Safety Can Be Dangerous: Secure Communications Impair Smart Grid Stability Under Emergencies

Mingkui Wei
Department of Electrical and Computer Engineering
North Carolina State University
Raleigh, NC, 27606

Wenye Wang
Department of Electrical and Computer Engineering
North Carolina State University
Raleigh, NC, 27606

***Abstract*—Smart grid features real-time monitoring and control by integrating advanced communication networks into traditional power grids. This integration, however, makes smart grid vulnerable to cyber attacks, i.e., the anomalies caused by attackers in the communication network can affect ordinary operations of the power grid and result in severe physical damage. To protect smart grid from cyber attacks, many traditional countermeasures, such as message encryption, have been proposed to be directly migrated to fit this system. In this regard, the very first fundamental questions that need to be addressed are *how to evaluate and compare the physical impacts of cyber attacks and countermeasures, and whether traditional cyber security countermeasures can result in satisfactory performance in smart grid*. Motivated by these questions, we establish a small-scale smart grid prototype, and use both experiments and cross-domain simulations to evaluate and compare the reaction of the power system under cyber attacks, with and without the presence of traditional countermeasures. Our study reveals that traditional countermeasures can not be readily migrated to protect smart grid in particular, and shows that during system emergencies where prompt system reactions are critical, the extra latency caused by message encryption and decryption can result in more than 10 times in the magnitude of voltage collapse. Our work indicates that traditional countermeasures may not fit smart grid, the newly emerging cyber-physical system, which has strict time constraint. Therefore it is essential for researchers to seek solutions to address smart grid specific security threats.**

I. Introduction

Smart grid, i.e., the communication assisted power grid, has been undergone intensive study in the recent decade. By integrating advanced communication networks into traditional power grids, various power devices, which were unable or with very limited capacity to communicate, are granted with full capability to communicate with their peers. And as a result of the real-time information exchange, the smart grid is expected to manage power distribution more wisely, and react to emergencies more promptly and accurately, and therefore facilitates a more reliable and stable power system.

Despite all benefits that smart grid can bring, however, there is one concern that attracts even more attention, which are the threats caused by cyber attacks [1], [2]. By taking advantage of the integration of the cyber and the physical systems, cyber attacks, once a concern limited only in the cyber world, e.g., Internet, are now able to escalate their targets from ruining data and information to dismantling physical infrastructures.

We all witnessed in recent years that how can cyber threats hinder or even degenerate the evolution of traditional power systems to smart grid, from both academic researches and industrial applications: the false data injection attack identified in [2] points out that attackers are able to modify monitored data in smart grid without being detected by the system; smart meters, which are intend to provide fine-grained system monitoring and enhance system stability, are rejected in various regions all over the world [3], [4], because they tend to leak uses' private information; and the Stuxnet [5], a computer worm targets at the SCADA system [6], the control system widely used in power systems, infected and ruined unclear plants in many countries.

Being aware of the threats, a lot of researchers are motivated to explore feasible solutions, i.e., countermeasures, to protect smart grid from various cyber attacks [2], [7]–[14]. However, we noticed that there are very few works which thoroughly considered the validity of these countermeasures. Particularly, although most countermeasures are theoretically feasible, and may even have been proven effective in many other fields, it still remains unclear that *how to evaluate and compare the physical impacts of cyber attacks and countermeasures, and whether traditional cyber security countermeasures can result in satisfactory performance for smart grid in particular*. We believe these are important questions because their answers provide a standpoint which allows us to observe the cyber attacks and their countermeasures in a negative perspective, i.e., what are the negative impacts can be caused by a countermeasure and how they are compared to the cyber attacks themselves, and therefore gain a more comprehensive understanding of the cyber security issues in smart grid.

