Reliability and Criticality Analysis of Communication Networks by Stochastic Computation

Peican Zhu, Jie Han, Yangming Guo and Fabrizio Lombardi

-

***Abstract*— Reliability is an important feature in the design and maintenance of a large-scale network. In this paper, the reliability of information transmission between a transmitter and a receiver (i.e. a two-terminal network) is considered as a generalized connectivity framework of terminal nodes. As network complexity increases, existing approaches to reliability analysis are encountering significant challenges. In this paper, stochastic computational models are presented to efficiently analyze the reliability and criticality of a two-terminal network. Non-Bernoulli sequences with fixed numbers of 1's and 0's are utilized to encode the signal probabilities and to improve the computational efficiency and accuracy. Both unidirectional and bidirectional links are considered for the probabilistic information transition process by imperfect links. Imperfect nodes are also modeled by the stochastic model of an imperfect unidirectional link. Non-exponential failure distributions and correlated signals in a two-terminal network are readily handled by the stochastic approach. The reliability of a system with external deterministic failures on a link is compared to that of the system prior to the occurrence of the failures. The difference in reliability is referred to as the criticality of the link. An analysis is pursued for the critical links based on the value of criticality. The proposed approach can be used to analyze and improve network reliability when utilizing a limited redundancy for protecting the links.**

I. INTRODUCTION

Networks exist in many large-scale systems such as those for communication, power delivery, water distribution and gas supply. For these systems, large economic losses and security risks are likely to be incurred if the underlying network fails. Hence, the robust operations of these systems are critical, and reliability is a very important requirement. A network often connects its two end terminals, also referred to as the *transmitter* and the *receiver*; hence, this type of network is commonly referred to as a *two-terminal network*. Such a network is usually modeled by a probabilistic graph, i.e., $G(V, E)$, consisting of a node set V and a link set E [1]. The set V consists of a transmitter (T in Figure 1), a receiver (R in Figure 1) and the intermediate nodes ($I_1 \cdots I_m$, IN_k and $J_1 \cdots J_n$ in Figure 1). The set E consists of the links between the nodes of the network (either unidirectional or bidirectional).

Such a network is likely to be affected by various catastrophic failures due to externally induced events (e.g., earthquakes and hurricanes). It fails when the anticipated delivery service cannot be completed through a fault-free path connecting the transmitter and the receiver. Therefore, it is important to predict its performance under these failures, for example, to evaluate whether a gas supply network can reliably function following a hurricane. The *reliability* of a two-terminal network is defined as the probability of a successful communication (or the anticipated information transmission) between the transmitter and the receiver of a network. Hence, reliability evaluation usually deals with the connectivity probability between the transmitter and the receiver [1]. Redundancy is often utilized to guarantee the network to be operational in the presence of failures. However, it requires a detailed analysis to determine the critical links [2].

Methods found in the technical literature can be classified into two major categories: Monte Carlo (MC) simulation and probabilistic analysis. In MC simulation, a large sample size is usually required for achieving a suitable accuracy and obtaining a stable probability due to the slow convergence [3]. Thus, a long simulation time is usually incurred. For probabilistic analyses such as the path- [4] and cut-based algorithms [5], an accurate result can be derived by decomposing a network into disjoint paths; however, a large computational complexity results for path-based algorithms. The reliability evaluation process is cumbersome, because the number of paths increases exponentially with the number of network edges or nodes. [6] has presented an improved recursive algorithm to calculate the reliability; however, only approximate results (within an error bound) can be obtained. [7] has provided an exact algorithm to find the reliability of two-terminal networks; however, the process for deriving the expressions is rather complex. Binary decision diagram (BDD) based approaches have also been proposed [8] and the reliability assessment of multiple-valued networks has been

P. Zhu was with the Department of Electrical and Computer Engineering, University of Alberta, Edmonton, AB T6G 1H9, Canada. He is currently with the School of Computer Science and Technology, Northwestern Polytechnical University (NWPU), Xi'an, Shaanxi, China.

J. Han is with the Department of Electrical and Computer Engineering, University of Alberta, Edmonton, AB T6G 1H9, Canada (e-mail: jhan8@ualberta.ca).

Y. Guo is with the School of Computer Science and Technology, Northwestern Polytechnical University (NWPU), Xi'an, Shaanxi, China.

F. Lombardi is with the Department of Electrical and Computer Engineering, Northeastern University, Boston 02115, MA. E-mail: lombardi@ece.neu.edu.

