Concordia Institute for Information System Engineering (CIISE)

Concordia University

INSE 6640: Smart Grids and Control System Security

Assignment -1

Submitted to:

Dr. Jun Yan

Submitted By:

Sai Chandra Sekhar Reddy Dwarampudi - 40139233

Assignment #1 (**100 points**): Due 11:59 pm, Friday, October 21, 2022

1. (**10 points**) The peak load of a power grid refers to the highest load demand seen during a certain period. The table below shows the weekly peak load in a regional power grid, in terms of the percentage with respect to the peak load of the entire year: for example, the peak load observed in Week 1 is 86.2% of the peak load observed over the entire year. Weeks 1-8 and 44-52 are in the winter, weeks 9-17 are in the spring, weeks 18-30 are in the summer, and weeks 31-43 are in the fall. Answer the following questions.

Week	Peak load (%)	Week	Peak load (%)	Week	Peak load (%)	Week	Peak load (%)
1	86.2	14	75.0	27	75.5	40	72.4
2	90.0	15	72.1	28	81.6	41	74.3
3	87.8	16	80.0	29	80.1	42	74.4
4	83.4	17	75.4	30	88.0	43	80.0
5	88.0	18	83.7	31	72.2	44	88.1
6	84.1	19	87.0	32	77.6	45	88.5
7	83.2	20	88.0	33	80.0	46	90.9
8	80.6	21	85.6	34	72.9	47	94.0
9	74.0	22	81.1	35	72.6	48	89.0
10	73.7	23	90.0	36	70.5	49	94.2
11	71.5	24	88.7	37	78.0	50	97.0
12	72.7	25	89.6	38	69.5	51	100.0
13	70.4	26	86.1	39	72.4	52	95.2

(Reference: IEEE Reliability Test System (RTS) - 1996)

   a. Which weeks have the highest and lowest peak load of the year? If the annual peak load is 2,850 MW, what are the average peak loads (in MW) of the winter weeks and the summer weeks, respectively?
   b. If the annual peak load is 2,850 MW and we have two power plants whose capacities (maximal generation power) are 1,500 MW and 1,000 MW, respectively. During the week with the highest peak load, how much extra power generation capacity (in MW) do we need to meet the peak load of the year? During the week with the lowest peak load, at least how much power generation capacity (in MW) would be in idle?

Answer:

a. As per the given table,

Highest peak load was observed on **Week 51** with a load of **100%.**

Lowest peak load was observed on **Week 38** with a load of **69.5%.**

Given the values

Annual peak load = 2850MW, Winter weeks are from Weeks 1-8 and 44-52

Week	**Winter peak load (%)**	Calculations	Values
1	86.2%	(86.2%*2850)/100	2456.7
2	90%	(90%*2850)/100	2565
3	87.8%	(87.8%*2850)/100	2502.3
4	83.4%	(83.4%*2850)/100	2376.9
5	88%	(88%*2850)/100	2508
6	84.1%	(84.1%*2850)/100	2396.85

7	83.2%	(83.2%*2850)/100	2371.2
8	80.6%	(80.6%*2850)/100	2297.1
44	88.1%	(88.1%*2850)/100	2510.85
45	88.5%	(88.5%*2850)/100	2522.25
46	90.9%	(90.9%*2850)/100	2590.65
47	94%	(94%*2850)/100	2679
48	89%	(89%*2850)/100	2536.5
49	94.2%	(94.2%*2850)/100	2684.7
50	97%	(97%*2850)/100	2764.5
51	100%	(100%*2850)/100	2850
52	95.2%	(95.2%*2850)/100	2713.2
	Total		43325.7
	Average = Total/ Number of Weeks (17)		2548.570588

The average peak load in winter is **2548.57 MW**

Summer weeks range from week 18-30.

