Microsoft Cyber Security Engage

Saloni Dabgar

August 24, 2022

1 Methodology and Assumptions

This paper derives its assumptions on the entity of interest: power grid cyber-physical system based on through literature research. In this paper,the following assumptions have been put into place.

1.1 Power Grid Cyber Physical Infrastructures

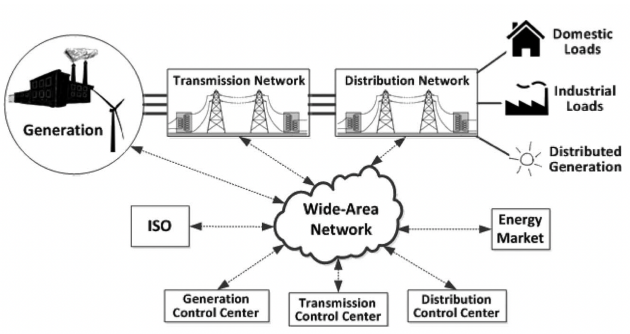

Figure 1: Power Grid Cyber Physical Infrastructures

Current cyber systems as described in [1] consists of electronic field devices, Independent System Operators(ISOs), substation automatic systems, communication networks, and control center which are embedded throughout the physical grid for efficient and reliable generation, transmission and distribution of power.

1.1.1 Power System Control Applications

- Generation Control and Security

Control loops under the generation section of the power system control controls the generator power output and the terminal voltage. Local(Automatic voltage regulator and governor control) and wide-area(automatic generation control) control schemes are used in generation of power. Their details are as follows:

1. Automatic Voltage Regulator(AVR)
   - The digital exciter control module is used to provide power system stability. It controls the amount of reactive power absorbed by the system. It is connected to the control center via Ethernet and uses communication protocols such as Modbus[4].
2. Governor Control
   - It is primarily a frequency control mechanism and communicates using protocol such as Modbus with the control center over the Ethernet.
3. Automatic Generation Control(AGC)
   - AGC is a secondary frequency control loop that fine tunes the system frequency to its nominal value by making corrections to inter area tie-line flow and frequency deviation[3].

- Transmission Control and Security

The system normally operates at 13 KV and ensures that the power flow in the lines are within the safe operation margins.

1. State Estimation
   - Estimates of system variables such as phasor angle and voltage magnitude is made on the basis of presumed faulty measurements from the field devices even in case of device/communication channel malfunction.
2. VAR compensation
   - Volt-ampere reactive compensation controls reactive power performance of the transmission system by minimising voltage fluctuation at a given end of the transmission line. They also enhance the transferable power through a given transmission line and also has the potential to prevent a blackout situation.
3. Wide Area Monitoring System
   - Work on PMU based wide area measurement systems are currently in progress. Measurements made by the PMUs directly help in the computation of real power flows in the network and help in decision making in the control center. They use Global Positioning System(GPS) to accurately timestamp phasor measurements.

Distribution Control and Security

This system is responsible for power delivery to the costumer.

1. Load Shedding
   - These schemes are useful in preventing a system collapse during emergency operating conditions. In cases when system generation is insufficient to match up the load, automatically load shedding schemes are employed to maintain the system frequency within safe operating limits and thus protect the system from any potential damage. In such a scenario, load shedding is done by a utility at the distribution level by the under-frequency relays connected to the distribution feeder.
2. AMI and Demand Side Management
   - AMI primarily relies on the deployment of "smart meters" at consumers' locations to provide real-time meter readings. Smart meters have utilities that implement Load Control Switching(LCS) that disables consumer devices when the demand spikes. Meter's current configuration is controlled using a meter data management system(MDMS) which lies under utility control. MDMS connects to an AMI head-end device which forwards commands and aggregates data collected from the meters. Networking within AMI relies on technologies such as RF mesh, WiMax, WiFi and power line carrier.

