithmetic because of their inalienable properties which make them profoundly helpful in Digital Signal Processing (DSP) applications. RNS can bolster convey constrained and fast number-crunching and error discovery and in addition error remedy applications [8]. As a result of these one of a kind highlights, its utilization in assortment of fields is developing quickly. Residue number systems are extremely valuable in error recognition and rectification on the grounds that a blunder in one digit does not degenerate some other digits. This article presents a survey of the available agent-based fault tolerant and RNS energy efficiency in WSNs. It also conducts performance evaluation based on the power usage, reliability, delay in the sent data and efficiency for each approach.

### 1.1. Energy-Efficiency and Fault Tolerance in WSNs

Energy efficiency in WSNs is the set of rules to manage various vitality supply mechanisms and then efficient utilization of the provided power in a sensor node. Energy efficient involves using less power to achieve the same service. A WSN that provides a higher event detection accuracy for less amount of vitality is said to energy-efficient. It is of paramount importance for WSNs because once deployed it is difficult to recharge or replace it power source [3]. Therefore, WSN should be planned in a vitality efficient way in order to reduce the usage of available power. The life span of a sensor network can be unmitigated by applying different methodologies. Energy efficient schemes usually aimed at reducing the vitality consumption during network activities. However, a great quantity of energy is used by node components such as, CPU, radio, etc. even if they are inactive. Some power-management schemes are thus used for switching off hub parts that are not temporarily needed [8].

However, a system is considered fault tolerant if the conduct of the system, regardless of the disappointment of a portion of its parts, is reliable with its details. Fault tolerant systems have the capacity to work within the sight of errors. By utilizing adaptation to non-critical failure, numerous potential disappointments are turned away, in this manner expanding the dependability and proficiency of the system. The objective of adaptation to non-critical failure is to expand the system accessibility, which is to build the ideal opportunity for which the system is accessible for client administrations. Computers can be made more reliable by preventing errors as
well as detecting and correcting identified errors. Fault can be defined as a sort of deformity that prompts an error. An error compares to an inaccurate system state, and such a state may prompt a failure. A failure is the (noticeable) indication of an error, which happens when the system veers off from its determination and cannot convey its proposed usefulness [4].

In WSNs, fault event likelihood is high contrasted with traditional networking administration. Then again network upkeep and hubs substitution is incomprehensible because of remote deployment. Adaptation to non-critical failure in WSNs can be grouped into four levels from system perspective. These are: hardware layer, programming layer, networking layer and application layer [5]. Generally, the error area plot requires certain measure of overhead in term of additional bits which are added to the total transmitted data. These additional bits are used by the recipient to check for mistake on the progression of data that may occur in the midst of the transmission. Adaptation to non-critical failure is imperative for some WSNs applications as they work in antagonistic conditions and ought to stay operational regardless of whether a few disappointments happen. WSN failures are for example caused by dropped bundles because of remote impedance, over-burden, hub/connect failures, and separated systems [6]. To have the capacity to keep up effective tasks, WSNs must be intended to be flexible to these systems flow. The extraordinary case is with the end goal that requires a crisis reaction, for example, in fire, surge, fountain of liquid magma checking and military reconnaissance. It is, therefore, necessary to make automatic fault management techniques in wireless sensor networks. One of the objectives of the remote sensor systems is to empower dependable information accumulation to meet the objectives of the applications. Giving unwavering quality is a critical issue to address since dominant part of the sensor systems are remotely worked with next to no human intercession once sent; and the support/maintenance is additionally infeasible now and again. Also, the sensor network is naturally presented to a few wellsprings of inconsistency, for example, errors from equipment commotion, correspondence errors, errors in sensors, and so forth, requiring the requirement for unwavering quality components [7].

1.2. Faults Propagation in WSN’s Applications

Wireless sensor systems are ordinarily conveyed in hostile condition and are liable to flaws in a few layers of the network. Figure 2 demonstrates a layered order of the parts in a WSN which can cause issues [3]. A fault in each layer has the likelihood to spread over every one of the levels. Hubs have a few equipment and programming parts that can have deficiencies. The fenced in area can endure effects and uncover the equipment of the sensor hub to the outrageous states of the earth, for example, presentation to coordinate contact with water will cause short-circuits. Likewise, at the point when the battery of a sensor accomplishes a particular stage, sensor readings may wind up erroneous. For the most part, equipment failures will prompt programming malfunctioning. A Data Acquisition application will not perform appropriately if the hidden sensors are giving error readings. In any case, some equipment failures do not influence every one of the administrations in a sensor hub. In spite of the fact that the hub cannot be utilized to give adjust sensor readings, it can be utilized to course bundles in the sensor network. Be that as it may, Programming bugs are a typical wellspring of error in WSNs. Programming bug could cause the longest nonstop system blackout taking the system disconnected for quite a long time until the point when the hubs could be reinvented physically.

