On the Impact of Cyberattacks on Voltage Control Coordination by ReGen Plants in Smart Grids

Kamal Shahid, Egon Kidmose, Rasmus L. Olsen
Department of Electronic Systems (WCN),
Aalborg University, Denmark
Email: {ksh, egk, rlo}@es.aau.dk

Lennart Petersen, Florin Iov
Department of Energy Technology,
Aalborg University, Denmark
Email: {lep, fi}@et.aau.dk

Abstract—**Wind power and Solar photovoltaic plants are expected to jointly produce a lion's share of renewable energy generation capacity needed to reach the target of having green energy around the globe. In this respect, investigation of voltage stability support and coordinated control are crucial step stones towards a future resilient power system. The ability to provide online voltage stability support from Renewable Generation plants highly depends on the communication infrastructure that allows an exchange of information between different grid assets. Any attempt to attack this communication system can lead to an unstable grid and in worst case, a complete blackout. Therefore, this paper illustrates the impact of cyberattacks on the voltage control coordination between the renewable generation plants and the system operator in microgrid settings. More specifically, this work focuses to show how time-varying delays and manipulation of exchanged information caused by cyberattacks can affect the controller performance. Finally, security solutions are proposed that make voltage control coordination resilient against these cyberattacks without adding additional delays to the process.**

Keywords—**Information and Communication Technologies (ICT); Renewable Generation (ReGen) Plants; Voltage Control coordination; Cyber-Attacks**

I. Introduction

Today, a large part of the wind power in Denmark, i.e., 3799 MW is coming from onshore wind turbines [1] [2], which are distributed individually or in small scale clusters, while the PV production mainly consists of dispersed residential small units up to 6 kW [3]. The anticipated trend is that the increased share of installed renewable energy in Denmark in the coming years will mainly be accomplished by integrating large concentrations of off-shore WP plants (WPP) in the transmission system, as well as large scale concentrated PV plants (PVP) and new generation onshore WPP in the distribution system [1]. This foreseen high penetration of Renewable Generation (ReGen) plants into the Danish electricity supply may cause several problems, as discussed in [1] and [4]. According to [1], the provision of reactive power support from ReGen plants in the distribution grid will not only make it possible to down-regulate the entire voltage profile in the distribution system, but also keep the voltage within the limits at the given nodes. Thus, the needs for coordination in providing reactive power support and hence controlling voltage locally on a distribution grid is required in respect of the increasing number of dispersed units. It is foreseen that aggregators of these ReGen units may take the responsibility, in close cooperation with local DSOs, for hosting voltage control capabilities besides the trading energy [5]. Therefore, at this stage, we consider that it is the aggregator control unit that is responsible for providing reactive power support and controls the voltage locally on the distribution grid.

It has been ascertained in [4] that the provision of reactive power support from ReGen plants and hence controlling voltage locally on a distribution grid imposes high responsibility on the ICT infrastructure. In [4], the authors have illustrated the use of the existing public network communication infrastructure as a base case and outlined its impact in terms of added latencies due to, for instance, network failures on the online voltage control coordination functionalities for ReGen plants in distributed grids. However, vulnerabilities associated with the use of public communication networks and information systems may be exploited for financial or political motivation to delay, block, alter process related information (with fraudulent information) or even direct cyberattacks against ReGen plants, thereby preventing the aggregator control unit from obtaining production metrics. In any case, this will impact the integrity, confidentiality or availability of the ICT system [6] and, thus, strategies should be defined to cope with such risks. For this reason, as an extension of the work presented in [4], this paper illustrates the impact of time-varying delays and manipulation of the control messages caused by cyberattacks on the system's performance. The European Smart Grid Information Security (SGIS) working group [7] is used as a reference for determining the level of security threat to the system.

