SCADA Cyber Security Testbed Development

C. M. Davis, J. E. Tate, H. Okhravi, C. Grier, T. J. Overbye, and D. Nicol
School of Electrical and Computer Engineering
University of Illinois Urbana-Champaign
Urbana, Illinois

Abstract— **New technologies are increasing the vulnerability of the power system to cyber security threats. Dealing with these threats and determining vulnerabilities is an important task for utilities. This paper presents the development of a testbed designed to assess the vulnerabilities introduced by using public networks for communication.**

I. Introduction

The proliferation of new computer technologies in the power system has brought many advantages and risks. Increasingly powerful computers are becoming prevalent not just in control centers in offices but also in the field in the form of IEDs (Intelligent Electronic Devices). They allow for efficient network based communications, the use of next generation SCADA protocols, and more intelligent behavior. Unfortunately, using these new devices also has a down side. Using standard networks and protocols opens the devices to possible cyber attacks.

To address these new vulnerabilities, the TCIP (Trustworthy Cyber Infrastructure for the Power grid) project has been started under the ITI (Information Trust Institute). TCIP is an NSF funded project consisting of researchers in various areas of computer security and power systems.

Determining the vulnerabilities of systems using these devices is a complicated process because of the complex hardware and software interactions that must be considered. One approach is to build a comparatively simple system that captures the relevant complexity i.e. a testbed. This work first presents motivations for developing a testbed in the form of a brief review of cyber security basics. Next, several components developed for use in the testbed environment are discussed, and finally the pieces are put together and a simulation of a cyber attack scenario is presented.

II. Cyber Security Background

A. Traditional SCADA Architecture

Historically electric utilities have been regulated, vertically integrated monopolies. One company owned and controlled everything from the generators to the distribution system. Utilities knew their systems very well and data was shared only on a limited basis. SCADA systems often communicated over dedicated communication links like phone lines and microwave radio links. The SCADA system hardware possessed limited processing power and often utilized vendor-specific protocols.

B. Future SCADA Architecture

Presently utilities are structured very differently than they have been in the past. The transmission system allows open access, meaning that anyone owning a generator is allowed to supply power to the grid. Markets have been set up to decide which generators are used instead of the utility owning generation and determining dispatch. These changes mean the transmission system is used in a very different way. The changes in the operation of the transmission system make it more important to securely share data among system operators, while ensuring that only the appropriate market insensitive data can be accessed by marketeers. Thus, the restructuring of the utility industry has resulted in the need for varying levels of information access [1].

There is also a shift in the nature of SCADA systems. The old-style vendor-specific SCADA protocols are being replaced by next generation standards based protocols like IEC 61850. These next generation protocols are based on a common information models (CIM) [2]. Common information models are used to associate devices with services. This kind of abstraction makes useful features like device discovery possible. Making this sort of abstraction possible is the vastly improved computational power of new SCADA hardware. Instead of micro-controller based hardware programmed in assembly, present day hardware runs more advanced real-time operating operating systems(e.g. real-time linux and vxWorks). Not only are the protocols and hardware changing, but the communications links are evolving as well. Expensive dedicated phone lines and microwave links are being replaced by data networks.

C. Threats

There are many threats facing critical infrastructure today. The most famous threats in this day and age are the threats posed by terroristic groups and hostile nation states. These are organized groups with a clear goal and some level of sophistication. There is also a threat posed by a company's own employees. Company insiders have access to internal controls and data, and either by accident or malicious intent can cause equipment outages. A third category of threat is the threat posed by casual hackers, known as ”script kiddies”. These are people without great computer ability who download and use prepackaged tools.

D. Vulnerabilities

The term vulnerabilities is used to refer to equipment that is vulnerable to attack. This notion is distinct from threats. For example, a vulnerability would be a hole in the fence whereas a threat would be the person who wants to get through the fence. Power systems face a new array of cyber vulnerabilities as new equipment, running more standard real-time operating systems, is phased in because this more standard equipment is subject to well known attacks. The Cyber Emergency Response Team (CERT) has been tracking computer vulnerabilities since the late 1980s. Their statistics show that the number of vulnerabilities has been increasing dramatically in recent years [3].

