International Journal for Modern Trends in Science and Technology, 8(09): 162-166, 2022

ISSN: 2455-3778 online
DOI: https://doi.org/10.46501/IJMTST0809034
Available online at: http://www.ijmtst.com/vol8issue09.html

Stochastic Model Predicting Component Failures using JAVA

P. Somasundar Reddy[1] | B. N. Srinivasa Gupta[2]

[1]PG Scholar, Department of Computer Science, SVKP &Dr K S Raju Arts & Science College(A), Penugonda, W.G.Dt., A.P, India
[2]Associate Professor in Computer science, SVKP &Dr K S Raju Arts & Science College(A), Penugonda, W.G.Dt., A.P, India

To Cite this Article
P. Somasundar Reddy and B. N. Srinivasa Gupta. Stochastic Model Predicting Component Failures using JAVA. International Journal for Modern Trends in Science and Technology 2022, 8(09), pp. 162-166. https://doi.org/10.46501/IJMTST0809034

Article Info
Received: 22 August 2022; Accepted: 12 September 2022; Published: 17 September 2022.

ABSTRACT

When a component fails in a critical telecommunications service, how urgent is the repair? How does repair within 1, 2, or n hours affect the probability of service outage? Formal model can help with impact assessment, prioritization, planning repairs in the event of component failure, and predicting maintenance costs? These are some of the questions asked by large organizations. Here we develop probabilistic frameworks based on discrete space models and temporal logic and report our experience in answering them. It defines and studies both steady-state and transient standard logical properties related to the probability of service outages within specified time limits, predicts maintenance costs, and introduces the new concept of operational domains. Service Availability. The resulting models are highly parameterized and user interaction for experimentation is supported through a lightweight web-based interface.

1. INTRODUCTION

We report our experience developing probabilistic models and temporal logic analysis to support the management of critical telecommunications services deployed in large organizations. Services are key to most safety-critical systems, so they must always operate while accepting the risk of failure. The components of the service are hierarchical with multiple levels of redundancy. The service operates continuously and individual component failures are monitored and recorded. Most likely the service is in a degraded configuration. H. A configuration in which a component has failed, but the service continues to operate due to redundancy. The time and cost of repairing a component depends on many factors, including the nature of the failure and physical distance and access to the component (many components are physically remote).

The development of model-based methods for quantitatively evaluating the reliability of computer systems has a long and rich history. A wide range of model-based evaluation techniques are now available, from combinatorial techniques that are useful for quick and coarse analysis, to state-based techniques such as Markov reward models, to detailed discrete-event simulations.

The use of quantitative safety assessment techniques is less common and usually takes the form of formal analysis of small portions of the overall design or

experimental red team-based approaches. We argue that much can be gained from developing a robust model-based methodology for quantifying the safety that can be expected from a given design. We examine existing model-based techniques for assessing the reliability of systems and summarize how they are currently extended to assess system security. We have found that many techniques of trustworthiness assessment can be applied to security, but mainly between the random nature of failures commonly assumed in trustworthiness assessments and the intentional, human nature of cyber-attacks.

2. LITERATURE SURVEY

"Model-based evaluation: from dependability to security,"

The development of techniques for quantitative, model-based evaluation of computer system dependability has a long and rich history. A wide array of model-based evaluation techniques is now available, ranging from combinatorial methods, which are useful for quick, rough-cut analyses, to state-based methods, such as Markov reward models, and detailed, discrete-event simulation. The use of quantitative techniques for security evaluation is much less common, and has typically taken the form of formal analysis of small parts of an overall design, or experimental red team-based approaches. Alone, neither of these approaches is fully satisfactory, and we argue that there is much to be gained through the development of a sound model-based methodology for quantifying the security one can expect from a particular design. In this work, we survey existing model-based techniques for evaluating system dependability, and summarize how they are now being extended to evaluate system security. We find that many techniques from dependability evaluation can be applied in the security domain, but that significant challenges remain, largely due to fundamental differences between the accidental nature of the faults commonly assumed in dependability evaluation, and the intentional, human nature of cyber attacks.