The security of power systems using cellular networks for control purposes has been addressed in several papers. For instance, in [8], the authors analyze end-to-end security of the communication between DSO substation and distributed energy resources (DERs) over heterogeneous networks through TLS encryption and authentication in compliance with IEC 62351-3. Reference [9] describes an approach to use standardized technologies to provide secure communications for ancillary services with minimal configuration by administrators of corporate networks. The authors in [9] also discuss the problems of integrating legacy devices. However, the authors in [9] do not focus on the voltage control coordination in particular considering the high penetration of ReGen plants in the power grid. Reference [6] focuses on medium voltage grids characterized by a high level penetration of ReGen plants and examines the risks associated to the communication malfunctions of an ICT architecture implementing the voltage control function. Reference [6] is mainly based on the studies related to the Italian medium voltage grid without actually showing the impact of ICT malfunctioning on the grid implementation and voltages due to cyber-attacks. Whereas, in this paper the results are based on a Danish medium voltage (MV) distribution grid located in the Northern Denmark as a benchmark model to show the impact of cyber-attacks in terms of power losses in the system.

The remainder of this paper is organized as follows: Section 2 explains the voltage control coordination scenario in power distribution systems, highlighting several ways and challenges to connect ReGen plants to the aggregator control unit. The security challenges related to ICT in providing the online voltage control coordination in the MV grid are outlined in Section 3. Section 4 provides the impact that cyberattacks have on the online voltage control coordination between ReGen plants and aggregator control unit. While, in Section 5, solutions are proposed to secure this communication without effecting the control's performance. Finally, the conclusion of this study is given in Section 5.

II. Benchmark Grid And System Description

In MV distribution grids, one of the challenges is to keep the voltage within ± 10% of its nominal value [4]. In case these limits are violated at certain points within the grid, affected generation and consumption units need to be disconnected, which can eventually lead to severe stability problems in the entire power system. Fig. 1 shows one of the ways for a single ReGen plant to contribute to voltage regulation, realized by a local voltage controller.

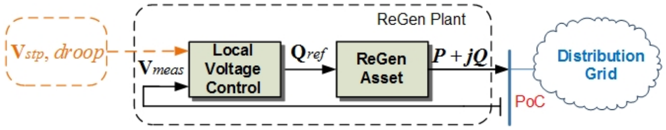

Fig. 1: Voltage control scheme of ReGen plant [4]

Here, the ReGen plant has an inner control loop for regulating reactive power provision at the Point of Connection (PoC) and an outer voltage control loop for controlling the voltage in the PoC [1] [4]. A voltage reference point (V_{stp}) and a droop value needs to be specified for the ReGen plant controller. The other control objectives imposed by the DSO, e.g. to reduce the grid power losses which are caused by reactive power provision, can be achieved by optimizing the control settings in a so-called distributed on-line coordination scheme [10]. Since the power output of ReGen plants varies continuously and thereby the voltages in the distribution grid, an aggregator of grid support services may take over the task to update the controller settings of the ReGen plants continuously in real-time according to the actual operating point [4].

Fig. 2 illustrates the actors involved in such a coordination scheme. As defined in [1] [4], the DSO needs to provide the system parameters of the distribution grid. The aggregator receives measurement signals of voltage, active and reactive power ($V_{meas}, P_{meas}, Q_{meas}$) as well as the available reactive power (Q_{ava}) from all ReGen plants $(1, ..., N)$ and dispatches the droop settings ($V_{stp}, droop$) for the voltage controllers.

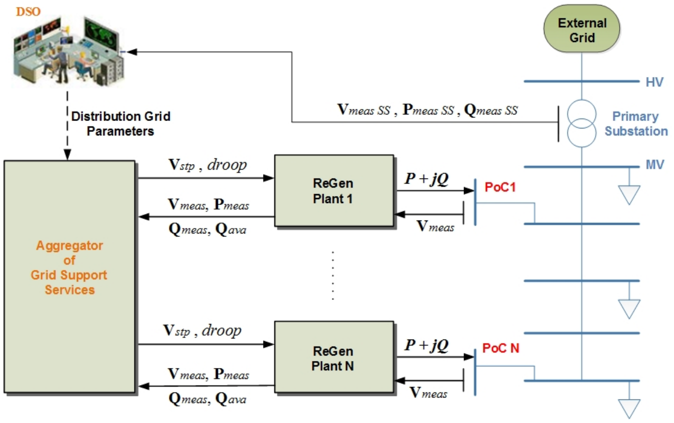

Fig. 2: Scheme for Distributed On-Line Coordination of voltage control functionalities [4]

