The clique approach to identifying critical elements in gas transmission networks

Sergey Vorobev[1*], *Anton* Kolosnitsyn[1] and *Ilya* Minarchenko[1]

[1]Melentiev Energy Systems Institute, 130 Lermontov str., Irkutsk, Russia

Abstract. We consider the gas transmission network operating on the territory of the Russian Federation. This network includes gas fields, gas consumers, nodal compressor stations, underground gas storages, which, depending on the given scenario of the system operation, can act as gas sources or gas consumers. The nodes are connected by means of gas pipelines. Because natural gas is used in heat and power engineering and electricity, the gas transmission network may be exposed to terrorist threats, and the actions of intruders may be directed both at gas production facilities and gas pipelines. To simulate intruders attacks, a model of the attacker-defender type was proposed. In this model, the defender, represented by the system operator, solves the problem of finding the maximum flow to meet the needs of gas consumers. The attacker, in turn, attempts to minimize the maximum flow in the gas transmission network by excluding either nodes or gas pipelines. Gas transmission networks in Russia and Europe are very extensive, ramified, and have many bridges and reserve gas pipelines. Therefore, to inflict maximum damage to the system, attacks on cliques, that is, on several interconnected objects, are modelled. The article presents the results of test calculations, in which we identify the most significant combinations of objects in the gas transmission network in terms of the potential threat from terrorist attacks.

1 Introduction

Ensuring an uninterrupted supply of fuel and energy resources to consumers and safeguarding overall energy security is a matter of high state concern [1]. Large-scale energy accidents due to the breakdown of various critical energy network facilities entail considerable damage for consumers in terms of severe shortages of end use energy. Therefore, major current challenges include searching for and defining critical elements and their combinations in energy networks.

The above is confirmed by research on energy networks currently conducted all over the world. The studies [2, 3] focus on various issues concerning the modeling of energy networks as critical infrastructures. Researchers also investigate the vulnerability of critical energy infrastructures to acts of terrorism and risk analysis methods for interdependent critical infrastructures in extreme weather conditions [4, 5]. Probabilistic risk assessment methods are adopted when an infrastructure vulnerability assessment is impossible for want of sufficient information [6–9]. If relevant data is available, statistics theory is applied to analyze and forecast the impacts of natural disasters on infrastructure performance [10]. Network approaches, such as complex network theory, are used consider infrastructure topology when analyzing its structural vulnerability [11]. The latest international research places increased emphasis on interconnected infrastructures [12] and the effects of interactions between them on their vulnerability [13, 14].

Natural gas is the dominant boiler and furnace fuel in the Russian energy sector, and the share of fuel consumption by Russia's electric power industry amounts to about 75%. In case of disruptions occurring in the gas sector during periods of peak gas consumption, the amount of electrical power supplied to consumers may decrease by 50% to 60% in certain areas. As of now, about 90% of Russian natural gas is extracted in one gas producing region, i.e. in the north of Tyumen Oblast, located 2,000–2,500 kilometers from main gas consumption areas and 4,000–5,000 kilometers from gas-importing countries. Consequently, almost all Russian gas is transported over long distances through main gas pipelines having many mutual intersections and cross junctions; moreover, major gas pipelines often run at short distances one from another.

Current research suggests that consumers in regions will face considerable shortages of end use energy after accidents occuring at the important intersections of main gas pipelines [15]. In addition to main gas pipeline intersections, industrial and nodal compression stations as well as the linear sections of main gas corridors can also be potentially dangerous to the proper functioning of the network. Work is being done to specify, out of all potentially dangerous facilities listed above, the most significant ones and their combinations, followed by the development of measures intended to enhance these facilities' operational reliability with a view to maintaining uninterrupted fuel supply to consumers.

* Corresponding author: seregavorobev@isem.irk.ru

A number of studies have been undertaken to identify critical facilities in gas transmission networks. A list was compiled of the main gas pipeline intersections within the Unified Gas Supply System of Russia whose disruption will lead to a system-wide shortage of daily gas supply equal to or exceeding 5% [15]. Research was conducted to search for and identify combinations of various sections of main gas pipelines where a simultaneous disruption may result in a considerable shortage of daily gas supply (5% and more) across the entire network [16, 17]. Based on practical experience and analysis of current international research [15, 18], a methodology was elaborated, using the Russian gas sector as an example, to draw up lists of critical facilities in energy networks in order to ensure the latter's efficiency.

