

# **Parameters determining the Information Flow in Smart Meters Complex Networks Smart Metering and Smart Grid Security**

**Robert Czechowski**

Department of Electrical Power Engineering/Wroclaw University of Science and Technology  
Wyb. Wyspianskiego 27, Wroclaw, Poland  
robert.czechowski@pwr.edu.pl

**Abstract** - The development of technology, falling costs of production, as well as the development of more and more computer applications contributed significantly to the rapid development of computerization in all aspects of our lives. Considerable progress in Information and Communications Technology (ICT) services allows their effective use in intelligent power networks (Smart Grids). Particularly important for the efficient management of the low voltage networks (Smart Metering) is to know the dynamically changing network topology by emerging transmission of digital information to the physical network operator.

**Keywords:** Smart Metering, Smart Grid, Data Flow, Digital Information, Complex Networks.

## **1. Introduction**

In today's age of digital data transmission technologies' integration with infrastructures of large companies such as manufacturers and suppliers of gas, biofuels and electrical energy, these companies are systems of crucial importance to the functioning of what is often an entire country. Modernization of these systems and their continued development not only increase the security of the offered services, system functionality and modern infrastructure management, but also allow the development of a new field of knowledge which encompasses discovering previously unknown data, the so-called Data Mining. The increase in generated information throughout the past several years has allowed for scientists and analysts of large corporations to dig ever deeper into acquired information and seek previously unknown data. Thus acquired information will not only serve within the economic aspect of management, but also allow to understand and learn more about the architecture and operational principles of one's own network. The vast majority of this information will have its source in the automated communication process of Smart Devices. Understanding their functionality and more precise awareness of communication failures caused by internal interference in the future will allow for construction of better and better network interfaces, which, along with increasingly perfected communication and encryption algorithms, will allow for improvement of Smart Grids [1].

## **2. Connection dynamics in Complex Networks**

Modern low-voltage power grids are, from the system operator's perspective, the most important source of information on a network's state. One also cannot ignore the importance of digital information monitoring and transfer throughout distribution networks which, due to them being the grid backbone, are the most important element of the entire system. Networks of smart meters and Intelligent Electronic Devices (IED) provide the most interesting data whose sheer amount will be an additional challenge to the operator in terms of its analysis. Power systems comprised of hundreds of thousands of power meters, what is typical for a nation-wide operator, make automated communication between terminal devices (power meters, concentrators, IED) quite a challenge for the designer of such a network. One should also take into account for not only communication from the power meter to the concentrator, but also the possibility of data reading on demand, remote parameterization and remote software updates. Two-way communication, being the basic functionality of smart grids, despite its simple assumption, is not so easy to implement and exploit. In the context of high performance networks transferring even small amounts of information at speeds like kB/s, given hundreds of thousands of devices, the designer is required to be able to predict the outcomes of unusual errors and potential modernization of the network in the future. It is also important to remember that information exchange digital systems in power networks often make use of the same mechanisms as tele-information systems (protocols: communication, encryption and routing). Connection dynamics

in complex networks encompass automated selection of an optimal route and its upkeep in the system's segment where the designer enables free communication, so-called dynamic routing. The most prevalent solution in power grids (and more) is a grid model based on statistical backbone being the basic infrastructure (communication channels) and a dynamic sensory network of devices working within a low voltage network. Dynamic connection solution has many advantages, but it is not free of flaws, either. Its decisive advantage is the possibility to independently create connections under varied conditions prevalent within the network (mainly short-lived interference), and to independently establish a new connection without the system administrator's input. Its disadvantage is allowing for too much independent "wandering" of devices (their communication interfaces) over the network, which causes unneeded logging into remote concentrators, and especially changing phases. Understanding the principles of automated creation of these networks is the very basis for design of sensory networks, such as low-voltage power meter grids [2].

### 3. Forming the Network Parameters

The efficiency of information transfer not only depends on the distance between the sender and the recipient. Information passed from one node to the other can still get lost somewhere along the way, for example, a node that not cope with the fast data processing. For this reason, end device (smart meter - terminals) and end counters (switches), involved in the transfer of information may be of strategic importance and will have their impact on determining the quality and the level of data transmission efficiency. The transmission rate of information (usually PLC networks), depends on many parameters, for example: the network topology, place of data origin, brokering environment, fault tolerance and external interference or partial destruction of the network (for more information on this topic please see article [3]). The information obtained by shaped network topology can be represented as a directed graph (Fig. 1: Network 1).

