Data-Centric Threats and Their Impacts to Real-Time Communications in Smart Grid

Mingkui Wei Wenye Wang
Email: {mwei2, wwang}@ncsu.edu
Department of Electrical and Computer Engineering
North Carolina State University, Raleigh, NC, 27606

***Abstract*—One of the most distinguished challenges in studying the aftermath of cyber attacks in smart grid lies in *data-centric* threats, which refer to cyber attacks aimed at gaining advantage or sabotage the infrastructure by manipulating the data exchanged in the underlying communication network. Even though such attacks are critical by itself in the information network, they will result in more serious impacts to the power grid. This is because for an information-centric network, distorted or delayed information undermines services and applications, in the case of a power grid, however, these data-centric attacks may result in unstable systems, which may further detrimentally impact the power supplies. In this paper, we study the impacts of data-centric attacks in the real-time communication network of smart gird, and further the consequences caused to the power grid. Our study provides insights to both smart grid security research and operation.**

***Index Terms*—Smart Grid, Cyber Security, Co-simulation.**

I. Introduction

SMART grid is emerging to be a typical application of the cyber physical systems (CPS), which integrates advanced communication networks, i.e., the cyber system, with conventional power grids as the physical system. Assisted by advanced communications, power devices, which were unable or with very limited capacity to communicate, are granted with the capability to exchange critical information with their peers. The real-time information exchange expedites power devices to make more accurate and prompt reactions, and further facilitates the implementation of a more reliable, effective and efficient bulk power delivery and distribution.

However, despite all promising benefits of the smart grid, we must be aware that this integration also brings a new host of vulnerabilities to conventional power systems, which are the threats of *cyber attacks* [1]–[4]. Cyber attacks are offensive maneuvers conducted by adversaries and target the computer network and information system, and the purpose of which is to seek unlawful benefits by infiltrating the information that is exchanged in the network. To this end, we define *data-centric attacks* as the attacks in the cyber system which aim at gaining advantage by manipulating the data that exchanged within.

Data-centric attack is one of the biggest concerns by itself in the cyber world, even worse, the integration of the communication network opens a backdoor in the power system, which leads in cyber attackers and allows them to make detrimental impact to this critical infrastructure without the necessity of any physical access. Over years we have witnessed various data-centric attacks and their devastating impacts in both academic researches and real industries. For example, the false data injection attack [5]–[8] proves that the bad-data detection mechanism in modern power grid can be bypassed, where attackers are able to make modification on monitored system status variables without being detected; more practically, the Stuxnet [9]–[11] that has been identified in early 2010s is a computer worm, which infected the SCADA system [12] and distorted its control data, and eventually destroyed many nuclear power plants in multiple countries. Therefore, it is undoubted that data-centric attacks are real and imperative threats to smart grid, and it is of great importance to study them and understand their impacts.

However, existing researches on evaluating and understanding data-centric attacks in smart grid are primarily conducted in an "ad-hoc" manner [13]–[15]. In particular, we notice that there lacks a well-established scheme or approach that allows us to effectively evaluate, compare and prioritize various cyber threats. To this end, one of the biggest challenge is *how to effectively evaluate the physical impacts that are caused by data-centric attacks in smart grid based on an unified platform*. The answer to this question is non-trivial, because only by understanding their impacts based on an unified platform, can we prioritize and optimally allocate our resources and efforts on treating the most imperative risks.

In this paper, we are motivated to tackle this question by adopting a simulation-based approach. In particular, we present *Greenbench*, a cross-domain simulation benchmark, and use case studies to demonstrate its capability by quantitatively evaluating the impacts of data-centric attacks. The simulation-based approach is chosen over experiments and theoretical modelings for the following reasons. Although experiment is the most accurate and practical method in evaluating the physical impacts, it is cost-prohibitive to build a laboratory with real power devices for destructive experiments. Theoretical modelings, on the other hand, are difficult to reflect dynamic system behaviors in real-time, which is a critical factor in evaluating the impact of data-centric attacks.

We carry out case studies to leverage our understanding of both the impact of data-centric attacks, and the effectiveness of their countermeasures. A preliminary study of this work has been published in [16], in which we built the Green Hub, a 17-bus smart grid prototype, and evaluated the impact of 2

Earlier version of this work was published in the 2014 IEEE Conference on Computer Communications (INFOCOM'14).

data-centric attacks, i.e., *jamming the price signal attack*, and composite attack with *Load-redistribution attack* and the *Man-in-the-Middle attack*. In this paper we extend previous study in the following aspects. First, we evaluated another composite attack, which is composed by the *false data injection attack* and the *Distributed Denial-of-Service (DDoS)* attack. This case differs from the previous composite case in that the Man-in-the-Middle attack mainly concerns the confidentiality and integrity of information, while the DDoS attack is to impair information availability. Second, we evaluated the effectiveness of a classic cyber-attack countermeasure, i.e., using Hash-based Message Authentication Code (HMAC) to ensure information authenticity. We demonstrated that conventional countermeasures may not be readily adopted to address smart grid security issues. Third, we scale-up the smart grid model and evaluated data-centric attacks in a larger scale power system, i.e., the IEEE 57-bus system. Our results show that smart grid with larger scale is relatively less sensitive to data-centric attacks. Nevertheless, we denote that it is imperative and non-trivial to address cyber-attacks in smart grid, because more intensive attacks can still result in serious results even in large scale smart grid.

The remainder of this paper is organized as follows. In Section II we introduce related works and the background of *data-centric attacks*. In Section III, we demonstrate *Greenbench*, the cross domain simulation benchmark we developed for data-centric attacks evaluation. In Section IV we describe the setup of each case, present simulation results and draw in-depth observations. And we conclude our work in Section V.

II. Background

A. Related Works

The cyber security issue in smart grid have attracted a lot of attentions in recent years. However, there are very few works which covered the perspective of simulating cyber attacks and evaluating their results in the power grid. The DETER project [17] is a testbed that is built for studying cyber-security issues in cyber-physical systems, and based on which several studies [18], [19] were conducted on smart grid cyber-security. However, it has been shown in these works that it is difficult for DETER to capture the transient time reactions of power systems, since it is not a dedicated design for smart grid. The Electric Power and Communication Synchronizing Simulator (EPOCHS) [20], [21] is a cross domain simulator which integrates the power system and the communication network, however, its focus was on studying the behavior of the power grid with the assistant of communications, where communications are treated as a way to deliver information, and security issues were left unconsidered. In [14], the authors studied the impacts of cyber attacks in smart grid, and showcased the results of cyber attacks with a 13 nodes distribution power system. Our work differs from this work in that our work provides a more generalized framework, which is able to accommodate power systems with different topology. As the most practical approach, many major national research laboratories also developed various testbeds for smart grid study [12], [22], which are, unfortunately, not publicly available for researchers in general. Motivated by these existing works, we develop *Greenbench* by integrating off-the-shelf simulators in both domain, which makes it an easily accessible, and dedicated smart grid simulation benchmark for cyber-attack simulation and evaluation.

B. Data-centric Attacks

We denote the data-centric attack is the type of cyber-attack which targets at manipulating the *information* (i.e., data) that is exchanged in the communication network of a smart grid.

The CIA-triad [23] has been well known as the most fundamental principles in *information security*, which comprises *Confidentiality*, *Integrity*, and *Availability*. For the scope of smart grid in particular, data confidentiality means keeping the secrecy of the data and preventing it from being known by unauthorized parties. For example, the profile of power usage of a user should be disclosed only to the utility company and the user himself. Data integrity means the data delivered to the receiver should be complete and intact. For instance, the data sent by distributed monitoring devices and received by the control center should reflect real system status, any distortion will cause the system to deviate from correct operation. Data availability ensures the data should be delivered within required time, e.g., a delayed "trip" message sent to a circuit breaker may be unable to stop a fault propagation, and thus is unacceptable. We propose several case studies according to these three aspects in the later section, such that we are able to thoroughly evaluate the impacts of data-centric attacks.

III. Greenbench: The Cross-Domain Simulation Benchmark

A. Greenbench *Framework and Implementation*

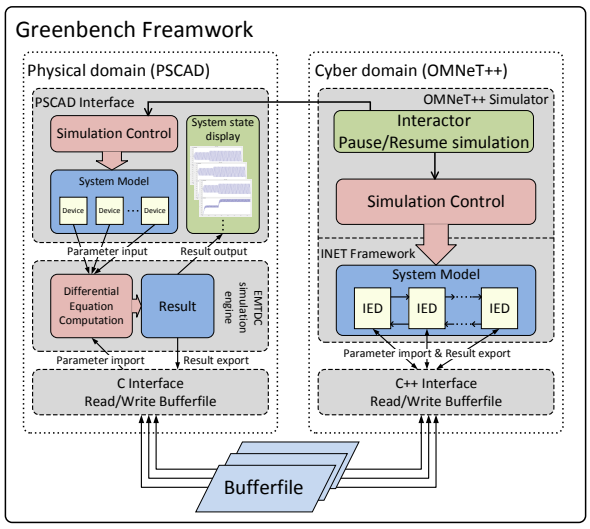


Fig. 1. Software implementation of *Greenbench*.

In Fig. 1 we present the framework of *Greenbench* and its software architecture. The *Greenbench* framework is composed by two modules (simulators), the physical module (PSCAD [24]) and the cyber module (OMNeT++ [25]), which

interact through two interfaces, the *interactor*, and the *bufferfiles*.

1) Interactor: The interactor is a special module built *within* OMNeT++, whose main function is to maintain the synchronization of simulation between the two simulators.
2) Bufferfile: The bufferfile is a pool of binary files, which provides a "buffered zone" and enables the two simulators exchange data during simulation in real time.

The physical domain part can be further divided into 3 functional blocks.

1) Interface: The interface function block provides Human-Machine interaction, which allows users to control the simulation operation such as begin, pause, resume and stop. Within the interface block, user can build the system model and observe graphical system behavior.
2) EMTDC simulation engine: EMTDC is a electromagnetic transients simulation engine which takes device parameters as the input, computes system state by solving differential equations, and exports the result as the output.
3) C interface: The C interface is a bi-directional interface written with C language. It fetches data from bufferfiles and pass it to EMTDC; and receives the results from EMTDC, and write them back to bufferfiles.