As in [4], to account for a realistic penetration of renewables in the Danish distributed grids in the future, a MV distribution grid in the Northern Denmark has been used for this study (see Fig. 3). This distribution grid represents a typical radial feeder topology with primary substation (60/20 kV) and four ReGen plants. In Fig. 3, the ReGen plants are shown as WPP, PVP 1, PVP 2 and PVP 3 (the benchmark grid model is presented in detail in [11]). Fig. 3 also shows the connection of all ReGen to the aggregator unit through a communication network. This network is a third party public communication network, as illustrated in [4]. The following section explains different types of cyber security risks associated to the use of these public networks for the online voltage control coordination in the said scenario.

III. Security Scenarios in Online Voltage Control Coordination

Security of critical infrastructures is facing many threats, particularly when systems are connected to the internet. In private, isolated networks physical security provides an important layer of security. However on the internet, segregation and firewalling can limit the attack surface, but part of connected systems must be exposed for the internet to be of use and consequently also exposed to attacks.

A. Cyber-Attacks on ICT

There are several kinds of cyberattacks based on the types of "hackers", as elaborated in [12]. In context of the scenario explained in Section II, the sabotage caused by these attacks

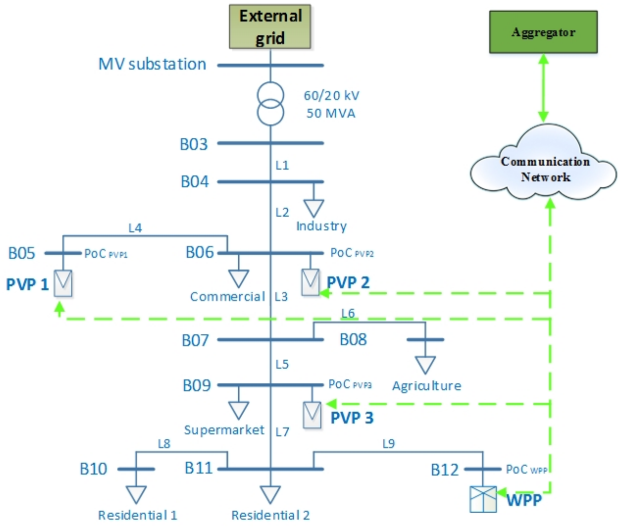

Fig. 3: Structure of MV benchmark grid showing communication of the aggregator control unit with ReGen plants

is considered as reducing/removing the availability of online voltage control coordination functionality or manipulation of the droop values. In terms of cyberattacks, reducing/removing the availability of service provided by the infrastructure can be achieved particularly by an interesting type of attacks called Distributed Denial of Service (DDoS). DDoS attacks are not novel or necessarily very sophisticated, but they are cheap, simple and often highly effective in achieving their goal of breaking the availability. Minute long attacks can be bought online as a service for as little as $5, [13]. By remote controlling networks of infected machines, so called botnets, the attackers abuse these distributed platforms to generate devastating amounts of traffic. Volumetric attacks, such as UDP flood, seek to starve network link capacity. Volumetric attacks easily reach hundreds of Gbps, while the recent extreme case of the Mirai botnet suggests that as many as 100,000 bots generated 1.2 Tbps at the peak [14]. Network and application layer attacks aim to exhaust resources (memory, CPU etc.) of either the protocol stack implementation or applications. For these attacks, hundreds of thousands of requests per second are sent to the target, rendering it unable to handle the legitimate traffic. Impacts of DDoS attacks range from no impact if they fail to exhaust the target, over increased packet loss, delay and jitter, to the successful attack, where the targeted service becomes fully disabled.

