Modeling Uncertain System Resilience with CTMCs

Nathan Jarus
Department of Computer Science
Missouri University of Science and Technology
Email: nmjxv3@mst.edu

***Abstract*—System resilience, the ability of a system to recover from failure, is a metric of growing importance in complex system analysis. We develop a Continuous Time Markov Chain (CTMC) model for individual component resilience. From this, we develop methods for composing these models into models of system resilience, allowing us to derive models for more complex systems without excessively complex models. Finally, we consider the behavoir of system resilience without perfect knowledge of all individual components' state. We derive resilience bounds for some systems, considering both independent and interdependent components.**

I. Introduction

Resilience is an important attribute of large-scale system performance. It can be seen as a non-binary availability measure; instead of the system only being 'up' or 'down', it is a continuous measure of performance. As such, it is essential to evaluating the architecture of complex systems and their failure mitigation and recovery techinques.

While there are several specific definitions of resilience, this paper will follow Laprie [] and Simonici's [] definition that resilience is the persistence of service delivery that can be justifiably trusted when the system experiences changes. Within our scope, we consider changes as component degradation and failure, but changes can include increased demand, system reconfiguration, or natural disasters, amongst others.

Most work on resilience has focused on modeling specific systems or provided qualitative measurement procedures. However, these studies do not provide much in the way of quantitative results for general system designs. They also require building a complete model of the system, which can be complicated and thus error-prone for large systems.

All resilience measurement depends on measures of interest for the system being studied. These measures of interest represent some attribute of the system or one of its components as a means of measuring system performance. However, it is difficult to choose one measure of interest that is sufficient to measure total system resilience for a complex system with many potential failure modes. As well, composing multiple measures of interest into a system-wide measure remains an open problem.

This paper makes three main research contributions:

1) A model for individual system component resilience
2) A methodology for composing these component models to derive total system resilience
3) A methodology for bounding system resilience in the case that not all component resiliences are known

II. Related Work

Trivedi et. al describe resilience and its relationship with other dependability metrics such as availability, reliability, and performability in [1]. They present several definitions of resilience and build some models that show how availability, performability, and survivability show changes in resilience as the system parameters are changed. They extend these models in [2] with state-space and non-state-space models of reliability for an emergency cooling system for a boiling water nulcear reactor and performability and availability models for a telephone switching system. All of these models are concerned with transient system behavior as the system undergoes changes.

Henry and Ramirez-Marquez introduce the concept of figures of merit (alternatively, measures of interest) [3]. They define resilience as the amount of service recovered after a degradation of service. In this model, the system begins at some initial level of functionality, experiences a disruption, spends some time in the disrupted state, then is recovered to a final state that may or may not be the same as the initial state. Furthermore, they quantify recovery time and cost, providing a basis for comparing recovery actions.

Performability bears a close resemblance to resilience, but they differ in that resilience considers the ability of a system to be repaired or to recover from degradation. Meyer formulates performability as a combination of performance and reliability; that is, the ability of the system to continue performing a task even when its capability is reduced [4]. It also uses measures of interest to measure the capability of the modeled system. Meyer develops a hierarchical system model and discusses the difficulties involved in solving it. Smith and Trivedi develop a Markov Reward Model (MRM) for multiprocessor system performability in [5]. They observe changes in system performability as utilization is increased. They also develop an algorithm for solving MRMs to calculate accumulated reward.

III. Methodology

We begin with a CTMC model of component resilience as seen in Figure 1. Each state represents a level of component service capability; continuous capability values can be bucketed into discrete states for the purposes of this model. These capability measures can be generalized to any component measure of interest. From each state it is possible for the component to fail to the next lowest service level with rate λ_i and to be repaired to complete functionality with rate μ_i. Since the resulting CTMC is finite and irreducible, it has constant

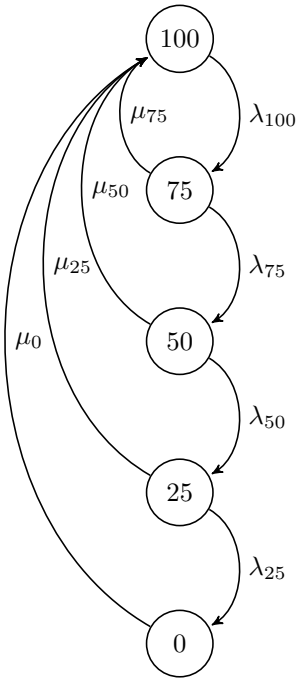

Fig. 1. Single Component Resilience Model

steady-state probabilities v which represent the percentage of time the component will deliver the service level specified by that state. We define the expected steady-state service level as the resilience of the component, that is,

$$R = \sum_{i \in S} i * v_i \tag{1}$$

To make use of this component model, we must be able to compose it into a model for a complete system. Within the scope of this paper we will consider some simple multiple-component systems. Consider a parallel two-component system. For the moment, assume that the components in the system behave independently. If we let R_1 and R_2 be the resilience of the subcomponents, it can be shown that the system resilience $R = R_1 + R_2$:

$$R = \sum_{(i,j) \in S_1 \times S_2} (i+j) * v_{1_i} * v_{2_j} = \sum_{i \in S_1} i * v_{1_i} + \sum_{j \in S_2} j * v_{2_j} = R_1 + R_2 \tag{2}$$

By similar argument, for a series two-component system, $R = min\{R_1, R_2\}$.