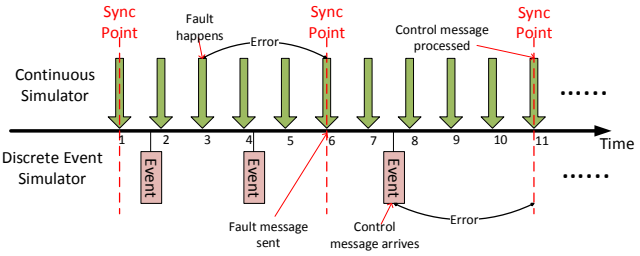
The cyber domain part comprises 2 function blocks:

1) OMNeT++ simulator/INET framework: The OMNeT++ is a platform which provides basic graphical interface and simulation control (begin, stop, etc). The INET is a framework that is built based on OMNeT++ and provides Internet-specific support, such as wireless/wired channels, and TCP/UDP protocols. The cyber domain entities of a smart grid, i.e., IEDs, and the communication network are built in OMNeT++ with models provided by the INET framework.
2) C++ interface: The function of the C++ interface is similar to the C interface in the physical domain, which is written with C++ and implements the functionality that import/export data from/to bufferfiles.

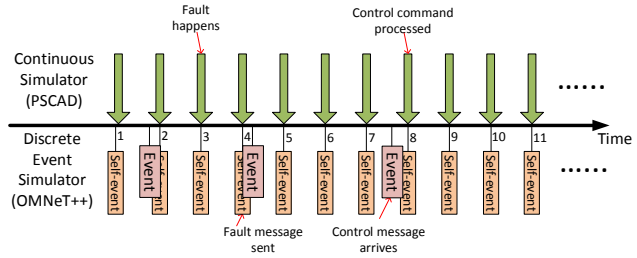
B. Design Challenges

Although the idea that make PSCAD and OMNeT++ simulate the counterpart of a smart grid on its own, and integrate the results seems intuitive and straightforward, two challenges stand out during its implementation, which are the *synchronization* of the simulation steps, and the *data exchange* between the two simulators during a simulation run. These two challenges are addressed by the *interactor* and the *bufferfile*, respectively.

1) Synchronization of Continuous and Discrete Events: Most of the network simulators, such as NS2, OPNET, OMNeT++, are *discrete event* simulators. A discrete event simulator is driven by queued events, each event occurs at a particular time and marks a change of system state. Between two consecutive events, it is assumed that the system state remains unchanged. As a result, the simulation of a discrete event simulator can directly jump from one event to the next without considering how much "wall-clock time" will be cost in between. On the contrary, power system simulators such as PSCAD and RTDS [26] are *continuous* simulators, which solve differential equations at a fixed time step. Therefore, the simulation of a continuous time simulator is executed step by step without any one can be skipped.



(a) Error-prone synchronization

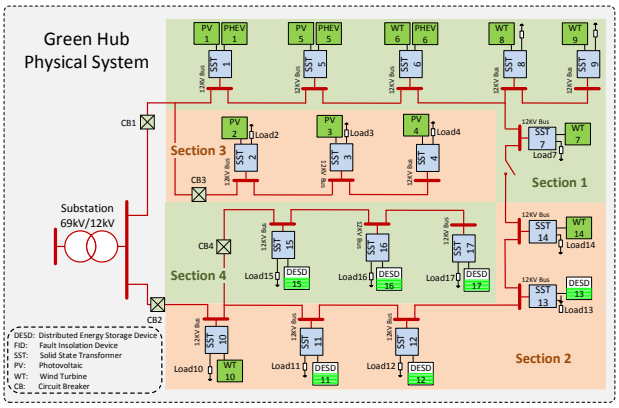


(b) Error-free synchronization

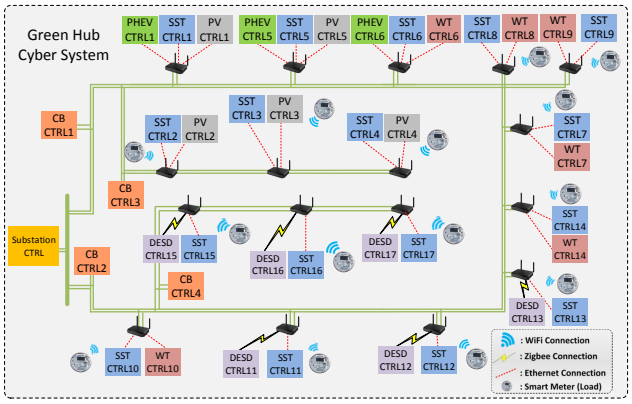
Fig. 2. Synchronization of continuous and discrete events.

The different ways to handle simulation time cause the synchronization problem, that is, how to keep the two simulators progress at the same pace. A few works addressed this problem by introducing an external scheduler [21], [27], which causes extra overhead, an may introduce error accumulation as is shown in Fig. 2(a), i.e., it is possible that between two sync-points, multiple events have happened in either domain, such that when a sync-point arrives, those events were accumulated and executed together with their timing indistinguishable. In *Greenbench* framework, we tackle this issue by developing a special module in OMNeT++ to handle simulation synchronization.

OMNeT++ is an event-driven simulator, and the "events" are implemented as *messages* that are exchanged among modules in the simulated system. For example, the event that "a data packet is passed down from TCP layer to IP layer" is implemented in the MONeT++ by having the TCP layer module generate a *message*, and pass it to the IP layer module. The OMNeT++ also allows a module to send messages to itself, i.e., *self-message*, at any scheduled time in the future. The *self-message* enables the OMNeT++ act as a continuous simulator that could be perfectly synchronized with PSCAD. Particularly, we developed a special application within OMNeT++ framework, named as the "interactor". The interactor periodically sends self-message to itself according to the simulation step of PSCAD, and at each time a self-message is received, the interactor switches the simulation execution between the two simulators, i.e., halts the simulation on one simulator and resumes on another. The *self-message* frequency of the interactor can be adjusted in order to accommodate the PSCAD simulation whose time-interval between



(a) Green Hub Physical System



(b) Green Hub Cyber System

Fig. 3. Green Hub implementation.

simulation steps is adjustable. The error-free synchronization scheme is shown in Fig. 2(b). For instance, the physical fault that happened at time t_3 can be known by the OMNeT++ immediately, instead of waiting to the next sync-point at time t_6, and the *event* in the OMNeT++ generated between time t_7 and t_8 will be processed at the PSCAD side at time t_8 instead of t_{11} where the next sync-point sits.

2) Data Exchange: Another key factor in implementing the integration is how to allow these two simulators to exchange their simulation status in real-time.

In [21], [27], a Runtime Infrastructure or a Globe Scheduler process is used as a globe manager to handle the interaction, this implementation is effective but lacks efficiency. Another alternative is to use Inter-Process Communication (IPC), a technique implemented in the operating system level for process communication, to directly exchange data between the two simulation process. Common IPC implementations includes named pipes (also known as fifo), Windows socket, and shared memory. The fundamental idea of IPC is to assign a media that is shared and can be accessed by both processes. Based on the concept, in this work we introduce the "bufferfile" in *Greenbench* to implement the status exchange. In particular, we create two binary files for each cyber-physical component pair, e.g., a circuit breaker in the power domain and its controller in the cyber domain. These two files are directional: one is written by the cyber component and read by the physical domain, another is operated in the reverse way. These files act as a buffered zone between the cyber system and the physical system, and thus we name them "bufferfiles". During a simulation, at the beginning of each simulation step for both simulators, the components will first check the bufferfile and import the data that has been written by its counterpart, and at the end of the step, it will write its own status to the bufferfile to inform its counterparts.

C. Green Hub: the Micro Smart Grid

The Green Hub [28] system is a distribution level microgrid developed at the Future Renewable Electric Energy Delivery and Management (FREEDM) Systems Center in North Carolina State University. It was summarized from the power system in the city of Raleigh where NCSU locates, and it was built specifically for smart grid study. Since it is more related to smart grid and its configuration is more up-to-data compared to multiple IEEE multi-bus systems [20], [29], we choose to use the Green Hub to carry our study in this work.

As shown in Fig. 3, Green Hub is a 17-bus distribution level power system. Green Hub contains various innovative power devices developed at the FREEDM center, such as the Solid State Transformer (SST) [30], and the Fault Isolation Device (FID) [31], and it is also connected with green energy sources such as Photovoltaics (PV) and Wind Turbines (WT). All devices are equipped with Intelligent Electronic Devices (IEDs), which are ARM-based embedded computers for real time communication. Those IEDs interact with each other to make the Green Hub a self-autonomous micro smart grid, which can either connects to main power grid, or operate in stand alone mode.

IV. Simulation Setup and Evaluation Results

A. Delayed Wireless Communication in AMI (Jamming the price signal attack)

The Advanced Metering Infrastructure (AMI) that is composed by the smart meters greatly facilitates more efficient power system management. For instance, smart meters are able to update the control center with real-time power usage information of each household, such that power consumption can be more accurately predicted and accommodated. On the other hand, however, the smart meter is one of the most vulnerable components in smart grid. For the first reason, it is physically accessible to the public, which facilitates various forms of physical intrusion [32]. Second, it transmits data by wireless communications, thus is susceptible to both active attacks such as jamming [33], and passive attacks such as eavesdropping [34] and user privacy prying [35], [36]. Therefore, it is critical to study the vulnerability of the AMI and understand how a power system can be impacted when the AMI is breached by cyber-attacks.

In this case we assume the data *availability* is breached by the *jamming the price signal attack* [33]. This line of research includes [33], [37], and stems from the concern that

in the paradigm of smart gird, more and more power load will become remotely controllable, and as a result, attackable. For instance, the smart meter of a household will be able to control the operation of major appliances such as water heaters or air conditioners, in this case, if an attacker is able to compromise a large number of smart meters [38] and manipulate these appliances to operate or shut down at the same time, the profile of power consumption can be significantly changed in very short time, and thus power system instability can be caused.

Particularly in this case, it is assumed the Time-of-Use pricing is implemented, in which the price for power usage is changing over time. The pricing information is decided by the control center, and disseminated to distributed aggregaters that locate close to consumers. The aggregaters then broadcast this pricing information wirelessly to smart meters, and the smart meters will decide how much power they want to use based on the current price. The wireless channel, however, is susceptible to the jamming attack [39], which is able to completely abrupt normal communication and make the pricing information *unavailable* to smart meters. If the attacker is able to jam the communication for sufficiently long time until there is a significant change on the price, and then stops the jam and let the meters receive the new price, the smart meters may all decide to make a considerable change on their power consumption and thus cause instability to the power system.

