Chapter 11

SECURITY CHALLENGES OF RECONFIGURABLE DEVICES IN THE POWER GRID

Suvda Myagmar, Roy Campbell and Marianne Winslett

Abstract Control systems used in the electrical power grid cover large geographic areas with hundreds or thousands of remote sensors and actuators. Software defined radios (SDRs) are a popular wireless alternative for replacing legacy communication devices in power grid control systems. The advantages include a low-cost, extensible communications infrastructure and the ability to reconfigure devices over-the-air, enabling the rapid implementation and upgrade of control networks.

This paper focuses on the security issues related to deploying reconfigurable SDR devices as communication platforms for substations and field instruments in the power grid. The security goals are to prevent the installation and execution of unauthorized software, ensure that devices operate within the allowed frequency bands and power levels, and prevent devices from operating in a malicious manner. The main challenges are to dynamically and securely configure software components supplied by different vendors, and to validate device configurations. This paper analyzes the security goals and challenges, and formulates security requirements for a trusted SDR device configuration framework.

Keywords: Power grid, reconfigurable devices, software defined radios, security

1. Introduction

Critical infrastructures are systems whose failure or destruction could have a debilitating impact on a nation's economy [2]. One of the largest critical infrastructure systems is the electrical power grid. The North American power grid involves nearly 3,500 utilities delivering electricity to 300 million people over more than 200,000 miles of transmission lines. Yet, this critical infrastructure is susceptible to grid-wide phenomena such as the 2003 blackout that affected

Myagmar, S., Campbell, R. and Winslett, M., 2008, in IFIP International Federation for Information Processing, Volume 253, Critical Infrastructure Protection, eds. E. Goetz and S. Shenoi; (Boston: Springer), pp. 147–160.

50 million people in the northeastern United States and Canada, and caused financial losses of approximately $6 billion.

As was highlighted in the aftermath of the 2003 blackout, the power grid has an antiquated communications infrastructure. The architecture often limits the deployment of control and protection schemes involved in managing power generation, transmission and distribution. Ideally, grid companies desire fine-grained monitoring and control of their distribution networks, even down to the last transformer. Supervisory control and data acquisition (SCADA) systems are being used to monitor and control substations and field instruments. However, many distribution substations do not have SCADA systems and require manual monitoring and control. For example, one Illinois power company has only 200 of its 550 substations equipped with SCADA systems.

A SCADA system gathers information (e.g., about voltage spikes) from field instruments, and transfers the information back to the substation and control center. It alerts the control center of alarm conditions (e.g., voltages above or below critical levels), and allows the control center to take the appropriate control actions on the distribution system. Implementing SCADA systems on power grid substations requires the installation of a communications infrastructure that connects the control center to legacy field devices such as remote terminal units (RTUs) as well as modern equipment such as intelligent electronic devices (IEDs) and synchronous phaser measurement units (PMUs) that give insights into grid dynamics and system operations [4]. However, this data cannot easily be utilized beyond the substation when the power grid has a limited communications infrastructure.

There is also a need for point-to-point communications between substations to implement special protection schemes (SPSs). SPSs address some of the wide-area control issues where the occurrence of events at one point in the grid trigger actions (e.g., tripping breakers) at another. Current communication architectures do not link substations directly. A communications network is needed to connect SCADA control centers with substations and field instruments, and to link substations. Such a network can be very expensive to build and maintain.

Most companies rely on leased lines from telecom providers, which have very high installation and maintenance costs. Leased telephone channels also provide limited reliability and sometimes may not even be available at substation sites. In fact, one company recently disclosed to us that the local phone company would no longer provide dedicated copper lines for their substations.

Power line carrier (PLC), which uses power lines to transmit radio frequency signals in the 30–500 kHz range [6], is more reliable than leased telephone lines. However, power lines are a hostile environment for signal propagation with excessive noise levels and cable attenuation. Also, PLC is not independent of the power distribution system, which makes it unsuitable in emergency situations as communication lines must operate even when power lines are not in service.