E. Countermeasures

To address vulnerabilities present in the power system, NERC, working with the DOE and the DHS and their Canadian counterparts, has developed a set of cyber security standards [4]. These standards are a protocol requiring companies to identify their vulnerabilities and risks and take steps to mitigate them. This is done in several steps. First, the impact of the loss of assets is determined. Next, the standard calls for the identification of vulnerabilities. Then, using this information, companies can preform risk analysis to decide which vulnerabilities are most important to protect against. Finally, companies decide which defenses are most cost effective and begin to implement them. Common defences against cyber attacks include application of firewalls and authentication methods. Peer-to-peer overlay routing is another possible defence against DDoS attacks [5].

III. Simulation Architecture

A. Network Client

1) Purpose: The network client provides several key functions needed to implement an accurate testbed that closely mimics real world operation of the power grid:

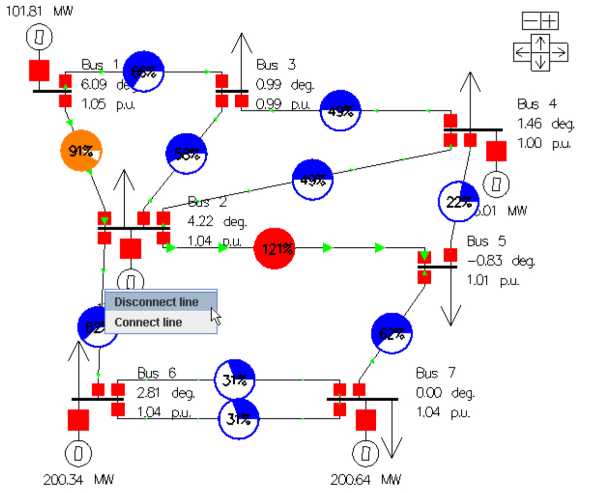


Fig. 1. Network client screenshot - opening a line in a 7 bus case

- The client provides a graphical view of power system states. The information used to drive the display is obtained via TCP/IP from a server (see Section III-C below for a description of the protocol used). This mimics a control room display that is obtaining SCADA data from the power grid over a communications network.
- The ability to control (rather than simply view) power system elements is also a key component of real power system operation. The client supports control actions, such as opening and closing of lines, in addition to simple display of data.
- All data displayed on the client must first be communicated over the network from the server to the client. This decoupling of the display (the network client) from the data source (the PowerWorld server) enables independent modification and testing of the display, communications networks, and power system without affecting other components of the testing environment.

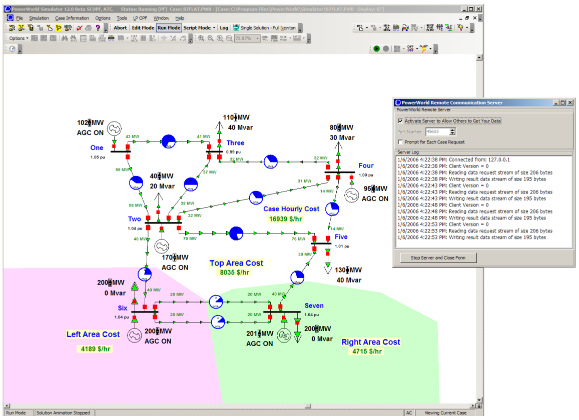
2) Capabilities: The client currently has the following key capabilities:

- An individual client can access any number of servers, with a highly configurable scheduling mechanism for retrieving data. Data retrieval from the server can be aperiodically initiated or set to occur at regularly timed intervals. By setting the intervals between retrievals to a very small value, it is easy to stress the underlying communications system to examine bandwidth effects.
- Opening and closing of lines
- Support for major operating systems (Windows, Mac OS X, Linux)
- Ability to run as a Java applet inside of a web browser (for remote testing)

A sample screen shot of the network client displaying retrieved data for a 7 bus system is shown in Figure 1.

