# Modeling Interdependencies with Complex Network Theory in a Combined Electrical Power and ICT System

Stine Fleischer Myhre
*Dept. of Electric Power Engineering*
*Norwegian University of Science and Technology (NTNU)*
Trondheim, Norway
stine.f.myhre@ntnu.no

Olav Bjarte Fosso
*Dept. of Electric Power Engineering*
*Norwegian University of Science and Technology (NTNU)*
Trondheim, Norway
olav.fosso@ntnu.no

Poul Einar Heegaard
*Dept. of Information Security and Communication Technology*
*Norwegian University of Science and Technology (NTNU)*
Trondheim, Norway
poul.heegaard@ntnu.no

Oddbjørn Gjerde
*SINTEF Energy Research*
Trondheim, Norway
oddbjorn.gjerde@sintef.no

Gerd Hovin Kjølle
*SINTEF Energy Research*
Trondheim, Norway
gerd.kjolle@sintef.no

***Abstract*—The extensive integration of information and communication technology (ICT) in the future electrical power system transforms the power system to a cyber physical system (CPS), making it a system-of-systems. This new system topology creates interdependent relationships between the cyber and the physical parts in the power system and introduces new possible vulnerabilities and risks which might lead to unwanted events such as outages and blackouts. For electrical power system operators, it is important to understand the new complexity of the system and how to address these new changes in order to ensure safe system operation and security of electricity supply. This paper focuses on the introduction of complex network theory as a method to discover and measure the importance of the system nodes, both electrical and ICT, in a combined electrical power distribution and communication network. There are two different methods used for measuring the importance, *1) betweenness centrality* and *2) node attack method*. The methods are evaluated through a case study and found suitable in capturing the important nodes in the combined electrical power and communication network.**

***Index Terms*—Complex network theory, graph theory, ICT, power system, security, smart grid, reliability**

## I. Introduction

Information and communication technology (ICT) systems are becoming an increasingly important part of the power systems and are predicted to be the key enabler for the future power systems [1]. The introduction of ICT lays the foundation for more intelligent power systems and the transition to smart grids. The smart grid vision aims to make the power systems more reliable, robust, efficient, flexible, and resilient [1] and by that increase the security of electricity supply. Through the implementation of the smart grid, a cyber layer will be added on the already existing power system, making the power systems cyber physical systems (CPS)—a system with behavior defined by both a cyber and a physical part—making it a system-of-systems, resulting in a more complex network structure [2]. In this new system topology, both the physical power system and the ICT system will depend on the other system's reliable service to function. This will create an interdependent relationship between the two sub-systems. As an example, some ICT systems needs electrical power in order to function while the power system needs the ICT system to function in order to monitor and perform correct operations. These new interdependencies can introduce new vulnerabilities in the system and expose the power system to new risks and threats, which have been seen in, e.g., the blackouts in North America and Europe in 2003 [3], [4].

For electrical power system operators, i.e., the distribution system operators (DSOs) and the transmission system operators (TSOs), it will be important to address these new changes in the power system and to understand the complexity of the new system configuration in order to ensure a safe operation of the system as well as the security of electricity supply. Security of electricity supply is defined as *"the ability of an electricity system to supply final customers with electricity"* [5], and can be classified into four groups 1) energy availability, 2) power capacity, 3) reliability of supply, and 4) power quality [6]. These classifications divide the security of electricity supply into energy availability (the ability to supply the energy demand), reliability of supply (the ability to supply the electrical power to the end-users), and power quality (the quality of the supplied power), where the responsibility might vary in different parts of the power system.

While power system reliability has long been an important topic of study and even though the electrical power system and the ICT system have been extensively studied separately, there is a lack of research related to interdependencies and reliability in the combined electrical power and ICT system. However, multiple studies have been conducted on classifying approaches for modeling interdependency in critical infrastructures [7]–[10]. These studies have revealed several methods

Funded by FME CINELDI - Centre for intelligent electricity distribution/Norwegian Research Council, C.no 257626/E20

This is the accepted version of an article published in PMAPS 2020
http://dx.doi.org/10.1109/PMAPS47429.2020.9183667

applicable to model interdependencies in a combined electrical power and ICT system. Some of these methods are agent-based methods [8], [10], cascading diagrams [8], Markov models and reliability block diagrams [11], [12], Petri nets [12], [13], and complex network theory [14].

