An Active Command Mediation Approach for Securing Remote Control Interface of Substations

Daisuke Mashima
Advanced Digital Sciences Center
Singapore
daisuke.m@adsc.com.sg

Prageeth Gunathilaka
Advanced Digital Sciences Center
Singapore
prageeth.g@adsc.com.sg

Binbin Chen
Advanced Digital Sciences Center
Singapore
binbin.chen@adsc.com.sg

Abstract—Electrical substation is a crucial component in power grids. A number of international standards, such as IEC 60870 and 61850, have emerged to digitize and automate substations for efficient and timely control. However, owing to insufficient security consideration and implementation, the resulting systems could be vulnerable to cyber attacks. In fact, the digitization and automation of a large number of connected substations can dramatically increase the scale of potential damage on power grids. In this paper, we focus on attacks that inject malicious remote control commands targeting substations and discuss a practical, standards-based design of an active command mediation mechanism deployed in each substation to offer an additional layer of defense against attacks that somehow bypass other cyber security measures. Furthermore, as a concrete example of mitigation mechanism implemented on the command mediation system, we discuss autonomous command-delaying and evaluate its effectiveness. The simulation results show that our approach can significantly reduce the attack impact on power grid stability.

I. INTRODUCTION

In order to keep our lights on, electricity from generators needs to be reliably transformed through different voltage levels for efficient delivery to end consumers. Such voltage transformation operations are usually carried out in substations. Besides, substations enable intelligent switching operations to facilitate automatic fault response and optimize power grid operations. Depending on the size of service, there can be hundreds or thousands of substations, and within each substation, there can be many kinds of physical components, such as transformers, circuit breakers, shunt reactors, and so forth. For example, in Singapore, there are over 10,000 transmission/distribution substations under a single utility company [1].

The power industry has put in significant efforts to manage substations. In particular, standard technologies, including IEC 60870 and IEC 61850, have been established for substation remote control and automation, and the number of substations that employ these technologies has increased significantly over the years. However, coming with such modernization is the increased risk of cyber attacks that could subvert power grid services. For instance, by exploiting the remote control interface, attackers can manipulate a large number of circuit breakers to cause blackout and/or critical instability such as voltage drop. Such attacks could be mounted either via network or from the control center. The former could be made possible owing to insufficient security implementation for communication channels between the control center and substations, which may be vulnerable to man-in-the-middle attacks and replay attacks [10], [13]. The latter could be performed by disgruntled insiders, malwares, or cyber/physical intruders at the control center. A major incident in this category recently occurred in Ukraine [20], where the control center system was hacked and manipulated remotely to issue a large number of circuit breaker open commands, making 30 substations offline for hours.

In general, the security risk associated with substation remote control interface can be assessed based on the feasibility/probability of successful attacks and the impact of them. The former can be reduced by implementing appropriate security measures (e.g., firewall, authentication, and anti-virus software). Intensive research and engineering efforts have been devoted in those areas, but effective deployment of them remains a challenge in practice. The Ukraine incident demonstrated not only the difficulty to eliminate the possibility of such attacks but also inability of mitigation once those security measures are circumvented. Thus, in this paper, we focus on risk mitigation through the latter aspect, by reducing the potential scale of negative impact on power grid. Our approach is to introduce an additional layer of security in each substation that actively mediates — inspects and (when necessary) modifies — remote control commands from the control center to physical devices. We make three contributions.

- First, we propose a practical and effective way for deploying an active command mediation mechanism in each substation, which is compatible with widely-used IEC standards and the reference substation architecture.
- Then, we present a concrete command mediation scheme called autonomous command-delaying to enhance grid resiliency. Our scheme lets each substation autonomously introduce artificial time delay (from milli-seconds to seconds) before executing a remote control command.
- Finally, using PowerWorld simulator [3], we show that introducing well-bounded delay can significantly reduce (by over 90%) potential attack’s impact on the grid stability, without affecting legitimate grid operations.

The paper is organized as follows. In Section II, we discuss the related work. Section III provides an overview of modernized substations and related IEC standards. Section IV discusses the scope and threat model. Section V presents our active command mediation approach for mitigating attack impact. In Section VI, we evaluate the effectiveness of the
proposed scheme. Finally we conclude the paper with some future research directions in Section VII.