B. PowerWorld Server

1) Purpose: The PowerWorld server serves two purposes which, when combined, allow it to serve as a surrogate for the real power grid when performing experiments:


PowerWorld Simulator 12.0 Beta SCOPF, ATC. Status: Running (PF) Case: B7FLAT.PWB - [Case: C:\Program Files\PowerWorld\Simulator\B7FLAT.PWB Display: B7]

PowerWorld Remote Communication Server

PowerWorld Remote Server

☑ Activate Server to Allow Others to Get Your Data

Port Number 45605

☐ Prompt for Each Case Request

Server Log

```
1/6/2006 4:22:38 PM: Connected from: 127.0.0.1
1/6/2006 4:22:38 PM: Client Version = 0
1/6/2006 4:22:38 PM: Reading data request stream of size 206 bytes
1/6/2006 4:22:38 PM: Writing result data stream of size 195 bytes
1/6/2006 4:22:43 PM: Client Version = 0
1/6/2006 4:22:43 PM: Reading data request stream of size 206 bytes
1/6/2006 4:22:43 PM: Writing result data stream of size 195 bytes
1/6/2006 4:22:48 PM: Client Version = 0
1/6/2006 4:22:48 PM: Reading data request stream of size 206 bytes
1/6/2006 4:22:48 PM: Writing result data stream of size 195 bytes
1/6/2006 4:22:53 PM: Client Version = 0
1/6/2006 4:22:53 PM: Reading data request stream of size 206 bytes
1/6/2006 4:22:53 PM: Writing result data stream of size 195 bytes
```

Fig. 2. PowerWorld server screenshot - serving data for a 7 bus case

- The server simulates the power grid with a feature-rich power flow solver. This allows us to simulate systems with a high degree of modeling accuracy by taking advantage of the advanced modeling facilities built into the PowerWorld Simulator software.
- The server provides the SCADA data that would typically be fed into a control center display (represented by the client). The server provides the simulated data to the client over a TCP/IP network using a custom networking protocol (see Section III-C below).

2) Controls: The server also accepts control commands sent by clients, e.g., the opening and closing of lines. The server continuously solves the power flow, so network flow impacts are instantly solved and propagated to all connected clients. The ability to accept control commands from the client allows us to study the effects of various network attacks on control actions.

3) Data Provided: The server currently provides the following data to clients:

- Bus voltage magnitude and phase angle
- Line status
- Line flow
- Generator status

A sample screen shot of the PowerWorld server providing client data on the 7 bus case is shown in Figure 2.

C. Client-Server Protocol

The protocol used for communicating between the client and server is a simple request/response protocol which uses the TCP/IP networking protocols. All network communication is initiated by the client, which can either send or receive an arbitrary amount of data in a single session.

D. Network Emulator : RINSE

1) Purpose: The Real-time Immersive Network Simulation Environment for Network Security Exercises (RINSE) is a tool for realistic emulation of large networks as well as network transactions, attacks, and defenses [6].

RINSE has unique capabilities which make it suitable for cyber security and game-playing exercises including large-scale real-time human/machine-in-the-loop network simulation support, multi-resolution network traffic models, and novel routing simulation techniques.

RINSE consists of five components:

- the iSSFNet network simulator,
- the Simulator Database Manager,
- a database,
- the Data Server,
- and client-side Network Viewers

The internal architecture of RINSE is shown in Figure 3. The iSSFNet is the core network simulator which is built on top of Scalable Simulation Framework (iSSF), an Application Programming Interface (API) for parallel large-scale simulation [7]. In this architecture, the Simulation Database Manager is responsible for collecting simulation data from simulator nodes and puts it into the database. In the RINSE architecture, many simulator nodes can work in parallel to support large-scale real-time network simulation. Clients run Network Viewer which connects to the database through the Data Server and gives each client a separate view of the simulated network. This view is the portion of the simulated network in which the client is interested in and is able to play security games with. This feature can be used in exercises like the October 2003 Livewire cyber war exercise which was conducted by the Department of Homeland Security [8].