1.1.2 Supporting Infrastructure

A secure supporting infrastructure is necessary to safe and accurately store and transmit information to appropriate applications. Some definite properties of the infrastructure include:

1. Long system life cycles
2. Limited physical environment protection
3. Restricted updating/change management capabilities
4. Heavy dependency on legacy systems/protocols
5. Limited information processing abilities

A good supporting infrastructure should enforce confidentiality of its data to protect it from unauthorised users. It should also must provide sufficient availability of information to the authorised users. Hence, security mechanisms such as cryptography, access control, and authentication are necessary to enforce the aforementioned traits.

Let us now choose a scenario of the smart grid system under attack and the attack vector is a DoS(Denial of Service). We shall further(in Solution Architecture section) explore the possible attacks made by DDOS on our infrastructure and develop framework to mitigate the attack.

2 Defining the Cyber Deterrence Challenges

2.1 What is Cyber Deterrence?

Just like a war strategy, in the cyber space as well, deterring threats instead of fighting war damage is the most widely used strategy. Deterrence is the practice of discouraging or restraining someone, in world politics, usually a nation-state from taking unwanted action-such as a armed act[2].

2.2 The Challenges to Cyber Deterrence

2.2.1 Challenge of Attribution

For a direct counter- attack, a nation must be clear about the identity of the perpetrators, but it often happens that the locations are spoofed and identities hidden, false flags being raised to deceive identity of the attackers. Even if these attackers are identified as belonging to a particular country, it is very difficult to prove that they are state-sponsored. Intelligence operations can be compromised if the fingerprint of the state is declared openly. However, this hesitation to respond might also result in weakened credibility and deterrence.

2.2.2 Uncertainty of the Effect

In nuclear deterrence, we know the atomic potential of the attacker. However, in cyber warfare's, since the national cyber capabilities are zealously guarded, there is absolute no certainty how a cyber attack would impact the adversary[1]. There is also a danger of unintended collateral damage. For example, in the case of attack of Stuxnet on Iranian Uranium enrichment facility at Natanz in 2009, the malware was designed to precisely affect only the Siemens supervisory control and data acquisition systems, it spread beyond the intended target and went on to infect more than 200,000 computers worldwide.

3 Legal and Treaty Assumptions

3.1 Treaty Principles

In order to regulate the method of warfare and its consequences, treaty principles are put in place. In this section of the paper, we review some of the core principles of LOAC that can be used as guide to lay future cyber-treaty discussions. These principles are:

3.1.1 Military Requirements

Enemy forces are assumed to be aggressive' according to this principle.Consequently, the enemy forces along with their equipment's and supplies are likely to be attacked at will. This directly implies that non-combatants and civilians having no direct involvement in war, and whose destruction would yield little or no military advantage are immune from the attack[2]. However, as the line between military and civilian networks become blur in the realm of cyberspace, large swaths of public infrastructure face huge risk of a cyber-attack during an actual state of hostility. In the heat of battle, it also becomes difficult for the military commanders to figure out which are on the network service strategic purposes and which on civilian[2]. Effective issue resolution can take place with the involvement of electronic engineers, military strategists and international legal experts.

3.1.2 Distinction

Principle is specifically designed to designate combatants from non-combatants. It is put into place so as to make sure the current application of LOAC is implemented. This can be achieved by keeping a check on the lawful and unlawful activities. However, it is difficult to apply this principle in today's warfare scenario as the location of the attacker is not same as its actual location

3.1.3 Proportionality

In military context, this principle requires a balance test between the concrete and direct military advantage anticipated in attacking a legitimate military target and the expected incidental civilian injury. However, in a cyber warfare scenario, the major issue lies in drawing the line between civilian and military targets. On top of it, the ever increasing use of non-military infrastructure by the military, in the cyber space, makes it even difficult to apply this principle.

3.1.4 Indiscriminate Weapons

Under LOAC, since the first World War, ban of weapons that can cause damage beyond the intended target has been put into place. Hence, militaries using public internet for distribution of malicious code that damages non-combatant systems more than the combatant ones can be seen as violating this principle. Major issue with this principle is lack of general consent to what is a cyber-weapon.

