Paper

Bayesian Network Based Fault Tolerance in Distributed Sensor Networks

B. Bhajantri Lokesh[1] and N. Nalini[2]

[1] *Department of Information Science and Engineering, Basaveshwar Engineering College, Karnataka, India*
[2] *Department of Computer Science and Engineering, Nitte Meenakshi Institute of Technology, Karnataka, India*

Abstract—A Distributed Sensor Network (DSN) consists of a set of sensors that are interconnected by a communication network. DSN is capable of acquiring and processing signals, communicating, and performing simple computational tasks. Such sensors can detect and collect data concerning any sign of node failure, earthquakes, floods and even a terrorist attack. Energy efficiency and fault-tolerance network control are the most important issues in the development of DSNs. In this work, two methods of fault tolerance are proposed: fault detection and recovery to achieve fault tolerance using Bayesian Networks (BNs). Bayesian Network is used to aid reasoning and decision making under uncertainty. The main objective of this work is to provide fault tolerance mechanism which is energy efficient and responsive to network using BNs. It is also used to detect energy depletion of node, link failure between nodes, and packet error in DSN. The proposed model is used to detect faults at node, sink and network level faults (link failure and packet error). The proposed fault recovery model is used to achieve fault tolerance by adjusting the network of the randomly deployed sensor nodes based on of its probabilities. Finally, the performance parameters for the proposed scheme are evaluated.

Keywords—Bayesian network, distributed sensor networks, fault detection, fault tolerance, fault recovery, network control, routing.

1. Introduction

Distributed Sensor Network (DSN) is a collection of sensor nodes organized in a cooperative network, which are densely deployed in hostile and unattended environment with capabilities of sensing, wireless communication, and computations. The most important characteristics of DSN are:

- sensor nodes are prone to maximum failures,
- sensor nodes make use of the broadcast communication pattern and have severe bandwidth restraint,
- sensor nodes have limited amount of resources [1].

Sensor nodes may fail by impact of deployment such as fire or extreme heat, animal or vehicular accidents, and malicious activity. These failures may occur upon deployment or over time after, extensive operation may drain power or external factors may physically damage their part. Additionally, hazards may change devices positions over time, possibly disconnecting the network. Any of these initial deployment errors, sensor failures or change in sensor positions cause the network to be disconnected or malfunctioning, and need to deploy additional sensors to fix the network. Fault occurrence in a DSN may exist at hardware, software, network communication, node levels and application layer [2].

In this work, BN is used for fault tolerance in DSN and to represent conditional independencies between a set of random variables (nodes). The network representing different variables (nodes) have edges that constitutes relationship among random variables that are often casual. BN consists of a set of variables and directed edges between variables (nodes), and each variable has finite set of mutually exclusive states, together with the edges forms a directed acyclic graph. The acyclic network state means there must not be any feedback link or loop.

Over the last decade, the BN has become a popular representation for encoding uncertain knowledge in expert systems [3]. More recently, researchers have developed methods for learning BNs from data. The techniques that have been developed are new and still evolving but they have been shown to be remarkably effective for some data analysis problems. There are numerous representations available for data analysis, including rule bases, decision trees, and artificial neural networks. There are also many techniques for data analysis such as density estimation, classification, regression, fault tolerance and clustering [4].

2. Related Works

The work presented in [5] depicts a distributed fault tolerant topology control in static and mobile wireless sensor network (WSN). The distributed algorithm for assigning minimum possible power to all the nodes in the WSN, such that the network is K-connected is proposed. The paper given in [6] presents a distributed topology control in WSN with asymmetric links. It considers the problem of topology control in a heterogeneous wireless network devices with different maximum transmission ranges. The research given in [7] presents a Bayesian decision model for intelligent routing in sensor networks. A new efficient energy-aware routing algorithm is proposed based on learning patterns that minimizes the main constraints imposed by this kind of networks. The probabilistic decision model both considered the estimation of the available energy at

the neighboring nodes and the importance of the messages to make intelligent decisions. The paper [8] presents a survey on fault management in WSNs. The fault management process is divided into three phases such as fault detection, diagnosis and recovery and also summarizes the existing management architectures, which are adopted to support fault management in WSNs.

The work given in [9] addresses fault-tolerant topology control in a heterogeneous WSN consisting of several resource rich super nodes, used for data relaying, and a large number of energy constrained wireless sensor nodes. It introduces the K-degree anycast topology control (K-ATC) problem. The paper [10] presents a distributed Bayesian algorithm for fault-tolerant event region detection in WSN. The proposed solution in the form of Bayesian fault-recognition algorithms, exploits the notion that measurement errors due to faulty equipment are likely to be uncorrelated, while environmental conditions are spatially correlated. It presented two Bayesian algorithms, the randomized decision and threshold decision schemes, and derived analytical expressions for their performance.

Bayesian fusion algorithm for inferring trust in WSNs is presented in [11]. This paper introduces a new fusion algorithm to combine more than one trust component (data and communication) to infer the overall trust between nodes. Simulation results demonstrate that a node is highly trustworthy provided that both trust components simultaneously confirm its trustworthiness and conversely, a node is highly untrustworthy if its untrustworthiness is asserted by both components. The some of the related works are given in [12]–[17].