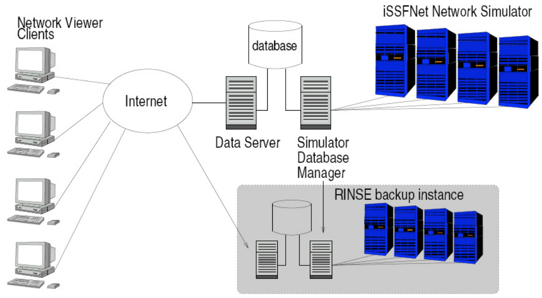
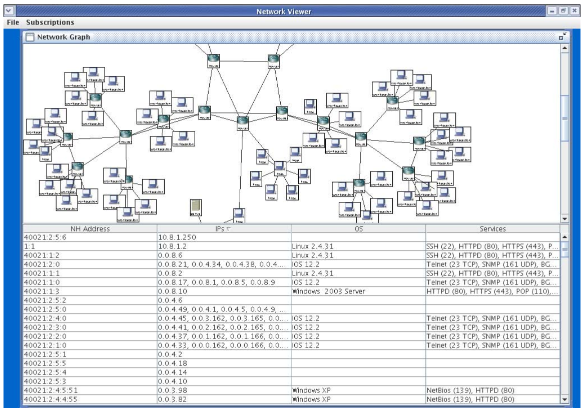


Fig. 3. RINSE Architecture

2) Capabilities: In addition to parallel real-time large-scale simulation, RINSE is capable of multi-resolution traffic simulation, meaning it can simulate traffic with varying levels of detail. This makes it suitable for simulating high-volume traffic and attacks. When traffic is presented and simulated in a multi-resolution fashion, traffic with important dynamic behavior (foreground traffics) are simulated with high-resolution packet-level details whereas traffics showing other activities in the network (background traffics) are simulated using coarse-grain fluid model [9] [10] . RINSE uses both resolutions for different traffics at the same time [11] coupled with a fixed point solution technique resulting in several orders of magnitude speed-up in simulation [12] [13]. As for attack traffics (e.g. DoS attacks) the details of the traffic is of little importance and we are only interested in the coarse behavior (volume of the traffic), coarser multi-resolution model is used to increase the efficiency of simulation and to make real-time simulation possible [14].

Another important feature of the RINSE architecture is the Network Viewer which gives clients the ability to have different views of the simulated network and also to issue commands to the simulator (Figure 4). Five types of commands are currently supported:

- Attacks: for initiating attacks (particularly DDoS attacks) in the network.
- Defenses: for applying countermeasures against attacks. These commands include filtering packets at routers which can mitigate attack effects.
- Diagnostic Tools: which simulate common networking utilities such as ping.
- Device Controls: for controlling (shutting down, rebooting,) individual devices in the network



NH Address	IPs	OS	Services
40021:2:5:6	10.8.1.250		
1:1	10.8.1.2	Linux 2.4.31	SSH (22), HTTPD (80), HTTPS (443), P...
40021:1:2	0.0.8.6	Linux 2.4.31	SSH (22), HTTPD (80), HTTPS (443), P...
40021:2:0	0.0.8.21, 0.0.4.34, 0.0.4.38, 0.0.4....	IOS 12.2	Telnet (23 TCP), SNMP (161 UDP), BG...
40021:1:1	0.0.8.2	Linux 2.4.31	SSH (22), HTTPD (80), HTTPS (443), P...
40021:1:0	0.0.8.17, 0.0.8.1, 0.0.8.5, 0.0.8.9	IOS 12.2	Telnet (23 TCP), SNMP (161 UDP), BG...
40021:1:3	0.0.8.10	Windows 2003 Server	HTTPD (80), HTTPS (443), POP (110),...
40021:2:5:2	0.0.4.6		
40021:2:5:0	0.0.4.49, 0.0.4.1, 0.0.4.5, 0.0.4.9, ...		
40021:2:4:0	0.0.4.45, 0.0.3.162, 0.0.3.165, 0.0....	IOS 12.2	Telnet (23 TCP), SNMP (161 UDP), BG...
40021:2:3:0	0.0.4.41, 0.0.2.162, 0.0.2.165, 0.0....	IOS 12.2	Telnet (23 TCP), SNMP (161 UDP), BG...
40021:2:2:0	0.0.4.37, 0.0.1.162, 0.0.1.166, 0.0....	IOS 12.2	Telnet (23 TCP), SNMP (161 UDP), BG...
40021:2:1:0	0.0.4.33, 0.0.0.162, 0.0.0.166, 0.0....	IOS 12.2	Telnet (23 TCP), SNMP (161 UDP), BG...
40021:2:5:1	0.0.4.2		
40021:2:5:5	0.0.4.18		
40021:2:5:4	0.0.4.14		
40021:2:5:3	0.0.4.10		
40021:2:4:5:51	0.0.3.98	Windows XP	NetBios (139), HTTPD (80)
40021:2:4:4:55	0.0.3.82	Windows XP	NetBios (139), HTTPD (80)