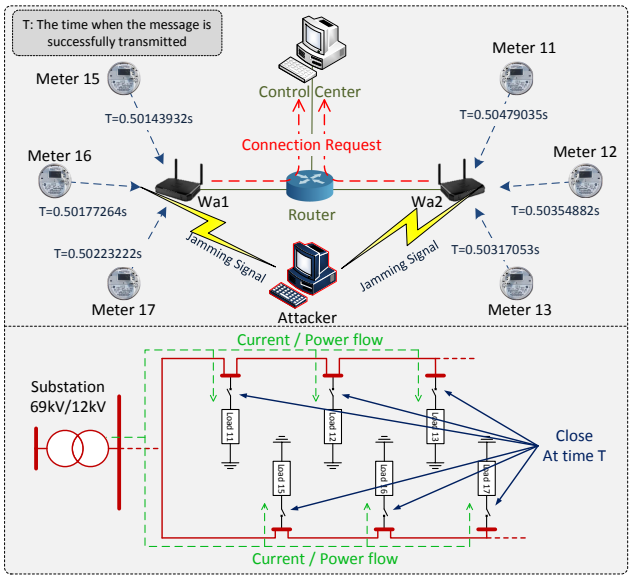


Fig. 5. Jamming the Price Signal attack.

As shown in Fig. 5, there are 2 sets of smart meters that have been chosen as the jamming targets, i.e., $\{m_{11}, m_{12}, m_{13}\}$, denoted as set_1, and $\{m_{15}, m_{16}, m_{17}\}$, denoted as set_2, since they are geographically adjacent. There are two wireless aggregaters that distribute the pricing information to these two sets of meters. We set the two set of meters randomly distributed in a 100-by-100 meter area, which essentially represents a geographical area such as a small community, and the two sets of meters do not interfere with each other. We then set one attacker, who is able to transmit with much higher transmission power such that he is able to interrupt the normal communication in both areas. We assume that the attacker is able to jam both areas for sufficiently long time until the price has been significantly changed. And we denote the time $t = 0.5s$ as when the attacker decides to stop jamming and let the smart meters receive the updated pricing information.

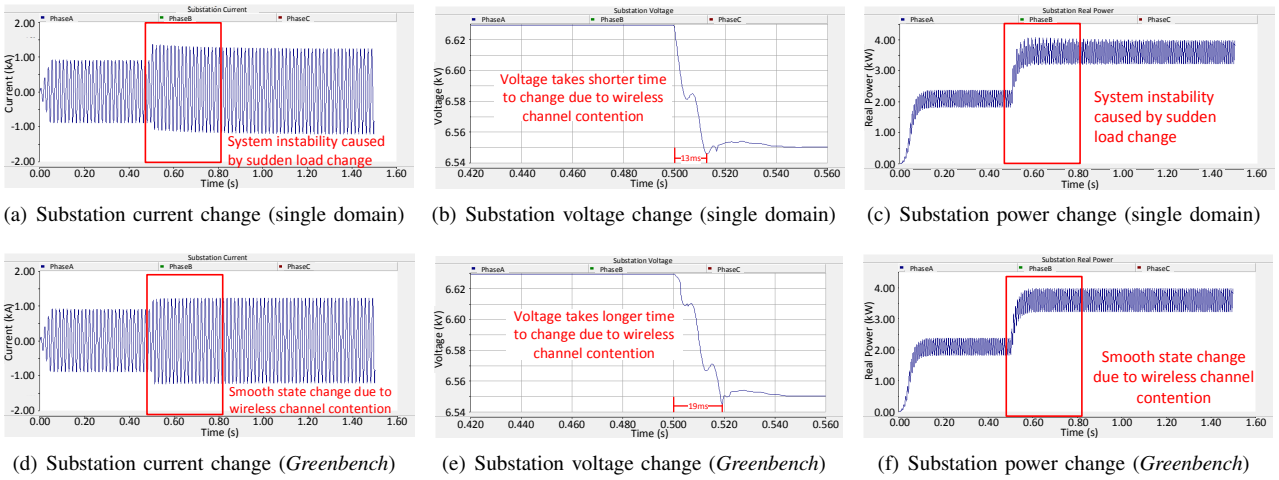
1) Single domain simulation: It has been well studied that sudden change of large amount of load will cause various problems in the power system. For instance, sudden load change will cause load-generation imbalance and drive the system frequency deviate from its normal value, which can result in economic loss to the utility companies, or even cause permanent damage to power devices [40], [41]. We hereby simulate this case in the single domain, i.e., the power system only, for the purpose of both baseline the result of the load change, as well as to showcase the difference that can be provided by the *Greenbench*.

When being simulated in the single domain without considering the characteristics of the communication network, this attack can be simply applied as the action to close the circuit breakers at all 6 buses. In Fig. 4(a), Fig. 4(b) and Fig. 4(c), we demonstrate the change on the current, voltage, and real power at the substation. In order to most clearly demonstrate the result, in this simulation we assume the extreme case, in which all the loads consume the least possible power, i.e., zero consumption, before and during the jamming, and request the maximum power when the jamming is terminated.

As shown in Fig. 4(a), Fig. 4(b) and Fig. 4(c), the jamming stops at 0.5 seconds. Because the load controlled by these 6 meters comprises almost 45% of the total load in the system, this change causes a significant variation in this power grid. We are able to observe a distortion lasting about 1 second on both the current and the power, as highlighted by the red box in Fig. 4(a) and Fig. 4(c), which may cause adverse effects to the power grid [42], such as generator and transformer overheating.

2) Greenbench simulation: When being considered in the cross domain with the interaction between the power grid and the communication network, however, the scenario stated above is oversimplified. The main concern is that in the single domain scenario, the communication is implicitly assumed as ideal, i.e., communication delays do not exist. In practice, however, the smart meters won't be able to communicate with the wireless aggregater all at the same time. This is because wireless channels are exclusive, which means that at one time instance there is only one pair of host is allowed to communicate, otherwise, collisions will happen and the communication will not succeed. In order to reflect how can a practical communication network affect the result of this jamming attack, we reconsider the case in cross domain and simulate it in *Greenbench*.

As shown in Fig. 5, wireless aggregators (Wa_1 and Wa_2) communicate to the two sets of smart meters. Within each aggregator's transmission range, meters contend with each other to access the wireless channel [43]. And the physical load is connected to the power system only when its smart meter gains the opportunity to send its connection request to control center. And because of the exclusive nature of the



(a) Substation current change (single domain) (b) Substation voltage change (single domain) (c) Substation power change (single domain)

(d) Substation current change (*Greenbench*) (e) Substation voltage change (*Greenbench*) (f) Substation power change (*Greenbench*)

Fig. 4. Jamming the price signal attack simulation.

wireless channel we mentioned above, all meters actually take turns to send their messages, and therefore, loads are not connected exactly at the same time. We also shows the time when the messages are received at the control center in Fig. 5, from which we observe the delays are relatively insignificant for most Internet applications. Nevertheless, we are interested to find out whether this small delay can cause any impact on the power grid.

The *Greenbench* simulation result is demonstrated in Fig. 4(d), Fig. 4(e) and Fig. 4(f). Compared with single domain simulation, the current and power transition is more smooth and there are no visible distortions. We can also observe that the voltage takes longer time to drop to the stable value, i.e., 19 ms versus 13 ms in the single domain case, which is also favorable, because for a practical physical generator, it can not adapt to any sudden change, but have to slowly speed up/down its rotor to generate more/less power, thus a slower voltage change is preferable for power grid stability.

3) Summary: We demonstrate in this case that the *Greenbench* is able to reflect communication network characteristics, e.g., wireless channel contention and message delay in this particular case, and integrate them into the reaction of the power grids. As a result, we can evaluate the impact of data-centric attacks from a more realistic perspective.

We also observe that for this simulated case in particular, the jamming-the-price-signal attack is not as harmful as it appears to be theoretically. And this observation essentially suggest that, when evaluating the impact of cyber attacks in the smart grid, it is indispensable to consider the communication network characteristics (e.g., wireless channel contention) and anomalies (e.g., message delay). Shown by this case, although the channel contention and message delay are generally considered as negative factors, their existence ironically enhanced the power grid reliability.

B. Impact of Composite Attacks

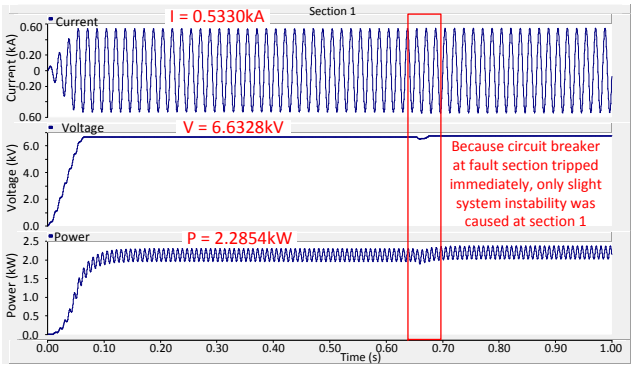
In the previous case, we studied the reaction of the smart grid when the data *availability* is breached by the *jamming the price signal*. We demonstrate that the impact of such attacks can be different (i.e., less significant) than their theoretical results, when practical communication characteristics are considered.

In this subsection, we further evaluate two *composite attack* cases, to demonstrate the results when multiple attacks are combined together to attack smart grid. We argue this is an very realistic assumption because the power grid is one of the most critical infrastructures, thus it is very likely that smart grid attackers are well prepared and will exploit every possible means to maximally deteriorate the impact.

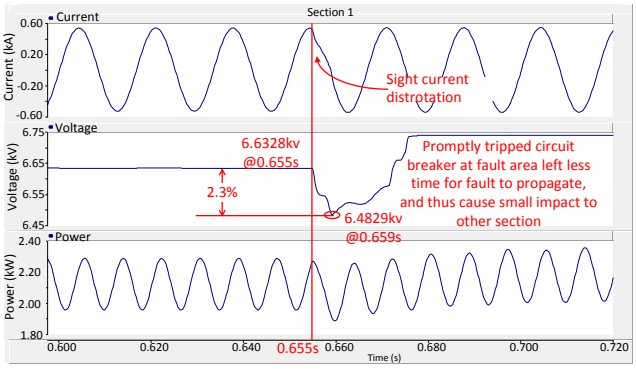
1) False Data Injection and DDoS Attacks:

a) False data injection attack: The healthy operation of the smart grid relies on real-time information exchange between distributed power devices and control centers. For instance, the Intelligent Electronic Devices (IEDs) located at distributed substations periodically report to control center of monitored system values, such as voltages or currents, and based on these aggregated data the control center estimates the running status of the whole power grid, and make necessary adjustment. The implementation of this process essentially relies on the *confidentiality* and the *integrity* of the information that is exchanged between the IEDs and the control center. For example, an attacker who knows the operation status, i.e., confidentiality is breached, can evaluate and thus identify the most vulnerable parts in the grid, even worse, an attacker who is able to modify such information, i.e., integrity is breached, can manipulate the grid at his will and cause unpredictable demolishing results. In one of the recent researches, namely the *false data injection attack* [5], it has been identified that the state estimation algorithm [13], [44] in the power gird, rely on which the control center estimates system states and identify any anomalies, can be bypassed by attackers, in particular, the attacker is able to introduce arbitrary errors into state variables without being identified by bad measurement detection techniques.

