Reliability Modeling of Context Aware Wireless Sensor Network

Latha Venkatesan , Chandrasekaran Subramaniam, and Shanmugavel S.

***Abstract*—The objective of the paper is to propose a reliability model for a fault tolerant wireless sensor network using context awareness feature in order to evaluate network reliability by modeling in PI Calculus. The earlier Propositional Directed Acyclic Graph (PDAG) approach leads to an identification of a suitable structure function in polynomial time to evaluate the reliability of wireless Sensor Network (WSN). In that approach, the nodes and links of the network are assumed as context free, makes the determination of the reliability function complex if the number of nodes is increased. The context awareness of the nodes and links are used to decompose and reduce the structure function for that network of any topology. The proposed context aware structure function algorithm helps not only to determine the structure function but also decide the most reliable path from source to terminal without affecting the network performance and accurately determines the reliability in the case of node and link failures.**

***Index Terms*—Acyclic graph, context awareness, fault tolerance, network reliability, stochastic PI calculus**

I. Introduction

The technology improvement in wireless communication and integrating devices have enabled the development of low cost, small size and low power sensor nodes with the abilities of sensing, computing and communication. A large number of sensor nodes are densely deployed in the working environment to form a wireless network and accomplishes the functions of monitoring, detection and tracking the movement of physical objects. Fault tolerance is a critical feature in such Wireless Sensor Network (WSN) because many end user applications require the low cost and low power sensor nodes to work in the uncontrolled environment. In such an environment, to keep the functionality of the WSN unaffected even with faults occurred in some of the sensor nodes or in the communication link between two sensor nodes. Generally fault tolerance is achieved through four phases like fault detection, fault diagnosis, fault isolation and fault recovery to fulfill the reliability requirements. The fault tolerance attribute enables the system to fulfill the reliability requirement and WSN is a large scale system where a high degree of reliability is crucial. A large number of researches have been carried in modeling and computing the network reliability which are based on graph theory, Markov model and fault tree analysis. But in that network reliability approach the vertices representing the nodes are assumed as perfectly reliable however the links are subjected to fail. In the Binary Decision Diagram approach, variable ordering with composition operations are introduced to reduce the given network for its reliability function. A generally faster algorithm known as Composition After Expansion (CAE) is proposed to substitute the given edge in the graph and the BDD technique is iteratively used to determine the network reliability through two strategies namely EE,CAE [1]. In the Three Universe Model for WSN addresses the security and reliability failures and proposes a framework in which Priority AND gates (PAND) and Functional DEPendency gates (FDEP) are used. In the above model, where the message driven approach is used to determine the WSN reliability with hierarchical layers of nodes and the probability of message arrival from sink to cluster head [2]. This approach may not be applicable in the case of short burst of data transmission between nodes and at the same time this does not give importance to the type or criticality of the message that is to be transmitted between the layers. In the distributed sensor network (DSN) approach, a fault tolerant clustering protocol is proposed with algorithms for calculating the reliability and the message delay in the collaborative environment. This model has assumed that a message from the sink to a target sensor node always takes the shortest path with multi-hops [3]. The performance of the WSN and the reliability of WSN are always in a trade-off that without compromising the performance, a network cannot be designed to have maximum reliability. And the sensor nodes assumed in the above model are simply forwarding the incoming messages with the same transmitting and receiving capacity. In other network reliability evaluation methods, Markov models are used for different types of sensors and spares when the sensors failed. The model addresses the pooled spares in the case of failure and the cost function associated with the activation of nodes [4]. The multimodal fusion sensor network does not exhibit any situation and time awareness features so that failure rate can be made dynamic instead of a static one. In the reduced ordered binary decision diagram (ROBDD), the common cause failures (CCF) are addressed [5] but the common cause events need not be mutually exclusive and the fault coverage under this assumption will not be a complete coverage. In the Constructed ordered binary decision diagram (COBDD) approach [6], the reliability evaluation time is reduced by the proposed algorithm without focusing on the reliability

Manuscript received May 13, 2012; revised June 26, 2012.

Latha Venkatesan is with the Electronics and Communication Engineering Department, Velammal Engineering College, Chennai, 600066 India (e-mail:lathavenkatesanpnag@gmail.com).