The rest of the paper is organized as follows. A proposed work for fault tolerance approach to network control is discussed in Section 3. Simulation and results analysis are presented in Section 4 and Section 5 finally concludes the article.

3. Proposed Work

Earlier works do not consider the zones or regions of network construction in DSN. The size of the network becomes complex and divided into number of networks. They are compared against the different networks in sensor network environment and also prolonging sensors operable lifetime is a main design challenge. This work considers the problem of network control in heterogeneous wireless devices with different maximum transmission ranges in the network. Objectives of the proposed scheme are as follows:

– formation of BN as a mesh network in DSN,

– construct the zones/regions using BN as the network becomes complex,

– placing of Control Manager Node (CMN) in each zone which acts as sink node for monitoring the network,

– achieving fault tolerance by using BNs in two phases: fault detection and fault recovery for transmission of data between source nodes and sink node,

– to achieve optimization of routing as well as energy of all nodes in the DSN.

3.1. System Model

Failures are inevitable in DSNs due to inhospitable environment and unattended deployment. Therefore, it is necessary that network failures are detected in advance and appropriate measures are taken to sustain network operation. The work presents an approach to achieve fault tolerance in two phases:

- fault detection – the fault detection phase is used finds the faulty nodes and the type of faults in the DSN environment based on their probabilities,
- fault recovery re-initializes the network to establish path between sources and sink node.

These two methods are based on the probabilities using BNs to achieve fault tolerance in the DSN.

The proposed system model is composed of distributed sensor nodes with diversified sensing competence and sink node. Group of sensor nodes can be constructed in the form mesh network using BNs in DSN environment. A sensor node V is connected to the BN, G = (V, E), where V set of nodes or vertices in the network and E is the set of edges in the network. While the data is traveling on the BN, it is automatically configured to reach the destination by taking the shortest route which means that least number of hops. Data travels by hopping from one node to another to reaches the destination node in a DSN as shown in Fig. 1.

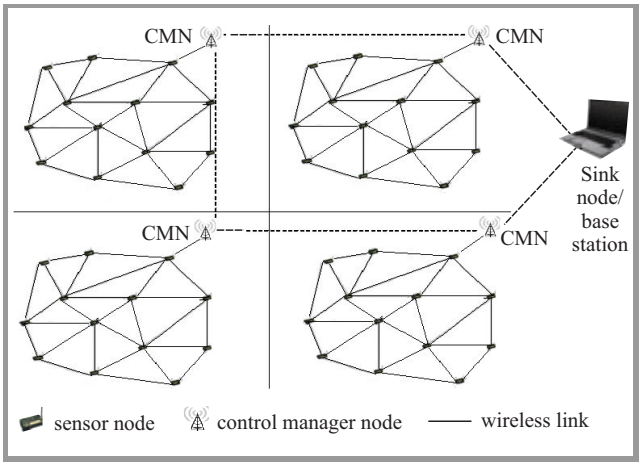

Fig. 1. System architecture.

Nodes sense the data periodically and send it to the sink node with multi hop communication. It is assumed that all nodes (sensor and sink nodes) in the network are static

and have initial energy. All the sensor nodes are equipped with Global Positioning System (GPS), processor and transceiver for the communication able to set the transmission power level. It is assumed that during deployment or construction of network phase each node has full initial energy. All the sensor nodes are equipped with message updating function such as: node_id, residual energy, threshold level energy, number of nodes connected, number of faulty nodes, and connection status in the network. This function is used to calculate the probabilities of each node by using BNs.

As the number of nodes increase, the network becomes complex. Hence the network is divided into number of zones or square regions. Each zone has BN in the form of mesh network for reducing complexities in the environment.

This research using no cluster head mechanism and most of the works are on the basis of cluster heads. Because each round cluster head changes in the network as its takes more end to end delay. The data is transmitted from nearest nodes or distance from different zones and each region employs a network CMN on behalf of sink node. CMN is responsible for monitoring and detecting failure in its region because base station or sink node is far away from the regions. It is also able to directly communicate with other CMN for fault detection.

The fault model is done at two levels using BNs as follows. A node or sink level is used when the nodes probability is less than the threshold level probability, which is based on the residual energy, bandwidth and link efficiency. Otherwise a network level is used as a link failure between nodes and packet error.

3.2. Construction of Bayesian Networks

Figure 2 shows the BN for proposed scheme in which the nodes represent the variables of BN and arcs indicate probabilistic dependencies between nodes. Every node calculates

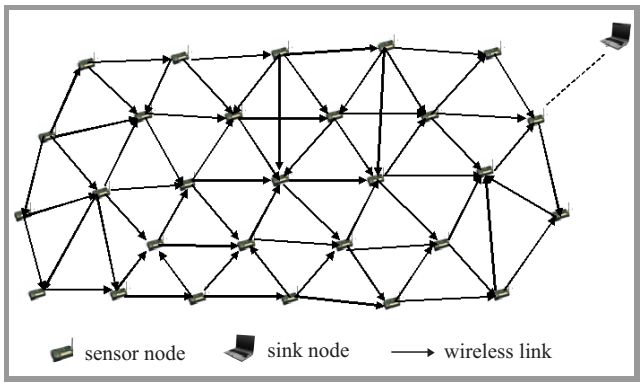

Fig. 2. Bayesian Network for proposed scheme.

the conditional probabilities at each node. Root nodes do not have any parents and its uses the prior probability $P(S_i)$. The ordering guarantees that the BN will have no cycles. The construction of BN algorithm is given by following procedure.