II. RELATED WORK

A number of research efforts have been devoted to securing automated/digitized electrical substations, ranging from detection of intrusion or anomaly within a substation [11], [14], [18] to multi-layer security platform [19]. The approach discussed in this paper is complementary to those mechanisms and can provide an additional layer of defense when they are bypassed by the attackers. In particular, while there are intrusion detection systems, e.g., Bro [11], that provide support for SCADA (Supervisory Control And Data Acquisition) protocols, those systems raise alarms only when they detect incorrect or unusual packet format and content. As a result, such approaches are not adequate to defend against attacks that issue legitimate-looking commands and mimic normal traffic patterns. Also, attacks may be detected only after serious damage has been caused.

In [17], Temple et al. discussed a mechanism to enhance resilience of smart grid systems against remote connect/disconnect attacks targeting a large number of smart meters. Although our idea of protection using artificial delay is similar to theirs, securing substations requires different considerations for timing requirements, communication mechanisms, and system design. Moreover, their evaluation relies on the number of disconnected meters and did not quantitatively evaluate the impact on power grid stability. Hershey et al. [6] also proposed the use of artificial delay in critical systems, including smart grids, to slow down and/or to detect and mitigate cyber attacks. However, they only discussed the high-level framework and did not propose specific designs on how to determine and continuously update the rules for adding delay. They also didn’t focus on securing the remote control interface of substations or provide evaluation regarding the positive and negative impacts of added delay in a power grid environment.

To the best of our knowledge, the work most closely related to ours is [12]. They also consider attacks exploiting remote control interface of substations, hence sharing threat models similar to ours. For mitigating impact of attacks, they use command-reversing, which sends reversing control commands shortly after the execution of detected malicious commands. However, it may not be always ideal. For instance, in the case of commands to stop or change setpoint of generators, it may take time to restore to the original state even if reverse control is initiated immediately afterwards. Moreover, if circuit breakers connected to loads are opened even for a short while, it would cause inconvenience on electricity customers owing to the disturbance. On the other hand, the mitigation scheme discussed in this paper aims at canceling at least part of the malicious control commands before execution, which can reduce the cost associated with such issues. Having that said, our scheme can benefit from the attack detection mechanism proposed in [12], which is based on the analysis of commands’ consequence and impact on power systems. Some of our experiments will discuss how well our scheme would work when used with their attack detection mechanism.

III. MODERNIZATION OF ELECTRICAL SUBSTATIONS

In order to modernize electrical substations, a number of standards have been established by the International Electrotechnical Commission (IEC) [2]. The notable ones related to substations include IEC 60870 and IEC 61850 [8]. The former defines specification for telecontrol by the control center or central SCADA system (in particular, IEC 60870-5-104 over TCP is increasingly used) while the latter focuses on substation automation (i.e., for communication within each substation or among substations). According to [7], [8], a digitized substation consists of three levels — station, bay, and process level. As shown in Figure 1, there is a component called Proxy/Gateway at the station level, which may be implemented on a remote terminal unit (RTU) or may be deployed as a separate box. One of its key responsibilities is protocol translation, for instance from IEC 60870-5-104 to IEC 61850 and vise versa. Thus, all control commands and configuration changes sent by the control center using IEC 60870-5-104 is mediated by Proxy/Gateway [8]. After such translation, commands are sent to intelligent electronic devices (IEDs) at the bay level, which are communication end points that are responsible for controlling and monitoring physical devices, such as circuit breakers, at the process level.

Remote control of power system devices in substations can happen in a number of different occasions. For instance, topology control for generation/transmission cost optimization [15] is usually done by opening or closing circuit breakers. Also, some utility companies are in a daily basis controlling shunt reactors according to the change in loads for the sake of voltage regulation. Yet another possibility would be to cut outputs from generators when the amount of generation exceeds the desired range. Such “power shedding” may be needed especially in the case of renewable generation as...
discussed in [10]. For cost-efficient and timely grid operation, it is expected that an increasing number of substations will implement interface for handling remote control commands.