Wireless technologies are an attractive option because they offer lower installation and maintenance costs than fixed lines, and provide more flexibility in

network configurations. The possibilities include satellites, very high frequency radio, ultra high frequency radio and microwave radio. Advantages of satellite systems are wide coverage, easy access to remote sites and low error rates; the disadvantages include transmission time delay and leasing costs incurred on a time-of-use basis.

Very high frequency (VHF) radio operates in the 30–300 MHz band and is mostly reserved for mobile services. On the other hand, ultra high frequency (UHF) systems operate in the 300–3,000 MHz band, and are available in point-to-point (PTP), point-to-multipoint (PTM), trunked mobile radio (TPR) and spread spectrum systems. VHF radios and UHF radios (PTP and PTM) can propagate over non-line-of-sight paths and are low-cost systems, but they have low channel capacity and digital data bit rates. Spread spectrum systems are the basis for many wireless applications, including 802.11 networks, and can operate with low power radios without licenses. However, these radios are subject to interference from co-channel transmitters and have limited path lengths because of restrictions on RF power output.

Microwave radio is a UHF scheme that operates at frequencies above 1 GHz. These systems have high channel capacities and data rates. However, microwave radios require line of sight clearance, are more expensive than VHF and UHF, and the appropriate frequency assignments may not be available in urban areas.

A SCADA radio device can be implemented using any of the technologies mentioned above. Figure 1 illustrates how wireless communications could be deployed in the power grid. Researchers have conducted evaluations of radio technologies, especially 802.11, GPRS and 900 MHz [8, 9]. Each technology has one or more disadvantages, and may become outdated in the long term. More importantly, it is costly and time consuming to upgrade thousands of devices. This is the reason why power grid communications lines and equipment that were installed decades ago are still in place.

An ideal radio platform for the power grid would accommodate future wireless communication needs, have low installation and maintenance costs, and support reconfiguration and updates of its operation and software. These considerations favor the use of software defined radio (SDR) as a platform for the power grid. SDR implements radio device functions such as modulation, signal generation, coding and link-layer protocols as software modules running on generic hardware platforms. Traditional radios are built for particular frequency ranges, modulation types and output power. On the other hand, SDR radio frequency (RF) parameters can be configured while a device is in use. This enables highly flexible radios that can switch from one communications technology to another to suit specific applications and environments. Furthermore, the protocols that implement various radio technologies and services can be downloaded over-the-air onto SDR devices.

Software radio is a suitable wireless media to replace legacy communications devices in the power grid. The reconfigurability of SDR supports the integration and co-existence of multiple radio access technologies on general-purpose

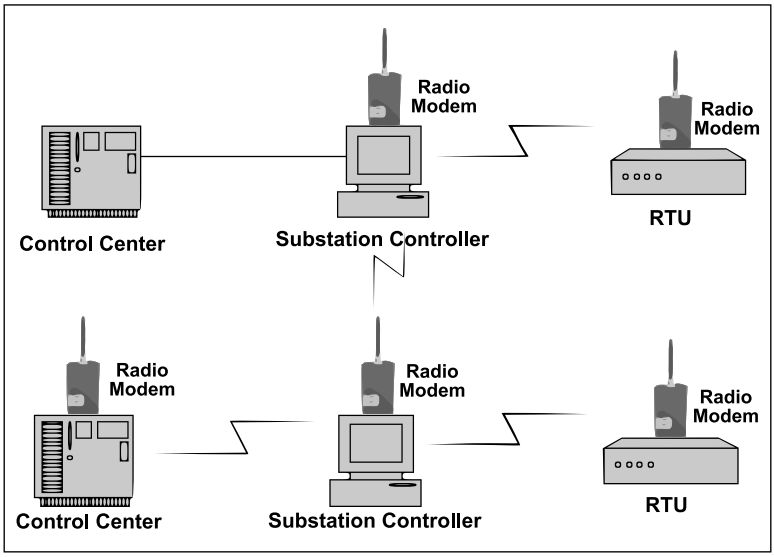

Figure 1. Wireless communications in the power grid.

radio equipment, facilitating the implementation of powerful SCADA networks. At the same time, the wireless and reconfigurable nature of SDR introduces potentially serious security problems such as unauthorized access, spoofing or suppression of utility alarms, and the configuration of malfunctioning or malicious radio equipment.