Chandrasekaran Subramanium was with the Computer Science and Engineering Department, Rajalakshmi Engineering College, Chennai, India. He is now with the Computer Science and Engineering Department, Kumaraguru College of Technology, Coimbatore, India (e-mail: chandrasekaran_s@msn.com).

Shanmugavel S. is with the Anna University, Chennai, India (e-mail: ssvel@annauniv.edu.in).

DOI: 10.7763/IJIEE.2012.V2.193

importance of each node or link with respect to the context of transmitted message or data over the network. In the PDAG approach, a generic structure function is formed in polynomial time using terminal selectors within the network to compute the WSN reliability [7]. In the earlier Sensor Context Aware Routing, a protocol was proposed for reliable delivery of data through context awareness about the neighborhood of the node [8]. The reliability prediction was totally based on the predictability of context which is dynamically varying by an additional component. A flexible context aware model of wireless sensor network was studied in logistic applications to enhance the communication efficiency [9] but the reliability assessment was not arrived for different node and link failures. The main focus of the paper is to address a reliability enhancement technique for wireless sensor network through tolerance of faults at the nodes as well as links and propose a reduction mechanism for reliability computation.

The paper is organized as follows: Section II introduces a fault model for WSN encompassing the criticality of the data and the node battery level with a mapping needed for the context awareness in any particular environment. Section III introduces stochastic PI modeling for the various sources of faults in clustered sensor nodes in different channels of communication. Section IV introduces a reliability modeling through a context aware structure function with the help of various context aware variables and identifies the reliable path and its reliability of WSN deployed for monitoring the health status of a building structure. Section V concludes with the advantage of this proposed technique in determining the WSN reliability in the case of node and link faults.

II. Fault Mapping of Wireless Sensor Network

A wireless sensor network may be designed and deployed as a fault tolerant network in the case of end user applications like weather monitoring, health monitoring of complex civil structures and even in monitoring the animals in wildlife preservation systems. The probability distribution of individual fault can be fixed based upon the application which is running on the top of the network. For example in the case of weather monitoring system, a multitude of data packets are to be streamed between the nodes in smaller time interval. This transmission can be completed with one or multiple hops. To get a reliable performance of the weather monitoring system using wireless sensor network, the hardware configurations like the memory capacity, the clock speed of the processor in each and every node and the battery are more susceptible to fault. In the case of query processing using the same WSN like wild life preservation system, the data rate will be low and the number of packets may be less but the correctness and the integrity of the data is important. In such case, the sensor and the driver software are of more important. So the reliability importance of the individual network elements depend upon the performance or quality attributes of the applications running on the network. In the case of security parameters of the applications, the secured communication protocol, access control to the network and the trust relation between the individual nodes are to be established for a reliable network. Thus the applications running in these systems need not only be reliable but also secured since the possibilities of faults and vulnerabilities of the network are high. Apart from the correctness of the data received in any part of the system, the communication protocol must be made efficient. The faults that may occur in the above systems may be broadly classified into reliability faults and security faults even though the two expected quality attributes can be separated fully or otherwise they are inter-twined. In the proposed work, the fault in wireless sensor network may be considered as a tuple consisting of an event which may be internal or external, the network environment, and the status of the objects in the network or network elements and a time factor.

The fault may be represented as <environment, event, object, time>.

For example, the unexpected conditions like earthquakes or flooding may be considered as a fault in the environment. A non specified function like buffering or processing the received data or the operating system events when carried out by the network elements, these events will be considered as event faults. The network elements like the nodes including the sensor, transceivers, memory or the links may be faulty at any point of time in its operational period.

The time sensitiveness or the time frame within which the data to be transmitted is also major factor in determining the behavior of the WSN. The fault tree of a WSN is a structured hierarchical AND, OR tree, which explores the possible entities and their failure nature which will cause the overall network or system failure. In order to improve the end to end packet delivery, the WSN elements have to do fault free functionalities not only against faults due to their hardware, power, driver software and misbehaving nodes but also their location importance and inter cluster communication synchronization faults. Even though the nodes are handling the same type of data, the time of sensing and transmission are the important values in the health status monitoring of buildings. Each data packet has to include extra information about their location and time. The various faults can be mapped to the different awareness features embedded into the cluster nodes as shown in Fig 1.