Step 1. Choose a set of variables (nodes) that describes the application domain.

Step 2. Choose an ordering of variables (nodes), i.e., $S_1 \ldots S_N$.

Step 3. Start with the empty network and add variables (nodes) to the network in DSN environment.

For i = 1 to N

Add S_i to network

Select parents from $S_1 \ldots S_N$ such as

$P(S_i \mid \text{parents}(S_i)) = P(S_i \mid S_i \ldots S_{i-1})$

Next i

This choice of parents guarantees the global semantics.

$P(S_1 \ldots S_N) =$

$= \prod_{i=1}^{N} P(S_i \mid S_i \ldots S_{i-1})$ (by chain rule)

$= P(S_1)\, P(S_2 \mid S_1) \ldots P(S_N \mid S_1 \ldots S_{N-1})$

$= \prod_{i=1}^{N} P(S_i \mid \text{parents}(S_i))$ (by construction).

Step 4. Draw an arc from the each variable (node) in parents (S_i) to S_i.

This scheme may be expressed as the product of the prior probabilities of all the root nodes and the conditional probabilities of all the other nodes in the network. The conditional probabilities are important for building BNs. But BNs are also built to facilitate the calculation of conditional probabilities, namely the conditional probabilities for variables (nodes) of interest given the data (evidence). Each variable (nodes) S_1 with parents $S_2 \ldots S_N$ in a BN has an attached conditional probability table $P(S_1 \mid S_2 \ldots S_N)$.

3.3. Inferences or Probability Tables

The given inferences are used in the process of deriving logical conclusion from premises known or assumed to be true. Here BN is used to determine the probabilities of particular types of events. Inference is used to compute the conditional probability for variables with given information (evidence) concerning other nodes or variables. The evidence is available on ancestors of the variables or interests nodes. The evidence is available on a descendant of the variable(s) or nodes of interest to perform inference against the direction of the edges. The proposed Bayes' theorem is given by [18]:

$$P(S_2 \mid S_1) = \big(P(S_1 \mid S_2) P(S_2)\big) / P(S_1). \tag{1}$$

Let d_i be the distance between nodes in the network. It can be computed by using Euclidian Distance Formula (EDF) given by Eq. (2) [19]:

$$d_i = \sqrt{(x_1 - x_2)^2 + (y_1 - y_2)^2}. \tag{2}$$

Link efficiency can be computed as follows. Let C_i be capacity of a discrete-time discrete-valued channel, B be the

bit rate (Hz) of a channel, E_T be the total energy consumed for transmission of a bit in link i, SNR be the signal-to-noise ratio [20]. Capacity of channel i is:

$$C_i = B \log_2(1 + SNR). \tag{3}$$

Assume E_N stands for energy consumption for the transmission of the packets. E_N can be computed by

$$E_N = S_E \cdot P_i/\text{bits} + T_E \cdot P_i/\text{bits}, \tag{4}$$

where S_E – energy required for sensing data or packets, T_E – energy required for transmission of data or packets, P_i – size of packets in terms of bits.

Let E would be the energy consumed for the transmission of a bit per distance d_i. The energy of node E is [20].

$$E = E_N d_i. \tag{5}$$

Assume L_{eff} is the link efficiency for the nodes in the network [21].

$$L_{eff} = \frac{C_i}{E}. \tag{6}$$

Let R_E be the residual energy of each node:

$$R_E = I_E - E_i, \tag{7}$$

where I_E – initial energy of node, E_N – energy consumption.

Assume E_T as the total energy consumption of the path for optimization of routing over the nodes. The total energy required by nodes to sink node over the path is

$$E_T = S_i \cdot C_i \cdot 0.05\ [\text{nJ}], \tag{8}$$

where S_i – number of sensor nodes, C_i – number of Control Manager Node (CMN).

Based on above equations the inferences for the proposed work as given in Tables 1–3 was derived.

Table 1
Inferences

Energy	Distance	Bandwidth	Result
Max.	High	Min.	High
Max.	Fair		Fair
Min.	High		Min.
Fair			High
Max.	Min.	Fair	Fair
Max.		Max.	Min.

Table 2
Distance vs. bandwidth

	Low	Fair	High	Result 1
Min.	0.55	0.80	0.96	2.31
Fair	0.52	0.72	0.85	2.09
Max.	0.44	0.63	0.71	1.78
Result 2	1.51	2.15	2.52	

Table 3
Energy vs. channel capacity

	Low	Fair	High
Min.	0.40	0.56	0.70
Fair	0.55	0.74	0.85
Max.	0.60	0.78	0.97

3.4. Fault Management System

The proposed fault management system consists of two main phases such as: fault detection and recovery.

The fault detection is the beginning phase of the DSN, where faults and failures in the network are properly identified either by using node, sink or CMN. In this work, fault detection by two mechanisms such as self detection (passive detection) and active detection is proposed.

