Physica A xx (xxxx) xxx–xxx

Contents lists available at ScienceDirect

Physica A

journal homepage: www.elsevier.com/locate/physa

Network topology and resilience analysis of South Korean power grid

Dong Hwan Kim [a], Daniel A. Eisenberg [b], Yeong Han Chun [c], Jeryang Park [a,*]

[a] School of Urban and Civil Engineering, Hongik University, Seoul 04066, South Korea
[b] School of Sustainable Engineering and the Built Environment, Arizona State University, Tempe, AZ, USA
[c] Department of Electrical and Electronic Engineering, Hongik University, Seoul 04066, South Korea

HIGHLIGHTS

- Detailed information on power grid may produce highly-skewed degree distribution.
- Resilience of KPG is analyzed with multiple approaches including recovery.
- KPG is revealed as most vulnerable compared to ER and BA networks.

ARTICLE INFO

Article history:
Received 1 April 2016
Received in revised form 1 July 2016
Available online xxxx

Keywords:
Complex network
Scale-free
Vulnerability
Robustness
Critical infrastructure

ABSTRACT

In this work, we present topological and resilience analyses of the South Korean power grid (KPG) with a broad voltage level. While topological analysis of KPG only with high-voltage infrastructure shows an exponential degree distribution, providing another empirical evidence of power grid topology, the inclusion of low voltage components generates a distribution with a larger variance and a smaller average degree. This result suggests that the topology of a power grid may converge to a highly skewed degree distribution if more low-voltage data is considered. Moreover, when compared to ER random and BA scale-free networks, the KPG has a lower efficiency and a higher clustering coefficient, implying that highly clustered structure does not necessarily guarantee a functional efficiency of a network. Error and attack tolerance analysis, evaluated with efficiency, indicate that the KPG is more vulnerable to random or degree-based attacks than betweenness-based intentional attack. Cascading failure analysis with recovery mechanism demonstrates that resilience of the network depends on both tolerance capacity and recovery initiation time. Also, when the two factors are fixed, the KPG is most vulnerable among the three networks. Based on our analysis, we propose that the topology of power grids should be designed so the loads are homogeneously distributed, or functional hubs and their neighbors have high tolerance capacity to enhance resilience.

1. Introduction

Infrastructure systems provide and maintain functions of transporting energy, material, human, and information, all of which are essential to modern society, through their networked structure. Some infrastructure systems, such as electric power transmission and distribution grids, are also called critical or lifeline infrastructure because they provide

* Corresponding author. Fax: +82 2 322 1244.
E-mail address: jeryang@hongik.ac.kr (J. Park).

http://dx.doi.org/10.1016/j.physa.2016.08.002
0378-4371/

Please cite this article in press as: D.H. Kim, et al., Network topology and resilience analysis of South Korean power grid, Physica A (2016), http://dx.doi.org/10.1016/j.physa.2016.08.002

interconnected functions such as emergency response or the provision of essential resources, without which society cannot operate as intended [1]. As such, improving the structural and functional resilience of critical infrastructure systems (CIS) to various natural and man made hazards has always been an important problem to public and research disciplines [2].

One novel method for improving the resilience of a CIS is to study it as a complex network. This approach enables the identification of important underlying structures within the CIS and assessment of structural and functional robustness in multiple (e.g., meso- or macro) scales perspectives [3]. Many types of CIS, including power grids [4–6], roads [7], public transportation [8], natural gas supply [9], and water supply [10] have been studied as complex networks. Among those, power grids are one of the most important infrastructure systems to consider, as numerous other CISs depend on the reliable and stable provision of electricity for proper functioning [11].

In general, power grids have a centralized structure, where power plants generate large amounts of electricity and transmission lines direct power across vast regions for end-point consumption. This is evident in South Korea (Korea hereafter), where manufacturing facilities that use over 50% of total electric power generated nationally [12] are often located far from power generation, suggesting a strong spatial mismatch between electricity supply and demand. Thus, the negative impacts of a failure occurring somewhere in the power grid are not geographically isolated, but rather easily propagated to places far away from its origin. Furthermore, strong interdependency of the power grids with other infrastructure systems typically aggravates this situation, as a failure can propagate across multiple systems [13]. For example, the water distribution system uses electric power to pump water, and electric power plants, in turn, use this water for running turbines and cooling systems. The interdependency between these CISs increases their local vulnerability, as disruptions occurring in either system can trigger cascading of failures across both [11,14]. Moreover, recent blackouts in several countries (e.g., India in 2012; Korea in 2011; USA and Canada in 2003; Italy in 2003) were initiated by local malfunctioning but resulted in huge economic damages in multiple sectors across large spatial regions.

Recently, several studies analyzed the topological properties of real power grid networks, and some of those works try to link the topology of those networks with system vulnerability. In particular, we refer interested readers to Cuadra et al. [15], who provided a thorough review of extant literature on power grid network and robustness analyses research. Here we discuss several important works in detail to give background on the field. Also, note that we provide thorough descriptions of complex network terminology relevant to this work in the methods section.

Albert et al. [16] analyzed North American power grid (115–765 kV) – which is composed of 14,099 nodes and 19,657 edges – and found that, in spite of being characterized by exponential degree distribution, the network exhibits similar behavior as a scale-free network to errors and attacks. Rosato et al. [17] studied high-voltage electrical power transmission networks of three European countries – Italy (380 kV), France (400 kV), and Spain (400 kV) – all of which exhibit a very large clustering coefficient with a larger characteristic path length than random networks characterizing small world systems. Rosato et al. [17] also assessed the vulnerability of each network by evaluating the minimum number of links needed to break each power grid into two sub-networks (the "min-cut" problem). Their results conclude that the specific geography of each country has a strong influence on network topography and associated vulnerability. Rosas-Casals et al. [4] and Sole et al. [18] analyzed 33 networks within the Union of the Coordination of Transport of Electricity (UCTE) power grid (110–400 kV) and found that all the networks were characterized by exponential degree distributions. However, they concluded that most of the networks did not have a small world topology, and the networks displayed similar vulnerability behavior to scale-free networks under random and selective node removal.

The works described above are representative of the majority of complex network analyses in literature since they focus on high-voltage electrical transmission systems. While analyses often remain at this scale because of data availability, this macro-scale focus may result in an only partial realization of topological properties due to limited information. To obtain a more detailed view to a real system, it is better to analyze the power grid with a broader range of voltage classes, i.e., including sub-transmission and distribution circuits [19,20]. Moreover, many of these studies claim to assess power grid resilience [18,21–24], but their methods focus solely on the remaining system structure or function after the removal of individual components (either nodes or links), which only assesses network vulnerability or robustness Resilience, however, also requires information on how systems recover and adapt during or after failure scenarios [25,26].

In this work, we analyze the Korean power grid (KPG) as a complex network. The KPG data is composed of power generation plants, transformers, transmission substations represented as vertices (or nodes), and transmission lines represented as edges (or links). Our data is unique because it spans a much wider voltage range (3.3–765 kV) than those networks considered in the literature by including sub-transmission circuits that terminate at distribution substations and transformers. Using this network data, we investigate topological properties of the KPG and its structural vulnerability and resilience, including its recovery performance. The rest of this paper is organized as follows: Section 2 introduces the KPG data and methods for topological, vulnerability, and resilience analyses. Section 3 presents results and discussion for these analyses. Finally, Section 4 summarizes the results and recommends new design principles for more resilient power grids.

2. Methods

2.1. Korean power grid (KPG) dataset

We generated complex network representations of the 2011 KPG by digitally extracting it from PSS/E (power system simulation for engineering) data of the national electric power system provided by the Korean Power Corporation (KEPCO).