The above studies used the trial-and-test method to identify critical facilities and their combinations. Multiple iterational tests were carried out during which all elements and pairs of elements were turned off, one by one, in the network under investigation. As a result, the network elements and their combinations were identified which, if disrupted, would lead to the greatest shortage of gas within the network. Cases of simultaneous shutdown of three or more network elements were not taken into consideration due to computational limitations. Nonetheless, such cascade emergencies are possible, given the operational specifics of the gas transmission network. This is why, to take a comprehensive and detailed account of various factors in researching critical facilities, this study uses the maximum clique problem aimed at detecting the most interconnected sections of the gas transmission network which, if disrupted, could inflict maximum damage to the network in terms of reduced gas supply to consumers. Another justification for using of the maximum clique problem is the wide geographical distribution of facilities in the Russian gas transmission system. Intruders may have difficulties coordinating terrorist attacks in the wide territory of the Russian Federation. Therefore, a more reasonable approach to planning attacks on gas transmission system facilities may be to consider those objects that are located relatively close to each other, which fits into a clique approach of threats identification.

The clique problem is formulated as part of a methodology for modeling attacks on infrastructures. This methodology connects two sides into a single mathematical framework: an attacker and a defender. Such models are based on a class of Stackelberg network interdiction games [19] in which two actors, a leader and a follower, have opposite interests. Considering the given resource limitations, the leader aims to maximize the damage inflicted to the follower by reducing the network's transmission capacity, increasing transport costs at certain arcs or removing nodes or arcs from a network model. The follower solves his optimization problem (searching, for instance, for the maximum flow of a specific resource throughout the network, etc.) in the network modified by the leader [20]. Importantly, the mathematical description of such problems can be reduced to the attacker-defender, defender-attacker and defender-attacker-defender multilevel optimization models that have found widespread application in research on threat modelling and counter measures at various critical infrastructures [21–27]. In a sense, such models identify the best possible protective action plan within a limited budget.

The present study focuses mostly on the safe operation of the Russian gas transmission network in terms of security against terrorism. To this end, the authors will examine an attacker-defender model in which the solution of the attacker's problem is based on maximum clique search. The defender's objective is to ensure the maximum gas flow through the network. This approach will identify the critical network nodes and combinations whose failure results in the largest decrease of the network's overall transmission capacity. The weighted maximum clique problem will also be considered to account for disparities between different nodes of the gas transmission network.

The paper is structured as follows. In Part 2, a brief overview will be provided of the above-mentioned defender-attacker, attacker-defender and defender-attacker-defender models. Part 3 presents a mathematical model of the Russian gas transmission network and a description of the problem of finding the maximum gas flow through the transmission network. Part 4 deals with maximum clique search. Finally, Part 5 articulates the attacker-defender model and identifies cliques using the Russian gas transmission network as an example. In the conclusion, the authors sum up the main findings of the study.

2 Threat Modeling at Critical Infrastructures

2.1. The Attacker-Defender Model

The attacker-defender model [21] is based on the optimization model of an infrastructure network with an objective function representing either its value or expenses from the defender's perspective.

Let us consider that the defender operating the network minimizes expenses represented by the following linear function:

$$\min_{y \in Y} \langle c, y \rangle,$$

where c is a vector of operating expenses and y represents choices or actions related to network operation under given constraint $y \in Y$.

The attacker tries to maximize the optimal operational expenses by forbidding a set of steps represented by the vector y. Let $x_k = 1$ correspond to an attack on the network element k and, otherwise, $x_k = 0$. Then, x is a vector of the attacker's choices, i.e. his plan of attack. Let us consider that, if $x_k = 1$, the network element k crashes, and $y_j = 0$ for any action j related to the network element under attack. Therefore, the attack on the network element k forbids any set of actions directly dependent on this network element. Some reasonable constraints on the attacker's resources combined with the

binary type of variable x are representative of the constraint $x \in X$ whereas $Y(x)$ is a set of the defender's feasible actions limited by the plan of attack x. As a result, the attacker solves the following type of problem:

$$\max_{x \in X} \min_{y \in Y(x)} \langle c, y \rangle, \quad (1)$$

which is a bilevel optimization problem. Based on Stackelberg game theory, it comprises a number of key principles: the attacker and the defender act in a consistent manner; the attacker has at his disposal a complete model of the defender's optimal operation of the network even after an attack; and the attacker will manipulate the network to his greatest advantage.

