Ing. Dalibor Válek
Doc. Mgr. Ing. Radomír Ščurek, Ph.D.
Technical University of Ostrava

Utilization of graph theory in security analysis of power grid

Introduction

Within last fifty years was realized significant diversification of technical infrastructure from telegraph to internet. From wide point of view the electric network, traffic network and communication network make the foundation of all prosperous companies. Usually these networks are based on big amount of heterogeneous components characterized by complex dependences and relationships between them. To ensure its structural integrity, effectivity and reliability of network, it has to be taken into account its illegal acts security and terrorist protection.

Within last two decades extremely growed electricity consumption. It was caused mainly by the social-economic changes in eastern Europe. Directly proportional to energy consumption were newly built and expanded nuclear power plants as same as power plants producing electricity from renewable sources.

After the disaster at Fukushima nuclear power plant started in Europe discussions about safety of nuclear power plants and cosequences of the radioactive substances leak. If there would be reduced production of electricity from nuclear power plants in Europe, there would be significant shortfall in over year electric energy production. This shortfall should be covered with mainly electricity produced from renewable energy sources and fossil fuels plants. If this will happen there will mean very serious impact to energy security. If there would be a massive production of electricity from renewable energy sources, there would be much more opportunities to one-off impacts to the transmission system.

These hard predictable impacts are caused mainly by renewable sources, mainly caused by wind power plants. Wind power plants work on the opposite principle than conventional power plants because they supply electricity only in case of wind blowing.

DOI: 10.5604/18984509.1140884

ISSN: 1898-4509

During these large fluctuations of electricity transfers the important thing is having the robust electricity system which has to be resistance to damage of its particular components such as electrical wiring, transformers or power plants. Due to this it is necessary to have all particular components protected and secure them against the attacks of different crime or terrorist organizations. These attacks could cause blackout which could mean a very severe consequences to the human lifes and country economy. Therefore it will be increasingly important to deal with security measures on devices across our electricity system. With selection of the most important components can help utilization of graph theory which is described in this article.

1. Electricity system

All devices that provide electricity from the production to the final customer are the assets where its decommissioning can result in a threat of the electricity supply to the final consumer. Among the main devices in electricity system we can mention electrical grid, electrical stations and electrical wiring.

1.1. Electrical grid

Devices which are considered in the analysis are parts of the electrical grid. Electrical grid is the system of interconnected devices which are used for electricity transmission, transformation, distribution. Further devices are used for metering, controlling and another security systems and the power plants.

The transmission system is a system of devices which are used to transmit electrical energy with a voltage of 400kV and 220kV from the manufacturers to the power nodes. Distribution system transmits electrical energy with a voltage of 110kV and 22kV from the transmission system to the customers. Customers in this context are the cities, the factories and the households.

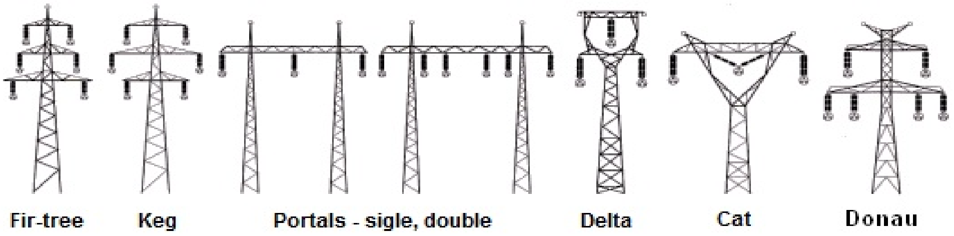
1.2. Electrical wiring

Voltage is transmitted by the different types of wiring. Usage of a specific wiring type depends on many factors such as quantity of the transmitted voltage, quantity of the transmitted electric current, voltage drop and so on. Wiring is most often outdoors but can also be cabeled on the ground or under ground but this is more expensive solution.

Outdoor wiring has to be resistant to weather changes, extreme weather conditions, humidity and it must have sufficient mechanical solidity to the intention damage. Cable wiring is used in residential areas, industrial areas and in the buildings.

Outdoor wiring is carried by electrical pylons. Construction of electrical pylons can be made of wood, reinforced concrete, steel or aluminum alloy. Many types of electrical pylons exist and the difference is mainly it their design of construction. Existing types of pylons are shown on the picture number 1.

Fig. 1. Types of pylon constructions



Source: *Internet encyclopedia of energy. Elektrizační soustavy*, http://www.energyweb.cz [2014-03-20].