In contrast to the simple, cheap and readily available DDoS attacks, there are the so-called targeted attacks. A targeted attack involves investment of time from a team of highly trained specialist to tailor the attack. Such effort is costly, but obviously also likely to succeed, given enough resources, and the outcome will typically be complete, covert control, of the targeted systems. In the case of SCADA networks, attack will typically give the attackers full control over some part of the plant. This can be used to perform espionage by exfiltrating data or to interfere with operation of a plant. By tampering with actuation and sensing signals, attackers can disturb production and even cause physical damage. A well-known example of a targeted attack on SCADA systems is the Stuxnet malware. The goal appears to have been to disrupt Iranian uranium processing plants. The attack was carried out over years, it was designed to break mechanical parts very slowly to stay undetected and it relied on agents on the ground to facilitate breaching into isolated networks. Furthermore, the attack exploited multiple zero day vulnerabilities —Software vulnerability which are not known to the public at the time and which are traded on underground markets for tens of thousands of dollars. All this speaks to a large amount of resources being invested in the attack and it has been speculated that nation states are behind, [15]. The point is that in the end an attacker with enough resources appears to be able to compromise and tamper with any ICT. According to [6], voltage control coordination is important because it has a direct influence on both the power operation and economy, and includes a high level of inter-networking requirements for its ICT architecture. Therefore, in the case of aggregator control units communicating with the ReGen plants, the risks involve espionage and sabotage towards any part of the whole power system.

B. Modeling the Cyberattacks test cases

Following scenarios can be defined to model the real attacks discussed above.

Case 1: Small UDP flood on aggregator control unit. This exemplifies a volumetric DDoS attack of the sort that can be launched with hardly any knowledge and only a few dollars. A 200 Mbps stream of UDP packages, lasting 5 minutes, is sent to the IP address of the aggregator control unit.

Case 2: Large UDP flood on aggregator control unit. Unlike Case 1, the modelled attacker makes use of a botnet and relies on techniques such as amplification and reflection to sustain a 1.2 Gbps DDoS attack for 5 days. This requires a lot more technical knowledge and preparation than Case 1, yet it is still simple compared to a targeted attack. The throughput is set to the estimate of the largest known attack, while the duration reflects the arbitrary choice of the attackers to discontinue the attack. Apparently, this attack seems too long to be realistic and one might think of turning off the server, reset the configuration or even cutting off the communication to prevent further sabotages. However, the DDoS attack may not necessarily just disappear by going offline. It highly depends upon the motivation and anger the attacker has to harm the system. He might wait for the system to get online again.

Case 3: TCP Reset on aggregator control unit. In this targeted attack the attacker have invested many resources and relied on advanced techniques to get access to a real-time copy of the traffic to and from the aggregator control unit, as well as the ability to send forged traffic to the aggregator control unit. The attacker exploits this to transmit forged TCP Reset packets, effectively closing all TCP connections to and from the aggregator control unit. It is assumed that engineers are reacting very promptly and can identify and mitigate the problem after 12 hours.

Case 4: Small UDP flood on ReGen. Same as Case 1, but targeted at a ReGen plant.

Case 5: Large UDP flood on ReGen. Same as Case 2, but targeted at a ReGen plant.

Case 6: TCP Reset on ReGen. Same as Case 3, but targeted at a ReGen plant.

Case 7: Targeted attacker tries to break the power plant physically, for instance, through oscillations or manipulate the droop values. The interesting bits requires understanding of the plant. For instance, what changes will the attacker make to droop values and control signals to cause catastrophic damage to the ReGen plant or the power system?