Please cite this article in press as: D.H. Kim, et al., Network topology and resilience analysis of South Korean power grid, Physica A (2016), http://dx.doi.org/10.1016/j.physa.2016.08.002

Table 1
Quantification of nodes and links in the KPG by voltage class.

Voltage levels	765 kV	345 kV	154 kV	23–66 kV	19–22.9 kV	15–18 kV	3.3–13.8 kV	Total
# of nodes	11	167	1189	319	91	142	164	2083
(%)	(0.5)	(8.0)	(57.1)	(15.3)	(4.4)	(6.8)	(7.9)	(100%)
# of links	42	538	1954	0	2	18	17	2571
(%)	(1.6)	(20.9)	(76.0)	(0)	(0.1)	(0.7)	(0.7)	(100%)

It contains information about power grid buses, power plants, transformers, and transmission lines ranging from 3.3 to 765 kV, but excludes low voltage distribution circuits (see Table 1). We represented power plants and substation buses (transformers and switching stations) as nodes and transmission lines as links. Although variation exists in voltage class, actual power flow in a power grid changes depending on time and space requirements (including contingency situations), and more power may flow over low voltage power lines than over higher voltage power lines. Thus, it is not suitable or realistic to weigh the links based on their voltage class unless one needs to consider longitudinal variations of actual flow in a power grid. To focus the analysis on power grid topology of specific generation-demand scenario, instead, we treated links and nodes as being homogeneous and unweighted. Moreover, while power flows in the direction from generation to distribution and from high to low voltage, we assumed all the links are undirected as was done in several other studies (e.g., Refs. [4,23,27]). With these assumptions, we generated an undirected and unweighted graph $G = (N, M)$ where N is the set of nodes and M is the set of edges. The graph is represented by $N \times N$ adjacency matrix, A, in which the element a_{ij} is equal to 1 when there exists connection between nodes i and j, and 0 otherwise [3].

2.2. Complex network measures

In this work, we study the KPG using three node-based measures (i.e., degree, clustering coefficient, and betweenness) and three network-based measures (i.e., degree distribution, average clustering coefficient, and efficiency) to characterize network structure and function. Taken together, we use these six measures to present a comprehensive understanding of network topology, vulnerability, and resilience.

2.2.1. Node-based measures

For this analysis, we use three common node centrality metrics to characterize the KPG: degree, clustering coefficient, and betweenness. Degree centrality, k_i, is the number of links connected to a node i. With k_i for all nodes, we obtain the average degree of the network, $\langle k \rangle$, which is also calculated as $2M/N$. Whereas degree centrality measures the local importance of nodes, the clustering coefficient relates a node's connectivity to its neighbors. This measure is defined as $C_i = 2e_i[k_i(k_i - 1)]^{-1}$, where e_i is the number of links connecting the k_i neighbors of node i to each other [3].

While degree and clustering coefficient evaluate the structural importance of nodes, betweenness centrality measures their functional importance by relating a node's structural position to the efficient flow paths throughout the network. A path length from node i to node j is the number of links connecting both nodes. Efficient flow paths within a complex network are assumed to be the path with the fewest possible links between i and j, l_{ij}, or the shortest path. The betweenness of node k, B_k, is defined as the number of shortest paths between any two nodes that pass through k [3]. It is mathematically expressed as $B_k = \sum_s \sum_t \frac{\sigma_{st}(k)}{\sigma_{st}}$, where $\sigma_{st}(k)$ is the number of shortest paths between nodes s and t that pass through node k and σ_{st} is the total number of shortest paths between s and t. Betweenness is often used to approximate loads of a node [28], and is an important metric for CIS networks because it characterizes network flow contribution (e.g., traffic flow for street networks; electricity flow for power grids).

2.2.2. Network-based measures

With the degree for all nodes in a network, we generate the node degree distribution, $P(k)$, a probability of a node to have degree k. The first and second statistical moments of this distribution provide the average number of connections per node and the variance, respectively. However, for some distributions, especially those with heavy tails, these statistical moments are not obtainable because the degree varies over several orders of magnitude which does not allow the integration for probability. When studying networks that follow a power-law distribution, $P(k) \sim k^{\alpha}$, the value of α may be more useful for characterizing underlying form and function of the network than the statistical moments. Numerous real-world networks such as World Wide Web, citation networks in scientific publications, collaboration network of actors, protein and gene networks are known to exhibit power-law node degree distribution [29]. However, power grids are rarely described with a power-law distribution, but rather are better described by an exponential distribution [4,16,17]. In this work, we hypothesize that previous studies characterize power grids with exponential degree distributions as an artifact of using limited data on high voltage transmission lines. Instead, we propose that the inclusion of low voltage, sub-transmission and distribution infrastructure in analysis produces a degree distribution with higher skewness and heavier tail. In this study, we test this hypothesis using the KPG.

We also use average clustering coefficient and network efficiency measures to study network vulnerability and resilience. The average clustering coefficient, $C(G)$, is calculated as the average of clustering coefficients for all nodes in graph G. $C(G)$ is

Please cite this article in press as: D.H. Kim, et al., Network topology and resilience analysis of South Korean power grid, Physica A (2016), http://dx.doi.org/10.1016/j.physa.2016.08.002

useful for describing network redundancy, by taking the local property of how connected nodes are among their neighbors and normalizing it over the entire network [30]. In particular, as the clustering coefficient increases, more alternative paths exist among nodes. Therefore, a high average clustering coefficient may relate to a more resilient network to flow disruptions, because it has a large number of redundant flow paths.

In addition, we use network efficiency to measure the response of networks to the deletion of nodes (vulnerability) or cascading failures and recovery (resilience). Efficiency is the inverse of the harmonic mean of the shortest paths between all possible pairs of nodes [31,32], and is treated as a normalized measure of flow over a network. When a node on the shortest path between source i and destination j is removed, the value of l_{ij} may change. This shift in l_{ij} represents flow redistribution, as we assume existing network flow takes alternate paths with this new value to minimize energy consumption. The global efficiency of network G captures and normalizes these changes for the entire network, and is defined as:

$$E(G) = \frac{1}{n(n-1)} \sum_{i \neq j \in G} \frac{1}{l_{ij}}. \quad (1)$$

2.3. Reference networks

In this study, we use the above measures to characterize the topology of the KPG, to rank nodes, and measure network performance during and after perturbations for resilience analysis. In order to generalize results, we compare the KPG analysis to reference networks. In particular, we use extensively studied synthetic networks as reference cases to the KPG. For this work, we generated an Eröds–Rényi random (ER) network [33] and a Barabasi–Albert scale-free (BA) network [29] for comparison. We chose these two classes of network because they represent two end members in a spectrum of topological properties, especially their degree distributions (e.g., single-scaled versus scale-free). Moreover, the average degree, $\langle k \rangle$, is used to match synthetic network size to the KPG (both N and M).

ER network is generated by starting with N nodes and connecting each pair of nodes with probability p, creating a graph with approximately $pN(N-1)/2$ randomly distributed links. The distribution of degree, $P(k)$, of an ER graph follows a Poisson distribution for large N. This indicates that the variation of degree is limited to a narrow range and all degrees are approximately equal to the average degree $\langle k \rangle$. Moreover, the tail of the $P(k)$ decreases exponentially resulting in, if ever, the rare existence of nodes that significantly deviate from $\langle k \rangle$. This topological property characterizes ER graphs as homogeneous networks typically limited in a single scale.

