Stochastic Fault Trees for cross-layer power management of WSN monitoring systems

L. Carnevali, L. Ridi, E. Vicario
Dipartimento di Sistemi e Informatica - Università di Firenze
{carnevali, ridi, vicario}@dsi.unifi.it

Abstract

Critical systems require supervising infrastructures to keep their unreliability under control. We propose safety-critical systems to be modeled through a fault-tolerant architecture based on Stochastic Fault Trees (SFTs) and we refer to a scenario where the monitoring infrastructure is a Wireless Sensor Network (WSN). SFTs associate the failure time of leaf events with a non-Markovian (GEN) cumulative distribution function (CDF) and support the evaluation of system unreliability over time. In the reference scenario, the SFT model dynamically updates system unreliability according to samples delivered by the WSN, it maintains a dynamic measure of the safe time-horizon within which the system is expected to operate under a given threshold of unreliability, and it also provides the WSN with a measure of the contribution of each basic event to system unreliability.

1. Introduction

A *Wireless Sensor Network* (WSN) is constituted by battery-powered computing nodes, which integrate information acquisition and transfer capabilities and organize themselves in ad-hoc networks through wireless connections [7]. This enables development of monitoring utilities in operational scenarios that cannot be afforded through more conventional monitoring technologies. However, these characteristics also determine strict limits over energy resources and computation and communication power, and make the network subject to faults and diffuse unavailability.

This comprises a major hurdle in the realization of monitoring utilities dedicated to the control of safety critical systems and equipments. To overcome the problem, energy efficiency strategies are being widely studied, to prolong the lifetime of the network through duty-cycling mechanisms, that act on the selection of nodes which acquire and transfer sensor measurements (topology control) and on the power-on timing of the selected nodes (power management), even at the cost of a reduction of data quality and an increase of latency of data transfer [8][25]. Such strategies include cross-layer adaptivity mechanisms which combine functionalities at different layers of the protocol stack. In particular, this often involves the application layer conditioning the actual operation of the network on the basis of achieved measurements and on forecasts on the monitored system. In [15] the node transfers to a manager node the model of the dynamics of the measured variable and does not transmit any data on the evolution of the measurement until the model adequately approximates the measurement. In [19] the sensor sampling period is adapted to the dynamics of the monitored system in order to create a feedback loop that keeps an error function within a predefined stability interval. An explicit reference to the reliability requirements of the application level is proposed in [9] to select routing paths through the network.

Few experiences have been reported on schemes based on a discrete event model of the monitored system. In [13], TinyDB [19] queries to a network of nodes are approximated by taking into account the state of a model of the monitored system, represented as a Markovian process which evolves with time progress and measurements acquisition. In [21], a sensor network is integrated in a wearable device to monitor the vital parameters of a human; to limit the energy loss, an adaptive sensing strategy which traces the parameters in real-time against a Markov Decision Process is applied. None of such models adopts a non-Markovian distribution of timing. This largely restricts the expressive power and accuracy of models, and in particular it excludes the representation of timing with finite support and prevents the verification of real-time requirements (e.g. maximal acquisition and transfer latency) and the representation of communication and fault-tolerance mechanisms (such as timeouts, watchdog timers, sleep/wakeup protocols [17]).

We address the problem with reference to an abstract scenario open to various monitoring applications: a critical system is made by a set of components, each associated

with a nominal range of safe operation, organized into a fault-tolerant hierarchical structure; the operation point of each component is periodically sampled and transported to a base-station through a WSN infrastructure; the sampling period can be adjusted, but samples can be lost in the routing to the base-station, so that the monitoring system has only an indirect best-effort control over the time elapsed between subsequent deliveries at the base station of each component sample; during the period between subsequent samples delivery, the probability that the component has diverged from its nominal range is estimated with a worst-case unreliability cumulative distribution function (CDF); when the overall unreliability CDF of the fault-tolerant architecture exceeds a given threshold, some kind of escalation occurs, consisting in the activation of more expensive monitoring components, the execution of a maintenance operation, or even the stop of some system components.

With reference to this scenario we are interested in supporting power-management of the WSN infrastructure during nominal operation and escalation-decision when critical conditions are reached. To this end, we propose a solution that: supports derivation of the evolution over time of the overall system-unreliability and rejuvenates it according to the flow of delivered samples; maintains a dynamic measure of the safe time-horizon within which the system is expected to operate under the given threshold of unreliability; provides a quantitative measure of the safe time-horizon sensitivity with respect to the successful delivery of samples from each different system node.

In the rest of the paper, we first introduce *Stochastic Fault Trees* as the fault-tolerant architecture of the monitored system (Sect.2), and we then develop the calculus that supports symbolic evaluation of system unreliability (Sect.3), of the safe time-horizon and of the quantitative measure of sample relevance (Sect.4). Finally, conclusions are drawn in Sect.5.

