Review and Evaluation of Security Threats on the Communication Networks in the Smart Grid

Zhuo Lu Xiang Lu Wenye Wang
Department of Electrical and Computer Engineering
North Carolina State University, Raleigh NC 27606
Emails: {zlu3, xlu6, wwang}@ncsu.edu

Cliff Wang
Army Research Office
Research Triangle Park, NC 27709
Email: cliff.wang@us.army.mil

***Abstract*—The smart grid, generally referred to as the next-generation power electric system, relies on robust communication networks to provide efficient, secure, and reliable information delivery. Thus, the network security is of critical importance in the smart grid. In this paper, we aim at classifying and evaluating the security threats on the communication networks in the smart grid. Based on a top-down analysis, we categorize the goals of potential attacks against the smart grid communication networks into three types: network availability, data integrity and information privacy. We then qualitatively analyze both the impact and feasibility of the three types of attacks. Moreover, since network availability is the top priority in the security objectives for the smart grid, we use experiments to quantitatively evaluate the impact of denial-of-service (DoS) attacks on a power substation network. Our work provides initial experimental data of DoS attacks against a power network and shows that the network performance degrades dramatically only when the DoS attack intensity approaches to the maximum.**

I. Introduction

Power systems are very complex interconnected networks. For example, statistics [1] showed that there are over 2000 power distribution substations, about 5600 distributed energy facilities, and more than 130 million customers all over the US. The smart grid [2], which is in general referred to as the next-generation power electric system, integrates varieties of digital computing and communication technologies to provide efficient, secure, and reliable electricity and information delivery between power generators, suppliers and customers. The smart grid will further introduce millions of intelligent computing components that communicate in much more advanced ways (e.g. two-way communication) than current power systems [3]. As such, *how to address networking security issues* is critically important in the design of communication networks for the smart grid. Potential networking intrusion caused by intentional attackers may lead to a variety of consequences [4], from customers' information leakage to a cascade of failures, such as massive power outage and destruction of infrastructures.

In this paper, we aim to address security issues on communication networks for the smart grid. Since the research on networking security in the smart grid is still at a preliminary stage, our goal is *to provide an initial step to classify potential security threats and evaluate their feasibility and impact upon communication networks for the smart grid*. To this end, we first introduce the fundamental architecture of the smart grid communication network and present the main differences between the smart grid network and another large-scale real-world network, the Internet. Then, we use a top-down approach to categorize attacks in the smart grid into three major types in terms of their goals: network availability, data integrity, and information privacy. We evaluate both the feasibility and impact of the three types of attacks against the communication networks in the smart gird.

Further, as pointed out in [3], the design of communication networks that are robust to attacks targeting network availability is the top priority, since network unavailability may result in the loss of real-time monitoring of critical power infrastructures and possible global power system disasters. In order to further assess the vulnerability of power networks under attacks targeting network availability, we use experiments to quantitatively evaluate the impact of denial-of-service (DoS) attacks on an experimental power substation network with the distributed network protocol (DNP3) [5], which is an extensively used communication protocol in nowadays power electricity systems. Our experiment results show that long DNP3 packets are more vulnerable to DoS attacks than short DNP3 packets and that the performance of the power network does not degrade gradually with the increasing of the DoS attack intensity. In fact, there exists a phase transition phenomenon: the performance will degrade dramatically when the DoS attack intensity approaches to the maximum.

The remainder of this paper is organized as follows. In Section II, we introduce the fundamental architecture of the communication networks in the smart grid. In Sections III and IV, we categorize potential security threats towards the smart grid, and in particular evaluate via experiments the impact of denial-of-service attacks on a power substation network. Finally, we conclude in Section V.

II. Network Architecture in the Smart Grid

The smart grid is a network of networks, including a variety of sub-systems such as the demand response (DR) system [6] and the advanced metering infrastructure (AMI) system [7]. All these systems are interconnected with each other to form a highly distributed network over a very large geographical

The work was supported by Army Research Office (ARO) under Grant Number 53435-CS-SR.