We generate a BA network based on two basic rules: growth and preferential attachment [34]. The model starts with the initial small number of m nodes. At every time step, a new node with M links is added to the network, which connects to already existing node i with probability $k_i / \sum_j k_j$, where k_i is the degree of node i, and j is the index denoting the sum over the network. The growth lasts until the total number of nodes reaches N. The degree distribution of BA network follows power-law function ($P(k) \sim k^{\alpha}$), indicating that the degree distribution can span several orders of magnitudes with non-negligible probability to have hubs which are nodes with extremely high k. When $P(k)$ is plotted on a log–log scale, it produces a linear curve typically with the slope $\alpha = 2$–3 [29]. Contrary to ER network, this topological property characterizes BA network to be heterogeneous and scale-invariant (also referred to as scale-free).

2.4. Resilience assessment

In this work, we expand upon previous vulnerability assessments and include dynamic recovery processes to assess network resilience. As a first step, we use static and dynamic analysis methods to measure network robustness: 'error and attack tolerance' [34,35] and 'cascading failure' [32,36], respectively. However, according to definitions of critical infrastructure resilience (cf., Refs. [37,38]), networks should not only be robust to absorb external perturbations but remain recoverable and adaptive during and after adverse events. Thus, resilience analysis builds upon methods for measuring robustness to include measures of recovery quality and speed [25]. In order to assess network resilience, we expand our dynamic analysis to include a recovery model that enables quantification of these processes.

2.4.1. Static analysis

Static analysis assesses the tolerance of a network to node removal. In this work, we evaluate network robustness using two failure scenarios: random error and intentional attack. In the random error scenario, we choose nodes to remove using uniform probability distribution and quantify damages to the network by measuring a difference in efficiency. Network losses investigated in this scenario are representative of those experienced via unpredicted natural disasters and human errors [39]. In the intentional attack scenario, we use degree and betweenness centrality to rank nodes; nodes are removed starting from the highest rank, and damages are measured using efficiency. Network losses quantified here are representative of, for instance, acts of terrorism that seek to cause the most harm to the entire network with the removal of important nodes. The efficiency (E) of the networks gradually changes over the fraction of the nodes removed but how much it degrades depends on the topology of networks and types of disturbance [35].

Please cite this article in press as: D.H. Kim, et al., Network topology and resilience analysis of South Korean power grid, Physica A (2016), http://dx.doi.org/10.1016/j.physa.2016.08.002

Table 2
Topological features of networks (KPG, random, and scale-free).

	KPG	Random	Scale-free
# of nodes (N)	2083	2051	2083
# of links (M)	2571	2482	2578
Mean degree ($\langle k \rangle$)	2.47	2.42	2.48
Maximum degree (k_{max})	18	8	128
Characteristic path length (L)	12.49	8.45	5.65
Diameter (D)	28	28	14
Initial efficiency (E_0)	0.09	0.11	0.19
Clustering coefficient (C)	50×10^{-3}	1.2×10^{-3}	3.3×10^{-3}
Network heterogeneity (H)	0.83	0.52	1.74

2.4.2. Dynamic analysis

Damages on a small part of a network can cause much larger losses in the function if the damage easily propagates to the whole system. Sometimes power facilities are overloaded due to an excess of power use or breakdown of a transmission line. The overloaded facilities decrease systems function and affect other neighboring facilities by redistributing the loads which consequentially causes the overloading of neighbors. This is the process of cascading failure in a power grid which is the reason for large-scale blackouts that occasionally occur [23,40]. Here, we use Crucitti–Latora–Marchiori (CLM) model [32]. If the electricity is transferred with equal probability from any generator to any distribution substation and that the electricity is delivered by the shortest path, then nodes with high betweenness refer to the nodes where the high load of electric power flow exists. With this assumption, the initial loads of nodes, $L_i(0)$, are first set up based on their betweenness, and the capacity, C_i, to handle the loads is defined by their tolerance parameter, α. When a node with the highest load is removed, the betweenness of all other nodes is recalculated, which gives the redistributed load after one iteration. Then the edge efficiency, e_{ij}, which was unity in initial phase, is recalculated in each iteration by the following equation,

$$e_{ij}(t+1) = \begin{cases} e_{ij}(0)\dfrac{C_i}{L_i(t)} & \text{if } L_i(t) > C_i \\ e_{ij}(0) & \text{if } L_i(t) < C_i \end{cases} \qquad C_i = \alpha L_i(0). \tag{2}$$

2.4.3. Recovery analysis

Once a network is damaged, it does not recover immediately, but it takes certain time until a recovery action takes place. We assume that the degree of damage, from where recovery action initiates, may affect how such actions taken are effective for retrieving the form and function of a network. In order to analyze network resilience, we develop a recovery model that brings failed nodes back into the network. After initiating cascading failures by removing a node and its links from the network, this node is assumed to start recovering its links during the cascade or after the degraded system reaches a steady-state. Only the links that are directly linked to the initially failed node begin with the full edge weight ($e_{ij} = 1$), and other links of which e_{ij} was degraded during cascading failure gradually recover following the algorithm which is similar to CLM model but in inverse form as in Eq. (3). That is, the edge weight, e_{ij}, only increases when the load, which is redistributed by the recovery of the failed node, is less than tolerance capacity.

$$e_{ij}(t+1) = \begin{cases} e_{ij}(0)\dfrac{C_i}{L_i(t)} & \text{if } L_i(t) \le C_i \\ e_{ij}(0) & \text{if } L_i(t) > C_i. \end{cases} \tag{3}$$

3. Results and discussion

3.1. Topological features of networks

Table 2 summarizes the results of basic topological analyses using selected metrics. KPG shows the highest characteristic path length (L) and diameter (D) with the lowest initial efficiency (E_0) compared to the random and scale-free networks with similar quantities of nodes and links. This result indicates that the KPG has an inefficient structure, as it requires longer paths to exchange the same amount of information or power compared to reference networks. However, it turns out that KPG has the small-world property by having relatively high clustering coefficient (C). Although the L of KPG is the greatest among the three networks, it satisfies the following criteria for being a small world, especially when it is compared with the random network [4,30]:

$$\begin{cases} C \gg C_{rand} \\ L \geq L_{rand} \end{cases} \tag{4}$$

Please cite this article in press as: D.H. Kim, et al., Network topology and resilience analysis of South Korean power grid, Physica A (2016), http://dx.doi.org/10.1016/j.physa.2016.08.002

Table 3
Small world index of KPG and other networks.

	N	M	C	C_{rand}	L	L_{rand}	C/C_{rand}	L/L_{rand}	SWI	Refs.
KPG	2083	2571	0.05	0.012	12.49	8.45	41.67	1.48	28.19	This work
Western US power grid	4941	6594	0.08	0.005	18.7	12.4	160.0	2.16	74.10	[30]
MAPP[a]	575	754	–	–	–	–	18.4	2.39	7.70	
Nordel[b]	410	564	–	–	–	–	21.4	2.37	9.03	[41]
KEPCO[c]	553	783	–	–	–	–	23.5	1.24	18.95	
ERCOT[d]	148	209	–	–	–	–	7.3	1.47	4.97	
Italian 380 kV	127	171	0.156	0.0005	8.47	4.89	320.64	1.73	185.12	
French 400 kV	146	223	0.279	0.0212	6.61	4.46	13.16	1.48	8.88	[17]
Spanish 400 kV	98	175	0.316	0.0209	4.92	3.60	15.10	1.37	11.06	
East China	769	1029	0.088	0.004	11.79	8.06	22.0	1.46	15.04	[42]

[a] Mid-continental area power pool network.
[b] Nordel network, the interconnected power systems of Finland, Norway, Sweden, and parts of Denmark.
[c] Korea electric power corporation network.
[d] Electric reliability council of texas network.