"The Probabilistic Model Checking Landscape,"

Randomization is a key element in sequential and distributed computing. Reasoning about randomized algorithms is highly non-trivial. In the 1980s, this initiated first proof methods, logics, and model-checking algorithms. The field of probabilistic verification has developed considerably since then. This paper surveys the algorithmic verification of probabilistic models, in particular probabilistic model checking. We provide an informal account of the main models, the underlying algorithms, applications from reliability and dependability analysis-and beyond and describe recent developments towards automated parameter synthesis

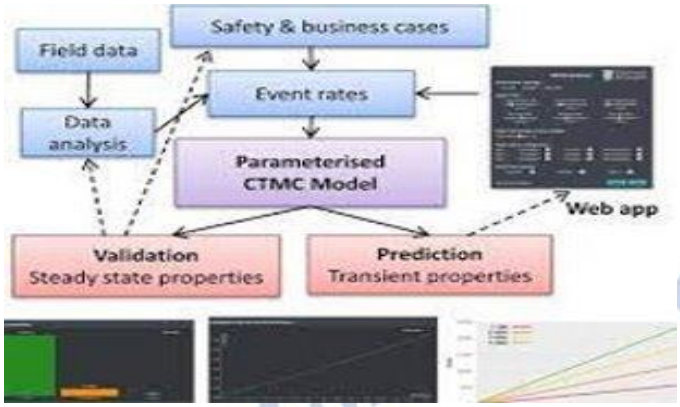
3. PROBLEM STATEMENT:

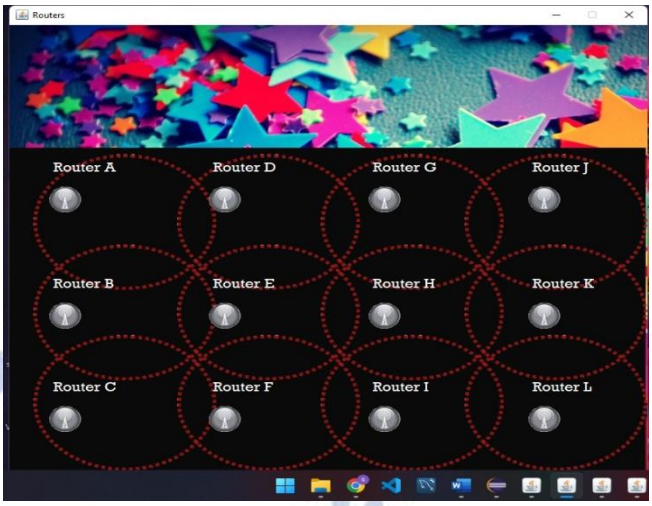
Our framework is based on treating each component as a separate process with events representing failures, repairs, etc. The entire system is a simultaneous composition of all components synchronized to a common event. The underlying model is a continuous-time Markov chain, since the passage of time is modeled continuously. H. State space is discrete, but time is continuous. Modeling component-based systems is standard in CTMC, but is modeled at a higher level using the PRISM (for reactive systems) language. This allows you to elegantly treat components as modules, events as protected commands, and levels of hierarchy as modular constructs. The properties we consider are probabilistic, such as the probability of service failure and a new concept called behavioral envelope that quantifies the impact of different combinations of states of lower-level components on service availability.

Disadvantages:

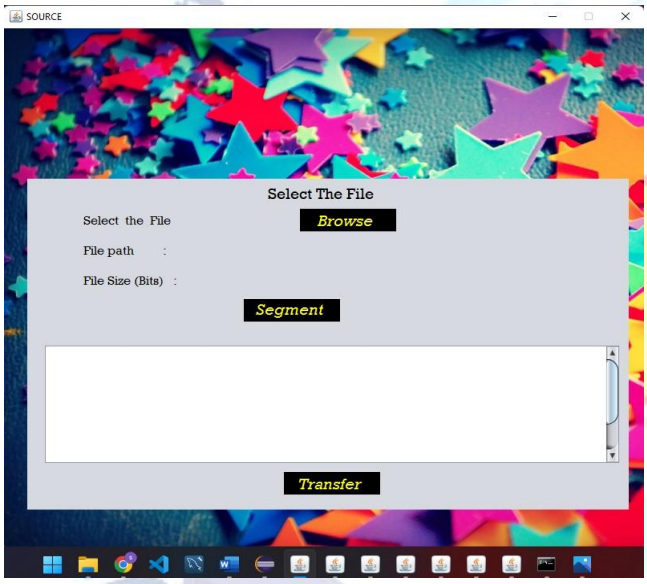
- Modeling reliability analysis using CTMC is well known, but it was not an obvious solution to the problem originally posed.
- We had to work with engineers to uncover the probabilistic nature of the errors required by the model and modeling approach. Modeling reliability analysis using CTMC is well known, but it was not an obvious solution to the problem originally posed.