At the network layer, routing is a major factor of a WSN that is fundamental in the gathering of sensor information, conveyance of programming and design updates, and coordination among the hubs and this could likewise have shortcomings. Faults on the routing layer can prompt dropped or misinformed messages, or unsuitable postponements. Radio obstruction can likewise make the connection between hubs wind up broken. Another wellspring of connection failure is the collision of messages. Be that as it may, for a more elevated amount of the system, a sink gadget gathers the majority of the information produced in the system and transmits it to the back-end system. It is additionally in charge of deficiencies in its segments. When a failure occurs at the sink and fault-tolerant measures have not been implemented, the aftermath effect of the failure spreads to all nodes of network, resulting in sensor nodes that cannot be accessed. At long last, the software that stores the information gathered from the system, forms them and sends them to the back-end system, is also liable to bugs which when display, can prompt loss of information inside the period where the fault happened.

2. Literature Review

There have been a few investigations on error control
procedures in wireless systems and particularly in mobile systems, none of them are specifically appropriate to Wireless Sensor Networks (WSNs). Also several energy conservation schemes have been proposed aimed at reducing the power consumption of the radio interface. The two main approaches are: Duty Cycling and In-Network Aggregation [8-9]. The first approach comprises in putting the radio transceiver in the sleep mode at whatever point correspondences are not required. In any case, vitality sparing is gotten to the detriment of an expanded hub unpredictability and system dormancy. The second approach is proposed to consolidate routing and information accumulation strategies went for lessening the quantity of transmissions. Multipath routing calculations are generally utilized. In any case, multiple paths could remarkably consume more power than the shortest path because a few duplicates of a similar bundle could reach the destination. However, to increase reliability, Automatic Repeat reQuest (ARQ) which requires that the receiving node to detect lost data and then request the sending node to resend the packets was proposed [10]. Forward Error Correction (FEC) necessitates that the aggregator must disentangle the received data, total them with new information and encode them before sending them to sink [10]. They both reason a critical end-to-end deferral and high vitality utilization which diminish in the system lifetime. What's more, since no single approach gives broad adaptation to non-critical failure bolster covering a wide range of flaws that a WSN hub is exposed to. Therefore, it is necessary to develop an efficient, fast operation and reliable fault tolerant WSNs while still conserving the limited energy of the network.

3. Agent-Based Fault Tolerant in WSNs

An agent is a software framework that is arranged in some condition, and that has an ability of performing self-sufficiently in this condition to meet its plan destinations. Operators self-rulingly sense the earth and react appropriately [2]. In late time, MAS are utilized in different territories, for example, reproduction, artificial intelligence and robotic, picture handling and so forth and are incorporated into the WSNs, on account of their significance to the field. MAS applied to the WSN for the capturing information processing, and also directing, and the discovery of the most limited ways. In reality, late patterns toward this joining of multi-agentt approaches in WSN innovation are presented in numerous levels and working angles. Agent technology has been successfully used in WSNs at different levels such as application, middleware and network. In DMWSNs, a distributed monitoring system for WSNs implemented in multi-agent system was proposed with main purpose of software design and the organization of the network topology [11]. However, the aim was to have an error controllability network and increase its usage time. The system was implemented in Castalia simulator based on the simulator Omnet++. In addition, error detection and correction that was based on multi agent system was proposed in MFTS. Energy reduction was done with multi-agent and mobile agent configuration simulated with Java.

EDFBRP, presents an operator based routing calculation for remote sensor systems, in view of the determination of the possibility of dynamic hubs [12]. The steering calculation is connected with vitality and separation elements of every hub. The primary target was to expand the lifetime of a sensor network while not trading off information conveyance. JADE was utilized as operator structure. Also, MACB-WSN, proposed multi-agent which involves grouping of WSN using two models [13]. The first model was Data aggregation (Multi Agent Controlled Dynamic Routing Protocol -MACDRP) which was done by means of one Base Station in each round; and data direction is changeable. In the second model (Multi-agent and Base Stations Route Clustering -MABCDCP), Cluster Heads select and then sensing nodes send their messages to the Cluster Heads and then Cluster Head transmits the collected information to the nearest sink. The proposed models increase security in synchronization, better coverage and increased reliability.

Moreover, in IWSNM-MAS, intelligent multi agent that used mobile agent to gather data in a cluster was proposed. According to its design, each sensor node has processing capability with an agent each for local data processing [14]. The nodes were grouped together with a clustered head using Local Closest First (LCF) algorithm to determine a scheme for the nodes belonging to the same group. Network Simulations were done using C++ Builder. The result shows decrease in power usage and increase in packet delivery. A multi-agent framework that will enhance the mapping of parameters between heterogeneous systems, call affirmation control and handover administration with the goal of certification end-to-end delay and QoS was proposed [32]. The fundamental preferred standpoint of this system is an enhanced execution of the remote correspondence in light of the fact that the best system is chosen by the QoS parameters.