Week	**Winter peak load (%)**	Calculations	Values
18	83.7%	(83.7*2850)/100	2385.45
19	87%	(87*2850)/100	2479.5
20	88%	(88*2850)/100	2508
21	85.6%	(85.6*2850)/100	2439.6
22	81.1%	(81.1*2850)/100	2311.35
23	90%	(90*2850)/100	2565
24	88.7%	(88.7*2850)/100	2527.95
25	89.6%	(89.6*2850)/100	2553.6
26	86.1%	(86.1*2850)/100	2453.85
27	75.5%	(75.5*2850)/100	2151.75
28	81.6%	(81.6*2850)/100	2325.6
29	80.1%	(80.1*2850)/100	2282.85
30	88%	(88*2850)/100	2508
	Total		31492.5
	Average = Total/ Number of Weeks		2422.5

The average peak load in summer is **2422.5 MW**

b. Given the values

Annual peak load = 2850 MW

Highest peak load was observed on week 51 with 100%

=> 100% of annual peak load

=> 100% of 2850 MW = 2850 MW

Lowest peak load was observed on week 38 with 69.5% => 69.5% of annual peak load

=> 69.5% of 2850 MW = 1980.75 MW

Total power generation of 2 power plants = 1500 + 1000 MW = 2500 MW

Extra power required to meet the requirements of the highest peak week (week 51)

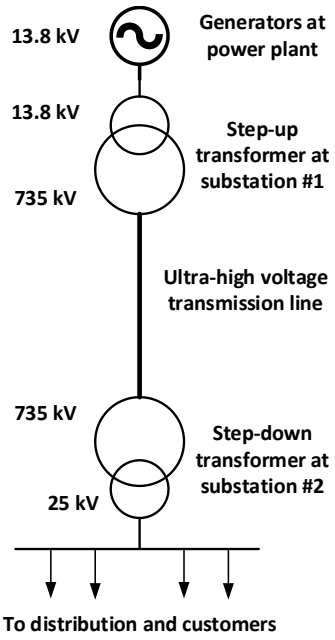
= 2850 – 2500MW

= 350 MW

Excess power generated during the lowest peak week (week 38) = 2500 – 1980.75 MW

= 519.25 MW

2. (**15 points**) The figure on the right shows an abstract model of power transmission grids in Quebec, where the ultra-high voltage transmission line has a rated voltage of 735 kilovolts (kV). The Ohm's law states that the active power consumption at the end of the line is $P = UI$ and the active power loss along the line $P_{loss} = I^2R$, where U, I, and R are the rated voltage, line current, and line resistance, respectively. Assume that the active power consumption at substation #2 is $P = 1{,}000\ MW$.
   a. If the 735-kV line is 100 kilometers long with a resistance of 0.5Ω per kilometer, what is the active power loss along the line according to the Ohm's law? Show your result in megawatts (MW). If the rated voltage of this line is reduced from 735 kV to 315 kV (the length and resistance remain the same) what is the active power loss along the new 315-kV line?
   b. According to recent data, the average power consumption of a household in Quebec is 1.9 kilowatts (kW); the average charging demand of an all-electric vehicle over a common 120 V outlet is 1.4 kW. When increasing the rated voltage from 315 kV to 735 kV, the saved active power loss can power up how many households in Quebec? How many all-electric vehicles?



Answer:

a. Given the values,

Rated Voltage U=735KV = 735000 V

Active power consumption P = 1000 MW = 1000 * 10^6 V

P = UI where U is rated voltage, I is the current and P is the Active power consumption

=> I = P / U => I = 1000 * 10^6 / 735000

=> I = 1360.544 Amps

Given resistance of wire is 0.5 Ω per kilometer, since total length is 100 KM then

total resistance is 0.5 * 100 = 50 Ω

Active power loss $P_{loss} = I^2 * R = (1360.544^2) * 50 = 92553998.8$ W

$P_{loss} = 92.55$ MW

Given the value of rated voltage can vary from 715kV to 315kV

U = 315kV

We already know that P = UI

=> I = P / U => I = 1000 * 10^6 / 315000

=> I = 3174.6 Amps

Total resistance is 0.5 * 100 = 50 Ω

Active power loss $P_{loss} = I^{\wedge 2} * R = (3174.6^2) * 50 = 503904265.8$ W

$P_{loss} = 503.9$MW

b. Given the values of

Average charging demand of all-electric vehicles is 1.4 kV over the common 120 V outlet.