In this paper, we are motivated to explore these questions with case studies. In particular, we consider the cryptography, i.e., encrypting messages to enhance security, which is a well accepted countermeasure against various cyber attacks and has been proposed in smart grid communication standard [7], and evaluate its feasibility in smart grid communication. To conduct the evaluation, we exploit *Greenbench*, a cross-domain simulation benchmark developed in our previous work [15], and run simulation with data that is obtained by experiments with physical devices. Our study reveals a dilemma in the study of cyber attacks and countermeasures in smart grid, and demonstrates that although the cleartext communication is susceptible to cyber attacks and thus endangers smart grid,

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

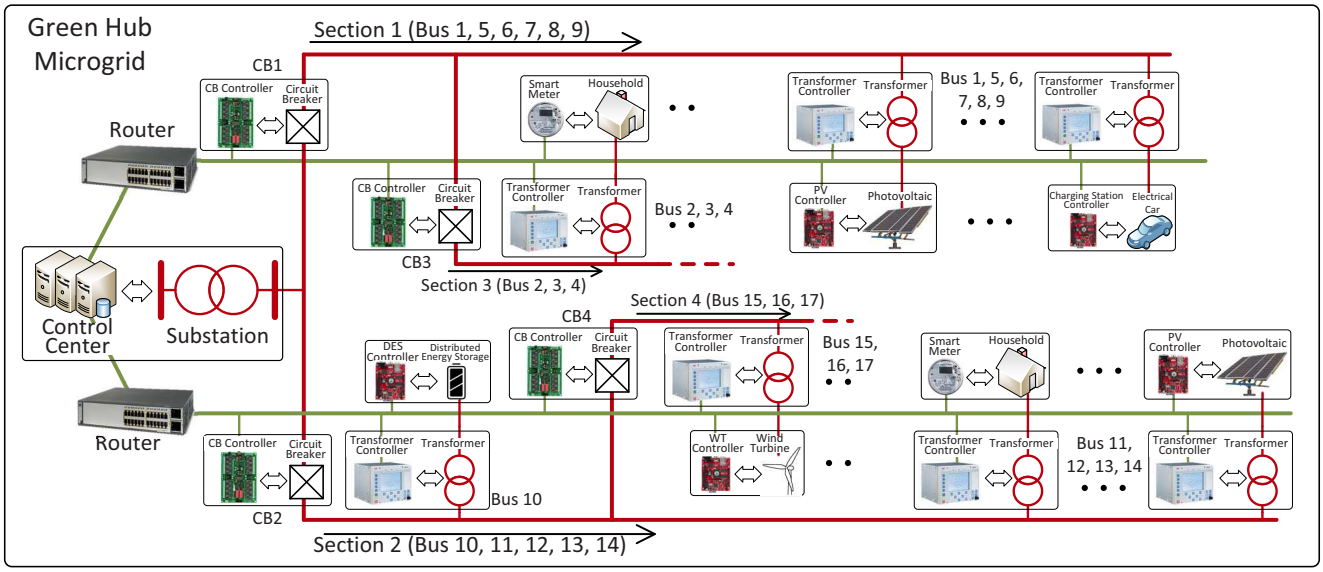


Fig. 1: Green Hub Implementation.

cryptography, however, brings non-trivial trade-off which can even exacerbate the consequence of cyber attacks.

The following of this paper is organized as follows: In section II we introduce background of our work, i.e., *Greenbench* and the Green Hub which are used in our study; in section III we describe in detail of our experiment and simulation, result and analysis; and in section IV we conclude our work.

II. Background

In this section we briefly introduce *Greenbench*, the cross-domain simulation benchmark for cyber attack evaluation in smart grid, and the Green Hub, a 17-bus smart grid model built in *Greenbench*. The implementation details for both can be found in [15].

A. Greenbench: the cross domain simulation benchmark for smart grid security evaluation

Greenbench is a cross-domain simulation platform which is built for smart grid cyber security evaluation in particular. It is comprised of two counterpart simulators, the PSCAD [16] for power system simulation, and the OMNeT++ [17] for communication networks simulation. *Greenbench* provides a well designed synchronization mechanism such that these two simulators are able to simulate in their own domain, and meanwhile exchange simulation data in real-time.

