

Signal Strength Based Self Reconfiguration to Ensure Reliability in Wireless Sensor Networks

M. A. Manivasagam¹, T.V Ananthan²

¹Research Scholar, Department of Computer Science and Engineering,
St. Peter's University, Chennai, India

²Professor, Dr. M.G.R. Educational and Research Institute (University), Chennai, India

Article Info

Article history:

Received Nov 20, 2017

Revised Jan 25, 2018

Accepted Feb 12, 2018

Keywords:

Reliability

Self reconfiguration

Stability

ABSTRACT

Providing reliability in Wireless sensor networks is considered to be a challenging task, due to the limited capabilities in terms of energy, power and memory. The applications of these systems run in sensors with low level programming abstractions, limited capabilities and routing protocols. In this paper, we propose a strategy to adjust radios in the sensor network depending on the signal strength of the neighboring nodes to ensure reliability using self reconfiguration (S2R2). Redundancy-based reliability is achieved by performing encoding/decoding either at the source and the destination node or each pair of communicating sensor nodes from the source to the destination. Along with the reliability, the link and the stability of the link are checked. The stability of the route makes the route a valid one to send data. Simulation analysis shows that the proposed mechanism performs better in terms of stability and reliability compared to the existing mechanism

*Copyright © 2018 Institute of Advanced Engineering and Science.
All rights reserved.*

Corresponding Author:

M.A. Manivasagam,
Department of Computer Science and Engineering,
St. Peter's University,
Chennai, India.
Email: manivaasagam.phd@gmail.com

1. INTRODUCTION

Indoor climate monitoring and control, intrusion detection, and energy-use monitoring are examples of Wireless Sensor Network (WSN) applications being deployed in large numbers. Often, each new application requires installation of a dedicated WSN. Reconfiguration is the process by which the sensor network/ some sensors in the sensor network are instructed to change this configuration data. The stored energy in sensor nodes cannot be easily constituted in a WSN due to their geographical position and the environment nature. The frequency and survivability of each node are more or less uniformly distributed throughout the WSN. The failure of the link can negatively influence the performance of the network, reliability and availability.

Redundancy-based reliability is achieved by performing encoding/decoding either at the source and the destination node or each pair of communicating sensor nodes from the source to the destination. The link and the stability of the link are checked for reconfiguring the network. The stability of the route makes the route a valid one to send data in the communication network.

Reconfigurable Wireless Sensor Networks (RWSN) is assumed to be composed of a set of communicating nodes such that each one executes reconfigurable software tasks to control local sensors [1]. Three reconfiguration forms are adapted in RWSN: software reconfiguration allowing the addition/ removal/ update of tasks, hardware reconfiguration allowing the activation/deactivation of nodes, protocol reconfiguration allowing the modification of routing protocols between nodes. A zone-based multi-agent architecture for RWSN is designed where a communication protocol is well-defined to optimize distributed

reconfigurations. Each agent of this architecture is modeled by nested state machines in order to control the problem complexity.

RWSN is controlled by a multi-agent architecture. Timed automata models are designed for the specification and verification of this architecture [2]. Each agent is modeled by Timed Automata (TA) to verify functional and temporal constraints when communicating with remote agents. RWSN is a set of networked nodes that execute reconfigurable software tasks for the control of local sensors. RWiN of an RWSN was designed using Unified Modeling Language (UML) to analyze, construct, develop, and verify easily RWSN architectures [3]. For that, a meta model of RWSN was formulated based on UML to describe a zone-based architecture that uses a communication protocol for the optimization of distributed reconfigurations. To control the design complexity, each agent of this architecture was modeled by nested state machines. To verify the temporal constraints by communicating agents, each one is modeled by a timed automaton.

In STEM-Net, self-organization is managed through fully-reconfigurable wireless devices (called stem-nodes), that can undergo mutations to fulfill a specific tasks, like their biological counterpart [4]. The main characteristics of stem-nodes are presented and the evolutionary behaviour is discussed which can result in an extreme flexibility of the whole network segment, transforming the technological heterogeneity from a limitation to a richness.

