Research Journal of Applied Sciences 12 (2): 139-147, 2017
ISSN: 1815-932X

Building Fault Tolerance Within Wireless Sensor Networks: A Butterfly Model

[1]M. Sai Rama Krishna, [1]J.K.R. Sastry and [2]J. Sasi Bhanu
[1]Department of ECM, KL University, Vaddeswaram, Guntur, 522501 Andhra Pradesh, India
[2]Department of CSE, St. Martin College of Engineering, Dupally, Hyderabad, India

Abstract: The wireless communication is creating revolution in the present day life. A WSN is a system of wirelessly communicating nodes where each node is equipped with multiple components. Wireless sensor networks plays a major role in providing support for observing, processing and making decisions depending on the observations. WSN is a self-organized network that consists of large number of low cost and low powered sensor devices called sensor nodes. These networks are most widely used in industries, military, surveillance, environmental monitoring, etc. WSNs are prone to be affected by different failures such as power depletion, environmental impact, interference, communication link failure, dislocation of sensor node and collision. If those faults are not handled properly they will not meet their desired goals. So, a sensor network should be fault resistant. Fault tolerance is the property that enables asystem to continue operating properly in the event of failure of some of its components. Fault-tolerance mechanisms such as fault-detection and fault-recovery are needed to protect these networks from various faults. In this study, a butterfly network based WSN is presented that enhance the reliability and fault tolerance capability of the WSN.

Key words: Wireless sensor networks, fault tolerance, butterfly model, surveillance, communication link failure

INTRODUCTION

Wireless Sensor Networks (WSNs) play a major role in present day technology which acts as a bridge between the physical and virtual worlds. These sensors are small with limited processing and computing resources which are inexpensive and helps in sensing, computing and gathering information from the environment based on the requirement they can transmit the sensed data. A wireless sensor network is a self-configuring network of small sensor nodes which helps in communicating among them using radio signals deployed in quantity to sense, monitor and understand the physical world. A typical wireless sensor network is shown in Fig. 1.

From the network July 1, 2017, it can be seen that many components are to be inter-conceded for remote sensing and transmitting data to a distantly situated server and also to receive data from the server and accordingly control the functioning of a local environment. WSN's work in harsh environments and may be subjected to failure by several layers in a system. If a node which is to be broadcasted is in a failure state then all the other nodes will be starved waiting for the data. There may be several faults that may occur which includes node faults, link faults, sink and source faults and network faults. WSN must be free from faults. The network must be recovered from the fault as soon as possible when the fault occurs. A WSN can be made to be operating under normal conditions even when a fault occurs by implementing fault recovery techniques. Faults can happen within WSN involving many components of the network. Different fault tolerance techniques when introduced into the system make the WSN more reliable. Replication has been one of the major concepts that have been implemented over the time for making the WSN fault tolerant. The quality of WSN may suffer due to the introduction of redundancy within the wireless networks.

Any WSN can be made to be fault tolerant by implementing fault recovery methods. Many components that are used in a WSN can be the sources for creating faults within WSN. Many fault tolerant techniques of different types have been proposed in the past to be able to implement highly reliable functions of a WSN. Two classes of recovery techniques are in uses which include either the active or passive replication techniques. In the case of active replication, a request is processed by all replicas whereas in the cases of passive replication only one replica process the request and if it fails the next replica will take over and continues till the last replica. If none of the replica could process the request the WSN will be moved to a failure state.

Corresponding Author: M. Sai Rama Krishna, Department of ECM, KL University, Vaddeswaram, Guntur, 522501 Andhra Pradesh, India