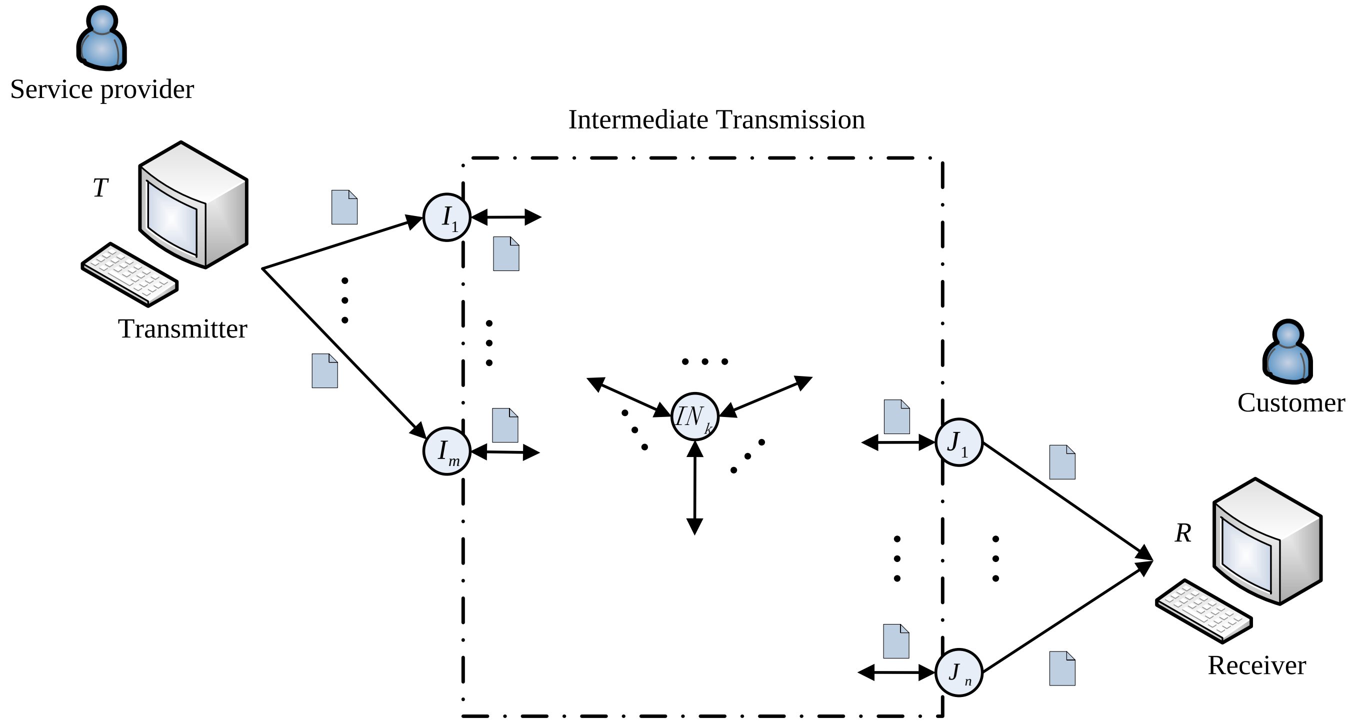

Figure 1. A general structure for a two-terminal network. I_i, $i \in \{1, 2, \cdots, m\}$, is a node connected transmitter. IN_k is a node connected to the intermediate nodes. J_i, $i \in \{1, 2, \cdots, n\}$, is a node connected receiver .

pursued in [9]. The methods using BDDs have been shown to be very efficient for network analysis; however, the construction of a BDD is not always simple. Additionally, a reduced order BDD (ROBDD) (as the most efficient form of BDD) requires variable ordering, thus further increasing the complexity of BDD construction process. Finally, the failure distributions of imperfect links/nodes are not limited to fixed values, but they vary with the mission time. The mission time is defined as a time period and the status of the system is investigated within this time period. The analysis of exponentially or non-exponentially distributed failure events is even more complex. Hence, a more comprehensive and efficient approach is required for the reliability analysis of a network. Recently, stochastic computation has been proposed for reliability analysis of logic circuits [10] and dynamic fault trees (DFTs) [11][12]. The use of non-Bernoulli sequences leads to an efficient evaluation [10]. Signal correlations are preserved in stochastic sequences, thus they are correctly accounted in a network. Non-exponential distributions can also be efficiently modeled [11][12].

In this paper, a stochastic computational approach is proposed for analyzing the reliability of a two-terminal network, i.e., a network in which information flows from the transmitter to the receiver through intermediate nodes and links. This can also be generalized to other networks with minor modifications [13]. Stochastic models are proposed for imperfect unidirectional and bidirectional links between two nodes, as well as for the imperfect nodes considered in [1]. Non-Bernoulli sequences are used to encode the failure probabilities, and the evaluation accuracy is found to be high at a reasonable sequence length. A stochastic analysis is further performed for modeling information transmission for reliability and criticality assessment. In the sequel, we first present a review of stochastic computation. Then, we present the stochastic models for the imperfect links and nodes respectively. A criticality analysis and an evaluation procedure are then provided; they can be used to improve the performance of a network by utilizing a limited redundancy.