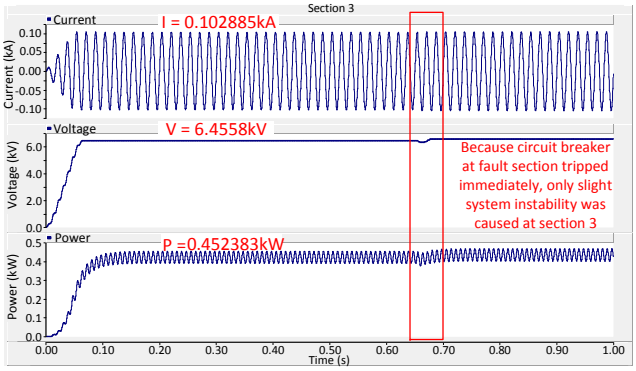
Since our objective is to observe the impact of such attacks but not to study its detailed implementations, we hereby assume the attacker already compromised the smart meter at load l_{15}, and thus takes control of all the subsequent power devices. He commands the devices to consume more power,



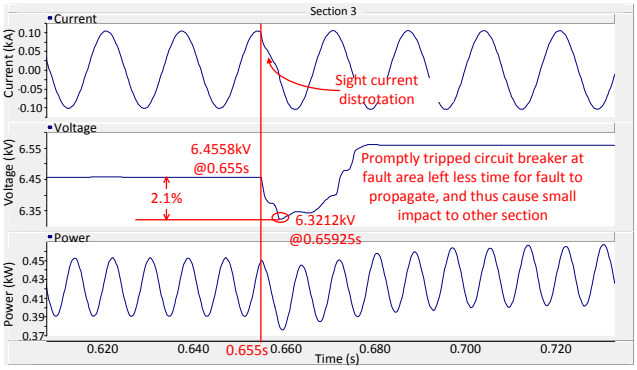
(a) Section 1 Bird-view



(b) Section 1 Zoom-in



(c) Section 3 Bird-view



(d) Section 3 Zoom-in

Fig. 6. Green Hub operation on sections 1 and 3 without DDoS attack.

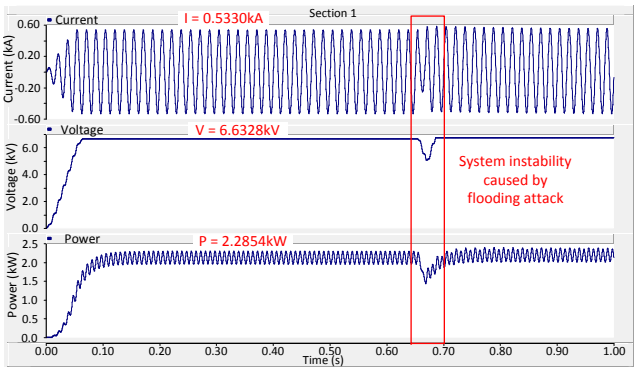
while at the mean time he modifies the power consumption message from this smart meter by means of the *false data injection* attack, such that although the actual power flow and current keep increasing at the compromised section, the control center is unable to realize this situation. Eventually, the current on this section exceeds threshold and causes a fault on transmission lines. The overcurrent fault is detected by a higher level device, i.e, the IED locates at circuit breaker 4, and informed to the control center. On knowing this emergency event, the control center sends a *trip* command to circuit breaker 4, and the fault is isolated.

In this case we assume all messages in this network are delivered correctly and timely. In particular, whenever an IED senses the fault current, it sends the event to the control center immediately, and the control center replies with a trip command to open the circuit breaker once the report is received. The only delay involved in this scenario is the processing delay (message being passed through different network layers) at each communication host, and transmission delay between them.

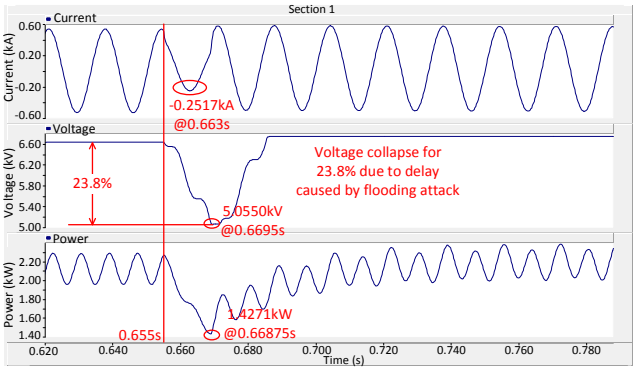
In Fig. 6 we demonstrate the system reaction by showing the change on current, voltage and real power. We choose to demonstrate the results on section_1 and section_3, as classified and depicted in Fig. 3, because these two sections are relatively distant from the fault, i.e., load l_{15}, such that we are able to understand how can a system fault impact the system as a whole. Also the results for section_2 and section_4 are similar to those of section_1 and section_3, but only with different significance. In Fig. 6 we present the result in two scales, the "bird-view" scale display the system operations before, during and after the fault happens, and the "zoom-in" scale shows specifically the time instance when the system is impacted.

From the figure, we can find that although the information at load l_{15} is distorted, the power grid still retains high resilience to this attacks since the system fault can still be reported and reactions can still be taken in time. From the bird-view figures we can tell that there are not noticeable current disturbance on both sections, and voltage collapse is also insignificant. We zoom in the voltage collapse of section 1 and section 3 and show them in Fig. 6(b) and 6(d), from which we can see the maximum voltage collapse is less than 3% of their original value, which is within acceptable voltage instability range according to industry standards (voltage swing are typically required to be within $\pm 5\%$ in practical power systems) [45].

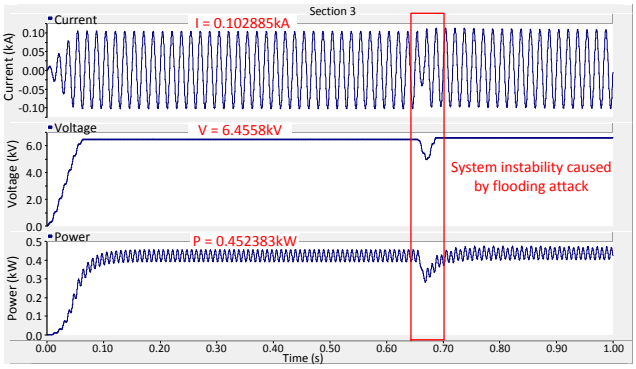
b) False data injection and DDoS attack: We have shown in the former case that the power grid possess high resilience to cyber-attacks. In particular, although instability can be caused in the system by data-centric attacks, the impact is largely limited, this is because although the control center is deceived at the first time and thus unable to prevent the negative event from happening, it can limit the damage by taking prompt reactions after the event is caused, thanks to the inter-connected communication network in which an fault



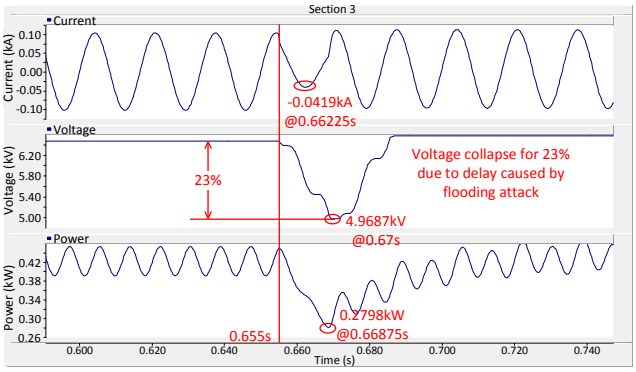
(a) Section 1 Bird-view



(b) Section 1 Zoom-in



(c) Section 3 Bird-view



(d) Section 3 Zoom-in

Fig. 8. Green Hub operation on sections 1 and 3 under DDoS attack.

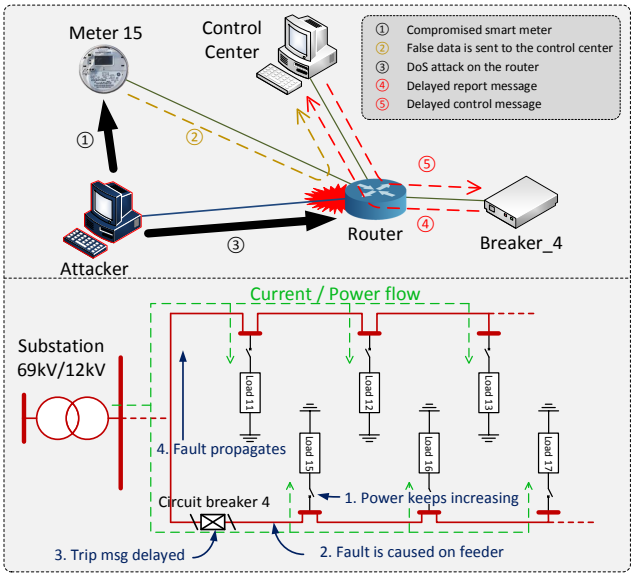


Fig. 7. DDoS attack to the communication channel.

event can be escalated by multiple components.

This fact leads to another interesting question, which is, *to what extent can smart grid resist to composite attacks*? In this case, we assume a more competent attacker who can not only modify the monitored data, but also break into the communication network and apply a Distributed Denial-of-Service (DDoS) attack to slow down the message transmission. The DDoS attack congests the communication channel by overwhelmingly sending useless data packets to the control center and impedes legitimate message delivery, which eventually makes the control center unable to instantly respond to system emergencies. In this case we are interested in observing how can the DDoS attack, a classic cyber-attack, affect the power grid operation.