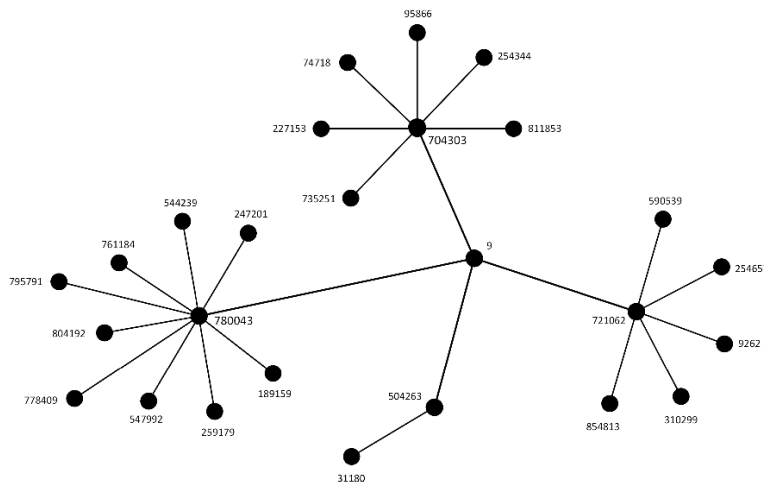


Fig. 1: Connections in Complex Network 1 (sample: 240). Network Interpretation (Treat the network as directed), Network Analysis as (Shortest Path Length Distribution), Map of node size to (Indegree), Map of nodecolor (Indegree).

The key parameter is the level of attendance and stability of the given connection (Fig. 2: Network 2, indicated by red line), and the existence of the largest the coherent component to the surrounding neighbourhood (Fig. 3: Network 3, indicated by a red spot). These parameters are of highest importance for the functioning of complex power grids. It is worth mentioning that additional information is necessary to create data flow paths (Fig. 2: Network 2) between the energy meters (green dots), concentrators (yellow dots) and the logging units (orange dots) [4, 5]. The system operator can provide historical data, to discover previously unknown information which will help in selecting appropriate choice of transmission technology and devices in the future with improved communication specifications which will improve efficiency and quality the whole energy network.

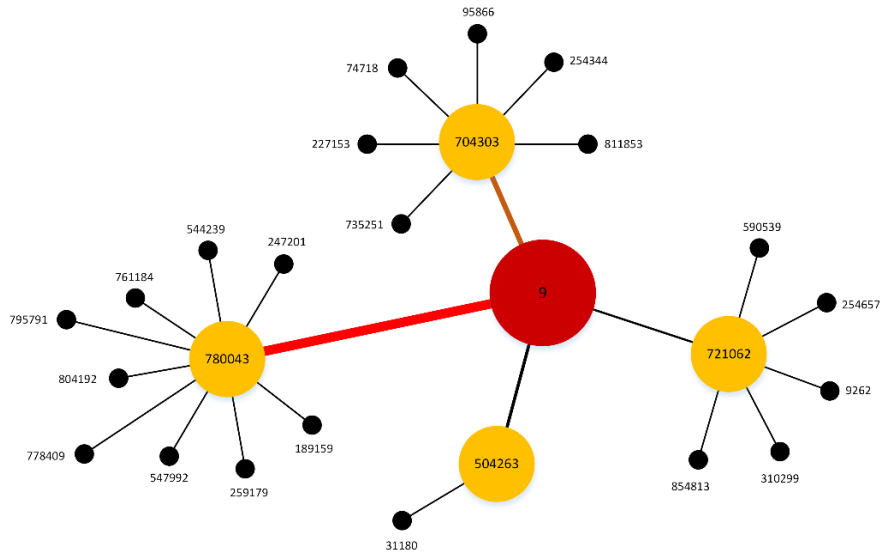


Fig. 2: Connections in Complex Network 2 (sample: 232). Network Interpretation (Treat the network as directed), Network Analysis as (Shortest Path Length distribution), Map of node size to (Eccentricity), Map of nodecolor (Eccentricity).