B. Green Hub: the micro smart grid

The Green Hub system is a novel distribution level microgrid which has been developed by the Future Renewable Electric Energy Delivery and Management (FREEDM) systems center in North Carolina State University for smart grid study. The Green Hub is abstracted from an actual residential distribution system in the Raleigh area where the FREEDM center locates, meanwhile its traditional power devices are replaced by various innovative ones which are developed in the FREEDM center, e.g. the Solid State Transformer (SST) and the Fault Isolation Devices (FIDs). It is also equipped with green energy resources such as the Photovoltaic (PV) and Wind Turbine (WT). In order to implement real-time system control and monitor, all devices are equipped with Intelligent Electronic Devices (IEDs), which are ARM-based embedded computers that can communicate using various technologies (e.g., WiFi, Ethernet, Zigbee) and conduct computation and make decisions locally. We model the Green Hub, which is shown in Fig. 1, in *Greenbench* such that we are able to study and observe the impact of cyber attacks in smart grid.

III. Cyber Attack and Countermeasure Evaluation

Cleartext communications suffer from many aspects and therefore are not a desired option for information exchange in critical infrastructures. For example, an attacker can tap the communication network and overhear the information exchanged among hosts, or he can even modify messages or impersonate other hosts in this network, and cause unexpected system behavior. For smart grid in particular, cleartext can leak users' private information [8] and give attackers opportunity to exploit for more sophisticated attacks [2], [10]. The risk of cleartext communication can be largely reduced by adopting cryptography [18], i.e., encrypting the messages to be sent, which has been adopted and proven an very effective solution in various applications. Based on this reason, cryptography is also proposed for smart grid communication to protect it from cyber attacks [7]. Despite its effectiveness in protecting information secrecy, however, a concern need to be justified is whether traditional encryption algorithm (such as the AES [7]) fits smart grid application. This concern is drawn based on two facts. First, different from many applications, smart grid communication is time-critical [19] and milliseconds delay can result in distinct consequences during system emergency. Second, encryption algorithms are computation intensive and therefore prolongs communication delay. As a result, although cryptography can undoubtedly enhance system security,

whether its benefit outperforms the negative impact, i.e., longer communication delays, need to be evaluated and justified.

In this section, we use both experiments and cross-domain simulations to compare the performance of the power system under emergencies, with both cleartext and cyphertext (encrypted text) communication. This section is composed by two scenarios, both of them have the same initial assumption that attackers have managed to cause local emergencies that need the control center's prompt reaction, and the difference between the two scenarios is that cleartext and cphyertext are used in the communication networks, respectively.

A. Cyber attack under cleartext communication

This scenario is begun with the assumption that the attacker has managed to compromise a local load and its controller (smart meter), which can be implemented by many means identified in recent studies [2], [8], or the attacker can be the owner of the load himself and intends to sabotage the power system. We further assume the attacker compromised a router, and is able to freely read and modify the packets exchanged through this router [20], because all messages in this scenario are sent with cleartext.

We present the attack procedure in Fig. 2, and provide detailed description in the following.

1) The attacker obtained control of of a local load and its controller (smart meters), which is load 15 as shown in Fig. 2, and is able to modify the reading of the smart meter without being detected by the control center. Through the smart meter, the attacker manipulates local load and keeps increasing the power consumption at this area; in the meantime, the attacker forges meter readings and sends the fake data to the control center, which makes it unaware of the power consumption increase.
2) The current at this area increases along with the increased power consumption without being controlled by the control center, and exceeds a threshold. This event should have triggered the overcurrent protection, such as the control center sends commands and trips a circuit breaker to isolate the failure, however, because the control center is deceived by incorrect information, it fails to make correct decision.
3) Because the overcurrent event is not handled correctly by the deceived control center, eventually a failure is caused on the transmission line by the overcurrent. This failure propagates along the transmission lines and is detected by a higher level protection device which is not compromised by the attacker, i.e., the IED 4.
4) IED 4 sends this event to the control center. On receiving this event, the control center makes decision and sends back a "trip" message to circuit breaker 4, in order to isolate the failure. However, the attacker identifies this trip message on the compromised router, and modified the destination of this packet from IED 4 to IED 3. As the results of this cyber attack, section 3 loses power supply completely because IED 3 receives trip message and opens circuit breaker 3, and the failure in section 4 is failed to be isolated.
5) The fault on load 15 further propagates along the power grid and may cause even more damage to other devices in the power system.