This paper aims at presenting complex network theory as an appropriate tool for modeling interdependencies in the combined electrical power distribution and communication network with focus on measuring the importance of the nodes in the network based on paths and energy not supplied. Through this, the system operators are able to reveal possible vulnerabilities that might result in unwanted events such as blackouts. Complex network theory can also be used as a tool for analyzing criticality in possible future network development since it conveniently capture the networks topology.

The rest of this paper is organized as follows. Section II focuses on presenting the concept of graph theory and how this is applicable on the combined electrical power and ICT system. Section III presents the constructed network model as a case study. Section IV presents and discusses the results of the simulations done on the case study while the conclusion is presented in Section V.

## II. Complex Network Theory

Complex network theory is a concept based on graph theory where the graphs obtain non-trivial topologies, more complex structures, and can dynamically evolve in time [15]. The concept of complex networks and real world networks was initiated by Watts and Strogatz in 1998 on ”small-world networks” [16] and Barabási and Albert in 1999 on ”scale-free networks” [17]. This research established a starting point for investigating larger and real networks such as the electrical power system.

Complex network theory is a beneficial method for modeling the interdependencies in a combined electrical power and ICT system since it is able to capture the complex topology of the network. In addition, the network can easily be visualized and important parts of the system identified, resulting in a comprehensible model. In research, complex network theory has been used as a method to measure the reliability of the electrical power system. References [14], [18] review a high number of studies which uses complex network theory as a method to analyze the power system. Most of the research focus solely on electrical power systems, as in [19]–[21] while for CPS, often the cascading failure is in focus, as in [4], [22]. However, the majority of the studies focus on investigating the complexity in transmission grids and not distribution grids, where other criteria might hold for the system operation.

### A. Vertices and Edges

A graph $G$ is a pair of sets ($V$, $E$), where $V$ is the set of vertices and $E$ is the set of edges in the graph. The vertices $V = \{v_1, v_2, v_3, ..., v_n\}$, where n is the total number of vertices, can be represented as the system elements such as the system's nodes and routers. The edges $E = \{e_1, e_2, e_3, ..., e_m\}$, where m is the total number of edges, illustrate the connection between the different vertices and can be the power lines, communication links and optical fibers in the system. However, one could also have represented the vertices as power lines, communication links and/or optical fibers, making the edges the system nodes, depending on which elements aim to be investigated. In graph theory, one distinguishes between undirected and directed graphs, where the edges in the undirected graphs do not have any given direction unlike a directed graph. Fig. 1 and Fig. 2 illustrates an example of an undirected and a directed graph for a combined electrical power and ICT system, respectively.

For a combined electrical power and ICT system, the vertices can be divided into two sub-types, $V_e = \{v_{e1}, v_{e2}, v_{e3}, ..., v_{ep}\}$ and $V_c = \{v_{c1}, v_{c2}, v_{c3}, ..., v_{cq}\}$ (where p and q are the total number of electrical power and ICT nodes), based on whether the vertex is an electrical power node or an ICT node respectively. If relevant, these two sub-types can be further divided into new sub-types based on, e.g., the type of node (load bus, router node, base station node). The same approach can be conducted on the edges which can be divided into three or four different types dependent on if the graph is an undirected or a directed graph. The different types can be 1) electrical edge connecting electrical vertices, 2) ICT edge connecting ICT vertices, 3) electrical edge connecting an electrical vertex and an ICT vertex, and 4) ICT edge connecting an ICT vertex and an electrical vertex. Type 3 and 4 will be similar for an undirected graph. The division of vertices and edges into types helps classifying the interdependencies of the network.