2. Stochastic Fault Trees as the fault-tolerant architecture of safety-critical systems

We address the operation scenario devised in the Introduction under the assumption that:

- system components follow a decaying model according to which their working functionalities lower themselves as time goes by;
- the monitored system is modeled through a fault-tolerant hierarchical architecture that takes into account the evolution of unreliability over time and describes how the behavior of each component affects the unreliability of the whole system.

Such a scenario can be effectively described by modeling the supervised system through a fault-tolerant architecture based on *Fault Trees* (FTs), which are widely employed in the industrial practice [5][1][2][3] as a means to represent the hierarchical relationships among causal factors that can yield an undesired outcome called *Top Event* (TE). A system can be modeled through a FT following a top-down approach, which identifies the events leading to the occurrence of the TE and expresses their relationships by combining them through boolean logic gates (i.e. *AND*, *OR*, *KofN*); this step is then repeated for each event until the so-called *basic events* are identified. Qualitative analysis of a FT provides the enumeration of the set of *Minimal Cut Sets* (MCSs), i.e. minimal combinations of leaf events that lead to the occurrence of the TE.

In the usual formulation, leaf events are associated with fixed, time-independent failure probabilities, calculated in a rather static manner on the basis of statistical information concerning the reliability of single components [27]. Quantitative evaluation of a FT supports reliability and safety analysis [24][16] through the derivation of the TE failure probability. This can be accomplished by following either an *indirect approach*, which derives the probability of the TE by combining the probabilities of all the MCSs, or a *direct approach*, which repeatedly combines nodes probabilities at each gate of the tree [23].

The probability of the TE depends only on the structure of the tree, with no reference to time. However, reliability of system components often evolves over time, due to such factors as: components aging; operation modes changing over time; maintenance and rejuvenation processes. In these cases, probability of the TE at different instants of time must be repeatedly recomputed in a kind of polling process, in order to take into account how the probability of component failures is conditioned by the actual operating conditions. In our reference scenario, evolution over time of system unreliability is mainly due to the lack of observations between subsequent delivers of samples by the WSN infrastructure. We assume that, during this period, the probability that the component behavior has diverged from its nominal range is estimated on the basis of a worst-case unreliability CDF. Each time the WSN delivers an observation stating the correct behavior of a component, the esteem of its unreliability is rejuvenated.

Various approaches manage evolution of reliability of system components over time. In [23], leaf events of a Fault Tree with Repeated Events (FTRE) [20] can be associated with an exponential CDF and the TE probability over time is derived by composition of exponential rates through approximate analysis. In [22], the time of occurrence of each leaf event is associated with a CDF and the FTRE is translated into a Generalized Stochastic Petri Net (GSPN) model [6]. Thus, under the assumption that all leaves have a negative exponential CDF, the evaluation of the FT is reduced to the analysis of a Continuous Time Markov Chain (CTMC).

This also opens the way to extend modeling power with state space concepts that may account for dependencies and complex repair mechanisms. In [10], a parametric fault tree is translated into a Stochastic Well-Formed Colored Net in order to generate a lumped Markov chain. As a common trait, in all these works the time of occurrence of leaf events is associated with a negative exponential CDF. This rules out representation of relevant patterns occurring in reliability engineering such as a periodic operation or maintenance process which results in a synchronous recurrent regeneration. In our scenario, reliability may decay between subsequent observations according to non-Markovian (GEN) CDFs, possibly supported over finite domains and possibly represented in piece-wise form.

To overcome the limitation and fit the needs of our application context, we extend standard FTs into *Stochastic Fault Trees* (SFTs). These allow the failure time t_i of a component C_i (i.e. the time of occurrence of the corresponding leaf event E_i) to be a random variable that follows a generalized (GEN) CDF $U_{t_i}(x)$, absolutely continuous and thus represented as the integral function of a probability density function (PDF) $u_{t_i}(y)$:

$$U_{t_i}(x) = P(t_i \leq x) = \int_0^x u_{t_i}(y)\, dy \tag{1}$$

The corresponding *defective* CDF represents the *reliability* $R_{t_i}(x)$ of the component C_i and it accounts for the probability that C_i performs its required functions under stated conditions for a time longer than x (i.e. the probability that its failure time t_i is greater than x):

$$R_{t_i}(x) = P(t_i > x) = 1 - U_{t_i}(x) \tag{2}$$

3. Symbolic evaluation of system unreliability

In our reference scenario, the WSN monitoring infrastructure periodically delivers observations on the behavior of single components. The proposed approach is oriented to the estimation of the safe time-horizon within which the system is expected to operate under a given threshold of unreliability, even in absence of new samples. To this end, we estimate the evolution over time of the unreliability of a component through a conservative CDF and we derive the symbolic form of the analytic representation of system unreliability, rejuvenating estimations on the basis of delivered observations.