The pipeline of reconfiguration is a novel approach that gives a decision making mechanism for any system of tasks when several reconfiguration scenarios are required [5]. In the case of their frequent income, the pipeline follows a specific set of steps in order to figure out the scenarios that need to be applied without altering its own performance. The steps are represented by a sequence of modules. The first module checks the availability of the resources needed by the tasks. The second maintains the stability by rejecting any insupportable flow of software reconfigurations that can destabilize a system. The third module checks the availability of memory for each software reconfiguration request, whereas the fourth verifies the availability of energy for the execution of a new system software configuration.

A method is proposed to design a reconfigurable smart sensor interface for industrial WSN in IoT environment, in which complex programmable logic device (CPLD) is adopted as the core controller [6]. Thus, it can read data in parallel and in real time with high speed on multiple different sensor data. The standard of IEEE1451.2 intelligent sensor interface specification is adopted for this design. It comprehensively stipulates the smart sensor hardware and software design framework and relevant interface protocol to realize the intelligent acquisition for common sensors. A new solution is provided for the traditional sensor data acquisition.

An intelligent agent is developed, which provides four solutions to reconfigure the system at runtime [7]. For these solutions, in order to reconfigure the probabilistic tasks to be feasible, the agent modifies their temporal parameters dynamically; moreover, in order to feasibly serve the probabilistic tasks and reduce the system's power consumption, the agent provides three virtual processors by dynamically extending the periods of the periodic tasks.

In a traditional wireless sensor device, sensor and communication electronics are built as separate components and their integration consists of designing a board to accommodate multiple integrated circuits (ICs). In contrast, the FPGA core allows us to put a standard sensor interface, embedded Digital Signal Processing (DSP) algorithms for Software-Defined Radio (SDR), and a microprocessor control system on a single-chip reconfigurable device [8].

TWIST is based on an analysis of typical and desirable use-cases. It provides basic services like node configuration, network-wide programming, out-of-band extraction of debug data and gathering of application data, and also introduces several novel features [9]. Firstly, TWIST supports experiments with heterogeneous node platforms. Secondly, it supports active power supply control of the nodes. This enables easy transition between USB-powered and battery-powered experiments, dynamic selection of topologies as well as controlled injection of node failures into the system. Thirdly, TWIST supports creation of both at and hierarchical sensor networks.

Based on the supervisory control theory (SCT) of timed discrete-event systems (TDES), this study presents a dynamic reconfiguration technique for real-time scheduling of real-time systems running on uni-processors [10]. A new formalism is developed to assign periodic tasks with multiple-periods. By implementing SCT, a real-time system (RTS) is dynamically reconfigured when its initial safe execution sequence set is empty. During the reconfiguration process, based on the multiple-periods, the supervisor proposes different safe execution sequences.

Autonomous network Reconfiguration System (ARS) enables a multi-radio WMN to autonomously recover from local link failures to preserve network performance. By using channel and radio diversities in WMNs, ARS generates necessary changes in local radio and channel assignments in order to recover from failures [11]. An Optimized Routing Scheme with Self Reconfiguration (ORSSR) enables a multi-radio

WMN to autonomously recover from local link failures to preserve network performance [12]. The Ad hoc On-Demand Distance Vector (AODV) is enhanced by proposing a new hybrid routing metric and is then coupled with an Autonomous Network Reconfiguration System (ARS). Multi-hop wireless mesh networks (WMNs) experience frequent link failures due to channel interference, dynamic obstacles, and bandwidth demands. These failures cause severe performance degradation in WMNs [13]. Quick Autonomous Reconfiguration System (QARS) enables a multi-radio WMN to autonomously recover from local link failures.