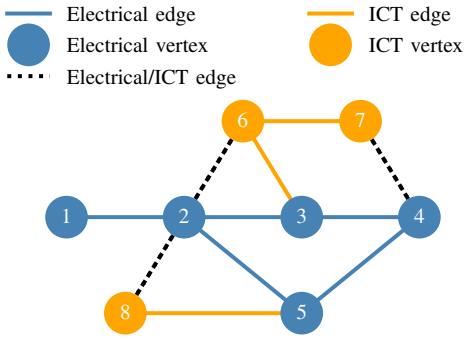


Fig. 1: Example of an undirected graph for a combined system

### B. Betweenness Centrality

In graph theory, centrality indicates the importance of a vertex in the graph. The importance of the vertex can be measured through different types of centrality where the most common measures are degree centrality, closeness centrality, and betweenness centrality [23].

Betweenness centrality is a measurement used to highlight the importance of the vertices in the system based on shortest paths. The importance of a vertex can then be decided based on crucial connections to other parts of the system, i.e., how important a specific vertex is for connecting different parts of the system. From the example in Fig. 1, if vertex 3 is removed

This is the accepted version of an article published in PMAPS 2020
http://dx.doi.org/10.1109/PMAPS47429.2020.9183667

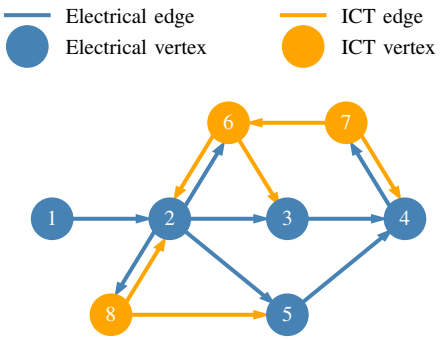


Fig. 2: Example of a directed graph for a combined system

from path 1-2-3-4, then the path between 1-2-5-4 will remain illustrating that vertex 3 is not crucial for the flow between vertices 1-4. However, if vertex number 2 is removed, then all paths from vertex 1 will be lost.

Betweenness centrality can be measured as in eq. (1), introduced by Freeman in [24]. Here, $\sigma_{ij}$ is the number of shortest paths between vertices *i* and *j* and $\sigma_{ij}(h)$ is the number of shortest paths between vertices *i* and *j* that passes through vertex *h*. For a combined electrical power and communication network, the betweenness centrality should be distinguished based on if the edges are electrical edges or communication network edges since the edges contain different flows.

$$b_h = \sum_{h \neq j \neq i} \left( \frac{\sigma_{ij}(h)}{\sigma_{ij}} \right) \tag{1}$$

The betweenness centrality will be different for undirected and directed graphs. For an undirected graph, the importance will be decided on the edges connecting the vertices. However, for a directed graph, the importance will be decided based on outgoing edges from the vertex.

Betweenness centrality will be the method of choice in this paper since this method is a reliable measure for illustrating the vertices' importance in combined electrical and communication network. This method emphasizes how a given vertex connects to the other parts of the system through shortest paths and will promote a vertex located on the majority of the possible paths in the network. However, betweenness centrality is unable to distinguish the vertices importance based on, e.g., energy not supplied.

### C. Node Attack Method

A *node attack method* can be applied on the combined network to investigate how the system manages when the systems nodes are removed. The aim of the method is to try to *destroy* as much as possible in the system. Through this, the survivability and operation of the system can be illustrated and measured. Similar methods have been used in other research as [4]. The proposed algorithm can be seen in Algorithm 1. The algorithm will first remove one vertex and then compute a power flow with this vertex removed before the vertex is placed back in the system and a new vertex is removed. For a DSO, it is important to ensure the security of electricity supply and prevent outages in the system, and the *node attack method* is a good strategy to investigate how the system will respond to different changes in the system. Another way of using the method is to take out one vertex without inserting it back in the system, in order to simulate how well and long the system is able to perform. For probabilistic analysis, the method can be applied with, e.g., failure rates and Monte Carlo simulations.

**Algorithm 1:** *Node attack method* algorithm

```
for vertex in vertices of system do
    Remove vertex in the system;
    Calculate power flow;
    Calculate total active power load in system;
    Calculate total active power loss over lines in
      system;
    Insert removed vertex again;
    Go to next vertex;
end
```

### D. Application of the Methods

Both methods are general methods that can be used on different network topologies. However, when considering typical radial operated distribution systems, the methods will be simplified since an outage of a node will cause all the down stream nodes to be lost if a generation unit is not present.