For the rated voltage U = 735 kV the P_{loss} is 92.55 MW

For the rated voltage U = 315 kV the P_{loss} is 503.9MW

So due to the variation in the rated voltage the active power loss = 503.9 - 92.55 MW

= 411.35 MW

Total number of households that can utilize the saved active power loss = 411350 kV / 1.9

= 216500 households

216500 households can be powered by utilizing the saved power

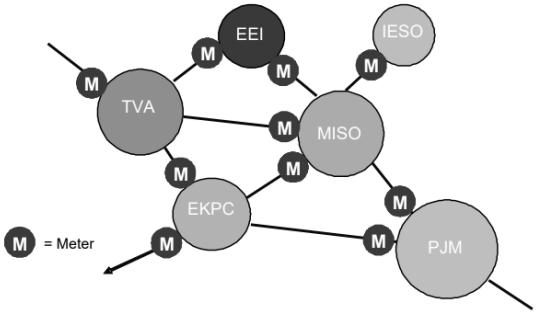
Total number of vehicles that can utilize the saved active power loss = 411350 kV / 1.4

= 293821.43 vehicles

Approximately **293821** vehicles can be powered by utilizing the saved power.

3. (**15 points**) The diagram shows some of the interconnected balancing authorities (Bas) in North America, where the grid frequency is 60 Hz. Recall that the area control error (ACE) is calculated by:

$$ACE = (NI_a - NI_s) - \beta(f_a - f_s) - \epsilon$$



In practice, the power flowing into a grid (generation P_{gen} and purchase P_{import}) is often assigned a negative sign, and that out of a network (consumption P_{load} and sales P_{export}) is assigned a positive sign. With this notion, we shall rewrite the power balance equitation as:

$$P_{gen} + P_{load} + P_{import} + P_{export} = 0.$$

Note that this is slightly different from our lecture notes, where $P_{gen} + P_{import} = P_{load} + P_{export}$.

Assume the active power generated or flowing into a BA is negative, and the active power consumed or flowing out of a BA is positive. Assume that the frequency bias β of **IESO** is -500 MW/Hz, and that the meter is error free ($\epsilon = 0$).

Answer the following questions:

RTO/ISOs:

- **IESO**: Independent Electricity System Operator (Ontario)
- **MISO**: Midcontinent Independent System Operator (Manitoba and multiple mid-west and southern states in the US)
- **PJM**: Pennsylvania-New Jersey-Maryland Interconnection LLC (13 eastern states/districts in the US)

Local Utilities:

- **TVA**: Tennessee Valley Authority (7 southeastern states in the US)
- **EEI**: Electric Energy, Inc (Illinois)
- **EKPC**: East Kentucky Power Cooperative, Inc. (Kentucky)

Source: "Balancing and Frequency Control" by the NERC Resources Subcommittee

a. Assume that IESO has NOT scheduled to purchase any electricity from MISO. According to the tie line meter, the actual NI between MISO and IESO is zero; the actual frequency of IESO is 60.01 Hz. Find the ACE of IESO. How shall we adjust the generation according to ACE?

b. Assume that IESO has scheduled to purchase 100 MW from MISO. According to the tie line meter, the actual NI between MISO and IESO is -110 MW; the actual frequency is 60.01 Hz. Find the ACE of IESO. How shall we adjust the generation according to ACE?

c. Assume an attacker plans to manipulate the ACE, which can be done by injecting an error ΔNI to NI_a or injecting an error Δf to f_a. Find the expression of injected error to the ACE (Δx) using an equation with ΔNI, Δf, and β.

d. Consider the operation scenario in Question 1.b and the attack model in Question 1.c above. If an attacker only manipulated the actual NI by adding an NI error of $+20$ MW and the actual frequency 60.01 Hz was reported accurately, what is the perceived ACE after manipulation? If an attacker caused an ACE error of -1 MW by only manipulating the actual frequency, what was the frequency error added by the attacker?

Answer:

a. Given the values,

Frequency of the grid f_{MISO}= 60 Hz
Frequency Bias of **IESO** $\beta = -500$ MW/Hz
Meter is error free $\epsilon = 0$
Power flowing into a grid P_{gen} + P_{import} is a negative sign
Power flowing out of a network P_{load} +P_{export} is positive sign
Given $P_{gen} + P_{load} + P_{import} + P_{export} = 0$

As per the tie line meter, the actual NI between MISO and IESO is zero which means NI_{MISO} = 0 and NI_{IESO} = 0.