3.1 Quantitative analysis of STFs

Quantitative analysis of SFTs derives the CDF of the TE failure time, thus allowing the evaluation of system-unreliability over time. To this end, unreliability CDFs of components are combined according to the architecture of the tree, following either a direct or an indirect approach. We implemented quantitative analysis of SFTs following the direct method [23], which derives the unreliability of the TE through a bottom-up approach that combines CDFs of events failure time at each gate of the tree. This prevents the representation of repeated events but reduces the computational effort and, as a by-product, provides the CDFs at intermediate gates of the tree.

The CDF of the TE is derived by repeatedly computing the unreliability of the combination of a set of events at each gate of the tree. Let $E_1, ..., E_N$ be N events whose failure times $t_1, ..., t_N$ are random variables having unreliability CDFs $U_{t_1}(x), ..., U_{t_N}(x)$, respectively, and let $U_{t_{AND}}(x)$, $U_{t_{OR}}(x)$, $U_{t_{KofN}}(x)$ be the unreliability CDF of the failure time of their AND, OR and KofN combinations, respectively. As usual, $U_{t_{AND}}(x)$, $U_{t_{OR}}(x)$ and $U_{t_{KofN}}(x)$ are derived by combining $U_{t_1}(x), ..., U_{t_N}(x)$ through sums and products. More specifically:

$$U_{t_{AND}}(x) = \prod_{i=1}^{N} U_{t_i}(x) = \prod_{i=1}^{N} (1 - R_{t_i}(x)) \tag{3}$$

$$U_{t_{OR}}(x) = 1 - \prod_{i=1}^{N} (1 - U_{t_i}(x)) = 1 - \prod_{i=1}^{N} R_{t_i}(x) \tag{4}$$

KofN gate models a failure event that occurs if and only if at least K out of the N input events occur and thus turns out to be equivalent to the OR configuration of the events represented by the AND configuration of K out of N events. In so doing, $U_{t_{KofN}}(x)$ is derived as follows:

$$\begin{aligned} U_{t_{KofN}}(x) &= 1 - \prod_{I \in C(N,k)} (1 - \prod_{i \in I} U_{t_i}(x)) \\ &= \prod_{I \in C(N,K)} (1 - \prod_{i \in I} (1 - R_{t_i}(x))) \end{aligned} \tag{5}$$

where $C(N, K)$ is the set of K-combinations from the set $\{1, ..., N\}$ of event indexes.

3.2 Expolynomial unreliability CDFs

We implemented the symbolic calculus of system unreliability under the assumption that the failure time of basic events follows a piece-wise expolynomial CDF [12][14], i.e. a function that partitions the support in a finite number of sub-domains and that assumes over each of them an expression of the form:

$$\sum_{j=1}^{L} c_j x^{\alpha_j} e^{-\lambda_j x} \qquad \forall\, c_j \in \mathbb{R},\ \lambda_j \in \mathbb{R}_0^+.$$

The class of expolynomial functions exhibits a number of properties that nicely fit the needs of our application:

- it is closed with respect to various operations (i.e. sum, multiplication, derivation, integration);
- it includes common basic distributions (e.g. uniform, exponential, gamma) and polynomial distributions, which support the derivation of good approximations over finite domains (e.g. Bernstein Polynomials [18][26] enable the construction of straightforward approximations [11]);
- it enables the construction of fine approximations when distributions must be derived by the interpolation of statistical data.

According to this and to Eqs.(3-4), the unreliability CDF $U_{t_i}(x)$ of an intermediate event E_i and the overall system unreliability CDF $U_{t_{TE}}(x)$ turn out to be piece-wise expolynomial functions. This enables the implementation of their symbolic calculus in closed-form. Note that the unreliability PDF $u_{t_i}(x)$ of any event E_i is a piece-wise expolynomial function too.

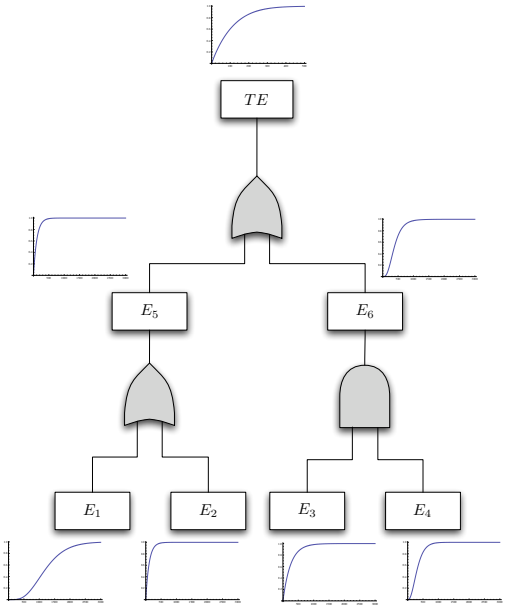

Figure 1. A Stochastic Fault Tree composed of the TE, two intermediate events and four leaf events.