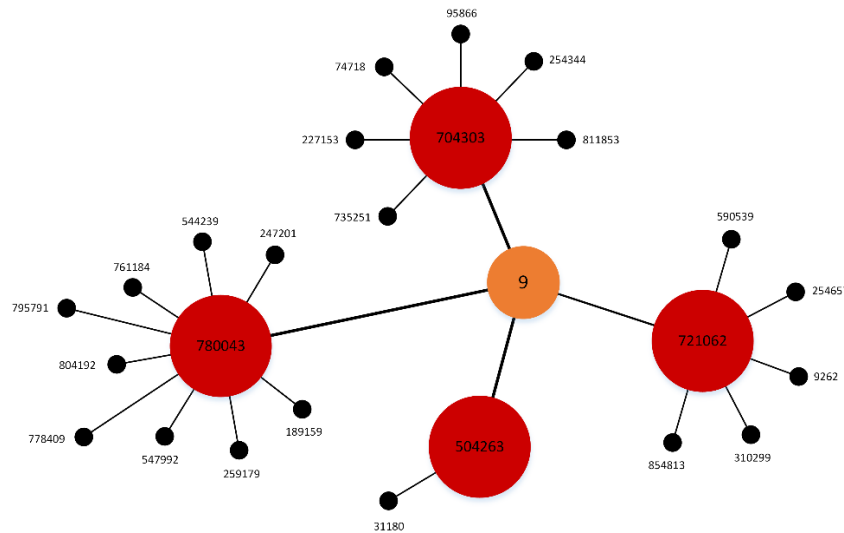


Fig. 3: Connections in Complex Network 2 (sample: 224). Network Interpretation (Treat the network as directed), Network Analysis as (Betweenness Centrality), Map of node size to (Closeness Centrality), Map of nodecolor (Closeness Centrality).

#### 4. Theory and Parameters of Complex Grids' Communication

Detailed topological analysis can be very time-consuming in case of expansive networks. Calculating the local parameters of nodes is much quicker than calculating global (i.e. accounting for paths between nodes) parameters. Local parameters include the degree of a node, neighborhood connectivity, the topological factor and the clustering factor. Centrality, in turn, - due to its mediation - as well as closeness centrality and stress centrality count as global parameters. NetworkAnalyzer features an option to analyze a subset of nodes, which allows for narrowing down the calculations of local parameters to a node subset. If, before initiating an analysis, the user selects one or more nodes, the analysis will only cover the selected subnetwork. Because in such a case only local parameters are calculated, the results will not include e.g. a distribution of the shortest paths or common neighbors. The length of a path is indicated by the number of its edges. There can be only one path between two nodes. The shortest path between two  $n$  and  $m$  nodes is called a distance and

marked as  $L(n,m)$ . The greatest distance between two nodes determines the network diameters. In case of unconnected network, the diameter is determined by the greatest distance within its connectivity components. The diameter can also be described as the maximum eccentricity of nodes (definition of eccentricity - see Attributes). The network radius is the smallest nonzero eccentricity within the network. The average shortest path length, also known as characteristic path length, indicates the expected distance between any two connected nodes of a network. The stress centrality of a given node is the number of the shortest paths which pass through that node. The more of such paths, the higher the node's stress centrality. This parameter is only calculated in case of networks without multiplied edges. When there is a path composed of edges between two nodes of an undirected network, the nodes are connected. All interconnected nodes make up a connected component. The number of connected components indicates the network's cohesion - the less of them there are in a given network, the greater its cohesion. An  $n$  node's neighborhood is referred to as a collection of its neighboring nodes. The size of  $n$  node's environment is called its connectivity and marked as  $k_n$ . The average number of neighboring nodes indicates the average connectivity of nodes in a given network. The normalized version of this parameter is the network density which assumes a value within  $[0, 1]$  and indicates the degree of edges' extinguishing within a network (looped and multiplied edges are ignored here). A network with no edges, composed only of isolated nodes, has a density equal to 0. The number of isolated nodes can indicate the degree of a network's density. Another parameter is a network's centralization. In networks with star topology, it gravitates towards 1, and in decentralized networks - towards 0. Network heterogeneity, in turn, reflects a tendency of central nodes (i.e. with many neighbors) to appear in a network. The number of multi-edge node pairs indicates how often neighboring nodes are connected by more than one edge. The connectivity of a given node is the number of its neighbors. The neighborhood connectivity of a node is defined as the mean connectivity value for all its neighbors. Distribution of connectivity assigns to integer numbers of  $k = 0, 1, \dots$  a mean value of neighborhood's connectivity of all nodes with  $k$ . The shortest path between  $n$  and  $m$  nodes is marked as  $L(n,m)$ . Distribution of the shortest paths assigns to integer numbers of  $k = 1, 2, \dots$  a number of node pairs  $(n,m)$  whose shortest path is  $L(n,m) = k$ . The greatest distance between two nodes determines the network diameter. In case of unconnected network, the diameter is determined by the greatest distance within its connectivity components. The network diameter and distribution of the shortest paths can indicate whether the analyzed network demonstrates quality of a small world.