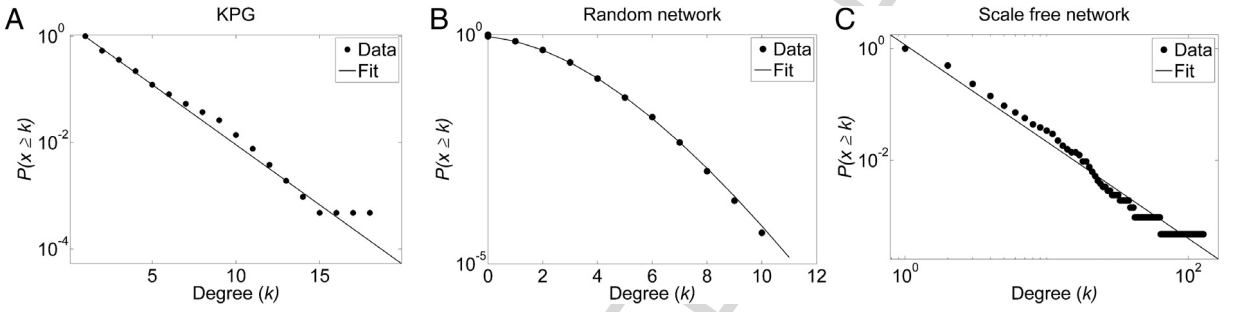

Fig. 1. Cumulative degree distributions of (A) KPG fitted with exponential distribution, (B) random network fitted with Poisson distribution and (C) scale-free network fitted with power-law distribution.

where, $C_{rand} \sim \langle k \rangle / N$ and $L_{rand} \sim \ln(N)/\ln(\langle k \rangle)$. We obtain C and L of the KPG as 0.05 and 12.49, respectively (Table 2), while C_{rand} and L_{rand} are calculated as 0.0012 and 8.45, respectively, satisfying the above criteria.

Kim and Obah [41] suggested small world-ness index ($SWI = [C/C_{rand}]/[L/L_{rand}]$) which enables more accurate evaluation of a network for its small world-ness. They calculated SWIs of several power grids which were in the range of 4.97–18.95, and concluded that these networks are characterized as small worlds. Using this same index, we obtain $SWI = 28.2$ for KPG, which is much greater than SWIs of these networks and it indicates that KPG is closer to a small world. We also compiled several power grids from other studies and calculated SWIs to compare with KPG (Table 3).

In spite of large L, electric power should be able to spread efficiently across the KPG due to large C. Watts and Strogatz [30] reported a similar trend for the US western power grid. Still, the calculated efficiency of the KPG is lower than reference networks, revealing that the KPG is, in fact, inefficient in its structure. Given these conflicting topological properties, we conclude that high C does not guarantee an efficient structure for a network even though it may increase the number of alternative paths. By having the small world property and a low efficiency, we verify that the KPG has a heterogeneity (H) between reference networks—higher than that of the random network and lower than the scale-free network. This result implies that the KPG has a higher probability of containing high connectivity nodes than a random network, but not as much as the scale-free network in which hubs exist.

Fig. 1 compares the cumulative degree distribution of the KPG to reference networks. Whereas various natural and technological networks are characterized by power-law degree distributions [43,44], power grids are one of the exceptions. While few studies found power grid networks have power-law degree distributions (cf., Ref. [30]), the cumulative degree distribution of the KPG is best described by a single-scaled exponential function (Fig. 1(A)). This result supports the vast majority of literature and suggests that the topology of power grids deviates from the universal behavior of other complex systems. One primary reason may be that the power grids are spatially embedded networks by which the growth of connectivity is constrained by geography, limiting the emergence of scale-free hubs, and resulting in an exponentially truncated degree distribution [45]. However, we also hypothesize that the use of partial information (i.e., only high voltage class infrastructure) and neglecting directionality and link weight (i.e., for spatial distance, electrical distance, or electrical flow) may cause the deviation of the network topology from the universal pattern of scale-invariant structure.

We tested our hypothesis by generating subnetworks of the KPG that incrementally include lower voltage class infrastructure (from 765 to 3.3 kV) and comparing their cumulative degree distributions (Fig. 2). As more information about the KPG is included in each network, the degree distribution shifts from the one with low variance (0.8 for only 765 kV infrastructure) to that with high variance (4.22 for the full KPG). In addition, the mean degree, $\langle k \rangle$, decreases while

Please cite this article in press as: D.H. Kim, et al., Network topology and resilience analysis of South Korean power grid, Physica A (2016), http://dx.doi.org/10.1016/j.physa.2016.08.002

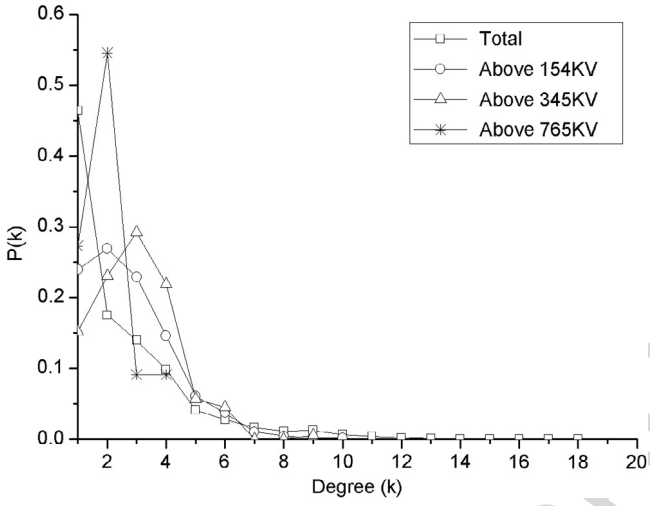

Fig. 2. Degree distributions of KPG over the different voltage levels.

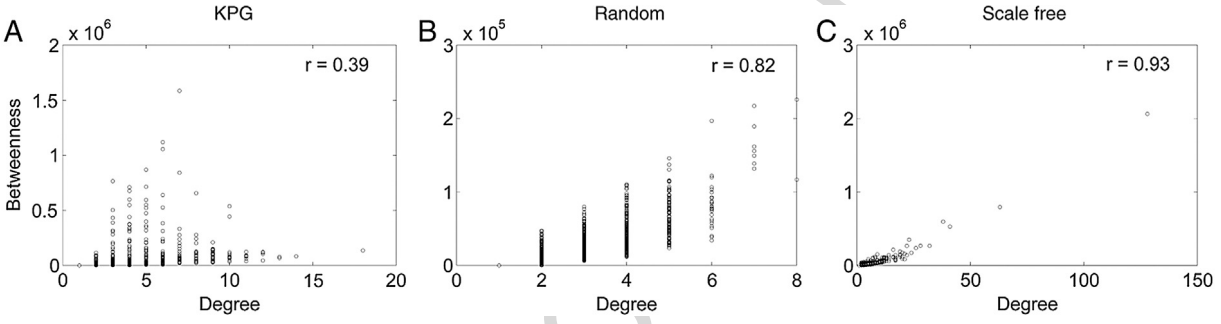

Fig. 3. Correlations between degree and betweenness for (A) KPG, (B) random network, and (C) scale-free network.

Table 4
Change of statistical characteristics of KPG by increasing the lower-voltage components.

	≥765 kV	≥345 kV	≥154 kV	≥19 kV	≥15 kV	Total
N	11	178	1367	1858	1926	2083
M	11	264	1854	2345	2414	2571
$\langle k \rangle$	2	2.97	2.71	2.52	2.51	2.47
σ_k^2	0.8	1.90	2.27	4.09	4.08	4.22
L	Inf	8.18	12.25	12.09	12.17	12.49
D	Inf	19	28	28	28	28
C	0.33	0.17	0.09	0.06	0.06	0.05
H	0.45	0.46	0.56	0.80	0.81	0.83
k_{max}	4	9	10	13	14	18

heterogeneity, H, increases (Table 4). This result indicates that inclusion of additional power grid data below 3.3 kV may eventually shift the exponential distribution found in Fig. 1(A) to a highly skewed, heavy tail distribution with scale-free properties. This result supports work by Chassin and Posse [46], in which the authors evaluate the reliability of the North American electric grid with the same model used here to generate a scale-free reference network. Since the dataset we analyzed is still far from the full network, our hypothesis remains inconclusive.