This paper examines the security issues involved in deploying SDR devices in the power grid. The security goals are to prevent the installation and execution of unauthorized software, ensure that devices operate in the allowed frequency bands and power levels, and prevent devices from operating in a malicious manner. The main challenges are to dynamically and securely configure software components on radio devices that possibly originate from different vendors, and to attest the validity of radio device configurations to a master node. This paper analyzes the security challenges in detail, and formulates security requirements and a trusted configuration framework for SDR devices in the power grid.

2. Software Defined Radios

The Federal Communications Commission (FCC) has adopted the following regulatory definition for a software defined radio (SDR) [3]:

> A radio that includes a transmitter in which the operating parameters of frequency range, modulation type or maximum output power (either radiated or conducted) can be altered by making a change in software without making any changes to hardware components that affect the radio frequency emissions.

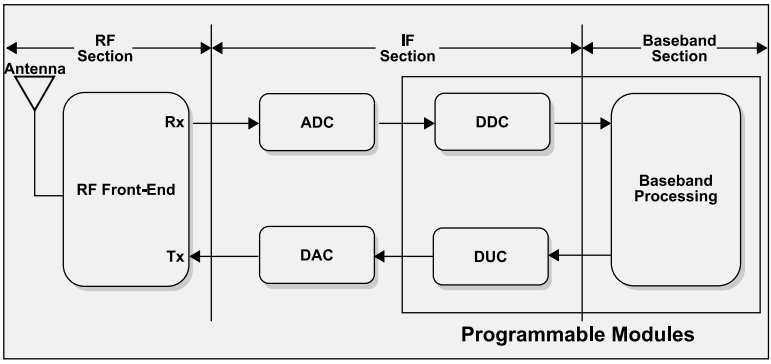

Figure 2. Digital radio transceiver.

We begin by examining how a software radio differs from a regular digital radio. Figure 2 shows the block diagram of a digital radio transceiver consisting of a radio frequency (RF) front-end, intermediate frequency (IF) section and baseband section. The RF front-end serves as the transmitter and receiver of RF signals transmitted/received via the antenna. It "down-converts" an RF signal to an IF signal or "up-converts" an IF signal to an RF signal. The IF section is responsible for analog-to-digital conversion (ADC) and digital-to-analog conversion (DAC). The digital down converter (DDC) and digital up-converter (DUC) jointly assume the functions of a modem.

The baseband section performs operations such as connection setup, equalization, frequency hopping, timing recovery and correlation. In SDR, baseband processing and the DDC and DUC modules (highlighted in Figure 2) are designed to be programmable via software [10]. The link layer protocols, modulation and demodulation operations are implemented in software.

In an electric utility environment, system upgrades and bug fixes are easier with reconfigurable devices than fixed devices. SDR enables the rapid introduction of new applications in a SCADA system. However, SDR technology has several technical challenges that need to be resolved before it can be successfully deployed. The challenges include advanced spectrum management for dynamic allocation of spectrum according to traffic needs, robust security measures for terminal configuration, secure software downloads, prevention of system misuse, and open software architectures with well-defined interfaces.

To successfully deploy SDR devices in the electrical power grid, it is important to address the problems of secure configuration of radios and the attestation of radio configurations to a master node in the grid. Before examining the security issues, we briefly discuss SDR configuration and attestation.

2.1 Radio Configuration

The primary challenge in SDR configuration is to compose radio software components according to certain constraints (e.g., regulatory requirements,

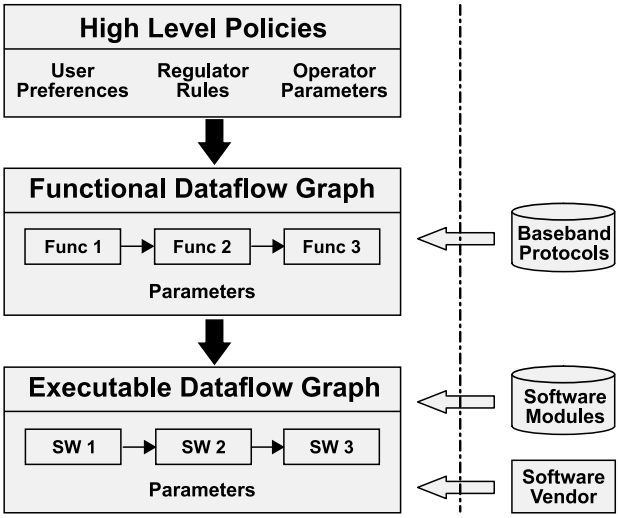

Figure 3. Composition model.