II. Review of Stochastic Computation

Stochastic computation has been proposed in the past for reliable circuit design [14]. In a *stochastic sequence*, a proportional number of bits is set to a specific value; for example, a fixed number of 1's is assigned in a non-Bernoulli sequence to encode a probability. Computations can be efficiently implemented by logic gates; the stochastic sequence at the output encodes the (output) probability. Therefore, Boolean logic operations are transformed into probabilistic computation in the real domain.

In stochastic computation, the number of 1's in the output sequence is not deterministic, but probabilistic due to stochastic fluctuations [10] [11][12]. However, the use of non-Bernoulli sequences (as initial inputs) can greatly reduce the stochastic fluctuation [10]. A longer sequence length is usually required for achieving a higher accuracy. Stochastic logic circuits can handle correlated signals (usually caused by reconvergence of fanout signals), because signal dependencies are maintained and propagated [11][12]. This is useful when analyzing common components in a network.

III. Stochastic Models for Imperfect Links

A link connecting two intermediate nodes is bidirectional, while the link connecting the transmitter or the receiver to an intermediate node is unidirectional. There are two possible states for an imperfect link: operational (fault-free) and disconnected (faulty). Usually, the state of an imperfect link is

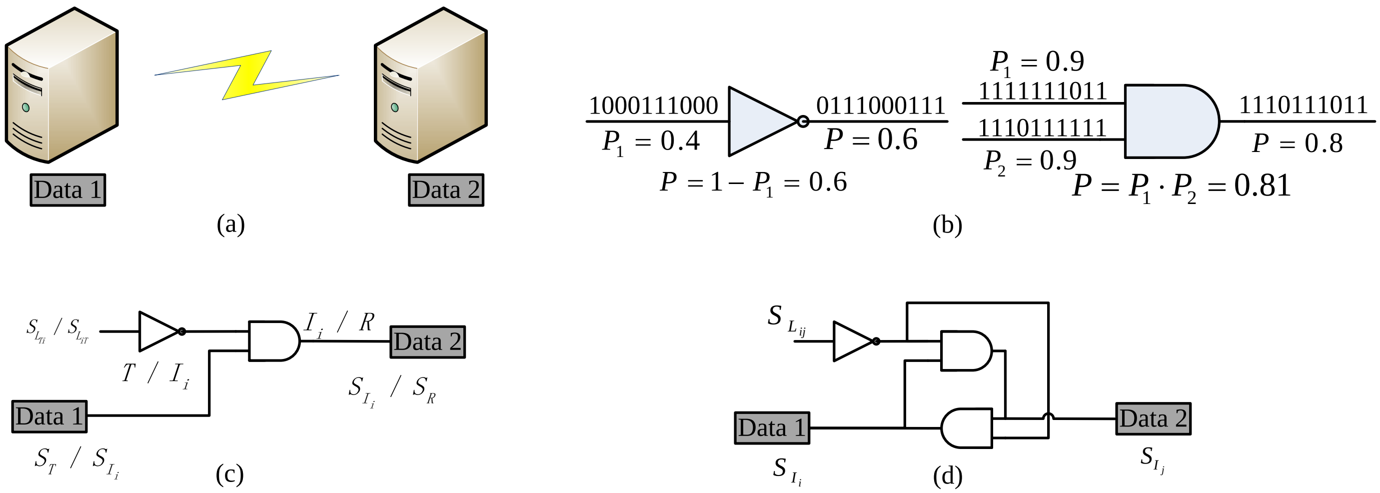

Figure 2. (a) Probabilistic transition between Data 1 and Data 2; let the probability of imperfect link be p. (b) The logic gates used for stochastic computation. (c) A stochastic model for the imperfect unidirectional link from Data 1 to Data 2. The transition can occur from the transmitter T to an intermediate node I_i or from an intermediate node I_i to the receiver R. (d) Stochastic model for an imperfect bidirectional link between two intermediate nodes I_i and I_j.

denoted by a binary variable a, $a \in \{0,1\}$, where 1 or 0 indicates that the link is either faulty (disconnected) or operational (fault-free). The information is passed on by an operational link, i.e., when $a = 0$. In the following analysis, it is also assumed that all imperfect links and nodes fail with known probabilities; the failure probabilities are either fixed or time-dependent (i.e. they vary with the mission time, either exponentially or non-exponentially distributed). Input parameters for evaluating the reliability include network configuration, mission time, and failure parameters or failure probability for each link/node.

In a network, the anticipated information, e.g. the telecommunication data in a wireless network or gas for a gas supply network, is delivered from the transmitter to the receiver. For simplicity, denote the information from the transmitter by 1, which indicates that the transmitter is totally reliable. Then the initial stochastic sequence for the signal probability of the transmitter, i.e., S_T, is a sequence of 1s, i.e., the ith bit of S_T is given by $S_{T,i} = 1$, $i \in \{1, 2, \cdots, L\}$ where L is the length of the stochastic sequence. The reliability is determined by analyzing the stochastic sequence received by the receiver in the network with imperfect links and nodes.