C. Summarizing the effects caused by Cyber-Attacks

Based on the few (out of many) cyberattack cases described above, the effects caused by these attacks can be categorized into two types: First, added latencies in sending status updates from ReGen plants to the aggregator control unit or set-points from aggregator to the ReGen plants. Second, false messages sent to/from the aggregator/ReGen. These attacks may become a high risk to the integrity, availability and confidentiality of the whole power system. Therefore, depending on these two cases, we now analyze the impact of different level of latencies and false messages due to cyberattacks on the on-line voltage control coordination and ultimately on the power losses in the following.

IV. Impact Of Cyber-Attacks on Power System

In [4] and [11], it has been ascertained that for adjusting the voltage set-point, various update rates in the range of seconds to minutes have a minor impact on the resulting power losses within the grid. Therefore, it can be remarked that delays caused by UDP flood attacks or even TCP Reset attacks in the time range of seconds to minutes would not affect the control performance significantly, assuming that the update rate of the voltage set-point is 10 seconds (minimum). Even if the communication between ReGen plants and the aggregator control is disrupted for several minutes, the local voltage controller of the ReGen plant will apply the last sent set-point, which results in negligible deviations in the power losses in the distribution feeder [4].

However, as revealed in Section III, cyberattacks can disrupt the connection up to several hours, which may affect the power losses more significantly. For this, taking into account different test cases for communication failure in [4], we have evaluated the extent to which the latencies in communication up to several hours will affect the on-line coordination of voltage control functionalities in distribution grids.

A. Test Cases for added latencies due to cyberattacks

For testing long-lasting communication failures, a benchmark test scenario with a time frame of 24 h was applied in [4]. Four test cases were considered in terms of hours of delay caused due to communication failure i.e., 1 h, 6 h, 12 h and 24 h.

Fig. 4 shows the line losses expressed as percentage of the total generated power by all ReGen plants, averaged over the simulation period of 24 hours, with and without various communication failures [4]. It can be observed in Fig. 4 that the power losses increase for longer communication failures. The blue-colored bars show the power losses without any voltage control. However, in this case the tolerance band margins of the voltage (±10%) are not fulfilled. Then, voltage regulation with maintained settings for the ReGen plant controllers (off-line, red-colored) leads to a considerable increase of the power losses. By introducing distributed on-line coordination (no fail., green-colored), the losses can be reduced to a significant extent. However, it can be observed from Fig. 4 that the power losses increase depending on the duration of the communication failure in the system.

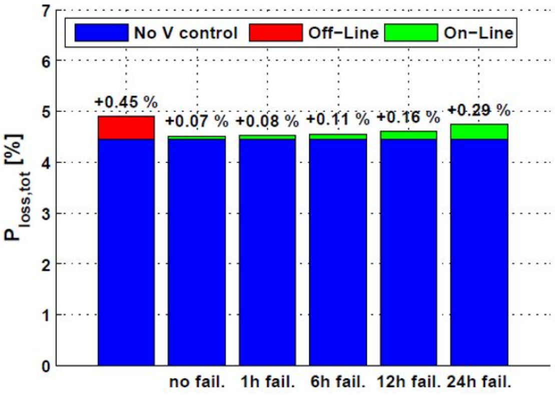

Fig. 4: Average power losses over the simulation period for various durations of communication failure for updating the voltage set-points [4]

B. Manipulation of Droop/Set-point Values due to cyberattacks

In [1] and [4], it has been ascertained that relatively flat droop characteristics of the local voltage controller in the ReGen plants lead to instable voltage regulation within the distribution grid due to hunting effects between the individual controllers. In case a hacker is able to manipulate the droop values accordingly, by attacking the aggregator control unit and sending updated reference signals to all ReGen plants, severe grid situations can occur. This is illustrated by Fig. 5, showing the voltage and reactive power profile for a case when all droop values are set to 0.5%, leading to a very flat droop characteristic.