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
OCT 2010		**00-00-2010 to 00-00-2010**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Review and Evaluation of Security Threats on the Communication Networks in the Smart Grid	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **North Carolina State University,Department of Electrical and Computer Engineering,Raleigh,NC,27606**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES
in Proceedings of IEEE Military Communications Conference (MILCOM), 31 Oct ? 3 Nov 2010, San Jose, CA.

14. ABSTRACT
The smart grid, generally referred to as the nextgeneration power electric system, relies on robust communication networks to provide efficient, secure, and reliable information delivery. Thus, the network security is of critical importance in the smart grid. In this paper, we aim at classifying and evaluating the security threats on the communication networks in the smart grid. Based on a top-down analysis, we categorize the goals of potential attacks against the smart grid communication networks into three types: network availability, data integrity and information privacy. We then qualitatively analyze both the impact and feasibility of the three types of attacks. Moreover since network availability is the top priority in the security objectives for the smart grid, we use experiments to quantitatively evaluate the impact of denial-of-service (DoS) attacks on a power substation network. Our work provides initial experimental data of DoS attacks against a power network and shows that the network performance degrades dramatically only when the DoS attack intensity approaches to the maximum.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**Same as Report (SAR)**	**6**	

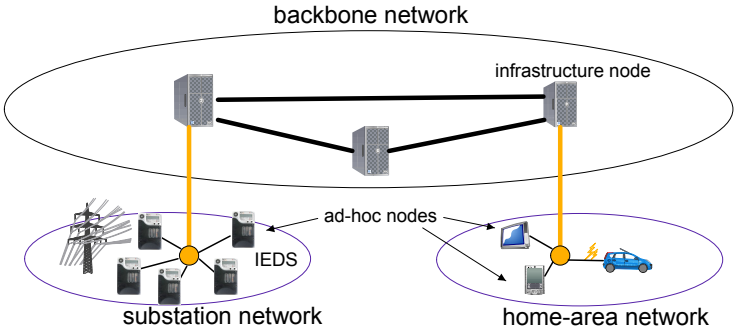

Fig. 1. The network architecture in the smart grid: the network consists of the backbone network and local-area networks. A local-area network can be a power substation network or a home-area network.

area. In the following, we map the smart grid network into a hybrid and hierarchical network as shown in Fig. 1. There are two types of networks in the smart grid, the backbone network and local-area networks. The backbone network consists of infrastructure nodes, which could be either gateways for local-area networks or high-throughput routers to forward messages across a variety of domains in the smart grid. A local-area network consists of ad-hoc nodes, which could be smart meters in a home-area network or intelligent electronic devices (IEDs) in a power substation network.

Compared with conventional power networks, ad-hoc nodes in a local-area network can use wireless technologies to communicate with each other. It has been shown that there are a number of advantages for using wireless communication technologies in the smart grid [5], including untethered access to information, mobility, reduced cost, low complexity, and the availability of off-the-shelf wireless products such as WiFi and ZigBee. One of the Smart Grid Priority Action Plans of the National Institute of Standards and Technology (NIST) is to provide the guidelines for the use of wireless communications in the smart grid, which is expected to be completed in mid 2010 [2]. The industry is also endeavoring to develop new wireless communication products for the smart grid. For example, ZigBee embedded products have been released recently to target the smart grid applications, such as smart meters, demand response, and home area network devices [8].

Despite efforts from the community to integrate the smart grid with wireless technologies, there are still technical challenges existing in wireless networks, especially the security issues due to the broadcast nature of wireless channels, which will be discussed later.

As we can see, the smart grid network is similar to the Internet in terms of the complexity and hierarchical structure; however, there are fundamental differences between the smart grid network and the Internet.