A. A stochastic model for unidirectional links

A unidirectional link usually exists between either the transmitter T and an intermediate node I_i, or an intermediate node I_i and the receiver R (as in the unidirectional transition from Data 1 to Data 2 in Figure 2(a)). For simplicity, denote the unidirectional link between T and I_i by L_{Ti} and the unidirectional link between I_i and the receiver by L_{iR}. As an imperfect link, L_{Ti} fails with a probability p (that can be either fixed or having a value dependent on the mission time), then, the two nodes T and I_i is connected with a probability of $1 - p$. The stochastic model for the unidirectional link is shown in Figure 2(c).

Let $S_{L_{Ti}}$ denote the stochastic sequence generated for the failure probability p of the imperfect link L_{Ti}; then $S_{L_{Ti},j}$ denotes the jth bit of the stochastic sequence $S_{L_{Ti}}$. Furthermore, let $S_{I_i,j}$ denote the jth bit of the stochastic sequence for the reliability of an intermediate node I_i, i.e. S_{I_i}. If $S_{L_{Ti},j} = 1$, the link between the transmitter and the destination node is disconnected. Thus, $S_{I_i,j} = 0$, i.e., the intermediate node I_i receives no information from the transmitter, because the link L_{Ti} is disconnected for the jth trial (or bit). Otherwise, $S_{I_i,j} = S_{T,j}$, i.e., the information can be delivered to node I_i through the fault-free link.

As an imperfect link L_{Ti} fails with probability p, then the probability of the information reliably received by node I_i from the transmitter T is given by $1 - p$. The stochastic model of Figure 2(c) accurately implements the information transmission from transmitter through an imperfect link. A similar analysis can be applied to a unidirectional link between the intermediate node I_i and the receiver R. If the reliability of the imperfect link is provided (instead of the failure probability), then the NOT gate in the stochastic model can be removed, because the reliability is represented as $p' = 1 - p$. This also applies to the bidirectional stochastic model, as presented next.

B. A stochastic model for bidirectional links

A bidirectional link usually exists between two intermediate nodes (unless specific assumptions are made), e.g. I_i and I_j, as shown in Figure 2(a) for a bidirectional transition. The bidirectional link between I_i and I_j is represented by L_{ij}. The stochastic model for the imperfect link is illustrated in Figure 2(d).

$S_{L_{ij}}$ denotes the stochastic sequence generated for the failure probability of the imperfect link L_{ij}. For the kth trial, the state of the imperfect link is denoted by $S_{L_{ij},k}$. If $S_{L_{ij},k} = 1$, then the link L_{ij} is disconnected; hence, the states of the two intermediate nodes I_i and I_j do not affect each other. Otherwise,