The model (1) allows the attacker to perform a variety of actions. As an example, the aim of an attack may be to increase the defender's expenses rather than to limit his set of actions. The attacker can also reduce the value of network elements to the point of entirely excluding them.

2.2. The Defender-Attacker Model

In the attacker-defender model [21], the solution depends on numerous key network elements. The defender uses the available information to devise a protection plan with a view to minimizing the greatest damage on the attacker's art, which produces a complex three-level defender-attacker-defender model. However, in cases where the internal problem of network parameter optimization is lacking or is solved in a trivial way, the result will be a bilevel defender-attacker model:

$$\min_{w \in W} \max_{x \in X(w)} g(w, x),$$

where w is a vector of the defender's choices, W is its feasible set and g is the objective function representative of the damage inflicted to the network. Defender-attacker models occur, for example, in territorial boundary patrol problems [21].

2.3. The Defender-Attacker-Defender Model

This section focuses on the mathematical framework of the three-level defender-attacker-defender optimization models [21] permitting an accurate solution under some natural assumptions, i.e. it provides the best possible set of protective measures for infrastructures. In planning protective measures, an important assumption is the attacker's reasonably limited resources; for instance, in case of energy networks, such a limitation may be the upper bound of the number of facilities under attack.

Generally, the defender-attacker-defender model looks as follows with account taken of (1):

$$\min_{w \in W} \max_{x \in X(w)} \min_{y \in Y(x)} \langle c, y \rangle. \quad (2)$$

For the sake of simplicity, we assume that, if the network element k is protected, i.e. $w_k = 1$, this element becomes invulnerable. Let $h^+ \equiv \max\{0, h\}$ be component-wise for the arbitrary vector h, then the vector $(x - w)^+$ is a plan of attack being part of the attacker's plan x as opposed to the defender's plan w. The result is a three-level optimization problem formulated as follows:

$$\min_{w \in W} \max_{x \in X} \min_{y \in Y} \langle c, y \rangle, \quad 0 \le y \le D(1 - (x - w)^+), \quad (3)$$

where $D = \mathrm{diag}(d)$, d is a vector with the highest y component values permitted by the network. A number of specificities to be considered when solving the problem (3) are presented in [21]. The authors highlight the possibility to solve this three-level optimization problem in the same way as the defender-attacker problem using Bender's decomposition. In doing so, various techniques have been adopted within the decomposition algorithm to find a solution to the problem (3) [28].

Generally, the problem (2) is difficult to solve, given that it is often impossible to reduce it to mixed-integer programming problem and complex decomposition techniques are to be applied [21].

3 Identifying the Maximum Gas Flow in the Russian Transmission Network

Russia's vast gas transmission network is made of 388 nodes, including the following: 96 consumers, 33 producers, 29 underground gas storage facilities and 230 nodal compressor stations. Nodes with underground gas storage facilities may be used within the network as both gas consumers (if gas storage is required) and producers (if accumulated gas is needed to meet consumer demand). Internodal connection is ensured by 755 gas pipelines.

Network operators have access to the following information about the gas transmission network specifications: gas production volume at production nodes, amount demanded at consumption nodes, capacity of underground gas storage facilities and the transmission capacity of gas pipelines.