1) Performance metric. The major goal of the Internet is to provide data service, such as web surfing and music downloading. Thus, the throughput is one of the most widely-used performance metrics in the Internet. Whereas, the goal of the smart grid communication network is to ensure reliable, secure, and in-time message delivery. Hence, the message delay is much more important than the throughput in the smart grid, leading to the delay-oriented design of communication protocols in the smart grid. For example, the power substation communication protocol, IEC 61850 [9] maps time-critical messages from the application layer directly to the link layer to reduce the processing delay.
2) Communication pattern. The Internet is built up on the end-to-end principle, ensuing an arbitrary end-to-end communication model. However, there are only two major directional information flows in the smart grid: *top-down* (center to devices) and *bottom-up* (devices to center). Arbitrary peer-to-peer communication model across networks in the smart grid may be invalid. For instance, the peer-to-peer model between intelligent electronic devices is usually restricted in local-area networks [3].
3) Traffic model. It is well known that many Internet traffic flows have the self-similarity property, such as the World Wide Web (WWW) traffic [10]. In power networks, however, a large amount of traffic flows are periodic [9], [11] due to consistent monitoring of electricity devices. Thus, it can be expected that part, if not all, of the traffic in the communication networks for the smart grid differs from the traffic in the Internet.

III. Security Threats towards the Smart Grid Network

We have shown that the smart grid communication network is an aggregate of multiple networks with varying levels of communications and coordination between power providers, operators, and customers. Such complex communication networks require a comprehensive security design, as they are likely targets of sophisticated cyber attacks, which can be launched from any vulnerable component in the highly distributed system.

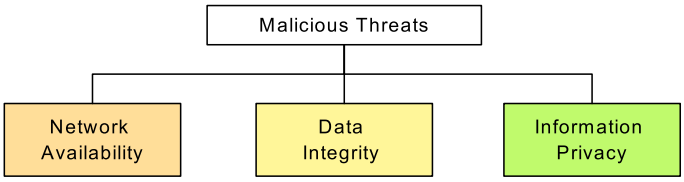

Fig. 2. Classification of security threats towards communication networks in the smart grid.

However, enumerating all possible threats in the smart grid is not practical due to its complexity and some sophisticated attacks that have not been yet identified. Thus, we in this section use a top-down approach to categorize malicious attacks into three major types based on their goals: (i) network availability, (ii) data integrity, and (iii) information privacy, as shown in Fig 2. We then evaluate the impact and feasibility of each type of attacks in turn, and at the same time summarize the related work on each type of attacks against the power networks.

A. Network Availability

Malicious attacks targeting network availability can be considered as denial-of-service (DoS) attacks, which attempt to delay, block or corrupt information transmission in order to make network resources unavailable to nodes that need information exchange in the smart grid. Since it is widely expected that at least part, if not all, of the smart grid will use IP-based protocols (e.g., IEC 61580 [9] has already adopted TCP/IP as a part of its protocol stacks) and TCP/IP is vulnerable to DoS attacks, sophisticated and efficient countermeasures to DoS attacks are essential to the smart grid. DoS attacks against TCP/IP have been well studied in the literature regarding attacking types, prevention and response [12]–[14]. Therefore, in the following, we will discuss potential attacks that specifically target power network availability.

As aforementioned, a major difference between the smart grid and the Internet is that the smart grid is more concerned with the message delay than the data throughput due to the timing constraint of messages transmitted over the power networks. Indeed, network traffic in power networks is in general time-critical. For instance, the delay constraint of generic object oriented substation events (GOOSE) messages is 4 ms in IEC 61850 [3].

Such a timing constraint ensures reliable monitoring and control of power devices. But on the other hand, it becomes one of the most vulnerable parts in power networks to DoS attacks. More specifically, instead of using some extreme means (e.g., channel jamming), an attacker can even use legitimate methods to intentionally delay the transmissions of time-critical messages to violate the timing requirements. For instance, an attacker can physically connect to a communication channel in a power network and generates legitimate but useless traffic to capture the channel and to delay the transmission of power monitoring and control devices

Since intruders only need to connect to communication channels rather than authenticated networks in the smart grid, it is very easy for them to launch DoS attacks against the smart grid, especially for the wireless-based power networks that are susceptible to jamming attacks [15]–[17]. Hence, it is of critical importance to evaluate the impact of DoS attacks on the smart grid and to design effective countermeasures to such attacks. We will provide initial experimental results of the impact of DoS attacks on the performance of a power network in Section IV.