The cyber-domain setup of this simulation is described as follows. We assume all communication links among the communication hosts, i.e., the control center, IEDs, and attackers, are ideal, which does not have any packet loss or message delay. And we set the bandwidth of each link to be 10 Mbps. We choose the bandwidth to be relatively small for two reasons. For the first, a practical smart grid network contains far more communication components than that is in our model, which will result in much larger background traffic. Therefore, we set the bandwidth relatively small as a compensation for such background traffics. For the second, larger bandwidth only requires more intensity in the DDoS attack, e.g., more compromised hosts that send more flooding data, while the result, i.e., extra delays caused on legitimate messages, can remain at the same level. Based on above two reasons, we set the 10Mbps communication link to facilitate our simulations.

For the DDoS attackers, we assume there are 12 communication hosts that have been compromised in the network, which are manipulated by the attacker to continuously send useless messages to the control center, we set the data rate of each communication host to be 0.5 Mbps. Here we assume

a relatively "mild" attack, because our interests are not on studying the effectiveness of any DDoS attacks, but to observe the impact of DDoS attacks in smart grid. And for the value we chose, it is already sufficient enough to show a noticeable impact. We set all communications in this network to use UDP protocol, because TCP cost longer time to achieve reliability, which does not fit such time-critical scenario.

The simulation result is given in Fig. 8, which shows that combining with the DDoS attack, the false data injection attack can cause more significant impact to the smart grid. As shown in Fig. 8(a) and Fig. 8(c), DDoS attack causes visible current distortion, and voltage collapse becomes much larger as well compared with that in the DDoS-free case. Especially, as shown by Fig. 8(b) and Fig. 8(d), due to the extra delay introduced by the DDoS attack, the voltage collapses more than 20% in both sections, which will further cause these two sections be disconnected for protection purpose [45] (this consequential impacts are not shown in our simulation).

Compare the composite attack with the single attack, we see that assisted by the DDoS attack, the damage of the false data injection attack can be remarkably escalated. In order to better understand the relationship between delayed messages and the consequent damages in the power grid, we measure the message delays in both cases, and compare them in Tab. I. We notice that the DDoS attack introduces about 7 milliseconds delay to the messages which are sent from IEDs to the control center. Although this short delay is insignificant in most generic Internet applications, it causes non-trivial consequences in the real-time control system in smart grid. This result demonstrates the necessity of a secure and reliable communication network in smart grid, as it shows even a data-centric attack which is considered mild in the cyber world can result in significant damage in the cyber-physical system, it also justifies the stringent delay requirements that have been specified in the smart grid communication standards, such as [46], [47].

TABLE I
MESSAGE TRANSMISSION DELAY, ROW 1 SHOWS UNDER DOS ATTACK, ROW 2 SHOWS NORMAL COMMUNICATION.

	Obj	at CB	CB→CC	at CC	CC→CB	at CB
1	CB2	t=656	Δt=7.182	t=663.182	Δt=0.135	t=663.317
	CB4	t=656	Δt=7.115	t=663.115	Δt=0.135	t=663.250
2	CB2	t=656	Δt=0.202	t=656.202	Δt=0.134	t=656.336
	CB4	t=656	Δt=0.134	t=656.134	Δt=0.135	t=656.269

Note: CB denotes Circuit Breaker, and CC denotes Control Center, unite is in millisecond (ms).

2) Load Redistribution and Man-in-the-Middle Attack:

a) Load redistribution attack: In this case we evaluate the Load Redistribution (LR) attack identified in [48]. The LR attack is a special type of the false data injection attack which has more practical constrains on the attackable nodes in smart grid. Particularly, while false data injection attack treats each node homogeneously, LR attack assumes that the attacker can only attack the load, i.e., the power consumers. Other components such as generators are not attackable because those critical components are usually more intensively protected, e.g., by physical protections such as fences or video

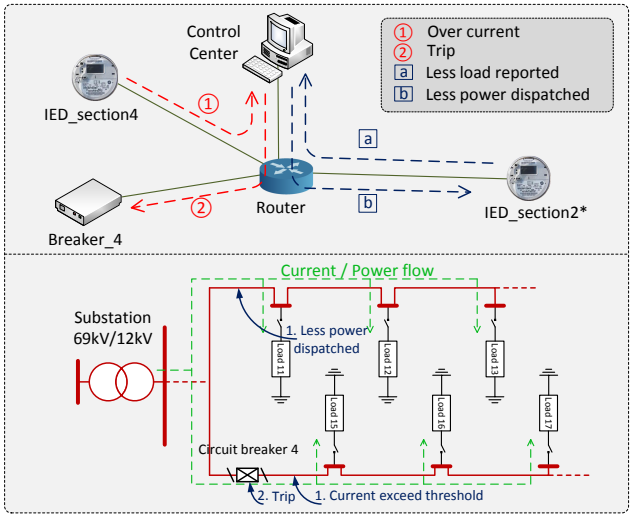


Fig. 9. Load Redistribution attack.

surveillance. Note in this attack, the attacker's goal is not to change the actual load, i.e., the power consumed, but to modify the load reading, which is the monitored value that is sent to the control center.

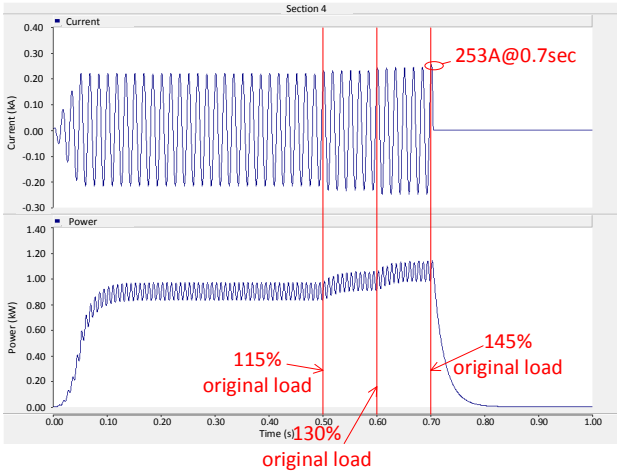
In this case, we assume that the attacker compromised smart meters m_{11}, m_{12}, m_{13}, m_{15}, m_{16}, and m_{17}. Two critical constrains of the LR attack are that the summation of the load readings in the attacked area remains unchanged, which means if the attacker increases the reading on some meters, he has to reduce the same amount on others such that that summation of total readings matches the total power that is actually consumed, such that the control center is less likely to identify any system anomaly; and the changed reading on each individual load does not exceed 50% of its actual load, since the more significant on the changes, the more likely the control center will notice the existence of such attack. The attack scenario is shown in Fig. 9.

1) The attacker increases the readings on meter m_{15}, m_{16}, and m_{17}; and decreases the readings on meter m_{11}, m_{12}, and m_{13} accordingly, and the total increased value at load l_{15}, l_{16}, l_{17} equals the total decreased value at load l_{11}, l_{12}, l_{13}.
2) The attack is deployed in 3 steps, each of which takes 0.1 seconds. Within each step, at load l_{15}, l_{16}, and $_{17}$, the attacker increases their readings by 15% of their actual load, and at the same time he decreases the same amount on the readings of load l_{11}, l_{12}, and l_{13}. The total change (increase/decrease) of readings for each load is 45% of its actual load at the end of the 3rd step.

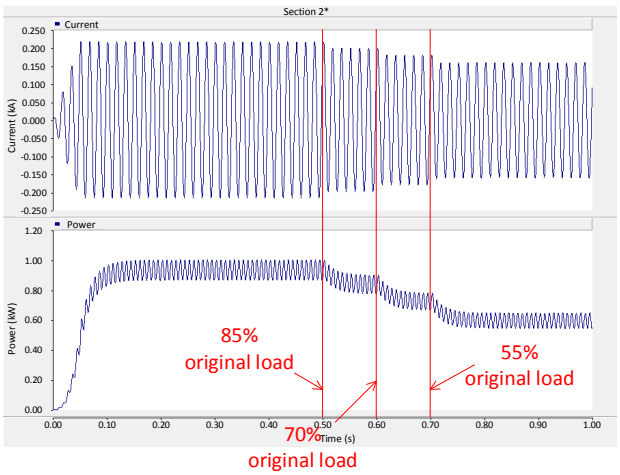
In Fig. 9, we use section_2* to denote the section which is comprised by load l_{11}, l_{12}, l_{13} and l_{14}, i.e., section_2 excludes load l_{10} and section_4, which is the most direct victim of this attack and therefore the results are more straightforward to be analyzed.

The maximum threshold on feeders in both section_2* and section_4 is set to be 250A.

The simulation result is shown in Fig. 10, in which we only present the change on the current and power, where voltage



(a) Current and power flow at section 4.



(b) Current and power flow at section 2*.

Fig. 10. Load redistribution attack simulation in *Greenbench*.

shows the same trend and is omitted.

1) **t=0.5s:** Attacker starts the attack. Before this time instance, both branches are running normally and the current remains at 210A before the attack.
2) **t=0.5s-0.7s:** Readings in section_4 increases with 15% per each 0.1 sec, while readings in section_2* decreases with the same pace.
3) **t=0.7s:** Current at section_4 reaches 253A and exceeds threshold, an overcurrent message is sent to the control center. The control center sends trip message to breaker_4, and section_4 loses power supply, as shown by Fig. 10(a).

On the other hand, as shown in Fig. 10(b), because the monitored load decreases in section_2*, less power is dispatched to this branch, and consequently the current becomes lower than it should be, which will also cause abnormal behavior of power devices in this section.