IV. SCOPE AND THREAT MODEL

While a smart grid system can be protected in multiple layers, in this paper we focus on mitigation of attacks that abuse remote control interface of modernized substations. As recently demonstrated in the real incident in Ukraine [20], this is a crucial and urgent problem that requires solution. Our goal is to design an additional layer of security to improve the resiliency of smart grid systems against such cyber threats.

There are a number of operations that need to be executed with minimum delay, such as automated protection of transformers. They are performed locally within substations, which therefore are not remotely triggered by the control center. Thus, control commands for such operations are left outside of our scope. In addition, false data injection attacks, which forge or tamper data reported to the control center, is also outside of our scope since we focus on substations’ remote control interface. Anomaly detection mechanisms in the control center can mitigate the impact of false data injection. The security scheme discussed in this paper is orthogonal to them.

Our proposed solution does not intend to replace typical, widely-used cyber security measures, including firewall, access control, authentication, anti-virus, and intrusion detection systems. Even with such mechanisms in place, it is still possible for attackers to impersonate the legitimate control center and send out malicious control commands. For instance, as discussed in [10], [13], protocols used for this purpose, such as IEC 60870 and IEC 61850, are often vulnerable to replay attacks and man-in-the-middle attacks. Although security standards for those protocols are defined in IEC 62351, in reality it is not yet widely deployed in the field owing to constraints in cost and resources. Moreover, even if the communication channel were fully secure, another type of threat would be attacks mounted in the control center by malicious insiders, physical/cyber intruders, or zero-day malware, which can evade the aforementioned security measures. Our goal is to achieve higher power grid resiliency by reducing physical impacts caused by such attacks, even when attackers somehow succeed in bypassing other security measures and injecting malicious commands to substations.

V. ACTIVE COMMAND MEDIATION

A. Design Overview

When designing an additional security mechanism for existing smart grid systems, the following issues are crucial for practical, large-scale deployment:

- minimize changes required on existing systems;
- minimize impact on operations of existing systems;
- minimize dependencies on other systems or entities.

Having these as well as the threat model discussed in Section IV in mind, our approach for enhancing security and resiliency of smart grid systems is to introduce an additional “thin” layer between the control center and physical components in substations, inspired by the traditional information security principle of complete mediation. Specifically, we place a command mediation system that cannot be bypassed and is responsible for actively inspecting and pre-processing incoming remote control commands before execution on physical power system devices. There can be a number of possible implementation of such pre-processing schemes, including rule-based blocking or filtering, delaying command execution, and adaptive handling based on contextual information. We will discuss one concrete example in Section V-B.

As discussed in Section III, all remote control commands sent by the control center go through Proxy/Gateway (called Proxy hereafter), making a Proxy an ideal place to deploy the command mediation mechanism. As shown in Figure 1, we propose to implement our active command mediation system as a plug-in component of a Proxy. One advantage of our approach is that utility companies do not need to replace or upgrade individual IEDs, which is beneficial for minimizing introductory cost and efforts. Moreover, although in this design a Proxy needs to be trusted, protecting and monitoring one system component is more practical than securing multiple, heterogeneous IEDs.

At the same time, because a Proxy is a critical system component in terms of communication availability and responsiveness, the added security mechanism should be light-weight to minimize negative impact on its throughput and should require minimal coordination and reliance on external systems, such as other substations, since such interaction would not only increase communication and computational overheads but also unnecessarily broaden the attack surface.

B. Autonomous Command-delaying

Here we present one mitigation mechanism that can be implemented on the active command mediation system on a Proxy in each substation. We call it autonomous command-delaying. As the name implies, under our scheme, each Proxy independently adds artificial, but bounded, time delays before forwarding the control center’s commands to IEDs. The purpose of the artificial delay is to provide the control center with time buffer to detect attacks and then to cancel any suspected malicious commands. If the detection and cancellation can happen before delayed malicious commands are issued to the IEDs by the Proxy, those commands will not be seen by the IEDs and hence will cause no physical impact.