wireless communication requirements for the power grid and device hardware specifications). These constraints are provided in the form of machine-readable policies, which specify the radio access technology (e.g., GSM, UMTS), allocated frequency band (e.g., 806–902 MHz), and hardware parameters (e.g., IF, power, interfaces). The difficulty lies in mapping the configuration policies into a "functional dataflow graph" and, then, into an "executable dataflow graph." The executable dataflow graph specifies the software modules that implement various functional blocks; it is used to activate new radio modes.

The configuration process involves a sequence of steps. First, the utility application or SCADA master node requests a new configuration of the terminal. Next, rules and policies specifying regulatory and power grid communication requirements are downloaded to the terminal. Then, the requester sends its specifications for a new configuration along with the request if the specific configuration has not been activated previously on the terminal.

At the heart of configuration composition is the problem of mapping high-level policies into the executable dataflow graph. High-level policies are a collection of regulatory rules and wireless communication parameters for the power grid. First, these policies are mapped into an intermediate graph that we call a "functional dataflow graph." The functional graph is constructed according to a baseband protocol specified in the high-level policies, and it consists of functional blocks and their parameters. Then, the functional graph is mapped into the executable dataflow graph consisting of software modules and their associated parameters. If suitable software modules are not available in the local repository, they may be downloaded from a software vendor via the SCADA control center. Figure 3 presents a high-level view of the composition model.

A baseband protocol specifies the order and type of the mathematical functions used to process the signal stream. For example, if the radio access technology is GSM, the baseband protocol specifies the types and order of the modulators, encoders and filters used for processing signals.

2.2 Remote Radio Attestation

The substation or control center may request a proof of conformity with the standards before allowing a field instrument or substation to participate in utility operations. The challenge in remote attestation is to enable the terminal to prove to its master node that its configuration is in compliance with standards and regulations, and it is not a rogue or malfunctioning device. Should the configuration be found as non-conforming at any point, the terminal rolls back to a previously-validated configuration.

The remote attestation process starts with a request from the master node to attest the configuration of the remote device before it participates in utility communications. This is done to ensure that the terminal is configured correctly to fully benefit from the service, and also to prevent a misconfigured terminal from interfering with other communications. Normally, the master node validates the remote device once in the beginning; it subsequently verifies that the device configuration has not been modified.

3. Security Challenges

The *IEEE Guide for Electric Power Substation Physical and Electronic Security* [5] cautions that the increased use of computers to remotely access substations may be exposing control and protection devices to the same vulnerabilities as traditional IT systems. Indeed, serious concerns have been raised about cyber threats to critical infrastructure components such as the power grid. The President's Commission on Critical Infrastructure Protection (PCCIP) [2] and IEEE [5] have issued reports that highlight the threats to utilities. Categories of threats that are specific to SCADA systems, substation controllers and field instruments are [7]:

- Blunders, errors and omissions
- Fraud, theft and criminal activity
- Disgruntled employees and insiders
- Recreational and malicious hackers
- Malicious code
- Industrial espionage
- Foreign espionage and information warfare

Security issues relating to general RTUs, substations and wireless devices are discussed elsewhere (see, e.g., [7]). This paper focuses on security issues

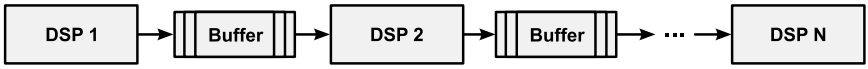

Figure 4. Generic flow graph of DSP modules.

that are unique to software radios. Since the distinguishing characteristic of a software radio is its reconfigurability, the primary issue is configuration security.

Before designing protection mechanisms for SDRs in the power grid, it is necessary to conduct a detailed security analysis of the system. For this purpose, we utilize a three-step threat modeling technique:

- **System Characterization:** This step focuses on understanding system components and their interconnections, and creating a system model that captures its main characteristics.