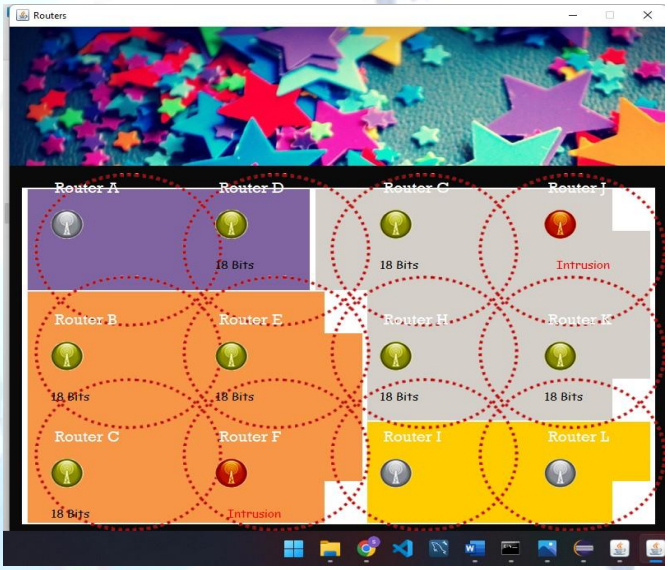
4. ARCHITECTURE:

