Analyzing Resiliency of the Smart Grid Communication Architectures under Cyber Attack

Anas AlMajali Arun Viswanathan Clifford Neuman
USC/Information Sciences Institute

Abstract

Smart grids are susceptible to cyber-attack as a result of new communication, control and computation techniques employed in the grid. In this paper, we characterize and analyze the resiliency of smart grid communication architecture, specifically an RF mesh based architecture, under cyber attacks. We analyze the resiliency of the communication architecture by studying the performance of high-level smart grid functions such as metering, and demand response which depend on communication. Disrupting the operation of these functions impacts the operational resiliency of the smart grid. Our analysis shows that it takes an attacker only a small fraction of meters to compromise the communication resiliency of the smart grid. We discuss the implications of our result to critical smart grid functions and to the overall security of the smart grid.

1 Introduction

Utilizing new communication, control and computation technologies in the modern smart grid can enhance the reliability of the smart grid, reduce electricity costs and provide new real-time customer services [3, 7, 11]. For example, adding smart metering systems and other devices to collect critical information from customer premises will assist power utilities in better decision-making which improves the overall reliability of the smart grid. A customer plugging in an electric vehicle (EV) and programming it to charge during off-peak hours is an example of how smart grid capabilities promise to reduce electricity costs [3]. These enhancements also create new cyber vulnerabilities that are exploitable by malicious entities to disrupt smart grid operations at a large scale. For example, some electric vehicles offer a smart phone interface that enables remote control over vehicle charging and discharging. An attacker gaining malicious control of this interface for a large number of EVs can trigger simultaneous charging to create peak loads on the power grid, eventually leading to a large scale blackout [14]. As discussed by Pelechrinis et al. [18], cyber attacks in the form of denial-of-service (DoS) attacks can be trivially launched by malicious entities against a wireless-based communication infrastructure. In the context of a smart grid, such attacks have potential to disrupt smart grid functions such as smart metering, demand response and outage management, thus impacting its overall resiliency.

Our objective is to experimentally evaluate the resiliency of smart grid communication architectures under cyber attacks by studying the performance of higher-level functions dependent on it. We consider the RF mesh as our choice of communication architecture. The RF mesh architecture involves smart meters communicating with each other over a wireless protocol. As discussed subsequently, the choice of communication architecture and its deployment impacts the overall resiliency of the smart grid. Our focus here is on evaluating the resiliency of RF mesh-based communication architecture for the smart grid under the presence of DoS attacks.

As shown in Figure 1, the smart grid can be logically decomposed into a physical power layer, a monitoring and communication layer called Advanced Metering

This material is based upon work supported by the United States Department of Energy under Award Number DE-OE000012, the Los Angeles Department of Water and Power, and by the Department of Homeland Security and the Department of the Navy under Contract No. N66-001-10-C-2018. Neither the United States Government nor any agency thereof, the Los Angeles Department of Water and Power, nor any of their employees make any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States government or any agency thereof. Figures and descriptions are provided by the authors and used with permission.

Infrastructure (AMI), and an application layer consisting of higher-level functions such as automated metering, outage management (OM), demand response (DR) and automated charging/discharging of EVs. In addition to the essential functional layers, there is a need for an orthogonal cyber security layer (CS) for protecting the system against failures and attacks and ensuring the integrity, confidentiality and availability of the system. At the lowest level of its operations, operational resilience for a smart grid is the ability to deliver sustained power. But, as shown in Figure 1 the resiliency of the overall smart grid also depends on the resiliency of its higher-level functions which in turn are directly dependent on the resiliency of the AMI communication layer. We observe that a resilient smart grid design rests on a resilient communication infrastructure.

In this work, we present a methodology to measure impact of communication on the performance of higher-level functions dependent on it. Our approach consists of modeling an RF mesh communication network deployed in a typical smart grid region, simulating the behavior of higher-level smart grid functions and analyzing the performance of those functions under a DoS attack on the communication infrastructure. The results we found, quantitatively demonstrate that the RF mesh is not resilient to the DoS attack as characterized in our work and impacts performance of higher level functions that depend on it. We hope that our results assist smart grid architects in making informed design choices. We intend our work as a first step in designing a secure smart grid, accounting for security as an important component of the system architecture [13].

In the remainder of this paper, we provide an overview of resiliency in the smart grid in Section 2, followed by a detailed account of the experiments and results in Section 3. Section 4 discusses the lessons learned, Section 5 discusses related work and we conclude with our contributions and future work in Section 6.

