Network Science Center at West Point

Advancing the Study of Network Science

VOLUME 2, ISSUE2 FEBRUARY 2012

SPECIAL POINTS OF INTEREST

6th Annual Network Science Workshop
22-24 April
See website for more information
http://www.netscience.usma.edu/

1st Annual Minerva at West Point Workshop
16-17 April
For information see the Minerva webpage:
http://ow.ly/8Lu6i

Social Networks:

Facebook

Twitter

Linked In

Central Node

Smart Grid Vulnerability Research at West

Aaron St. Leger, PhD

The smart grid is defined by IEEE as "a next-generation electrical power system that is typified by the increased use of communications and information technology in the generation, delivery and consumption of electrical energy (http://smartgrid.ieee.org/ieee-smart-grid). Tremendous research and investment efforts are underway developing smart grid devices, software and standards. Smart devices and metering infrastructure are currently being deployed in power grids across the world, for example, the development of "smart buildings". A smart building contains advanced sensors, software and automation technology with the end goal of reducing energy consumption and costs. In addition, these buildings can tie into the smart grid and adjust energy consumption based on external signals such as the current price of energy. This is one of many applications being developed and deployed as the smart grid is established. However, the smart grid is currently in its infancy. The operation and vulnerabilities of the power grid are rapidly changing as this technology is developed and deployed.

The focus of a Defense Threat Reduction Agency (DTRA) funded research project at West Point is to investigate new and future vulnerabilities of the smart grid. The smart grid consists of cyber, and physical components. The physical components generate, transmit and consume energy and in addition, a physical infrastructure for communication among smart devices. Cyber components consist of software, controllers and data related to the smart grid. Each classification of component, cyber and physical, have their own vulnerabilities. In addition, the integration of these components into the smart grid is yielding complex interdependencies between the components and additional vulnerabilities. For example, cyber vulnerabilities could result in physical failures of power system components in the smart grid in a similar fashion as the Stuxnet worm targeted a Siemens supervisory control and data acquisition system in an Iranian uranium enrichment plant. The focus of the research effort at West Point is on physical vulnerabilities of the smart grid, more specifically, the impacts of weapons of mass destruction (WMD). This includes attacks on cyber and physical components.

The research project is focusing on developing appropriate smart grid models, custom simulation tools for simulating the models, including physical attacks, and analytical methods for quantifying the vulnerability of a system to such attacks. The models are quantitative in nature with an emphasis on modeling the interdependencies between cyber and physical components of the smart grid. This quantitative model will be suitable to analyze the effects of WMD attacks at various points in a system, identify critical points of the system, and provide insight into how to strengthen or protect the system from WMD related failures. Physical components of the power grid are being modeled and simulated with a modified version of the open source Power System Toolbox (PST) software which has been developed at Rensselaer Polytechnic Institute (RPI) (http://www.ecse.rpi.edu/pst/PST.html). This modified code has been integrated into a MATLAB/Simulink software environment where models of communication networks and cyber elements of the smart grid are being developed. While the software is still under development a functioning framework containing cyber and physical components has been developed. Moreover it is flexible in nature, based off of open source and MATLAB/Simulink software, such that additional models, smart grid components and smart grid control schemes can be incorporated and tested as the smart grid continues to evolve.

Software to Locate Weapons Caches in Combat: New Possibilities

MAJ Paulo Shakarian, Ph.D.

Can we use network science to locate enemy weapons caches in Afghanistan? I firmly believe that this is possible based on a new research area known as "geospatial abduction." This theory purports that if there are two items in a geographic space and we only know the location of one item, we can locate the second item based on relationship constraints of the two items. To apply this to finding weapons caches, consider the following: An improvised explosive device (IED) detonates in a certain location. If we know minimum and maximum distances (i.e. on a road network) between detonation events and weapons caches and perhaps some other data (i.e. social demographics, physical terrain, etc.) we can identify potential locations of the cache to help direct other intelligence, surveillance, and reconnaissance (ISR) assets to search for them. Sound far-fetched? Not really. A piece of software known as SCARE was able to successfully locate weapons caches in Iraq and Afghanistan based on unclassified, open source data.

The Algorithmic Network Science Group here at the West Point NSC is currently engaged in joint work with the West Point Operations Research Center (ORCEN) to take the SCARE software to the next step – get it ready for combat. Funded by the U.S. Army Geospatial Center, we are looking to integrate SCARE into tools currently used by intelligence analysts and operational planners such as ArcGIS, CPOF, and TIGR. This semester, MAJ Charles Levine (DSE/MATH) is advising a cadet capstone project to start this process. Then, in the summer, MAJ Levine and I are creating an internship held here at West Point where cadets will actively support combat units in Afghanistan with the SCARE software. Sound interesting? See Important dates for a schedule of upcoming talks on SCARE as well as articles for further information.

Article: "Software Pinpoints Afghan Fighters," MSNBC CosmicLog

Article: "SCARE Software Predicts Insurgent Weapons Cache Locations Based on IED Attacks," PopularScience

Important Dates:

15 February—**Brown bag lunch**—Finding Weapons Caches with Geospatial Abduction
16-17 April—**1st Annual Minerva at West Point Workshop**
22-24 April—**6th Annual Network Science Workshop**

Current Publications/Presentations:

Current articles are on NSC website under Publications or linked below:
Graffiti Decomposition
Simulating Counterinsurgency and Coalition Strategies