B. Data Integrity and Information Privacy

Differing from attacks targeting network availability, attacks targeting data integrity can be regarded as less brute-force yet more sophisticated attacks. The target of the attacks is either customer's information (e.g., pricing information and customer account balance) or network operation information (e.g., voltage readings, device running status). In other words, such attacks attempt to deliberately modify information shared within the smart grid in order to corrupt critical data exchange in the smart grid. On the contrary, attackers targeting information privacy do not attempt to modify information transmitted over power networks but to eavesdrop on communications in power networks to acquire desired information, such as a customer's account number and electricity usage. Such attacks can be considered to have negligible effect on the functionality of the communication networks in the smart grid. Consequently, compared with attacks targeting data integrity, attacks targeting information privacy may not lead to catastrophic consequences, such as massive blackout.

The risk of attacks targeting data integrity in the power networks is indeed real. A notable example is the recent work of [18], which proposed a new type of attacks, called *false data injection* attacks, against the state estimation in the power grid. The paper assumed that an attacker has already compromised one or several meters and pointed out that the attacker can take advantage of the configuration of a power system to launch attacks by injecting false data to the monitoring center, which can legitimately pass the data integrity check used in current power systems. More recently, new methods [19] have been developed to provide state estimation that is robust to the false data injection attacks.

In order to launch attacks that attempt to compromise data integrity or to acquire privacy information, an attacker has to first stealthily intrude the computer system of a legitimate node, or by some means access a power network with authentication. Therefore, the design of countermeasures to attacks targeting data integrity and information privacy can consist of the following perspectives.

1) *Authentication protocol design*. Authentication is an important identification problem for any communication network. Strong authentication schemes are required for customers and electronic devices to ensure communications with full security and to meet the stringent requirements of the communication network in the smart grid, such as message delay and power consumption constraints. To this end, existing work [20]–[22] in general aims at providing efficient and fast authentication protocols for a variety of power subsystems, including transmission and operation systems, distribution networks, and customers' home-area networks. For example, the work of [22] showed that the time-critical constraint implicitly results in the following requirements for the design of authentication protocols: (i) efficient algorithms to minimize computational cost, (ii) low communication overhead, and (iii) robustness to attacks. Towards these goals, the work in [22] and [23] focused on the design of authentication protocols to meet the requirements for the low latency and DoS attack resilience.
2) *Intrusion detection*. The smart grid must have the ability to detect the attempt of an intruder to gain unauthorized access to computer systems. Recently, a few papers have investigated the problem of cyber intrusion detection in power networks [24]–[26]. In general, the intrusion detection for computer systems falls mainly into the cyber security field and has been well studied in the literature.

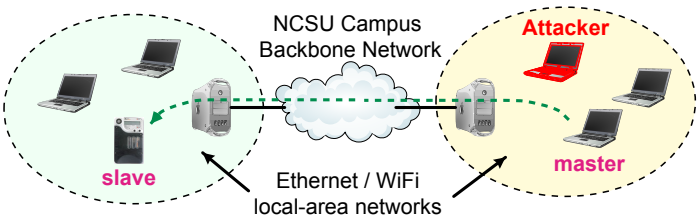

Fig. 3. The network scenario for the experiments: we constructed two local-area networks with either Ethernet or WiFi connections, which are interconnected with the campus backbone network at NC State University.

3) *Firewall and Gateway Design*. As mentioned before, differing from the Internet, the smart grid has only two major directional information flows: bottom-up and top-down. Thus, it will be easy for gateway or firewall softwares to perform traffic control on information flows in smart grid to block undesired or even suspicious flows generated by malicious nodes.

Note that it may be non-trivial to assume an attacker can easily compromise a legitimate node or access the power network with authentication. But due to the ubiquitousness of the smart grid network, it is still possible that an malicious attacker can, by some means, connect to a power network and launch attacks targeting data integrity or information privacy.

IV. Experimental Evaluation of Denial-of-Service Attacks against Power Networks

We have qualitatively evaluated the feasibility and impact of attacks targeting network availability, data integrity, and information privacy. Dependent on its purpose, an attacker can aim at any of these three goals to disrupt, falsify or wiretap the information transmitted in the smart grid. While as stated in [2], the highest priority in the security objectives in the smart grid is availability. Therefore, in this section, we will further quantify via experiments the impact of attacks targeting network availability, i.e., DoS attacks against the communication networks in the smart grid.