Fig. 4. Network viewer screenshot

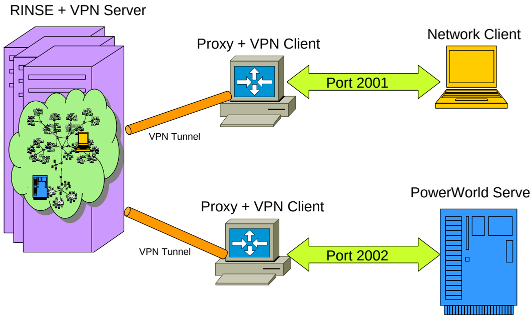


Fig. 5. Client-Server-RINSE Integration Scheme

TABLE I
SCADA Services Mapping

Modbus Device	PowerWorld Service
Branch RTU	open/close transmission line
Generator RTU	read generator information

- Simulator Data: for controlling the output of the simulator.

RINSE is also capable of emulation, i.e. it can represent real nodes with virtual nodes in the simulated network and generate real packets for transactions with the outside world. Emulation is the key feature of RINSE that has been used in the integration of RINSE and PowerWorld. Emulation also needs some extra components which will be discussed in detail below.

E. Protocol Converter

The protocol converter is a program designed to convert the custom power world protocol into real SCADA protocols. This allows the network client to interface with actual hardware. The protocol converter also provides a means of testing protocols by grabbing the server's output and forwarding it across a (possibly simulated) network.

One function that must be performed by the protocol converter is mapping between the simple PowerWorld server and the more complicated actual devices. Table I shows the mapping between the available PowerWorld functionality and Modbus SCADA models. Modbus is a commonly used SCADA protocol [15]. A free open-source Modbus implementation was used for the implementation of the protocol converter [16].

F. Integration of Simulators

The scheme that is used for integration of the PowerWorld simulator with RINSE is shown in Figure 5 ̇This architecture has four major components:

- PowerWorld Server
- Network Client(s)
- Proxy Servers + VPN Clients
- RINSE + VPN Server

In this architecture, the network client sends packets to the PowerWorld server via a proxy server on a specified, arbitrary port (in this case port 2001). The proxy server then translates the destination of these packets to the virtual IP address of the PowerWorld server in the simulated network. The packets are then delivered through a VPN tunnel to the RINSE node. A daemon grabs the packets from the RINSE end of the VPN tunnel and injects them into the simulator using the emulation capability of RINSE. RINSE then simulates a large network in which there are virtual nodes representing the PowerWorld Server and the Network Client(s). Upon arrival of the packets to the virtual node representing the PowerWorld server, the simulator generates real packets with virtual IP addresses and delivers them to the kernel. These packets are sent trough another VPN tunnel to proxy server. Finally, the proxy server translates the virtual address and sends the packets to the real PowerWorld Server. The same process happens in the reverse direction when the PowerWorld Server responds to the Network Client requests.

With this setup, the traffic between PowerWorld Server and its client passes through RINSE making it possible to study the effect of cyber attacks and security countermeasures on the power grid. One advantage of this setup is that the network simulator (RINSE) is completely transparent to the PowerWorld Server and the Network Client(s).

IV. Attack Scenario

A. Scenario Description

Increasing load levels cause the transmission system serving a load pocket to become overloaded. At the same time a network attack hinders the operator's ability to receive data and issue commands. Under normal circumstances, the operator has the ability to switch in local generation or reconfigure the transmission system to relieve the overload. In this case, however, the network attack has blinded the operators from knowledge of the problem and removed their ability to

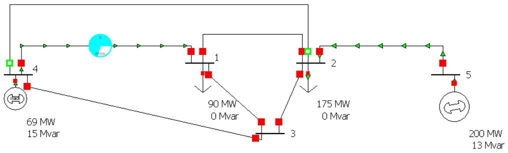


Fig. 6. Scenario one-line diagram 90 MW bus 1 load

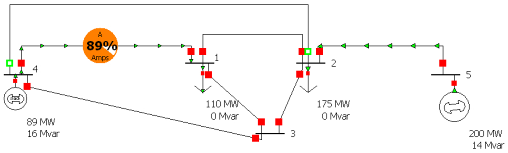


Fig. 7. Scenario one-line diagram 110 MW bus 1 load

respond. The situation deteriorates as protection equipment forces the overloaded line service. A cascading outage has begun that will result in a blackout for the load pocket.

