Venkatasubramanian, V, Malik, T, Giridhar, A, Villez, K, Prasad, R, Shukla, A, Rieger, C, Daum, K, McQueen, M (2010). RNEDE: Resilient network design environment. Proceedings of the 2010 AIChE Annual meeting, Salt Lake City, UT, USA, November 7-12, 2010, 317

RNEDE: Resilient Network Design Environment

Thursday, November 11, 2010: 9:10 AM

Grand Ballroom H (Salt Palace Convention Center)

Venkat Venkatasubramanian[1], Tanu Malik[2], Arun Giridhar[1], Kris Villez[3], Raghvendra Prasad[4], Aviral Shukla[3], Craig Reiger[5], Keith Daum[5] and Miles Mcqueen[5], (1)Chemical Engineering, Purdue University, West Lafayette, IN, (2)Cyber Center, Purdue University, West Lafayette, IN, (3)School of Chemical Engineering, Purdue University, West Lafayette, IN, (4)Computer Science, Purdue University, West Lafayette, IN, (5)Instrumentation, Control and Intelligent Systems, Idaho National Labs, Idaho National Labs, Idaho, ID

Modern living is more and more dependent on the intricate web of critical infrastructure systems. The failure or damage of such systems can cause huge disruptions. Traditional design of this web of critical infrastructure systems was based on the principles of functionality and reliability. However, it is increasingly being realized that such design objectives are not sufficient. Threats, disruptions and faults often compromise the network, taking away the benefits of an efficient and reliable design. Thus, traditional network design parameters must be combined with self-healing mechanisms to obtain a resilient design of the network.

As part of the Complex Networks Project at Purdue University in collaboration with Idaho National Labs, our goal is to develop a resilient network design environment (RNEDE) that not only optimizes the network for performance but tolerates fluctuations in its structure that result from external threats and disruptions. To incorporate auto-tolerance, the environment efficiently evaluates a set of remedial actions that can bring a compromised network to an optimal level of functionality. The objective is to deliver such an environment to system administrators who regularly need an understanding of the current state of the network and need efficient and remedial solutions. The environment helps the network administrator to answer critical questions, such as:

- Which remedial action must be taken?

- Where in the current network remedial actions should be taken?

- Whether remedial actions are even worth taking?

The design of such an environment, however, can be a challenging task. Disruptions in the network, more often than not are unpredictable in nature, i.e., it is difficult to ascertain what kind of disruption may arise and thus which component will fail next. Even if the disruption is known, the space of remedial actions is often very large and the system needs to choose the most cost efficient remedial action. Further, it is important that the remedial action leads to a network structure that is optimal in that it maximizes/minimizes the objective function. It may be equally possible that no remedial action is taken.

The environment will act as a guide for the network administrator to replay various threat scenarios and thus design and maintain resources for remedial measures in a proactive manner. The environment will consist of an Optimizer and a Decision-controller, which when subject to a series of disruptions determines a topology that achieves the functionality of the network and determine cost-efficient remedial measures. The combined process of optimization and decision making is iterative in that a different network emerges as the system undergoes a sequence of threats. To facilitate ease of use, the framework is coupled with a Visualizer that allows the network administrator to continuously visualize the topology as it undergoes iteration. Figure 1 shows the architecture of RNEDE. The system administrator can play several disruption scenarios such as viral, targeted, and random to understand how to build self-tolerance within a network.

So far network theory has largely been limited to the topological analysis of existing or emergent complex networks, such as discovering the power law degree distribution [1] and the small-world phenomena [2]. The inverse operation, laws and principles that govern the design and operation of complex networks has only been explored recently [3,4,5]. In communication networks, dynamic organization of the network under changing communication patterns has also received significant attention [6,7]. In this project, we are exploring an orthogonal aspect of dynamic self-organization, i.e., understand how a self-organization of the topological structure in a network can aid in overcoming various threats and disruptions. In our presentation, we will present the details of this system and discuss some case studies.

[1] A.L. Barabasi and R. Reka Albert, Emergence of scaling in random networks, Science, vol. 286, pp. 509-512, 1999.
[2] J. Travers and S. Milgram, An experimental study of the small world problem, Sociometry, vol. 32, no. 4, pp. 425-443, 1969.
[3] V. Venkatasubramanian, A theory of design of complex teleological systems: Unifying the darwinian and boltzmannian perspectives, Complexity, vol. 12(3), pp. 14-21, 2007.
[4] V. Venkatasubramanian, S. Katare, P. Patkar, and F. P. Mu, Spontaneous emergence of complex optimal networks through evolutionary adaptation, Computers and Chemical Engineering, vol. 28, pp. 1789-1798, 2004.

[5] A. Tero, S. Takagi, T. Saigusa, K. Ito, D. P. Bebber, M. D. Fricker, K. Yumiki, R. Kobayashi, and T.Nakagaki, Rules for biologically inspired adaptive network design, Science, vol. 327, pp. 439-442, 2010.
[6] T. Malik, R. Prasad, S. Patil, A. Chaudhary, and V. Venkatasubramanian, Providing scalable data services in ubiquitous networks, In Workshop on Ubiquituous Data Management, DASFAA, 2010.
[7] J. Fan, M. Ammar, Dynamic topology configuration in service overlay networks: A study of reconfiguration policies, In IEEE Conference on INFOCOM, 2006.

Extended Abstract: File Not Uploaded

See more of this Session: Complex and Networked Systems
See more of this Group/Topical: Computing and Systems Technology Division