A. Experiment Setups

1) Network Scenario: As shown in Fig. 1, the communication network for the smart grid is a hierarchical network consisting of the backbone network and local-area networks. Therefore, in our experimental scenario, as illustrated in Fig. 3, we use the campus network at NC State University as our backbone network and set up two local-area networks: one network includes a laptop serving as a monitoring and control center (master) and another laptop serving as an attacker that attempts to launch DoS attacks within the network. The other network includes a TS7250 ARM-based single board computer serving as an electronic device (slave) for a power system. In our experiments, we will test the performance of both Ethernet and WiFi in the two local-area networks.

2) Communication Protocol and Performance Metric: We use the distributed network protocol (DNP3) [5], which is widely used in current power systems, as our communication protocol between the control center and the electronic device. The control center communicates with the electronic device in a master-slave model; i.e, the control center first initiates a connection request and issues commands to the electronic device, then the device responds to the center accordingly. In all experiments, the control center will initiate connections to the electronic device every 500 ms. We use the round-trip delay as our performance metric to evaluate the performance of the DNP3-based network. The round-trip delay is defined as the time interval from the instant the center sends a DNP3 packet to the instant that the center receives the DNP3 ACK from the device.

3) Attack Model: There are a variety of methods to implement DoS attacks against a network [14]. As we discussed in Section III-A, instead of using some extreme schemes, an attacker can use legitimate methods to delay the transmission of a message such that the overall delay of the message violates the timing requirement. Thus, we choose our attacker to be a traffic flood attacker, which uses *iperf* (a commonly-used network traffic generator) to generate legitimate but useless UDP traffic over the testing network to occupy the communication channel, thereby reducing network availability. We use the attack intensity index to indicate the intensity of the attack, which is defined as

$$\text{attack intensity index} = \frac{\text{traffic flooded by the attacker}}{\text{total channel bandwidth}} \in [0, 1].$$

B. Experiment Results

We first evaluate the impact of DoS attacks on the experimental network where both local-area networks use Ethernet cables with 100 Mbps. Fig. 4 shows the empirical complimentary cumulative distribution functions (CCDFs) of the round-trip delay of DNP3 packets under attacks with intensity indexes equal to 20%, 60%, 90%, and 100%, respectively. From Fig. 4, we can see that there are no significant differences between the 20%, 60%, and 90% cases. However, the delay performance degrades significantly when the attacker increases the intensity to 100%. For example, about 17% packets have round-trip delays greater than 100 ms when the attack intensity index is equal to 100%. In this case, a large amount of packet delays may violate a certain timing requirement in power networks.

Fig. 5 illustrates the average round-trip delay of DNP3 packets as a function of attack intensity index. It is further verified in Fig. 5 that the delay performance significantly degrades only when the traffic generated by the attacker overwhelms the communication channel. Our results indicate that there exists an interesting phase transition phenomenon between the delay and attack intensity index: the delay performance does not degrade gradually with the increasing of the attack intensity index and dramatically degrades when the attack intensity index approaches 1.

We also evaluate the impact of packet length on the round-trip delay. Fig. 6 illustrates the mean round-trip delay as a function of DNP3 packet length (73, 146 and 292 bytes). We found that the mean delay is inversely proportional to

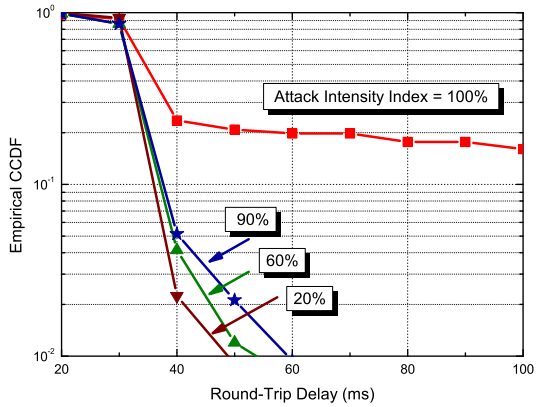

Fig. 4. The empirical CCDF of the round-trip delay of DNP3 packets for different values of the attack intensity indexes. The length of DNP3 packets is fixed to be 292 bytes in this experiment.