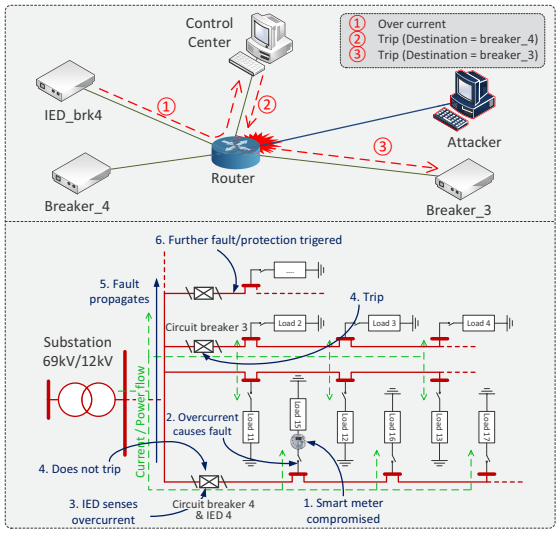


Fig. 2: Cyber attack under cleartext communication.

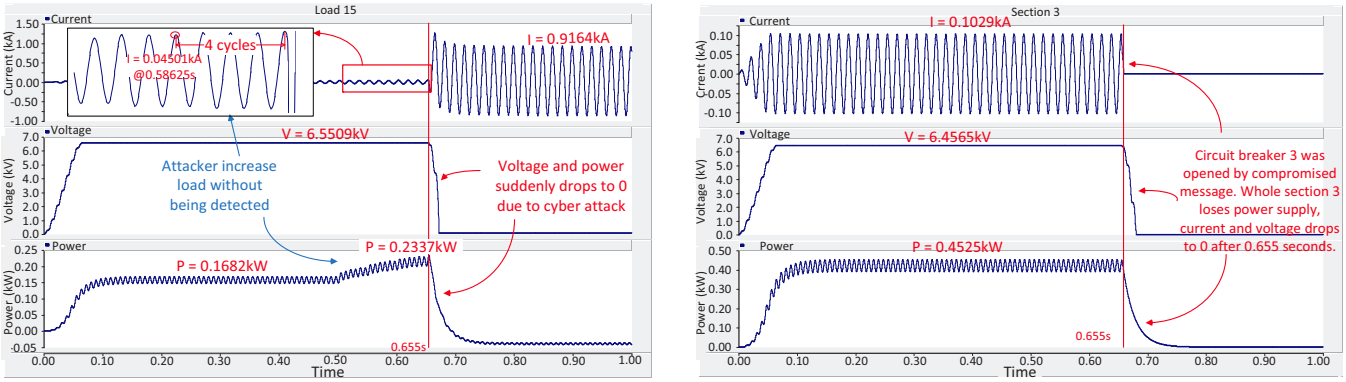
In Fig. 3 we present the simulation result for section 3, and load 15, results on other sections follow the similar character and therefore are omitted. The attacker begins to increase load 15 at t=0.5s, and as shown in Fig. 3a, the current exceeds 45A (the preset overcurrent threshold) at t=0.58625s. At t=0.655s, after about 4 cycles the current exceeds threshold for the first time, a short circuit fault is caused. The current at load 15 suddenly jumps to more than 20 times of its normal value, meanwhile the voltage drops to 0 in a few milliseconds, which may cause significant damage to connected devices. And as shown in Fig. 3b for section 3, power supply is cut off at t=0.655s because the circuit breaker 3 is opened then.

B. Cyber attack with cyphertext communication

Previous case explicitly demonstrates that smart grid with cleartext is susceptible to cyber attacks, i.e., cleartext makes attackers easily identify useful information and exploit benefit based on which. In order to protect the secrecy of critical information in smart grid, cryptography is proposed to be used in smart grid communication [7], as it has been proven effective in many other fields. However, every countermeasure will bring certain sacrifice, and as stated before, before any cryptography algorithm is to be implemented, it is necessary to evaluate and compare its benefits and the trade-offs.

In this section we take the same initial assumption as previous case, but assume the communication is based on cyphertext. By making this assumption, we are motivated to evaluate the trade-offs brought by cryptography, and explore whether traditional cryptography fits smart grid application.