The goal is to investigate the importance of the system nodes through energy not supplied when using the *node attack method* and compare it with the betweenness centrality of each node. The node importance can then be decided based on the percentage of energy not supplied in the system when a certain node is removed. Nodes where the percentage of energy not supplied is high can be assumed to be of great importance. Additionally, the percentage of the active power losses in the network can be calculated in order to investigate how the power flows in the network. Besides, this result can further be used to investigate possible capacity problems the network might encounter, where a high percentage illustrates a higher network loss.

## III. Combined Electrical Power and ICT Network

### A. Test System

The test system is a distribution system with 22 nodes, based on the distribution power system presented by Baran and Wu [25], with some modifications and a constructed ICT layer. The combined electrical power and communication network is illustrated in Fig. 3. The distribution system has 22 power nodes, 22 power lines, 21 loads, and one HV/MV transformer placed at the slack bus (node 1). No generation is added to the distribution network, but it could be integrated. The loads are not distinguished hierarchically, but the total amount of active power drawn at each node might be different.

In addition to the traditional power system, the communication network is constructed by 22 remote terminal units (RTU), one at each power system node, 14 mobile base stations, and

This is the accepted version of an article published in PMAPS 2020
http://dx.doi.org/10.1109/PMAPS47429.2020.9183667

9 routers constructing a router link, where node 37 is a super router connecting to the control center.

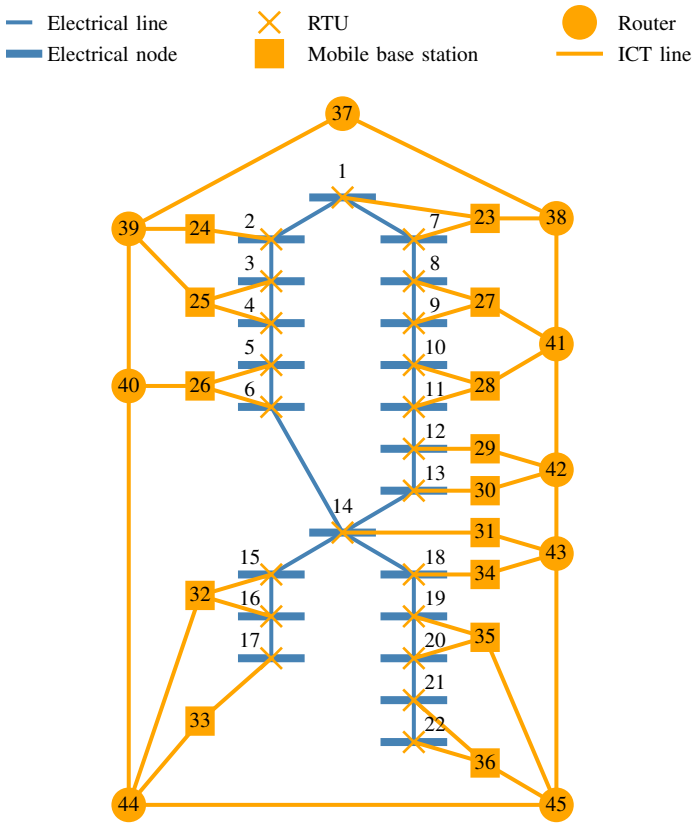


Fig. 3: The combined electrical power and communication network

### B. Modeling of the Network

In the model, the electrical power and communication network nodes were constructed as the network's vertices, while the electrical power lines/cables and the communication links were constructed as the edges of the network. This was done in order to investigate the importance of the system nodes, but could similarly be constructed to investigate important lines in the system. Fig. 3 is an undirected graph representation of the combined network. A directed graph representation of the electrical power system was achieved with a power flow analysis, while the communication lines are assumed to go in both directions since the electrical nodes are able to send data while receiving control signals from the control center.

Since node 1 is connected to the overlying HV network and node 37 is connected to the control center, an outage in these nodes will result in a total blackout of the whole combined system. When an outage on a node happens, the lines connected to the node will likewise fail and if a communication network node fails, it is assumed that an outage of the electrical nodes connected to the communication network node will occur since the node is unable to receive or send signals.