Particle Swarm Optimization (PSO) has already proved its effectiveness in enhancing clustering operation, energy efficiency, etc. However, PSO also suffers from a higher degree of iteration and computational complexity when it comes to solving complex problems, e.g., allocating transmittance energy to the cluster head in a dynamic network [14]. Cluster based Energy Efficient Routing Protocol (CBEERP) gathers the sensor hubs in the system into clusters. In this manner it productively decreases the flooding traffic during discover the routing. CBEERP will balance the Energy in the Group by using some second order nodes [15]. All the nodes have the option of electing next Data Communication Node. The next data communication node is chosen depending on the intensity of link, remaining energy, and the node with distance towards the Base Station [16].

2. RESULTS AND ANALYSIS

The self reconfigurable wireless sensor networks include the following as the key points.

2.1. Self reconfigurable WSN

The reconfiguration mechanism can be used depending upon the reconfigurable forms:

Hardware reconfiguration: Activation and deactivation of detectors and nodes are performed in the hardware reconfiguration. To deactivate a node, all the detectors should be deactivated. For activating the same node, the detector node is activated.

Software reconfiguration: The behavior of the nodes can be changed during run time. This change can be applied to the software architecture by insertion or removal of QS tasks to be executed in nodes, the change of data used by tasks and by the modification of their scheduling.

Protocol reconfiguration: Modification in data routing is required when the programming and equipment reconfigurations are executed at run time. This reconfiguration allows the degradation and optimization of the protocol by the removal, update and addition of the exchanged messages between the nodes and their routing paths.

The radio cognition component is responsible for gathering information that the cognitive radio network needs to be aware of. The information of radio environment includes information regarding the interference distribution and signal to interference noise ratio.

Adjusting radios is nothing but the effective swapping of frequencies according to the QoS demand in the network. The received signal strength is one method to estimate both the distance and the quality of service required by the network. If the underlying MAC allows switch between the radios, then possibly depending on the current fault occurrence, a radio switch is a possible self-reconfiguration method for a WSN.

2.2. Path stability

Path Stability (PS) can be calculated by equation 1.

$$PS = \text{Max}_{i=1}^{hc} LS(i) \quad (1)$$

where hc represents the maximum number of hop count in the selected route. The path that has the maximum PS will be selected as the most stable route to carry the data packets from the source. LS denote the stability of the link in the communication network.

The algorithm is shown below for the proposed system. Initially the source sends route request to all its neighbors. The nodes which receive the route request will reply back to the source and thus routes are formed. The Signal to Interference Noise Ratio (SINR) for all the neighbor nodes is calculated in the communication network. The node with high SINR value is selected as the next node. Finally a valid route is found from source to destination. The data is send from source to destination in the selected path. IF any link failure occurs in the path, then there is chance for the data to be lost. Therefore the self reconfiguration comes into existence in this process. The link failure node is detected in the network using SINR and the distance between the communication nodes in the network. Alternate node is checked for data transmission. The

alternate node is selected in terms of path stability and reliability. The path stability and reliability of the nodes are calculated in their average and is defined as Quality link. The Quality link is calculated using the equation 2.

$$QL = \frac{\sum_0^n Pathstability + reliability}{2} \quad (2)$$

Where n = number of nodes

The threshold is calculated with the quality of the link. The value with higher threshold is selected as the QL node. The route is recovered in this process. The data is transmitted from the quality link to the next node. If there is no link failure, the data is sent from source to destination successfully.

Signal strength based Self Reconfiguration to ensure Reliability S²R²- algorithm

```

Process
Begin Source (S) broadcasts → RREQ
        receive RREP ← Destination (D)
Several route discovered from S → D
Calculate SINR
Data Transmission do {
  Select Intermediate Hop (IH) ← max SINR node
  Transmit the data via IH nodes
  If Link Failure occur
    Go to Self Reconfiguration
    Detect Link Failure Node (LFN)
    Route discovery process in LFN Neighbour do
      Compute LFN neighbour Path Stability
      Compute LFN neighbour Reliability
      Calculate Quality Link (QL) value
    Check QLThresh
    Select QL node > QLThresh
    Route recovered
    Now send data from current QL node to Dest
  else
    Send data from S to D
End

```

2.3. Reliability

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

3. PERFORMANCE EVALUATION

In this section, we provide performance evaluation of the S2R2 is analyzed by using the Network Simulator (NS2). This software is an open source programming language written in C++ and Object oriented Tool Command Language (OTCL). NS2 is a discrete event time driven simulator that is used to mainly model the network protocols. The nodes are distributed in the simulation environment. The simulation of the S2R2 scheme is described in table 1.