The overview of the concept is illustrated in Figure 2. In the figure, for the sake of simplicity, only one IED under each Proxy is drawn, but in practice there can be multiple IEDs per Proxy. After receiving any incoming remote control command, a Proxy at each substation independently inserts an artificial time delay before execution. Such a delay is illustrated as $d_1, d_2, \ldots, d_n$. The upper bound of the delay $(D_{ub})$ can be pre-configured according to the system needs or can be determined based on context (e.g., importance of substation, current grid status, and so on). The Proxy sends confirmation of the command receipt according to the IEC 60870-5-104 standard. However, this confirmation is usually sent to the sender of the command within the same TCP session, which might be directed to an attacker. Thus, to make
our scheme reliable, the Proxy needs to send an additional command acknowledgment message to a specific server at the control center, ideally via a separate, secure communication channel. Just like the command confirmation defined in the IEC standard, this acknowledgment should convey copy of the command payload to enable inspection by the control center. In the example illustrated in Figure 2, although an attack command sent to Proxy 1 is executed on the IED, the other commands are successfully canceled. In this way, our scheme is expected to reduce the number of attack commands executed, even if those commands were not blocked by other security measures, and therefore can mitigate the impact on the grid. We should also note that any computationally intensive task is not required on a Proxy, which meets our design principles discussed in Section V-A.

We assume that the control center is equipped with some attack detection mechanism that captures potential attacks based on received command acknowledgments etc. and then sends cancellation of the pending attack commands (i.e., malicious commands that are received by a Proxy but not yet executed owing to the delay). Again, the cancellation message should be sent via a trusted channel to prevent, for example, denial-of-service attacks that attempt to block execution of legitimate commands. Some examples of such a detection mechanism will be discussed in Section VI-B. Although, in this specific design, attack detection is out-sourced to the resource-rich control center, another, fully self-contained option is also possible. For instance, the active command mediation system (or a trusted sensor in the same substation) can monitor bus voltage, frequency, etc. for its decision making during the delay. We will further explore this direction in our future work.

Because pending commands need to be kept on memory until their execution, memory consumption may be a concern especially when a Proxy is implemented on a RTU. Based on measurements using our prototype, the size of a pending command is on average 50 Bytes. Given that middle-class RTUs or higher nowadays have free memory of Megabyte order, we believe this amount of memory usage is acceptable.

It might be argued that, instead of such an autonomous command-delaying solution, some simpler mechanism may be sufficient. For instance, each substation could be configured to enforce a threshold in the number of remote control commands that are allowed to be executed, e.g., per minute. Unfortunately, such an approach is effective only when a large number of commands are sent to a single substation. In practice, there can be tens of thousands of substations under a single power grid system, so even a small number of malicious commands per substation would still be enough to cause significant damage on the grid. Alternatively, one may propose to have all substations communicate with one another to enforce the threshold over all commands throughout the grid. While such a coordinated rate-limiting approach might work, the required coordination makes the solution difficult to deploy (see our discussion about design goals in Section V-A).

As discussed earlier, ideally the autonomous command-delaying scheme should utilize secure, dedicated communication channel for exchanging command acknowledgment and cancellation messages. Some may wonder why not simply direct all communications through it, if such a trusted channel is available. Although it may address many security problems, the main reason not to do so is to minimize the impact on existing infrastructure. In reality, power grid operators have already established the system based on standards such as IEC 60870-5-104, and the control center system is also implemented accordingly. If one mandates the use of a non-standard secure channel for all communication, it would require a major upgrade or replacement of the current system. On the other hand, use of trusted communication only between newly-added system components, namely an attack detection system at the control center and a Proxy in each substation, requires minimal change on existing systems.

C. Design Consideration on Artificial Delay

Perhaps the most controversial point in our command delaying design is whether it may cause negative impact on normal grid operations. IEEE Power Engineering Society’s guideline [9] says that the delay for communicating with nodes external to substations (including the control center) is normally greater than 100ms, hence accommodating delay of this order is already considered acceptable. Moreover, the same document says that maximum delivery time for transfer switching, line sectionalizing, and load control and shedding are 1, 5, and 10 seconds respectively. Thus, seconds-level delay is also tolerable in these use cases, which correspond to the remote control use cases discussed in Section III. In Section VI-A, we will further use simulation to quantitatively study the potential impact of artificial delay.

