Louis Wilder
Los Alamos National Laboratory

CODE --a Tool to Solve Unobservable Elements of Electric Power and SCADA Networks

This presentation describes a major Los Alamos initiative to address DoD requirements in Critical Infrastructure Protection although multiple sponsors supported this work. Analyses from this work differ from peers in that each peer offered their own specialty and each gained responsibility for a piece of the problem domain. However, we relied upon expert judgment and design rules with limited ability to quantify uncertainty to infer network topologies.

In order to estimate unobserved networks' missing components, our approach initially constructs a model of the target infrastructure by incorporating the observable portions of the network.

Next, using heuristic rules, a synthetic network was overlaid onto the target infrastructure model. Finally, the coupling of the synthetic network nodes was accomplished by inferring the interdependent nodes of the target model. By developing a software application (Conus and Oconus Distribution Estimator, CODE), Los Alamos automated the process of estimating EP and SCADA networks' topology.

The science incorporates inference methods using computer science, computational physics, and computational geometry, which reveal both physical and logical features of a network. The algorithm is a force-directed technique for graph drawing similar to that introduced by Eades[1] in 1984. The method involves representing the vertices of the graph with masses and representing the edges of the graph with springs. Optionally, additional springs may be added between those vertices not connected by an edge. The graph can then be treated as a dynamical system and allowed to converge to an equilibrium configuration. If the spring constants are chosen appropriately, the forces on the system lead to an equilibrium condition that has an aesthetically pleasing layout. The graph's equation of motion is essentially that for the Brownian motion of particles coupled by harmonic oscillators. A case study will be presented to illustrate the use of this technique. See figure 1.

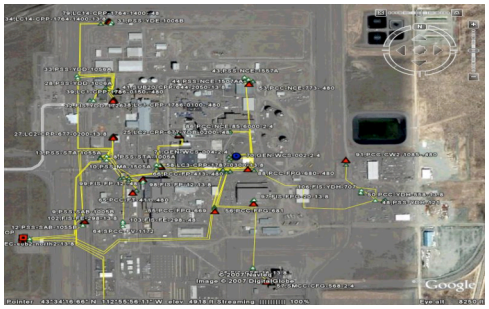


Figure 1: An illustration of the power distribution network topology of an INL Test Range Facility.

Figure 1 illustrates the physical network topology for an electric power distribution system served by the external substation, depicted in the lower left corner of the image. In this case, the

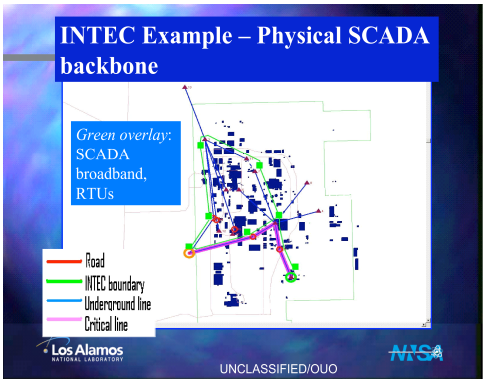
1. P. Eades, "A Heuristic for Graph Drawing," *Congressus Numerantium,* **42** (1984)
2. R.J. Landman, "Standard Handbook for Electrical Engineers: Section 10 Power-System Components

substation capacity was 138 kV step-down to 13.8 kV, which represents the distribution system.

In addition to inferring the electric power distribution physical network, the substation serves as *loci* for anchoring the synthesized telecommunication network. The first step in constructing the telecommunication network is the assignment of the regional broadband data network node shown in green geolocated at the substation. A separate narrowband network was constructed with several points tangent to the regional broadband network node. This permits substation data collected through narrowband circuits to be accumulated and placed on the broadband network for transmission to electric power operations centers.

The proposed narrowband circuit mesh is shown grouped within the green loop each node is a data collection point. The groupings are necessarily somewhat arbitrary but the intent is fixed: to move remote terminal unit (RTU) and some Intelligent Electronic Deice (IED) data onto the broadband network. Figure 2, depicts the physical SCADA backbone for an electric power system.

Figure 2: Depicts the physical SCADA backbone for an electrical power distribution system.



SCADA systems consist of one or more computers with appropriate applications software (Master Stations) connected by a communications system (wire, radio, power line carrier or fiber optics) to a number of RTUs placed at various locations to collect data, remote control, and more recently perform intelligent autonomous (local) control of electrical systems and report results back to the remote master(s).