Table 1. Simulation parameters

Parameter	Value
Channel Type	Wireless Channel
Simulation Time	50 s
Number of nodes	50
MAC type	802.11
Traffic model	CBR
Antenna Model	Omni Antenna
Simulation Area	1000×1000
Transmission range	250m
Network Interface Type	WirelessPHY

In this proposed scheme, every node has the direct link with the nodes within the range 250m. The nodes are communicated with each other by using User Datagram Protocol (UDP). All the nodes receive the signal from all directions by using the omni-directional antenna. The performance of the S2R2 scheme is analyzed by using the parameters Packet Delivery Rate (PDR), Packet Loss Rate (PLR), average delay, throughput and residual energy.

3.1. Packet Delivery Rate

The Packet Delivery Rate (PDR) is the rate of number of packets delivered to all destinations to the number of data packets sent by the source node. PDR is measured by the equation 3.

$$PDR = \frac{\sum_0^n \text{Packets Received}}{\text{Time}} \tag{3}$$

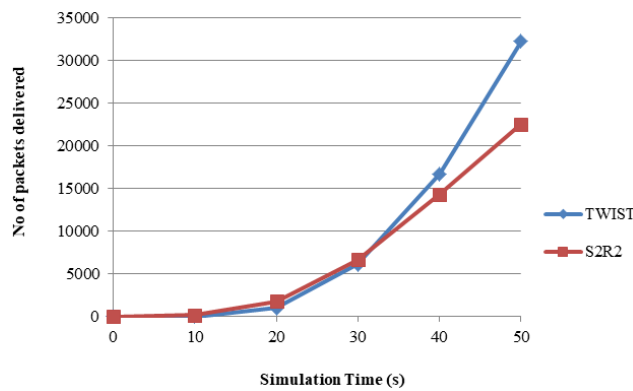


Figure 1. Packet Delivery Rate

The Figure 1 refers the PDR of the proposed scheme S²R² is higher than the PDR of the existing method TWIST.

3.2. Packet Loss Rate

The Packet Loss Rate (PLR) is defined as the difference between the sent packets and received packets in the network per unit time as in equation 4.

$$PLR = \frac{\sum_0^n \text{Sent Pkts} - \text{Rcvd Pkts}}{\text{Time}} \tag{4}$$

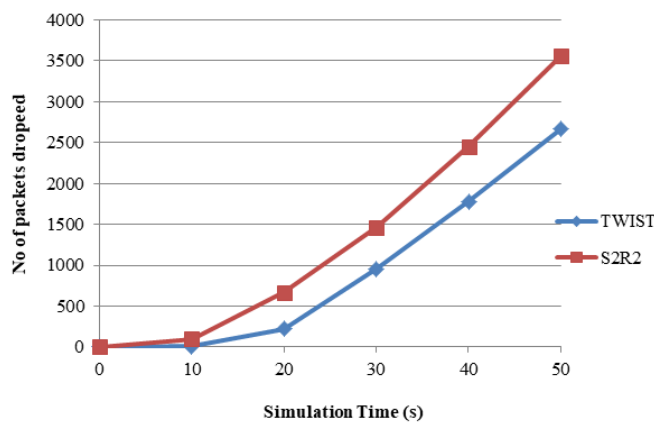


Figure 2. Packet Loss Rate

Figure 2 indicates that the total packets lost of TWIST are greater when compared to the S²R² mechanism. The S²R² has reduced packets lost due to highest security routing.