Frequency of IESO f_{IESO} = 60.01 HZ

Area Control Error ACE of IESO => $ACE_{IESO} = (NI_{IESO} – NI_{MISO}) - \beta\ (f_{IESO} - f_{MISO}) – \epsilon$

$= (0 – 0) – (-500)\ (60.01 – 60) – 0$

$= 500 * 0.01 =$ **5 MW**

Power of 5MW is required to adjust the power generation at ACE.

b. Given that, IESO has scheduled to purchase 100 MW from MISO.
Actual NI between the MISO and IESO is – 110 MW which means $NI_{MISO} = 100$ MW and $NI_{IESO} = -110$ MW

The actual frequency $f_{IESO} = 60.01$ HZ and $f_{MISO} = 60$ HZ

Area Control Error ACE of IESO => $ACE_{IESO} = (NI_{IESO} – NI_{MISO}) - \beta\ (f_{IESO} - f_{MISO}) – \epsilon$

$= (-110 - 100) – (-500)\ (60.01 – 60) – 0$

$= -210 + 500 * 0.01$

$= -205$ MW

205 MW excess power is generated which can be adjusted according to generation in the ACE.

c. Given that, Attacker plans to manipulate ACE by injecting an error in ΔNI to NI_a (NI_{IESO}) or injecting an error Δf to f_a (f_{IESO}). The expression of injected error to the ACE (Δx) using an equation with ΔNI, Δf, and β is
Area Control Error ACE (Δx) = $\Delta NI - \beta\ (\Delta f) - \epsilon$

d. Given that,
Attacker can manipulate the actual NI by adding an NI error of ΔNI = +20 MW
The actual frequency f_{IESO} is 60.01 HZ
$NI_{IESO} = -110$ MW + 20 MW = -90 MW

$NI_{MISO} = 100$ MW, $f_{IESO} = 60.01$ HZ and $f_{MISO} = 60$ HZ
Frequency Bias of **IESO** $\beta = -500$ MW/Hz and $\epsilon = 0$

Area Control Error ACE of IESO => $ACE_{IESO} = (NI_{IESO} – NI_{MISO}) - \beta\ (f_{IESO} - f_{MISO}) – \epsilon$

$= (-90 - 100) – (-500)\ (60.01 – 60) – 0$

$= -190 + 500 * 0.01$

$= -185$ MW

Calculating the error added to the actual frequency which made the area control error ACE of IESO to -1 MW.

$$-1 = (-110 - 100) – (-500)\ (f_{IESO} – 60) – 0$$

$$-1 = -210 + 500\ f_{IESO} + 30000 – 0$$

$$500\ f_{IESO} = 30209 \Rightarrow f_{IESO} = 30209 / 500 = 60.42\ HZ$$

4. (**15 points**) Answer the following questions:
   a) List the two major interconnections and three minor interconnections in North America.

   b) In addition to Dragos and Nozomi Networks that were mentioned in our slides, identify three more industrial control system (ICS) security solution providers in the world. Show the names of the companies and the links to their home page in your answer.

   c) Create an account on Shodan.io, then follow the Explore => Industrial Control Systems => Protocols to identify which **port number** was used by this search engine to identify Internet-connected ICS devices communicating over the following protocols, respectively:
   1) Modbus; 2) DNP3; 3) IEC 60870-5-104 4) S7 (S7 Communication)

Answer:

a. Two major interconnections in the North America are
   - Eastern Interconnections
   - Western interconnections

   Three minor interconnections in the North America are

   - Quebec Interconnection
   - Alaska Interconnection
   - Texas interconnection

b. In addition to the Dragos and Nozomi Networks the following are some other industrial control system ICS security solution providers.
   - Scadafence (https://www.scadafence.com/)
   - BayShore Networks (https://bayshorenetworks.com/)
   - Attivo Networks (https://www.attivonetworks.com/)

c. Port Numbers used by the protocols are

Protocol	Port Number
Modbus	502
DNP3	20000
IEC 60870-5-104	2404
S7 (S7 Communication)	102