Electrical pylons are designed from the construction point of view to resist extreme weather conditions and wind power. Instead of main cantilevered pylons, the grid consists of reinforcement pylons to ensure stability in case of wires break because without the main cantilevered pylons would not stay in the right position. These reinforcement pylons are made of special steel which can resists the climatic exposure (http://www.energyweb.cz, 2014).

1.3. Electrical stations

Electrical stations belong to electrical grid and are divided into transformations, switch stations and substations (http://www.energyweb.cz, 2014). Big part of these devices are created by the substations which can be a single building or a bounded area. These substations take care of the input and output electricity flow and they are consisted of conductors, insulators and switch, safety or control devices (http://en.wikipedia.org/wiki/Electrical_substation, 2014). In the buildings are mainly situated substations with voltage up to 35 kV and in the outdoor areas are situated substations with very high voltage over 52 kV.

2. Utilization of graph theory

Electrical wiring, telecommunication, transport infrastructure or others engineering network form system of nodes which make together graphs of different shapes with many degrees of complexity. Many networks are designed on the basis of landscape relief.

2.1. Graph characteristics

By the graphs we can represent a set of objects which we illustrate the interdependence of the various elements. Objects are assigned as vertices (power plants, transformers etc.) and their connections are called edges (transmission network, distribution network). Graph can be basically represented by simple model of a real network which emphasizes topological properties of objects and neglects their geometric properties.

Graphs can be devided as a directed and undirected. Undirected graph is defined as G = (V,E) where V indicates vertices and E indicates edges. In case of undirected graph we do not consider the order of vertices which is used in case electrical network analysis (Ochodkova, 2009, p. 20).

2.2. Graph theory

Given a connected graph G it is possible to devide it into two smaller graphs having roughly the same number of edges and vertices and one shared edge. There are many methods to achieve this. One is the Spectral graph Partitioning. This method involves the usage of Laplacian matrix and divide vertices of a connected graph G into two subgraphs by usage of Laplacian matrix eigenvectors (Slininger, 2013, p. 2).

2.3. Adjacency matrix

Graph can be represented by the adjacency matrix. It is defined as G, $A(G) = (a_{i,j})$

$$a_{i,j} = \begin{cases} 1, (i,j) \in E \\ 0, (i,j) \notin E. \end{cases}$$

This means that the adjacency matrix A represented by the graph G has for i-th row and j-th column value equal to 1 in case there is an edge between node *i* and *j*. Otherwise there is assigned value 0 for this possition.

2.4. Degree matrix

Other matrix defined by graph G is degrese matrix $D(G) = (d_{i,j})$

$$d_{i,j} = \begin{cases} d(i), & i = j \\ 0, & i \neq j. \end{cases}$$

Degree matrix is a diagonal matrix, which provides us information about degrese of each vertex – number of edges entering or exiting from concrete vertex. This matrix is used together with the adjacency matrix to create a Laplacian matrix.

2.5. Laplacian matrix

Laplacian matrix is another way how to represent graph. Matrix L(G) defined by graph G

$$L(G) = D(G) - A(G).$$

Laplacian matrix is difference between the degree matrix and adjacency matrix.

2.6. Spectral graph partitioning

Spectral graph partitioning is based on simple principle. For the graph G defined by vertices and edges G = (V,E) which has to be dividend is calculated Laplacian matrix L(G). By the spectral partitioning of Laplacian matrix are calculated eigenvalues and eigenvectors. Such an eigenvector which is related with the second smallest eigenvalue provides us required graph partitioning. This vector is named as a Fiedler's vector.

2.7. Algorithm for finding the most important electrical wirings

Input parameter of the algorithm to calculate the most important electrical wirings is adjacency matrix. Values of single rows and columns of the adjacency matrix are the inputs given by user according to the power lines map. These values are loaded into Excel and then exported to computer program.

Computer program then calculate from adjacency matrix the degree matrix and Laplacian matrix followed by spectral graph partitioning and finding the requiered Fiedler's vector.