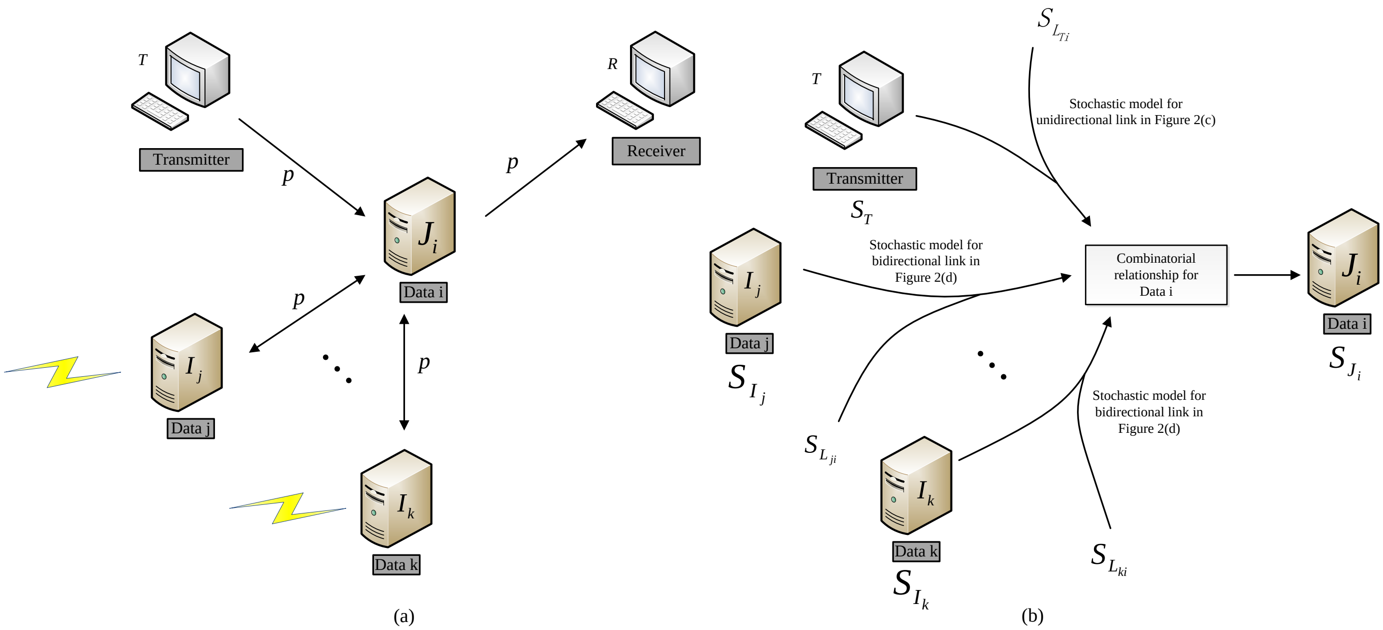

Figure 3. (a) Links connected to the node J_i. (b) A stochastic model for determining the state of J_i. I_j, ⋯, I_k indicate the intermediate nodes connected to J_i, with links denoted as L_{ji}, ⋯, L_{ki} .

$S_{I_i,k} = S_{I_j,k}$. If either I_i or I_j has received the information (indicated by a "1"), then the other node also receives the information through the fault-free link L_{ij}. Given the stochastic sequence $S_{L_{ij}}$ (for the failure probability of the imperfect link L_{ij}), the stochastic model in Figure 2(d) accurately evaluates the reliability of the bidirectional link. For the bidirectional link, there is no order in the transmission of the anticipated information, and this is also the case in the model of Figure 2(d). Hence, the system is considered as stable, unless the stochastic sequences for each node at two adjacent time steps are different.

C. A stochastic model for nodes with multiple links

Multiple links can be connected to a node (Figure 3(a)). If all incoming links to a node J_i (either an intermediate node or receiver) are disconnected, then J_i cannot receive any information. However, if any of the links is connected, i.e., at least for a link connecting I_j and J_i, say, L_{ji}, $S_{L_{ji},j} = 0$, then J_i receives the information once any of the nodes connected to J_i has already received it (I_j can be the transmitter or an intermediate node, i.e., $I_j \in \{S, I_j, \cdots, I_k\}$) for jth trial. The state of the intermediate node J_i is determined by the states of other intermediate nodes connected to J_i. If any of the nodes connected to J_i has already received information (e.g. $S_{I_i,j} = 1$, $I_i \in \{S, I_j, \cdots, I_k\}$) and the link L_{ji} is fault free, i.e., $S_{L_{ji},j} = 0$, then information can be received by J_i, i.e. $S_{J_i,j} = 1$. The relationship in Figure 3(a) can be modeled by an n-input OR gate where n denotes the number of nodes connected to J_i.

Moreover, if J_i is an intermediate node connected to the receiver (R) (Figure 3(a)), then R has no effect on the state of J_i; hence, the connection from J_i to the receiver can be neglected for the purpose of determining the state of node J_i.

IV. Stochastic Models for Imperfect Nodes

In addition to links, nodes can also be imperfect; an analysis of an imperfect node I_d is pursued in this work. There are m incoming links, n outgoing links and h bidirectional links connected to other nodes. A bidirectional link is effectively considered as two unidirectional links.

The imperfect node I_d is further assumed to be divided into two virtual perfect nodes, $I_{d'}$ and $I_{d''}$. The imperfection of a node is therefore implemented by the imperfect unidirectional link, $L_{d'd''}$, between the two virtual nodes. Let $S_{I_{d'}}$ and $S_{I_{d''}}$ be the stochastic sequences encoding the probabilities of a successful information arrival at $I_{d'}$ and $I_{d''}$, respectively. The sequence encoding the failure probability of the imperfect link $L_{d'd''}$ is denoted by $S_{I_{dd''}}$. If p_{I_d} is the probability of the node to be operational, then S_{I_d} is the stochastic sequence for the failure probability of the imperfect virtual unidirectional link between the two nodes. If the ith bit in S_{I_d} is 1, i.e., $S_{I_d,i} = 1$, the link between $I_{d'}$ and $I_{d''}$ is disconnected, then the information is lost after the imperfect node; otherwise, $S_{I_{d'},i} = S_{I_{d''},i}$. Hence, the probabilistic information passing through an imperfect node can be also implemented by the stochastic model for the unidirectional link in Figure 2(c).

The stochastic sequence $S_{I_{d'}}$ consists of 1s and 0s. If $S_{I_{d'},i} = 1$, the node successfully receives the information for the ith trial; otherwise, no information is received. If $S_{I_{dd''},i} = 1$, then the imperfect unidirectional link is faulty and the information cannot be passed to the virtual node; hence, the state of node $I_{d''}$ is 0, i.e., $S_{I_{d''},i} = 0$. If $S_{I_{d'},i} = 0$, irrespective whether the link fails or not, there is no information received, i.e. $S_{I_{d''},i} = 0$. Furthermore, if the imperfect links in/out of the imperfect node I_d are considered, the stochastic models for imperfect links presented previously can be applied.