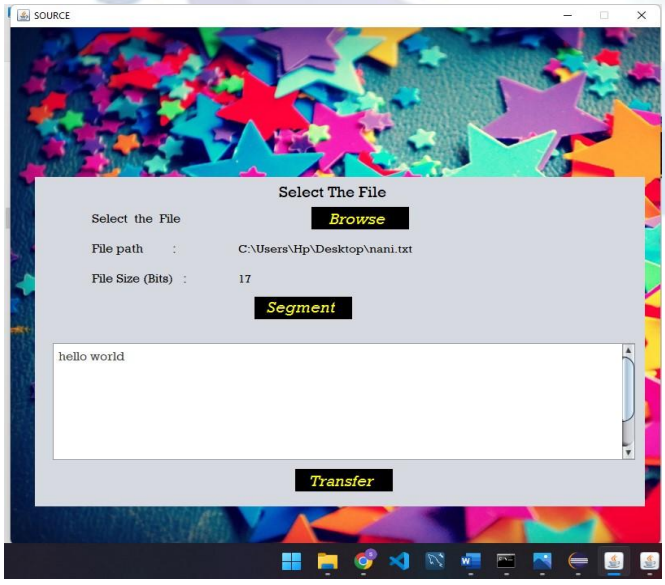


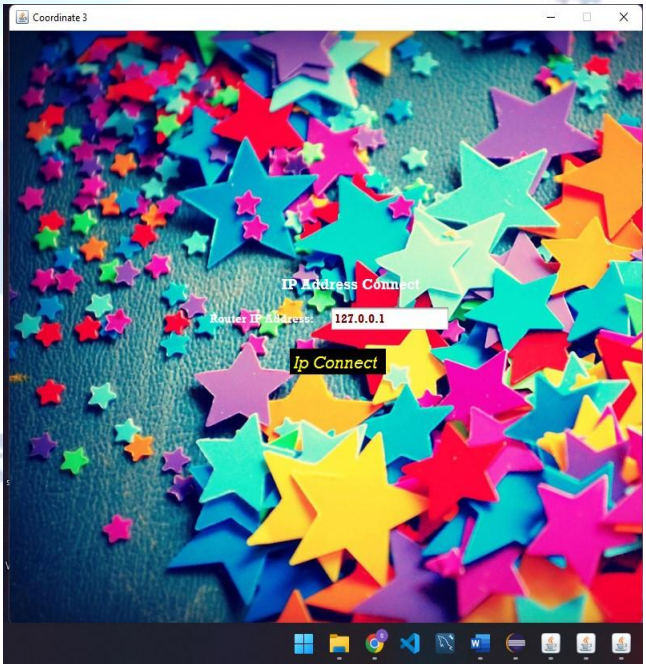


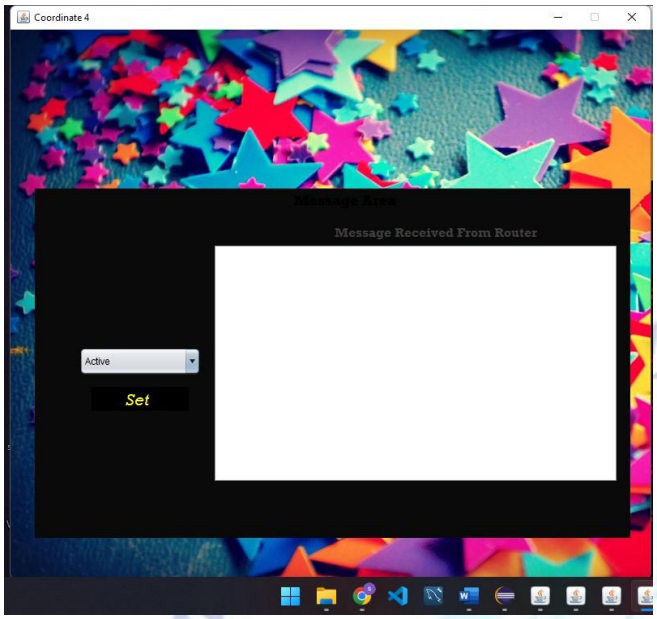
5. RESULT:

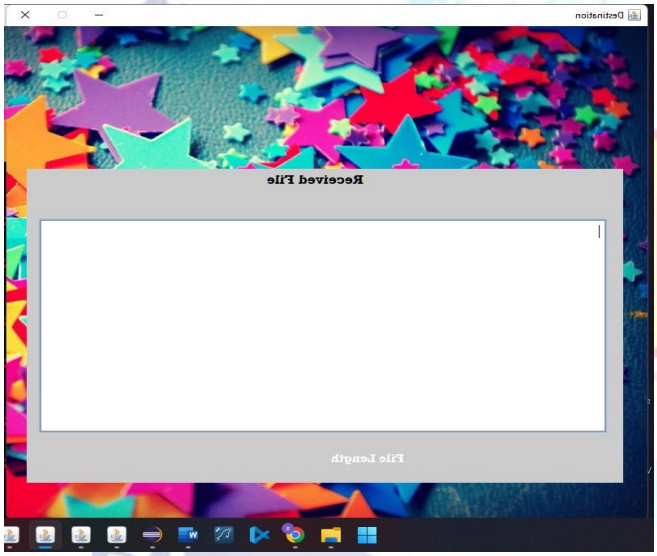


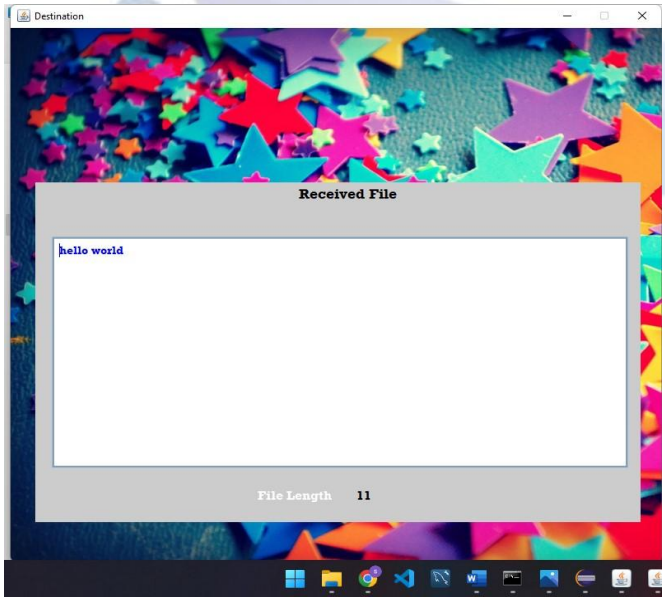












6. CONCLUSION:

We presented a probabilistic framework that supports decision-making in the event of component failure, and our experience applying it to critical communication services deployed in large organizations. Typical questions it helps address are: For the system we are considering, this includes answering questions such as: Given a particular degraded configuration, how likely is it that the system will become insecure at a given future time period and security threshold? This is not an obvious solution to the problem originally posed was. What is new in our contribution is that rather than textbook analysis and simulation, we used CTMC as a model and used probabilistic temporal logic CSL to answer the question. We also defined and applied a new concept of motion envelopes. This allows you to map the effects (best/worst) of lower-level component states to higher-level component properties.