2 Resilience

Resilience is the capability of a system to fulfill its mission in a timely manner, even in the presence of attacks or failures. An operationally resilient system continues delivering essential services even under adverse operating conditions and rapidly recovers its full services when conditions improve. A number of factors such as cyber attacks, internal system failures, policy changes, configuration changes, or deployment changes can result in adverse conditions and disrupt system operation. We are specifically interested in analyzing the resiliency of the smart grid under cyber attacks. Furthermore, as discussed in Section 1, our focus is specifically on analyzing the resiliency of the smart grid communication layer. In the following subsections, we first elaborate on

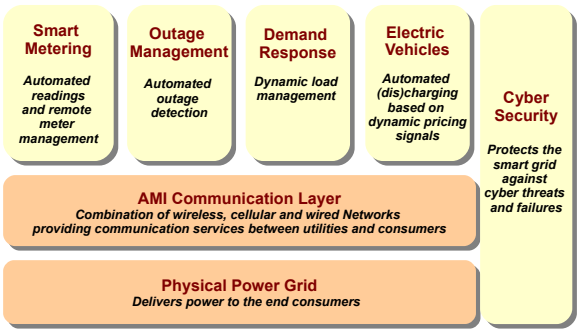

Figure 1: A functional view of the smart grid layers.

the resiliency requirements of smart grid functions, followed by a discussion of our approach used to measure resiliency.

2.1 Resiliency of Smart Grid Functions

In this section, we discuss four high-level smart grid functions: remote metering, demand response, outage management and cyber security, and discuss their resilience with respect to the underlying communication architecture. Additionally, we discuss the minimum conditions necessary for the functions to be resilient.

Remote Metering Automated remote metering requires meters to send meter reads to the utility at a configurable frequency. This function depends on reliable and timely delivery of meter data to the utility by the underlying AMI communication infrastructure. Long-term disruption of the metering function impacts the operational resiliency of the smart grid by interfering with revenue. Remote metering is resilient *if data from some percentage of the meters is always delivered to the utility and within a bounded time, where the percentage and time are dependent on utility-specific requirements*.

Demand Response (DR) DR is a critical component of automated load management and relies on the ability of the AMI communication infrastructure to reliably send load curtailment requests to smart meters and other end devices for dynamically managing the overall system load. DR signals to the Home Area Network (HAN) could travel through the Internet or the AMI system, but we only consider the latter. Unlike metering, disruption of DR operations can have near-term effects on operational resiliency of the smart grid by destabilizing the power grid. Demand response is resilient *if required* kWh *of load is always curtailed within a bounded time, where the required load and time are dependent on utility-specific requirements.*

Outage Management (OM) Automated outage management requires smart meters to send outage information in a *last gasp* message on detection of an outage by the meter [5]. The utility uses the information such as time and location of the outage from the message to re-

store power in a timely manner. A disruption of this function directly affects the operational resiliency of the grid by delaying the recovery and restoration of power to end customers. Outage management is resilient *if the utility can always identify and recover from outages within a bounded time, where the time is dependent on utility-specific requirements*.

Cyber Security (CS) The cyber security component protects the smart grid system against attacks and failures and provides integrity, availability and confidentiality services for the smart grid. CS functions such detection, diagnosis and response depend on the underlying communication infrastructure for tasks such as transporting monitored data from different critical points in the system, exchanging detection and diagnosis messages across its components and communicating response actions for responding promptly to adverse situations. Disruption of these functions has direct consequences to the security of the smart grid and impacts its overall resiliency. Cyber security component is resilient *if it always detects and responds to security threats before performance and security requirements of other functions are violated*.

2.2 Measuring and Analyzing Resiliency

Our approach to analyze the resiliency of the communication architecture under a cyber attack relies on measuring the impact of the attack on performance of higher-level functions. We capture the resiliency requirements of high-level functions as low-level communication metrics and measure the low-level metrics under different experiment scenarios.

Specifically, our simulation, discussed later in Section 3, simulates the normal behavior of two functions, namely, (a) automated metering, and (b) demand response and measures the performance of those functions during a cyber attack on the communication infrastructure. We choose only the automated metering and demand response functions in our study as they are characteristic of two typical behaviors, periodic and asynchronous, seen on a smart grid.

Our attack scenario consists of an attacker taking advantage of the large scale deployment of meters within the RF mesh to generate a DoS condition on the network by simultaneously generating low bit-rate traffic (hundreds of kbits/s) from individual meters. Since the attack is directly performed on the communication infrastructure, it causes legitimate packets belonging to higher-level functions to be dropped or delayed which impacts their performance and consequently their resiliency. We analyze the performance of these higher-level functions for different configurations of the communication architecture, discussed later in Section 3.5. A resilient communication architecture is one which sustains the cyber attack without compromising the performance requirements of the higher-level functions.