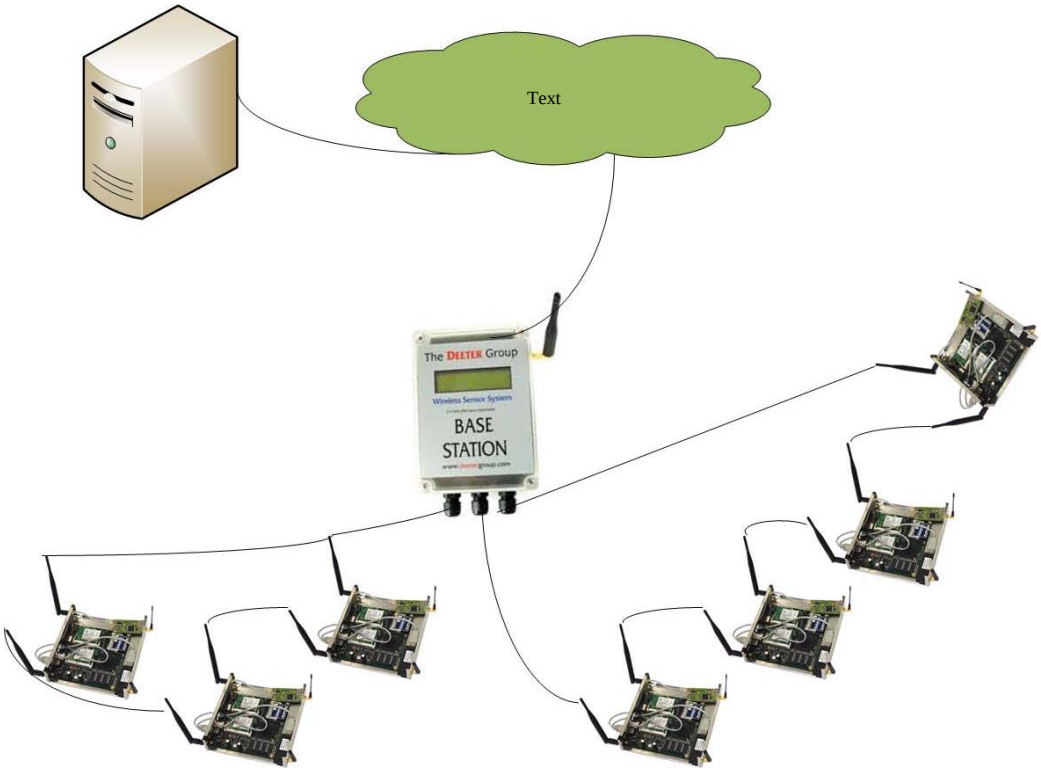

Fig. 1: Prototype of a wireless sensor network

A WSN can be K connected so that failure of K-1 nodes will still make the system functional. Paths in a WSN can be replicated and used using the multipath routing protocols. Many algorithms have been developed that determine minimum number of additional nodes to be added into a WSN so that the network is K connected and therefore, allows k-1 failures. The position of the additional nodes also determines whether the WSN is K connected. Aggregation is a method that fuses data at higher level node that has been sensed and transmitted by the sensors which are situated in a low level within the network. The data fusion techniques provides high level information. There is always trade-off between the precision with which the data aggregation is done and the number of additional nodes included to achieve node duplication/replication. It is simple to implement to ignore the data transmitted by a faulty node. However, in this case also it becomes a challenge to determine the faulty node. Lot save of computation time can be save if the data sensed by a failed node has not been transmitted across the network.

A node must be selected as a service provider. A new service provider must be selected when it is known that primary replica has failed. After one node is selected as primary replica, one or more nodes must be selected to make them act as backup replicas. Many methods have been presented in literature using which one can determine the nodes as primary and backup service providers. The approaches to selection of nodes are completely based on the stage of processing and also the nodes that must be made to be doing the replica processing. The selection of the nodes can be achieved by using several methods that include self-selection, group selection and hieratical selection.

In the case of self-selection every node executes an algorithm to find whether it should serve as a cluster head for the neighboring nodes. The algorithm implements a random probabilistic distribution. Every node changes it role in the network for acting as a cluster head. It takes little time in this case to make some other node as cluster head if the acting cluster head node fails.

The issue of group-selection arises when a clustered head fails. A set of nodes are grouped and one of the nodes is identified as cluster head. When a cluster head fails a new group of nodes with a different cluster head are chosen and brought into the service. Every cluster head will maintain a group of neighboring nodes and another set of nodes as backup processing units. By selecting a cluster head all the processing nodes and the backup nodes could be found. When a gateway or a

cluster fails, the nodes in its cluster are relocated to some other cluster head as either primary processing nodes or backup processing nodes. If node is allocated to more than one cluster head then in that case the node is assigned to the cluster head that has the least communication cost.

A coordinator selects a primary node in the case of hierarchical selection. Once a node is selected as primary node, the routing paths are determined and also the new cluster head is identified. The coordinator selects a node to be a cluster head based on its closeness to the base station. Fuzzy logic is frequently used to find the cluster head which is close to the base station an algorithm is used within the coordinator that takes into consideration of fuzzy descriptor, concertation at different nodes, level energy each of the node and the centrality of the nodes within the cluster of nodes.

WSN are being used for many critical and mission critical systems, failure of which may sometimes leads to disastrous situations and MSN lead to great losses in many forms. The WSN networks are delicate as the networks are established using tiny and fragile devices and generally quite prone for failures. Therefore, it is necessary that WSN are built considering the failures of the devices used for networking. It is necessary to build as much fault tolerance as possible into WSN so that the networks can be made to work as much reliably as possible.