In self detection, sensor nodes are required to periodically monitor their probabilities of the nodes which are based on: residual energy, bandwidth and link efficiency, and then identify the potential failure. This scheme considers the energy depletion as a main cause of nodes sudden death. A node is termed as failing when its probability drops below the threshold level. Detection of decrease in the probabilities of a node by a node itself is called self detection method and is shown in Fig. 3. The probabilities of each node in the network are calculated by using probabilities or inference tables.

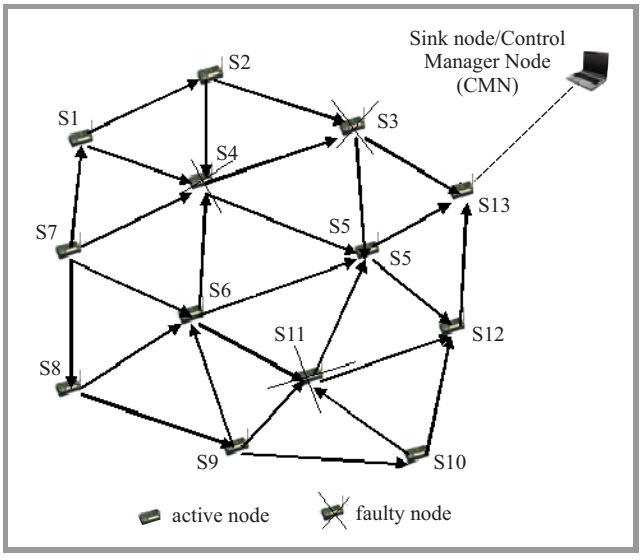

Fig. 3. Self detection method.

In active detection, network control manager node or base station/sink node are continuously monitoring the status of each node in the network. The sink node maintains the update message function. It consists of node ID, energy, bandwidth and link efficiency. Based on the update message function, sink node calculates the probabilities of each node. If sink node do not receive any data from a node for defined time period, then sink node considers that node

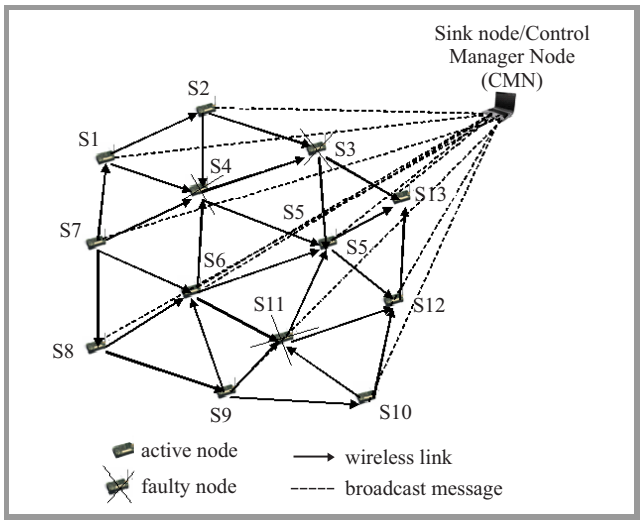

Fig. 4. Active detection method.

as a faulty with low probability in the network and reconstruct the network with node probabilities. Also if any node is below threshold level probabilities, it is assumed to be faulty node in the network, sink node or control manager node broadcast the message or beacon packet to all its nodes in the network and reconstruct the network with active nodes. The beacon packet consists of probabilities of each node. So, this detection is called as active detection as shown in Fig. 4.

Fault recovery is the phase where the sensor network is restructured or reconfigured in such way that failure or faulty nodes to not impact further on network performance. Faulty recovery process is carried out as follows:

- Nodes probability less than threshold – once fault is detected in the network, the nodes with low probability are sent to sleep mode;
- Link Failure – in case of link failure in network, the next nearest node with probability greater than threshold level is selected for forwarding the packets or route the data;
- Packet Error – in case of packet error, the timestamp field is checked. If it is non zero then there is no packet error. Otherwise error has occurred and the packet has to be retransmitted to the desired node through alternate path.

3.5. Routing

Each node in the network senses and forwards the data to sink node. The operations of self detection method for routing over the networks using BN is:

– each node has probability tables in the network,

– each source sensor node checks the probabilities of its neighboring node,

– it always selects the highest probabilities of its neighboring node for forwarding the data,

– it selects another path for transmission if any node is fault in the path or its neighboring node is fault due to some reasons,

– the optimal path for transmission from sources to sink node is based on the highest probabilities,

– sink node takes the action upon receiving the information.

The procedure of active detection method for routing over the networks using BN is as follows:

– network control manager node or base station/sink node are continuously monitoring the status of each node information in the network,

– the sink node maintains the update message function or probability tables,

– in each round sink node or CMN continuously monitors the each nodes probabilities in each region or network,

– if sink node do not receive any data every for some period of time, then sink node considers the node as a faulty and reconstruct the network,

– otherwise, sink broadcast the beacon packet to all its nodes in the network, to detects the faults,

– to reconstruct the network,

– the source node forward the data with highest probabilities of nodes in the network.