We define four metrics to measure the impact of the attack on the performance of higher-level functions. For purposes of this work and the definitions below, we assume the *sender* to be a customer-side device such as a smart meter and the *receiver* to be a node such as the data collector node within a smart grid region.

Packet Delivery Ratio (PDR) defined as the number of packets successfully received by a receiver over the expected number of packets.

Average End-to-end Delay defined as the average time taken for packets to be transmitted from the sending application to the receiving application.

Average Packet Hop Count defined as the average number of intermediate nodes through which the packets sent by a sender are routed. In the case of an RF mesh-based network, the average hop count measures the number of meters traversed by a packet before it reaches the receiver.

Successful DR Requests Ratio defined as the number of DR requests that successfully receive a reply over the total DR requests that were issued.

The first three metrics measure performance of the metering function while the last metric applies to DR. The above metrics are not unique to our work and have been previously used by other researchers to measure resiliency in different domains. Liu et al. [10] define network resilience as the percentage of lost traffic upon failures. Cholda et al. [2] define network resilience as general ability to improve network fault tolerance and reliability. Metrics derived from dependability attributes of systems like availability and performance have also been proposed to quantify resilience. For example, Liu et al. [10] use packet loss rate and Najjar et al. [12] use packet loss rate and packet delay to quantify resiliency in their work. Lee et al. [8] quantify the resilience of a system under DoS attack by the amount of traffic that needs to be sent to the system to make it unavailable. Our choice of metrics is due to our approach based on measuring performance of higher-level functions.

3 Methodology

Our overall goal is to design security components for the smart grid and our simulations described in this section are a step in that direction. Specifically, modeling and simulating the system at the early stages will help us (1) know the realistic attack scenarios that can interrupt the operation of the smart grid, and (2) know the realistic impacts achieved by those attacks [23]. We intend to use the knowledge derived from such simulations to build cyber security solutions for the smart grid in the future. In this section, we first discuss our high-level design choices for the experiment, followed by the details of the experiment

Figure 2: Geographical image of the simulated region. Each house in the image has one meter and the star represents the collector in the center of the region.

topology, simulated smart grid functions and the DoS attacks, followed by the experiment procedure and results.

3.1 Choice of Experimentation Platform: Simulation vs. Emulation

A key challenge in this work involved choosing an appropriate experimentation platform given that we had to faithfully model a wireless RF mesh with hundreds of wireless nodes and different wireless protocols. Our options involved either using a simulator such as ns-2 [15] or a network testbed such as DETER [1].

DETER is a wired network testbed and allows using real nodes and links to create a network but, it does not directly support creating wireless networks. Using a tool like SWOON [4], one can emulate wireless nodes on DETER but it does not scale to hundreds of nodes since simulating a wireless node requires two physical nodes.

ns-2 is a widely used network simulator, has support for a variety of wireless protocols and scales well to the situations needed to model the smart grid. Although, DETER allows us to emulate the real smart meter nodes, using real software if available, and can generate real network traffic, this is not a requirement for us, since we are only concerned with the network-level behavior of the meters. Our choice of platform for this work is thus ns-2.

3.2 Experiment Topology

We model a real geographical region, shown in Figure 2, in ns-2. Each house shown in the figure represents a real smart meter node and they communicate with a collector, represented by a star, located at the center of the region. The collector is responsible for relaying packets between the meters in the RF mesh and the utility through the Wide Area Network (WAN).

Meter Configuration We configure each meter in the region with the following parameters derived from specifications of a real smart meter [21]: *radio frequency* = 900 MHz, *data rate* = 100 kbits/s, *transmitter output* = 30 dBm (1 Watt), *receiver sensitivity* = -97 dBm.

Meter Distribution We use the region shown in Figure 2, to make an informed guess about the meter coordinates. The chosen region allows placing meters uniformly and placing the collector at the center of the region.

Propagation Model We configure the ns-2 simulator to simulate an outdoor "shadowed urban area" using the *shadowing propagation model* with the following parameters: *path loss exponent* = 2.7, *standard deviation* = 4, *reference distance* = 1 m.

3.3 Simulation of Smart Grid Functions

We simulate behavior of two smart grid functions: (a) automated, periodic meter reads from meters, and (b) DR load curtailment signals. For metering, we assume that all meters send their meter reads to the central collector, where each meter read is 1000 bytes, according to a preconfigured sending interval set by the utility. For DR, we simulate sending of a DR load curtailment signal from the collector to a group of enrolled homes requesting that they curtail certain amount of load. We assume that only 20% of the smart meters register in the DR program to receive DR requests from the utility. Upon receipt of a DR request, the smart meter immediately responds by sending a DR reply to the collector.