The task facing network operators is to determine whether the gas transmission network can provide consumers with the required amount of gas under given network specifications, the transmission capacity of pipelines and the existing production volume. For this purpose, a maximum flow problem is set up [29], in which the following symbols are used: n is the total number of nodes in the model; m is the total number of arcs in the model; I is a set of numbers corresponding to the model's nodes ($I = \{1, 2, ..., n\}$); $I_p \subset I$ is a set of numbers corresponding to producers' nodes; $I_c \subset I$ is a set of numbers corresponding to consumers' nodes; $I_0 \subset I$ is a set of numbers corresponding to branch nodes; f is the value of the total network flow; U is the symmetric adjacency $n \times n$-matrix with elements

$$u_{ij} = \begin{cases} 1, \text{ node } i \text{ is adjacent to node } j, \\ 0, \text{ node } i \text{ is not adjacent tonode } j; \end{cases}$$

x_{ij} is the flow rate outcoming from node i and incoming to node j; the corresponding arc is designated as (i, j)

, $i, j \in I$; d_{ij} is the maximum value of the flow rate along the arc (i, j), $i, j \in I$; b_i, $i \in I_p$ is the total gas production; b_i, $i \in I_c$ is the total gas consumption; i_O is the number of a fictitious node, which is a cumulative source

$$b_{i_O} = \sum_{i \in I_p} b_i,$$

i_S is the number of a fictitious node, which is a cumulative runoff

$$b_{i_S} = \sum_{i \in I_c} b_i.$$

The maximum flow problem has the following interpretation: the aim is to find the greatest possible amount of gas that can be transmitted throughout the network under the given specifications of internodal links accounting for the lines' established transmission capacity, available production volumes and the given consumption volumes. Finding a solution to the maximum flow problem determines whether the network can provide consumers with the required gas volume delivered to them along gas transmission lines. Such a problem statement does not consider the gas flow rate for the gas transmission network's in-house needs. To take account of this flow rate, this study increased the system-wide gas flow rate by 10%, this figure being based on numerous previous technical and economic research studies on the operation of Russia's gas transmission network [30].

The following additional operations are to be performed to ensure the proper functioning of the maximum flow algorithm. Add to the set I two fictitious nodes numbered i_O and i_S. Connect all production nodes to the fictitious node i_O:

$$u_{ij} = 1, \quad i = i_O, \quad j \in I_p.$$

Set the transmission capacity of lines d_{ij}, $i = i_O$, $j \in I_p$ as equal to the production volume in nodes $j \in I_p$. Connect all the nodes of consumers to the fictitious node i_S:

$$u_{ij} = 1, \quad i \in I_c, \quad j = i_S.$$

Set the transmission capacity of lines d_{ij}, $i \in I_c$, $j = i_S$ as equal to the consumption volume in nodes $i \in I_c$. Set the equality of variables:

$$x_{ij} = x_{ji}, \quad i, j \neq \{i_O, i_S\}.$$

Estimate the transmission capacity of lines taking account of the symmetric adjacency matrix U:

$$0 \le x_{ij} \le d_{ij}, \quad 0 \le x_{ji} \le d_{ij}, \quad i \in I, j \in I.$$

Define the matrix $\bar{U}$ with elements $\bar{u}_{ij}$, $i, j \in I$, identified as follows:

$$\bar{u}_{ij} = \begin{cases} u_{ij}, & \text{if } i < j, \\ -u_{ij}, & \text{if } i > j. \end{cases}$$

The problem statement for calculating maximum flow will look as follows:

$$\max f,$$
$$\sum_{j \in I} \bar{u}_{ij} x_{ij} = \begin{cases} -f, i = i_O, \\ 0, i \notin \{i_O, i_S\}, \ i \in I, \\ f, i = i_S, \end{cases} \tag{4}$$
$$x_{ij} = x_{ji}, \quad i, j \notin \{i_O, i_S\},$$
$$0 \le x_{ij} \le d_{ij}, \quad i \in I, \ j \in I.$$

The problem (4) solved, the network operator gains access to the information on the gas transmission network's capacity to shut consumer load. Additionally, it becomes possible to detect the so-called weak points, i.e. fully loaded sections of the pipeline as well as sections having important transmission reserves. These data can facilitate modifications to the gas transmission network's specifications in terms of increasing or decreasing the transmission capacity of these or those gas lines taking into account consumer load.

4 Setting Up the Maximum Clique Problem

The most vulnerable targets for attacks within the Russian gas transmission network are suggested to be defined as combinations of interconnected nodes. In other words, the maximum clique problem is set up [31], which can be clarified with terms from graph theory.