It is assumed that all the mobile base stations and routers have backup power in case of temporary blackouts. Therefore, the electrical link between an electrical node and a communication network node is not considered in this system. This is applicable for short duration power outages where an outage of the supplying electrical node will enable the system to continue with the ICT equipment still intact running on backup power. However, if considering longer time blackouts or outages due to, e.g., bad weather such as a hurricane, the electrical supply to the communication network nodes will play a considerable role and be of high importance and should be included.

The system is constructed and simulated using the open-source programming language Python.

## IV. Results and Discussion

### A. Betweenness Centrality Results

For this system topology, the electrical power system nodes (nodes 1 to 22) will only influence the betweenness centrality for the electrical connections, while the communication network nodes will influence the betweenness centrality for the communication network connections. However, this would be different if the power supply to the communication network nodes is considered. Fig. 4 illustrates the betweenness centrality for the electrical nodes in the system. Here, bus 14 is the most important node since this node connects to multiple radials. Furthermore, nodes 6, 13 and 18 obtain high betweenness centrality since they are the shortest path links to longer radials. Nodes 17 and 22 obtain a betweenness centrality equal to zero for both the undirected and the directed graph topology since these are end nodes in each radial. On the other hand, node 1 obtains a betweenness centrality different from zero for the undirected graph topology, while zero for the directed graph topology. This is an expected result since node 1 is connected to two different radials, but for the directed graph topology, there are only outgoing lines from node 1.

The betweenness centrality for the communication network nodes is showed in Fig. 5, where the routers can be seen as the most important communication network nodes. The result is expected since all the information from and to the electrical power system will be transferred through the router links. The end nodes for the communication network connections will be the RTUs at the electrical nodes.

In both figures, a distinction between the betweenness centrality for the undirected graph and the directed graph can be seen. For the electrical system, the highest betweenness centrality is observed for the undirected graph since the power are then *seen* to flow in both directions, while the opposite result is observed for the communication network nodes where the directed graph gives the highest betweenness centrality. This illustrates the importance of considering both scenarios (undirected and directed graph topology) when measuring the betweenness centrality to avoid loosing information.

### B. Node Attack Method Results

Fig. 6 shows the energy not supplied in the network when the electrical nodes are removed as in Algorithm 1. Here, the highest percentage energy not supplied happens when

This is the accepted version of an article published in PMAPS 2020
http://dx.doi.org/10.1109/PMAPS47429.2020.9183667

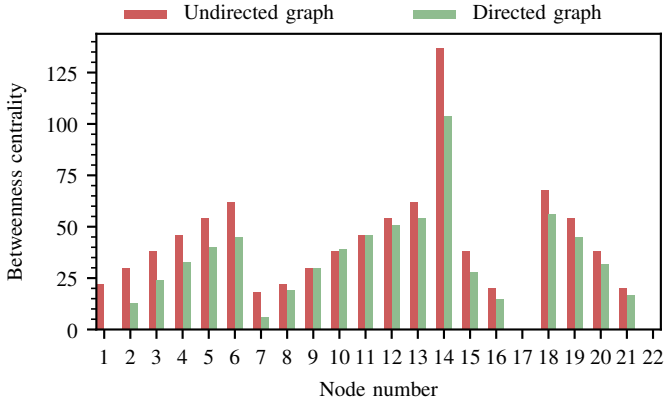


Fig. 4: Betweenness centrality electrical nodes.

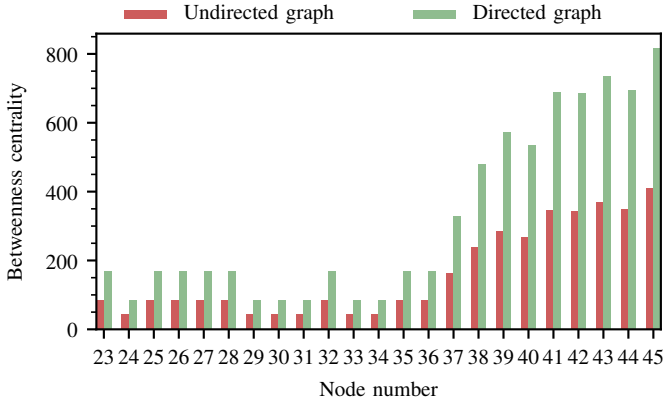


Fig. 5: Betweenness centrality communication network nodes.