The algorithm for proposed scheme is as given below:

Step 1. Deploy S_N number of nodes in DSN as randomly,

Step 2. Find the probability of each node by considering the parameters such as: Energy (E_N), Bandwidth (b), link efficiency (L_{eff}),

- Find the prior probability for parent node,
- Find the joint probability for parent node and child node by using: $P(S_1, S_2 \ldots S_N) = = \prod_{i=1}^{N} P(S_i \mid \text{parents}(S_i))$
- Find the conditional probability for each node: $P(S_1 \mid S_2, S_3, S_4 \ldots S_N) = (P(S_1 \mid S_2, S_3, S_4 \ldots S_N) \times \times P(S_2, S_3, S_4 \ldots S_N)) / P(S_1)$

Step 3. Find the path for each node:

```
For (i = 0; i < N; i++)
{
  if (Probability_Node(Prob_S_N)>=Neighbor_Node)
  {Select highest probability of node for forward
  the data} //Optimization of routing
  Else
  {Select next node with highest probabilities
  in the network}
}
```

Select the highest probability node among these neighboring nodes and make it as next source node and continue this process until it reaches the sink node. This algorithm avoids the cycle formation and find optimal path. After finding optimal path transmit the packets to sink node. Once packets are sent probability of each node is compared with the threshold level probability Th_b. If it is less than Th_b, then the node will be indicated as a dead. Recover the network topology and then consider next optimal path to transmit the packets.

3.6. Fault Tolerance in Network

When node S_1 wants to send packets to S_2 first it will measure the probability of nodes that are in the path between S_1 and sink node. If the probability of nodes in path between S_1 and S_2 are greater than the threshold level probability then packets are forwarded from node S_1 to S_2. If any of the node's probability level is below threshold then it is sent to sleep mode and reconstruct the network. So, this is used to achieve fault tolerance in the network.
Link failure between nodes is detected as follows. If node S_N does not receive packets from its nearest neighbors, whose probability level is less than threshold within predetermined time interval then it assumes that link from those nodes to node S_N are failed. Packet error rate can be used to monitor the network health and help debug potential problems. If errors do occur a pattern can be identified. This can help isolate and solve problems before the system fails. Packet errors are node specific i.e., nodes only check their own packets and ignore all other. In case of error, the timestamp field in message is checked. If it is zero then it cause to reconstruct the network.

Theorem 1. Suppose N = (V, E) is a Bayesian Network. Algorithm has time complexity for fault tolerance as $O(\log_n)$ for routing in DSN.

Proof. Let N = (V, E) is a BN with Directed Acyclic Graph (DAG) having set of vertices or nodes V = $(v_1, v_2, \ldots v_n)$ and set of edges E = $(e_1, e_2 \ldots e_n)$. To associate with G and a given integer K >= 2 (number of neighboring nodes) is in the network. Phase one involves a simple construction of BN is given in Section 3.2. Phase two is a detection of faults in the network over an environment. The proposed work involves two phases such as self and active detection methods. The computation of fault tolerance is done by selecting S_1 as a source node, and then calculating probability for its neighbor nodes in presence of faulty nodes in the network. Next an optimization of routing in presence of faulty nodes, if presence of probability of node greater than threshold level is needed. Then calculate the probability of nodes (i.e. nodes or sink node/CMN) in each round is processed. Therefore, time complexity of fault tolerance is $O(\log_N)$ for optimization of routing in DSN.

3.7. Functioning Scheme

This section describes the algorithm for fault detection and recovery using BNs to find the optimal path for transmitting the packets. This work finds the joint and conditional neighbor nodes probabilities of selected source node. A prior probability is used in distinguishing the ways in which values for probabilities can be obtained. In particular, an "a prior probability" is derived purely by deductive reasoning. The joint probability distribution of the network is the joint probability of all variables or nodes in the network. Using the chain rule, this may be expressed as the product of the prior probabilities of all the root nodes and the conditional probabilities of all the network.

Algorithm for Fault Detection and Recovery

Nomenclature: {$S_N = S_1, S_2, S_3, \ldots S_N$, Prob_$S_N$ = Probability of sensor nodes, Th_b = Threshold level probability, L_{eff} = Link efficiency, $Th_{L_{eff}}$ = Threshold level link efficiency}.

Step 1. Node failure/Sink node failure
if (Prob_S_N < Th_b)
{
Send node to sleep mode and disconnect the links of that node.
- Reconstruct the network with Prob_S_N >= Th_b, (i.e., for considering each node should be higher than threshold level probability Th_b in the network).
- Select next highest probability of node in the network for routing.
- Repeat Step 1 // Fault recovery

}
Else
{
Transfer packet to next node over the network
} Repeat Step 1

Step 2. Link or Path failure
if (Prob_S_N < Th_b !! L_{eff} <= ThL_{eff})
{
Path or link failure
Select new neighbor node with highest probability
}
Else
{
Continue with the same node.
}

Step 3. Packet transmission failure
if (time stamp == 0)
{
Re-transmit the packet over the network
}

4. Simulation

The authors conducted simulation in various network scenarios of the proposed scheme by using C programming language. Simulations are carried out extensively with random number for 100 iterations. This section presents

the simulation model, procedure, performance parameters, and results.

4.1. Simulation Model

The simulation model consists of S_N number of nodes deployed in a distributed environment and connected as in BN. The performance parameters such as probability of fault tolerance, time complexity, energy optimization, network lifetime and fault detection ratio (FDR) is measured.