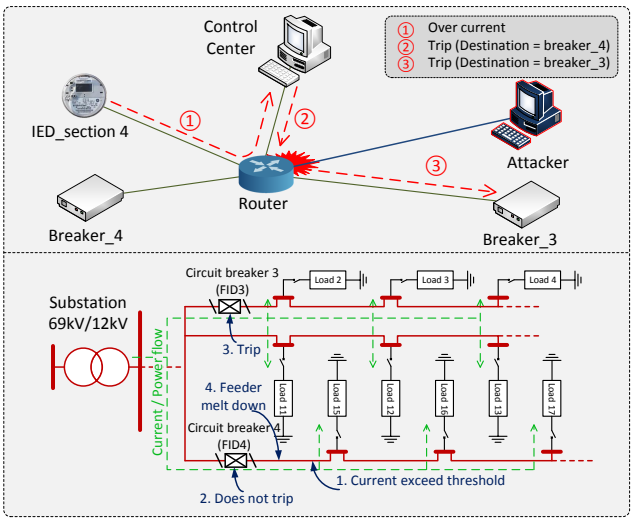
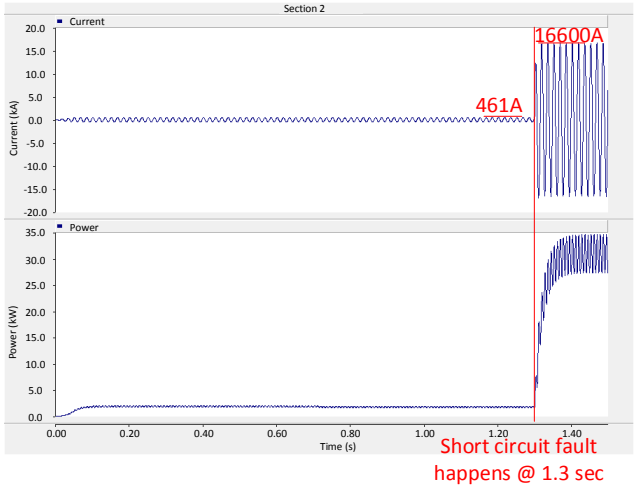


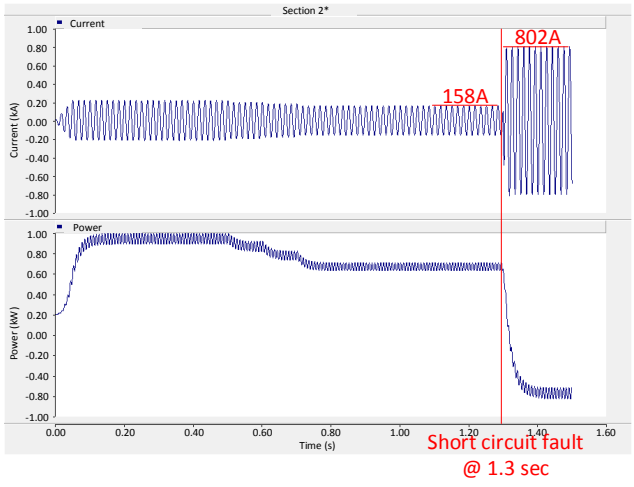
Fig. 11. LR attack and Man-in-the-middle attack.

b) Load redistribution and man-in-the-middle attack: As shown previously, composite attacks are able to cause holistic results compared with single attacks. In this case, we consider another classic cyber-attack, i.e., the Man-in-the-middle attack, and further explore the impacts of composite attacks. Specifically, we assume that at the same time the LR attack is launched, the attacker also compromises a router and applies a Man-in-the-middle attack, in which he eavesdrops messages processed by the router, locates the "trip" message sent from the control center to breaker_4, and modifies the destination of the "trip" message to breaker_3. This scenario is shown as in Fig. 11.

Fig. 12 shows the result of this scenario. Same as in the LR single attack case, the attack begins at 0.5 second, and at 0.7 second, the monitored current at section_4 exceeds 250A, and the control center sends the "trip" message to breaker_4 in order to isolate the fault. However, because the attacker also compromised the router, the "trip" message sent by the control center was redirected to breaker_3. As a direct result of the redirected message, breaker_3 trips and causes a blackout at section_3, which is shown in Fig. 12(d). On the other hand, because breaker_4 does not receive the "trip" message from the control center, the circuit breaker remains closed, which makes the feeder in section 4 run under a overcurrent situation. At time 1.3 second, 0.5 seconds after running with overcurrent, the extra heat caused by the overcurrent causes the transmission line to melt down and a line-to-ground short circuit fault happens, which results in a disastrous impact to the whole power grid. Fig. 12(b) and Fig. 12(c) show the current and power flow at section_2* and section_4, in which the current jumps more than 4 times of its normal value; and the power on both branch suddenly dropped to negative, which indicates a reverse current flow. As the summation of both section_2* and section_4, the situation in section_2 is much worse as is shown by Fig. 12(a). The current surges from 461A to 16,600A, which is more than 30 times of the normal value. Such a significant change will surely cause severe damage to all power devices that are connected in the grid, which can serve as a starting point of a larger-area cascading failure.

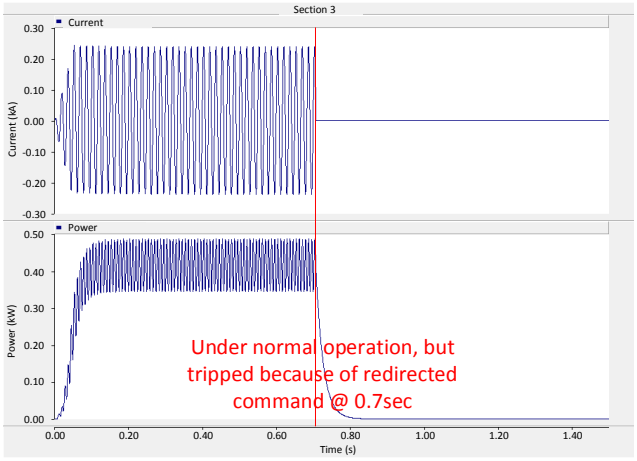


(a) Current and power flow at section 2.



(b) Current and power flow at section 2*.

(c) Current and power flow at section 4.



(d) Current and power flow at section 3.

Fig. 12. LR attack and Man-in-the-middle attack.

3) Summary: In these two *composite attack* cases, the attacker targets at the control center instead of any practical power devices, and as shown by the simulation results, the control center targeted attacks are much more destructive than those targeted on any individual power devices. This conclusion follows our commonsense, because the control center is analogous to the brain of a human being, and a damaged brain is undoubtedly more dangerous than any broken limbs. Nevertheless, our study and *Greenbench* simulation also provides insights to smart grid security study.

First, it provides quantitative results to show the significance of data-centric attacks, both control center targeted and power devices targeted. For example, as shown by the false data injection and DDoS attack, we see not only that composite attack is more destructive than single attacks, but also that the a composite attack can result in more than 10 times (in perspective of voltage collapse) in the consequence compared with single attack. With these quantitative results, we are able to compare their impact, and more wisely allocate our efforts on addressing the most imperative threats in smart grid.

Second, more practically, even though it is impractical to entirely eliminate all data-centric attacks, which serve as the ideal optimal option, we can at least greatly limit their impacts, i.e., achieve the sub-optimal option, by making it difficult for attackers to combine multiple attacks at the same time. This conclusion essentially sheds light on the necessity of a robust and secure quarantine policy on maintaining such critical infrastructures. For example, the Stuxnet [9] is a computer worm targets at the SCADA system [49], which is the control system used in power grids, and ruined many nuclear power plants in multiple countries in the world. Studies has shown that the Stuxnet worm is originally introduced in to the control system by personnel with removable devices, e.g., USB flash drives. It can be imagined that, although it is not practical to prevent attackers from exploiting vulnerabilities of the SCADA system, since it is a generally available commercial application, and developing malicious code to attack it, this disaster can be at least greatly limited if a better quarantine policy is deployed, e.g., strictly separate personal digital devices from accessing critical infrastructures. Furthermore, according to the author's working experience in the industry, it is not uncommon in practice that the usernames and passwords for multiple servers are set to be exactly the same, or with easy-to-guess patterns. This practice also greatly weakens the

security level, and exposes the system to more potential risks.

C. Evaluation of Countermeasures

In this case we evaluate and discuss one possible countermeasures regarding data-centric attacks stated above, which is the *authentication*. Authentication is a common practice in modern communication networks to guarantee the *authenticity* of the message. Authentication can be implemented in multiple means [50], and some of the most generally used methods include using cryptography, i.e., encrypt the message with a key that is only known to the message sender and the receiver, or using the message authentication code (MAC), which generates a unique value based on the message and the key shared by the sender and the receiver. Although there is no doubt that message authentication can prevent messages from being tampered by attackers, the concern here is the extra delay that is caused by running the algorithm, i.e. as we have shown in the *false data injection and DDoS attacks*, smart grid is so time-critical such that merely 7 millisecond delay is able to make significant difference in the power grid. In this case we evaluate a case which implements *data authentication*, and observe that whether authentication can benefit smart grid.

We build this case based on the *false data injection attack* that is demonstrated above, and we briefly revisit the case here. Remind that in the *false data injection attack*, the attacker compromised the meter m_{15}, and causes a fault in the system. This fault is immediately detected by the IED located on breaker_4, and reported to the control center. And the control center then sent the "trip" message to breaker_4 and isolated the fault. In that case, we did not assume any authentication is applied between the communication of the control center and the breaker_4, therefore, messages exchanged between them may be tampered by attackers who is able to intercept the message, such as by the *Man-in-the-Middle* attack. In this case, we assume data authentication is implemented on the communication between the two components, and evaluate whether the authentication delay is acceptable in smart grid.

In this case we choose to implement the Hash-based Message Authentication Code (HMAC) [51] with slight variations to facilitate our simulation. We assume that the breaker_4 and the control center share a secret key (denoted as key), and for each message to be exchanged between them (denoted as msg), they will calculate the HMAC as $H(key \oplus msg)$, where $H(\cdot)$ denotes the *hash function* [52], and we choose to use the SHA1 [50] as the implementation, which is one of the most widely adopted hash functions. The HMAC will be sent along with the original message, and the message is verified by the receiver by recalculating the HMAC based on the message and comparing with the one that was received.

In order to obtain a practical value of the algorithm running time, we conducted experiments with physical devices described as follows. We use a laptop (Intel Core i7 2.9Ghz, 4GB memory, running Ubuntu 12.04LTS) as the representation of the control center, in the meantime we use a relatively high-end (compared to current commercial devices in industry such as [53]–[55]) ARM based embedded computer (ARM9 500MHZ, 128MB memory, running tx-linux2.6.21) as the representation of the IED located on the circuit breakers.

We emulate the communication scenario stated before my letting the IED generate a message and calculate the HMAC, and send the message along with its HMAC to the control center. The control center will re-compute the HMAC to verify the authenticity of the message, and then generates another message, calculates the HMAC and sends both the message and its HMAC to the IED, and the IED will run the algorithm again to verify the message.

We choose the message length to be 240 Bytes, which is the packet size of the Modbus protocol [56], a communication standard generally used in power grids. Note that the packet size can vary for different commercial implementations, and it is not our intention to match exactly to practice, nevertheless, we argue that 240 Bytes is a reasonable size considering a message should at least contains various high-precision values such as voltage, current, phase, frequency, etc.