We also analyzed the correlation between degree and betweenness in each network (Fig. 3). The correlation between degree and betweenness is an important predictor of cascading failure dynamics, where a network with high correlation coefficient, r, and high H tends to have a few nodes that interact with a large proportion of network flow. If these nodes fail, cascades can quickly propagate to the entire system. The scale-free reference network has the highest correlation coefficient ($r = 0.93$) followed by the random network ($r = 0.82$), indicating that nodes with high connectivity also have high betweenness in both networks. In the KPG case, however, the correlation between degree and betweenness is lower ($r = 0.39$) indicating that betweenness and degree-based attack strategies will cause different cascading phenomena. More importantly, this result justifies the use of betweenness as a criterion for assessing node importance.

Please cite this article in press as: D.H. Kim, et al., Network topology and resilience analysis of South Korean power grid, Physica A (2016), http://dx.doi.org/10.1016/j.physa.2016.08.002

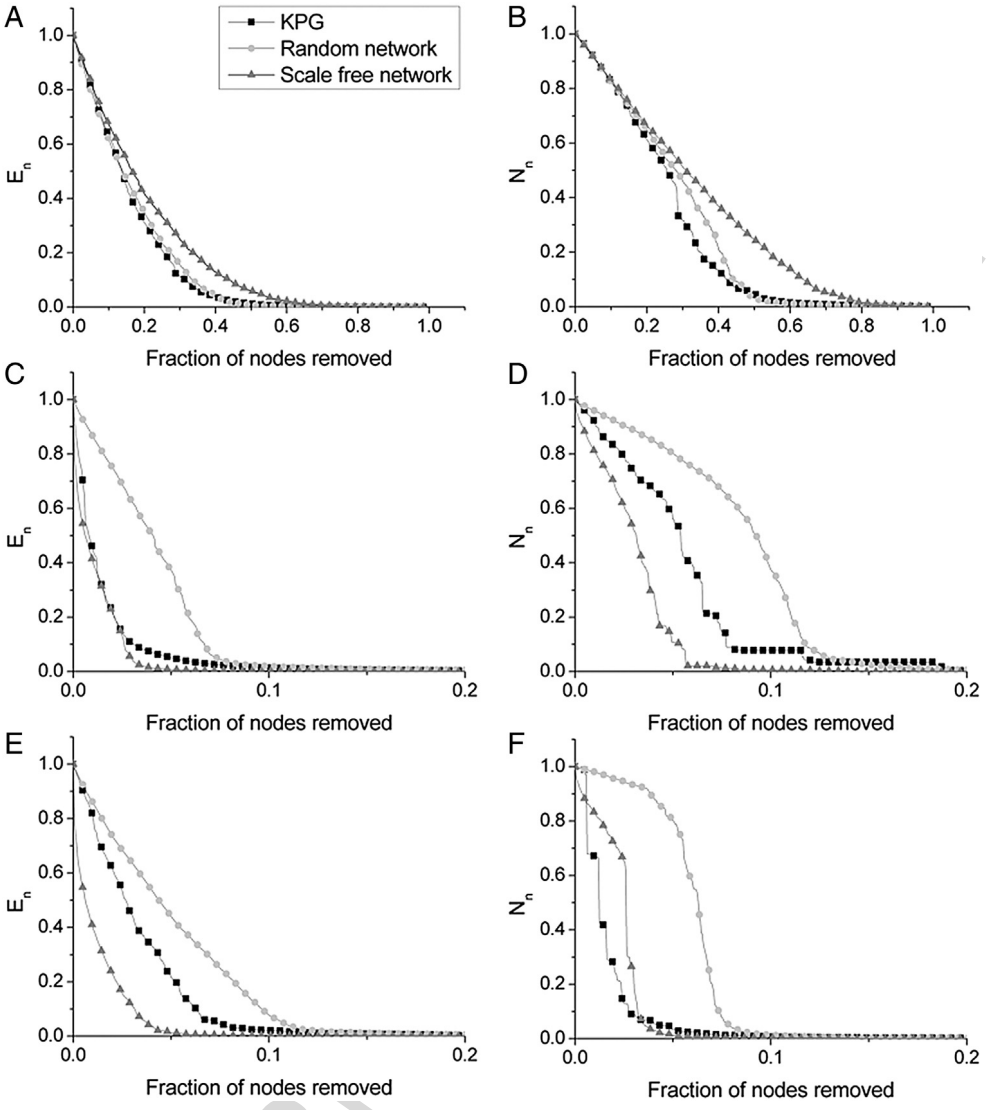

Fig. 4. Results of static vulnerability analysis to random node removal (A) and (B), degree-based attack (C) and (D), and betweenness-based attack (E) and (F). The first column shows the change of normalized efficiency E_n while the second column shows the normalized giant component size N_n.

3.2. Resilience analysis: error and attack tolerance

Figs. 4 and 5 present the error and attack tolerance results for KPG and reference networks under three node removal scenarios: random, degree-based, and betweenness-based removal. We measure the impact of node removal with two metrics: (1) normalized network efficiency, $E_n = E/E_0$, where E_0 is the initial network efficiency prior to node removal and E is the efficiency after, and (2) normalized giant component size, $N_n = N/N_0$. Results indicate that all networks are more robust against random removals than intentional attacks. After 20% of nodes are randomly removed, the values of E_n were 0.31, 0.35, and 0.42 for KPG, random, and scale-free networks, respectively (Fig. 4(A) and (B)) whereas E_n reached almost zero for all cases of intentional attack with the same portion of nodes removed (Fig. 4(C)–(F)). Although the KPG and random networks have similar losses in network efficiency (Fig. 4(A)), they have characteristic differences in the breakdown of their giant components (Fig. 4(B)). Fragmentation of the KPG occurs earlier than the random network when roughly 25% of nodes are randomly removed (Fig. 4(B)) while both E_n and N_n of scale-free network gradually drop without abrupt changes due to high portion of nodes with low connectivity resulting in the less occurrence of a large fragmentation.

The difference in the behavior of the three networks under intentional attacks is more prominent than random removals. As nodes are removed using degree-based methods, the KPG is more robust than the scale-free network but less than the random network (Fig. 4(C) and (D)). For betweenness-based removals, the E_n of the KPG is similar to that of the scale-free network, and N_n is the lowest among the three networks (Fig. 4(E) and (F)). This result suggests that topological analyses of power-grids with limited information predicting exponential degree distributions may overestimate their robustness to

Please cite this article in press as: D.H. Kim, et al., Network topology and resilience analysis of South Korean power grid, Physica A (2016), http://dx.doi.org/10.1016/j.physa.2016.08.002

