International Journal of Business, Human and Social Sciences
ISSN: 2517-9411
Vol:7, No:8, 2013

Agent-Based Modeling of Power Systems Infrastructure Cyber Security

Raman Paranjape

***Abstract*—**We present a new approach to evaluation of Cyber Security in Power Systems using the method of modeling the power systems Infrastructure using software agents. Interfaces between module and the home smart meter are recognized as the primary points of intrusion.

***Keywords*—**Power Systems, Modeling and Simulation, Agent systems.

I. Introduction

POWER systems deliver electrical power from the generation site through a transmission network to the ultimate users of electrical energy. Modern power systems are sometimes referred to as the 'Smart Grid'. The term smart grid is used because modern power systems have become very agile and adaptive by learning about customers and their needs and by considering efficiency, reliability, economics and even sustainability in making decisions about operations and operating conditions of the system. In order to achieve this type of advanced flexibility, power systems have become increasingly reliant on Information and Communication Technology (ICT) [7], [10]. While there have been significant benefits through this evolution of the power system, it has also led to a significant increase in the vulnerability of the power system to cyber attacks and electronic intrusion.

The most stunning example of these issues in recent days is the Stuxnet event [1], [2], [10], in which electronic viruses were used to disrupt the function of specific types of Siemens Supervisory Control and Data Acquisition (SCADA) systems, which are configured to control and monitor specific industrial processes. Many thousands of machines were infected by the Stuxnet virus, but the virus contained very specific targets, and only those units were actually affected. In the remaining SCADA systems, the virus lay dormant and eventually removed itself after a certain amount of time. In the Stuxnet event, the specific industrial processes that were in fact targeted were the centrifuges in Iran that were being used for the enrichment of uranium. The effect of the Stuxnet virus was immediate and dramatic, and caused the abrupt suspension of the nuclear program in Iran until the infected controllers could be cleared of the virus. Interestingly the Stuxnet virus is now open source, allowing anyone access to the code through the internet. The Stuxnet event clearly shows that it is certainly possible to have a significant impact on industrial processes and to adversely affect the operation of complex interconnected systems, such as is the case in the effort by Iran to develop nuclear technology.

This proposal identifies a comprehensive set of cyber security challenges for real-world power systems including: information security, communication infrastructure security, and application-level security. Developing a strategy for addressing the vulnerability of the power grid is clearly the final goal of this work; however, before such a strategy can be created, a detailed understanding of the vulnerability must be developed. This detailed understanding can be created through the modeling of power systems and the subsequent testing and evaluation of cyber vulnerabilities, as presented in this proposal.

Dr. Raman Paranjape is with Electronic Systems Engineering, University of Regina (phone: 306 585 5290; fax: 306 585 4844; e-mail: Raman.Paranjape @uregina.ca).

II. Methods

A. Overview

We propose to develop a software agent modeling system to represent the power system. There are three broad categories of components which work together to form the power system. These components can be broadly described as: (1) power generation, (2) power distribution, and (3) power delivery/utilization. Our agent models will simulate the dynamics of each of these categories of components. For example, within the power generation category, there are various types of generation stations including coal, natural gas, hydro electric, wind, solar, nuclear, etc. Each of these types of generator stations has unique characteristics such as start up times, levels of operation, expenses, and the need for consistent fuel supply, among others. Each agent model will capture the unique characteristics of the component for generation.

The generation models will be connected to the locations of utilization using models for transmission and distribution. Typically most transmission lines use high-voltage three-phase alternating current (AC). Transformers are used to convert electrical power from the generation levels to high voltages for transmission. Models for these transformer components will be developed. The transmission lines themselves will also be modeled and will have specific characteristics including losses, coronal discharge, likelihood of failure, etc. High-voltage direct-current (HVDC) lines are also used for greater efficiency in long distance transmission. HVDC links can be better controlled in situations where there are sudden new loads or blackouts in parts of the network.

Electric transmission networks are interconnected into regional, national or continental networks, thereby providing

multiple redundant alternative routes for power to flow should failures occur. Electricity is transmitted at high voltages (110 kV-750 kV) to reduce the energy lost in long-distance transmission. Power is usually transmitted through overhead power lines. Underground power transmission has a significantly higher cost but is sometimes used in urban areas or other sensitive locations. The models will have to incorporate these attributes.