3.4 Denial-of-service Attack

We assume that an attacker wants to generate a DoS attack targeting the collector in a certain RF mesh. The attack takes advantage of the large number of meters within the geographical region to generate a DoS on the collector node by simultaneously generating low bit-rate traffic (hundreds of kbits/s) from individual meters. Realistically, an attacker can accomplish this attack using different means, for example, an attacker could compromise smart meters in a certain RF mesh and reprogram them to increase the frequency at which they send meter reads. Or, an attacker could take control of other customer devices such as the *service gateway* within a HAN to send spurious traffic creating a DoS attack.

In our experiment, we simulate a DoS attack by assuming that an attacker compromises some fraction of the meters within the region and reprograms them to send spurious meter reads at a higher frequency. As discussed later in Section 3.5, we control the effect of the DoS, that is, the amount of traffic in the network, by varying the meter sending intervals between 20 s to 60 s.

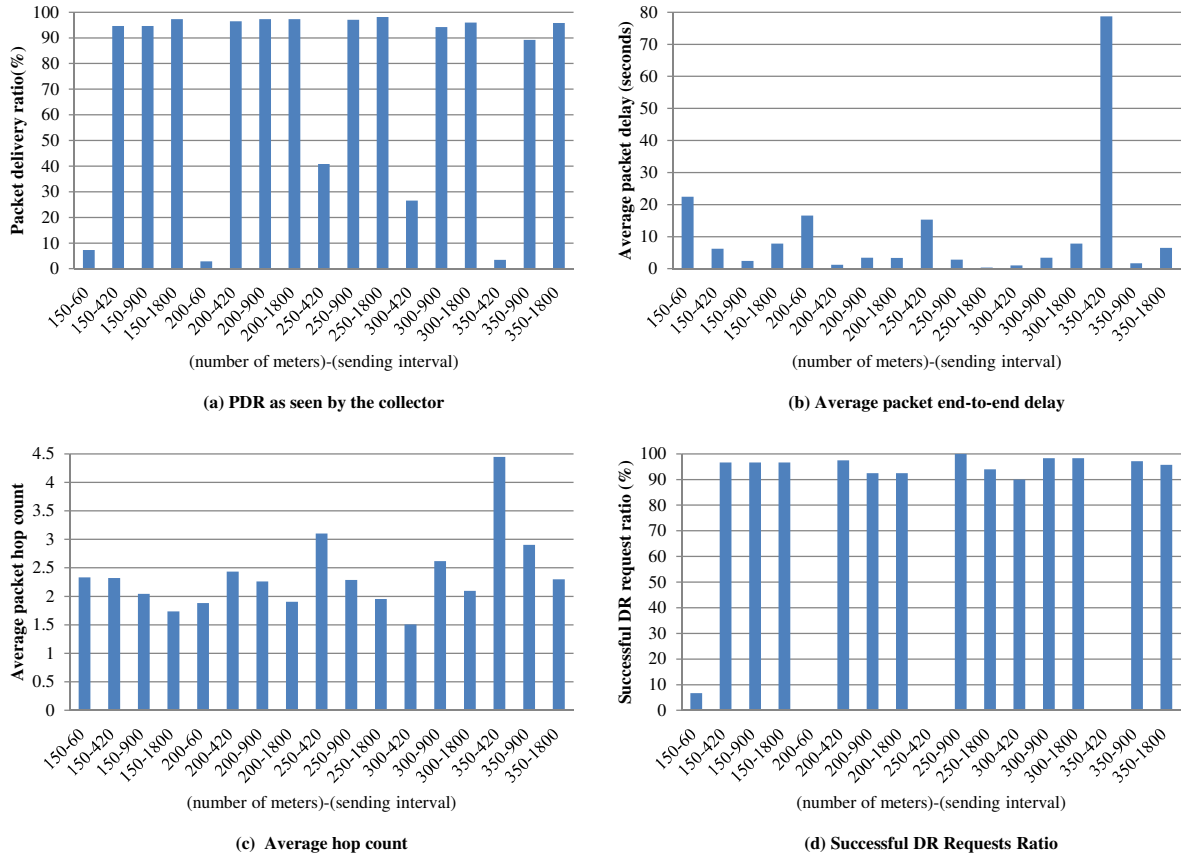

Figure 3: Plots of performance metrics for determining the baseline experiment configuration under normal operating conditions. Each X-axis entry represents a unique experiment configuration, as a combination of (number of meters)-(sending interval) and the AODV routing protocol.

3.5 Experiment Procedure and Results

Our high-level procedure involves first running experiments under normal operating conditions, that is, without any DoS attack to determine a *baseline experiment configuration*. We then use the parameters from the baseline configuration to study the resiliency of the communication architecture and the performance of functions under the DoS attack discussed in Section 3.4.