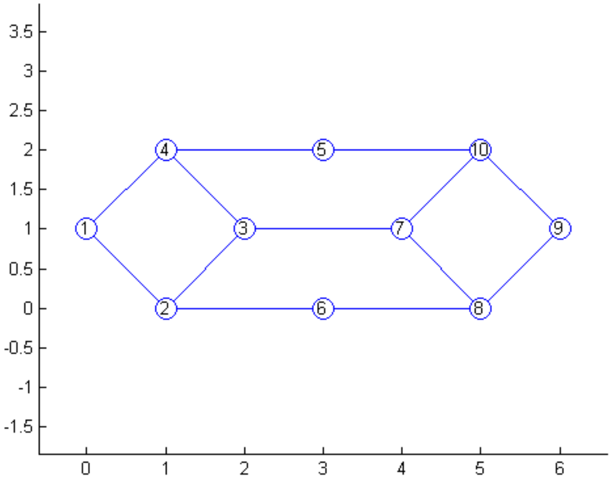
Distribution of final graph is determined by the sign related to Fiedler's vetor. Vertices with possitive numbers are assigned to first part of graph and vertices with negative numbers are assigned to second part of graph. As a most important power line is then selected line which connects both parts of graph.

2.8. Example of spectral graph partitioning

To illustrate the above theory is shown a very simple example of spectral graph partitioning.

Given a simple network of ten vertices and eleven edges. To the single vertices are assigned coordinates to display them in program according to its potential deployment in the territory.

Fig. 2. Example of simple graph



Accodring to picture 2 is designed adjacency matrix where single rows and columns are valued on the basis of existence the edges between single vertices.

Tab. 1. Adjacency matrix

	j=1	*j*=2	*j*=3	*j*=4	*j*=5	*j*=6	*j*=7	*j*=8	*j*=9	*j*=10
i=1	0	1	0	1	0	0	0	0	0	0
i=2	1	0	1	0	0	1	0	0	0	0
i=3	0	1	0	1	0	0	1	0	0	0
i=4	1	0	1	0	1	0	0	0	0	0
i=5	0	0	0	1	0	0	0	0	0	1
i=6	0	1	0	0	0	0	0	1	0	0
i=7	0	0	1	0	0	0	0	1	0	1
i=8	0	0	0	0	0	1	1	0	1	0
i=9	0	0	0	0	0	0	0	1	0	1
i=10	0	0	0	0	1	0	1	0	1	0

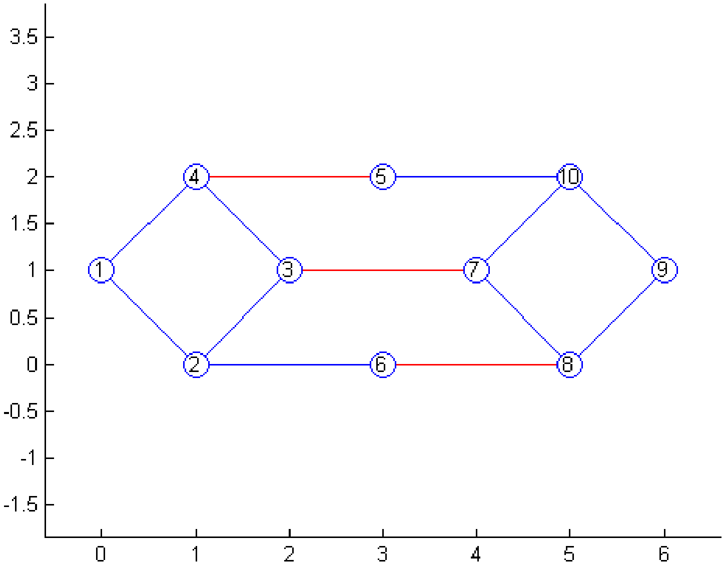
From adjacency matrix we can get according to defined equation the Laplacian matrix and Fiedler's vector related to the second smallest eigenvalue.

Tab 2. Laplacian matrix and related Fiedler's vector

											Fiedler´s vector	Vertices number
2	-1	0	-1	0	0	0	0	0	0		0.5117	1
-1	3	-1	0	0	-1	0	0	0	0		0.3162	2
0	-1	3	-1	0	0	-1	0	0	0		0.1954	3
-1	0	-1	2	-1	0	0	0	0	0		0.3162	4
0	0	0	-1	2	0	0	0	0	-1		-0.0000	5
0	-1	0	0	0	2	0	-1	0	0		0.0000	6
0	0	-1	0	0	0	3	-1	0	-1		-0.1954	7
0	0	0	0	0	-1	-1	3	-1	0		-0.3162	8
0	0	0	0	0	0	0	-1	2	-1		-0.5117	9
0	0	0	0	-1	0	-1	0	-1	3		-0.3162	10

Fiedler's vector divides the network into two approximately equal parts. Positive values of vertices are part of the first portion and negative values of vertices are part of the second portion. Red marked edges displayed on the picture number 3 represent the smallest amount of edges between both network parts. If we bring this situation into the electrical grid environment so we talk about electrical lines in which its failure mean blackout on the largest possible area.