At t = 500s, the cyberattack (in terms of manipulation of the droop values) is initiated, leading to subsequent voltage oscillations. At t = 524s, the WPP experiences a voltage exceeding the limit of 1.1 pu and needs to shut down. Voltage

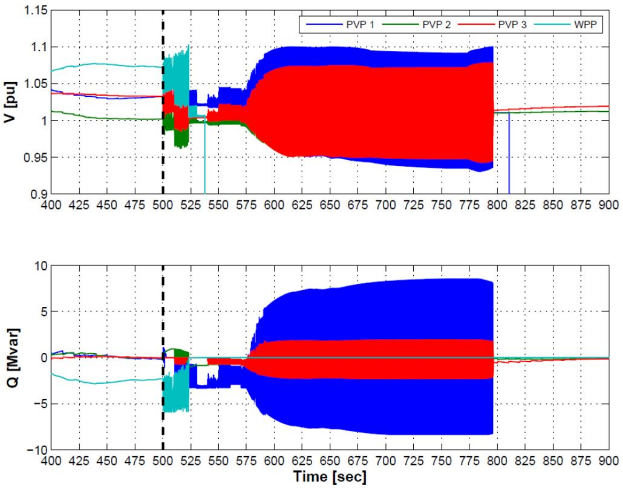

Fig. 5: V and Q of all ReGen plants when subject to a cyberattack (manipulating droop value at t = 500 s)

oscillations between all PVPs sustain, until PVP 1 shuts down at t = 795 s due to overvoltage.

Fig. 6 shows a case where the hacker was capable of manipulating the voltage set-points being sent from aggregator to the ReGen plants. At t = 500 seconds, a reference signal of Vset=1.08 pu is sent to all ReGen plants, which instantaneously leads to a rising voltage profile in the distribution feeder. At t = 567 seconds, the WPP shuts down due to overvoltage. The remaining PVPs will eventually provide reactive power (+Q) to boost the voltage according to the droop characteristic with the relatively high voltage set-point.

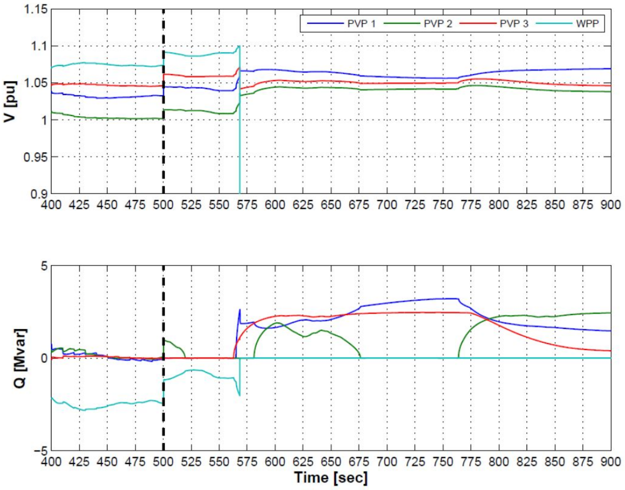

Fig. 6: V and Q of all ReGen plants when subject to a cyberattack (manipulating voltage set-point at t = 500 s)

C. Test Summary

The impact of cyberattacks on on-line voltage control coordination can be summarized by means of SGIS five scale likelihood levels in [7], as presented in Table 1.

TABLE I: Impact of cyberattacks on on-line voltage control coordination –SGIS likelihood levels

Security Level	Effects of Cyber-Attacks
Critical	False Message Signals
Medium	Latency up to Several Hours
Low	Latency from Seconds to Minutes

V. Cyber-Security Solutions

Cyber-attacks can be mitigated in many ways, depending on the attack vector among other things. Two approaches to handle the cases described above are introduced in the following.