There are some different ways to add artificial delay, but one straightforward strategy is to delay all commands by a constant value to spare sufficient time for attack detection and response, subject to any upper bounds based on the latency requirements or publicly-available guidelines [9]. Let the time needed for malicious commands detection and response be $T_d$. If the detection mechanism at the control center is deterministic (e.g., rule-based attack detection) and the round-trip time through the trusted communication channel is stable, one may regard $T_d$ as a pre-known constant value. In this case, delaying all commands by $T_d$ (or slightly longer to include some safety margin) allows the best possible mitigation —
all attack commands detected can be canceled. On the other hand, the obvious drawback of this approach is that no command is executed immediately (or with shorter delay). In practice, possible and legitimate sets (or combinations) of remote control commands are limited and, to some extent, known in advance. Hence, a grid operator could evaluate the command combinations, perhaps by using a simulator as we will do in Section VI-A, to find the maximal delay, $D^*$, that does not cause any negative impact. If $D^*$ is longer than $T_d$, then the operator can simply choose to configure all command mediation systems to add delay $D^*$ before executing remote control commands.

It can happen that some legitimate command combinations cannot be delayed that long (i.e., $D^* < T_d$), especially when $T_d$ is relatively long (e.g., in the order of seconds). In such a case, we propose that the grid operator can identify (e.g., by simulation) how many of the commands have to be executed immediately to avoid negative consequence (e.g., frequency/voltage violations), if the rest of commands are delayed by $T_d$. In other words, the operator executes some commands immediately to earn sufficient time for the attack detection and response mechanism to complete its task to save the rest. This can be realized without any coordination among substations using a discrete-random-delay approach, where each Proxy, for each remote control command, independently adds delay of $T_d$ with probability $1 - P_{nd}$ and adds no delay (i.e., immediate execution) with probability $P_{nd}$. The value of $P_{nd}$ that ensures high probability of having the minimum number of commands immediately executed can be analytically calculated based on binomial distribution.

For the cases with more advanced attack detection schemes (e.g., ones running online power system contingency analysis), there can be significant variance in the attack detection time, which may make it even complicated to balance the timeliness of legitimate command execution and resilience to attacks. One option is to conduct extensive search over a variety of delay distributions (including one using continuous probability distribution, which we call continuous-random-delay approach) to find a good one that strikes the desired trade-off. Another potential advantage of this option is increased uncertainty in command execution timing from attackers’ perspective, making timing-sensitive attacks less feasible.

Next, we briefly discuss the level of mitigation under the discrete-random-delay setting and the more complicated continuous-random-delay setting. For the discrete-random-delay setting, we use 10% and 25% as $P_{nd}$. With probability $1 - P_{nd}$, each command is delayed by a constant of $D_{ub}$. To illustrate the continuous-random-delay setting, we pick three continuous distributions for random delay selection (more extensive investigation is part of our future work). One of them is a uniform distribution in $[0, D_{ub}]$ where $D_{ub}$ is the upper bound of the delay. We also evaluated the case with non-uniform delay distribution. Specifically, distribution skewed toward no delay is favorable for timely operation while distribution skewed toward maximum delay is desired for higher resiliency gain. To evaluate the difference, we chose two triangular distributions: one with its peak at 0-second and the other with its peak at $D_{ub}$. Finally, for the sake of comparison, we here consider the same $T_d=620ms$ for all cases, while admitting that it may not be the use case that continuous-random-delay approach is the most effective.

The results are summarized in Figure 3. When $D_{ub} < T_d$, regardless of the attack detection results, all attack commands will be executed in all cases. Assuming attack detection at the control center is 100% accurate, when $D_{ub} \geq T_d$, probability that each attack command is canceled before execution is calculated as follows. The probability under discrete-random-delay approach is equal to $1 - P_{nd}$. The probabilities under continuous-random-delay distributions are $1 - \frac{D_{ub}}{T_d}$ (uniform), $1 - (\frac{D_{ub}}{T_d})^2$ (triangular with the peak at $D_{ub}$), and $\left(1 - \frac{T_d}{T_{ub}}\right)^2$ (triangular with the peak at 0). As can be seen, the discrete-random-delay setting performs better than continuous-random-delay ones with short delay upper bounds (less than or around 1 second). For $P_{nd}=0.1$, the discrete option outperforms the best continuous option (triangular with peak at $D_{ub}$) until $D_{ub}$ increases to around 1.9s. In Section VI, we will focus on the evaluation of discrete-random-delay approach while leaving the study of continuous-random-delay options for future work.