V. Criticality Analysis

A two-terminal network can be evaluated by using the stochastic models proposed previously for imperfect links and nodes. Catastrophic failures can occur due to externally induced events. Redundancy is often introduced to improve the reliability and guarantee the network to remain operational. When only a limited amount of redundancy can be provided, it is important to determine the most critical links. In this manuscript, the reliability of an imperfect network without external catastrophic (i.e., deterministic) failures is considered as a reference. *Criticality* of a link is defined as the reliability difference of an imperfect two-terminal network with a set of failure parameters, when that link works with a predefined failure probability and fails deterministically (e.g. due to a catastrophic failure). If multiple network components fail at the same time (so there is a common cause failure), this scenario can be readily taken into account by the proposed stochastic models.

A stochastic model can be constructed using the stochastic models presented in previous sections to analyze the criticality of a link, e.g., L_i, in the network. S_{L_i} encodes the failure probability of the imperfect link L_i not affected by a catastrophic failure, while S'_{L_i} encodes the failure probability of L_i when it is affected by a catastrophic error. Due to the deterministic nature of a catastrophic failure, S'_{L_i} is a sequence of 1s. For the stochastic two-terminal network at time t, the stochastic sequences obtained by the receiver under these two failure scenarios of L_i are given by S_R and S'_R respectively. An XOR gate is utilized to measure the difference in these two sequences, this is denoted by ΔS_R. The *criticality* of L_i is then encoded in ΔS_R. This process can be applied to other links to find the most critical link to ensure the functionality of the two-terminal network.

The process of evaluating the reliability of a two-terminal network (with an analysis of criticality) is shown as follows:

(1) Determine failure probabilities of the imperfect links and nodes at the specified mission time point based on the provided failure parameters and distributions;

(2) Generate the non-Bernoulli sequences for the different failure probabilities of the links and nodes;

(3) For unidirectional or bidirectional links, the proposed stochastic models presented previously are applied to build the stochastic model;

(4) If more than one link are connected to a node, the stochastic OR gate model is applied;

(5) If an imperfect node is considered, then the stochastic model for the imperfect node is applied;

(6) Generate a stochastic sequence (consisting of 1s) for the transmitter and propagate the sequence through the network (made of stochastic logic gates);

(7) Calculate the probability of the information obtained by the receiver; then the reliability of the network is determined;

(8) By varying the failure probability of a specific link or node for the mission time, the criticality of each link or node in the network reliability is found by analyzing the stochastic sequence $\Delta S_R(t)$ obtained.

VI. Analysis and applications

The stochastic analysis is performed for an imperfect bridge network. The network [15] consists of four nodes (2 intermediate nodes, A and B; a transmitter T, a receiver R) (Figure 4). Initially, the nodes are assumed to be perfect, while each link fails with a fixed probability $p_i = 0.1$. The failures of different links are assumed to be mutually independent; then, the reliability of the links is given as $r_i = 1 - p_i = 0.9$, $i \in \{1, 2, \cdots, 5\}$. As in [15], the algebraic expression for the reliability of this network is given by $R_S = r_5(r_1 + r_2 - r_1 r_2)(r_3 + r_4 - r_3 r_4) + (1 - r_5)(r_1 r_3 + r_2 r_4 - r_1 r_2 r_3 r_4)$, where R_S denotes the system reliability; r_i denotes the link reliability, $i \in \{1, 2, \cdots, 5\}$. The exact reliability is calculated as 0.9785. While the accurate analytical expression can be derived here, the required computational complexity increases exponentially with the number of connections among nodes and the scale of a network. It becomes difficult, if not impossible, to perform an accurate analysis for large networks.

The stochastic structure of the bridge network in Figure 4 can be constructed with the application of the stochastic models for imperfect links presented in Figure 2(c) and (d). Here, the stochastic sequences for the failure probabilities of links L_{TA}, L_{TB}, L_{AB}, L_{AR} and L_{BR} are denoted as $S_{L_{TA}}$, $S_{L_{TB}}$, $S_{L_{AB}}$, $S_{L_{AR}}$ and $S_{L_{BR}}$ respectively; while S_T and S_R denote the information sequences sent by the transmitter T and received by the receiver R respectively. Then, a stochastic analysis can be performed by propagating the stochastic sequences through the constructed stochastic model. The mean and the variance of the network reliability found using a stochastic analysis with 30 simulations are given in Table 1 for different sequence lengths. The mean and variance of the average run time are also provided to show the efficiency of the proposed analysis.