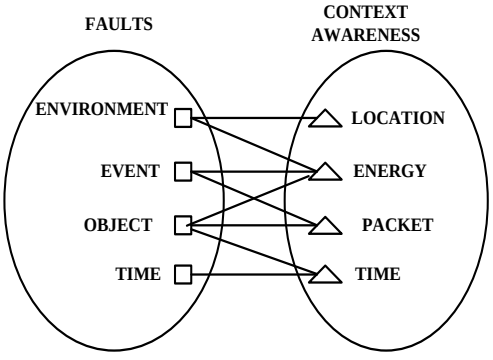


Fig. 1. Fault - context mapping in WSN

III. Stochastic PI Modeling

The faults in a wireless senor network may be due to the cluster of nodes and the links since the communication processes between cluster to cluster or between cluster to

node are basically stochastic in nature. All the nodes are connected in a cluster and all clusters are connected to the sink thereby the communication faults can be depicted through channel type faults where the cluster is of process nature. The WSN can be thought of a graph, G = (V, E) directed or undirected graph representing a network.

Let V be a set of sensor nodes and represented as $\{v_1, v_2, ...v_n\}$ connected by a set of edges given by E = $\{e_1, e_2,...e_n\}$. The network is composed of clusters among which some clusters are composed of nodes handling critical data and others are handling ordinary data as far as the health information is considered.

Let V_c be a set of nodes $\{v_1, v_2, ...v_n\}$ having context awareness for their energy at that instant of time, where V_c is a subset of V and similarly let E_c be the set of edges having awareness of criticality of packets they forward and represented as $\{e_1, e_2,...e_n\}$. Let s ϵ V be a source node and t ϵ V be a terminal node, the context awareness can be considered as a four tuple as shown below:

$c_i = <p_i, t_i, l_i, e_i>$, a tuple representing contexts.

The packet format is so designed to incorporate the parameters like node_ id, cluster_ id, number of nodes in that cluster, criticality of the packet, time awareness bit, parity bit and the data value from the sensor. Since all nodes are forwarding information in a concurrent manner, the synchronization faults and the inter cluster communication can be calculated with the help of PI calculus. The formal modeling of a fault tolerant WSN can be specified using Stochastic PI calculus. In the formal specification and modeling given below, the stochastic nature of the WSN is described based on the redundant nodes in the data cluster and critical data clusters. The stochastic pi calculus notation is used to represent the channels and state change of the cluster in establishing communication with the nodes as well as sink.

Stochastic PI Calculus Modeling of Fault Tolerant WSN:::
Variables;
Conditions:
α → 3 out of 5 nodes work
e→ packet sent from cluster CDC1
f → packet sent from cluster CDC2
g →data sent between nodes
Declarations:
CDC1 = {*n1, n2, n3, n4*}
CDC2 = {*m1, m2, m3, m4*}
DC1 = {*p1, p2, p3, p4*}
DC2 = {*q1, q2, q3, q4*}
x and y are channels bn() and fn() represent a set of bound and free names respectively.
Packet = {Node id, Cluster id, No_of nodes_cluster, Criticality_of_packet, Time_awareness_bit, Energy awareness bit, Sensor data, Parity}

$CDC1 \xrightarrow{\alpha} CDC1`_{active}$
// Cluster CDC1 becomes active only when at least 3 out of 5 nodes are active //
// Node Fault Tolerance//

$CDC2 \xrightarrow{\alpha} CDC2`_{active}$
// Cluster CDC2 becomes active only when at least 3 out of 5 nodes are active //
//Node Fault Tolerance//

$CDC1`_{active} \xrightarrow{!x(e)} CDC1`` \; S \xrightarrow{?x(e)} S` => CDC1`_{active}$
$| S \xrightarrow{x} CDC1`` | S`$
// Cluster $CDC1`_{active}$ becomes CDC1`` on sending packet "e" via channel "x" to sink S which becomes S`

$CDC2`_{active} \xrightarrow{!y(f)} CDC2`` \; S` \xrightarrow{?y(f)} S`` => CDC2`_{active}$
$S` \xrightarrow{y} CDC2`` | S``$ //Cluster $CDC2`_{active}$ becomes CDC2`` on sending packet "f" via channel " y" to sink S` which becomes S``