VI. Evaluation

A. Impact of Artificial Delay on Legitimate Operations

We first quantitatively study the acceptable delay that does not cause negative impact on legitimate power grid operations. We use PowerWorld simulator [3] and employ a 37-bus system (from [5]) that consists of 57 branches (i.e., transmission lines), 9 generators, 14 transformers, 8 switched shunts, and 25 loads. Although the 37-bus system is hypothetical, the model is designed to well represent a small to medium-scale power grid [16]. A grid operator may perform similar simulations on her own system setup to configure the command-delaying mechanism.

Among the remote control use cases discussed in Section III, the most time-critical one is the reaction to unexpected increase of renewable generation (i.e., power shedding). We simulated such a situation by inserting significant increase of generation (by 100MW) on some combinations of 3 (out of 9) generators. Based on the transient stability analysis using
PowerWorld, if the delay between the generation increase and the curtailment control is less than 5.5 seconds, we did not observe violation in frequency or voltage (Figure 4). We also confirmed that there is no frequency violation even with tighter (±0.2Hz) criteria when the delay is less than 2 seconds.

Moreover, we ran 100 simulations in which 6 randomly-selected circuit breakers (i.e., 10% of all branches), are opened and then, after 0.1, 1 or 2 seconds, closed (i.e., recovered). In term of the occurrences that lead to frequency violation, the empirical probability remains around 8%, and we did not observe obvious negative trends for the case with 1 or 2 seconds delay, as compared to the case with 0.1 second delay.

Based on these observations, second-level delay is acceptable for common remote control use cases. However, optimal delay upper bound would vary for each power grid system, so careful simulation study is desired in the design phase.

B. Setup for Attack and Mitigation Experiments

The parameters to be defined to simulate the proposed command mediation scheme are upper bound of artificial delay added by each Proxy ($D_{ub}$), probability that no delay is added ($P_{nd}$), and time required by the security system in the control center for detection of attacks and cancellation of commands ($T_d$). Among them, $D_{ub}$ and $P_{nd}$ can be configured by grid operators based on their operational consideration, while $T_d$ is determined by the attack detection system employed.

$T_d$ consists of the communication latency between the control center and a substation and the processing time at the control center. We set the average network latency to 20ms (for command acknowledgment from substation and cancellation from the control center) based on measurements from our testbed that consists of industrial Ethernet switches. As the processing time, we use 10ms for quick detection and 600ms for advanced detection. The former assumes a simple detection scheme, which, for instance, checks if the command acknowledgment corresponds to a remote control command that the control center actually sent out in the recent past. The latter captures the processing time of a detection scheme that runs power system simulation to estimate commands’ consequences, and the number is set based on the detection scheme discussed in [12]. In summary, we use $T_d=30$ms for quick detection and $T_d=620$ms for advanced one.

To analyze the attack impact on power grid systems in both stable state and transient state, we again use PowerWorld simulator [3] and the 37-bus system [5].

C. Mitigation of Large-scale, Simultaneous Attacks

Although there are a number of attack strategies, the scenario that we particularly worry about is one where attackers inject a large number of malicious control commands within a short time period. Such an attack can cause significant impact before being detected by (traditional) intrusion detection mechanisms. Thus, in this section, we evaluate the impact of large-scale, simultaneous attacks on the simulated power grid and the effectiveness of the proposed mitigation scheme. As metrics of attack impact, owing to the space limitation, we focus on the discussion of the following:

1) the number of buses that experience voltage violation;
2) the occurrence of over-/under-frequency violation;
3) the amount of unserved load (i.e., reduction in load).

To maintain the quality of power grid service, it is crucial to maintain electricity frequency and voltage within a certain range from the nominal values. For instance, according to Western Electricity Coordinating Council (WECC) in the US, voltage deviation should be less than 20% from the nominal values [4] and a common threshold for frequency is ±0.5Hz. We use these criteria for the experiments. Besides, after execution of malicious control commands, some of the loads are entirely disconnected or shed as a result of balancing process, which has direct impact on demand-side experience as well as utility companies’ revenue. Thus, we included the third one in the list. For each load in the simulated power system, it is calculated as the difference of the load at the beginning of the simulation (i.e., before attacks) and the value at the end of 60-second simulation, and then summed up.