In conclusion, multi-agent technology was connected to wireless sensor network with space keeping in order to adjust programming engineering, and to streamline its execution in monitoring [33]. Agent based algorithm for adaptation to internal failure and topology control in a remote sensor organize was proposed. This comprises of inserting an agent at every hub that is in charge of choosing its parent or the following bounce to the sink while exchanging parcels. The fundamental commitment is the proposition of another procedure of evolving parent, which depends on the calculation of an adaptation to internal failure degree, figured each time by the agent in participation with its neighbouring hubs. The results of simulation demonstrate that this technique for changing parent permits an upgraded lifetime, and additionally arrange adaptation to non-critical failure, when contrasted and the accumulation tree convention.

4. RNS-Based Energy Efficiency in WSNs

A lot of research has been completed to investigate diverse regions in energy efficient and fault tolerant wireless sensor systems, those researches have brought new challenges in creating secure and reliable data storage and access facility in
WSNs. One of the main benefits of residue number system is that they facilitate the detection and correction of error because all the digits are independent [16]. However, there are several approaches that have been studied for fault tolerant wireless sensor network, some of which are discussed. Low Energy Adaptive Clustering Hierarchy (LEACH) is the first and most effective energy-efficient hierarchical clustering algorithm for WSNs that was proposed for reducing power consumption [18]. In LEACH protocols, the sensor nodes are divided into clusters, then sensor node with higher resources is selected as cluster head (CH). The CH organizes all the activities within its cluster. It is also the responsibility of CH to gather information from cluster nodes, aggregate and remove between gathered data in order to reduce the energy requirements for sending data packets from the CH to another CH or to the base station [18]. In any case, an approach that depends on a packet-splitting algorithm based CRT that is characterized by a simple modular division between integers was proposed [17]. The application has low overhead in calculation, correspondence and capacity, resistant to DoS assault. A trade-off between vitality effectiveness and dependability of the CRT sending plan when obligation cycling systems are considered was explored [10]. This was accomplished with a direct increment in the general multifaceted nature and with low overhead. It was also observed that the constrained vitality utilization prerequisites and the low many-sided quality in the sensor equipment require vitality proficient error control and avoid high unpredictability codes to be sent [7]. Redundant moduli that assume no part in deciding the dynamic range was presented. This was utilized as a part of WSNs to diminish renew information sending by means of happen error in information packet which was centered around low many-sided quality error detection techniques which was executed with low information repetition and productive vitality devouring in remote sensor hub utilizing residue number systems.

A novel vitality proficient and rapid error control conjure that depends on the Redundant Residue Number System (RRNS) in a real-time use of WSNs was proposed [10]. An effective reverse converter which depends on the Mixed Radix Conversion (MRC) scheme was proposed which utilized a novel 3-moduli set \( \{2^{2n-1}, 2^{2n+1} - 1, 2^n - 1\} \) and accomplished huge changes both regarding transformation deferral and equipment outline. Two-redundant moduli set \( \{2^{2n+1} - 1, 2^{2n+1} - 1\} \) was included request to get error controllability. The hypothetical outcomes sponsored by recreation tests affirm that the arrangement outflanks famous error control techniques for WSNs regarding error controllability, vitality productivity, and decrease of end-to-end delay. Authors in [19] likewise proposed information transmission convention that gave dependable association amongst hubs and sink. Residue number system and some redundant modules were utilized to furnish security in transmission concerning vitality in sensors and ideal course is additionally chosen.

As indicated by Authors in [27], remote information uprightness checking is an unequivocal innovation in distributed computing. They introduced a paper on a Proof of Retrievability [POR] plot, which guarantees the accuracy of information, which fundamental trust is kept up. Authors in [27] anyway connected the Number theory based systems such as Residue Number System (RNS) and Chinese Remainder Theorem (CRT) to ensure amends information ownership as well as guarantees retrievability upon a few information debasements. The paper additionally demonstrated the information proprietor that an objective document is unblemished, that is, the customer can recover the whole record from the server with high likelihood. This plan demonstrated the rightness and the likelihood of hacking the information and is wiped out. In light of hypothetical investigation, they exhibited that the proposed convention has a provably secure and exceptionally capable information honesty checking measure. Moreover, authors in [28] directed an exploration on procedures to lessen the effect of the information messages dispose of in ad hoc network. The strategy combines a RRNS and multipath routing. The proposed component utilized the RRNS to part information packets into n-parts and then sent through disjoint courses utilizing a multipath routing convention. Multipath directing convention was utilized to ensure that the n-parts of a message don not go over an extraordinary course from the source to the receiver. This made the proposed method to stay away from malevolent or congested hubs with no past information about such a hub. The examination convincingly was performed utilizing NS-2 which demonstrated that the proposed procedure was substantial. It could outflank other multipath directing conventions in all situations.