Fig.1 reports a SFT composed of four basic events E_1, E_2, E_3 and E_4, connected through three boolean logic gates within an architecture that comprises intermediate events E_5 and E_6 and the TE. The picture highlights unreliability CDFs of leaf events, intermediate events and the TE. Failure times t_1, t_2, t_3, t_4 of basic events E_1, E_2, E_3, E_4 follow expolynomial unreliability CDFs $U_{t_1}(x), U_{t_2}(x), U_{t_3}(x), U_{t_4}(x)$, respectively, with support $[0, \infty]$:

$$U_{t_1}(x) = 1 - e^{-0.004x}\left(1 - 0.004x - 8 \cdot 10^{-6}x^2 - \right.$$

$$\left. -1.06667 \cdot 10^{-8}x^3 - 1.06667 \cdot 10^{-11}x^4\right)$$

$$U_{t_2}(x) = 1 - e^{-0.009x}$$

$$U_{t_3}(x) = 1 - e^{-0.004x}$$

$$U_{t_4}(x) = 1 + e^{-0.009x}\left(-1 - (0.009 + 0.0000405\, x)\; x\right)$$

According to Eqs.(3-4), system unreliability $U_{t_{TE}}(x)$ turns out to be:

$$U_{t_{TE}}(x)$$

$$= 1 - 1.06667 \cdot 10^{-11} e^{-0.013x}(396694 + x(135.278 + x))$$

$$(236328 + x(864.722 + x))(1 - e^{-0.013x}(-1 + e^{0.004x})$$

$$(-1 + e^{0.009x} + (-0.009 - 0.0000405\, x)\, x))$$

3.3 Pruning heuristics

Quantitative analysis of SFTs based on the direct method repeatedly combines unreliability CDFs at each gate of the tree through Eqs.(3-5). According to this, the unreliability CDF associated with an intermediate event has a number of exp-monomial terms at least equal to the product among the number of exp-monomial terms of unreliability CDFs of its input events. Therefore, the shorter is the depth of an event, the more is the number of exp-monomial terms of its unreliability CDF. More specifically, consider a SFT where: *i)* all leaf nodes follow an expolynomial CDF having L exp-monomial terms; *ii)* all gates have input degree N; *iii)* the tree has depth H. The TE turns out to have an unreliability CDF with $O(L^{N^H})$ exp-monomial terms and the problem is further exacerbated if CDFs of leaf nodes have piece-wise representation. In fact, if unreliability CDFs of leaf nodes partition the support in W pieces and any two sub-domains belonging to CDFs of connected events do not match, then the unreliability CDF of the TE will be defined over $O(W \cdot N^H)$ sub-domains, with $O(L^{N^H})$ exp-monomial terms over each sub-domain.

To overcome the problem, we approximate unreliability CDFs at each gate of the tree by pruning exp-monomial terms according to various heuristics. Let $\tilde{U}_t(x)$ be the approximant function of the unreliability CDF $U_t(x)$ of an event E and let $U_t(x)$ be defined over a domain D partitioned into M sub-domains $D1, ..., D_M$, with a number $L_1, ..., L_M$ of exp-monomial terms over sub-domains

$D_1, ..., D_M$, respectively:

$$U_t(x) : D = \bigcup_{i=1}^{M} D_i \rightarrow [0,1]$$

$$U_t(x) = \begin{cases} \sum_{j=1}^{L_1} c_{1j} x^{\alpha_{1j}} e^{-\lambda_{1j} x} & \text{if } x \in D_1 \\ ... & \\ \sum_{j=1}^{L_M} c_{Mj} x^{\alpha_{Mj}} e^{-\lambda_{Mj} x} & \text{if } x \in D_M \end{cases}$$

where $c_{ij} \in \mathbb{R}$, $\alpha_{ij} \in \mathbb{N}_0^+$ and $\lambda_{ij} \in \mathbb{R}_0^+$, $\forall j \in [1, L_i]$, $\forall i \in [1, M]$. We propose three heuristics to discard the less significant exp-monomial terms of an unreliability CDF. Unit measure of the corresponding PDF can be restored through normalization, even though the emphasis is not on PDF property preserving but on the estimation of the safe time-horizon through the unreliability CDF of the system.

Monomials number heuristic The heuristic defines the maximum allowed number L_{max} of exp-monomial terms over any sub-domain. The relevance of an exp-monomial term is evaluated through the maximum value that it assumes over its support, and the approximant function $\tilde{U}_t(x)$ is obtained by pruning the $L_i - L_{max}$ less significant exp-monomials over each sub-domain D_i. This guarantees constant complexity in the derivation of the unreliability CDF at each gate of the tree.