There are methods presented in the literature for increasing the fault tolerance of the WSN network and none of the methods presented have presented verifiability of the fault tolerance levels of the WSN network. The problem is to find the methods, techniques and mechanisms using which the WSN can be made to be fault tolerant and verifiable. In this study, two methods have been proposed using which fault tolerance levels can be computed. The fault tolerance computed by both the methods provides for verifiability of the reliability of the WSN networks.

Literature review: Wireless sensor networks are small devices, low cost, limited memory, low power and low power consumption devices. The main aim of the sensor networks is to provide the reliability, maintainability, availability. In general, there will be faults which may occur due to various factors such as node fault, sink fault, network faults. Mishra *et al.* (2012) have expressed that WSN can be subjected to many faults and may fault detection methods have been inn use which includes self-diagnosis and group detection.

Chouiki *et al.* (2015) have presented two fault tolerant routing solutions which include re-transmission in which the source node sends their data over an established path and if this path fails to forward the information, the source retransmits those data through another path. The second technique is the data replication that performs by sending different copies of the same data over multiple paths. They have classified the fault tolerance techniques into preventive and curative techniques. They has also presented performance metrics of fault tolerance mechanisms which are related to complexity, overhead, impact of the fault tolerance on performance, etc. Fault tolerance techniques are presented according to their main objectives which include energy and flow management in small scale WSN, data management in small scale sensor networks and coverage and connectivity in small scale networks while the Large Scale Wireless Sensor Networks (LS-WSNs) are composed of thousands of sensors based on different objectives that include energy and flow management in LS-WSNs, Data management in LS-WSNs and coverage and connectivity in LS-WSNs.

Hila have presented a detailed survey on fault tolerance within sensor networks. They presented that major components required for a sensor node include Sensing unit, processing unit, transceiver unit and power unit. Mannan *et al.* (2015) and Chouiki *et al.* (2015) have presented that wireless devices are battery operated for maintaining routing protocols in an efficient manner. The denser levels of sensor node deployment, server power and higher unreliability of sensor nodes, computations and memory constraints are the main issues that provide challenges in WSN's.

Flooding is a blind method that is used to broadcast data and packets to the rest of the nodes in the network. It continues until the destination node is reached by flooding, which results in impulsion or overlap. When same region is sensed by two sensors and the sensed data is broadcasted at the same time, the neighbours will receive the duplicated packets.

Yuan and Zhang (2008) have presented the securing of the data through introducing fault tolerance within WSN. Inside the network, all sensor nodes are equal in hardware and software configuration, hence having the identical talents in computation, verbal exchange and storage. Due to its inherent restricted capabilities, a node can be operational if they are able to perform their duties in the modern-day WSN application or non-operational or fail because of various troubles together with device crash or energy depletion. The position of aggregating

and forwarding the information is known as sink. A node can't be each a sink and a source due to the fact this will substantially dissipate the constrained power electricity inside the node. A node routing protocol is assumed to be present which can efficaciously supply messages from distinctive assets to the sink thru one or more wireless hops.

Kakamanshadi *et al.* (2015) have presented that limited bandwidth; power, fixed infrastructure and many types of problems such as path and node failures characterise WSN networks. The WSN networks also are venerable for attacking. The nodes within a WSN must be self-organised and self-configurable so that efficiency, performance and data transmission rates can be enhanced and improved. One of the main objectives of WSN is to make the SNs functional for longer durations. SNs as such are amenable for failures for various reasons which include environmental impact, radio interference, battery depletion, failure of hardware component, transmission link instability, etc. A WSN should be such that even in the event of failures the system must be functioning smoothly. The WSN can be made to be fault tolerant through use of methods that can be classified into clustering based mechanisms, redundancy based mechanisms and deployment based mechanisms.

Liu *et al.* (2016) has presented a scale-free topology model which has both fault-tolerance against random faults and intrusion-tolerance against selective remove attacks at the same time. Koushanfar *et al.* (2002) have presented fault tolerance techniques for wireless adhoc networks. Embedded sensor network is a system of nodes which is effective and efficient embedded sensor systems of low cost, low overhead, high resilient fault-tolerance techniques. The problem of embedded sensor network fault tolerance is proposing heterogeneous back-up scheme where one type of resources is substituted with another.