3.1.5 Perfidy

This principle is designed to oversee targeting of some specific sanctuaries that are historically considered as legal and thereby regulate false sanctuary markings by misusing their symbols and/or locations on the military map. Similar thing can be done in the cyber space as well. for example, a nation state re-branding a military supply chain portal with Walmart logos, which is a violation of this principle.At the same time, it should be ensured that clear demarcation is made around critical systems concerning hospitals, telecommunication center, power grids in the cyberspace to save them from hostile cyber attacks.

3.1.6 Neutrality

The principle came into existence to safeguard states that willingly seek immunity from the attack by holding back support for any side during open hostilities. However, in a highly globalised and networked cyber world, it becomes very difficult to apply this principle. This is because it is hard to apply territoriality standard to cyberspace and most cyber attacks when staged on the internet may make use of network infrastructures of multiple countries. Take a hypothetical example, suppose a nation state orchestrated a military sanctioned DOS attack on a known enemy via the internet, wherein the TCP/IP packets can flow from both neutral and allied countries and hence a nation can risk its neutral status in such a case.

4 Solution Architecture

Since a smart grid involves bidirectional data transfer and routing, it makes it very lucrative target for DoS attack. A DoS attack on smart grid has the potential to target all the sections, from generation, transmission, distribution to consumption. Out of these, a DoS attack might exploit the vulnerabilities with respect to the communication protocols peculiar to the utility companies. For example, as stated in [3] the networking protocol, IEC 61850 used for substation automation runs on top of TCP/IP and hence inherits all the

vulnerabilities from the internet domain. Another example is the DoS attack on an Advanced Metering Infrastructure(AMI) network wherein attackers use IP Spoofing to carry out the attack. They spoof the victim's IP address and send packets to many unsuspecting destinations with victim's address spoofed as the source address. This results in destinations flooding the victim with a huge amount of unwanted traffic. This makes it unavailable for a significant duration for the legitimate traffic. There are seven technique categories that a DoS attack may utilise as shown in Figure 2: Signal jamming which is done at the physical level to deny, delay, or degrade an information service. Resource exhaustion DoS targets a device/network. In a cryptographic DoS attack, a message authentication code that was used to avoid data corruption can be used to trigger a DoS attack as stated in [4]. Data manipulation, false data injection may also be used as techniques for DoS attack. A false data injection scenario can also disturb the Automatic Voltage Control(AVR) as seen in [5]. Even a compromised smart meter has the potential to inject a variety of different attacks in Neighbourhood Area Network(NAN). Smart grids are also susceptible to routing -based DoS attacks, such as the sybil, wormhole, blackhole and puppet attacks.

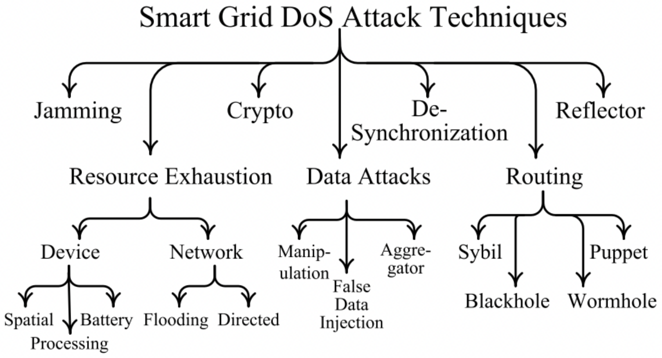

Figure 2: Classification of DoS attack techniques in the smart grid

A final classification of DoS attacks on the basis of techniques employed can be seen in Figure 2.