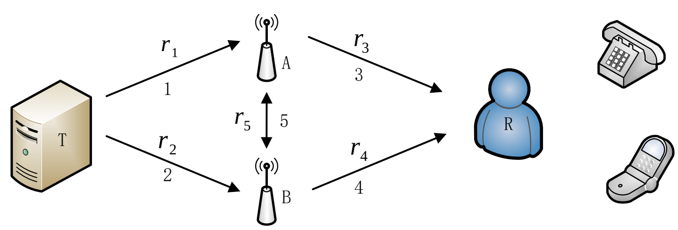

Figure 4. A bridge network [15].

As shown in Table 1, the accuracy of the stochastic approach is affected by the sequence length. A more accurate result can be obtained by increasing the sequence length. However, a longer run time is also incurred, because longer stochastic sequences must be generated to represent the signal probabilities. Hence, the stochastic sequence length is determined by a tradeoff between accuracy and efficiency. Nevertheless, with a reasonable sequence length, the stochastic approach provides a relatively accurate estimate of the reliability of a two-terminal network. The precision of the stochastic analysis is affected by: (1) failure probabilities of imperfect nodes/links and the inherent random fluctuations, i.e., permutations of 1s, in the sequences; (2) the numbers of imperfect links/nodes and the network topology. As in [10], *quantization error* is incurred when converting a probability into a stochastic sequence; however, *quantization error* can be avoided if using an appropriate sequence length to encode the probabilities. For instance, for a probability of 0.001, a sequence length of 1000 bits is sufficient to avoid *quantization error*. Furthermore, due to the existence of a limited resolution, a *resolution error* is incurred in the process of stochastic computation; hence, a minimal sequence length should be determined by the provided signal probabilities. For instance, in order to encode a probability of 0.01, at least a sequence length of 100 bits should be used. Any probability with a precision higher than that of 0.01 cannot be represented by a sequence length of 100 bits. Let ϵ denote the resolution requirement and N_g indicate the number of gates in a network, a stochastic sequence with a length $L \geq N_g/\epsilon$ is usually sufficient [10]. Although the accuracy of an analysis is affected by the network topology, the number of nodes, the number of imperfect links and so on, for a network with thousands of gates, a sequence length of 1000k bits is usually able to meet the precision requirement of 0.01. Thus in practice, a shorter sequence length is often utilized to produce a result with acceptable accuracy.

Table 1 Mean and variance for the bridge network's reliability obtained by the stochastic approach.

Stochastic computation				
Sequence length (L)	Reliability		Average run time (s)	
	Mean	Variance	Mean	Variance
1k	0.978300	0.000417	0.000368	0.000957
10k	0.978530	0.002483	0.002001	0.001160
100k	0.978502	0.002294	0.016803	0.005379

To assess criticality, link j is considered with a failure probability that varies with the mission time t. Assume that the failure of link j is exponentially distributed; its probability density function (*pdf*) and cumulative density function (*cdf*) are $f(t) = \lambda\, e^{-\lambda t}$ and $F(t) = \int_0^t f(t)\, dt = 1 - e^{-\lambda t}$ respectively, where λ is the (constant) failure rate of link j for an exponential distribution. Let $t = 100$ hours, $\lambda = 0.008$ and $L =$ 100,000 bits. The failure probabilities of the other links are kept constant at 0.2; the reliability for the bridge network from T to R is shown in Figure 5.

Table 2 Different failure scenarios analyzed for the bridge network. p_i denotes the failure probability of link i, $i \in \{1, 2, 3, 4, 5\}$.

case 1	$p_i = 0.2$,
case 2	the failure of link 1 is exponentially distributed; $p_i = 0.2$, $i \neq 1$
case 3	the failure of link 2 is exponentially distributed; $p_i = 0.2$, $i \neq 2$
case 4	the failure of link 3 is exponentially distributed; $p_i = 0.2$, $i \neq 3$
case 5	the failure of link 4 is exponentially distributed; $p_i = 0.2$, $i \neq 4$
case 6	the failure of link 5 is exponentially distributed; $p_i = 0.2$, $i \neq 5$

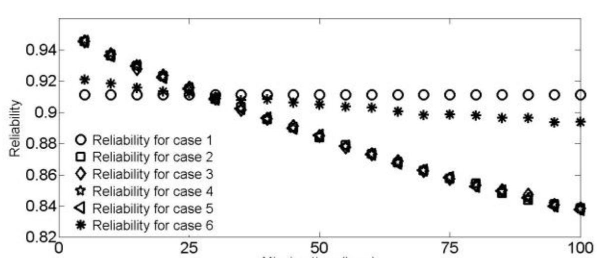

Figure 5. Reliability by varying the failure probability of different links by the proposed stochastic approach (sequence length L = 100,000 bits). The failure scenarios are illustrated in Table 2.

If the failure probability of link j, $j \in \{1, 2, 3, 4, 5\}$, is changed, then the reliability varies (Figure 5). Links i, $i \in \{1, 2, 3, 4\}$ have the same criticality on the reliability of the bridge network. Link 5 is the least critical because the reliability change is the smallest, as also found by the comparison of the reliabilities for case 1 and case 6.