Parweekar and Rodda (2015) have presented a method to find primary paths to ensure fault tolerance within WSN. Energy conservation has become almost primary goal while throughput and fault tolerance have found second place. Routing in WSNs is usually classified based on the network structure as flat-based, hierarchical and location-based. The nodes in the network are assigned equal or same functional roles. The nodes in the network are assigned differing roles in a hierarchical-based routing architecture. Location-based routing uses sensor node positions used to route network data. Depending on the method of the source finds a route to the destination classified into three categories viz. the proactive, the reactive and the hybrid. In the proactive protocols, all the routes are computed and stored before they are actually needed and in the case of reactive protocols, these routes are computed in real time whereas in the case of hybrid protocols both ideas are optimally used. The data from the sensor is collected and further processed by a central node. Cooperative routing aims at reducing the energy use and thereby the route cost. Cluster Head (CH) has a task of grading the sensors based on several parameters

Cardi *et al.* (2007) have presented fault-tolerant topology control for heterogeneous wireless sensor networks. Resource-constrained wireless sensor nodes deployed randomly in large numbers and a much smaller number of resource-rich super nodes, placed at known locations. The super nodes have two transceivers, one to connect to the Wireless Sensor Network (WSN) and another to connect to the super node network. The super node network provides better QoS and is used to quickly forward sensor data packets to the user. Data gathering in heterogeneous WSNs has two steps: first, sensor nodes transmit and relay measurements on multihop paths towards a super node. Once a data packet encounters a super node, it is forwarded using fast super node-to-super node communication toward the user application. Additionally, super nodes could process sensor data before forwarding. Topology control is a range assignment problem for which the communication range of each sensor node must be computed. The objective is to minimize the maximum sensor transmission power while maintaining k-vertex disjoint communication paths from each sensor to the set of super nodes. In this way, the network can tolerate the failure of up to k-1 sensor nodes. In contrast with range assignment in ad hoc wireless networks, this problem is not concerned with connectivity between any two nodes.

Pilot wireless sensor network: A pilot sensor network which is used for spraying of water and pesticide for turmeric plantation based on the existence of humidity is shown in Fig. 2. The sensor senses the humidity and actuates the spraying of water. The date, time, humidity value, longitude and latitude, extent of water pumped are sent to the central server through internet via base stations. The data is stored at the central server where the data is analysed and any specific instructions required are sent to the formers through SMS messages. Connectivity of the base station to the central server is achieved through a cable connection or through a combination of WiFi/cellular interface.

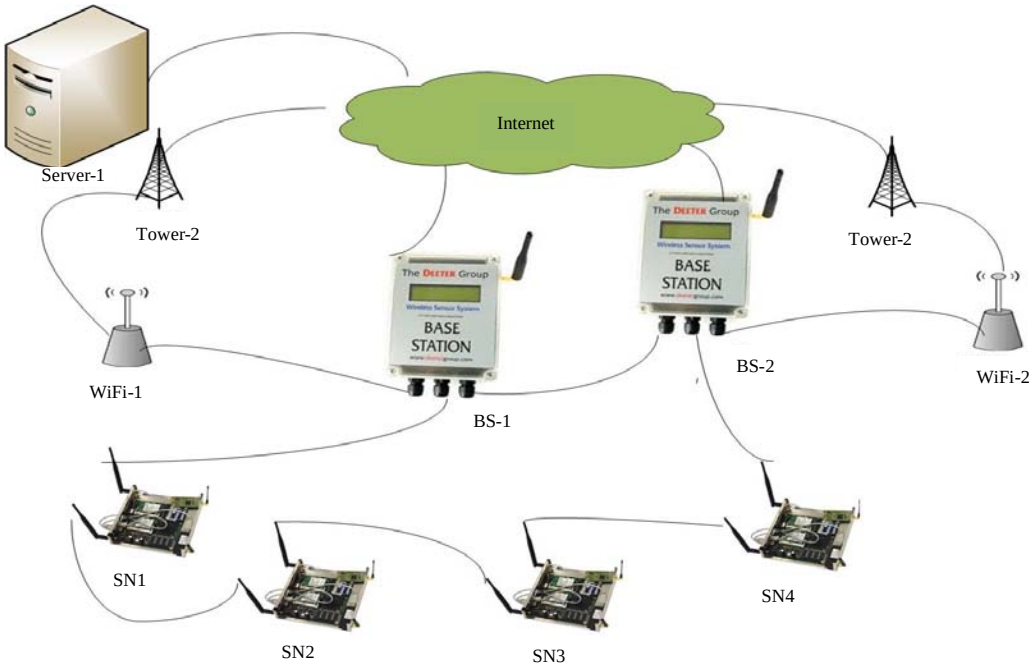

Fig. 2: Application specific WSN

MATERIALS AND METHODS

Computing reliability through FTA of the pilot network: The main investigation made and presented in this paper is to show how the reliability of a WSN can be enhanced based on networking topology implemented at Hardware level. To start with Fault tree for the existing WSN is developed and overall fault rate is computed. The fault tree diagram for the existing WSN is shown in Fig. 3. The failure rates as computed for each of the path in the wireless senor network are shown in Table 1. It could be see from Table 1 that the failure rate of the sample WSN network is 0.684.