$E |-- n_i \xrightarrow{fault} E |-- n_{i\ idle}$
// In environment E a node n_i when faulty becomes $n_{i\ idle}$ in CDC1 //

$E |-- m_i \xrightarrow{fault} E |-- m_{i\ idle}$
// In environment E a node m_i when faulty becomes $m_{i\ idle}$ in CDC2//

$E |-- p_i \xrightarrow{fault} E |-- p_{i\ idle}$
// In environment E a node p_i when faulty becomes $p_{i\ idle}$ //

$E |-- q_i \xrightarrow{fault} E |-- q_{i\ idle}$
// In environment E a node q_i when faulty becomes $q_{i\ idle}$ where i={1,2,3,4}//

$bn(\alpha) \cap fn(DC2) = NULL \quad DC1 \xrightarrow{\alpha} DC1` => DC1$
$| DC2 \xrightarrow{\alpha} DC1` | DC2$ // Only DC1 is active //

$bn(\alpha) \cap fn(DC1) = NULL \quad DC2 \xrightarrow{\alpha} DC2` => DC1|$
$| DC2 \xrightarrow{\alpha} DC1 | DC2`$ // Only DC2 is active //.

$X_i \xrightarrow{z(g)} X_k$ //where $i \neq k$; $i, k \in \{1, 2, 3, 4\}$;
$X \in \{m, n, p, q\}$ //

A propositional directed acyclic graph (PDAG) of WSN can be formed and decomposed into sub graphs and these sub graphs are evaluated in order to determine the overall reliability. If large number of nodes is connected in WSN, then the reliability evaluation technique should not be affected in terms of time complexity.

IV. Reliability Modeling of WSN

A WSN may be considered as a structure where any number of nodes is normally connected by different paths making the structure intrinsically reliable. Using a polynomial time algorithm, the reliability of the WSN can be determined through acyclic directed graph techniques. The WSN applicable for weather forecasting, huge structure health monitoring or wild life preservation system involves the packet transmission in a more directed way rather than a bi-directional one. The network can be well represented by a propositional directed acyclic graph (PDAG) through which the reliability can be evaluated. By convention leaf nodes are represented by □ and labelled with T (True), ⊥ (False) or xϵ

V and non leaf nodes are represented by Δ(Logical AND), Δ(Logical OR), ◊(Logical NOT). The set of all PPDAGS with respect to V constitutes a language which is denoted by $PDAG_v$.

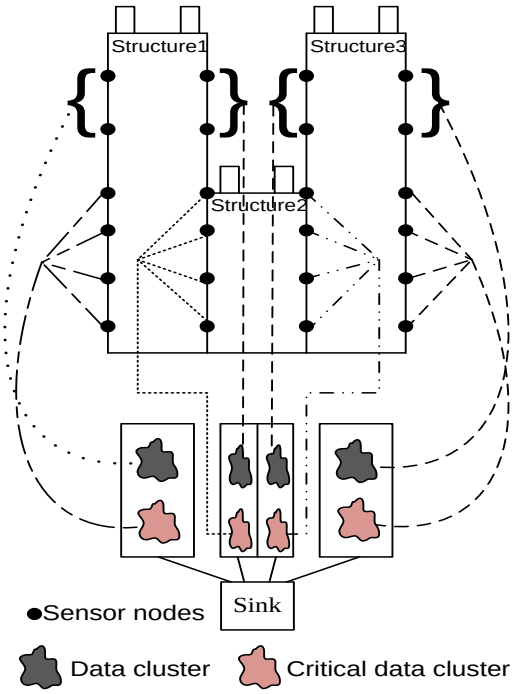
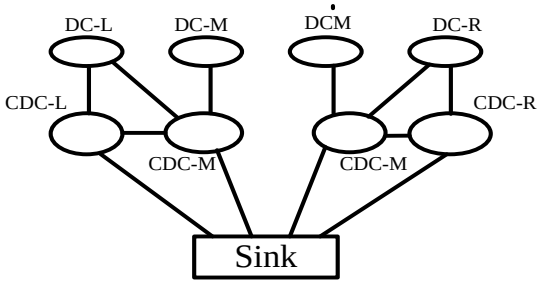