NetworkAnalyzer allows for two methods of visualization of a topological analysis' results. The first one entails assigning specific colors and sizes to nodes and edges, depending on the values of selected parameters. The other method is to map out the selected pair of parameters on a graph (Table 1). Both these visualization methods can be used to graphically represent both the attributes calculated by the NetworkAnalyzer plugin and other numerical values assigned to nodes and edges of the selected network.

Table 1: Connections in Complex Network [4].

Parameters of Complex Network	
Simple Network Parameters	Complex Network Parameters
(1) Number of Connected Components, (2) Parameters Related to Shortest Paths, (3) Parameters Related to Neighborhood.	(5) Degree Distributions, Neighborhood Connectivity, (6) Shortest Paths, (7) Clustering Coefficients, (8) Shared Neighbors, (9) Topological Coefficients, (10) Stress Centrality, (11) Analysis of Subset of Nodes, (12) Batch Analysis.

Visualization is only possible when the calculation parameters for the selected network are stored as attributes of nodes and edges. To accomplish that, the option Store Node / Edge Parameters in Node / Edge Attributes in the plugin settings should be enabled. It is not possible to visualize parameters loaded from a .netstats file, as it does not store any information about the network itself. If, after performing a topological analysis, the network is modified by addition or removal of nodes or edges, it is recommended (and sometimes even necessary) to restart the plugin before attempting parameter visualization [4, 5].

The following article presents general information and functionality problems related to elements of a power grid infrastructure where information is collected from several sources and different network topologies. A model of the subject network can be used to simulate a system's behavior during its normal operation, as well as be a priceless source of information on the system's behavior in case of a failure or a deliberate attack by third parties. A simulation model can also

show the characteristics of a complex network in case of a sudden voltage increase or decrease, and be an inspiration for implementing new ideas contributing to increased security and stability of an entire electric power system [6].

At the same time, it is difficult to unequivocally explain a close relationship between formation of complex networks and the internal mechanism of operation and behavior of an electric power system. Complex network theory constitutes a new tool helpful in analysis of the problem of information flow optimization and design of high efficiency electric power systems utilizing two-way data transmission [7]. Research and utilization of information transit optimization in complex networks (the most important and stable connections in the graph) and data mining technique are some of the most important and latest techniques of data acquisition and data flow optimization.

## **5. Security of Power Energy Network**

Security of a power grid is the total amount of measures encompassing both the security of information transferred between the network's nodes, and of information gathered by it in the data base. Wide utilization of tele-information techniques (especially online) introduces previously unknown threats to security of IT systems: intrusions, viruses, spam, activity blocks, etc. Therefore, the importance of data protection and authentication of objects connected to the network grows. Hacking into computer systems and interruptions of service cause significant financial losses and often, which is very important, decrease trust for the institution that was entrusted with processing personal data of specific clients. Network security includes not only technical means and software solutions for system protection, but also clearly defined and observed security policies. Security is the problem of both security measures and management of resources and information. It results from good organization and proper security policy implemented on all organizational levels. The problem of a power grid's security should be considered on all levels of its organizational structure, and the security policy has to be clear and specific. Implementation of said policy requires every employee of the company to be familiar with it to an extent adequate to their position. The basic stage of organizing a protection system is recognition of the protected area. Most of all, one must establish what the power system is composed of, what the network diagram looks like, what is the security class of network access points and who uses them. Moreover, one must assess valuable information, what informational resources are important enough, where they are located to be effectively protected. Training the personnel in terms of information protection is beyond dispute, yet often neglected. It is crucial to have data protection personnel in constant cooperation with the company's organizational units, as well as to support, understand and be flexible towards the end user. The educational process for the entire personnel should be tailored to the expectations and needs of each employee group, otherwise security will be omitted, disabled or ignored. Undoubtedly, the issue of tele-information security is the key element of a power system, crucial for its efficient and reliable operation [8].