For this scenario, the load pocket consists of buses 1, 2, and 3. The increasing demand is modeled by step changes of the load at bus 2. The load starts at 90 MW. At this load level, the transmission line from bus 4 to bus 1 is loaded at 70.5% of capacity. The next load level is 110 MW. The corresponding line loading is 89.4%. The final load level is 125 MW. At this load level the transmission line is overloaded, operating at 103.5% of capacity. Images of the system under each loading level can be seen in figures 6, 7, and 8.

B. Attack Description

To study the effect of cyber attacks on the simulated power system, we have used the architecture shown in Figure 5. A relatively large network with hundreds of hosts and routers and many sub-nets is used for simulation with two of the hosts representing the Power Server and its client.

Three different scenarios have been simulated to study the effect of attack and defense. In the first scenario, the network runs under normal conditions with some transactions and background traffic present. The goal of this scenario is to study the interaction of the PowerWorld server and client under normal operating conditions of the network. In the second scenario after a while of operating normally, distributed denial of service (DDoS) attack starts in the network. This is done by issuing the following command to RINSE:

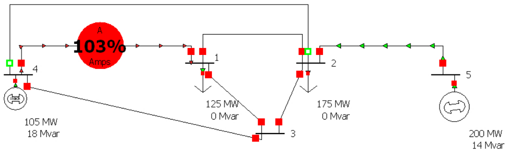


Fig. 8. Scenario one-line diagram 125 MW bus 1 load

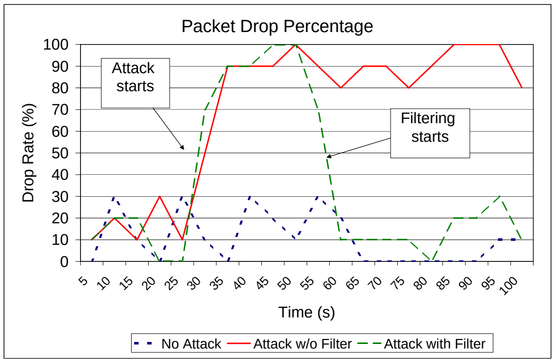


Fig. 9. Packet drop percentage in simulated network for a 100s run

```
ddos-attack attacker server 100 700
```

Attacker and server are symbolic names for the virtual nodes representing the attacker and the victim server in the simulated network. Note that the server here is an arbitrary server in the simulated network and is different from the virtual node representing the PowerWorld Server. Upon reception of the command, the attacker sends attack signals to zombie hosts in the network and they start emitting packets to the victim server at the rate of 700 Kbits/s. The attack starts after 30 seconds of simulation and lasts for 100 seconds. With this scenario we study the effect of attack on the power system that uses a public network as its communication medium.

The third scenario complements the second one by applying countermeasures in the network to mitigate the negative effects of the attack on the power grid. This is done by issuing the command:

```
filter router add 0 deny all all * all * 33333
```

in which router is the symbolic name for the intermediate router connecting the zombies network to the server network. This filter drops packets coming in on `all` interfaces, using `all` protocols, from all source IP addresses (”*”) and `all` source ports to all destination IP addresses (”*”) and destination port `33333` on which the vulnerable service works. This command is issued after 60 seconds of simulation.

C. Results

The three scenarios described above have been run and the effect of DDoS attack on the power system has been studied. To get an estimate of the responsiveness of the network under normal condition, attack, and attack with filters, packet drop percentage between the power server and its client has been measured using ”ping” and is shown in Figure 9.

When there is not attack occurring, the operator(s) at the network client see data that is refreshed at the proper rate and have the ability to open and close lines. If an attack is in progress the SCADA data and commands are prevented from getting to and from the network client. The DDoS attack floods the network with packets, causing the real data to be delayed or lost. This is evident in the divergence of the one-line views between the network client and the PowerWorld server. When an attack is under way, the network client continues to display old data showing that the system is operating safely even though a transmission line is overloaded. So an operator continues to see Figure 6 instead of Figure 7 or Figure 8. The application of a filter is one defense against a DDOS attack. Applying a filter after an attack has begun successfully mitigated the attack and allowed SCADA data to transit the network as illustrated in Figure 9 .