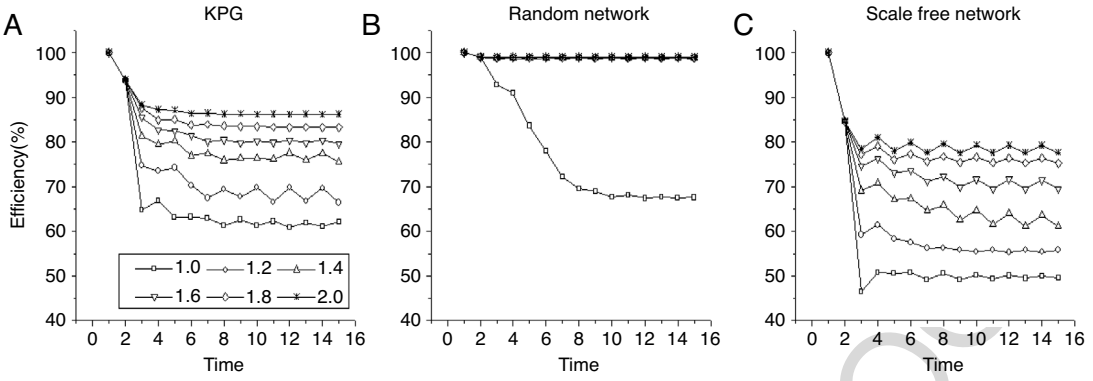

Fig. 5. Results of cascading failure analysis of (A) KPG, (B) random, and (C) scale-free networks.

intentional attacks. Although, the cumulative degree distribution of the KPG is more like the random network, with a single-scaled and less-skewed degree distribution, the KPG's high heterogeneity and maximum degree may be factors attributing to its breakdown to intentional attacks converges towards a scale-free network. Rosas-Casals et al. [4] also reported that the static tolerance of all the 33 networks in European power grid to errors and attacks was similar to scale-free networks instead of random networks, concluding that power grids are "exponential, but not that much".

3.3. Resilience analysis: cascading failures

Results for cascading failure analysis for all three networks are presented in Fig. 5. While multiple nodes are sequentially removed in the static vulnerability analysis, only one node is initially selected and removed in the dynamic vulnerability analysis. Results presented in Fig. 5 are for failures caused by removing the node with the highest betweenness for each network as it approximates the greatest potential for a large cascading failure.

Results, with varying the tolerance capacity α (from 1 to 2), show that cascading failure robustness decreases from the random network, to the KPG and scale-free networks. The scale-free network has the least robustness because of its highly correlated node degree and betweenness with high heterogeneity (Fig. 3). In the scale-free network, high betweenness nodes are also hub nodes with many links. When these nodes fail, network flow redistributes to numerous neighbors that are readily overloaded, and the efficiency of the whole network rapidly decreases. In the random network, degree and betweenness have a high correlation, yet, the nodes are more homogeneous with low connectivity, and network flow redistributes to fewer neighbors. The robustness of the KPG to cascading failures lies between these two reference cases due to its low correlation between degree and betweenness and high heterogeneity.

The effect of changing the tolerance capacity, α, on the robustness of KPG and the scale-free network was distinct from that of the random network. While the E_n, which was measured when the cascade of failure stabilized, of KPG and scale-free network incrementally increased with increasing α, the random network showed that only a slight increase in α (from 1 to 1.2) dramatically improved its robustness (from $E_n = 67\%$ to 99%). Increasing α from 1 to 2 improved the E_n from 61% to 86% for KPG and from 46% to 77% for scale-free network implying that enhancing network robustness through manipulating the tolerance capacity may not be sufficient, and it requires further or different strategies including topological redesign.

3.4. Recovery analysis

Here we test two factors that affect recovery performance of the networks: (1) time, t_r, when recovery initiates during or after the cascading failure and (2) initial tolerance capacity, α. Once recovery initiates, the global efficiency of the networks rapidly reaches to their final value. Thus, our analysis focuses on comparisons of this final efficiency instead of recovery time.

Fig. 6 presents E_n recovery results for various α values and recovery initiation times. Results indicate that faster recovery initiation (or, equivalently, the lower t_r) produces higher final efficiencies for all networks. For example, at $\alpha = 1$, the final E_n of the random network is 98% if the recovery starts the time step directly after initial node removal ($t_r = 2$), but it only reaches below 93% when the recovery starts after the E_n reached a steady-state post cascade ($t_r \geq 7$). For the scale-free network, final E_n values range from 92% ($t_r = 2$) to 89% ($t_r \geq 6$). The behavior of KPG is similar to the scale-free network, with worse final E_n values of 93% ($t_r = 2$) and 87% ($t_r \geq 7$) when $\alpha = 1$ due to a relatively high fluctuation. This result demonstrates that the agility of emergency response – to respond quickly after initial failures – is an important factor for determining overall system resilience. There is also a critical value for t_r, after which the recovery performance is more or less the same for each network. Finding these critical t_r values may serve as important thresholds for resilience analysis, before which irreversible malfunctioning of networks is preventable (see Fig. 7).

Please cite this article in press as: D.H. Kim, et al., Network topology and resilience analysis of South Korean power grid, Physica A (2016), http://dx.doi.org/10.1016/j.physa.2016.08.002

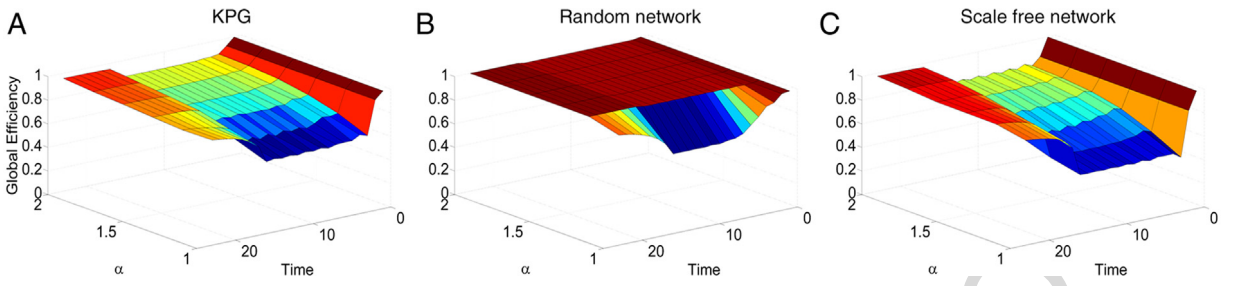

Fig. 6. Example results for the behavior of E_n over time step when the networks initiate recovery after E_n reached a steady-state post cascading failure.

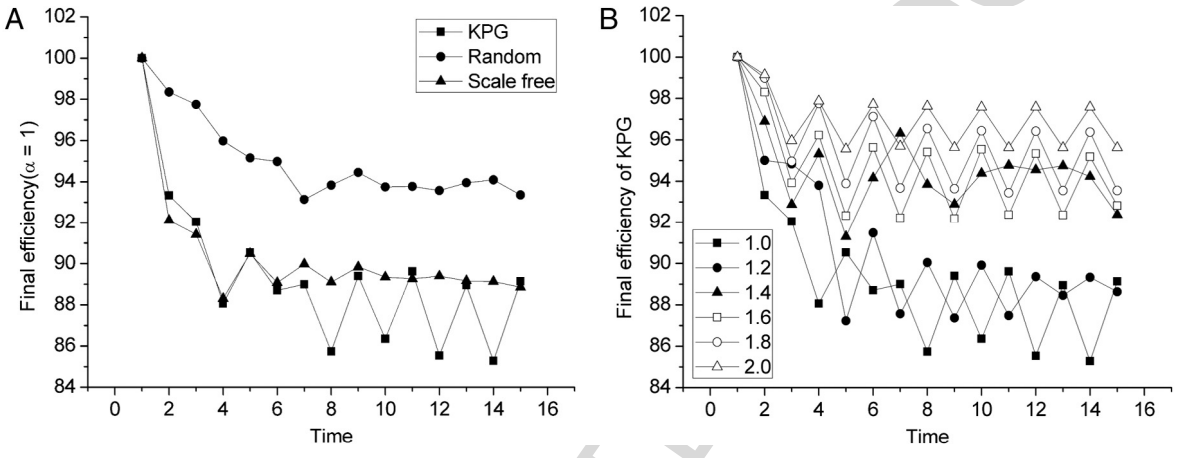

Fig. 7. (A) Final efficiency of the three networks over the recovery initiation time and (B) final efficiency of KPG with varying tolerance capacity.