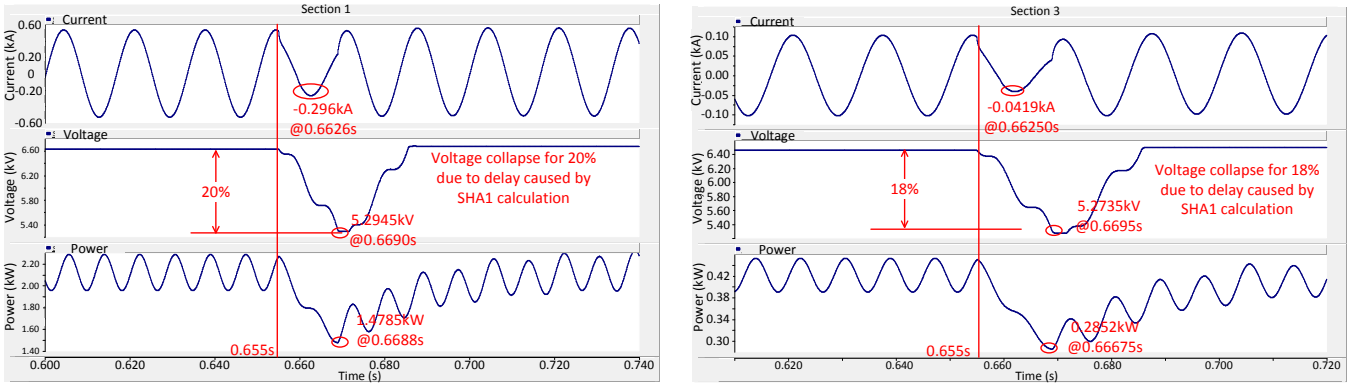
We measure the total delay from the beginning the IED generates the message, to the end when it successfully verified the message replied by the control center, which is *3.9 milliseconds* according to our experiment, and add this extra delay into the *Greenbench* simulation. We present the simulation result in Fig. 13, in which we omit the "bird-view" figures as they are very similar to those shown in Fig. 6 and Fig. 8.

From Fig. 13 we observe very interesting yet counter-intuitive results, i.e., the delay caused by the HMAC calculation can also cause very serious system instability, although slightly better than the DDoS case shown in Fig. 8. The voltage collapse for 20% and 18% percent in section_1 and section_3, which are not acceptable values as in most case the voltage variation is allowed within only 5% in practical power systems.

As a summary, in this case we evaluated a countermeasure which is generically used in Internet application to enforce message authentication, i.e., the Message Authentication Code. Ironically, the result shows that conventional cyber-attack countermeasures may not be directly used in the paradigm of smart grid, mainly because the smart grid is extraordinarily sensitive to delays. This observation suggests the necessity of smart grid specific security solutions are under high demand.

D. Extended Study: Large Scale Smart Grid

An intuitive yet non-trivial question regrading the impact of data-centric attacks lies in the scale of the power grid. In a larger scale power grid in which substations are connected to a larger grid, the same attacks may not be able to result in the same significance as they did in the Green Hub. Therefore, it is necessary to evaluate and understand the impact of data-centric attacks in a larger scale power grid. To this end, we build the IEEE 57-bus power transmission system [57] in *Greenbench*, and we pick the *jamming the price signal* attack, and the *false data injection* attack that have been evaluated on the Green Hub, as two representative cases, in order to study the impact of data-centric attacks in larger scale smart grid. Since the IEEE 57-bus is a standardized power grid models that are used in many research works, and its detailed information, such as topology and bus/line parameters, are commonly available online (such as [57]), we skip the description of this system, and directly refer to the index/name of buses and transmission lines in the following description.



(a) Section 1 Zoom-in.

(b) Section 3 Zoom-in.

Fig. 13. Authentication Delay Causes Significant Voltage Collapse during Smart Grid Emergency.

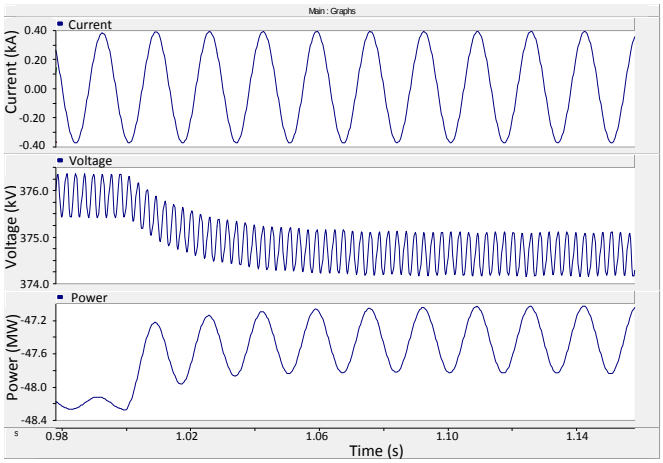


Fig. 14. Jamming attack in IEEE 57-bus system: large amount of load change does not cause noticeable distortion on any curves, in both single-domain and Greenbench simulations.

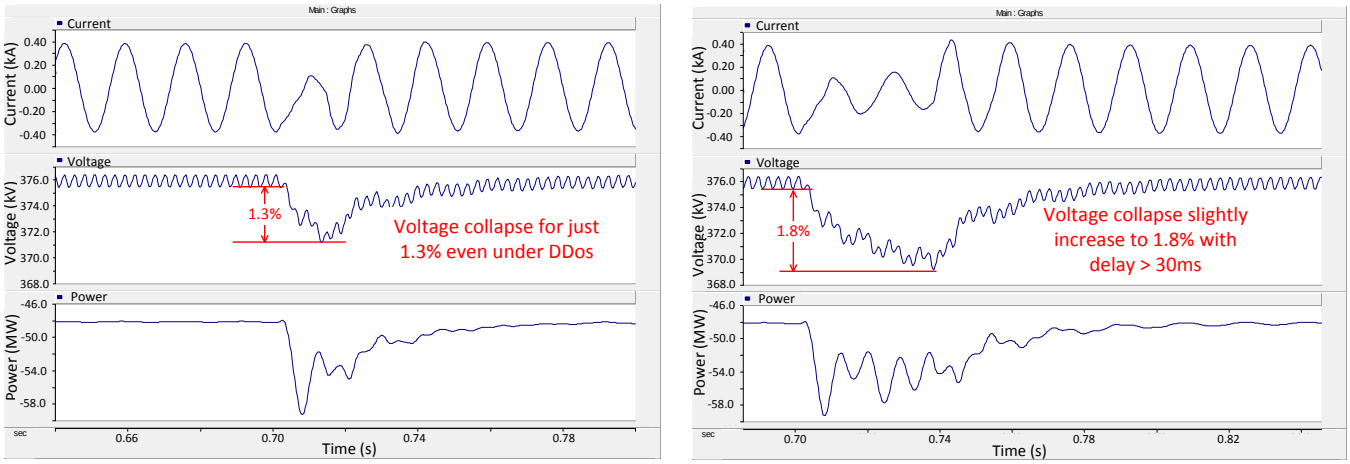
1) Jamming the Price Signal Attack: In order to make a significant load change, we pick the top 3 buses which are connected to the largest load in the system, which are *Glen Lyn*, *Clinch Rv* and *Saltville*, these 3 buses consume more than half of the power in the system (648MW/1250.8MW). We simulate this system in *Greenbench* follow the same procedure as has been conducted previously, and we present the simulation result in Fig. 14. Note that since the IEEE 57-bus system contains 57 buses and 81 transmission lines, it is nor feasible to demonstrate the change of parameters at every line or bus. Therefore, we randomly choose the transmission line between bus b_{13} and b_{14}, and present the voltage, current and power change on this line. During our simulation, we also measured other lines, which shows similar trend but only with different value, thus these results are omitted here.

Surprisingly, although the portion of load change in this case (i.e., more than 50%) is larger than that in the Green Hub case, the simulation does not show any visible distortion for current, voltage or power, with (i.e., *Greenbench* simulation) or without (i.e., single domain simulation) communication delays. As a matter of fact, The simulation result for both *Greenbench* simulation and single domain simulation are exactly the same as shown in Fig. 14, which indicates that the IEEE 57-bus system is less sensitive to large load change, and one possible reason could be this system is powered by multiple generators and thus the load change can be off-loaded by all of them, instead of the Green Hub which has only one generators.

2) False Data Injection Attack and DDoS Attack: Remind that in the previous study of the *false data injection attack*, the attacker managed to cause a overcurrent fault on a transmission line. Further, in the DDoS attack case, we demonstrated that because an extra 7 milliseconds delay is caused by this attack, the power system undergoes severe instability. We hereby simulate a similar scenario in the IEEE 57-bus system. In particular, we assume that with the same attack, the attacker causes overcurrent on the line between bus b_{23} and b_{24}, which is a randomly chosen location in the system. We first show the result with only processing and transmission delay in Fig. 15(a). We observe that a larger scale system is less sensitive to the false data injection attack. For instance, in Fig. 15(a) we can see the voltage drop is less than 1.5%. We further simulate the DDoS case in this system, and we notice that for the 7 milliseconds delay that resulted in significant voltage collapse in Green Hub, it is unable to make any visible change compared to the result of the DDoS-free case. In order to identify the resilience of this system to message delays, we manually increase the message delay in the OMNeT++, and find out that the reaction of the power system begins to generate slight changes only when the delay is larger than 30ms, and the result is shown in Fig. 15(b).

3) Summary: In this section, we studied the impact of data-centric attacks in a larger scale power system, i.e., the IEEE 57-bus system. Compared with the Green Hub, which represents a *power distribution system* with relatively lower voltage and fewer buses, the IEEE 57-bus system is a *power transmission system* that covers larger geographic area, and has much higher voltage and more buses and generators. Our *Greenbench* simulation shows that while communication delay is extraordinarily critical for the Green Hub, the IEEE 57-bus system is less sensitive to delays. This observation, however, does not indicate data-centric cyber-attacks are trivial in large-scale smart grid.

For the first reason, the power system is comprised with



(a) False Data Injection Attack in IEEE 57-Bus System.

(b) False Data Injection Attack with 30ms Delay.