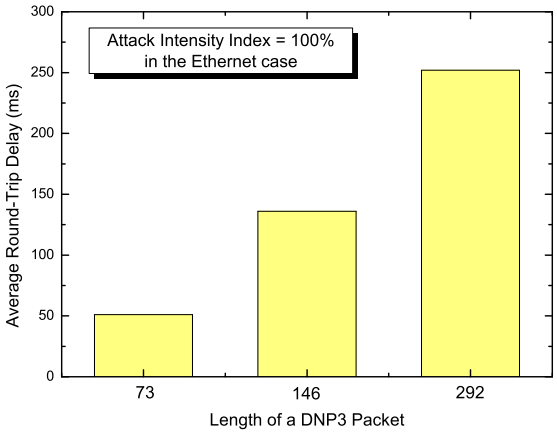

Fig. 6. The effect of packet length on the mean round-trip delay of DNP3 packets.

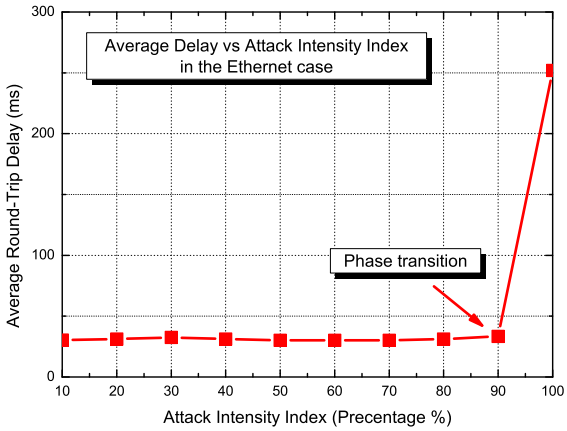

Fig. 5. The average round-trip delay of DNP3 packets for different values of the attack intensity indexes.

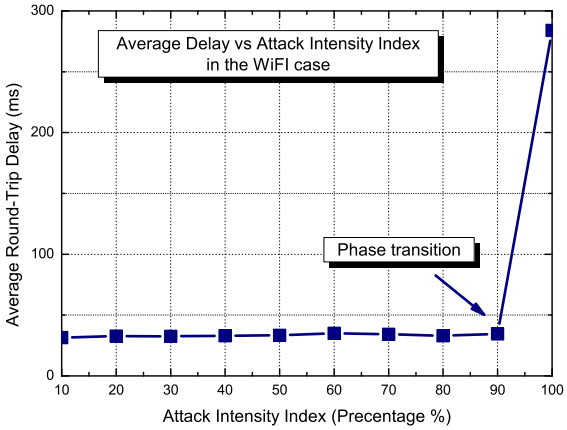

Fig. 7. The mean round-trip delay of DNP3 packets for different values of the attack intensity indexes in the WiFi case.

the packet length, which implies that a shorter DNP3 packet is more resistent to traffic flood attacks. Therefore, if we have no countermeasures to DoS attacks in a power network, a practical way is to compress the information data at a transmitter and then transmit short DNP3 packets to the receiver.

Then, we change the network connection of the electronic device from Ethernet to IEEE 802.11g. Thus, in current setups, the electronic device is using wireless while the control center still has Ethernet connection. Such a scenario can be mapped to a practical situation (e.g., key use case 24 in the smart grid [3]) that the supervisory control and data acquisition (SCADA) center tries to communicate with a wireless-based remote distribution equipment in a power substation.

Our goal in this experiment is two-fold. First, as it is widely expected that the smart grid will use wireless technologies to delivery data messages, we aim at evaluating the feasibility of real-time message exchange in a power network with wireless access. Second, we are going to quantify via experiments the impact of DoS attacks on the performance of DNP3 over WiFi networks, showing to what extent wireless access is vulnerable to DoS attacks compared with wireline access in a power network.