The tolerance capacity (α) is important because increasing it improves network recovery and robustness to cascading failures by allowing higher values of E_n from which recovery starts. For example, for the random network, slight increases in α dramatically improves the robustness to the point that further recovery is not required. For the scale-free network, however, recovery with $\alpha = 1$ is $E_n = 92\%$ at best and 89% at worst but improves to about 98% regardless of t_r when α increases to 2. The recovery performance of KPG, when measured with the final E_n (87%–100% ($\alpha = 1$) and 97%–100% ($\alpha = 2$)), is similar to or sometimes worse than scale-free network although KPG begins recovery from higher initial E_n (61%–94% when $\alpha = 1$ and 86%–94% when $\alpha = 2$).

4. Conclusions

In this work, we analyzed the topology and resilience of the Korean Power Grid network by comparing results with random and scale-free reference networks. We find the degree distribution of the KPG to be an exponential distribution similar to those as reported by many previous studies on power grids, yet the KPG has higher characteristic path length and clustering coefficient than the random network characterizing it as a small world system. Moreover, the heterogeneity of KPG is greater than the random network but lower than the scale-free network, implying that the KPG is likely to contain a hub-like structure. Moreover, analysis of KPG subnetworks of varying network size by sequentially adding lower voltage components showed that the variance of degree gradually increases while the average degree decreases. This result implies that topological analysis with an addition of low voltage class data (e.g., for distribution infrastructure) may eventually produce a highly skewed degree distribution.

We assess the resilience of the KPG in three different ways: (1) error and fault tolerance, (2) cascading failure robustness, and (3) recovery analysis. For error and fault tolerance, the KPG is the most vulnerable network when subjected to random node removal. In contrast, the KPG showed modest performance when nodes are intentionally removed by degree-based strategies whereas it again became the most vulnerable one when nodes were intentionally removed by the betweenness. This analysis demonstrates that only taking a structural perspective based on node degree does not capture the static robustness of a network, and, when a correlation between degree and betweenness is low, multiple attack strategies should be tested.

The cascading failure analyses reveal that the robustness of the KPG is higher than the scale-free network and lower than the random network for the same tolerance coefficient. When the tolerance coefficient doubles, the normalized efficiency E_n of the KPG measured in steady-state dramatically improves from 61% to 86%. In case of scale-free network, the E_n declines rapidly due to the existence of hubs with high loads. After recovery, however, scale-free network generally shows a better

Please cite this article in press as: D.H. Kim, et al., Network topology and resilience analysis of South Korean power grid, Physica A (2016), http://dx.doi.org/10.1016/j.physa.2016.08.002

performance than KPG although the difference between the final E_n values is small. For the random network, reduction in E_n during the cascading failure is low due to a homogeneous structure and relatively low correlation between degree and betweenness. Moreover, network recovery is small due to minimal damages incurred from failures. The KPG, on the other hand, suffers larger collapse and recovery than the random network but lower than scale-free network due to the existence of functional hubs without structural hubs (i.e., low correlation between degree and betweenness). Still, the KPG is the least robust network after full recovery.

Based on our results, we make several suggestions to improve resilience of the KPG and similar networked infrastructure systems. Since the KPG is most vulnerable to betweenness-based intentional attacks, the power grid should be designed so loads are homogeneously distributed and decentralized. This design strategy is also consistent with recently proposed novel architectures, such as smart-grid and micro-grid, which typically pursue localized and distributed generation and homogeneous load reduction [47,48]. If it is unavoidable to have functional hubs in the power grid, then functional hubs and their neighbors should be given a higher tolerance capacity. Taken together, the damage the KPG suffers can be dramatically reduced, and a full network recovery post failure will have improved chances. Finally, recovery performance is dependent on when recovery begins, where early and agile recovery responses are important when the potential damage is high. Damage is reduced if collapse is sensed early and recovery actions immediately take place.

Acknowledgments

This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Science, ICT & Future Planning (NRF-2016R1C1B1011770). DE was supported by the National Science Foundation awards #1441352, 1311230, and 1415060. Any opinions, findings, conclusions, or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the NSF. Some of the works in this paper were conducted during the 2015 Synthesis Workshop on "Dynamics of Structure and Functions of Complex Networks" held in Korea University, Seoul, Korea.

References

[1] NRC, Sustainable Critical Infrastructure Systems — a Framework for Meeting 21st-century Imperatives, Washington, DC, 2009.
[2] S.E. Chang, Infrastructure resilience to disasters, Bridg. 44 (2014) 36–41.
[3] M. Newman, Networks: An Introduction, Oxford University Press, Oxford, U.K, 2010.
[4] M. Rosas-Casals, S. Valverde, R.V. Solé, Topological vulnerability of the European power grid under errors and attacks, Internat. J. Bifur. Chaos 17 (2007) 2465–2475. http://dx.doi.org/10.1142/S0218127407018531.
[5] G.A. Pagani, M. Aiello, The power Grid as a complex network: A survey, Physica A 392 (2013) 2688–2700. http://dx.doi.org/10.1016/j.physa.2013.01.023.
[6] L. Dueñas-Osorio, S.M. Vemuru, Cascading failures in complex infrastructure systems, Struct. Saf. 31 (2009) 157–167. http://dx.doi.org/10.1016/j.strusafe.2008.06.007.
[7] S. Lämmer, B. Gehlsen, D. Helbing, Scaling laws in the spatial structure of urban road networks, Physica A 363 (2006) 89–95. http://dx.doi.org/10.1016/j.physa.2006.01.051.
[8] J. Zhang, X. Xu, L. Hong, S. Wang, Q. Fei, Networked analysis of the Shanghai subway network, in China, Physica A 390 (2011) 4562–4570. http://dx.doi.org/10.1016/j.physa.2011.06.022.
[9] R. Carvalho, L. Buzna, F. Bono, M. Masera, D.K. Arrowsmith, D. Helbing, Resilience of natural gas networks during conflicts, crises and disruptions, PLoS One 9 (2014) e90265. http://dx.doi.org/10.1371/journal.pone.0090265.
[10] A. Yazdani, P. Jeffrey, Complex network analysis of water distribution systems, Chaos 21 (2011) 016111. http://dx.doi.org/10.1063/1.3540339.
[11] C.D. Brummitt, R.M. D'Souza, E.a. Leicht, Suppressing cascades of load in interdependent networks, 109 (2011) 13. http://dx.doi.org/10.1073/pnas.1110586109.
[12] KEPCO, STATISTICS OF ELECTRIC POWER IN KOREA, 2015.
[13] S.V. Buldyrev, R. Parshani, G. Paul, H.E. Stanley, S. Havlin, Catastrophic cascade of failures in interdependent networks, Nature 464 (2010) 1025–1028. http://dx.doi.org/10.1038/nature08932.
[14] M. Ouyang, Review on modeling and simulation of interdependent critical infrastructure systems, Reliab. Eng. Syst. Saf. 121 (2014) 43–60. http://dx.doi.org/10.1016/j.ress.2013.06.040.
[15] L. Cuadra, S. Salcedo-Sanz, J. Del Ser, S. Jiménez-Fernández, Z. Geem, A critical review of robustness in power grids using complex networks concepts, Energies 8 (2015) 9211–9265. http://dx.doi.org/10.3390/en8099211.
[16] R. Albert, I. Albert, G.L. Nakarado, Structural vulnerability of the North American power grid, Phys. Rev. E 69 (2004) 025103. http://dx.doi.org/10.1103/PhysRevE.69.025103.
[17] V. Rosato, S. Bologna, F. Tiriticco, Topological properties of high-voltage electrical transmission networks, Electr. Power Syst. Res. 77 (2007) 99–105. http://dx.doi.org/10.1016/j.epsr.2005.05.013.
[18] R.V. Solé, M. Rosas-Casals, B. Corominas-Murtra, S. Valverde, Robustness of the European power grids under intentional attack, Phys. Rev. E (3) 77 (2008) 1–7. http://dx.doi.org/10.1103/PhysRevE.77.026102.
[19] G.A. Pagani, M. Aiello, Power grid complex network evolutions for the smart grid, Physica A 396 (2014) 248–266. http://dx.doi.org/10.1016/j.physa.2013.11.022.
[20] G.A. Pagani, M. Aiello, Towards decentralization: A topological investigation of the medium and low voltage grids, IEEE Trans. Smart Grid 2 (2011) 538–547. http://dx.doi.org/10.1109/TSG.2011.2147810.
[21] J. Gao, X. Liu, D. Li, S. Havlin, Recent progress on the resilience of complex networks, Energies 8 (2015) 12187–12210. http://dx.doi.org/10.3390/en81012187.
[22] R. Cohen, K. Erez, D. Ben-Avraham, S. Havlin, Resilience of the Internet to random breakdowns, Phys. Rev. Lett. 85 (2000) 4626–4628. http://dx.doi.org/10.1103/PhysRevLett.85.4626.
[23] R. Kinney, P. Crucitti, R. Albert, V. Latora, Modeling cascading failures in the North American power grid, Eur. Phys. J. B 46 (2005) 101–107. http://dx.doi.org/10.1140/epjb/e2005-00237-9.
[24] E. Negeri, F. Kuipers, N. Baken, Designing reliable and resilient smart low-voltage grids, Int. J. Crit. Infrastruct. Prot. 9 (2015) 24–37. http://dx.doi.org/10.1016/j.ijcip.2014.12.006.