5. (**15 points**) In the false data injection (FDI) attack, assume that the normal measurement is $\mathbf{z} = \mathbf{Hx} + \mathbf{n}$ and the attacked measurement is $\mathbf{z_a} = \mathbf{z} + \mathbf{a}$. Assume that the weighted least square (WLS) solution is given by $\hat{\mathbf{x}} = \left(\mathbf{H^T R^{-1} H}\right)^{-1} \mathbf{H^T R^{-1} z}$ for the normal measurement $\mathbf{z}$, and let $\hat{\mathbf{x}}_\mathbf{a}$ be the WLS solution obtained from the attacked measurement $\mathbf{z_a}$. Use your linear algebra knowledge to prove that the pre-attack residual $\mathbf{r} = \mathbf{z} - \mathbf{H}\hat{\mathbf{x}}$ is the same as the post-attack residual $\mathbf{r_a} = \mathbf{z_a} - \mathbf{H}\hat{\mathbf{x}}_\mathbf{a}$ if $\mathbf{a} = \mathbf{Hc}$.

Answer:

Given that the False data injection attack is performed and the normal measurement is given by $z = Hx + n$.

Attack measurement $z_a = z + a$

Weighted least Square (WLS) solution => $\hat{x} = \left(H^T R^{-1} H\right)^{-1} H^T R^{-1} z$

pre-attack residual $\mathbf{r} = \mathbf{z} - \mathbf{H}\hat{\mathbf{x}}$ and post-attack residual $\mathbf{r_a} = \mathbf{z_a} - \mathbf{H}\hat{\mathbf{x}}_\mathbf{a}$ where a = Hc

From the post residual equation $r_a = z_a - H\hat{x}_a$ where $z_a = z + a$

WLS of the attack (WLS_a) $\hat{x}_a = \left(H^T R^{-1} H\right)^{-1} H^T R^{-1} z$ where z = z+a

$$\hat{x}_a = \left(H^T R^{-1} H\right)^{-1} H^T R^{-1} (z + a)$$

$$\hat{x}_a = \left(H^T R^{-1} H\right)^{-1} H^T R^{-1} z + \left(H^T R^{-1} H\right)^{-1} H^T R^{-1} a$$

$$\hat{x}_a = \hat{x} + \left(H^T R^{-1} H\right)^{-1} H^T R^{-1} a$$

Post-attack residual => $r_a = z_a - H\hat{x}_a$ where $\hat{x}_a = \hat{x} + \left(H^T R^{-1} H\right)^{-1} H^T R^{-1} a$

$$r_a = z_a - H\left(\hat{x} + \left(H^T R^{-1} H\right)^{-1} H^T R^{-1} a\right)$$

$$r_a = z_a - H\hat{x} - H\left(H^T R^{-1} H\right)^{-1} H^T R^{-1} a \text{ where } z_a = z + a$$

$$r_a = z + a - H\hat{x} - H\left(H^T R^{-1} H\right)^{-1} H^T R^{-1} a$$

$$r_a = z + a - H\hat{x} - H\left(H^T R^{-1} H\right)^{-1} H^T R^{-1} a$$

we know $H\left(H^T R^{-1} H\right)^{-1} H^T R^{-1} = 1$ (multiplication of a matrix and it's inverse = 1)

$$r_a = z + a - H\hat{x} - a \text{ (cancelling -a and +a)}$$

$$r_a = z - H\hat{x} = r = \text{pre-attack residual}$$

$$\text{Hence pre-attack residual} = \text{post-attack residual}$$

6. (**15 points**) Security is a fast-evolving area where professionals shall stay tuned for information from an array of credible sources. To answer this question, use an email of yours to subscribe to a total of five feeds from security agencies, organizations, firms, and/or researchers, all of which shall be related to topics in this course. Report your subscriptions in the table below (no need to submit proof of subscription). Make sure you subscribe to <u>at least</u> one newsletter from the

industry and one researcher/government agencies not in the industry. Feel free to add more lines in MS Word if needed.