Fig. 3. Selection of the smallest number of edges



Graph theory and its spectral graph partitioning is able to select the most important power lines. Then we can use conventional risk analysis only on the selected components of transmission and distribution network.

3. Analysis of attack on the electricity system

For consideration of vulnerability of single objects in the electricity system can be used modified method FMEA. This method was modified by the author to be more suitable

for consideration of illegal acts. Further in the article will be represented analysis named by shortcut FMEAIA (Failure Model and Effect Analysis of Illegal Acts).
Classic FMEA method is most commonly used in automotive industry to search and evaluation of potential defects in processes and products (http://www.pqm.cz/NV CSS/fmeacs.html, 2014). Level of risk is determined by the multiplying of subjectively evaluated coefficients which are Occurence „O“, Severity „S“, Detection „D“ and in additional in FMEAIA analysis is Appeal „A“ and Accessability „AA“. Level of risk is calculated according to formula $R = \frac{O \cdot S \cdot D \cdot A}{AA}$
Values of each coefficient may vary from 1 to 10 according to bellow mentioned table 3.

Tab. 3. Classification of each coefficient

	O	S	D	A	AA
Evaluation 1	Low probability	Low severity	Very easily detectable	Not very appealing to attack	Easily accessible
Evaluation 10	Very high probability	Very high severity	Almost impossibly detectable	Very appealing to attack	Almost unaccessible

In evaluation process of the electricity system we should start with the selection of the most important places given from Spectral graph partitioning method described above. Seleceted devices placed on calculated territory should be considered in the analysis according to above described method of FMEAIA.

Example of analysis procedure according to FMEAIA method can be used as follows:

1. Distribution of system into the devices in terms of production and in term of the electricity wiring.
2. Distribution of devices into the buildings, pylons, wiring and further devices which are fixed with the ground (for example wind power plants, photovoltaic power plant etc.).
3. Distribution into the further smaller technical devices.

Example of evaluation of several selected devices is shown in the table number 4.

Tab. 4. FMEAIA analysis

Purpose of device	Type of device	Specific device	Kind of attack	O	S	D	A	AA	R
Production	Thermal	Conveyor belt	Overload	1	2	2	1	3	1,3
			Blockage	2	2	2	1	3	2,7
		Cooling tower	Bomb attack	2	6	1	6	7	10,3
			Air attack	1	6	1	6	7	5,1
		Boiler	Diversionary activities	3	5	3	4	6	30
	Nuclear	Cooling tower	Bomb attack	2	9	1	8	9	16
			Air attack	1	9	1	8	8	9
		Reactor	Diversionary activities	3	9	3	9	9	81
		Pump	Pump blockage	2	7	2	3	9	9,3
	Water	Turbine	Blockage	2	4	2	7	7	16
		Electric generator	Removal of wires	4	4	4	4	8	32
		Water feeder	Feeder blockage	3	3	4	6	7	30,9
		Drainage canal	Canal backfilling	3	3	3	6	8	20,3
	Wind	Rotor	Collision with aircraft	2	1	6	1	2	6
		Tower	Placing the bomb	1	1	8	1	1	8
		Electrical connection	Cutting the wires	3	1	8	2	3	16
		Control system	Disposal of computer equipment	3	1	8	2	3	16
	Solar	Photovoltaic panels	Damage by stones	6	1	8	1	2	24
		Wire jumpers	Cutting the wires Placing	5	1	7	1	2	17,5
		Substation	the bomb	2	1	7	12	2	7
			Removal of wires	5	1	7		3	23,3
Wiring	Transmission system	Outside wiring	Air attack	1	5	7	5	8	21,9
			Pressure load	3	7	6	4	9	56
		Underground wiring	Cutting the wires	4	7	5	4	7	80
			Fusion	3	7	6	6	4	189
		Steel pylon	Incision	4	7	7	7	3	457
			Undermining of foundation	3	7	4	6	5	101
			Placing the bomb	2	7	8	6	3	224
			Fusion	3	8	6	7	4	252
		Reinforced pylon	Incision	4	8	7	7	3	523
			Placing the bomb	3	8	8	6	3	384
	Distribution system	Outside wiring	Damage by constr. machine	4	5	3	2	2	60
			Cutting the wires	5	4	3	4	6	40
		Underground wiring	Ignition	5	4	2	5	2	100
			Incision	4	4	3	4	2	96
		Wooden pylon	Dent	3	4	3	4	2	72
			Undermining	2	4	2	3	3	16
			Intentional breakage	3	4	3	2	4	18
			Fusion	4	5	5	5	4	125
			Incision	3	5	5	5	3	125
		Steel pylon	Undermining	2	5	4	4	4	40
			Flection	2	5	4	4	5	32