node 1 is removed. This is as expected, since this result in a total system outage. From there, node 14 achieve the highest importance since the removal of node 14 causes the system to be unable to supply the two radials (path 15-17 and path 18-22, see Fig. 3). From Fig. 6, nodes 18 to 22 do also give high percentage energy not supplied, illustrating a sufficient amount of load on these nodes. Compared to the result obtained with betweenness centrality, node 1 obtain a small importance for the betweenness centrality, subsequently node 14 and the nodes on the radials (path 15-17 and path 18-22) obtain the same pattern. For the other nodes, the importance is very low when considering energy not supplied. However, this can rapidly change if those nodes encounter higher loads.

The result in Fig. 7 illustrates that the active power losses in the network have increased when removing the nodes 2 to 13. These nodes are a part of the meshed network (see Fig. 3), where a removal of one node changes the operation of the distribution system and forces the power to travel a longer distance. For the removal of node 1, no losses in the system will be observed since all the system nodes will be lost.

Fig. 8 and Fig. 9 illustrate the same when removing the communication network nodes. Here, nodes 23, 37, and 38 are the most important since the removal of these nodes will lead to an outage in node 1 and make the whole system collapse. Otherwise, removal of nodes 31 and 43 leads to an outage in node 14 and can therefore be seen as important. Comparing Fig. 6 with Fig. 8, the cascading failure due to a communication network node outage often result in more

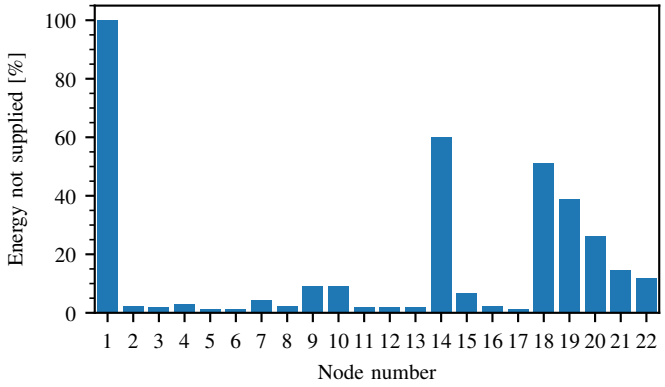


Fig. 6: The percentage of electricity not supplied in the network when electrical nodes are removed.

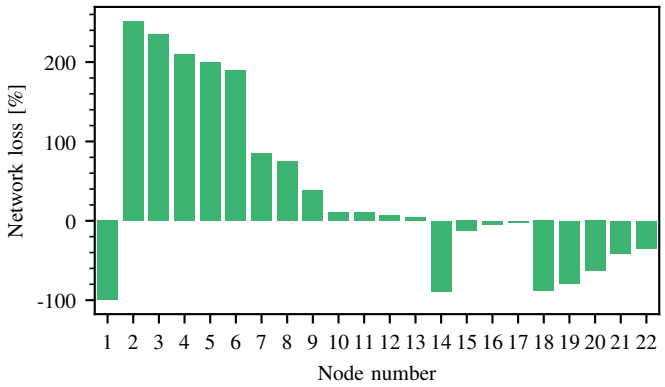


Fig. 7: The percentage of active power loss in the system when electrical nodes are removed.

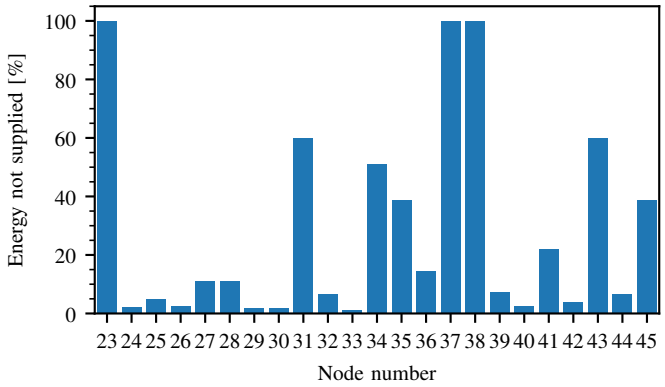


Fig. 8: The percentage of electricity not supplied in the network when communication network nodes are removed.

electrical nodes to fail, giving a higher percentage energy not supplied. Compared to the results obtained for betweenness centrality, the node importance differs. Since the betweenness centrality do not consider which type of electrical node the communication network node is connected to, the result will vary based on the amount of load that is connected to the removed nodes.