A gas transmission network can be represented as a directed graph in the nodes of which are located gas processing plants, gas consumers, underground storage facilities and compressor stations. Gas transmission pipelines are the edges of such a graph. The main objective of an offender is to cause maximum damage to the gas transmission network, that is, to reduce the maximum gas flow through the pipelines by attacking and rendering inoperative the network's major facilities. Needless to say, in planning an attack and searching for the clique, the fictitious nodes i_O, i_S are not considered.

Let us assume that the attacker is solving the maximum clique problem in order to deactivate the largest number of interconnected facilities of the gas transmission network. The list below contains the main symbols for describing the maximum clique problem. $G = (V, E)$ is an arbitrary undirected and weighted graph; $V = \{1, 2, ..., n\}$ is a set of the nodes of the graph G; $E \subseteq V \times V$ is a set of the edges of the graph G; $w = (w_1, w_2, ..., w_n)$ is weight vector, $w_i > 0$, $i = 1, ..., n$; $\bar{G} = (V, \bar{E})$ is the complement graph of G, where $\bar{E} = \{(i, j) : i, j \in V, i \neq j, (i, j) \notin E\}$.

The following problem has to be solved to find a maximum clique:

$$\max_{y \in Y} F(y),$$

$$F(y) = \sum_{i=1}^{n} w_i y_i, \tag{5}$$

$$Y = \left\{ y \in \{0,1\}^n, \; y_i + y_j \le 1 \quad \forall (i,j) \in \bar{E} \right\}.$$

The solution of the problem (5) when $w_i = 1$, $i \in I$ determines the set of facilities in the gas transmission network forming a maximum clique. If multiple solutions are possible, the result will be a set of such cliques, which may substantiate further detailed planning of an attack, the attacker's objective being to cause maximum damage to the target. In specifying weight values w_i, $i = 1,...,n$ in the problem (5), the solutions found can have interesting interpretations. One solution of the weighted maximum clique problem will be presented in Part 5. The solution of the problem (5) allows the attacker to identify the cliques linked to gas production, consumption and storage nodes.

5 Clique Identification in the Russian Gas Transmission Network

Considering (4) and (5), the attacker-defender problem for the Russian gas transmission network can be presented as follows:

$$\min_{y} \max_{x} \; f,$$

$$y \in Arg \max\{C(y) : y \in Y\},$$

$$r_{ij} = r_{ji} = \begin{cases} 1, \; (i,j) : y_i + y_j \ldots 1, \; u_{ij} = u_{ji} = 1, \\ 0, \; (i,j) : y_i + y_j < 1, \; u_{ij} = u_{ji} = 1, \end{cases} \quad i, j \in I \setminus \{i_O, i_S\}, \tag{6}$$

$$r_{i_O, j} = r_{j, i_S} = 0, \qquad j \in I,$$

$$\sum_{j \in I} \bar{u}_{ij} x_{ij} = \begin{cases} -f, \; i = i_O, \\ 0, \; i \notin \{i_O, i_S\}, \\ f, \; i = i_S, \end{cases} \quad i \in I,$$

$$x_{ij} = x_{ji}, \quad i, j \notin \{i_O, i_S\},$$

$$0 \le x_{ij} \le d_{ij}(1 - r_{ij}), \quad i \in I, \; j \in I,$$

where y is $\{0,1\}$-vector specifying the nodes to be attacked (the attacker's plan); $Arg \max\{C(y) : y \in Y\}$ is a set of maximum cliques; r_{ij}, $i, j \in I$ are parameters that define the edges coming in or out of the nodes under attack and removed along with them from the network (the attack's consequences). According to the problem statement and based on the problem's solution (5), the attacker selects a clique which, if removed from the network, causes maximum damage to the transmission capacity of the gas network. Nodes belonging to the clique are removed from the network along with all the adjacent edges. As a result, an attack on a node, first, renders inactive the facilities, located in this node, of the gas transmission network and, second, makes gas transit impossible through this node.

Let us now present maximum clique search and damage caused to the network for different types of clique problems, the weighted and the unweighted ones. The model of the Russian gas transmission network was described by means of the AIMMS modeling environment [32], also used to solve maximum flow and maximum clique problems. The calculations were made on a personal computer equipped with an 8-core AMD FX-8350 processor (each with a clock speed of 4 GHz) and 8GB of RAM.