- **Asset and Access Point Identification:** This step involves the identification of the abstract and concrete system resources that must be protected from misuse by an adversary, and the identification of the points of access to these resources.

- **Threat Identification:** This step involves an examination of the identified security-critical assets, a review of the attack goals for each asset that violate confidentiality, integrity or availability, and the creation of a threat profile of the system describing the potential attacks that must be mitigated.

First, we clarify some important concepts of the SDR architecture. In the previous section, we discussed the steps involved in the configuration process, but did not explain how a radio configuration is represented in the system.

An SDR configuration describes the waveform and digital signal processing (DSP) modules that define the radio operating mode, the interconnections between the modules, and the input parameters for the modules. At the core of a radio configuration is a set of pipelines, each containing several DSP modules in a row. A pipeline is also referred to as a "flow graph" because it depicts the flow of transmitted/received data as it is processed by one DSP module after another. Figure 4 shows a generic flow graph characterizing the configuration of an SDR terminal. The vertices of the graph are DSP modules that perform various mathematical manipulations (e.g., modulation, filtering or mixing) of the input signal stream. The edges of the graph indicate the direction of data flow and the connections to adjacent DSP modules via memory buffers, which temporarily store the signal stream being processed.

SDR threats may result from deliberate overt or covert actions of third parties (e.g., hackers and viruses), or through human error (e.g., software bugs). The points of attack are the communications infrastructure and end terminals.

3.1 Security Threats

The following security threats relating to SDR configuration were identified by the threat modeling effort. We provide the classification of each threat (in parentheses), and describe its effects and consequences.

- **Configuration of a Malicious Device (DoS, Disclosure)** A malicious user may configure a SDR terminal so that it becomes an eavesdropping or jamming device. A malicious device with sufficiently high power could force other devices in the communications network to operate at higher power levels, causing them to drain their batteries. If the network devices do not change their power levels, their communications are disrupted.
- **Violation of Regulatory Constraints (DoS):** A device may be configured so that it does not adhere to regional regulations and equipment specifications (e.g., EMC emission requirements). This may render the device inoperable. Also, the device may unintentionally operate in unauthorized bands (e.g., military use bands).
- **Invalid Configuration (DoS):** A device could be configured so that it does not work or it works incorrectly. The received and transmitted signal streams may be processed incorrectly, resulting in garbled messages. The wireless protocol specified by the master node or the utility provider could be disregarded.
- **Insecure Software Download (Tampering):** Configuration and other system software may be illegally modified en route, or an adversary may supply malicious software. This enables the launching of other attacks such as the configuration of a malicious device or exhaustion of system resources.
- **Exhaustion of System Resources (DoS):** Malicious or buggy software may launch DoS attacks against legitimate processes by consuming system resources such as memory.
- **Improper Software Functionality (Tampering):** Even software supplied by a certified vendor or downloaded from a trusted master node could be buggy. It might not work properly or implement the expected functionality. Such software can accidentally modify process parameters or garble a signal stream (e.g., via a buffer overflow).
- **Unauthorized Access to Private Data (Information Disclosure):** Sensitive information is involved in the configuration process. Access to information about communication specifications and configuration data must be protected.

The threats identified above serve as the basis for deriving the security objectives and requirements of the configuration framework. Note that other threats

(e.g., unauthorized use of network services and unauthorized login into radio devices) also concern SDR devices, but they are outside the scope of this work.

3.2 Security Requirements

To mitigate the above security threats, we specify the following security requirements for the SDR configuration framework:

- It shall prevent the loading, installation and instantiation of unauthorized or unproven software.
- It shall ensure the secrecy and integrity of over-the-air software downloads.
- It shall verify that downloaded software is supplied by a certified vendor.
- It shall ensure that SDR terminal operations are limited to frequency bands and power levels authorized by regulatory bodies and power grid operators.
- It shall implement a trusted configuration module responsible for flow graph construction.
- It shall provide fault domain isolation for reconfigurable modules so that each module has access only to its own memory area.
- It shall ensure that software installed on terminals is not modified or tampered with when the terminals are in a powered down condition.
- It shall ensure confidentiality, integrity and authenticity of information used in the configuration process.
- It shall provide trusted configuration information to other nodes in the power grid on request.