Fig. 2. WSN for structure health monitoring



DC-L =Data Cluster Left DC-M= Data Cluster Middle
DC-R = Data Cluster Right CDC= Critical Data Cluster

Fig. 3. Cluster nodes representation of WSN

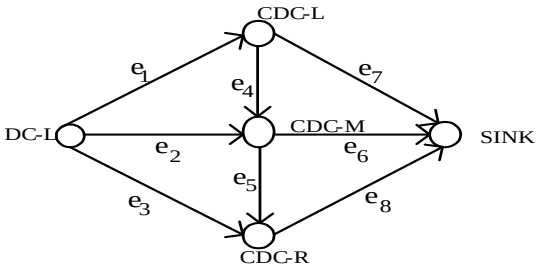


Fig. 4. Sample wireless sensor network

The above structure health monitoring system can be realized as a network to monitor the health status of the entire building. A number of homogeneous sensor nodes form a wireless sensor network as shown in Fig.2. The entire building structure is made up of three wings, the left and the right wings have more stories when compared with that of the middle wing or portion. The placed sensor nodes are so connected such that the information from the fire, temperature and crack sensors are to be read and they transmit the information as and when demanded. The queries are directed from the sink and so the nodes will reply by forwarding the essential information in a periodic or non periodic manner. The network may be connected to the outside world through a number of web services and gateway. The data collected from different nodes are treated in different clusters since some of the nodes especially the nodes in the bottom part of the structure are declared as critical nodes in that critical data cluster. The various data cluster and critical data cluster nodes and their association is shown in Fig 3. The reliability analysis of the mentioned WSN can be performed by considering the entire network as of four individual sub networks. The subnets for the two extreme left and right side of the structure may be considered as parallel networks and they are of the same topology. The middle section can also be considered as a parallel combination of another two subnets for left and right side of the middle wing portion.

Computationally, there are four subnets in which two are mirror replica representing the two sides of the entire structure and the other two subnets are replica of each other representing the middle wing. The reliability of the individual WSN can be evaluated to determine the overall network reliability.

$$\begin{aligned} \text{Reliability(WSN)} = {} & \text{Reliability of WSN(left)} * \\ & \text{Reliability of WSN(right)} * \\ & \text{Reliability of WSN(middle\_left)} * \\ & \text{Reliability of WSN(middle\_right)} \end{aligned} \quad (1)$$

Reliability analysis of a WSN can be done by considering not only the nodes and edges of the network but also the criticality of the data they handle. Each and every network elements have to operate in different contexts so that the reliability at that particular context will be of more importance than that of the network in different contexts. There may be many contexts like information criticality context, location context and timing context. To represent these features for the reliability analysis, corresponding variables may be introduced as context awareness variables at the sensor nodes or at the edges representing the links. The context awareness variable may also be introduced for the battery level at the node representing the energy awareness feature.

The reliability of any WSN is the probability that there exits at least one path from the sink node to one or more sensor nodes denoted by Edge(k) and corresponding reliability can be represented as Reliability(t, k). In order to determine the reliability of WSN starts with finding a generic function representing the snapshot of the network and applying the context awareness features at the nodes and links in appropriate places as mentioned in three steps below:

Step1: Generalization for Structure Function (GSF)

The above WSN can be represented as a directed acyclic graph as shown in Fig 4. The connectivity information of the network is given in matrix (a). The network can be reduced by eliminating the cluster nodes with the largest distance from the source in the network first (LDF) and the elimination continues till all the cluster nodes except the

source node. In the assumed network, cluster nodes DC-L is considered as source node and sink is the terminal node. The edges representing the inter cluster communication links are e_1, e_2, e_3. It has been assumed that all clusters and edges are not having context awareness features and therefore having a high complexity in estimating the reliability of the network.

The structure function can be determined by considering the clusters as nodes in the diagram and based on the LDF technique it is reduced according to the presence of connection between the clusters. The matrices are derived by iteratively applying the LDF and the truth values of the connectivity that are shown in the matrices c, d and e.

The structure function can be determined by considering the clusters as nodes in the diagram and based on the LDF technique it is reduced according to the presence of connection between the clusters. The matrices are derived by iteratively applying the LDF and the truth values of the connectivity that are shown in the matrices c, d, and e.