Please cite this article in press as: D.H. Kim, et al., Network topology and resilience analysis of South Korean power grid, Physica A (2016), http://dx.doi.org/10.1016/j.physa.2016.08.002

[25] A.A. Ganin, E. Massaro, A. Gutfraind, N. Steen, J.M. Keisler, A. Kott, et al., Operational resilience: concepts, design and analysis, Sci. Rep. 6 (2016) 19540. http://dx.doi.org/10.1038/srep19540.
[26] D.L. Alderson, G.G. Brown, W.M. Carlyle, Operational models of infrastructure resilience, Risk Anal. 35 (2015) 562–586. http://dx.doi.org/10.1111/risa.12333.
[27] M.A.S. Monfared, M. Jalili, Z. Alipour, Topology and vulnerability of the Iranian power grid, Physica A 406 (2014) 24–33. http://dx.doi.org/10.1016/j.physa.2014.03.031.
[28] K.-I. Goh, B. Kahng, D. Kim, Universal behavior of load distribution in scale-free networks, Phys. Rev. Lett. 87 (2001) 278701. http://dx.doi.org/10.1103/PhysRevLett.87.278701.
[29] A.-L. Barabasi, R. Albert, Emergence of scaling in random networks, Science 286 (1999) 509–512. http://dx.doi.org/10.1126/science.286.5439.509.
[30] D. Watts, S. Strogatz, Collective dynamics of "small-world" networks, Nature 393 (1998) 440–442. http://dx.doi.org/10.1038/30918.
[31] V. Latora, M. Marchiori, Efficient behavior of small-world networks, Phys. Rev. Lett. 87 (2001) 198701. http://dx.doi.org/10.1103/PhysRevLett.87.198701.
[32] P. Crucitti, V. Latora, M. Marchiori, Model for cascading failures in complex networks, Phys. Rev. E 69 (2004) 45104. http://dx.doi.org/10.1103/PhysRevE.69.045104.
Q8 [33] P. Erdös, a Rényi, On random graphs, Publ. Mat. 6 (1959) 290–297. http://dx.doi.org/10.2307/1999405.
[34] R. Albert, H. Jeong, A.-L. Barabási, Error and attack tolerance of complex networks, Nature 406 (2000) 378–382. http://dx.doi.org/10.1038/35019019.
[35] P. Crucitti, V. Latora, M. Marchiori, A. Rapisarda, Error and attack tolerance of complex networks, Physica A 340 (2004) 388–394. http://dx.doi.org/10.1016/j.physa.2004.04.031.
[36] A.E. Motter, Y.C. Lai, Cascade-based attacks on complex networks, Phys. Rev. E 66 (2002) 2–5. http://dx.doi.org/10.1103/PhysRevE.66.065102.
[37] S.L. Cutter, J.A. Ahearn, B. Amadei, P. Crawford, E.A. Eide, G.E. Galloway, et al. Disaster Resilience: A National Imperative, 2013. http://dx.doi.org/10.1080/00139157.2013.768076.
[38] J. Park, T.P. Seager, P.S.C. Rao, M. Convertino, I. Linkov, Integrating risk and resilience approaches to Catastrophe management in engineering systems, Risk Anal. 33 (2013) 356–367. http://dx.doi.org/10.1111/j.1539-6924.2012.01885.x.
[39] S. Wang, L. Hong, X. Chen, Vulnerability analysis of interdependent infrastructure systems: A methodological framework, Physica A 391 (2012) 3323–3335. http://dx.doi.org/10.1016/j.physa.2011.12.043.
[40] I. Dobson, B.a. Carreras, V.E. Lynch, D.E. Newman, Complex systems analysis of series of blackouts: Cascading failure, critical points, and self-organization, Chaos 17 (2007) 1–13. http://dx.doi.org/10.1063/1.2737822.
[41] C.J. Kim, O.B. Obah, Vulnerability assessment of power grid using graph topological indices, Int. J. Emerg. Electr. Power Syst. 8 (2007) http://dx.doi.org/10.2202/1553-779X.1738.
[42] P. Han, M. Ding, Analysis of cascading failures in small-world power grid, Int. J. Energy Sci. 1 (2011) 99–104.
[43] S. Boccaletti, V. Latora, Y. Moreno, M. Chavez, D.U. Hwang, Complex networks: Structure and dynamics, Phys. Rep. 424 (2006) 175–308. http://dx.doi.org/10.1016/j.physrep.2005.10.009.
[44] M.E.J. Newman, The structure and function of complex networks, SIAM Rev. 45 (2003) 167–256. http://dx.doi.org/10.1137/S003614450342480.
[45] L. a Amaral, a Scala, M. Barthelemy, H.E. Stanley, Classes of small-world networks, Proc. Natl. Acad. Sci. USA 97 (2000) 11149–11152. http://dx.doi.org/10.1073/pnas.200327197.
Q9
[46] D.P. Chassin, C. Posse, Evaluating North American electric grid reliability using the Barabasi-Albert network model, Physica A 355 (2005) 667–677. http://dx.doi.org/10.1016/j.physa.2005.02.051.
[47] X.C.X. Chen, H.D.H. Dinh, B.W.B. Wang, Cascading failures in smart grid - benefits of distributed generation, in: First IEEE Int. Conf. Smart Grid Commun. (SmartGridComm), 2010, IEEE, Gaithersburg, MD, 2010, pp. 73–78. http://dx.doi.org/10.1109/SMARTGRID.2010.5622022.
[48] S. Pahwa, A. Hodges, C. Scoglio, S. Wood, Topological analysis of the power grid and mitigation strategies against cascading failures, in: 2010 IEEE Int. Syst. Conf., IEEE, San Diego, CA, 2010, pp. 272–276. http://dx.doi.org/10.1109/SYSTEMS.2010.5482329.