5.1. Gas Network Analysis. Finding Maximum Cliques

The graph of Russia's gas transmission network was analyzed as follows. The problem (5) for this network was solved separately, resulting in the identification of forty-five cliques (size 3) of potential interest to offenders planning and launching an attack on the gas network. The established cliques constitute the set $F(y)$. Given that these cliques are small-sized, the authors decided not to place budget limitations on the attacker. The value of the maximum gas flow throughout the network, subject to the presence of all nodes in the model, was calculated and amounted to 2235 milion m^3/day. This total is set at 100%. The maximum flow problem (6) was solved individually for each clique identified $y_i \in Arg \max\{C(y) : y \in Y\}$, $i = 1,...,45$. The problem (6) solved, the maximum flow value was recorded for each of the cliques y_i, $i = 1,...,45$.

Table 1 shows data on the maximum flow with account of the excluded clique. Given that the number of cliques found is substantial, the cliques are grouped in terms of the damage caused to the gas transmission network. The Excluded cliques column specifies (in brackets) the number of excluded cliques, the damage resulting from which is, individually, within the range indicated in the Maximum flow column. The % column shows the damage expressed as a percentage of the maximum flow in contrast to the option with no attack.

Table 1: Maximum cliques

No	Excluded cliques	Maximum flow, milion m^3/day	%
1	3-node clique (6)	1361–1996	39–11
2	3-node clique (4)	2063–2064	8
3	3-node clique (2)	2072	7
4	3-node clique (6)	2110–2151	6–4
5	3-node clique (14)	2161–2221	3–1
6	3-node clique (13)	2235	0

As can be seen, the steps taken by the attacker in relation to a number of node combinations do not create any difficulties in providing consumers with the necessary amount of gas: as few as thirteen cliques of this kind have been detected. However, six 3-node cliques (gas network facilities physically interconnected by gas pipelines) were identified, the disruption of which will lead to a system-wide shortage of gas ranging from 11% to 39% of overall consumption. The importance of these combinations confirms that a 39-percent shortage of gas within the network is higher than the shortage resulting from the

disruption of the most important critical facilities and their combinations [18].

5.2. Gas Network Analysis. Finding Weighted Maximum Cliques

Depending on modelling objectives, a specific weight can be assigned to each node in the graph. When searching for potentially vulnerable cliques, it seems logical to set the volume of gas produced as weight for the network's nodes. In this case, the reason for excluding maximum cliques is to sabotage the facilities producing the network's highest volume of gas. Table 2 summarizes the results of the calculations. The Clique weight column shows the total volume of gas produced by all the nodes included in the clique.

Table 2: Weighted maximum cliques

No	Excluded clique	Clique weight	Maximum flow, milion m^3/day	%
1	1-node clique	384.36	1932.47	13.53
2	2-node clique	288.13	2028.7	9.23
3	2-node clique	51.68	2232.3	5.87
4	2-node clique	198.54	2118.29	5.22
5	1-node clique	167.63	2149.2	3.83
6	1-node clique	135	2181.83	2.37
7	1-node clique	107	2209.83	1.12
8	1-node clique	90.76	2227.07	0.35
9	2-node clique	52.29	2232.3	0.11
10	1-node clique	80	2235	0
11	1-node clique	69.92	2235	0
12	1-node clique	61.6	2235	0

The clique identification approach in terms of the maximum volume of gas produced helped detect the production facilities within the gas transmission network interconnected by gas pipelines. Interestingly, the most efficient gas processing plant with no connection to other gas producing facilities ranked first in significance. Ensuring its protection will avoid a possible 13.5-percent decrease in the maximum flow. In the problem examined above, there are four maximum cliques, of size 2. The remaining of the twelve identified cliques are of size 1, which points, in a sense, to gas producing plants' isolation from one another. In this case, due to the small size of the cliques, the authors decided not to place budget limitations on the attacker. The presented analysis of the gas transmission network will enable the defender to implement, on a priority basis, a range of defensive measures with respect to the identified cliques. These measures will concern only the nodes in which gas processing plants are located.