Maximum value heuristic The heuristic defines a threshold ϵ for values assumed by exp-monomial terms and the approximant function $\tilde{U}_t(x)$ is derived by pruning exp-monomial terms with maximum value lower than ϵ. With respect to Monomials number heuristic, this approach takes into account the contribution of each term to the overall unreliability CDF, in order to avoid the pruning of significant exp-monomials.

Error heuristic The heuristic derives $\tilde{U}_t(x)$ by pruning the less significant terms such that the distance between $U_t(x)$ and $\tilde{U}_t(x)$ is under a given threshold γ. The relevance of exp-monomial terms is evaluated on the basis of the maximum value assumed over the support and various metrics can be defined to determine the distance between two functions. In particular, we assume the $\mathcal{L}^2$-norm $||\cdot||_d$:

$$||U_t(x) - \tilde{U}_t(x)||_d \stackrel{def}{=} \int_D |U_t(x) - \tilde{U}_t(x)|^2 dt$$

For the sake of efficiency, the metrics $||\cdot||_d$ is approximated in discrete form, by evaluating the two functions in correspondence with samples taken over a regular grid:

$$||U_t(x) - \tilde{U}_t(x)||_d = \sum_{k=0}^{K} \left(U_t(x_k) - \tilde{U}_t(x_k)\right)^2$$

4. An application scenario in power management of WSN infrastructure

The fault-tolerant architecture based on SFTs allows the definition of a predictive engine that receives observations from the monitoring system and provides a dynamic measure of the horizon of safe behavior, thus supporting the definition of escalation policies in reaction to critical conditions attainment. We consider a general setting (see Fig.2) where a critical system is supervised by a monitoring infrastructure. The monitored system is made up of components, each characterized by a nominal range of safe operation; the monitoring utility consists of a fault-tolerant architecture for the system and a WSN.

- The system is represented through a SFT, where each basic event models a single component or a set of components. According to this, each of the blocks A, B, C and D in Fig.2 represents a supervised component (or a set of components) of the critical system, and it has a counterpart in the corresponding leaf event of the tree. SFTs associate the failure time of leaf events with a worst-case CDF and enable the derivation of the CDF $U_{t_{TE}}(x)$ of the TE failure time.
- The WSN monitoring system periodically samples the operation point of components and carries the observations to a *base station* or *sink node*, which, in turn, delivers messages to the fault-tolerant architecture through an application bus. An *observation* is a time-stamped message that states whether the current operation point of a supervised component is out of its safe range or not.
- Whenever the fault-tolerant architecture receives an observation, unreliability CDFs of the failure time of basic events are updated and $U_{t_{TE}}(x)$ is consequently recomputed. On the one hand, if a sample asserts correct behavior of the component associated with leaf event E_k at time x_0, the CDF $U_{t_k}(x)$ of its failure time t_k is rejuvenated (x_0 is assumed to be measured since the last delivered observation). The assumption that observation occurs at time x_0 conditions t_k, yielding a new random variable $t'_k = t_k | t_k \geq x_0$, that represents the life time of the component conditioned to the observation of correct behavior at time x_0. The corresponding CDF $U_{t'_k}(x)$ can be obtained by deriving the

conditional PDF $u_{t'_k}(x)$:

$$u_{t'}(x)dx = P(t' \in [x, x+dx])$$

$$= P(t \in [x, x+dx] | t \geq x_0)$$

$$= \begin{cases} 0 & \text{if } x + dx \leq x_0 \\ \dfrac{P(t \in [x, x+dx] \wedge t \geq x_0)}{P(t \geq x_0)} & \text{if } x > x_0 \end{cases}$$

$$= \begin{cases} 0 & \text{if } x + dx \leq x_0 \\ \dfrac{P(t \in [x, x+dx])}{P(t \geq x_0)} & \text{if } x > x_0 \end{cases}$$

$$= \begin{cases} 0 & \text{if } x + dx \leq x_0 \\ \dfrac{u_t(x)dx}{1 - U_t(x_0)} & \text{if } x > x_0 \end{cases}$$

$$U_{t'}(x) = \int_0^x u_{t'}(y)dy$$

$$= \begin{cases} 0 & \text{if } x + dx \leq x_0 \\ \dfrac{U_t(x)}{1 - U_t(x_0)} & \text{if } x > x_0 \end{cases}$$

We then define the new random variable $t''_k = t'_k - x_0$, that represents the residual life time of the component, and we compute the corresponding CDF $U_{t''}(x)$:

$$U_{t''}(x) = \begin{cases} 0 & \text{if } x \leq 0 \\ U_{t'}(x + x_0) & \text{if } x > 0 \end{cases}$$

$$= \begin{cases} 0 & \text{if } x \leq 0 \\ \dfrac{U_t(x + x_0)}{1 - U_t(x_0)} & \text{if } x > 0 \end{cases}$$

On the other hand, if a sample states that the component associated with leaf event E_k is broken down at time x_0, then its unreliability CDF $U_{t_k}(x)$ is dropped, obtaining $U_{t''_k}(x) = 1 \ \forall\, x \geq 0$.