## V. Conclusion and Future Work

To avoid unwanted events such as outages and blackouts in the future power system, it is important to analyze the complexity of the network. Complex network theory is an

This is the accepted version of an article published in PMAPS 2020
http://dx.doi.org/10.1109/PMAPS47429.2020.9183667

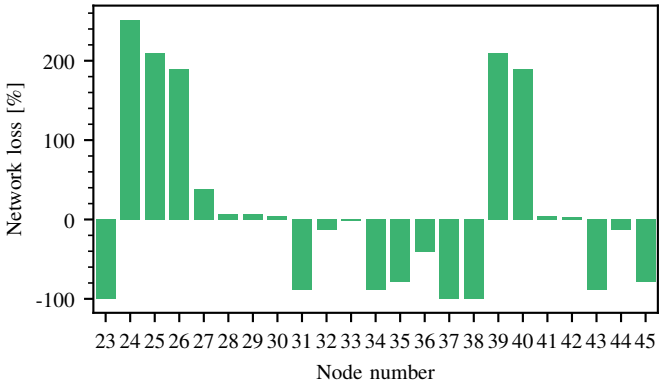


Fig. 9: The percentage of active power loss in the system when communication network nodes are removed.

advantageous method to capture the complex topology and interdependencies of a network such as a combined electrical power and communication network. In this paper, two different methods have been proposed *1) betweenness centrality* and *2) node attack method*. Both methods manage to capture the important nodes in the system, but with different criteria. The two methods obtain somewhat consistent results, especially when considering the electrical nodes. For the communication network nodes, the results differ more since the methods measure different criteria. The *node attack method* is more electric power system-oriented and does not consider the communication network to any extent.

For a system operator, it is more important to consider the security of electricity supply, and both methods are able to encounter the important nodes in the system. However, the *node attack method* is better at capturing important measures seen from a operators point of view since it considers the energy not supplied and illustrates how an outage in the communication network or the electrical power system influence the power flow. This gives a better overview of how outages might propagate in the network as well as to illustrate the consequences of a cascading failure from an outage in the communication network.

The methods proposed in this paper, will provide a basis for probabilistic analyses of the combined electrical power and communication network. This is a topic for the future work, e.g., using the methods to investigate the interdependencies in relation to the risk of short lasting blackouts.

## VI. Acknowledgment

This work is funded by CINELDI - Centre for intelligent electricity distribution, an 8-year Research Centre under the FME-scheme (Centre for Environment-friendly Energy Research, 257626/E20). The authors gratefully acknowledge the financial support from the Research Council of Norway and the CINELDI partners.

## References

[1] European Commission, "SmartGrids SRA 2035 Strategic Research Agenda Update of the SmartGrids SRA 2007 for the needs by the year 2035," Mar. 2012, Technical Report.

[2] E.A. Lee and S.A. Seshia, Introduction to embedded systems: A cyber-physical systems approach, 2nd ed., Cambridge, MA: MIT Press, 2017.

[3] G. Andersson et al., "Causes of the 2003 major grid black-outs in North America and Europe, and recommended means to improve system dynamic performance," IEE Transaction on Power Systems, vol.20, no. 4, pp. 1922–1928, Nov. 2005.

[4] S.V. Buldyrev, R. Parshani, G. Paul, H.E. Stanley, and S. Havlin, "Catastrophic cascade of failures in interdependent networks," Nature, vol. 464, no. 7291, pp. 1025–1028, 2010.

[5] Europa Commission, "Concerning measures to safeguard security of electricity supply and infrastructure investments," Directive 2005/89/EC of The European Parliament And Of the Council, European Council,, Strasbourg, 2006.