SCADA systems are used for fault identification, isolation and service restoration, breaker control, recloser blocking, generator control, feeder switching and reconfiguration, line switching, voltage control, load management, automated meter reading (AMR), archiving processes, automatic generation control (AGC), dispatch accuracy feedback, economic dispatch, energy purchased and sold, system load, system emulation, capacitor bank switching, monitoring voltage regulators, transformer temperature, as well as metering power functions.[2]

1. P. Eades, "A Heuristic for Graph Drawing," *Congressus Numerantium,* **42** (1984)
2. R.J. Landman, "Standard Handbook for Electrical Engineers: Section 10 Power-System Components

RTUs are special purpose computers, which contain analog to digital converters (ADC), digital to analog converters (DAC), digital inputs (status) and outputs (control). *Transmission Substation RTU:* These large RTUs are deployed at substations and generation facilities where a large number (perhaps several thousand) control and data points are required. *Distribution Automation RTUs:* These smaller RTUs are used to control air switches and VAR compensation capacitor banks on utility poles, pad mounted switches, monitoring and automating feeders and underground networks and in smaller distribution substations.[2]

Both network models provide a significant ability to identify network vulnerabilities in the electric power and SCADA networks, respectively. The power network allows a visual analysis for facility isolation based on a single point of failure.

Additionally, it serves an interdependent component for the synthetic overlay of the telecommunication (SCADA) network.

The telecommunication (SCADA) network details the vectors for penetration testing to identify vulnerabilities, which are similar vulnerabilities found in traditional networks.

The following details vulnerabilities that may be found within the SCADA network.

- The flow of data in a SCADA system is dictated by a communications protocol designed specifically for such application. The most common protocols are open (published) standards such as DNP 3.0, MODBUS, and UCA/MMS, etc. Proprietary protocols are supported also in many RTUs and communications processors. Such protocols, however, are similar in function to the open standards. Thus, these protocols can be use to accomplish a cyber penetration.

- However, the protective equipment and controllers within a substation, the SCADA system connecting the substation to control stations, and the utility's information processing networks are at risk to electronic intrusions. The vulnerability, and hence the risk, increases with connectivity. Thus, devices connected to public communications networks are the most accessible to the largest group of people, and therefore are the most at risk. For example, the use of an Ethernet LAN/WAN has inherent, traditional vulnerabilities for unauthorized access.

- Both the RTUs and the new automated devices, e.g. {IEDs}, are susceptible to electronic attack. By dialing into a port on a digital breaker, a utility

1. P. Eades, "A Heuristic for Graph Drawing," *Congressus Numerantium,* **42** (1984)
2. R.J. Landman, "Standard Handbook for Electrical Engineers: Section 10 Power-System Components

engineer can reset the device or select any of six levels of protection. An electronic penetration could dial into an unprotected port and reset the breaker to a higher level of tolerance than the device being protected can withstand. By doing so, it is possible to destroy a given piece of equipment within a substation. The penetration could also set the device to be more sensitive than conditions for normal operations and cause the system to shut down for self-protection.

- A regional substation is equipped with microwave towers that communicate with other regional centers and the centralized control center. Microwave sources are vulnerable to electronic eavesdropping. Electronic eavesdropping is a less visible form of penetration and can be achieved in all communications media by intercepting or tapping into communication signals.

- Many SCADA communications are now use TCP/IP—communications between the SCADA system and the end devices (RTUs, PLCs, IEDs, etc..) are encapsulated in TCP/IP to work over Ethernet systems

Los Alamos' approach to identification of vulnerabilities within infrastructure assets is to provide automated tools for modeling infrastructure that allows visual analysis, and the assessment of interdependency between sectors.

In summary, the CODE application allows analyst to visualize the infrastructure using models, which identify vulnerabilities in the EP network through isolation of a single point of failure.

In addition, the attack vector for the SCADA network is identified for further vulnerability investigation by cyber penetration. The cyber penetration will unveil additional vulnerabilities, which are analogous to traditional networks and system vulnerabilities.

1. P. Eades, "A Heuristic for Graph Drawing," *Congressus Numerantium,* **42** (1984)
2. R.J. Landman, "Standard Handbook for Electrical Engineers: Section 10 Power-System Components