- During the period between subsequent samples, evolution over time of system unreliability is estimated using the current function $U_{t_{TE}}(x)$: after x_n time units since the last delivered sample, the estimated system unreliability will be $U_{t_{TE}}(x_n)$.
- The fault-tolerant architecture maintains a measure of the time-horizon within which the system is expected to operate under a predefined threshold of unreliability, and it provides the WSN infrastructure with a measure of the contribution of each basic event to the overall system unreliability $U_{t_{TE}}(x)$. This supports the adoption of power-management and escalation-decision policies.

It is worth noting that in the proposed setting the SFT accounts for the unreliability of the monitored system. The inherent unreliability of the WSN monitoring infrastructure is involved in the scenario as it may causes loss of samples.

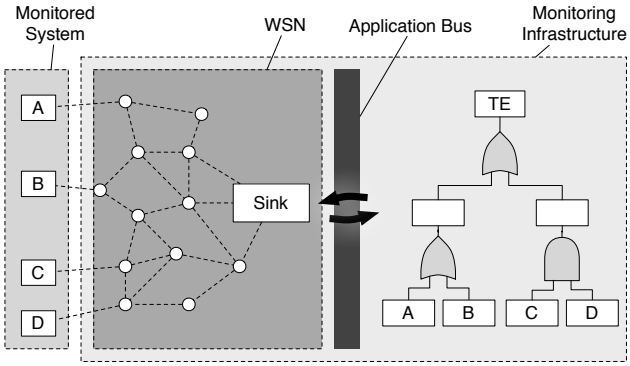

Figure 2. An abstract scenario made up of a safety-critical system supervised by a monitoring infrastructure. The monitoring utility is composed of a fault-tolerant architecture for the system and a WSN, sending messages to each other through an application bus.

4.1 Quantitative evaluation of the safe time-horizon

The fault-tolerant architecture based on SFTs provides symbolic evaluation of system unreliability over time and enables the derivation of the safe time-horizon within which the system is expected to operate under an assigned threshold of unreliability.

Given a threshold $\delta \in [0, 1]$ for system unreliability $U_{t_{TE}}(x)$, the safe time-horizon is the time $\bar{x}$ such that $U_{t_{TE}}(\bar{x}) = \delta$ and it turns out to be the root of function $U_{t_{TE}}(x) - \delta$ (see Fig.3). $U_{t_{TE}}(x)$ is a piece-wise expolynomial CDF and, according to this, it is a differentiable monotonic function taking values within $[0, 1]$. Thus, the equation $U_{t_{TE}}(x) - \delta = 0$ has one and only one root that can be estimated through the Newton's method, which iteratively derives approximations of the roots of a real-valued function. Starting from an initial guess for the root of function $U_{t_{TE}}(x) - \delta$, at each step the current function is substituted with its tangent line passing from the current approximation and the x-intercept of the tangent line is then taken as the new approximation.

Fig.3 reports the unreliability CDF $U_{t_{TE}}(x)$ for the system modeled through the SFT of Fig.1. The unreliability threshold δ is 0.4, which corresponds to a safe time-horizon $\bar{x}$ equal to 58 time units.

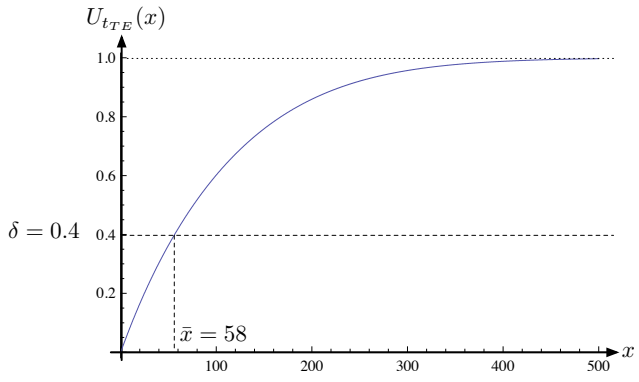

Figure 3. The unreliability CDF $U_{t_{TE}}(x)$ for the system modeled by the SFT of Fig.1. The unreliability threshold δ is set equal to 0.4 and the corresponding safe time-horizon $\bar{x}$ is 58 time units.

4.2 Escalation management

The fault-tolerant architecture based on SFTs provides symbolic evaluation of system unreliability and maintains a dynamic measure of the safe time-horizon of the system. This enables the derivation of a quantitative measure of components relevance that supports power-management and escalation-decision policies.