4.2. Simulation Procedure

To illustrate simulation results, the following variables have been considered: number of sensor nodes $S_N = 500$, energy of each nodes $E_N = 2$ J, number of sink nodes $N_s = 1$, number of control manager nodes CMN = 4, size of the network = $5000 \cdot 5000$ m, transmission range R_c = 100 m, energy required for sensing of data in each node $E_S = 50$ nJ/bit, energy required for transmission of data $E_T = 50$ nJ/bit, size_packets P = 64, 128, 512, 1024 bits and so on, threshold level probability $TH_b = 0.05\%$, and transmission of data = bits/s.

Begin

- Deploy the number of nodes randomly as in DSN environment.
- Divide the network into number of regions.
- Construct the BN in each region.
- Find the fault node on the basis of threshold level probability of each node.
- Find the link failures (node failure).
- Find the packet error (node error).
- Apply the proposed scheme to control network in DSN.
- Compute the performance parameters.
- Generate graphs.

End

4.3. Performance parameters

The following performance parameters were used in proposed scheme:

- probability of fault tolerance – it measures the ability of system to continue to operate properly in the event of failure in DSN environment;
- time complexity for fault tolerance – it is defined as the number nodes increases as the percentage of time complexity is increases for the fault tolerance in the network;
- network lifetime – as the probability of fault tolerance increases the network lifetime of DSN increases. The network lifetime is measured in terms of percentage;
- energy optimization – it is defined as the increase the probability of fault tolerance as the increase the optimization of energy of nodes in the network;
- Fault Detection Ratio – it is defined as the number of nodes increases the probability of fault detection ratio increases in the network.

4.4. Results and Discussions

Figure 5 shows that as the probability of Fault Detection Ratio (FDR) increases in the network, the probability of fault tolerance of the network decreases. The probability of FDR as 10%, and 20% for the total number of nodes ranging from 100 to 500 was considered. As the probability of FDR increases i.e., from 10% to 20% for 100 nodes, the probability of fault tolerance decreases with the number of neighboring nodes (K >= 2) on the network. The probability of fault tolerance of the proposed BN is more than the other network in the environment.

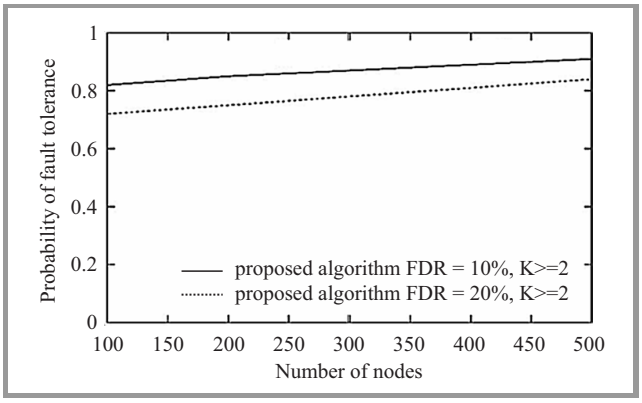

Fig. 5. Probability of fault tolerance vs. number of nodes.

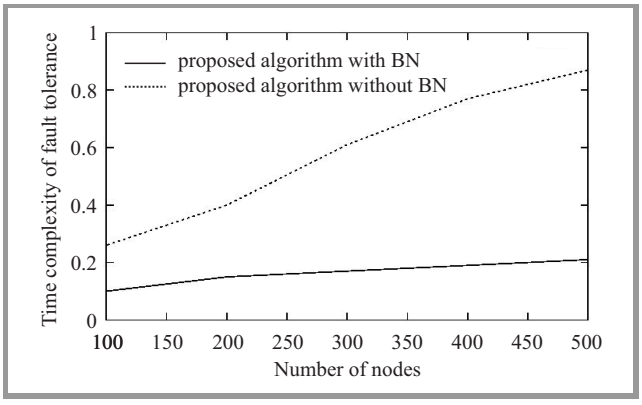

Fig. 6. Time complexity of fault tolerance vs. number of nodes.

Figure 6 depicts the time complexity for fault tolerance with given number of nodes in DSN. As the number of nodes increases, fault tolerance complexity increases. With proposed BN, time complexity of fault tolerance of DSN will be less than the case without BN. This work, we have considered that time complexity proposed method for fault tolerance of DSN is $O(\log_N)$. The proposed BN is more

efficient other than the network. Because, fault detection can be achieved by two mechanisms: self (passive) and active detections are considered in this scheme.

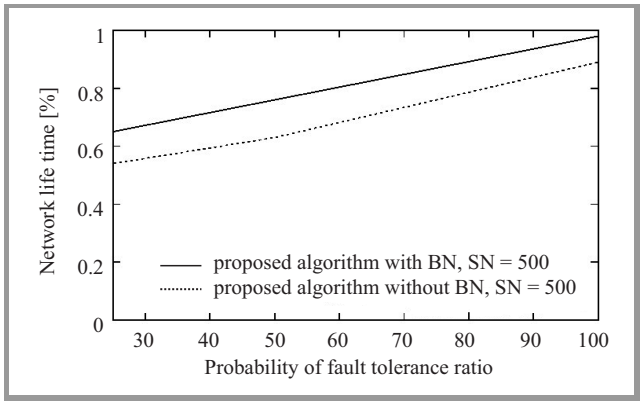

Fig. 7. Network lifetime vs. probability of fault tolerance.