Once power is delivered to an area in which it will be utilized, the transmission network is subdivided into distribution networks. The distribution networks typically operate at lower voltages than the transmission voltages, but at significantly higher voltages than the levels at which electric power is utilized. Transformers are used to bring down voltages and then a network of distribution lines is used to deliver the power. Again, these components and their behavior can be modeled with agent technology.

The utilization of power is typically by the private citizen at the household level and by the corporate user at the industrial level. Generally, each of these users has a demand profile, and power companies attempt to match their production with these dynamic demands. Smart meters which record time-of-use and real-time or near real-time notification to the power utility are at the core of new Advanced Metering Infrastructure (AMI). Smart meters promote efficient and intelligent use of electricity by providing customers with a mechanism to reduce costs of electrical power by scheduling their utilization to off-peak periods. On the other hand, AMI may be the first place where wide spread cyber interference with the operation of the power utility ICT infrastructure may occur. This is because the smart meter is installed on the user's premises and is susceptible to hacking 24 hours a day and 7 days a week. The consequences of this type of attack on the power system can be dramatic in that this usage information drives production and transmission control. Erroneous and misleading information about power usage will result in serious production and distribution problems. Models for AMI will be created in the agent simulation.

A critical factor in the operation of the electrical power system is that the electrical energy cannot be stored. This means that electrical power must be generated at the same rate at which it is consumed. The control system that governs the generation of electrical power must synchronize precisely with the demand. If the demand for power exceeds the supply various scenarios could occur. Depending on the extent of the under supply, brown outs and scheduled power interruption may be required. In the worst case of unplanned under supply, transmission equipment and even generating plants will fail and regional blackouts will result.

To limit the risk of failure, electrical power systems are highly interconnected with multiple sources from which power may be supplied. One can immediately see that with such operating conditions, there is a great need for precise regulation, and there is very little tolerance for unmatched consumption and supply. All of this leaves the power system highly vulnerable to cyber attacks. Any latency in control signals, and/or errors in information used to make supply decisions can lead to significant problems in the function of the system.

A key issue in this project will be the basis on which the model of the power system components will be formulated. The approach proposed will be to use the various models of the components of the power systems that are available in the literature. Numerous modeling packages have been developed and are available in the public domain [11]. In addition, MatLab has an extensive Power Systems Toolbox [12] which can be used to define the characteristics of the Agent models of each of the components in the simulation. Due to the extensive, sophisticated, and wide availability of these packages, it is expected that it will be relatively straight forward to incorporate the dynamic external behavior of the components into the agent simulation.

It will be critically important to examine and explicitly define the interfaces between the power system components. It is at these interfaces that cyber attacks will likely be carried out. By affecting the data communication between components, a would-be attacker will try to misalign the data between components and their actual operations.

B. Additional Cyber Security Challenges

There are clearly a number of additional cyber security challenges that must be overcome in order to develop a system that will be immune to cyber attacks [10]. These challenges include:

Physical Access. The physical infrastructure has not been built to seriously restrict access, particularly in the case of remote infrastructure. Thus entities which are focused on attacking the system can, with relative ease, come into contact directly with the system that we are trying to secure.

Long Term Deployments. The equipment which forms the Power System is typically deployed for many decades. The equipment's life span is very long when compared to typical information technology equipment. As a result, potential cyber-attackers of the infrastructure have a target that is unchanged for a very long time.

Typically "fail-open" Function. Most power system infrastructure is designed to fail-open. This means that in the event of failure the unit will continue to provide power to the system to the best of its ability. This approach is common in power systems in order to maximize service under fault conditions. However, this also means that a component under attack will not shut down or stop operating in the event that an attack is initiated against it. Thus the attacker has an unlimited opportunity to continue an attack until an intrusion becomes successful.

Legacy Systems. The power system is dependent on a large number of components that are called legacy systems. These legacy systems were built and put into service at a point in time when significant security mechanisms were not considered necessary.

C. Attributes of Cyber Secure Power Systems

In order for a power system to be secure from cyber attack, the system must have attack-resilient monitoring to detect and

recognize that an attack is underway. The system must have protection and control algorithms that have cyber resilience. The system must be able to withstand a coordinated attack, as this is a common feature of these attacks. The secure power systems must have sophisticated strategies to deal with attacks on Advanced Metering Infrastructure. Finally, a key issue is that power systems must have adequate trust management and data attribution so that it will be straightforward to identify who is responsible for data, control signals, and communication signals.

The agent models will eventually include these additional challenges.