Step2: Context Aware Reliability Computation

$$\begin{bmatrix} \alpha_A & e_1 & e_2 & e_3 & F \\ F & \alpha_B & e_4 & F & e_7 \\ F & F & \alpha_C & e_5 & e_6 \\ F & F & F & \alpha_D & e_8 \\ F & F & F & & \alpha_E \end{bmatrix}$$

Matrix (a)

$$\begin{bmatrix} \alpha_A & e_1 & e_2 & e_3 \\ F & \alpha_B \vee e_7 \wedge \alpha_E & e_4 & F \\ F & F & \alpha_C \vee e_6 \wedge \alpha_E & e_5 \\ F & F & F & \alpha_D \vee e_8 \wedge \alpha_E \end{bmatrix}$$

Matrix (b)

$$\begin{bmatrix} \alpha_A \vee (e_3 \wedge (\alpha_D \vee (e_8 \wedge \alpha_E))) & e_1 & e_2 \\ F & \alpha_B \vee (e_7 \wedge \alpha_E) & e_4 \\ F & F & (\alpha_C \vee e_6 \wedge \alpha_E) \vee (e_5 \wedge (\alpha_D \vee (e_8 \wedge \alpha_E))) \end{bmatrix}$$

Matrix (c)

$$\begin{bmatrix} \{\alpha_A \vee (e_3 \wedge (\alpha_D \vee (e_8 \wedge \alpha_E))) \vee \} & e_1 \\ [(e_2 \wedge (\alpha_C \vee (e_6 \wedge \alpha_E)) \vee (\alpha_C \vee e_6 \wedge \alpha_E \vee (e_5 \wedge (\alpha_D) \vee \} (e_8 \wedge \alpha_E))] & \\ F & \{(\alpha_B \vee (e_7 \wedge \alpha_E)) \vee e_4 \wedge (\alpha_C \vee e_6 \wedge \alpha_E) \vee \\ & (e_5 \wedge (\alpha_D \vee (e_8 \wedge \alpha_E)))\} \end{bmatrix}$$

Matrix (d)

$$\begin{bmatrix} \{\alpha_A \vee (e_3 \wedge (\alpha_D \vee (e_8 \wedge \alpha_E))) \vee \\ ((e_2 \wedge (\alpha_C \vee (e_6 \wedge \alpha_E)) \vee (\alpha_C \vee e_6 \wedge \alpha_E \vee (e_5 \wedge (\alpha_D) \vee \} (e_8 \wedge \alpha_E)))\} \vee \\ \{e_1 \wedge (\alpha_B \vee (e_7 \wedge \alpha_E)) \vee e_4 \wedge (\alpha_C \vee e_6 \wedge \alpha_E) \vee (e_5 \wedge (\alpha_D \vee (e_8 \wedge \alpha_E)))\}] \end{bmatrix}$$

Matrix (e)

The complex network structure function given in matrix (e) can be reduced by introducing the context sensitive information of sensor network. The context of a wireless sensor network may be expressed in terms of the network elements or the conditions in which the sensor nodes are deployed. For example, the packet awareness is represented in binary as '00' whereas the location awareness can be represented as '10' and similarly the other features can also be represented as two bit format. The Context Aware Byte (CAB) can be formed as a string of eight bits in which the fist two represents the packet awareness; the next two bits represent the time awareness. The remaining two sets, each of two bits correspond to location and energy awareness respectively. In a sample case, if the CAB string is "00 10 01 00", it indicates the nodes and the network elements that the incoming current packet is of less critical as far as the domain application is considered since the first two bits are "00". The WSN gets an indication from this CAB as the time delay for the current packet is to be within the system transmission delay since the third and the fourth bits are "10". The context features are transformed and transcribed into the network through the additional packets in the form of CABs. The nodes and edges are assumed True (T) or False (F) based on their context awareness. For example α_B of CDC-L and e_6 are assumed to be "false" and replaced by F in the connectivity matrix (a). Then the complexity of the generic structure function is reduced and is given below:

$$[\alpha A \vee (e3 \wedge (\alpha D? (e8 \wedge \alpha E)))] \vee [(e2 \wedge (\alpha C \vee (e5 \wedge (\alpha D \vee (e8 \wedge \alpha E)))] \quad (2)$$