An *experiment configuration* is a set of parameters controlling a particular experiment run and defined using three parameters: i) the routing protocol (R) used in the RF mesh, ii) the number of smart meter nodes (N) in the RF mesh network, and iii) the sending interval of the meters (I).

An experiment run consists of all N meters configured to use the routing protocol R, with each meter sending its readings periodically at the configured sending interval I. Each meter starts sending its data at a time (T) chosen from a uniform random distribution ($T \sim U(0,I)$). Additionally, the collector initiates DR requests to 20% of the N meter nodes. We collect the results for three reading cycles, that is, three sending intervals.

Baseline Experiment

To find a baseline experiment configuration, we run experiments by varying the choice of routing protocol, the number of meters, and meters' sending intervals, and record the performance metrics discussed in Section 2.2. We considered three RF mesh routing protocols: Ad-hoc On-Demand Distance Vector (AODV) [19], Dynamic Source Routing (DSR) [6] and Destination Sequenced Distance Vector (DSDV) [20]. Our initial simulations for comparing protocol performance showed that on-demand routing protocols like AODV and DSR outperform the proactive routing protocol DSDV by imposing less overhead on the network. We thus only consider AODV and DSR for determining the baseline experiment configuration. We vary the number of meters within the region starting from 150 to 350 in 50 meters step. Finally, we vary the sending intervals as 60, 420, 900 and 1800 s.

We discuss our results for the baseline configuration, choosing AODV as the routing protocol and omit the results using DSR due to space limitations. In brief, we observed that DSR performed badly compared to AODV as the number of meters increased for all monitored metrics.

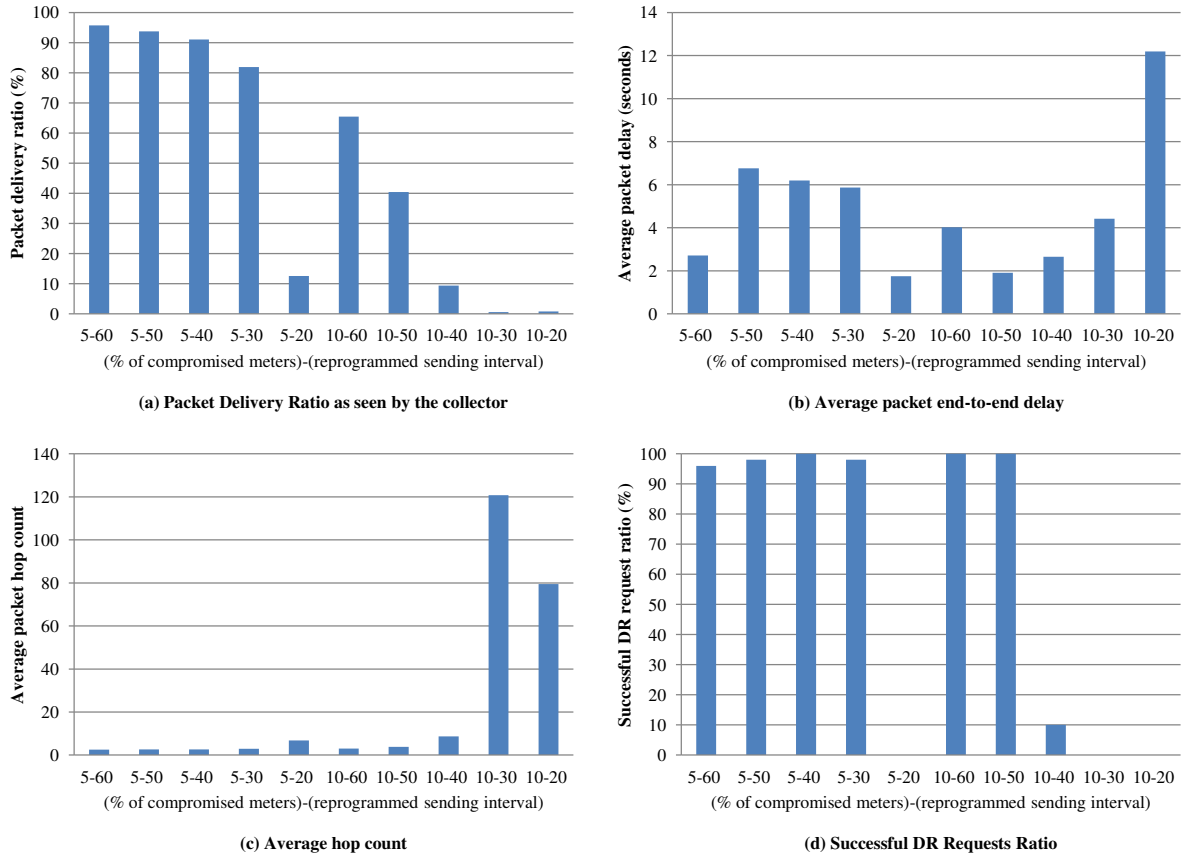

Figure 4: Plots of performance metrics with the network under an active DoS attack. The experiment configuration is the baseline configuration of 250 meters, meter sending interval set to 900 s, and the routing protocol as AODV. Each X-axis entry represents (percentage of compromised meters)-(sending interval of the compromised meters in seconds).

