Cyber Automated Report Linker: A Network Approach to Minimizing Expansion of Catastrophic Cyber Infiltrations

Parish, Stephen

Catastrophic cyber infiltrations can devastate a nation's information infrastructure. This project provides a new way to defend modern adaptive computer networks. Computer networks are automatically adapted and optimized, causing rapid network reconfiguration. These reconfigurations make intrusions difficult to localize and track. My Cyber Automated Report Linker (C.A.R.L) provides several innovations that meet the engineering goal to show that a computer network security server can monitor and entire computer network, evaluate and link threat reports, and fight attacks in real time within a fluid network model. CARL automatically tracks network intrusion, and calculates where to intercept attacks ahead of their current region of influence. The program can anticipate possible intrusion expansions and even track and attack's movement before it has been identified as an attack. I have successfully combined a new system for linking and managing attack reports with optimization principles for data association, network topology analysis, and probabilistic reasoning to build a complete concept for cyber network defense. Stochastic Monty Carlo testing using a network model confirms innovative mathematical design. Results show the effect of tuning detection thresholds as an optimization measure for specific network instances.

Awards Won:

Fourth Award of $500

Oracle Academy: Award of $5,000 for outstanding project in the systems software category.