Our experiments show that the WiFi case leads to the similar delay performance as the Ethernet case. For example, we found that, despite different maximum physical transmission rates (100 Mbps for Ethernet and 54 Mbps for IEEE 802.11g), the mean round-trip delay with WiFi is 31.8 ms while the mean delay with Ethernet is 30.4 ms, which in turn indicates that in our experimental network, the delay on the backbone network is dominant in the overall round-trip delay. Thus, in this case, WiFi-based and Ethernet-based local-area networks can provide similar delay performance for message delivery in the power systems.

We also found that the impact of the traffic flood attacker on the WiFi case is similar to that on the Ethernet case. For example, Fig. 7 illustrates the average round-trip delay of DNP3 packets with WiFi access. We can see that the phase

transition phenomenon also happens as the attack intensity index approaches 1. In fact, throughout our experiments, we found that the only difference between the Ethernet and WiFi cases is that the WiFi delay is slightly larger than the Ethernet delay.

C. Summary and Analysis

We have performed experiments to illustrate the impact of traffic flood attacks on the delay performance of an experimental power network. Our findings can be summarized as follows

1) We found that, out of our expectation, the delay performance does not degrade gradually as the attack intensity index increases and will dramatically degrade when the attack intensity index approaches 1, which means that a traffic flood attack has to pour traffic into the communication channel as much as it can to degrade the delay performance in a power network. This, on the other hand, indicates that such an attacker has a very high risk to be detected.
2) We found that the average delay is inversely proportional to the length of a DNP3 packet, indicating that a shorter DNP3 packet is more robust to traffic flood attacks. Therefore, it will be better to transmit short packets rather than long packets for time-critical transmissions that are vulnerable to such attacks.

V. Conclusion

In this paper, we briefly reviewed the security threats towards communication networks in the smart grid. Specifically, we classified the security threats into three types in terms of their goals: network availability, data integrity and information privacy, and evaluated their feasibility and impact on the smart grid. We showed via experiments that DoS attacks can lead to a phase transition phenomenon in the delay performance of the DNP3 protocol and that shorter DNP3 packets can be more resistant to DoS attacks. Our work provides initial experimental data of DoS attacks against a power network and our future work will include quantification of the impact of more sophisticated attacks via theoretical modeling and comprehensive experiments.

References

[1] A. Aggarwal, S. Kunta, and P. K. Verma, "An integrated architecture for demand response communications and control," in *Proc. of Innovative Smart Grid Technologies (ISGT)*, Jan. 2010.

[2] Office of the National Coordinator for Smart Grid Interoperability, "NIST framework and roadmap for smart grid interoperability standards, release 1.0," *NIST Special Publication 1108*, 2009.

[3] The Smart Grid Interoperability Panel - Cyber Security Working Group, "Smart grid cyber security strategy and requirements," *NIST IR-7628*, Feb. 2010.

[4] A. R. Metke and R. L. Ekl, "Smart grid security technology," in *Proc. of Innovative Smart Grid Technologies (ISGT)*, Jan. 2010.

[5] S. Mohagheghi, J. Stoupis, and Z. Wang, "Communication protocols and networks for power systems - current status and future trends," in *Proc. of Power Systems Conference and Exposition (PES '09)*, Mar. 2009.

[6] M. LeMay, R. Nelli, G. Gross, and C. A. Gunter, "An integrated architecture for demand response communications and control," in *Proc. of 41th Hawaii International Conference on System Sciences (HICSS' 08)*, Jan. 2008.

[7] H. Sui, H. Wang, M.-S. Lu, and W.-J. Lee, "An AMI system for the deregulated electricity markets," *IEEE Trans. Industry Applications*, vol. 45, no. 6, pp. 2104 – 2108, 2009.

[8] Z. Alliance, "RF micro devices features ember ZigBee technology in new family of high performance front end modules for smart energy applications," Mar. 2010.

[9] T. S. Sidhu and Y. Yin, "Modelling and simulation for performance evaluation of IEC61850-based substation communication systems," *IEEE Trans. Power Delivery*, vol. 22, no. 3, pp. 1482–1489, July 2007.

[10] M. E. Crovella and A. Bestavros, "Self-similarity in world wide web traffic: Evidence and possible causes," *IEEE/ACM Trans. Networking*, vol. 5, no. 6, pp. 835 – 846, 1997.