Figure 3 shows the simulation results of using AODV as the routing protocol and varying the other two experiment configuration parameters: number of meters and sending interval. The X-axis for each graph in Figure 3 represents a combination of number of meters and sending interval (number of meters)-(sending interval). We observe that performance is bad for the 60 s sending interval starting from 150 meters, that is, PDR is 7.33%, average packets end-to-end delay is 22.42 s and average hop count is 2.33. Only 6.66% of the DR requests received a reply. We do not show the results for sending interval = 60 s and number of meters $\geq$ 250 as the PDR was 0.0%.

Ideally, utilities would dictate the requirements for choosing an acceptable baseline configuration. Our method for choosing a baseline configuration relies on identifying the configuration values that result in high percentage of successful DR transaction, followed by a high packet delivery ratio, a low average end-to-end delay and finally a low average packet hop count. Using the above criteria and using Figure 3, we identify an acceptable configuration with number of meters = 250 and sending interval = 900 s, that is, a configuration for which PDR is 97.07%, average packet end-to-end delay is 2.86 s, average hop count is 2.28 and 100% of DR requests received a reply.

We want to emphasize here that we are not trying to find the best configuration for the RF mesh, but instead we try to find an *acceptable configuration* with which we can simulate the attack. For example, we understand that some routing protocols such as PRL [24] are more suitable for the RF mesh network and we plan to use these in our future simulations.

Experiment with DoS Attack

Our experiment configuration for the DoS attack consists of the AODV routing protocol, 250 meters, and 900 s sending interval for meters. The DoS attack assumes that the attacker has managed to comprise Y% of smart meters (uniformly distributed in the region) and has reprogrammed their sending interval to Z seconds. Figure 4 summarizes the results of the experiment. Each entry on the X-axis in Figure 4 represents a combination Y-Z.

We measure the same performance parameters as for the baseline case under the attack scenario. The results are as shown in Figure 4. We observe that for Y = 10% and Z = 60 s the percentage of successfully received packets drops from 97.07% to 65.45%. The average

packets end-to-end delay increases from 2.85 to 4.02 s.

Utilities may require the packet hop count in the RF mesh to be within a threshold so as to place deterministic bounds on the latency experienced by meters in a large network. As we lack the details for such a requirement, we do not enforce it in the simulation. We observe that enforcing such a requirement would further degrade the performance with respect to PDR and successful DR requests ratio when the network is under a DoS attack.

4 Lessons Learned

Analysis of the kind discussed in our work helps in understanding the attack scenarios that disrupt the operation of the communication architecture and the realistic impacts of those attacks on high-level smart grid functions.

We summarize our key finding as follows: *It requires an attacker to compromise only a small fraction of the meters in a typical RF mesh region to disrupt the communication resilience within the region.*

Specifically, we see from Figure 4 that a compromise of about 5% of the 250 meters was sufficient to reduce the PDR to 10% and the successful DR request ratio to zero. Although these figures apply to a single RF mesh region, we observe that given the cyber nature of the attack, an attacker can easily scale-up this attack by replicating it over multiple RF mesh regions. We discuss the implications of our result to key smart grid functions in subsequent paragraphs.

Remote Metering Utilities expect to receive a certain percentage of meter reads per reading cycle and within a bounded time. Missing meter reads from meters may not be severe as far as billing operations are concerned but the periodic meter reads are also used in a continuous manner as an input to important demand response functions such as load monitoring and forecasting. Disruption of these continuous inputs has consequences for the stability of the overall power grid thereby impacting its resilience.

Demand Response DR functionality depends on the ability to successfully curtail load within a bounded time period. This requires DR requests to be successfully communicated and acknowledged within a bounded time. As we observe from Figure 4, attacks can cause successful DR transactions (request-response pairs) to reduce to zero. With additional simulations, results of which are not included due to space limitations, we found that the average round trip time (RTT) for messages increased approximately 35 times during an attack (RTT was 0.11 s for the baseline case and around 4 s during an attack, for 5% compromised meters and 30 s sending interval). This again shows that attackers can easily disrupt the automated load management functions in the smart grid which can eventually lead to consequences such as large-scale blackouts.