In conclusion, authors in [29] proposed various applications for Redundant Residue Number System (RRNS) codes and furthermore exhibited how its codes can be utilized in global communication systems, keeping in mind the end goal to disentangle the related systems by bringing together the whole encoding and interpreting technique crosswise over global correspondence system. They expressed that the RRNS encoding activity can be actualized in light of a gathering of codewords having regular number qualities, by summoning solely expansion tasks. Notwithstanding the previously mentioned uses of RRNS codes for self-checking, error detection and error remedy, a helpful property of the RRNS is that a RRNS codeword does not change its error identification and error revision qualities after number-crunching activities, for example, addition, subtraction and multiplication.

5. Comparison Analysis

A considerable amount of research effort has been focused toward the development of techniques to detect faults that may occur in wireless sensor networks. However, this effort has been limited almost completely to the study of a particular technique for faults tolerant in sensor networks, no approach provides extensive fault tolerant support covering all types of faults that WSNs node is exposed to. It was also observed that none of the several researches on review of fault tolerant WSNs reviewed two techniques together. Nonetheless, there are a few research thinks about on WSNs with the point of
streamlining the vitality utilization of hubs utilizing inventive protection procedures to enhance arrange execution, including the expansion of its life. All in all, vitality preservation is at last to locate the best trade-off between the different vitality expending exercises. Table 1 summarizes the features of different methods used to guarantee wanted unwavering quality and vitality productivity in remote sensor systems.

<table>
<thead>
<tr>
<th>Name</th>
<th>Method</th>
<th>Reliability Improved</th>
<th>Constraint Satisfied</th>
<th>Performance Enhanced</th>
<th>Technique used</th>
</tr>
</thead>
<tbody>
<tr>
<td>EDFBRP [12]</td>
<td>Mobile Agent</td>
<td>Routing model for reliability</td>
<td>Energy and Distance Factor</td>
<td>Increasing the lifetime and data delivery</td>
<td>Location based and hierarchical routing using JADE as agent framework.</td>
</tr>
<tr>
<td>IWSNM-MAS [14]</td>
<td>Mobile Agent</td>
<td>Reliability improved by removing irrelevant redundant data</td>
<td>Redundancy in sensor architecture.</td>
<td>Rate of packet delivery and energy dissipation.</td>
<td>MBD-based wireless sensor network with clustering using C++ Builder</td>
</tr>
<tr>
<td>CRT-RSA</td>
<td>Based for Improving Reliability and Energy Efficiency [17]</td>
<td>Forwarding Schemes</td>
<td>It uses shortest path to enhance reliability also reduces the noise in the receiving end.</td>
<td>Topology change issue because of unreliable channels.</td>
<td>CRT-RSA based Packet splitting algorithm</td>
</tr>
<tr>
<td>RRNS-based</td>
<td>Packet forwarding Technique</td>
<td>Reliability and integrity of data.</td>
<td>More realistic WSNs</td>
<td>Energy consumption and increase in network lifetime</td>
<td>RRNS-based low complexity error detection technique</td>
</tr>
<tr>
<td>RRNS-based</td>
<td>Simple use of RRNS with reliable moduli set</td>
<td>Reliability and integrity of data.</td>
<td>Traffic rate and amount of data transmission.</td>
<td>Reduction in power consumption, simplicity and network efficiency</td>
<td>MBD-based low complexity error detection technique</td>
</tr>
<tr>
<td>High speed</td>
<td>Redundant residue number system (RRNS)-based</td>
<td>An enhanced reliable with high speed application in a real-time WSNs.</td>
<td>Error control and end-to-end delay</td>
<td>Improve security and enhanced error controllability capability techniques as well as power efficiency.</td>
<td>Mixed radix conversion (MRC) based efficient reverse converter.</td>
</tr>
</tbody>
</table>

6. Conclusion

Survey of different methods for providing efficient fault tolerant wireless sensor networks were discussed. The wellsprings of faults in WSNs were also identified and discussed. Different algorithms and/or techniques that were used to prevent, detect, identify, isolate, and treat faults in WSNs were summarized. The existing research works with the notion of improving reliability and energy efficiency were studied elaborately and compared based on their performance and reliability measures. However, it has been observed that no single technique or algorithm can provide a completely reliable solution for the fault tolerance problem of Wireless Sensor Networks. It is suggested that a multi-level approach for providing fault tolerant, reliability and energy efficiency in WSNs applications using agent technologies and redundant number system.

References