III. Limitation of Current Simulations

The currently available models and simulations have been focused primarily on operations [7], [10]. Therefore, they are designed to optimize the basic infrastructure of the power system with regard to functionality but are totally inadequate to deal with malicious and direct focused threats to the system. Traditional models and algorithms are robust enough to deal with random and naturally occurring faults, but in order to deal with malicious cyber attacks, there is a pressing need to develop novel models and attack resilient algorithms which span across generation, transmission, and distribution systems. The new models need to quantify the potential consequences of a cyber-attack on the power grid. This must include load loss, stability violations, equipment damage, and economic loss. The new models must characterize various forms of cyber-attacks including denial of service attacks, intrusion-based attacks, malware-based attacks, isolated attacks, and coordinated attacks. The countermeasures must address both outsider and insider attacks, and also operator errors. The algorithms must consider sophisticated attacker models (in addition to brute-force attacks) wherein the attacker(s) has knowledge of both cyber security and power system operation with the potential to cause maximum damage.

Fundamentally new algorithm characteristics will include: (1) Real-time correlation (temporal and spatial) of data streams and data logs to ensure consistency of data obtained from substations and control centers are needed. Appropriate hardware and software will need to be introduced in order to affect this type of confirmation of data streams. (2) Continuous monitoring and evaluation will be required in order to assess system stability/uncertainty due to cyber attacks (e.g., denial of service causing delayed or dropped sensing/control signals, etc.) (3) Physical defenses such as rerouting and network partitioning will have to be immediately available, as well as power defenses such as generation shift, reactive power dispatch, load shedding, etc. (4) Coordinated cyber attacks over the spatial and temporal extent of the power system will have to be considered as well.

IV. Recent Progress

The development of agent based models has been an important research theme in our lab. We have a great deal of expertise in the modeling and simulation of complex interacting systems using agent technology. We first started developing agent models in 1998 and shortly thereafter developed our own agent execution environment called TEEMA [27], [28]. The TEEMA environment has been used to model everything from load balancing [26], scheduling [13], [22], [23] to shopping [30] and e-commerce [24], and to a great extent health care system components. These include mammogram retrieval [19], [25], neuro-surgery ward utilization [20], and diabetes within the patient [14], [20] and diabetic patient interaction with the health care system [15], [16]-[18], [21], [29]. This work in agent based modeling demonstrates our ability to develop sophisticated simulations using agents and our ability to extract complex unpredictable system dynamics from the behavior of these agent models.

Objectives:

The short term objectives will be to develop an accurate representation of a subset of the components which form the power system. We will first build only a single generation station facility (likely a coal fired power plant model), a simple transformer/transmission/transformer distribution model, and a set of users both industrial and household. We will concentrate on the interfaces and the communication links. Our development will be in a cyclic spiral in which the scope and fidelity of the simulation increases with each cycle. This will represent 5-6 autonomous agent models which will interact. We will then challenge this simulation with various attacks such as denial-of-service, authentication, delay, erroneous data, loss of connectivity, etc. We will attempt to characterize the dynamics of this very small scale model. Based on these results we will expand the model and will add new components, such as additional generation, more complex transmission and distribution, and a full profile of users. We will quickly move to adding the AMI, as it is our belief that power utilities are keen to install these systems in order to improve operations, but are also weary of the dangers of the tampering and affecting of system operations.

Our long term objectives are to develop a framework for the systematic investigation of cyber vulnerability of the power systems. Thus we plan to characterize the dynamics of cyber attacks on the power system and extract from our simulations the fundamental dynamics of these systems in order to define this framework.

V. Literature Review

This area of research is very new and is very important to our modern society [7]-[10]. As indicated, there is a pressing need to evaluate cyber vulnerabilities and to develop strategies to limit the consequences of these types of attacks.

There is little scientific literature available in this area. A number of position papers have been proposed, which speak mainly to the importance of this work rather than the work itself [3]-[6].

It is universally agreed that modeling and simulation will be the most effective paradigm to investigate this system weaknesses [10].

The precise form of the structure of the model is open to

debate. However, given our long record of effective modeling of complex systems using agent technology, we are in a unique position to rapidly develop effective simulations which can then be used to test behaviors of the power system under attack.

Impact:

The impact and significance of this research is enormous [7], [10]. The Government of Canada recently reported to the National Parliament on the state of Canada's preparedness for cyber attacks on critical infrastructure. Power utilities are scrambling to address this issue. Locally, in Saskatchewan, the utility SaskPower has expressed a significant desire to have work done in this area.