[11] P. M. Kanabar, M. G. Kanabar, W. El-Khattam, T. S. Sidhu, and A. Shami, "Evaluation of communication technologies for IEC 61850 based distribution automation system with distributed energy resources," in *Proc. of the IEEE Power & Energy Society General Meeting (PES '09)*, July 2009.

[12] C. L. Schuba, I. V. Krsul, M. G. Kuhn, E. H. Spafford, A. Sundaram, and D. Zamboni, "Analysis of a denial of service attack on tcp," in *Proc. of IEEE Symposium on Security and Privacy (S&P 1997)*, May 1997.

[13] A. Yaar, A. Perrig, and D. Song, "Pi: A path identification mechanism to defend against DDoS attacks," in *Proc. of IEEE Symposium on Security and Privacy (S&P 2003)*, 2003.

[14] J. Mirkovic and P. Reiher, "A taxonomy of DDoS attack and DDoS defense mechanisms," *SIGCOMM Comput. Commun. Rev.*, vol. 34, no. 2, pp. 39–53, 2004.

[15] M. Strasser, S. Capkun, C. Popper, and M. Cagalj, "Jamming-resistant key establishment using uncoordinated frequency hopping," in *Proc. of IEEE Symposium on Security and Privacy (S&P 2008)*, May 2008, pp. 64–78.

[16] C. Popper, M. Strasser, and S. Capkun, "Jamming-resistant broadcast communication without shared keys," in *Proc. of the 18th USENIX Security Symposium (Security '09)*, Aug. 2009.

[17] Y. Liu, P. Ning, H. Dai, and A. Liu, "Randomized differential DSSS: Jamming-resistant wireless broadcast communication," in *Proc. of the 29th IEEE Conference on Computer Communications (INFOCOM '10)*, Mar. 2010.

[18] Y. Liu, P. Ning, and M. Reiter, "False data injection attacks against state estimation in electric power grids," in *Proc. of ACM Conference on Computer and Communications Security (CCS '09)*, Sept. 2009.

[19] O. Kosut, L. Jia, and L. Tong, "Improving detectors for false data attacks on power system state estimation," in *Proc. of 44th Annual Conference on Information Sciences and Systems (CISS '10)*, Mar. 2010.

[20] H. Khurana, R. Bobba, T. Yardley, P. Agarwal, and E. Heine, "Design principles for power grid cyber-infrastructure authentication protocol," in *Proc. of the 43rd Annual Hawaii International Conference on System Sciences (HICSS '10)*, Jan. 2010.

[21] R. Bobba, H. Khurana, M. AlTurki, and F. Ashraf, "PBES: A policy based encryption system with application to data sharing in the power grid," in *Proc. of the 4th ACM Symposium on Information, Computer and Communications Security (ASIACCS '09)*, Mar. 2009.

[22] Q. Wang, H. Khurana, Y. Huang, and K. Nahrstedt, "Time valid one-time signature for time-critical multicast data authentication," in *Proc. of IEEE INFOCOM 2009*, April 2009, pp. 1233–1241.

[23] Y. Huang, W. He, K. Nahrstedt, and W. C. Lee, "DoS-resistant broadcast authentication protocol with low end-to-end delay," in *Proc. of IEEE INFOCOM Workshops 2008*, April 2008.

[24] M. LeMay and C. A. Gunter, "Cumulative attestation kernels for embedded systems," in *Proc. of the European Symposium on Research in Computer Security (ESORICS '09)*, Sept. 2009.

[25] S. A. Zonouz, H. Khurana, W. H. Sanders, and T. M. Yardley, "RRE: A game-theoretic intrusion response and recovery engine," in *Proc. of the IEEE/IFIP International Conference on Dependable Systems and Networks (DSN '09)*, Jul. 2009, pp. 439–448.

[26] U. Premaratne, J. Samarabandu, T. Sidhu, B. Beresh, and J.-C. Tan, "Evidence theory based decision fusion for masquerade detection in IEC61850 automated substations," in *Proc. of the 4th International Conference on Information and Automation for Sustainability (ICIAFS 2008)*, Dec. 2008.