Conflict of interest statement

Authors declare that they do not have any conflict of interest.

REFERENCES

[1] User Interfaces in C#: Windows Forms and Custom Controls by Matthew MacDonald.

[2] Applied Microsoft® .NET Framework Programming (Pro-Developer) by Jeffrey Richter.

[3] Practical .Net2 and C#2: Harness the Platform, the Language, and the Framework by Patrick Smacchia.

[4] Data Communications and Networking, by Behrouz A Forouzan.

[5] Computer Networking: A Top-Down Approach, by James F. Kurose.

[6] Operating System Concepts, by Abraham Silberschatz.

[7] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. H. Katz, A. Konwinski, G. Lee, D. A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "Above the clouds: A berkeley view of cloud computing," University of California, Berkeley, Tech. Rep. USB-EECS-2009-28, Feb 2009.

[8] "The apache cassandra project," http://cassandra.apache.org/.

[9] L. Lamport, "The part-time parliament," ACM Transactions on Computer Systems, vol. 16, pp. 133–169, 1998.

[10] N. Bonvin, T. G. Papaioannou, and K. Aberer, "Cost-efficient and differentiated data availability guarantees in data clouds," in Proc. of the ICDE, Long Beach, CA, USA, 2010.

[11] O. Regev and N. Nisan, "The popcorn market. online markets for computational resources," Decision Support Systems, vol. 28, no. 1-2, pp. 177 – 189, 2000.

[12] A.Helsinger and T. Wright, "Cougaar: A robust configurable multi agent platform," in Proc. of the IEEE Aerospace Conference, 2005.

[13] J. Brunelle, P. Hurst, J. Huth, L. Kang, C. Ng, D. C. Parkes, M. Seltzer, J. Shank, and S. Youssef, "Egg: an extensible and

economics-inspired open grid computing platform," in Proc. of the GECON, Singapore, May 2006.
[14] J. Norris, K. Coleman, A. Fox, and G. Candea, "Oncall: Defeating spikes with a free-market application cluster," in Proc. of the International Conference on Autonomic Computing, New York, NY, USA, May 2004.
[15] C. Pautasso, T. Heinis, and G. Alonso, "Autonomic resource provisioning for software business processes," Information and Software Technology, vol. 49, pp. 65–80, 2007.
[16] A.Dan, D. Davis, R. Kearney, A. Keller, R. King, D. Kuebler, H. Ludwig, M. Polan, M. Spreitzer, and A. Youssef, "Web services on demand: Wsla-driven automated management," IBM Syst. J., vol. 43, no. 1, pp. 136–158, 2004.
[17] M. Wang and T. Suda, "The bio-networking architecture: a biologically inspired approach to the design of scalable, adaptive, and survivable/available network applications," in Proc. of the IEEE Symposium on Applications and the Internet, 2001.
[18] N. Laranjeiro and M. Vieira, "Towards fault tolerance in web services compositions," in Proc. of the workshop on engineering fault tolerant systems, New York, NY, USA, 2007.
[19] C. Engelmann, S. L. Scott, C. Leangsuksun, and X. He, "Transparent symmetric active/active replication for servicelevel high availability," in Proc. of the CCGrid, 2007.
[20] J. Salas, F. Perez-Sorrosal, n.-M. M. Pati and R. Jim´enez- Peris, "Ws-replication: a framework for highly available web services," in Proc. of the WWW, New York, NY, USA, 2006,

Authors Biography

P.Somasundar Reddy currently pursuing MCA in SVKP & Dr K.S Raju Arts & Science College affiliated to AdikaviNannayaUniversity, Rajamahendravaram. His research interests include Data Structures, WebTechnologies, OperatingSystems and Artificial Inteligence.

B.N.Srinivasa Gupta is working as Associate Professor in SVKP &Dr K S Raju Arts & Science College, Penugonda, A.P. He received Masters Degree in Computer Applications from Andhra University and Computer Science & Engineering from Jawaharlal Nehru Technological University Kakinada (JNTUK),Kakinada, India. His research interests include Data Mining, Cyber Security, Artificial Intelligence