Implementing butterfly topology within wireless networks: It is possible that the failure rate of the network can be reduced by implementing different topologies than the tree topology used for the sample WSN. Multi-stage networks are commonly used to connect a set of inputs to a set of outputs; the concept as such is similar to cloud computing. The connectivity is established through links between computing and switching systems. These networks use 2X2 switches. Each switch takes two inputs and produces 2 outputs via different connections (Straight, cross, upper broadcast and the lower broadcast. A butter fly network is a multi-stage networks. Number of stages used depends on the kind of connectivity required.

A butterfly topology which uses 4 stage networks has been considered and the same is fitted into a WSN network. A switch box in stage "I" is connected with the links that are at a distance of 2^i apart. The 4×4 butterfly network is achieved through two 2×2 networks. The probability that one of the paths exists for connecting to a WSN node can be computed as:

$$A_c = 2^{k\rho l}\,\Phi(k) \quad (1)$$

Where:

k = No. of stages
ρ = Probability that a node fails
Φ (k) = The probability that that a switch box in the stage K can fail

The Φ (k) can be computed using Eq. 2:

$$\Phi(k) = 1-(1-\rho l\,\Phi(k-1)^2 \quad (2)$$

The butterfly network connected for fitting the sample WSN has been shown in Fig. 4. The butter fly network has been established using 4×4 network containing 4 stages. The 4×4 network has become necessary due to the availability of 8 elementary levels of inputs and 4 different types of outputs required to make the network reliable and available.

Table 1: Fault rate calculations for sample WSN network

			Preceding devices (Device name)					
			D1	D2	D3	D4	D5	
Devices	Success rate	Gates used for connection	Success rate S1	Success rate S2	Success rate S3	Success rate S4	Success rate S5	Combined success rate
SN1	0.80	-	-	-	-	-	-	0.800
SN2	0.80	AND	SN1	-	-	-	-	0.640
			0.8					-
BS1	0.90	AND	SN1	-	-	-	-	0.720
			0.8	-	-	-	-	-
SN3	0.80	AND	SN2	-	-	-	-	0.512
			0.64	-	-	-	-	-
SN4	0.80	AND	SN3	-	-	-	-	0.410
			0.512	-	-	-	-	-
BS2	0.90	OR	SN4	BS1	-	-	-	0.720
			0.41	0.72	-	-	-	-
WiFi-2	0.80	AND	BS2	-	-	-	-	0.572
			0.72	-	-	-	-	-
Tower-2	0.80	AND	WiFi-2	-	-	-	-	0.460
			0.572	-	-	-	-	-
Internet	0.95	OR	Tower-2	Bs2	Tower-1	Bs1	-	0.720
			0.46	0.72	0.46	0.72	-	-
Server-1	0.95	AND	Internet	-	-	-	-	0.684
			0.72	-	-	-	-	-
WiFi-1	0.80	AND	BS1	-	-	-	-	0.576
			0.72	-	-	-	-	-
Tower-1	0.80	AND	WiFi-1	-	-	-	-	0.460
			0.576	-		-	-	-