4. Configuration Framework

The SDR configuration framework presented in Figure 5 is designed to support trusted radio platforms for field instruments and substations in the electrical power grid. The framework consists of the following components:

- **Execution Environment:** This environment provides a platform for executing all equipment functions, including configuration management and control. The challenge for SDRs is to ensure that applications cannot access information or interfere with the flow of information at a higher security classification (e.g., during device configuration). A secure partitioning method is needed to support multiple levels of security on a single processor. A secure memory management unit (MMU) with hardware-enforced memory protection can be used to isolate data in different partitions.

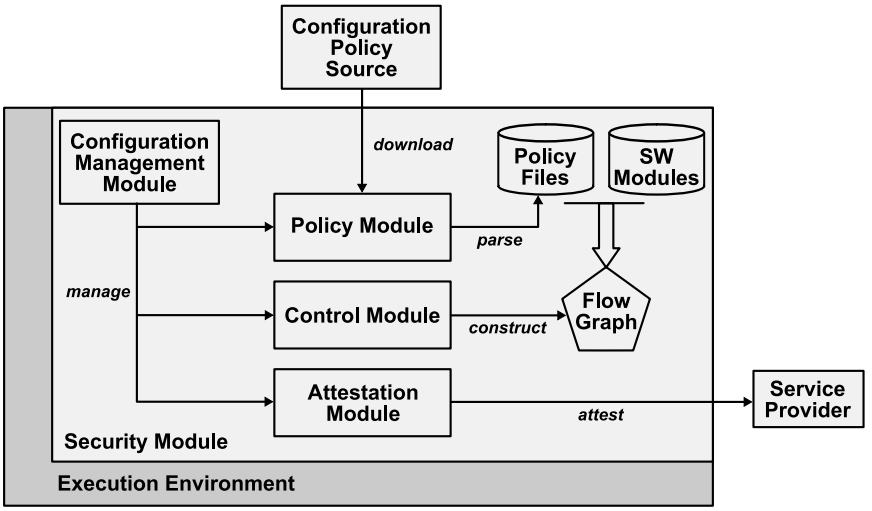

Figure 5. Configuration framework.

- **Security Module:** This module ensures that all the security requirements specified for the configuration process are satisfied. It provides the basic security functions to all other configuration modules. For example, it provides authentication functionality to the MMU when a DSP module attempts to access the shared memory buffer of a flow graph.

- **Configuration Management Module (CMM):** This module is responsible for managing all configuration activities. It initiates, coordinates and performs configuration functions, and manages communications between all configuration-related components. The module also supports tasks such as mode selection, download of configuration policies and software modules, and approval of new radio configurations.

- **Configuration Control Module (CCM):** This module is designed to support the CMM by controlling and supervising reconfigurations. The selected and verified configuration policy is passed to the CCM for construction of a flow graph composed of DSP modules specified in the policy. The flow graph is then executed by the runtime environment, which activates the requested radio operating mode. The module also ensures that the new configuration is in compliance with regulatory requirements before executing the configuration.

- **Policy Management Module (PMM):** This module provisions a configuration policy for a new configuration approved by the CMM. It parses and verifies downloaded configuration policies, and manages the update and versioning of the local policy repository. XML is used to specify

configuration policies and descriptors of reconfigurable software modules such as DSP modules.

- **Configuration Attestation Module (CAM):** This module provides trusted configuration information to the service provider upon request. Software attestation enables an SDR device to prove to its master node that it is configured properly.

Other modules within the framework include local repositories of configuration policies and reconfigurable software modules. The repository of software modules containing DSP modules and link protocols is not strictly a part of the configuration framework. However, these modules are the main target of the configuration process as it composes the modules into a flow graph according to the configuration policy to activate a particular radio operating mode.

The configuration framework described above satisfies the security requirements listed in the previous section. The focus of this paper has been to identify the security challenges that impact the deployment of SDRs in the power grid. Implementation details and proofs of security properties for the configuration framework will be provided in a future publication.