3.3. Throughput

Throughput refers to the total number of packets successfully delivered across the network for every 1000 packets sent. Throughput is obtained using equation 5.

$$\text{Throughput} = \frac{\sum_0^n \text{Packets Received}(n) * \text{Packet size}}{1000} \quad (5)$$

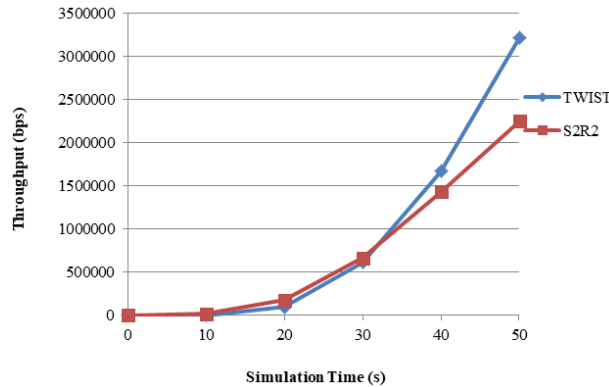


Figure 3. Throughput

Figure 3 show that S²R² has greater average throughput when compared to the TWIST mechanism. The security activity has improved the network performance greatly.

3.4. Average Delay

The average delay is defined as the time difference between the current packets received and previous packets received. It is measured by the equation 6, here n is the number of nodes.

$$\text{Avg_Delay} = \frac{\sum_0^n (\text{Packet Received Time} - \text{Packet Sent Time})}{n} \quad (6)$$

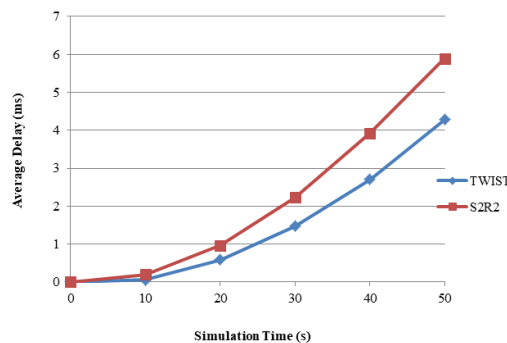


Figure 4. Average Delay

The average delay value is plotted in Figure 4, which shows that the delay value is low for the proposed scheme S2R2 than the existing scheme TWIST. The minimum value of delay means that higher value of the throughput of the network.

3.5. Residual energy

The amount of energy remaining in the node at the current instance of time is called residual energy.

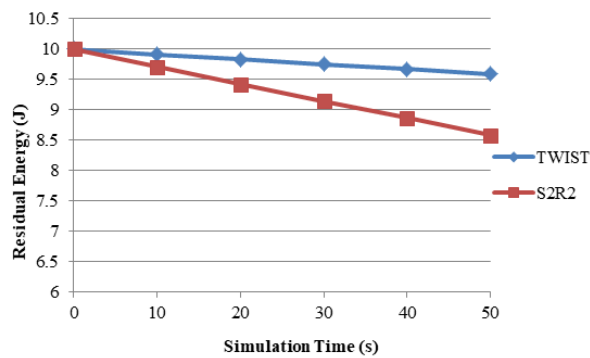


Figure 5. Residual Energy

Figure 5 shows that the proposed method S2R2 performs better compared to the existing scheme TWIST.

3.6. Network reliability

The capacity of the network to offer the same services even during failure is called as network reliability.

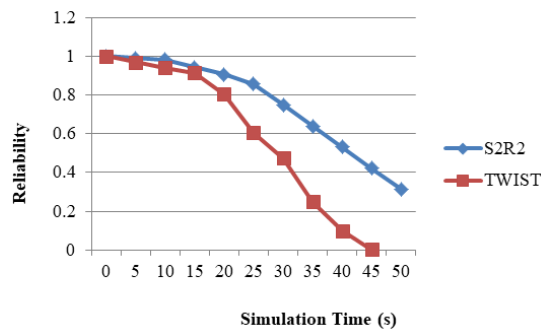


Figure 6. Reliability

Figure 6 shows that the proposed method S2R2 performs better compared to the existing scheme TWIST.