A. DDoS Scrubbing Centers

A small volumetric DDoS attack towards a server in a datacenter can possibly be handled by provisioning network capacity accordingly and well in advance. This is expensive as the excess capacity is wasted when there is no attack, which presumably is most of the time. For large volumetric attacks this approach is infeasible, and instead it is common to rely on so called DDoS scrubbing centers [16]. As shown in Fig. 7, all traffic to protected systems is routed through a DDoS scrubbing center, rules and proprietary methods are applied to filter out DDoS traffic. Legitimate traffic is ideally simply passed on to the protected services. Such centers generally claim to introduce no significant delay, as it merely modifies the BGP routing that is already done on the internet, and performs filtering at line speed. As these centers are specialized in handling DDoS attacks, they can provide network capacity to handle large DDoS attacks. In cases where DDoS traffic exhausts even scrubbing center capacity, or if such centers are not used, traffic from all or some parts of the internet can be dropped by modifying the BGP routing. Scrubbing can be always-on, such that no significant amount of traffic reaches the target. It can even be on demand, meaning that the DDoS traffic will hit the target for a few minutes, until the service is enabled. Thereby, imposing minor impact on the power losses.

B. IPsec Protocol

The TCP and IP protocols that make up the internet provides no confidentiality nor authenticity guarantees. When a determined attacker compromises the trivial security mechanism of the lower layers (e.g. physical security, network segmentation) the attacker can perform attacks like the TCP reset attack described in Cases 3 and 6 in Section III. A precondition for this attack is that confidentiality is breached, such that the attacker can learn the states of the TCP connections, and that authenticity is breached, such that the attacker can pretend to be the other party of the connection. The commonly deployed SSL/TLS protocol provides the required guarantees, but relies on the TCP protocol, hence it cannot mitigate the TCP reset attacks. IPsec is another protocol providing the required security guarantees. IPsec replaces the IP protocol and encrypts the wrapped TCP packet, among other things,

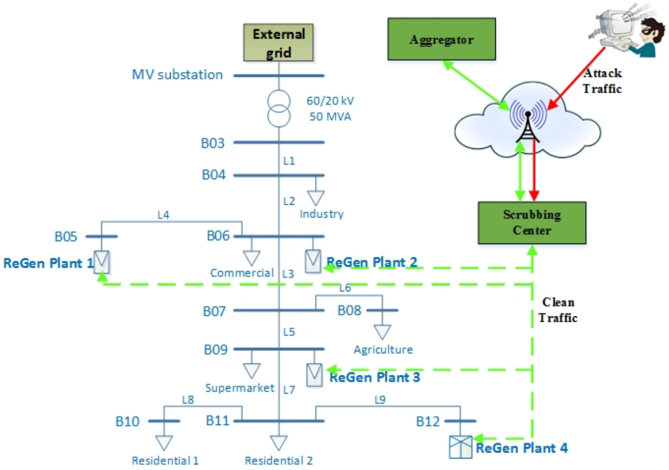

Fig. 7: Use of Scrubbing Center for clean traffic

providing authenticity and confidentiality. This stops attackers both from learning the TCP connection state and from impersonating a connection party, thereby thwarting the TCP Reset attack. Using IPsec have a price though, which comes in the form of protocol overhead. Since IPsec always require ESP header for the confidentiality issues, it has the highest communication overhead among other security protocols [17]. The communication overhead causes end-to-end delay to be affected the most by IPsec [17]. However, since the additional delay lies within a range of milli-seconds to seconds [17], it will not have much impact on the performance of the system, as ascertained in Section IV.

Conclusion and Future Work

Cyberattacks are an important issue for smart grid communication. This paper elaborates the impact of cyberattacks on on-line voltage control coordination from ReGen plants in a smart grid scenario. Various aspects related to the possible cyberattacks are evaluated with respect to the related latencies and validity of the signals being exchanged between aggregator and ReGen plants, resulting in deviating voltage control performance in the distribution grid. Based on the criticality of power system infrastructure, cyber-security solutions must be in place to provide a secure cyber environment. Although there exist many traditional cyber-security solutions that can be used to secure communication in smart grids, a lot more research has to be done. Here we have identified only two of such security solutions in this paper to stop/mitigate the effects of these cyberattacks. The motivation for this paper was specifically to analyze the impact of various cyberattacks on the performance of online voltage control coordination. However, as a future work the authors are currently working on implementing various cyber-security solutions in a test-bed (including IPSec and DDoS scrubbing center) to analyze how effective these solutions are to provide cyber-secure environment to the future smart grids.