5. Related Work

Several researchers have investigated the use of wireless protocols in the electrical power grid, but SDR applications have been largely ignored. Shea [9] has described the deployment of 900/928/952 MHz radios by the Houston Lighting and Power Company in its SCADA systems for power distribution. The deployment of these radios for master-RTU communications resulted in lower installation and maintenance costs, while providing higher reliability than leased phone lines. Problems included occasional interference from systems operating in neighboring bands, and regulatory constraints regarding frequency licensing and the maximum distance between master units and RTUs.

Eichelburg [1] has presented a wireless communication architecture that uses GPRS modems to connect medium-voltage substations in a German municipal utility; GRPS modems combined with VPN routers enable substations to communicate with the SCADA control center through the public Internet. Risley and Roberts [8] have analyzed the security risks associated with the use of 802.11 radios in the electrical power grid. Also, they have identified security flaws inherent in the WEP encryption of the 802.11 protocol.

6. Conclusions

The existing communications infrastructure for controlling the electrical power grid is inadequate. The installation of fixed communications lines is expensive. Wireless technologies such as VHF, UHF and microwave radios are reliable, low-cost alternatives, but they have some disadvantages that make it difficult for utility companies to incorporate them in long-term solutions.

Software defined radio (SDR) appears to be an ideal technology to accommodate current and future wireless communication needs. Like all radio solutions, it has low installation and maintenance costs. Furthermore, new wireless protocols may be downloaded and configured to activate new radio modes. This ability to reconfigure devices over-the-air facilitates the rapid implementation and upgrade of power grid control networks.

Our investigation of security issues specific to deploying SDRs in the power grid has identified several challenges. They include the configuration of malicious devices, insecure software downloads, and violations of regulatory constraints. These challenges can be addressed by dynamically and securely configuring SDR devices, and by validating device configurations. The configuration framework presented in this paper is an attractive solution because it supports secure radio configuration and remote attestation of SDRs.

Acknowledgements

This research was undertaken under the TCIP Project: Trustworthy Infrastructure for the Power Grid, which was supported by National Science Foundation Grant CNS–0524695.

References

[1] W. Eichelburg, Using GPRS to connect outlying distribution substations, *Proceedings of the Eighteenth International Conference and Exhibition on Electricity Distribution*, vol. 3, p. 54, 2005.

[2] J. Ellis, D. Fisher, T. Longstaff, L. Pesante and R. Pethia, Report to the President's Commission on Critical Infrastructure Protection, Special Report CMU/SEI-97-SR-003, Software Engineering Institute, Carnegie Mellon University, Pittsburgh, Pennsylvania, 1997.

[3] Federal Communications Commission, In the Matter of Authorization and Use of Software Defined Radios, First Report and Order (FCC 01-264), Washington, DC (www.fcc.gov/Bureaus/Engineering_Technology/Orders/2001/fcc01264.pdf), 2001.

[4] C. Hauser, D. Bakken and A. Bose, A failure to communicate, *IEEE Power and Energy*, vol. 3(2), pp. 47–55, 2005.

[5] Institute of Electrical and Electronics Engineers, IEEE 1402 Guide for Electric Power Substation Physical and Electronic Security, Document IEEE 1402, Piscataway, New Jersey, 2000.

[6] National Communications System, Supervisory Control and Data Acquisition (SCADA) Systems, Technical Information Bulletin NCS TIB 04-1, Arlington, Virginia, 2004.

[7] P. Oman, E. Schweitzer and D. Frincke, Concerns about intrusions into remotely accessible substation controllers and SCADA systems, *Proceedings of the Twenty-Seventh Annual Western Protective Relay Conference*, 2000.

[8] A. Risley and J. Roberts, Electronic security risks associated with the use of wireless point-to-point communications in the electric power industry, presented at the *DistribuTECH Conference and Exhibition*, 2003.

[9] M. Shea, 900 MHz radio signals operational control, *IEEE Computer Applications in Power*, vol. 5(4), pp. 29–32, 1992.

[10] Wipro Technologies, Software defined radio, White Paper (www.wipro.com/webpages/insights/softwareradio.htm), 2002.