1) Communication Scenario: In order to easily compare the results, we make the same assumption as in previous case, i.e., the attacker compromised load 15 and its smart meter. However, in this case we assume all messages exchanged between IEDs and the control center are encrypted, such that even the attacker compromised the router, he is unable to obtain any useful information, the main step of attacks in this case is provided in Fig. 4. While the benefit brought by encryption is obvious, it remains obscure whether it can justify itself and outperforms its trade-off, i.e., extra delay sacrificed



(a) Load 15 under attack.

(b) Section 3 was shutdown due to attack.

Fig. 3: System performance with cleartext communication.

by running encryption and decryption algorithms. We explore this question in the following.

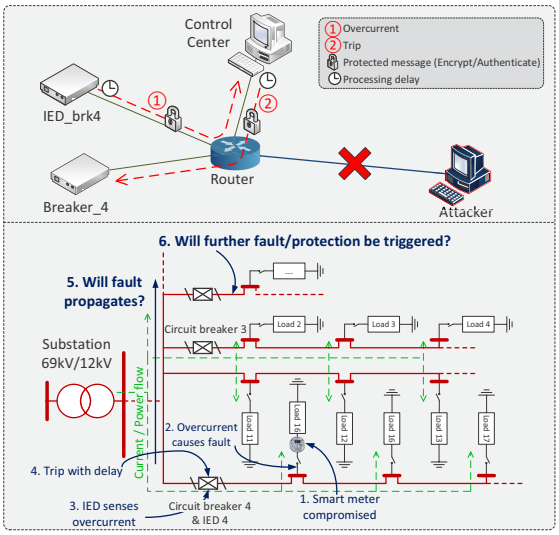


Fig. 4: Cyber attack with encrypted communication.

2) Methodology: One critical step in this evaluation is to obtain practical statistics about the delay caused by encryption/decryption algorithm, and we tackle this task with experiments. In particular, we set up a real communication network comprising the control center and IEDs, which are emulated by powerful laptop computer and ARM-based embedded computers, respectively. We have encryption/decryption algorithm