Cyber Security Given that an attacker needs to compromise only a small fraction of meters to launch a DoS attack, cyber security functions at the utility may not be able to detect and characterize the impact of the attack immediately and thus result in a delayed response. In addition, the DoS attack could disrupt critical meter events from reaching the utility which could add additional delays to detection and response.

Overall, in this work, we have quantitatively demonstrated through simulation, the effects of a cyber attack on the resiliency of the RF mesh communication architecture and its impact on the performance of two key higher-level functions of automated metering and demand response. An important implication of our work is that an improperly configured and improperly secured smart grid communication architecture, can lend itself to simple DoS attacks thereby compromising the resiliency of the overall smart grid.

5 Related Work

Researchers have used alternative simulation approaches to study the RF mesh architecture but our work differs with previous approaches on the objectives, scale and level of resolution of the experiments. The Smart Grid Communication Assessment Tool (SG-CAT) [17], developed on top of OPNET Modeler [16], evaluates the communication capabilities of RF mesh under different deployments but not under cyber attack scenarios. The CLEVER simulator [22] evaluated the impact of different communication technologies such as PLC, broadband, GPRS on the performance of AMI communication for large-scale scenarios. Licht et al. evaluated the predeployment performance of an RF mesh using the OMNeT++ simulator [9] and tested different design options such as message frequency to find a proper deployment configuration. In summary, most of the encountered work focused on evaluation of smart grid communication capabilities during normal operations whereas our objective was to study the resiliency of smart grid communications in the presence of cyber attacks.

6 Conclusions and Future Work

In our work, we experimentally studied the resiliency of a smart grid communication architecture, specifically the RF mesh, in the presence of DoS attack. We quantitatively demonstrated that it requires an attacker to compromise only a small fraction of meters to violate the resilience of the communication architecture and consequently the overall resiliency of the smart grid.

Our next step involves using the knowledge from our simulations to build cyber security solutions for mitigat-

ing the threats to communication architectures. We also need to (a) test and validate the basic implementation and operation of our cyber security solution with respect to its design goals, and (b) test the performance of the entire smart grid system under different scenarios to ensure that the system performance is within acceptable limits. We observe that modeling the smart grid using simulators is insufficient to capture behavior of real software and hardware components and requires using testbed-based environments like DETER. But, at the same time, simulators such as ns-2 allow us to rapidly prototype large-scale scenarios to gather quick understanding of general behaviors. For example, simulations can help us generate traffic traces for emulating aggregate behavior of an RF mesh network on a testbed. This is important in a nascent domain like smart grid where there is a lack of real world traces. We are actively investigating approaches to integrate the simulation and emulation approaches for modeling large-scale cyber-physical systems such as the smart grid.

Acknowledgements

The authors thank Matt Lampe, David Alexander, Kymie Tan, Wiley Gustafson, Bradley Clement, Brian Cox, Goran Scuric and Joe Touch for discussions that helped us form the ideas presented in this paper and for feedback on earlier drafts.

References

[1] BENZEL, T., BRADEN, R., KIM, D., NEUMAN, C., JOSEPH, A., SKLOWER, K., OSTRENGA, R., AND SCHWAB, S. Experience with DETER: A Testbed for Security Research. In *2nd Intl. Conf. on Testbeds and Research Infrastructures for the Devel. of Networks and Communities - TRIDENTCOM* (2006).

[2] CHOLDA, P., TAPOLCAI, J., CINKLER, T., WAJDA, K., AND JAJSZCZYK, A. Quality of Resilience as a Network Reliability Characterization Tool. *IEEE Network 23*, 2 (March 2009), 11–19.

[3] FARUQUI, A., MITAROTONDA, D., WOOD, L., COOPER, A., AND SCHWARTZ, J. The Costs and Benefits of Smart Meters for Residential Customers. White Paper, July 2011. URL: `http://www.edisonfoundation.net/iee/Documents/IEE_BenefitsofSmartMeters_Final.pdf`.

[4] HUANG, Y. L., TYGAR, J. D., LIN, H. Y., YEH, L. Y., TSAI, H. Y., SKLOWER, K., SHIEH, S. P., WU, C. C., LU, P. H., CHIEN, S. Y., LIN, Z. S., HSU, L. W., HSU, C. W., HSU, C. T., WU, Y. C., AND LEONG, M. S. SWOON: A Testbed for Secure Wireless Overlay Networks. In *Proceedings of USENIX Conf. on Cyber Security Experimentation and Test* (2008), CSET'08, USENIX Association, pp. 8:1–8:6.

[5] INTL. ELECTROTECHNICAL COMMISSION. IEC 61968-9 (ed 1.0): Interfaces for Meter Reading and Control, September 2009. URL: `http://www.iec.ch/smartgrid/standards/`.