4.1 Solutions

4.1.1 Filtering

Filtering or "packet dropping" means dropping packets on a network device if identified not being legitimate. Filtering, in traditional sense

was applied on perimeter devices such as firewalls, however this cannot save the smart grid network from insider attacks, for example, a malicious devices inadvertently deployed inside the trusted perimeter by an organisation's own personnel. For this principle, filtering could be implemented at multiple locations such as on the network path and in the local host itself. In principle, filtering is the most effective when applied closest to the attack source. This is because it minimises the bandwidth consumption of the DoS traffic in the network.

In [6], the authors elucidate design of a firewall to secure smart grid communication in a multlihop wireless network. The basic principle behind this solution was the ability of a node to report the intruder to its neighbouring nodes by raising a prealarm that makes the other nodes move the intruder out of the whitelist of trusted hosts. Hence, Bump-in-the-firewall can be considered to be the most viable option for legacy and/or low-endpoint devices in smart grid.

4.1.2 Intrusion Detection System(IDS)

There are basically three broad categories of IDS: (1) signature based detection which lies on signature database available, (2) anomaly based detection, it involves training the system with normal behaviour and detecting any deviations; (3)specification based detection: it is based on specifications that capture illegitimate behaviour.

Since a DoS attack includes deviation of statistics of the monitored traffic, thus a suitable detector with low false positive rate can be built. However, this also does not ensure reliable discrimination of malicious from legitimate flash event.

In [7], it was observed that signature based approach have limited effectiveness in smart grid deployments due to difficulty in designing accurate signatures for DoS attacks. Hence, deployments of specification becomes easier in use cases where homogeneous behaviour is involved, as in our case. The authors elaborated as to how device level state machine for smart meters could guide a set of valid behaviours monitored by the IDS sensors. In other research paper[8], the authors applied the idea of specification based detection to multi cast messages(SV and GOOSE) in a substation network that reported a low false negative ratio.

4.1.3 Cryptographic authentication

In a scenario of an attacker indirectly disrupting the services by injecting erroneous messages and commands, cryptography can be used to detect and reject unauthorised messages injected by outsiders. However, it should be kept in mind that even the use of cryptography can be a target for DoS attacks. If the verification of the authenticity of a packet consumes a significant amount of resources, then a attacker can take the advantage of this situation to launch a successful attack by the use of bogus packets. Hence designing cryptographic protocols to resist resource exhaustion is a difficult job and its efficiency matters the most even if a modest amount of resources are expended in a normal operation[9]. He et al. considered use of PKI-supported entity authentication verification in the smart grid. They considered the use of a lightweight polynomial based verification mechanism. The paper did not use certificate verification and signature verification as they could be the target of DoS attack. The major challenge posed by cryptographic solutions to smart grid is the problem of scalability and key management, hence to resolve these a standard PKI-based solution for the internet communication can be tailored as per the smart grid environment.

4.1.4 Protocol Solutions

The fact that internet protocols such as IP and UDP/TCP were not designed with security in mind, this results in majority of security problems we have today. On the other hand, if we use communication protocols which are not inherited from internet such as DNP3, they do not score much better. Henceforth, these are security protocols under development which deal with detecting DoS attacks along with other security requirements such as in IEC 62351 [10]. There are also some proposed solutions that resist some specific DoS attacks while staying compatible to the standard, like SYN cookies provide a solution to TCP SYN flood attacks using cryptographic hashing techniques. There is a dire need to design protocols for smart grids devices with long lifetime, which have the ability to updates or modified so that secure continued operation is ensured for a long period of time[11].

4.1.5 Rate Limiting

Blocking of DoS traffic is the next step after the identification of the attack source in the attack reaction process. There are two main challenges to this in IP4 networks: (1) Having no cyrptographic protection, source addresses can be easily forged. (2) Routers only know the next hop while forwarding a packet, hence it is difficult to trace packet back to its source[12].