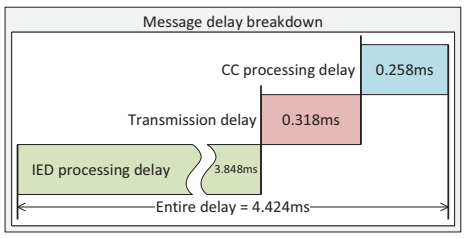


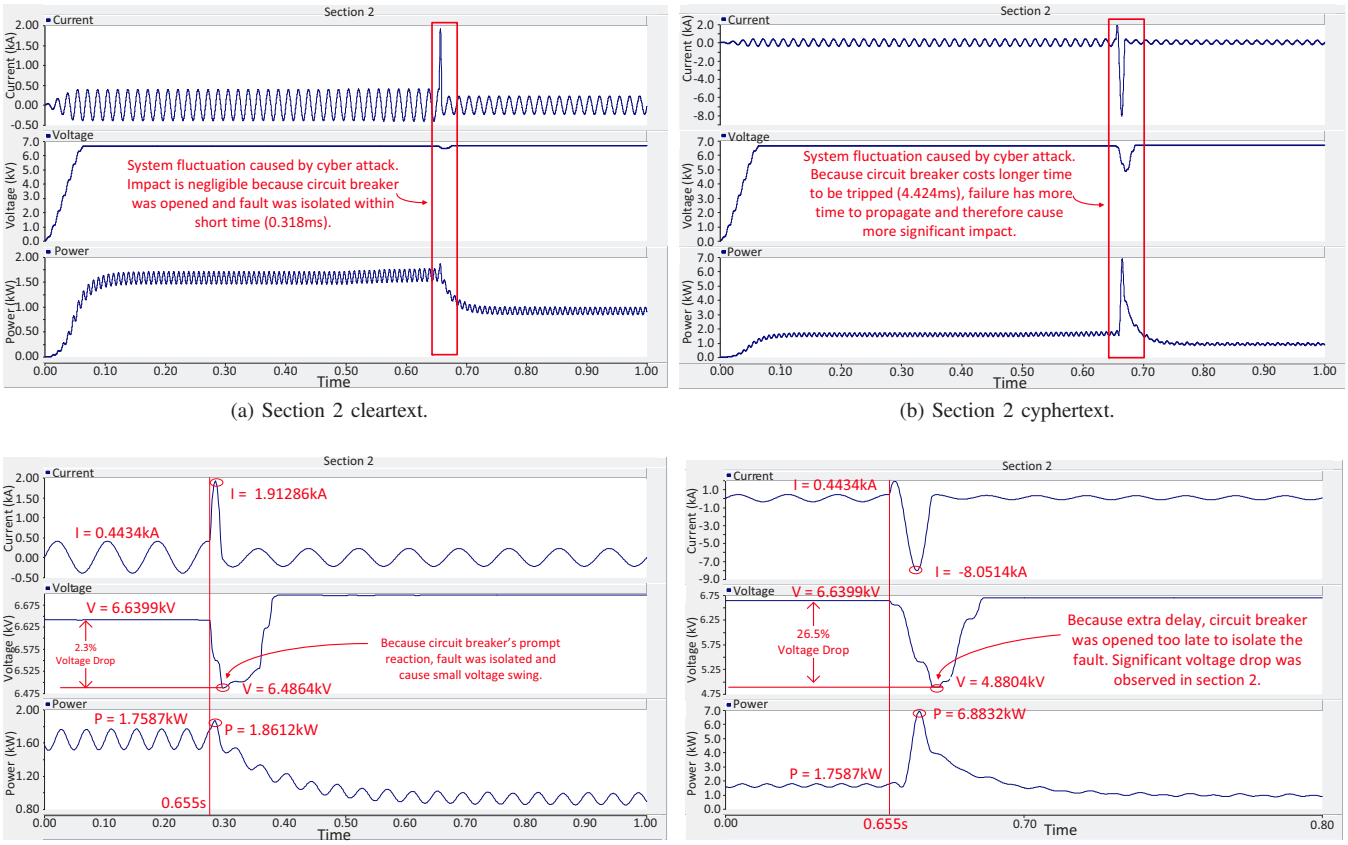
Fig. 5: Encrypted message transmission delay.

run on both hosts to implement the cypertext communication, and measure the delay caused by this process. We then use this delay as a parameter and import it into *Greenbench* simulation, and observe the consequence accordingly. In the following we provide the specifications for our experiment.

- Encryption/decryption algorithm: We choose the Advanced Encryption Standard (AES) [21] in our case study as which is recommended as the cryptography algorithm in IEC62351 standard [7] and also one of the most widely used symmetric-key algorithm. The AES algorithm has many implementations, and in this work we adopted the *mbed TLS* (formaly known as PolarSSL) [22], which is an open source SSL library and optimized for embedded products. For block cipher mode, we choose Cipher Feedback (CFB) [23] which provides a good balance between security level and encoding convenience (e.g., no padding needed).

- Message size: By message size we refer the size of the payload that is going to be encrypted, which excludes overheads such as headers added by each layer. In real system the size of messages may vary according to specific event, and the content and format of each message may subject to the definition of particular manufactures. To make it general and demonstrative, in this case study we assume the message is fixed, and whose size is 240 bytes. 240 bytes is the maximum packet size allowed for Modbus [24] Remote Terminal Unit (RTU) [25], which is a typical IED in distributed control system in power grid for system monitoring [26], and we assume the maximum value as a representation of the "worst case scenario". Furthermore, the 240 bytes assumption can also be justified by considering the content of a message: a typical message should includes exact time stamp, ranging from year to millisecond, and monitored values such as current, voltage, phase, frequency, and thus the summation of which can even exceed one packet limit.

- Hardware specifications: The detailed specifications of the control center and IEDs are listed in Tab. I. The IED chosen in our study is the one that has been widely adopted in the FREEDM center, and a industry survey also reveals that its CPU frequency (500MHz) is among the top-level in currently deployed IEDs [27]–[29]. Another reason we choose an ARM-based embedded computer instead of ASIC or FPGA, which can be designed dedicatedly for cryptography



(a) Section 2 cleartext.

(b) Section 2 cyphertext.

(c) Section 2 cleartext.

(d) Section 2 cyphertext.

Fig. 6: System performance: cleartext vs. cyphertext communication.

computation and thus provides shorter delay, is because to our best knowledge, we do not realize any such implementation on currently available products in the market during our survey.