As shown in the simulation results, the inaccuracy decreases with an increase of sequence length. In general, the use of the type of stochastic sequences remains a key issue to be investigated, because a different type of sequences such as low-discrepancy sequences may result in a shorter length for achieving a specific accuracy, thus significantly improving the efficiency of stochastic computation.

VII. CONCLUSION

Reliability of a network is of great importance. The rapid increase in network complexity causes substantial difficulty in evaluating its reliability when communication is required between a transmitter and a receiver through intermediate nodes and links in a two-terminal network. In this paper, a stochastic computational approach is proposed to efficiently investigate the reliability of such general two-terminal networks. Both imperfect links and nodes have been considered by arranging the failure probabilities with values either fixed or varying with the mission time. The imperfect links, either unidirectional or bidirectional, have been modeled stochastically for the process of information transmission by utilizing a combination of logic gates. Non-Bernoulli sequences have been used to improve the computational efficiency and accuracy of the stochastic approach. The imperfect nodes can be effectively modeled by the proposed stochastic model for unidirectional imperfect links. Hence, the stochastic approach can be used to evaluate a general two-terminal network under any failure distribution.

It has been shown that the reliability of a two-terminal network decreases with an external failure. Moreover, the reliability of the network varies if the external failure affects different links. Hence, the *criticality* of different links is analyzed using the proposed stochastic approach for improving the reliability of a two-terminal network by applying redundancy for those critical links. In the future, transmission of multiple signals through networks with multiple transmitters and receivers will be investigated using a stochastic analysis.

REFERENCES

[1] K.K. Aggarwal, J.S. Gupta and K.B. Misra, "A simple method for reliability evaluation of a communication system," IEEE Trans. Communications, vol. 23, no. 5, 1975, pp. 563-566.

[2] J. Andrews and T. Moss, "Reliability and Risk Assessment," Essex, U.K.: Longman Scientific and Technical, 1993.

[3] J. Li, "Lifeline Earthquake Engineering-basic Methods and Applications," Beijing: Science Press, 2005.

[4] L. Fratta and U. G. Montanari, "A Boolean Algebra Method for Computing the Terminal Reliability in Communication Network," IEEE Trans. Circuit Theory, vol. CT-20, no. 3, 1973, pp. 203–211.

[5] S. Tsukiyama, I. Shirakawa, H. Ozaki and H. Ariyoshi, "An Algorithm to Enumerate All Cut Sets of a Graph in Linear Time per Cutset," Journal of the Association for Computing Machinery, vol. 27, no. 4, 1980, pp. 619–632.

[6] W. Liu, and J. Li, "An improved cut-based recursive decomposition algorithm for reliability analysis of networks," Earthquake Engineering and Engineering Vibration, vol. 11, no. 1, 2012, pp. 1–10.
[7] C. Tanguy, "Exact two-terminal reliability of some directed networks," in Proc. Design and Reliable Communication Networks (DRCN), La Rochelle, France, 2007, pp. 155–162.
[8] L. D. Xing, "An efficient binary-decision-diagram-based approach for network reliability and sensitivity analysis," IEEE Trans. Syst., Man, Cybern. A, Syst., Humans, vol. 38, no. 1, 2008, pp. 105–115.
[9] Y. R. Chang, S. V. Amari, and S. Y. Kuo, "OBDD-based evaluation of reliability and importance measures for multistate systems subject to imperfect fault coverage," IEEE Trans. Dependable and Secure Computing, vol. 2, no. 4, 2005, pp. 336-347,.
[10] J. Han *et al*, "A Stochastic Computational Approach for Accurate and Efficient Reliability Evaluation," IEEE Trans. Computers, vol. 63, no. 6, 2014, pp. 1336-1350.
[11] P. Zhu *et al*, "A Stochastic Approach for the Analysis of Fault Trees with Priority AND Gates," IEEE Trans. Reliability, vol. 63, no. 2, 2014, pp. 480-494.
[12] P. Zhu *et al*, "A Stochastic Approach for the Analysis of Dynamic Fault Trees with Spare Gates under Probabilistic Common Cause Failures," IEEE Trans. Reliability, vol. 64, no. 3, 2015, pp. 878-892.
[13] H. Cancela, F. Robledo, G. Rubino, and P. Sartor, "Monte Carlo estimation of diameter constrained network reliability conditioned by pathsets and cutsets," Computer Communications, vol. 36, no. 6, 2013, pp. 611-620.
[14] B. R. Gaines, "Stochastic Computing Systems," Advances in Information Systems Science, 2: 37-172, 1969.
[15] G. S. Mahapatra, and P. Roy, "A Genetic Algorithm Approach for Reliability of Bridge Network in Fuzzy System," Journal of Information and Computing Science, 6.4, 2011, pp. 243-254.