A naive reaction can be to increase host and network resources or make the resource management more efficient. Rate limiting and fair

scheduling are fairly reliable DoS mitigation strategies, in the case where making distinction between DoS traffic and legitimate one is difficult. Rate limiting could be implemented physically on a perimeter device such as reverse firewall or logically on the server machines. even, well known CAPTACHAs can be considered a rate limiting tool for applications involving human interaction. The disadvantage with rate limiting is that attack traffic although limited is still allowed. More intelligent strategies can also be employed by exploiting the fact that data transmission in smart grid application is periodic, like the frequency of metering reporting is ¡1Hz [13], thus a higher rate is suspicious and could be limited without any side effect.

5 References

1. S. Sridhar, A. Hahn and M. Govindarasu, "Cyber–Physical System Security for the Electric Power Grid," in Proceedings of the IEEE, vol. 100, no. 1, pp. 210-224, Jan. 2012, doi: 10.1109/JPROC.2011.2165269.

2. A treaty for cyberspace - JSTOR. (n.d.). Retrieved June 22, 2022, from https://www.jstor.org/stable/40664079

3. B. Moussa, M. Debbabi, and C. Assi, "A detection and mitigation model for PTP delay attack in an IEC 61850 substation," IEEE Trans. Smart Grid, vol. 9, no. 5, pp. 3954–3965, Sep. 2018. [Online]. Available: https://ieeexplore.ieee.org/document/7797198/

4. V. Kolesnikov and W. Lee, "MAC aggregation protocols resilient to DoS attacks," IEEE SmartGridComm, vol. 7, no. 2, pp. 226–231, 2011. [Online]. Available: http://inderscience.metapress. com/index/XW8541375106697V.pdf

5. Y. Chen, S. Huang, F. Liu, Z. Wang, and X. Sun, "Evaluation of reinforcement learning-based false data injection attack to automatic volt- age control," IEEE Trans. Smart Grid, vol. 10, no. 2, pp. 2158–2169, Mar. 2019.

6. X. Wang and P. Yi, "Security framework for wireless communications in smart distribution grid," IEEE Trans. Smart Grid, vol. 2, no. 4, pp. 809–818, Dec. 2011.

7. R. Berthier and W. H. Sanders, "Specification-based intrusion detection for advanced metering infrastructures," in Proc. IEEE 17th Pacific Rim Int. Symp. Dependable Comput., Dec. 2011, pp. 184–193. [Online]. Available: http://ieeexplore.ieee.org/lpdocs/ epic03/wrapper.htm?arnumber=6133080

8. M. S. Kemal, W. Aoudi, R. L. Olsen, M. Almgren, and H.-P. Schwefel, "Model-free detection of cyberattacks on voltage control in distribution grids," in Proc. 15th Eur. Dependable Comput. Conf. (EDCC), Sep. 2019, pp. 171–176.

9. V. Kolesnikov and W. Lee, “MAC aggregation protocols resilient to DoS attacks,” IEEE SmartGridComm, vol. 7, no. 2, pp. 226–231, 2011. [Online]. Available: http://inderscience.metapress. com/index/XW8541375106697V.pdf

10. C. Rosinger and M. Uslar, “Smart grid security: Iec 62351 and other relevant standards,” in Standardization Smart Grids. Berlin, Germany: Springer, 2013, pp. 129–146.

11. H. Khurana, R. Bobba, T. Yardley, P. Agarwal, and E. Heine, “Design principles for power grid cyber-infrastructure authentication protocols,” in Proc. 43rd Hawaii Int. Conf. Syst. Sci., 2010, pp. 1–10.

12. T. Peng, C. Leckie, and K. Ramamohanarao, “Survey of network-based defense mechanisms countering the DoS and DDoS problems,” ACM Comput. Surveys, vol. 39, no. 1, p. 3, Apr. 2007.

13. W. Wang and Z. Lu, “Cyber security in the smart grid: Sur- vey and challenges,” Comput. Netw., vol. 57, no. 5, pp. 1344–1371, Apr. 2013. [Online]. Available: http://www.sciencedirect.com/science/ article/pii/S1389128613000042