Fig. 15. False data injection attack in IEEE 57-bus system: noticeable system change happens only when communication delay is larger than 30 milliseconds.

numerous small-scale distribution systems, if the attacker is able to breach multiple small-scale distribution systems, large scale system outage can still be expected. Further, as it is the distribution system which directly serves power to customers, tremendous loss can be caused if the attacker choose to attack the distribution system that contains critical loads, such as hospitals or data centers. For the second reason, in practice more serious attacks can be deployed compared to those have been showcased in this paper. For instance, we simulated a mild DDoS attack which only slightly increases communication delay at the milliseconds level, practically, however, DDoS attack can easily cause complete paralyze of the communication network.

V. Conclusion

In this paper, we studied the threats of data-centric attacks and effectiveness of cyber-attack countermeasures. We developed *Greenbench*, the cross-domain simulation benchmark to evaluate their impacts to the power grid. To leverage our understandings toward such attacks, we carry out case studies, which cover confidentiality, integrity, availability and authenticity aspects of data security, and evaluate them on *Greenbench*. Our results convey insights and instructive suggestions for solving smart grid security issues, from perspectives of both academic researches and industrial applications.

Acknowledgment

The authors would like to thank all reviewers who spend their valuable time and effort on reviewing this paper.

This work was supported by ERC Program of the National Science Foundation under Award Number EEC-0812121.

References

[1] "Cyber-attack," http://en.wikipedia.org/wiki/Cyber-attack.

[2] X. Lu, W. Wang, Z. Lu, and J. Ma, "From security to vulnerability: Data authentication undermines message delivery in smart grid," in *MILITARY COMMUNICATIONS CONFERENCE, 2011-MILCOM 2011*. IEEE, 2011, pp. 1183–1188.

[3] Z. Lu, W. Wang, and C. Wang, "From jammer to gambler: Modeling and detection of jamming attacks against time-critical traffic," in *INFOCOM, 2011 Proceedings IEEE*. IEEE, 2011, pp. 1871–1879.

[4] X. Lu, W. Wang, and J. Ma, "Authentication and integrity in the smart grid: An empirical study in substation automation systems," *International Journal of Distributed Sensor Networks*, vol. 2012, 2012.

[5] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," in *Proc. of ACM CCS*, NY, USA, 2009, pp. 21–32.

[6] G. Hug and J. A. Giampapa, "Vulnerability assessment of ac state estimation with respect to false data injection cyber-attacks," *IEEE Trans. on Smart Grid*, vol. 3, no. 3, pp. 1362–1370, 2012.

[7] S. Bi, Y. Jun *et al.*, "Graphical methods for defense against false-data injection attacks on power system state estimation," *arXiv preprint arXiv:1304.4151*, 2013.

[8] M. Rahman, H. Mohsenian-Rad *et al.*, "False data injection attacks with incomplete information against smart power grids," in *Proc. of IEEE GLOBECOM*. IEEE, 2012, pp. 3153–3158.

[9] "W32.Stuxnet Dossier," www.symantec.com.

[10] R. Langner, "Stuxnet: Dissecting a cyberwarfare weapon," *Proc. of IEEE S&P*, vol. 9, no. 3, pp. 49–51, 2011.

[11] T. M. Chen and S. Abu-Nimeh, "Lessons from stuxnet," *Computer*, vol. 44, no. 4, pp. 91–93, 2011.

[12] "NATIONAL SCADA TEST BED," http://energy.gov/oe/technology-development/energy-delivery-systems-cybersecurity/national-scada-test-bed.

[13] H. M. Merrill and F. C. Schweppe, "Bad data suppression in power system static state estimation," *Power Apparatus and Systems, IEEE Transactions on*, no. 6, pp. 2718–2725, 1971.

[14] D. Kundur, X. Feng, S. Mashayekh, S. Liu, T. Zourntos, and K. Butler-Purry, "Towards modeling the impact of cyber attacks on a smart grid," *Intl Journal of Security and Networks*, vol. 6, no. 1, pp. 2–13, 2011.

[15] F. M. Cleveland, "Cyber security issues for advanced metering infrastructure (ami)," in *Proc. of IEEE Power and Energy Society General Meeting*. IEEE, 2008, pp. 1–5.

[16] M. Wei and W. Wang, "Greenbench: A benchmark for observing power grid vulnerability under data-centric threats," in *Proc. of IEEE INFOCOM*. IEEE, 2014.

[17] "The DETER Project," http://deter-project.org/.

[18] T. Yardley, R. Berthier, D. Nicol, and W. H. Sanders, "Smart grid protocol testing through cyber-physical testbeds," in *Proc. of IEEE ISGT*. IEEE, 2013, pp. 1–6.

[19] J. Zhang and C. A. Gunter, "Application-aware secure multicast for power grid communications," *International Journal of Security and Networks*, vol. 6, no. 1, pp. 40–52, 2011.

[20] K. M. Hopkinson, K. Birman, R. Giovanini, D. Coury, X. Wang, and J. Thorp, "EPOCHS: integrated commercial off-the-shelf software for agent-based electric power and communication simulation," in *Proc. of IEEE Simulation Conference*, vol. 2. IEEE, 2003, pp. 1158–1166.

[21] K. Hopkinson, X. Wang, R. Giovanini, J. Thorp, K. Birman, and D. Coury, "Epochs: a platform for agent-based electric power and com-

munication simulation built from commercial off-the-shelf components," *IEEE Trans. on Power Systems*, vol. 21, no. 2, pp. 548–558, 2006.
[22] "Smart Grid System Testbed Facility," http://www.nist.gov/el/smartgrid/sgtf.cfm.
[23] Y. Cherdantseva and J. Hilton, "A reference model of information assurance & security," in *Availability, Reliability and Security (ARES), 2013 Eighth International Conference on*. IEEE, 2013, pp. 546–555.
[24] "PSCAD," https://hvdc.ca/pscad/.
[25] "OMNeT++," http://www.omnetpp.org/.
[26] "RTDS," http://www.rtds.com/index/index.html.
[27] H. Lin, S. Sambamoorthy, S. Shukla, J. Thorp, and L. Mili, "Power system and communication network co-simulation for smart grid applications," in *Proc. of IEEE ISGT*. IEEE, 2011, pp. 1–6.
[28] H. Hooshyar, "System protection for high pv-penetrated residential distribution systems (green hubs)." 2011.
[29] "Power Systems Test Case Archive," https://www.ee.washington.edu/research/pstca/.
[30] "Solid State Transformer," http://www.freedm.ncsu.edu/index.php?s=2&t=news&p=121.
[31] "Fault Isolation Device," http://www.freedm.ncsu.edu/index.php?s=2&t=news&p=84.
[32] S. McLaughlin, D. Podkuiko, and P. McDaniel, "Energy theft in the advanced metering infrastructure," in *Critical Information Infrastructures Security*. Springer, 2010, pp. 176–187.
[33] H. Li and Z. Han, "Manipulating the electricity power market via jamming the price signaling in smart grid," in *Proc. of IEEE GlobeCom Workshops*. IEEE, 2011, pp. 1168–1172.
[34] C. Efthymiou and G. Kalogridis, "Smart grid privacy via anonymization of smart metering data," in *Proc. of IEEE SmartGridComm*. IEEE, 2010, pp. 238–243.
[35] G. Kalogridis, M. Sooriyabandara, Z. Fan, M. Mustafa *et al.*, "Toward unified security and privacy protection for smart meter networks," *Systems Journal, IEEE*, vol. 8, no. 2, pp. 641–654, 2014.
[36] G. Kalogridis and S. Dave, "Pehems: Privacy enabled hems and load balancing prototype," in *Smart Grid Communications (SmartGridComm), 2012 IEEE Third International Conference on*. IEEE, 2012, pp. 486–491.
[37] A.-H. Mohsenian-Rad and A. Leon-Garcia, "Distributed internet-based load altering attacks against smart power grids," *IEEE Trans. on Smart Grid*, vol. 2, no. 4, pp. 667–674, 2011.
[38] S. E. McLaughlin, D. Podkuiko, A. Delozier, S. Miadzvezhanka, and P. McDaniel, "Embedded firmware diversity for smart electric meters." in *HotSec*, 2010.
[39] R. Muraleedharan and L. A. Osadciw, "Jamming attack detection and countermeasures in wireless sensor network using ant system," in *Defense and Security Symposium*. International Society for Optics and Photonics, 2006, pp. 62 480G–62 480G.
[40] C. Zhao, U. Topcu, and S. H. Low, "Frequency-based load control in power systems," in *American Control Conference (ACC), 2012*. IEEE, 2012, pp. 4423–4430.
[41] A. Molina-García, F. Bouffard, and D. S. Kirschen, "Decentralized demand-side contribution to primary frequency control," *Power Systems, IEEE Transactions on*, vol. 26, no. 1, pp. 411–419, 2011.
[42] "Harmonic Distortion in the Electric Supply System." in *INTEGRAL Energy, Technical Note No.3*, 2000.
[43] I. . W. Group *et al.*, "Wireless lan medium access control (mac) and physical layer (phy) specifications," 2012.
[44] J. Chen and A. Abur, "Placement of pmus to enable bad data detection in state estimation," *Power Systems, IEEE Transactions on*, vol. 21, no. 4, pp. 1608–1615, 2006.
[45] "U.S. - canada power system outage task force: Final report on the implementation of task force recommendations," energy.gov/oe/downloads.
[46] International Electrotechnical Commission, "Communication networks and systems for power utility automation: Basic communication structure Distributed energy resources logical nodes," *IEC International Standard IEC 61850 Part 7-420*, Mar 2009.
[47] IEC Standard, "IEC 61850: Communication networks and systems in substations," 2003.
[48] Y. Yuan, Z. Li, and K. Ren, "Modeling load redistribution attacks in power systems," *IEEE Trans. on Smart Grid*, vol. 2, no. 2, pp. 382–390, 2011.
[49] "SCADA," http://en.wikipedia.org/wiki/SCADA.
[50] C. Kaufman, R. Perlman, and M. Speciner, *Network security: private communication in a public world*. Prentice Hall Press, 2002.
[51] H. Krawczyk, R. Canetti, and M. Bellare, "Hmac: Keyed-hashing for message authentication," 1997.
[52] "Hash Function," https://en.wikipedia.org/wiki/Hash_function.
[53] "DPU2000R Distribution Protection Unit," www08.abb.com.
[54] "Bitronics M87x Family H11 Host Processor," www.novatechweb.com.
[55] "AQ L350 Line protection IED ," www.arcteq.fi.
[56] "MODBUS," http://en.wikipedia.org/wiki/Modbus.
[57] "57 Bus Power Flow Test Case," http://www.ee.washington.edu/research/pstca/pf57/pg_tca57bus.htm.