In our experiments, we simulate attackers sending “open” commands to randomly-selected circuit breakers. The experiments are performed with different fraction of attacked circuit breakers, ranging from 10% to 50%. We set $D_{ub}$ to 700ms for the experiments with $T_d=620$ms, and $D_{ub}$ to 50ms when $T_d=30$ms. For each setting, we repeated experiments for 100 times with randomly selected (i.e., different set of) circuit breakers, based on which we can calculate the average.

Figures 5 to 7 show results with the discrete-random-delay approach with different probability for delaying when $T_d=620$ms. Since we did not observe many over-voltage violations even without mitigation, we omit the corresponding plot. Regarding under-frequency violation, results are very similar to over-frequency violation. As can be seen, the improvement is significant especially when probability that no delay is added ($P_{nd}$) is 10% and 25%. In particular, in terms of under-voltage violation and unserved load, the negative impact is reduced by over 98% ($P_{nd}=10\%$) and 90% ($P_{nd}=25\%$) respectively. Due to space limitation, we do not show plots with $T_d=30$ms, which present similar fraction of negative impact reduction to the cases with $T_d=620$ms. Although we here assumed an ideal
case with 100% attack detection accuracy after $T_d$, based on the presented results, detection of 80-90% of attack commands is still expected to offer significant mitigation in practice.

VII. CONCLUSIONS

In this paper, we presented an additional layer of defense for securing the remote control interface of modernized electrical substations. Our approach to deploy an active command mediation system on the gateway of each substation is practical to roll out since it requires no change to existing IEDs and minimal upgrade in existing systems. As an example of security mechanisms that can be deployed on the mediation system, we discussed an autonomous command-delaying scheme. While the degree of effectiveness may vary across different power systems, our simulation with 37-bus system demonstrated that the proposed solution is highly promising – it can reduce negative consequences on the grid stability by over 90% without causing unacceptable impact on normal operations.

We plan to evaluate our proposed mechanism in larger, more complicated power system configurations to quantify the benefit of the added layer of security. Another direction is to develop context-aware command mediation, which adaptively defines delay and/or detects attacks based on local measurements etc. We also plan to study the use of continuous-random-delay in more complicated settings, and deploy our command mediation module with real-world devices.

ACKNOWLEDGMENT

The work was partly funded under the Energy Innovation Research Programme (EIRP, Award No. NRF2014EWT-EIRP002-040), administered by the Energy Market Authority (EMA) and in part by the research grant for the Human-Centered Cyber-Physical Systems Programme by the Energy Market Authority (EMA) and in part by the Programme (EIRP, Award No. NRF2014EWT-EIRP002-040), administered by the Energy Market Authority (EMA). The work was partly funded under the Energy Innovation Research mediation module with real-world devices.

VII. CONCLUSIONS

In this paper, we presented an additional layer of defense for securing the remote control interface of modernized electrical substations. Our approach to deploy an active command mediation system on the gateway of each substation is practical to roll out since it requires no change to existing IEDs and minimal upgrade in existing systems. As an example of security mechanisms that can be deployed on the mediation system, we discussed an autonomous command-delaying scheme. While the degree of effectiveness may vary across different power systems, our simulation with 37-bus system demonstrated that the proposed solution is highly promising – it can reduce negative consequences on the grid stability by over 90% without causing unacceptable impact on normal operations. We plan to evaluate our proposed mechanism in larger, more complicated power system configurations to quantify the benefit of the added layer of security. Another direction is to develop context-aware command mediation, which adaptively defines delay and/or detects attacks based on local measurements etc. We also plan to study the use of continuous-random-delay in more complicated settings, and deploy our command mediation module with real-world devices.

ACKNOWLEDGMENT

The work was partly funded under the Energy Innovation Research Programme (EIRP, Award No. NRF2014EWT-EIRP002-040), administered by the Energy Market Authority (EMA) and in part by the research grant for the Human-Centered Cyber-Physical Systems Programme at the Advanced Digital Sciences Center from Singapore’s Agency for Science, Technology and Research (A*STAR). The EIRP is a competitive grant call initiative driven by the Energy Innovation Programme Office, and funded by the National Research Foundation (NRF).

REFERENCES