Conclusion

Detecting critical combinations of facilities in the gas transmission network makes it possible to plan defensive measures and to reduce, in case of an attack, potential damage to the network's facilities such as gas processing plants, underground gas storages and compressor stations. This study presents an approach to identifying critical combinations of facilities in the gas transmission network by solving the maximum clique problem. Importantly, this approach does not guarantee the identification of the maximum damage that can be caused to the gas transmission network if the established node combinations are excluded. Nonetheless, finding a solution to the maximum clique problem helps assess the significance of this or that combination of the network's facilities with a view to preventing eventual attacks on critical facilities. In doing so, it is possible to proceed to analyse larger node subsystems without using iterative procedures for step-by-step exclusion of network elements and their combinations, which complements the previous work done on this topic. Furthermore, solving these problems allows for modifications to be introduced to plans for the long-term development of the gas transmission network in order to minimize the significance of the identified facilities and their combinations. Besides, the solution of the maximum weight clique problem suggests some major implications. The authors have identified node cliques with the highest volume of gas production. The identified node combinations are of considerable importance in terms of the gas transmission network's safe operation, and intensified safety monitoring of these facilities is a priority for the defense.

This work has been supported by the grant of the Russian Science Foundation, RSF 20-79-00242.

References

1. Pyatkova, N. I., Rabchuk, V. I., Senderov, S. M., Slavin, G. B., Cheltsov, M. B.: Energy security of Russia: problems and solutions. SB RAS, Novosibirsk (2011)
2. Thompson, J. R., Frezza, D., Necioglu, B., Cohen, M. L., Hoffman, K., Rosfjord, K.: Interdependent Critical Infrastructure Model (ICIM): An agent-based model of power and water infrastructure. International Journal of Critical Infrastructure Protection 24, 144–165 (2019)
3. Kai, L., Ming, W., Weihua, Z., Jinshan, W., Xiaoyong, Y.: Vulnerability analysis of an urban gas pipeline network considering pipeline-road dependency. International Journal of Critical Infrastructure Protection 23, 79–89 (2018)
4. Tichy, L.: Energy Infrastructure as a Target of Terrorist Attacks from the Islamic State in Iraq and