These equations can be composed to measure the resilience of series-parallel and parallel-series systems:

$$R_{SP} = min\{R_{P1}, R_{P2}\} = min\{R_{P1_1} + R_{P1_2}, R_{P2_1} + R_{P2_2}\} \tag{3}$$

$$R_{PS} = R_{S1} + R_{S2} = min\{R_{S1_1}, R_{S1_2}\} + min\{R_{S2_1}, R_{S2_2}\} \tag{4}$$

Until this point, we have assumed perfect knowledge of each system component's behavior. In practice, this is not always attainable for various reasons: it may be economically infeasible to install measurement devices on every component; system models may be constructed from incomplete data; or the paper authors may be seeking an excercise in masochism. In our models, we can represent this lack of knowledge as not knowing the state of one of the components. Let us consider the resilience of two-component systems where we have knowledge of only one component's state. For a parallel system, we can say

$$R = max\{R_K, R_K + R_U\} \tag{5}$$

where R_K is the reliability of the known component and R_U is the reliability of the unknown component. This places a lower bound on R of R_K. Likewise, for a series system,

$$R = min\{R_K, min\{R_K, R_U\}\} \tag{6}$$

placing an upper bound on R of R_U.

While considering components to be independent simplifies the analysis, in practice, many systems have interdependencies between components. For example, in a power grid with two parallel transmission lines, a failure of one line may result in excessive current draw on the other, causing it to fail as well. We can take advantage of this interdependence to provide even tighter bounds on system resilience. In order to encode this information, we will borrow theory from Hidden Markov Models and Partially Observable Markov Decision Processes. The state distribution X of our unknown component can be modeled as a function f of two random variables U and Y. U is the unknown distribution of the component itself and Y is a known distribution from some source external to the unknown component. X can be seen as describing a family of CTMCs where each member of the family is obtainable by fixing Y to some set value. It is not necessary for us to specify f for every possible input value to derive useful information from this model.

Consider the case of a parallel two-component system. Here, Y will be the state distribution of the known component. If we know that degradation of the known component will cause degradation in the unknown component, the rate at which the known component leaves the 'perfect' state is 1 when the second component is not in the 'perfect' state. In Figure 1, state 100 is the 'perfect' state.

Let M_U be the maximum capability acheivable by the unknown component when the known component is degraded. Combined with our previous result, we can bound the resilience of the system when the known component is degraded above and below:

$$R_K < R < R_K + M_U \tag{7}$$

We can also see that in order to restore the whole system to functionality, we must repair the known component before the unknown component; otherwise, the unknown component will fail again immediately after repair.

IV. Conclusions and Future Work

In this work, we developed a model for individual component resilience. Based on this model, we derived expressions for system resilience for several basic systems. This provides a method for deriving complex system models from simpler component models which abstracts component complexity from system complexity.

Furthermore, we considered the role of uncertain system state in calculating system resilience, both for independent and interdependent components. In order to express interdependence, we developed a method for combining known and unknown information about a component's state into its model. We saw that interdependence can allow us a stricter bound on system resilience than a simpler independent component model. Interdependence also allows us to optimize recovery techniques for a degraded or failed system.

This work can be extended in several directions. The system modeling technique must be expanded to include non series-parallel systems; this could perhaps be done with a Hierarchical Markov Model. Extending the component model to continuous measures of interest will allow for more detailed system resilience calculations. System recovery methods could be modeled with a Markov Decision Process, allowing us to rank recovery methods. Bounds on system resilience could be used to determine which components are most essential to the system and which measures of interest provide the most detail, allowing us to optimize failure mitigation strategies and system monitoring efforts. Finally, as both Hidden Markov Models and Partially Observable Markov Decision Processes have extensive roots in machine learning, real-world data could be used to learn resilience models for complex systems.

References

[1] K. S. Trivedi, D. S. Kim, and R. Ghosh, "Resilience in computer systems and networks," in *Proceedings of the 2009 International Conference on Computer-Aided Design*, pp. 74–77, ACM, 2009.

[2] R. Ghosh, D. Kim, and K. S. Trivedi, "System resiliency quantification using non-state-space and state-space analytic models," *Reliability Engineering & System Safety*, vol. 116, pp. 109–125, 2013.

[3] D. Henry and J. Emmanuel Ramirez-Marquez, "Generic metrics and quantitative approaches for system resilience as a function of time," *Reliability Engineering & System Safety*, vol. 99, pp. 114–122, 2012.

[4] J. F. Meyer, "On evaluating the performability of degradable computing systems," *Computers, IEEE Transactions on*, vol. 100, no. 8, pp. 720–731, 1980.

[5] R. Smith, K. S. Trivedi, and A. Ramesh, "Performability analysis: measures, an algorithm, and a case study," *Computers, IEEE Transactions on*, vol. 37, no. 4, pp. 406–417, 1988.