Whenever the WSN delivers an observation, the fault-tolerant architecture locates the safe time-horizon $\bar{x}$ and, for each basic event E_i in the SFT model, it evaluates an *Importance Measure* $I_i(\bar{x})$ that encodes the contribution of the corresponding supervised component to the global unreliability $U_{t_{TE}}(\bar{x})$. Then, the fault-tolerant architecture feeds back the WSN with a list of basic events ordered by their relevance at critical time $\bar{x}$, thus enabling the enforcement of preventive measures (e.g. variations of the sampling frequencies, activations of new wireless nodes). It is worth noting that the fault-tolerant engine cannot directly force the alteration of specific parameters of the WSN, because of a separation of concern between the supervised system and the monitoring infrastructure.

The Importance Measure $I_i(\bar{x})$ of a basic event E_i should take into account two main factors: *i)* the unreliability $U_{t_i}(\bar{x})$ of the corresponding monitored component at the safe time-horizon $\bar{x}$; *ii)* the weight that $U_{t_i}(\bar{x})$ has on the global system unreliability $U_{t_{TE}}(\bar{x})$ due to the static structure of the tree and the unreliability of nodes that are topologically related to E_i. A large part of the literature about Reliability Engineering and Fault Tree Analysis focuses on a few indexes to capture the importance of single components with respect to the overall system unreliability. Two significant measures are *Birnbaum measure* and *Fussell-Vesely measure*.

- *Birnbaum measure* calculates system unreliability at critical time $\bar{x}$ under the two hypothesis that at time $\bar{x}$ the unreliability of the component associated with event E_i is either rejuvenated (i.e. $U_{t_i}(\bar{x}) = 0$) or dropped (i.e. $U_{t_i}(\bar{x}) = 1$), and provides the difference between the obtained values:

  $$I_i^B(\bar{x}) = U_{t_{TE}}(\bar{x})_{|U_{t_i}(\bar{x})=0} - U_{t_{TE}}(\bar{x})_{|U_{t_i}(\bar{x})=1}$$

  Birnbaum measure is not suitable for the purposes of our treatment, because it does not adequately take into account the topology of the SFT model.

- *Fussell-Vesely measure* associates each component with the sum of probabilities (at critical time $\bar{x}$) of MCSs that contain the corresponding event E_i:

  $$I_i^{FV}(\bar{x}) = \sum_{CS_j \in MCS(E_i)} P(CS_j \text{ at time } \bar{x}),$$

  where $MCS(E_i)$ is the set of MCSs that contain the leaf event E_i and can be derived through the *MOCUS* algorithm (*Method of Obtaining Cut Sets*). Fussell-Vesely measure accounts for both the probability associated with events and the topology of the tree. However, any two events that are part of the same MCSs turn out to have the same Fussell-Vesely measure, regardless of their own probability of occurrence.

To overcome the problem, we adopt a variant of Fussell-Vesely measure that takes into account the unreliability at critical time $\bar{x}$ of the component under consideration:

$$I_i(\bar{x}) = U_{t_i}(\bar{x}) \cdot \sum_{CS_j \in MCS(E_i)} P(CS_j \text{ at time } \bar{x}) \quad (6)$$

This measure combines two factors:

- the unreliability $U_{t_i}(\bar{x})$ of the component at critical time $\bar{x}$ accounts for the decay of its working functionalities after $\bar{x}$ time units;
- $\sum_{CS_j \in MCS(E_i)} P(CS_j \text{ at time } \bar{x})$ provides a measure of how this degradation weights on the overall system unreliability at critical time $\bar{x}$ according to the topology of the SFT model.

5. Conclusions

This paper proposes SFTs as fault-tolerant models for safety-critical systems. SFTs associate leaf events with a non-Markovian (GEN) CDF of the failure time, possibly supported over finite domains and possibly represented

in piece-wise form, enabling symbolic evaluation of system unreliability CDF. The symbolic calculus has been implemented in closed form under the assumption that leaf events follow an expolynomial CDF and it takes advantage of heuristics to avoid explosion in the number of expmonomial terms. The remarkable simplicity of the analysis allows the construction of a predictive engine that can be employed in a variety of scenarios where a critical system is supervised by a monitoring infrastructure. In particular, the SFT architecture is able to maintain an estimation of system unreliability and of the safe time-horizon within which the system is expected to operate under a given threshold of unreliability, and dynamically updates them according to the flow of samples delivered by a WSN monitoring architecture, thus attaining a good adaptivity with respect to the evolution of system behavior over time. The fault-tolerant model also provides the WSN with a measure of the contribution of each basic event to system unreliability, thus supporting the enforcement of online power management and escalation decision strategies.

A prototype implementation of the SFT analysis engine was experimented on a small setting with a low number of wireless nodes in order to verify the feasibility of the overall approach. Moreover, integration of the SFT application with ns-2 simulator [4] is ongoing to the purpose of evaluating the impact of different energy efficiency and escalation decision strategies. Future work is oriented to the identification of a fault-tolerant infrastructure that takes into account the unreliability of the WSN monitoring system.