Network lifetime with nodes given number is shown in Fig. 7. As the number of probability of fault tolerance of the network increases with given number of nodes ($S_N = 500$), the increase in the network lifetime of the DSN environment. The proposed algorithm (BN) is used to achieve better network lifetime with 98%.

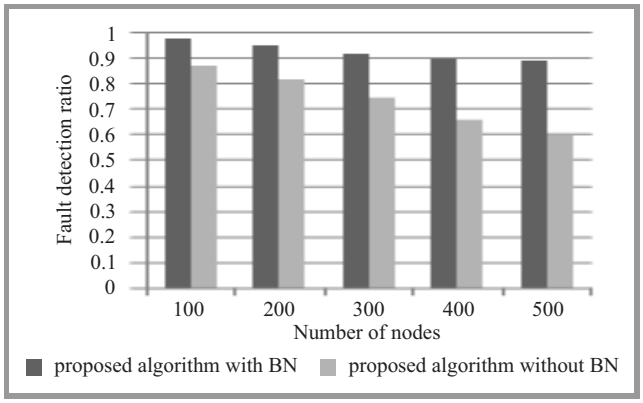

Fig. 8. Probability of FDR vs. number of nodes.

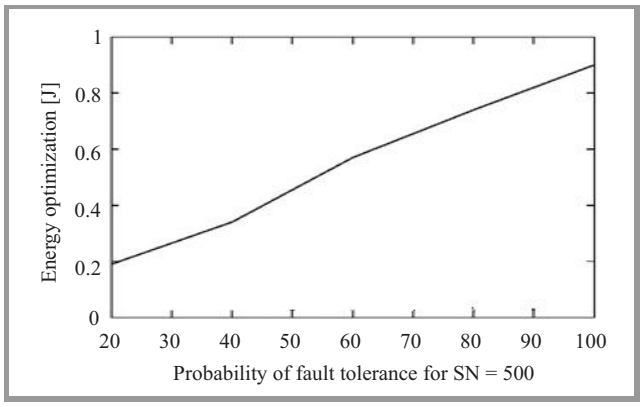

Fig. 9. Energy optimization vs. probability of fault tolerance.

Figure 8 shows probability of fault detection ratio (FDR) with given number of nodes. As the number of nodes increases, the probability of FDR decrease. The proposed method detects the fault detection in the network will be more in the network. Because proposed algorithm, works on the basis of proposed detection methods. As the size of the network increases, gradually probability of FDR decreases in the DSN. The size of the network is small, so probability of FDR is more. Otherwise probability of FDR is gradually decreases.

Figure 9 presents the energy optimization for varying number of fault tolerance among nodes. As the number of percentage of fault tolerance increases, optimization of energy of each node increases in the distributed sensor environment.

5. Conclusions

The proposed BN based fault tolerance mechanism is energy-efficient and responsive to network in DSN environment. It includes faults at node/sink, level and network level. The proposed system detects energy depletion of a node, link failure between nodes and packet error using their probabilities of nodes in the network.

Simulation results show that proposed system is more efficient than the other network. The proposed system continues to operate properly in the event of failure in DSN using BNs.

References

[1] S. S. Iyengar, T. Ankit, and R. R. Brooks, "An overview", in *Distributed Sensors Network*", S. S. Iyengar and R. R. Brooks, Eds. Chapman & Hall/CRC, 2004.

[2] B. B. Lokesh and N. Nalini, "Energy aware based fault tolerance approach for topology control in distributed sensor networks", *Int. J. High Speed Netw.*, vol. 18, no. 3, pp. 197–210, 2012.

[3] I. Ben-Gal, "Bayesian networks", in *Encyclopedia of Statistics in Quality and Reliability*, F. Ruggeri, R. Kenett, and F. Faltin, Eds. Wiley, 2007.

[4] R. E. Neapolitan, *Learning Bayesian Networks* [Online]. Available: http://www.cs.technion.ac.il/~dang/books/Learning%20Bayesian%20Networks

[5] I. Saha, L. K. Sambasivan, R. K. Patro, and S. K. Ghosh, "Distributed fault-tolerant topology control in static and mobile wireless sensor networks", in *Proc. 2nd Int. Conf. Commun. Syst. Softw. Middlew. COMSWARE 2007*, Bangalore, India, 2007, pp. 1–8.

[6] J. Liu and L. Baochun, "Distributed topology control in wireless sensor networks with asymmetric links", in *Proc. IEEE Global Telecommun. Conf. GLOBECOM 2003*, San Francisco, CA, USA, 2003, vol. 3, pp. 1257–1262.

[7] R. Arroyo-Valles, A. G. Marques, J. J. Vinagre-Diaz, and J. Cid-Sueiro, "A Bayesian decision model for intelligent routing in sensor networks", in *Proc. 3rd Int. Symp. Wirel. Commun. Syst. ISWCS 2006*, Valencia, Spain, 2006, pp. 103–107.

[8] P. Lilia and H. Qi, "A survey of fault management in wireless sensor networks", *J. Netw. Syst. Managem.*, vol. 15, no. 2, pp. 171–190, 2007.