Acknowledgment

This work was carried out by the Department of Electronic Systems in cooperation with the Department of Energy Technology at Aalborg University, Denmark. Energinet.dk is acknowledged for funding this work in contract number: PSO project 2015 no. 12347, “Ancillary Services from Renewable Power Plants (RePlan)”, www.replanproject.dk

References

[1] L. Petersen, F. Iov, A. D. Hansen, and M. Altin, “Voltage control support and coordination between renewable generation plants in mv distribution systems.” Vienna, Austria: Proceedings of the 15th Wind Integration Workshop, November 2016.

[2] “Danish wind industry association - the danish market,” Tech. Rep., 2016. [Online]. Available: http://windpower.org/

[3] “Overview of the danish power system and res integration.” [Online]. Available: file://es.aau.dk/Users/ksh/Downloads/energy-needs-in-denmark-executive-summary.pdf

[4] K. Shahid, L. Petersen, F. Iov, and R. L. Olsen, “On the impact of using public network communication infrastructure for voltage control coordination in smart grid scenario,” 2nd EAI International Conference on Smart Grid Inspired Future Technologies, Ed. Springer, March 2017.

[5] F. V. Hulle and I. Pineda, “Economic grid support services by wind and solar pv,” Tech. Rep., September 2014. [Online]. Available: https://windeurope.org/fileadmin/files/library/publications/reports/REserviceS.pdf

[6] G. Dondossola and R. Terruggia, “Security of communications in voltage control for grids connecting der: impact analysis and anomalous behaviours,” August 2014.

[7] “Cen-cenelec-etsi smart grid coordination group: Smart grid information security,” Tech. Rep., 2014. [Online]. Available: ftp://ftp.cencenelec.eu/EN/EuropeanStandardization/HotTopics/SmartGrids/SGCG_SGIS_Report.pdf

[8] R. Terruggia and G. Dondossola, *Cyber Security Analysis of Smart Grid Communications with a Network Simulator*. Cham: Springer International Publishing, 2015, pp. 153–164.

[9] M. Krebs, S. Röthlisberger, and P. Gysel, *Secure Communications for Ancillary Services*. Springer International Publishing, 2015.

[10] L. Petersen, M. Altin, K. Shahid, R. L. Olsen, F. Iov, A. D. Hansen, and X. Han, “Deliverable d1.1 - specifications for regen plant model and control architecture,” Tech. Rep. [Online]. Available: http://www.replanproject.dk/publications/deliverable-reports

[11] L. Petersen, K. Shahid, M. Altin, R. L. Olsen, F. Iov, A. D. Hansen, and X. Han, “Deliverable d 2 - voltage control support and coordination between regen plants in distribution systems,” Tech. Rep. [Online]. Available: http://www.replanproject.dk/publications/deliverable-reports

[12] E. Kyriakides and M. Polycarpou, Eds., *Intelligent Monitoring, Control, and Security of Critical Infrastructure Systems*. Springer Berlin Heidelberg, 2015.

[13] “Ddos threat landscape report 2015-2016,” Tech. Rep. [Online]. Available: https://lp.incapsula.com/rs/804-TEY-921/images/2015-16%20DDoS%20Threat%20Landscape%20Report.pdf

[14] “Dyn analysis summary of friday october 21 attack | dyn blog.” [Online]. Available: http://dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack/

[15] “Stuxnet was work of u.s. and israeli experts, officials say - the washington post,” (Accessed on 04/06/2017).

[16] N. Lee, *Counterterrorism and Cybersecurity: Total Information Awareness*. Springer New York, 2013.

[17] K. Hong, S. Jung, L. Lo Iacono, and C. Ruland, “Impacts of security protocols on real-time multimedia communications,” in *Proceedings of the 5th International Conference on Information Security Applications*, Berlin, Heidelberg, 2005.