4. CONCLUSION

In this paper, a strategy to adjust radios in the sensor network depending on the signal strength of the neighboring nodes to ensure reliability using self reconfiguration (S2R2) is proposed. The link and the stability of the link are checked along with the reliability. The stability of the route makes the route a valid one to send data. Simulation analysis shows that the proposed mechanism performs better in terms of stability and reliability compared to the existing mechanism.

REFERENCES

- [1] H. Grichi, *et al.*, "Reconfigurable Wireless Sensor Networks new adaptive dynamic solutions for flexible architectures," Software Engineering and Applications (ICSOFT-EA), 9th IEEE International Conference on, 2014.

- [2] H. Grichi, *et al.*, "Formal specification and verification of reconfigurable wireless sensor networks," Systems, Signals & Devices (SSD), 12th IEEE International Multi-Conference on, 2015.
- [3] H. Grichi H, *et al.*, "RWiN: New Methodology for the Development of Reconfigurable WSN," *IEEE Transactions on Automation Science and Engineering*, vol. 14, no. 1, pp. 109-125, 2017.
- [4] G. Alooi, *et al.*, "STEM-Net: an evolutionary architecture for highly-reconfigurable wireless networks," Future Network and Mobile Summit (FutureNetworkSummit), IEEE, 2013.
- [5] M. Gasmi, *et al.*, "R-node: new pipelined approach for an effective reconfigurable wireless sensor node," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 2016.
- [6] Q. Chi, *et al.*, "A reconfigurable smart sensor interface for industrial WSN in IoT environment," *IEEE Transactions on Industrial Informatics*, vol. 10, no. 2, pp. 1417-1425, 2014.
- [7] X. Wang, *et al.*, "Dynamic low-power reconfiguration of real-time systems with periodic and probabilistic tasks," *IEEE Transactions on Automation Science and Engineering*, vol. 12, no. 1, pp. 258-271, 2015.
- [8] V. Kindratenko and D. Pointer, "Mapping a sensor interface and a reconfigurable communication system to an FPGA core," *Sensor Letters*, vol. 3, no. 2, pp. 174-178, 2005.
- [9] V. Handziski, *et al.*, "Twist: a scalable and reconfigurable testbed for wireless indoor experiments with sensor networks," Proceedings of the 2nd international workshop on Multi-hop ad hoc networks: from theory to reality, ACM, 2006.
- [10] X. Wang, *et al.*, "Dynamic multiple-period reconfiguration of real-time scheduling based on timed DES supervisory control," *IEEE Transactions on Industrial Informatics*, vol. 12, no. 1, pp. 101-111, 2016.
- [11] K. Kyu-Han and K.G. Shin, "Self-reconfigurable wireless mesh networks," *IEEE/ACM Transactions on Networking (TON)*, vol. 19, no. 2, pp. 393-404, 2011.
- [12] G. Gayathiri, "An Improved Optimization Scheme for Self Reconfiguration in Wireless Mesh Networks".
- [13] A. Melveena, and D.R. Dorai, "QARS for Self Reconfiguration Mechanism in Wireless Mesh Networks," *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)*, vol. 2, no. 2, pp-739, 2013.
- [14] P. Hemavathi and A.N. Nandakumar, "Novel Scheme for Minimal Iterative PSO Algorithm for Extending Network Lifetime of Wireless Sensor Network," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 8, no. 2, 2018.
- [15] M.N. Elshakankiri, *et al.*, "Energy efficient routing protocol for wireless sensor networks," Intelligent Sensors, Sensor Networks and Information Processing, IEEE International Conference on, 2008.
- [16] J. Singh and V. Mansotra, "Prospect Convenient Steadfast Procedure in Wireless Sensor Network," *Indonesian Journal of Electrical Engineering and Computer Science (IJECS)*, vol. 9, no. 3, 2018.