Acknowledgment Research reported in this paper was partially supported by the project WiSeDeMon funded by the Italian Ministry of University and Research as a part of the PRIN 2007 Programme. We kindly thank Giuseppe Anastasi for his precious help in understanding WSN technology.

References

[1] *FaultTree+*. http://www.faulttree.org.

[2] *FTA-Pro*. http://www.dyadem.com.

[3] *ITEM ToolKit*. http://www.itemsoft.com.

[4] *The Network Simulator - ns-2*. http://nsnam.isi.edu/nsnam/index.php.

[5] *Relex Fault Tree Analysis software*. http://www.relex.com.

[6] M. M. Ajmone, G. Balbo, and G. Conte. A class of generalized stochastic petri nets for the performance evaluation of multiprocessor systems. *ACM Trans. on Comp. sys.*, 1984.

[7] I. Akyildiz, W. Su, Y.Sankarasubramaniam, and E.Cayirci. Wireless sensor networks: a survey. *Computer Networks*, 38(4), March 2002.

[8] G. Anastasi, M.Conti, M. D. Francesco, and A.Passarella. How to prolong the lifetime of wireless sensor networks. *Mobile Ad Hoc and Pervasive Communications*, to appear.

[9] S. Banerjee and A. Misra. Minimum energy paths for reliable communication in multi-hop wireless networks. *Proc. ACM MobiHoc 2002*, June 9-11 2002.

[10] A. Bobbio, G.Franceschinis, R.Gaeta, and L.Portinale. Parametric fault tree for the dependability analysis of redundant systems and its high-level petri net semantics. *IEEE Trans. SW Eng.*, 29(3), March 2003.

[11] L. Carnevali, L. Grassi, and E. Vicario. State-density functions over dbm domains in the analysis of non-markovian models. *IEEE Trans. on SW Eng.*, 35(2):178–194, 2009.

[12] G. Ciardo, R. German, and C. Lindemann. A characterization of the stochastic process underlying a stochastic petri net. *IEEE Trans. On Softw. Eng.*, 20(7):506–515, 1994.

[13] A. Deshpande, C.Guestrin, S.R.Madden, J.M.Hellerstein, and W.Hong. Model-based approximate querying in sensor networks. *Int. Journal on Very Large Data Bases*, 2005.

[14] R. German. *Performance Analysis of Communication Systems with Non-Markovian Stochastic Petri Nets*. John Wiley & Sons, 2000.

[15] S. Goel, A. Passarella, and T. Imielinski. Using buddies to live longer in a boring world. *Proc. IEEE Int.Workshop on Sensor Networks and Systems for Pervasive Computing (PerSeNS 2006)*, March 2006.

[16] E. J. Henley and H. Kumamoto. *Reliability Engineering and Risk Assessment*. Englewood Cliffs, N.J.: Prentice Hall, 1981.

[17] A. Keshavarzian, H. Lee, and L. Venkatraman. Wakeup scheduling in wireless sensor networks. *Proc. ACM MobiHoc 2006*, pages 322–333, May 2006.

[18] G. Lorentz. *Bernstein Polynomials*. University of Toronto Press, 1953.

[19] S. R. Madden, M. J. Franklin, J. M. Hellerstein, and W. Hong. Tinydb: an acquisitional query processing system for sensor networks. *ACM Trans. Database Systems*, 30:122–173, 2005.

[20] M. Malhotra and K. S. Trivedi. Power-hierarchy of dependability-model types. *IEEE Trans. Rel.*, 43(3):493–502, Sep. 1994.

[21] A. Panangadan, S. M. Ali, and A. Talukder. Markov decision processes for control of a sensor network-based health monitoring system. *Proc. Conf. Innovative Applications of Artificial Intelligence IAAI*, pages 1529–1534, 2005.

[22] K. G. Popstojanova and K. S. Trivedi. Stochastic modeling formalisms for dependability, performance and performability. *Performance Evaluation - Origins and Directions, LNCS*, pages 385–404, 2000.

[23] S. Rai. Evaluating FTRE's for dependability measures in fault tolerant systems. *IEEE Trans. Comput.*, 44(2):275–285, Feb. 1995.

[24] R. A. Sahner, K. S. Trivedi, and A. Puliafito. *Performance and Reliability Analysis of Computer Systems: An Example-Based Approach Using the SHARPE Software Package*. Kluwer Academic Publishers, 1996.

[25] P. Santi. Topology control in wireless ad hoc and sensor networks. *ACM Computing Survey*, 37(2):164–194, June 2005.

[26] T. Sauer. Multivariate Bernstein polynomials and convexity. *Computer Aided Geometric Design*, 8(6):465 – 478, 1991.

[27] W. E. Vesely, F. F. Goldberg, N. H. Roberts, and D. F. Haasl. *Fault Tree Handbook*. U. S. Government Printing Office, 1981.