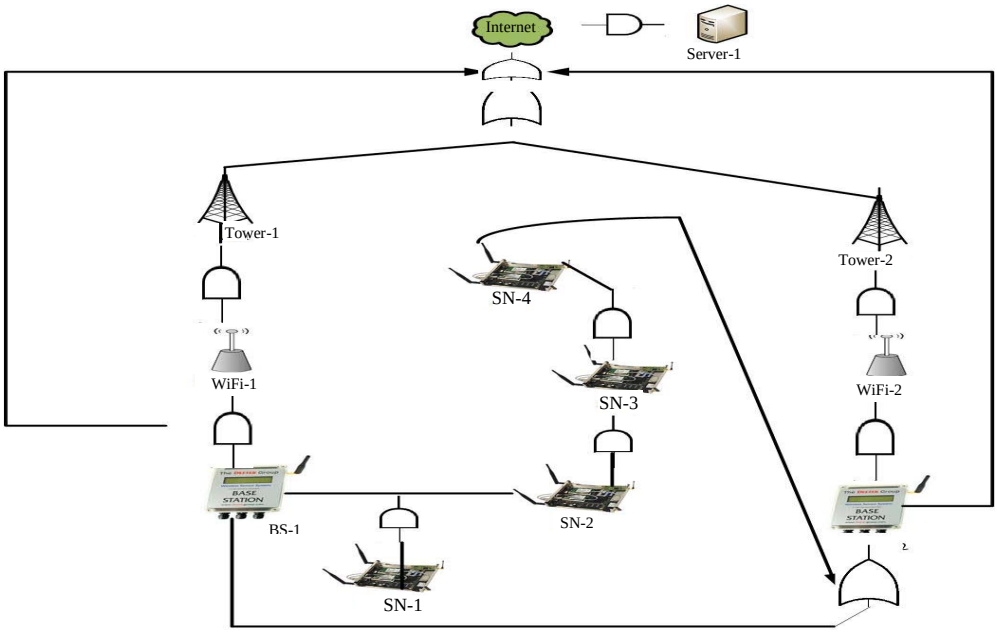

Fig. 3: Fault tree diagram for sample WSN network

Additional switches have been added to make it possible to connect the university cloud into a buttery network. Using Eq. 1 and 2, the probability of success that at least one path exists from input point to an output has been computed as 0.81.

About 4 extra switches have been added to make the WSN network follow butterfly topology and more fault tolerant. The modified network connectivity is shown in Fig. 4 and the connectivity in hierarchical manner fitting butterfly topology in it is shown in Fig. 5.

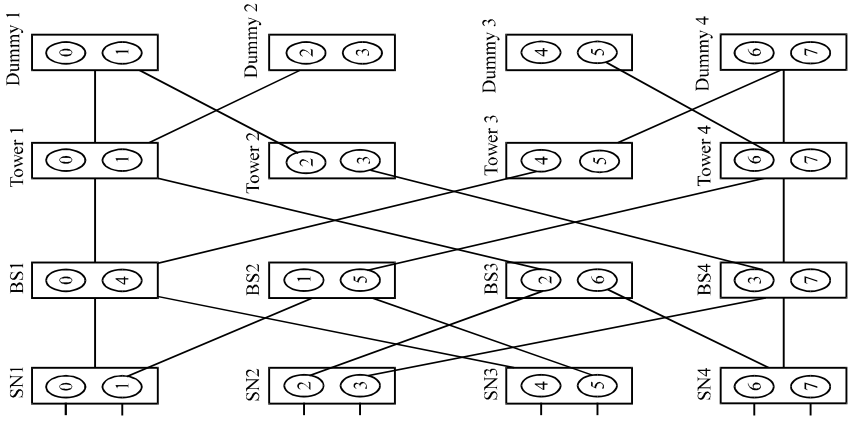

Fig. 4: Butterfly topology for WSN

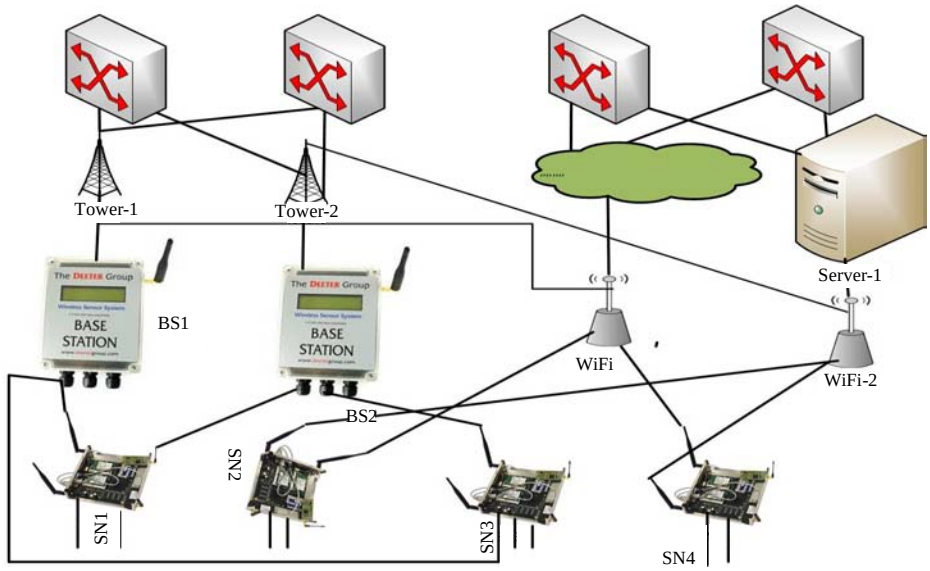

Fig. 5: Modified WSN network-butterfly topology hierarchical models

Table 2: Fault rate calculations for modified WSN network built using butterfly topology