Your email used for subscription	saichandrasekhar.dwarampudi@gmail.com		
Category	**Publisher**	**Publisher type**	**Starting date**
Example #1	Jun Yan	Researcher on Google Scholar	2022-10-17
Brief reason	Instructor of the course and researcher on cyber-physical security in the smart grid.		
Example #2	ICS-CERT alerts	Newsletter of a U.S. government agency	2022-10-17
Brief reason	Provides timely notification to critical infrastructure owners and operators concerning threats to critical infrastructure networks.		
Category	**Publisher**	**Publisher type**	**Starting date**
Subscription #1	SANS	Provides newsletters on latest advancements in security	2022-10-17
Brief reason	Provides semi-weekly, weekly and monthly reports about the important industry headlines and latest discovered attack vectors.		
Subscription #2	NIST	Newsletters related to various smart grids and cyber physical systems.	2022-10-17
Brief reason	Provides newsletters related to various NIST frameworks and various solution to prevent risks related to cyber security for all sizes of business.		
Subscription #3	Hacker News	Newsletters related to the security for not veteran programmers	2022-10-17
Brief reason	Hacker news contains large number of social media platform which are daily used can easily gain knowledge through them. They are sent daily basis.		
Subscription #4	Indian Government – Cyber and information security division	Government agency of India which is responsible cyber security wing.	2022-10-17
Brief reason	Provides information quarterly about the achievements of India in the field of security and about various cybercrime units, innovation centers and reporting portals.		
Subscription #5	We Live Security	Industry which provides various products like antivirus, malware and various security software.	2022-10-17
Brief reason	Provides reports on weekly basis based on the views and insights of industry professionals		

7. (**15 points**) Choose one ICS cyber security study or incidence from the following list, search for details via the links provided and from other online sources you can find, then formulate the attack model by summarize the details in the table below. (*Note*: Think about this as your personal note of what is going on While there is no "correct answer" here, you shall provide accurate, informative details, while keeping your answer as brief as possible. If any information was not given nor found, simply put "unspecified" in the corresponding blanks.)
   - **MaDIoT 2.0: Modern High-Wattage IoT Botnet Attacks and Defenses**
     https://www.usenix.org/conference/usenixsecurity22/presentation/shekari
     https://www.bitdefender.com/blog/hotforsecurity/madiot-iot-botnet-launch-major-attack-power-grid
   - **Compromise of U.S. Water Treatment Facility**
     https://us-cert.cisa.gov/ncas/alerts/aa21-042a
     https://www.cyberscoop.com/florida-water-facility-hack-password/
   - **Cyber Attack on the Ukrainian Power Grid**
     https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01
     https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf
   - **Hackers Remotely Kill a Jeep on the Highway**
     https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/
     http://illmatics.com/Remote%20Car%20Hacking.pdf
   - **Stuxnet targeting the Iran's nuclear-fuel enrichment program**
     https://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet
     https://www2.cs.arizona.edu/~collberg/Teaching/466-566/2012/Resources/presentations/topic9-final/report.pdf

Incidence	Compromise on U.S. water facility
Attacker/hacker	Unknown
Attack/report year	5th February 2021
Motive	There was no clear motive behind the attackers as the government did not receive any warnings from the adversaries. They simply increased the amount of sodium hydroxide, a caustic chemical. As per the assumptions, the adversaries performed the attack just to demonstrate their upper hand on U.S. government and create a damage to the public health.
Target	The target is the drinking water treatment facility in the Florida. The attackers have gained unauthorized access to the SCADA system using a desktop sharing software like the Team Viewer.
Vulnerability	The attackers identified several vulnerabilities in the systems in the plant like outdated windows operating system, poor passwords usage

	by the employees and no firewall. Moreover, most of the system share the same password which made the attackers work easy. Attackers exploited the vulnerabilities in the software called Team Viewer which was installed on various computers used to check the status to each operation in the facility through which attackers were able gain a remote access to the computers.
Tool	Team Viewer, a desktop sharing software became the pivotal point for the attackers to gain the remote access to the network. Social engineering attacks and several phishing campaigns were also made on the employees of the plant.
Method	The adversaries tried to gain the unauthorized access to the Supervisory Control and Data Acquisition (SCADA) by using a desktop sharing application called TeamViewer. The attackers gained remote access to various systems in the plant and increased the caustic chemical content without knowing the actual user of the system.
Impact	The raise in the sodium hydroxide content in the drinking water might have caused a severe impact on the public health. A person working in the treatment facility identified the change in the dosage amounts and corrected them even before the SCADA system identified it. Due to this the water treatment process remained unaffected and the plant continued to operate normally.