## **6. Future of Smart Grid**

In the recent years, an incredible spurt of development could be observed in power systems. Their modernization, along with utilization of communication and control means, contributes to creation of brand new, fully manageable and smart power grids. The future of these systems will be closely related to the dynamically developing digital technology, especially digital drivers and security measures based on fully programmable features. These features will be fully modifiable based on importing characteristics onto these devices. The future of managed grids draws its beginning from the strong grid, meaning a continent-wide network being the backbone of energy transfer. Modernization of the above-mentioned networks will affect all of their components, from altering the concept of network management on the operator's center, elevation and monitoring of medium and low-voltage networks to low-voltage networks, including smart metering ones. Power development will also affect photovoltaic installations, wind power stations and microgeneration. What will also matter is implementation of digital restitution automation dedicated for large agglomerations whose task in case of failures will be to undertake automated, independent action aimed at separating a damaged line and restoring the remaining part of a power system to its full functionality in a relatively short time. Along with modernization of power grids, SCADA (Supervisory Control And Data Acquisition) and HAN (Home Area Network) systems will also undergo development. As the discussed systems develop, one should not omit a very important issue regarding the cooperation between industry and universities. Electrical departments of universities should be equipped with modern devices and system models so that the graduates have not only solid theoretical foundations but also knowledge of devices available on the market and, more importantly, the skills to use them in an increasingly computerized power system.

## 7. Conclusions

The task of a system's architect and its future administrator is to find the golden mean between the utilized technology and the possibility of occurring anomalies and undesired communication phenomena such as: bottlenecks, duplication of messages or excessive information overhead. Shaping and upkeep of a digital information transfer route depends on many parameters, not only physical but also logical ones. The decisive parameters are: impact of interference, distance and Signal to Noise Ratio (SNR). What also counts are parameters indicating the density of devices belonging to a given network of their kind, the negotiated routed and automatically assumed function within the network. Mathematical description of the network can be presented via a directed graph generated based on logs of concentrators. One should remember that the route between the source and the target can, in some cases, be unclear, even difficult to ascertain. The theory of complex grids will allow system administrators to better understand processes in communication networks and maybe provide valuable data the use of which will make it possible in the future to construct increasingly perfected power systems using digital communication.

## Acknowledgements

This paper was realized within NCBR project: ERA-NET, No 1/SMARTGRIDS/2014, acronym SALVAGE. "Cyber-Physical Security for the Low-Voltage Grids". The author inform that the most information's were cited from his postgraduate thesis "Information Flow in Complex Network Simulation Study", Wroclaw University of Science and Technology, Faculty of Computer Science and Management, 2011, based on research come from open source program Cytoscape 2.4.1 and technical documentation of this program. This paper also is associated with following paper: Impact of Interference on Digital Information Flow in Dynamically Changing PLC Network Topology. Cyber Security in Smart Grid (DPSP 13th Conference 2016).

## References

- [1] S. F. Bush, *Smart Grid: Communication-Enabled Intelligence for The Electric Power Grid*, IEEE Press, Wiley, 2014.
- [2] M. J. Cronin, *Smart products, Smarter services: Strategies for Embedded Control*, Cambridge University Press, 2010.
- [3] R. Czechowski, "Impact of Interference on Digital Information Flow in Dynamically Changing PLC Network topology: Cyber Security in Smart Grid," in *Proceedings of DPSP 2016: The 13<sup>th</sup> IET International Conference on Developments in Power System Protection*, The Institution of Engineering and Technology, cop., Edinburgh, Scotland, UK, March 2016, pp. 1-6.
- [4] Cytoscape 2.4.1. User manual and program documentation [Online]. Available: <http://www.cytoscape.org/index.html>, [http://cytoscape.org/manual/Cytoscape2\\_4Manual.pdf](http://cytoscape.org/manual/Cytoscape2_4Manual.pdf)
- [5] Cytoscape 3.3.0. User manual and program documentation [Online]. Available: <http://www.cytoscape.org/index.html>, [http://www.cytoscape.org/manual/Cytoscape3\\_3\\_0Manual.pdf](http://www.cytoscape.org/manual/Cytoscape3_3_0Manual.pdf)
- [6] S. Boccaletti, V. Latorab, Y. Morenod, M. Chavezf and D. U. Hwanga, "Complex networks: Structure and dynamics," *Physics Reports*, vol. 424, pp. 175-308, 2006.
- [7] L. Liu, J. Liu, Y. Liu and J. Li, "Complex Network Characteristic of Power System Based on Energy Information in the Steady Transition Process," in *Proceedings of the Power and Energy Engineering Conference (APPEEC)*, pp. 1-5, 2011.
- [8] T. Flick and J. Morehousem, "Securing the Smart Grid: Next generation power grid security," *Elsevier*, 2011.