• Communication protocol: We assume the message is carried by Ethernet, which is based on the fact that many traditional communication protocols in power systems, such as the Modbus and Distributed Network Protocol (DNP) [30] and now being migrated over serial link to Ethernet to implement remote control. And we choose the UDP/IP protocol, because the ACK mechanism in TCP increases delay, which is undesirable under emergencies.

Device	CPU	Memory	System Version
IED	ARM9 500MHz	128MB	ts-linux 2.6.21
Control Center	CORE i7 2.9GHz	4GB	ubuntu 12.04 LTS

TABLE I: Device specifications.

We use the following scenario to emulate the bi-directional cyphertext communication between the control center and IEDs:

1) A message with size 240 bytes is generated on an IED, which is encrypted with AES algorithm specified above, and the encrypted message is sent to the control center via UDP/IP.
2) The control center receives the encrypted message and decrypt it. Then the control center generates another message with the same size, encrypts and sends it back to the IED.
3) The IED receives the encrypted message and decrypt it, which finishes one communication event.

We run the experiment for 5000 times, and for each time we record the processing time on the control center and IEDs, and the propagation delay between the two. The measured delays are shown in Fig. 5.

From Fig. 5 we see that the cryptography algorithm operation on ARM board takes more than 80% of the entire procedure. This result is significant but *not surprising*, considering the IED is an embedded system which is not specifically optimized for encryption/decryption computation. However, this observation leads to more interesting yet non-intuitive questions, i.e., how will this delay impact the power system performance during the fault management procedure? And is this impact better or worse compared with cleartext-but-insecure communication?

In the following we integrate the data obtained from the experiment into *Greenbench* and explore the answers.

3) Simulation Setup and Results: Our goal in this case is to identify the impact caused by the extra delay as a result of the encryption/decryption operation. Therefore, in this case we

simulation two scenarios and make them as comparisons. In particular, in the first scenario, we still consider the cleartext communication, but the transmission delay (0.318ms) is considered, and in the second scenario, we consider the cphyertext communication, where the message delay is the summation of transmission delay and processing (encryption and decryption) delay. Also remind that the initial failure is unchanged in this case (both scenarios), that the attacker increase load and trigger a failure at t=0.655s, but different from the first case, we assume the attacker does not tamper any message even in the cleartext scenario.

We provide the simulation result in Fig. 6, in which we compare the result caused to section 2 of the Green Hub by the transmission delay only (Fig. 6a and Fig. 6c) and by the summation of both transmission and processing delay (Fig. 6b and Fig.6d). We choose to display the result on section 2 is because section 2 is adjacent to section 4 where load 15 locates and therefore delivers the most demonstrative result.

We are able to observe a significant difference between the two scenarios from Fig. 6. In the cleartext scenario, circuit breaker 4 is tripped only after the transmission delay (0.318ms) after the failure is detected, which leaves little time for the failure to propagate and affect other sections in the same system. On the other hand, when the processing delay is integrated into this procedure, which essentially makes the entire delay 4.424ms, we observe non-trivial impacts caused by this failure. The difference is obvious enough to be identified by comparing Fig. 6b to Fig. 6a, in which current, voltage and power all show significant distortion. Closer inspections are provided in Fig. 6c and Fig. 6d, which numerically express the difference. For instance, the voltage collapse is 2.3% under cleartext communication, but boosts to 26.5% in cphyertext communication scenario, such a significant voltage collapse will further trigger undervoltage protection and cause section 2 to be disconnected from main power grid [31].

In this case it is to our surprise to observe that how vast distinction a relatively short delay can cause when the smart grid is under emergency. Moreover, this result provides insights to the study of smart grid security study, and suggests that there are many practical issues toward making smart grid secure, and the implementation of which is a compromise of various tread-offs. For the cases studied here in particular, we show that while cryptography can undoubtedly enhance the security level of smart grid, it increase devices' reaction time and endangers the system stability under emergencies, where latency is a more critical factor than secrecy.