The pseudo code for the step 1 & step 2 are as follows:

```
con_ aware_struct_function ::
  begin
   {
    // Declaration of Context Awareness//
    boolean values:  packet_aware,  time_aware
    let n = dimension(N) // the number of elements
                              in network matrix//
     while n >1 do
     {
     for i from 1 to n-1 do
         // check nodes for context variable//
         if energy_aware =00 AND  location_aware =00
           then replace  λ(i, i) by false
     for  i = 1 to n-1
     for  j=1 to n-1 do
         // check edges for context variables //
     for all  i≠ j,
         if packet_aware = 00  AND  time_aware = 00
            then replace  λ(i, j) by false }
// structure function generation//
     for  i = 1 to n-1 do // eliminate node v_n at the
                     largest distance from source//
         if λ(i,n) ≠ false
            then  replace  λ(i,i) by( λ(i,i) ∨ λ(i,n) ∧ λ(n,n))
     for j = 1 to n-1 do // eliminate the node with
                              outgoing link//
         if  i ≠ j AND λ(n,j) ≠ false
            then replace  λ(i,j) by (λ(i,j) ∨ λ(i,n) ∧ λ(n,j))
      end all }
     n = n-1
    end
   }
  return λ(1,1)
end
```

Step3: Context aware reliability computation

The computation of network reliability for the reduced context aware structure function is obtained by assigning the probabilities of connectivity to the nodes and the edges. Equation (2) is constructed using logical connectors ∨ (OR) and ∧ (AND) to obtain min path $[\alpha_A \vee (e_3 \wedge (\alpha_D \vee (e_8 \wedge \alpha_E)))]$ and numbered 1, $[(e_2 \wedge (\alpha_C \vee (e_5 \wedge (\alpha_D \vee (e_8 \wedge \alpha_E))))]$ is

numbered 2 for connectivity between DC-L and sink. From (2), it is found that the

Reliability important cluster Nodes [α_A, α_D, α_E, α_C] and Reliability important Edges= Edges (k) = [e_3, e_8, e_2, e_5].

The min paths are connected by logical operator $\vee$ and the reliability of the WS network is the reliability of that min path which has the maximum reliability out of many min paths. Reliability of $WSN_{(Left)}$ = {Max(Reliability of Min path) | Min path > =1} and hence it can be written as

Reliability(t, k) = Reliability(t, min path).

For verification purposes, if the probability of connectivity of WSN cluster nodes and links are assumed arbitrarily as

$p(\alpha_A) = 0.5$, $p(\alpha_D) = 0.6$, $p(\alpha_E) = 0.5$, $p(\alpha_C) = 0.6$, $p(e_2) = 0.4$, $p(e_3) = 0.3$, $p(e_5) = 0.5$, $p(e_6) = 0.2$, $p(e_8) = 0.4$,

then the reliability of the min path 1 is

$$(\alpha_A \vee (e_3 \wedge (\alpha_D \vee (e_8 \wedge \alpha_E))))$$
$$= (0.5 + (0.3 *(0.6 + (0.4 * 0.5))) = 0.74.$$

The reliability of the min path 2 is

$$(e_2 \wedge (\alpha_C \vee (e_5 \wedge (\alpha_D \vee (e_8 \wedge \alpha_E)))))$$
$$= (0.4 * (0.6 + (0.5 * (0.6 + (0.4 * 0.6))))) = 0.4$$

Reliability of WSN_{Left} = Max (0.7,0.4) = 0.7

Similarly the reliability of middle structure and right sided structure can also be calculated and the reliability of the WSN can be determined using (1).

V. Conclusion

The reliability of a fault tolerant wireless sensor network can be determined using the proposed technique using the context awareness feature embedded into the nodes and edges. The formal specification of WSN using Stochastic PI calculus helps to arrive at the reliability modeling in simple steps even if the nodes are more in number. The min paths are identified to know the most reliable path between the node and the sink with the help of the acyclic graph theory. The technique is suitable for application specific WSN but with additional overhead in terms of software to identify the appropriate contexts at each point of communication. The technique can be extended for similar network where continuous monitoring like weather forecasting with additional modifications in the algorithm. The future work focuses on the design and development of fault identification in the individual and the cluster node level so as to minimize the network fault recovery time.