			Preceding devices (Device name)					
			D1	D2	D3	D4	D5	
Devices	Success rate	Gates used for connection	Success rate S1	Success rate S2	Success rate S3	Success rate S4	Success rate S5	Combined success rate
SN1	0.8	-	-	-	-	-	-	0.800
SN2	0.8	-	-	-	-	-	-	0.800
BS1	0.9	AND	SN1	SN3		-	-	0.640
			0.8	0.8	-	-	-	-
SN3	0.8	-	-	-	-	-	-	0.800
SN4	0.8	-	-	-	-	-	-	0.800
BS2	0.9		SN1	SN3	-	-	-	0.800
			0.8	0.8	-	-	-	-
WiFi-2	0.8	AND	SN2	SN4	-	-	-	0.640
			0.8	0.8	-	-	-	-
Tower-2	0.8	AND	WiFi-2	BS2	-	-	-	0.640
			0.64	0.8	-	-	-	-
Internet	0.95	AND	WiFi1	BS1	-	-	-	0.608
			0.64	0.64	-	-	-	-

Table 2: Continue

			Preceding devices (Device name)					
			D1	D2	D3	D4	D5	
Devices	Success rate	Gates used for connection	Success rate S1	Success rate S2	Success rate S3	Success rate S4	Success rate S5	Combined success rate
Server-1	0.95	AND	BS2	WiFi2	-	-	-	0.608
			0.72	0.64	-	-	-	-
WiFi-1	0.8	OR	SN2	SN4				0.800
			0.8	0.8	-	-	-	-
Tower-1	0.8	AND	WiFI-1	BS1	-	-	-	0.512
			0.8	0.64	-	-	-	-
Dummy-1	1.0	AND	Tower-1	Tower-2	-	-	-	0.512
			0.512	0.8	-	-	-	-
Dummy-2	1.0	AND	Tower-1	Tower-2	-	-	-	0.512
			0.512	0.8	-	-	-	-
Dummy-3	1.0	AND	Internet	Server	-	-	-	0.608
			0.608	0.608	-	-	-	-
Dummy-4	1.0	AND	Internet	Server	-	-	-	-0.608
			0.608	0.608				

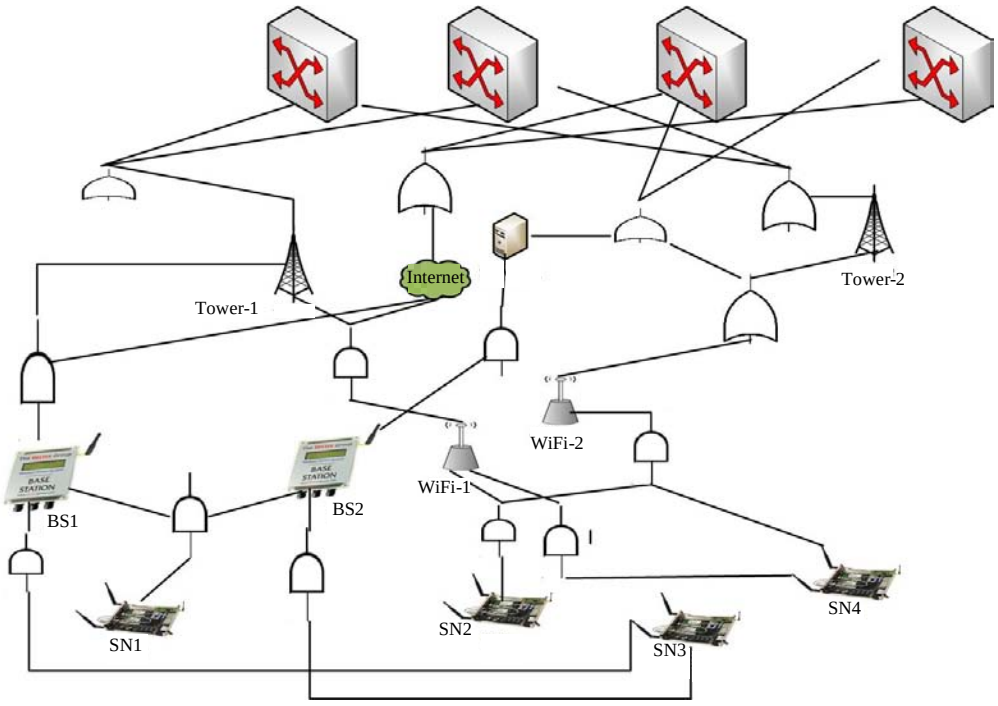

Fig. 6: Fault tree diagram for revised WSN network based on butterfly topology

Reliability of the above network has been computed using Eq. 2 and the failure rate of the same is computed to be 0.510.