[6] JOHNSON, D., HU, Y., AND MALTZ, D. RFC 4728: The Dynamic Source Routing Protocol (DSR)for Mobile Ad Hoc Networks for IPv4, Feb. 2007. URL: `http://www.ietf.org/rfc/rfc4728.txt`.

[7] KHURANA, H., BOBBA, R., YARDLEY, T., AGARWAL, P., AND HEINE, E. Design Principles for Power Grid Cyber-Infrastructure Authentication Protocols. In *Proceedings of the 43rd Hawaii Intl. Conf. on System Sciences* (2010), HICSS '10, IEEE Computer Society, pp. 1–10.

[8] LEE, K.-W., CHARI, S., SHAIKH, A., SAHU, S., AND CHENG, P.-C. Improving the Resilience of Content Distribution Networks to Large Scale Distributed Denial of Service Attacks. *Computer Networks 51*, 10 (2007), 2753–2770.

[9] LICHTENSTEIGER, B., BJELAJAC, B., MU ANDLLER, C., AND WIETFELD, C. RF Mesh Systems for Smart Metering: System Architecture and Performance. In *IEEE Intl. Conf. on Smart Grid Communications (SmartGridComm)* (Oct. 2010), pp. 379–384.

[10] LIU, G., AND JI, C. Scalability of Network-failure Resilience: Analysis Using Multi-layer Probabilistic Graphical Models. *IEEE/ACM Trans. in Networking 17*, 1 (Feb. 2009), 319–331.

[11] METKE, A., AND EKL, R. Smart Grid Security Technology. In *Innovative Smart Grid Technologies (ISGT)* (Jan. 2010), pp. 1–7.

[12] NAJJAR, W., AND GAUDIOT, J.-L. Network Resilience: A Measure of Network Fault Tolerance. *IEEE Transactions on Computers 39*, 2 (Feb 1990), 174–181.

[13] NEUMAN, C. Challenges in Security for Cyber-Physical Systems. *Workshop on Future Directions in Cyber-physical Systems Security* (2009).

[14] NEUMAN, C., AND TAN, K. Mediating Cyber and Physical Threat Propagation in Secure Smart Grid Architectures. In *IEEE Intl. Conf. on Smart Grid Communications (SmartGridComm)* (Oct. 2011), pp. 238–243.

[15] Network Simulator - 2 (ns-2). URL: `http://www.isi.edu/nsnam/ns/`.

[16] OPNET Modeler. URL: `http://www.opnet.com/solutions/network_rd/modeler.html`.

[17] PATEL, A., APARICIO, J., TAS, N., LOIACONO, M., AND ROSCA, J. Assessing Communications Technology Options for Smart Grid Applications. In *IEEE Intl. Conf. on Smart Grid Communications (SmartGridComm)* (Oct. 2011), pp. 126–131.

[18] PELECHRINIS, K., ILIOFOTOU, M., AND KRISHNAMURTHY, S. Denial of Service Attacks in Wireless Networks: The Case of Jammers. *IEEE Communications Surveys Tutorials 13*, 2 (2011), 245–257.

[19] PERKINS, C., BELDING-ROYER, E., AND DAS, S. RFC 3561: Ad-hoc On-Demand Distance Vector (AODV) Routing, July 2003. URL: `http://www.ietf.org/rfc/rfc3561.txt`.

[20] PERKINS, C. E., AND BHAGWAT, P. Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) For Mobile Computers. *SIGCOMM Comput. Commun. Rev. 24*, 4 (Oct 1994), 234–244.

[21] SILVERSPRING NETWORKS. Communications Module for Electricity Meters (datasheet). URL: `http://www.silverspringnet.com/pdfs/SilverSpring-Datasheet-Communications-Modules.pdf`.

[22] SONG, T., KALESHI, D., ZHOU, R., BOUDEVILLE, O., MA, J.-X., PELLETIER, A., AND HADDADI, I. Performance Evaluation of Integrated Smart Energy Solutions Through Large-scale Simulations. In *IEEE Intl. Conf. on Smart Grid Communications (SmartGridComm)* (Oct. 2011).

[23] STAMP, J., MCINTYRE, A., AND RICARDSON, B. Reliability Impacts from Cyber Attack on Electric Power Systems. In *IEEE Power Systems Conf. and Exposition* (March 2009), pp. 1–8.

[24] WANG, D., TAO, Z., ZHANG, J., AND ABOUZEID, A. RPL Based Routing for Advanced Metering Infrastructure in Smart Grid. In *IEEE Intl. Conf. on Communications Workshops (ICC)* (May 2010), pp. 1–6.