References

[1] S. Y Kuo, F. M. Yeh, and H. Y. Lin, "Efficient and exact reliability evaluation for networks with imperfect vertices," *IEEE Trans. Reliability*, vol. 56, no.2, pp. 288-300, June 2007.

[2] S. L. X. and H. E. Michel, "Integrated modeling for wireless sensor networks reliability and security," in *Proc. Reliability and Maintainability Symposium*, Jan 2006, pp. 594-600.

[3] H. M. F. AboElFotoh, S. S. Iyengar, and K. Chakrabarty, "Computing reliability and message delay for cooperative wireless distributed sensor networks subject to random failures," *IEEE Trans. Reliability*, vol. 54, no. 1, pp. 145 – 155, March 2005.

[4] D. Bein, V. Jolly, B. Kumar, and S. Latifi, "Reliability modeling in wireless sensor networks, *Int. J. Information Technology*, vol. 11, no. 2, pp. 1-8, 2005.

[5] A. Shrestha, L. Xing, and H. Liu, "Infrastructure communication reliability of wireless sensor networks," in *Proc. 2nd IEEE Int. Symp. Dependable, Autonomic and Secure Computing*, Oct 2006, pp. 250 – 257.

[6] Y. Xiao, X. LI, and Y. LI, "Evaluate reliability of wireless sensor networks with OBDD," in *Proc. Int. Conf. Communications*, pp. 1 – 5, 2009.

[7] J. Jonczy and R. Haennii, "Network Reliability Evaluation with Propositional Directed Acyclic Graphs," in *Advances in Mathematical Modelling for Reliability*, 1st ed. vol. 0.

[8] T. Bedford, J. Quigley, L. Walls, B. Alkali, A. Daneshkhah, and G. Hardman, Ed. USA: IOS Press, May 2008, pp. 25-31.

[9] C. Mascolo and M. Musolesi, "SCAR: Context-aware Routing in Delay Tolerent Mobile Sensor Networks," in *Proc. Int. Conf. Wireless Communications and Mobile Computing*, July 2006, pp. 1337- 1343.

[10] V. Q. Son, B. L. Wenning, A. T. Giel, and C. Görg, "A Model of Wireless Sensor Networks using Context-Awareness in Logistic Applications," in *Proc. 9th Int. Conf. Intelligent Transport System Telecommunications*, 2009, pp. 2-7.

Latha Venkatesan is currently a PhD candidate at Anna University in Chennai, India. She received the B.Eng degree from Madurai Kamaraj University in Madurai, India. She held a full time position as a Professor in Velammal Engineering College affiliated to Anna University, Chennai and pursuing her PhD degree in Information and Communication Engineering. Her research interests include fault tolerant wireless sensor network, reliability modelling and sensor data fusion.

Chandrasekaran Subranamiam is currently working as Professor in the department of Computer Science and Engineering of Kumaraguru College of Technology, Coimbatore, INDIA. He was awarded M.E.,in computer science and engineering and Ph.D degree in the area of Reliability Enhancement of Hybrid Fault Tolerant System by Anna University, Chennai, INDIA. He is an active researcher in the area of context aware computing, Reliability techniques in embedded systems and privacy assurance techniques. He is a member of IEEE, ACM, IET, SEI, WSEAS and ASQ. He published more than 60 papers in reputed International conferences and journals. He is at the age of 54 and have been acting as member in many international program committees of various conferences and acting as a chair cum reviewer in many journals and workshops.

Shanmugavel S. graduated from Madras Institute of Technology in Electronics and Communication Engineering in 1978. He obtained his Ph.D degree in the area of Coded Communication and Spread Spectrum Techniques from India Institute of Technology, Kharagpur, INDIA. At present he is working as Professor at Department of Electronics and Communication Engineering at Anna University, Chennai. He has published more than 95 research papers in the National and International Conferences and 35 research papers in Journals in the area of Mobile Ad hoc Networks, ATM Networks, Spread Spectrum Communication and Error Control Coding. His current areas of research interest are Mobile Ad Hoc Networks, Cellular IP Networks, Broadband ATM networks and CDMA Engineering and Digital Communication. He received IETE-CDIL Award in 2000 for the Best Paper Published in IETE Technical Review and IETE-SK Mitra Memorial award in 2006 for the Best Paper Published in IETE Journal of Research.