Fault tree is also constructed for the above network is constructed and shown in Fig. 6. The computed fault rates are shown in Table 2. The fault rate of such a network computed works out to be 0.51. It can be seen that the fault rate achieved when butterfly network is added falls down quite drastically.

RESULTS AND DISCUSSION

Comparative fault tolerance analysis: Table 3 shows the reliability values computed through fault tree analysis for the original and modified WSN network implement through butterfly topology.

The computation of success rates of different topologies used to develop the WSN is shown in the Table 3. It can be seen from the Table that butterfly topologies when incorporated into WSN network has

Table 3: Comparison of success rates of cloud related network when designed with different topologies

Topology serial	Topology	Failure rates
Mishra *et al.* (2013)	Star based WSN network based on FTA analysis	0.680
Jerlin *et al.* (2015)	Modified WSN with added switches and connected through butterfly topology using fault analysis	0.512
Mannan and Rana (2015)	Tree topology enhanced with identified redundancies included into butterfly network	0.510

increased the success rate making available more continuity of logging of the agricultural data as required.

CONCLUSION

Fault tolerance within a WSN can be enhanced by way of adding redundancy at network level requiring networking gadgets such as switches, bridges and gateways. The devices within the network when connected using the butterfly like topology will enhance the reliability of WSN networks. Fault tolerance as such can be included by way of creating as many paths as possible from a WSN node. In the case of butterfly topology, 3 paths are created from each of the node as 2X2 switches are used to switch the output from one device to other.

REFERENCES

Cardei, M., S. Yang and J. Wu, 2007. Fault-tolerant topology control for heterogeneous wireless sensor networks. Proceedings of the MASS 2007 IEEE International Conference on Mobile Adhoc and Sensor Systems, October 8-11, 2007, IEEE, Boca Raton, ISBN:978-1-4244-1455-0, pp: 1-9.

Chouikhi, S., E.I. Korbi, G.Y. Doudane and L.A. Saidane, 2015. A survey on fault tolerance in small and large scale wireless sensor networks. Comput. Commun., 69: 22-37.

Jerlin, C.A. and N. Rajkamal, 2015. Fault tolerance in wireless sensor networks. Intl. J. Innovative Res. Adv. Eng., 2: 142-146.

Kakamanshadi, G., S. Gupta and S. Singh, 2015. A survey on fault tolerance techniques in wireless sensor networks. Proceedings of the 2015 International Conference on Green Computing and Internet of Things (ICGCIoT), October 8-10, 2015, IEEE, Chandigarh, India, ISBN:978-1-4673-7910-6, pp: 168-173.

Koushanfar, F., M. Potkonjak and S.A. Vincentell, 2002. Fault tolerance techniques for wireless ad hoc sensor networks. Proceedings of the IEEE International Conference on Sensors, Vol. 2, June 12-14, 2002, IEEE, Berkeley, California, ISBN:0-7803-7454-1, pp: 1491-1496.

Liu, H., R. Yin, B. Liu and Y. Li, 2016. A scale-free topology model with fault-tolerance and intrusion-tolerance in wireless sensor networks. Comput. Electr. Eng., 56: 533-543.

Mannan, M. and S.B. Rana, 2015. Fault tolerance in wireless sensor network. Intl. J. Curr. Eng. Technol., 5: 1785-1788.

Mishra, S., L. Jena and A. Pradhan, 2012. Fault tolerance in wireless sensor networks. Intl. J., 2: 146-153.

Parwekar, P. and S. Rodda, 2015. Fault tolerance in wireless sensor networks: Finding primary path. Proceedings of the 2nd International Conference on Computer and Communication Technologies, September 05, 2015, Springer, New Delhi, India, pp: 593-604.

Yuan, T. and S. Zhang, 2008. Secure fault tolerance in wireless sensor networks. Proceedings of the IEEE 8th International Conference on Computer and Information Technology Workshops, July 8-11, 2008, IEEE, Shanghai, China, ISBN: 978-0-7695-3242-4, pp: 477-482.