[9] C. Mihaela, Y. Shuhui, and W. Jie, "Fault-tolerant topology control for heterogeneous wireless sensor networks", in *Proc. IEEE 4th Int. Conf. Mob. Adhoc and Sensor Sys. MASS 2007*, Pisa, Italy, 2007, pp. 1–9.

[10] K. Bhaskar and I. Sitharama, "Distributed Bayesian algorithms for fault-tolerant event region detection in wireless sensor networks", *IEEE Trans. Comp*., vol. 53, no. 3, pp. 241–250, 2004.

[11] M. Mohammad, C. Subhash, and A. Rami, "Bayesian fusion algorithm for inferring trust in wireless sensor networks", *J. of Netw.*, vol. 5, no. 7, pp. 815–822, 2010.

[12] C. Mihaela, Y. Shuhui, and W. Jie, "Algorithms for fault-tolerant topology control for heterogeneous wireless sensor networks", *IEEE Trans. Parall. Distrib. Syst.*, vol. 19, no. 4, pp. 545–558, 2008.

[13] N. Ababneh, A. Viglas, H. Labiod, and N. Boukhatem, "ECTC: Energy efficient topology control algorithm for wireless sensor networks", in *Proc. 10th IEEE Int. Symp. World of Wirel., Mob. Multim. Netw. & Workshops WOWMOM 2009*, Kos Island, Greece, 2009.

[14] A. Abolfazl, D. Arash, K. Ahmad, and B. Neda, "Fault detection and recovery in wireless sensor network using clustering", *Int. J. Wirel. & Mob. Netw*., vol. 3, no. 1, pp. 130–138, 2011.

[15] H. Xiaofeng, C. Xiang, L. L. Errol, and S. Chien-Chung, Fault-tolerant relay node placement in heterogeneous wireless sensor networks", *IEEE Trans. Mob. Comput.*, vol. 9, no. 5, pp. 643–656, 2010.

[16] J. L. Bredin, E. D. Demaine, M. T. Hajiaghayi, and D. Rus, "Deploying sensor networks with guaranteed fault tolerance", *IEEE/ACM Trans. Netw.*, vol. 18, no. 1, pp. 216–228, 2010.

[17] R. H. Abedi, S. Ghani, and S. Haider, "Selection of cluster heads in wireless sensor networks using bayesian network", in *Proc. Int. Conf. Comp., Electr. Sys. Sci., and Engin. ICCESSE 2010*, Venice, Italy, 2010.

[18] S. Nishant and S. Upinderpal, "A location based approach to prevent wormhole attack in wireless sensor networks", *Int. J. Adv. Res. Comp. Sci. Softw. Engin*., vol. 4, no. 1, pp. 840–845, 2014.

[19] H. Taub and D. L. Schilling, *Principles of Communication Systems*. Columbus, OH, USA: McGraw-Hill, 1986.

[20] G. Miao, N. Himayat, abd G. Y. Li, "Energy efficient link adaptation in frequency-selective channels", *IEEE Trans. Commun.*, vol. 58, no. 2, pp. 545–554, 2010.

B. Bhajantri Lokesh received his M.Tech. degree in Computer Science and Engineering (CSE) from Basaveshwar Engineering College, Bagalkot, India, in 2005. He is working as a Assistant Professor in the Department of Information Science and Engineering, Basaveshwar Engineering College, Bagalkot, India. Currently he is pursuing Ph.D. in CSE, Visvesvaraya Technological University (VTU), Belgaum, Karnataka, India. He has experience of around 10 years in teaching and research. His areas of interest include Distributed Sensor Networks, e-Commerce, u-Commerce, mobile computing and communications, networking protocols, genetic algorithms, applications of agents and real time systems. He has published one book chapter in Handbook of Research on Telecommunications Planning and Management for Business, 8 referred international conferences papers and 7 referred international journals. He is a reviewer of some journals and conferences. He is a member of Board of Studies (BOS) in the Department of Information Science and Engineering, Basaveshwar Engineering College, Bagalkot, Karnataka, India. He is a member of International Association of Computer Science and Information Technology (IACSIT).

E-mail: lokeshcse@yahoo.co.in
Department of Information Science and Engineering
Basaveshwar Engineering College
Bagalkot, India

N. Nalini received her Ph.D. from Visvesvaraya Technological University (VTU), Belgaum, Karnataka, India. She is currently working as Professor and Head of Department of Computer Science and Engineering, Nitte Meenakshi Institute of Technology (NMIT), Bangalore, Karnataka, India. She has experience of around 22 years in teaching and research. She is involved in research of wireless and Distributed Sensor Networks, cloud computing, Cryptography & Network Security, Genetic Algorithms, and Heuristic Algorithms in Secure Networks. She is an associate editor of Research Journal of Information Technology, Maxwell Scientific Organization. She has many given invited lectures and has conducted several seminars and conferences. She has published 30 in journals and about 50 conferences papers. She is a reviewer of many journals and conferences.

E-mail: nalinaniranjan@hotmail.com
Department of Computer Science and Engineering
Nitte Meenakshi Institute of Technology (NMIT)
Bangalore, Karnataka, India