Syria. International Journal of Critical Infrastructure Protection (2019)
5. Tsavdaroglou, M., Al-Jibouri, S. H. S., Bles, T., Halman, J. I. M.: Proposed methodology for risk analysis of interdependent critical infrastructures to extreme weather events. International Journal of Critical Infrastructure Protection 21, 57–71 (2018)
6. Praks, P., Kopustinskas, V.: Node Importance Analysis of a Gas Transmission Network with Evaluation of a New Infrastructure by ProGasNet. In: CRITIS 2018, LNCS vol. 11260, pp. 3–16, (2019). 10.1007/978-3-030-05849-4_1
7. Zio, E.: Challenges in the vulnerability and risk analysis of critical infrastructures. Reliability Engineering & System Safety 152, 137–150 (2016)
8. Zio, E.: Reliability engineering: Old problems and new challenges. Reliability Engineering & System Safety 94(2), 125–141 (2009)
9. Apostolakis, G. E.: How useful is quantitative risk assessment?. Risk analysis 24(3), 515–520 (2004)
10. Liu, H., Davidson, R. A., Apanasovich, T. V.: Spatial generalized linear mixed models of electric power outages due to hurricanes and ice storms. Reliability Engineering & System Safety 93(6), 897–912 (2008)
11. Cuadra, L., Salcedo-Sanz, S., Del Ser, J., Jimenez-Fernandez, S. Geem, Z. W.: A critical review of robustness in power grids using complex networks concepts. Energies 8(9), 9211–9265 (2015)
12. Ouyang, M.: Review on modeling and simulation of interdependent critical infrastructure systems. Reliability engineering & System safety 121, 43–60 (2014)
13. Wang, S., Hong, L., Chen, X.: Vulnerability analysis of interdependent infrastructure systems: A methodological framework. Physica A: Statistical Mechanics and its applications 391(11), 3323–3335 (2012)
14. Johansson, J., Hassel, H.: Modelling, simulation and vulnerability analysis of interdependent technical infrastructures. In: Hokstad, P., Utne, I.B., Vatn, J. (eds.) Risk and Interdependencies in Critical Infrastructures: A Guideline for Analysis, pp. 49–66. London: Springer-Verlag (2012)
15. Senderov, S., Edelev, A.: Formation of a List of Critical Facilities in the Gas Transportation System of Russia in Terms of Energy Security. Energy (2017). 10.1016/J.ENERGY.2017.11.063
16. Vorobev, S., Edelev, A.: Analysis of the importance of critical objects of the gas industry with the method of determining critical elements in networks of technical infrastructures. Management of Large-Scale System Development (MLSD), 2017 Tenth International Conference. IEEE (2017). 10.1109/MLSD.2017.8109707
17. Vorobev, S., Edelev, A., Smirnova, E.: Search of critically important objects of the gas industry with the method of determining critical elements in networks of technical infrastructures. Methodological Problems in Reliability Study of Large Energy Systems (RSES 2017). E3S Web Conf., vol. 25 (2017). 10.1051/e3sconf/20172501004
18. Senderov, S., Vorobev, S.: Approaches to the identification of critical facilities and critical combinations of facilities in the gas industry in terms of its operability. Reliability Engineering & System Safety 203(107046) (2020). 10.1016/j.ress.2020.107046
19. von Stackelberg, H.: The Theory of the Market Economy. William Hodge and Co., London, U.K. (1952)
20. Smith, J.C., Lim, C. Algorithms for Network Interdiction and Fortification Games. In: Chinchuluun, A., Pardalos, P.M., Migdalas, A., Pitsoulis, L. (eds) Pareto Optimality, Game Theory And Equilibria. Springer Optimization and Its Applications, vol 17. Springer, New York, NY. (2008) 10.1007/978-0-387-77247-9_24
21. Brown, G., Carlyle, M., Salmeron, J., Wood, R.: Defending Critical Infrastructure. Interfaces 36(6), 530–544 (2006). 10.1287/inte.1060.0252
22. Salmeron, J., Wood K., Baldick, R.: Analysis of Electric Grid Security Under Terrorist Threat. Power Systems, IEEE Transactions, 19(2), 905–912 (2004). 912.10.1109/TPWRS.2004.825888
23. Manshadi, S., Khodayar, M.: Resilient Operation of Multiple Energy Carrier Microgrids. IEEE Transactions on Smart Grid 6(5), 2283–2292 (2015). 10.1109/TSG.2015.2397318
24. Wang, C., Wei, W., Wang, J., Feng, L., Qiu, F., Correa-Posada, C., Mei, S.: Robust Defense Strategy for Gas-Electric Systems Against Malicious Attacks. IEEE Transactions on Power Systems 32(4), 2953–2965 (2017). 10.1109/TPWRS.2016.2628877
25. Wu, X., Conejo, A. J.: An Efficient Tri-Level Optimization Model for Electric Grid Defense Planning. IEEE Transactions on Power Systems 32(4), 2984–2994 (2017). 10.1109/TPWRS.2016.2628887
26. Apurba, K., Nandi, N., Hugh,. R.M., Satish V.: Interdicting attack graphs to protect organizations from cyberattacks: A bi-level defender–attacker model. Computers and Operations Research 75, 118–131 (2016). 10.1016/j.cor.2016.05.005
27. Kam-Fung, C., Michael G.H. Bell.: (2019) Attacker–defender model against quantal response adversaries for cyber security in logistics management: An introductory study. European Journal of Operational Research 22(30) (2019). 10.1016/j.ejor.2019.10.019
28. Israeli, E., Wood, K.: Shortest-path network interdiction. Networks 40, 97–-111 (2002)
29. Ford, L.R., Fulkerson, D.R.: Flows in networks. Princeton university press, Princeton, New Jersey (1962)
30. Korotaev, Yu., Margulov, R.: Extraction, preparation and transportation of natural gas and condensate, vol. 2. Nedra, Moscow (1984)
31. Bomze, I.M., Budinich, M., Pardaloz, P.M., Pelillo, M.: The Maximum Clique Problem. Handbook of Combinatorial Optimization, pp. 1–74 (1999). 10.1007/978-1-4757-3023-4
32. AIMMS Homepage, https://www.aimms.com. Last accessed 8 Feb 2021