

## Geographic Surveillance and Hotspot Detection for Homeland Security: Cyber Security and Computer Network Diagnostics

**Short Description** Securing the nation's computer networks from cyber attack is an important aspect of Homeland Security. Project develops diagnostic tools for detecting security attacks, infrastructure failures, and other operational aberrations of computer networks.

---

**Full Description** Securing the nation's computer networks from cyber attacks is an important aspect of national Homeland Security. Network diagnostic tools aim at detecting security attacks on computer networks. Besides cyber security, these tools can also be used to diagnose other anomalies such as infrastructure failures, and operational aberrations. Hotspot detection forms an important and integral part of these diagnostic tools for discovering correlated anomalies. The project research will be used to develop a network diagnostic tool at a functional level. The goal of network state models is to obtain the temporal characteristics of network elements such as routers, typically in terms of their physical connectivity, resource availability, occupancy distribution, blocking probability, etc. We have done prior work (Ghosh and Acharya, 2001; Sarangan et al., 2001, 2002) in developing network state models for connectivity, and resource availability. We have also developed models for studying the equilibrium behavior of multi-dimensional loss systems (Acharya, 2003). The probabilistic finite state automaton (PFSA) describing a network element can be obtained from the output of these state models. A time-dependent crisis-index is determined for each network element, which measures their normal behavior pattern compared to crisis behavior. The crisis-index is the numerical distance between the stochastic languages generated by the normal and crisis automata. We plan to use the variational distance between probability measures, although other distances will also be considered. The crisis behavior can be obtained from past experience. The crisis indices over a collection of network elements are then used for hot-spot detection using scan statistic methodology. These hot spots help to detect coordinated security attacks geographically spread over a network.

---

**Strategic** Prevention

**Cycle** Preemption

**Elements** Crisis Management

**Project** <http://www.stat.psu.edu/~gpp/PDFfiles/Prospectus%2016%20overview.pdf>

**URL** <http://www.stat.psu.edu/~gpp/PDFfiles/Prospectus%2016.pdf>

**Sponsor** NSF Digital Government Program, EPA STAR Grant Program

**Keywords** Computer networks, crisis-index, hotspot detection, probabilistic finite state automata, network connectivity, scan statistic methods, security attacks, stochastic languages.