There are many types of attacks which could be considered but for purpose of this this article were used only few attacks to better illustration of FMEAIA method.

On the basis of above analysis was found out that the highest value of risk has following attacks:

1. Incision of reinforced and steel pylon in transmission system.
2. Placing the bomb on the reinforced and steel pylon in terms of transmission system.
3. Pylon fusion by the welding machine.

4. Proposal of security measures

Procedure of risk evaluation is followed by the phase of security measures proposal on the highest risk evaluated devices. Security measures should be effective, economical and easily feasible. In general the principle ALARA should be considered in this case because this principle takes into account value of protected object and value of devices which protect this object.

For the minimalization of risk represented by the incision and fusion of reinforced and steel pylon in transmission system it is possible to apply measures which physically prevent contact with single pylon or make activity of attacker more uncomfortable and time prolonged. Among the suitable security measures we can classify:

- Usage of hardened steel for lower part of pylon construction.
- Concreting of pylon foundations up to heigh 2 meters above the ground level.
- The definition of perimeter around the pylon by the fence or barbed wire.

Proposed security measures are suitable to be realized mainly in terms of reinforced pylons which are included in grid of cantilevered pylons. Distance between cantilevered pylons of Donau type can be in suitable terrain 500 meters.

For the type of attack with bomb usage can be applied similar security measures like in case of the incision and fusion the pylon but in case of bomb attack it depends on the level of energy which will be released within the explosion.

Conclusion

In the article were described components which are included in the electricity system. Components used for the transmission and distribution of electric energy are connected into the network. This network can be understood as a vertices connected together with edges. In this case was used method of graph spectral partitioning to make selection of the most important power lines. After this selection we are able to consider components included in calculated territory with the conventional risk analysis. Applied risk analysis was modified by author from FMEA analysis to have more suitable analysis for the illegal acts. Two new coefficients were applied to this modified analysis – appeal and accessability. Due to this modification this FMEAIA analysis is more suitable for illegal acts consideration. The result from the analysis is that the most risky devices in terms of illegal acts are mainly devices for transmission of electric energy which have much better accessability then the devices for electricity production. Due to this conlusion it is necessary to select the most important devices in specific terrain. On these devices have to be applied security measures to reduce the risk of attack to acceptable level.

References

Internet encyclopedia of energy. *Elektrizační soustavy*, http://www.energyweb.cz [2014-03-20]

Internet encyklopedia Wikipedia, *Electrical substation*, http://en.wikipedia.org/wiki/Electrical_substation [2014-01-01]

Ochodková, E. (2009): *Graph algorithms*, Technical university of Ostrava – faculty of electrotechnics and informatics, Ostrava

Process Quality Management, *FMEA – Failure Mode and Effect Analysis*, http://www.pqm.cz/NVCSS/fmeacs.html [2014-03-20]

Slininger, B. (2013): *Fiedler´s Theory of Spectral Graph Partitioning*, University of California, http://www.cs.ucdavis.edu/~bai/ECS231/returnsfinal/Slininger.pdf

Dalibor Válek
Radomír Ščurek

Utilization of graph theory in security analysis of power grid

Abstract

This paper describes way how to use graph theory in security analysis. As an environment is used network of power lines and devices which are included here. Power grid is considered as a system of nodes which make together graph (network). On the simple example is applied Fiedler's theory which is able to select the most important power lines of whole network. Components related to these lines are logicly ordered and considered by author´s modified analysis. This method has been improved and optimalized for risks related with illegal acts. Each power grid component has been connected with possible kind of attack and every of this device was gradually evaluated by five coefficients which takes values from 1 to 10. On the coefficient basis was assessed the level of risk. In the last phase the most risky power grid components have been selected. On the selected devices have been proposed security measures.

Key words: *Security, matrix, power grid, graph*

E-mail contact to the Authors: dalikk@email.cz