[6] I.B. Sperstad, "The impact of flexible resources on the security of electricity supply," CINELDI WP5 Expert Group, 2018.

[7] M. Ouyang, "Review on modeling and simulation of interdependent critical infrastructure systems," Reliability Eng. Syst. Saf., vol. 121, pp. 43–60, 2014.

[8] P. Hokstad, I.B. Utne, and J. Vatn, Risk and interdependencies in critical infrastructures: A guideline for analysis, Springer, 2012.

[9] I.A. Tøndel, J. Foros, S.S. Kilskar, P. Hokstad, and M.G Jaatun, "Interdependencies and reliability in the combined ICT and power system: An overview of current research," Applied computing and informatics, vol. 14, no. 1, pp. 17–27. 2018.

[10] A.R. Ganguly, U. Bhatia, and S.E. Flynn, Critical infrastructure resilience: Policy and engineering principles, Routledge, 2018.

[11] J. Wäfler and P.E. Heegaard, "A combined structural and dynamic modelling approach for dependability analysis in smart grid," Proceedings of the 28th Annual ACM Symposium on Applied Computing, pp. 660–665, 2013.

[12] M. Rausand, Risk assessment: Theory, methods, and applications, John Wiley & Sons, 2013.

[13] G. Ramos, J.L. Sanchez, A. Torres, and M.A. Rios, "Power systems security evaluation using petri nets," IEEE Transactions on Power Delivery, vol. 25, no. 1, pp. 316–322, 2009.

[14] L. Cuadra, S. Salcedo-Sanz, J. Del Ser, S. Jiménez-Fernández, and Z.W. Woo, "A critical review of robustness in power grids using complex networks concepts," Energies, vol. 8, no. 9, pp. 9211–9265, 2015.

[15] S. Boccaletti, V. Latora, Y. Moreno, M. Chavez, and D-U. Hwang, "Complex networks: Structure and dynamics," Elsevier, Physics reports, vol. 424, no. 4–5, pp. 175–380, Jan. 2006.

[16] D.J. Watts and S.H. Strogatz, "Collective dynamics of 'small-world'networks," Nature, vol. 393, no. 6684, pp. 440–442, June 1998.

[17] A-L. Barabási and R. Albert, "Emergence of scaling in random networks," Science, vol. 286, no. 5439, pp. 509–513, Oct. 1999.

[18] G. A. Pagani and M. Aiello, "The Power Grid as a complex network: A survey", Physica A: Statistical Mechanics and its Applications, vol. 392, pp. 2688—2700, 2013.

[19] J. Wäfler and P.E. Heegaard, "Structural dependability analysis in smart grid under simultaneous failures," IEEE International Conference on Smart Grid Communications (SmartGridComm), pp. 67–72, 2013.

[20] S. LaRocca, J. Johansson, H. Hassel, and S. Guikema, "Topological performance measures as surrogates for physical flow models for risk and vulnerability analysis for electric power systems," Risk analysis, vol. 35, no. 4, pp. 608–623, 2015.

[21] J. Johansson, H. Hassel, and E. Zio, "Reliability and vulnerability analyses of critical infrastructures: comparing two approaches in the context of power systems," Reliability Engineering & System Safety, vol. 120, pp. 27–38, 2013.

[22] Z. Huang, C. Wang, S. Ruj, M. Stojmenovic, and A. Nayak, "Modeling cascading failures in smart power grid using interdependent complex networks and percolation theory," IEEE 8th Conference on Industrial Electronics and Applications (ICIEA), pp. 1023–1028, 2013.

[23] R. Mihalcea and D. Radev, Graph-based natural language processing and information retrieval, Cambridge university press, 2011.

[24] L.C. Freeman, "A set of measures of centrality based on betweenness," Sociometry, vol. 40, no. 1, pp. 35–41, 1977.

[25] M.E. Baran and F.F. Wu, "Network reconfiguration in distribution systems for loss reduction and load balancing," IEEE Trans. Power Delivery, vol. 4, no. 2, pp. 1401–1407, April 1989.

This is the accepted version of an article published in PMAPS 2020
http://dx.doi.org/10.1109/PMAPS47429.2020.9183667