IV. Conclusion

In this paper we studied the impacts caused by cyber attacks and their countermeasures in smart grid. With both experiments and cross-domain simulations, we reveal a dilemma in the security study of smart grid: although cyber attacks will undoubtedly damage smart grid, their countermeasures may also introduce non-trivial negative impacts and even result in worse consequences. Our study essentially suggests that there are still many practical concerns need to be addressed towards a secure smart grid, and judicious decisions are critical to balance various trade-offs during the implementation of a secure smart grid.

References

[1] Z. Lu, W. Wang, and C. Wang, "From jammer to gambler: Modeling and detection of jamming attacks against time-critical traffic," in *Proc. IEEE INFOCOM*. IEEE, 2011.

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

[3] "Palo Alto Municipal Utility District Rejects Smart Meters," stopsmartmeters.org.

[4] "Will Germany Reject Smart Meters?" renewableenergyworld.com.

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

[6] "SCADA," en.wikipedia.org/wiki/SCADA.

[7] International Electrotechnical Commission, "Power systems management and associated information exchange Data and communications security," *IEC International Standard IEC 62351*, 2007.

[8] S. McLaughlin, D. Podkuiko, and P. McDaniel, "Energy theft in the advanced metering infrastructure," in *Critical Information Infrastructures Security*. Springer, 2010, pp. 176–187.

[9] A. AlMajali, A. Viswanathan, and C. Neuman, "Analyzing resiliency of the smart grid communication architectures under cyber attack," in *5th Workshop on Cyber Security Experimentation and Test*, 2012.

[10] D. Kundur, X. Feng, S. Mashayekh, S. Liu, T. Zourntos, and K. L. Butler-Purry, "Towards modelling the impact of cyber attacks on a smart grid," *IEEE IJSN*, vol. 6, no. 1, pp. 2–13, 2011.

[11] D. Watts, "Security and vulnerability in electric power systems," in *35th North American power symposium*, vol. 2, 2003, pp. 559–566.

[12] O. Kosut, L. Jia, R. J. Thomas, and L. Tong, "Malicious data attacks on smart grid state estimation: Attack strategies and countermeasures," in *Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on*, 4-6 Oct. 2010, pp. 220–225.

[13] X. Lu, W. Wang, J. Ma, and L. Sun, "Domino of the smart grid: An empirical study of system behaviors in the interdependent network architecture," in *Smart Grid Communications (SmartGridComm), 2013 IEEE International Conference on*. IEEE, 2013, pp. 612–617.

[14] M. Wei and W. Wang, "Combat the disaster: Communications in smart grid alleviate cascading failures," in *High-capacity Optical Networks and Emerging/Enabling Technologies (HONET), 2014 11th Annual*. IEEE, 2014, pp. 133–137.

[15] ——, "Greenbench: A benchmark for observing power grid vulnerability under data-centric threats," in *INFOCOM, IEEE Proceedings*, 2014.

[16] "PSCAD - Manitoba HVDC Research Centre," hvdc.ca/pscad/.

[17] "OMNeT++," www.omnetpp.org/.

[18] C. Kaufman, R. Perlman, and M. Speciner, *Network security: private communication in a public world*. Prentice Hall Press, 2002.

[19] IEC Standard, "IEC 61850: Communication networks and systems in substations," 2003.

[20] "Electricity Grid in U.S. Penetrated By Spies," online.wsj.com/news/articles/SB123914805204099085.

[21] N. Aes, "Advanced encryption standard," *Federal Information Processing Standard, FIPS-197*, vol. 12, 2001.

[22] "POLARSSL," tls.mbed.org/.

[23] "Block cipher mode of operation," en.wikipedia.org/.

[24] "Modbus," en.wikipedia.org/wiki/Modbus.

[25] "Remote Terminal Unit," en.wikipedia.org/.

[26] "Power system automation," en.wikipedia.org/.

[27] "DPU2000R Distribution Protection Unit," www08.abb.com.

[28] "Bitronics M87x Family H11 Host Processor," www.novatechweb.com.

[29] "AQ L350 Line protection IED ," www.arcteq.fi.

[30] "DNP3," en.wikipedia.org/wiki/DNP3.

[31] U.S.-Canada Power System Outage Task Force, "Final report on the august 14, 2003 blackout in the united states and canada: Causes and recommendations," 2004.