V. Conclusion

The experiment presented in this paper uses the network client to act as a control station, the PowerWorld server to act as the power system, and RINSE to act as the communication network. This experiment demonstrated the vulnerability of the network client to a DDOS attack and the ability of filtering to mitigate an attack. The attack prevented data from being transmitted across the network, causing the control display to display incorrect data. So far this work presents a test bed created using only software. The next step to more accurately model the SCADA system is to incorporate actual hardware (RTUs, relays, etc.) in the simulations. Using the protocol converter it is possible already to interface with devices communicating using the ModbusTCP protocol. Work is ongoing to implement next generation protocols and to extend the functionality of the network client and PowerWorld server (i.e. add more commands). In it's final form, the test bed will consist of computer simulations, hardware, and people acting as controllers.

Acknowledgment

The authors would like to thank the NSF for their support under award number CNS-0524695.

References

[1] G. Zecevic and Z. Jovanovic, "Company intranet access to scada information," in *Proc. Budapest International Conference on Electric Power Engineering*, New York City, USA, Aug. 1999, p. 121.

[2] G.-S. Kim and H.-H. Lee, "A study on iec 61850 base communication for intellegent electronic devices," in *Proc. IEEE 9th Russian-Korean International Symposium on Science and Technology*, vol. 1, Novosibirsk,Russia, 2005, pp. 765–770.

[3] C. E. R. Team. (2006) Cert/cc statistics 1988-2006. [Online]. Available: http://www.cert.org/stats

[4] N. A. E. R. Council. (2006) Critical infrastructure protection. [Online]. Available: http://www.nerc.com/cip.html

[5] J. J. Farris and D. M. Nicol, "Evaluation of secure peer-to-peer overlay routing for survivable scada systems," in *Proceedings of the 2004 Winter Simulation Conference*, Washington D.C.,USA, Dec. 2004.

[6] M. Liljenstam, J. Liu, D. Nicol, Y. Yuan, , G. Yan, and C. Grier, "Rinse: the real-time immersive network simulation environment for network security exercises," in *In Workshop on Principles of Advanced and Distributed Simulation*, 2005.

[7] J. Cowie, D. Nicol, and A. Ogielski, "Modeling the global internet," *Computing in Science and Engineering*, vol. 1, pp. 42–50, Jan. 1999.

[8] A. Press. (2003, Nov.) T. bridis. gov't simulates terrorist cyberattack. [Online]. Available: http://www.zone-h.org/en/news/-read/id=3728

[9] B. Liu, D. R. Figueiredo, Y. Guo, J. Kurose, and D. Towsley, "A study of networks simulation efficiency: Fluid simulation vs. packet-level simulation," in *In Proceedings of IEEE Infocom*, Apr. 2001.

[10] G. Kesidis, A. Singh, D. Cheung, and W. Kwok, "Feasibility of fluid-driven simulation for atm network," in *In Proceedings of IEEE Globecom*, Nov. 1996.

[11] D. Nicol and G. Yan, "Discrete event fluid modeling of background tcp traffic," *ACM Transactions on Modeling and Computer Simulation*, vol. 14, pp. 1–39, July 2004.

[12] D. Nicol, J. Liu, M. Liljenstam, and G. Yan, "Simulation of large-scale networks using ssf," in *In Winter Simulation Conference (WSC)*, Dec. 2003.

[13] D. Nicol and G. Yan, "Simulation of network traffic at coarse time-scales," in *In Workshop on Principles of Advanced and Distributed Simulation*, 2005.

[14] ——, "Discrete event fluid modeling of background tcp traffic," in *Proc. ACM Workshop on Rapid Malcode*, Oct. 2003.

[15] Modbus-IDA. (2005) Modbus-ida:the architecture for distributed automation. [Online]. Available: http://www.modbus.org

[16] D. Wimberger. (2004) jamod. [Online]. Available: http://jamod.sourceforge.net