VI. Summary and Conclusions

The objectives of the proposed research program are to build a simulation of the typical components of a power generation system with sufficient detail to allow an examination of the issues around security of these systems from threats of cyber attack. This is a pressing and important problem in today's world. Canadian society is in significant danger of negative consequences if such attacks were to occur without appropriate planning and defensive strategies in place.

Our scientific approach will be to develop a software agent simulation of the power system. The use of software agents allows the development of independent software representations of each component. The interfaces between components then become the critical points at which cyber attacks can be initiated. The effects of various forms of cyber attacks will be considered, including denial of service, delay, failure of components, etc. Mitigation strategies can be tested within the model. Our development process will be an expanding cyclical spiral allowing an expanding degree of fidelity to be incorporated into the simulation. This is important practical and applied research which critically needs to be done for the safety and security of Canadian society.

Acknowledgment

The author acknowledges the support of University of Regina and SaskPower Inc.

References

[1] http://en.wikipedia.org/wiki/Stuxnet
[2] Symatec web page: http://www.symantec.com/content/ en/us/enterprise/ media/security_response/whitepapers/w32_stuxnet_dossier.pdf
[3] B. Dobras, M. Randic and G. Gudas, Agent-based Modeling of Transmission Power System for Supervision and Control, IEEE MELECON 2004, May 12-15,2004, Dubrovnik, Croatia
[4] J. Lin, S. Sedigh, and A. Miller, A General Framework for Quantitative Modeling of Dependability in Cyber-Physical Systems: A Proposal for Doctoral Research, 33rd Annual IEEE International Computer Software and Applications Conference, 2009, Seattle , Washington.
[5] B. Akyol, J. Haack, B. Carpenter, S. Ciraci, M. Vlachopoulou and C. Tews, VOLTTRON: An Agent Execution Platform for the Electric Power System, Agent Technologies for Energy Systems, 11th International Conference on Autonomous Agents and Multiagent Systems (AAMAS 2012), June 4–8, 2012, Valencia, Spain
[6] David Watts, Security & Vulnerability in Electric Power Systems, NAPS 2003, 35th North American Power Symposium, pp. 559-566., October 20-21, 2003, Rolla, Missouri
[7] Markus Braendle, White Paper: Balancing the Demands of Reliability and Security Cyber Security for Substation Automation, Protection and Control Systems, ABB Group, http://www02.abb.com/global/abbzh/ abbzh254.nsf/0/86bf36c9469666ddc125791200336283/$file/Whitepaper _BalancingReliabilitySecurity.pdf.
[8] W. Kroger, Critical infrastructures at risk: A need for a new conceptual approach and extended analytical tools, Reliability Engineering and System Safety, pp. 1781– 1787, vol. 93, 2008.
[9] CW. Ten, CC. Liu, M. Govindarasu, Vulnerability Assessment of Cybersecurity for SCADA Systems Using Attack Trees, IEEE Power Engineering Society General Meeting, June 2007.
[10] M. Govindarasu, A Hann, P. Sauer, Cyber-Physical Systems Security for Smart Grid Future Grid Initiative White Paper, PSERC Publication, February 2012.
[11] Federico Milano, An Open Source Power System Analysis Toolbox, IEEE TRANSACTIONS ON POWER SYSTEMS, VOL. 20, NO. 3, AUGUST 2005.
[12] MatLab Power System Toolbox, (available at) http://www.mathworks.com/matlabcentral/linkexchange/links/86-power-system-toolbox.
[13] Y. Yang, R. Paranjape, A Multi-agent System for Course Timetabling, Intelligent Decision Technologies, IOS Press, 5(2), 2011.
[14] R. Paranjape, S. Gill, S. Ghoreishi-Nejad, R. Martens, An agent-based simulation system for modelling a diabetic patient, Int. J. Intelligent Information and Database Systems, Vol. 4, No. 3,pp264-281 2010.
[15] R. Paranjape, A. Sadanand, (Editors) Multi-Agent Systems for Healthcare Simulation and Modeling: Applications for System Improvement, IGI Global Publishing, (304 pages) 2009.
[16] R. Paranjape, S. Gill, Agency in Health Care System Modeling and Analysis, Chapter 4, in Multi-Agent Systems for Healthcare Simulation and Modeling: Applications for System Improvement, Paranjape/ Sadanand (Eds), IGI Global Publishing, pp 45-68, 2009.
[17] S. Gill, R. Paranjape, A Review of Recent Contributions in Agent-Based Health Care Modeling, Chapter 3, in Multi-Agent Systems for Healthcare Simulation and Modeling: Applications for System Improvement, Paranjape/ Sadanand (Eds), IGI Global Publishing, 2009.
[18] Q-A Liu, R. Paranjape, Y. Yang, Dynamic Mammogram Retrieval from Web-based Image Libraries Using Multiagents, in Handbook of Medical Image Processing (2nd Edition), Issac Bankman (Ed), Elsevier, Chapter 53, pp 893-901, 2008.
[19] B. Tse, R. Paranjape, S. Joseph, Information Flow Analysis in Autonomous Agent and Peer-to-Peer Systems for Self-Organizing Electronic Health Records, In Agents and Peer to Peer Computing, Joseph S.R.H., Despotovic Z., Moro G. & Bergamaschi S., (Eds), Lecture Notes in Artificial Intelligence, Volume 4461, pp 1-20, 2008.
[20] S. Ghoreishi-Nejad, R. Martens, R. Paranjape, An Agent-Based Diabetic Patient Simulation, KES-AMSTA N.T. Nguyen (Ed), Lecture Notes in Artificial Intelligence, Volume 4953, pp. 832–841,2008.
[21] Tse B., Paranjape R., Macroscopic Modeling of Information Flow in an Agent-Based Electronic Health Record System, in Architectural Design of Multi-Agent Systems: Technologies and Techniques, H. Lin (Ed), Chapter 16, Information Science Reference, pp305-334, 2007.
[22] Saenchai K., Benedicenti L., Paranjape R., Solving Dynamic Distributed Constraint Satisfaction Problems with a Modified Weak-Commitment Search Algorithm, Lecture Notes in Computer Science, Volume 3910, pp. 130-137, 2006.
[23] Yang Y., Paranjape R., Benedicenti L., Reed N., A System Model for University Course Scheduling using Mobile Agents, Multiagent and Grid Systems - An International Journal, Issue 3, Volume 2, pp 267-275, 2006.
[24] Martens R., Paranjape R., Benedicenti L., Sankaran S., Sadanand A., Mobile Agent Strategies for the Provision of Public Goods: An Experimental Study., Electronic Commerce Research and Applications, Volume 5, Issue 2, pp 140-146, 2006.
[25] Alto H., Rangayyan R., Paranjape R., Desautels L., Bryant H., An indexed atlas of digital mammograms for computer-aided diagnosis of breast cancer., Annals of Telecommunications Vol. 58 n°5-6, may-june 2003.
[26] Smith K., Paranjape RB., Benedicenti L., Agent Behavior and Agent Models in Simple Markets. ACM Applied Computing Review, ACM Press, Fall, 2001.

[27] Benedicenti L., Wang W., Lee P., Paranjape R.B., Establishing Quality Control in Software Agents. ACM Applied Computing Review, ACM Press, Fall, 2001.
[28] Benedicenti L., Paranjape RB., Smith K, Flexible Manufacturing for Software Agent , Chapter 32, in EXtreme Programming Examined, G. Succi., M. Marchesi, Editors, Addison Wesley, pp537-544, 2001.552
[29] Paranjape RB. Smith K., Mobile Software Agents for Web-Based Medical Image Retrieval, Journal for Telemedicine and Telecare, Vol 6., S2, pp53-55, 2000
[30] Puttha J., Benedicenti LB., Paranjape RB., Mobile Agents for Economic Market Simulation, Canadian Conference on Electrical and Computer Engineering, Winnipeg, Canada, May 12-15, 2002.235423

Raman Paranjape (IEEE M'77) Dr. Paranjape's research interests are in both physical systems and software systems. Research in physical systems has focused on the development of sensor systems and new technologies in image and signal processing for real world applications in robotics and automated systems. Within the area of sensor technologies research applications include sensor packs for robotics in charged water pipe inspection, and flying robots (UAVs) using both vision and inertial sensor arrays.

Dr. Paranjape also has a strong research program in mobile and software agent systems in Health Care Simulation and Modeling. There are two main areas in this work: Analysis and Retrieval of Medical Data from Distributed Databases and Modeling of Agent and Human Societies.

Dr. Paranjape has worked as a Research Scientist, Software Engineer, Project Leader, and Project Manager in Canadian Industry. He is currently the Professor of Electronic Systems Engineering at the University of Regina. He has published 44 reviewed journal articles and book chapters, 74 conference papers and has numerous grants and research projects.