The Equitable Controller Placement Problem

Dritan Nace, Ambra Zajsi, Alban Zyle, Benjamin Lussier, Ahmed Lounis, Erison Ballasheni

The equitable controller placement problem

Dritan Nace, Ambra Zajsi, Alban Zyle, Benjamin Lussier, Ahmed Lounis
University of Technology of Compiègne,
Heudiasyc, UMR CNRS 7253
Compiègne, France

Erison Ballasheni
University Polytechnic of Tirana
Tirana, Albania
eballasheni@fti.edu.al

***Abstract*—Node-to-node connections refer to the links or channels that connect individual nodes (or devices) in a network. These connections allow nodes to communicate and exchange information with each other, forming a network of interconnected devices. To perform this function, nodes must have access to controllers – the devices (installed in selected node locations) necessary in the process of setting-up the connections. The problem of placing controllers in the network is well defined and solved for nominal state networks, but it becomes difficult when the network is subject to attacks, which can occur anywhere, anytime. We tackle this problem as a specific facility location one and look for controllers location solution that lexicographically maximises the covering in case of attacks. We call it the equitable controllers placement problem and will be the focus of this work.**

***Index Terms*—Controllers placement, SDN, resilience, maximal coverage, attacks.**

I. Introduction

Node-to-node connections refer to the links or channels that connect individual nodes (or devices) in a network. These connections allow nodes to communicate and exchange information with each other, forming a network of interconnected devices. To perform this function, nodes must have access to controllers – the devices (installed in selected node locations) necessary in the process of setting-up the connections. These network controllers also play a crucial role in mitigating the impact and protecting the network infrastructure in case of node attacks. Their proactive measures and quick response are essential in minimizing the impact of attacks and safeguarding the network infrastructure.

We focus on the problem of installing controllers at some nodes to monitor and protect the whole network. Each node of the network can be protected by multiple controllers at the same time but only one is active. Our focus is to protect the network from the attacks that can intrude nodes. Node attacks can take various forms, one of the most frequent being the Denial-of-Service (DoS) Attacks which prevent accessing the node or the services it provides. The impact of a node attack can vary depending on the criticality of the affected node, for instance if a controller is located at this node, that means all service provided by the controller is also disrupted. These attacks can disconnect the network and some parts of the network may be not monitored any more as there are not connected to any controller. Hence, these nodes will loose communication with the rest of the network including those directly connected to them. Our focus stands in choosing where to install controllers such that minimizing the loss of communication in case of attacks. This problem falls in the category of Maximal Coverage Location Problem. The Maximal Coverage Location Problem (MCLP) was firstly introduced in [1] and is NP-hard [2]. There have been multiple studies about facility location problems in [3], [4], [5], [6], [7]. In our study the objective is to provide (i) equitable protection to all nodes when the number of controllers that can be placed is limited (ii) robust protection under possibly full (or partial) attack of controllers. The Equitable Controller Location Problem [4], [6], [8] is an extension of the Equitable Facility Location Problem, see Ogryczak [9]. The problem considers placing facilities, (in our case controllers) so as to provide resilient service to all the network nodes are served by the closest facility (controller). The particular controller placement deployed in the network should be resilient to network intrusions, such as natural disasters [10], multiple link failures [11] and most importantly node-targeted attacks [12]. To improve the resilience to this kind of disruptions, additional controllers, called backup controllers, are generally required. Still, in our setting we don't do any distinction between them. The study proposes models to solve the probabilistic equitable controller location problem. The starting point of this work are [13] where the theoretical ground of the method is built and [14] where the problematic is precisely posed. The paper is organized as follows. In Section II we provide a short state of art. Section III recalls main facts on Max-Min fairness. Section IV is devoted to present the model. In Section V we provide the mathematical formulation for the equitable controller placement problem. In Section VI we provide some numerical results.

II. Related works

The paper addresses the problem of placing primary and backup controllers in a network to ensure its robustness against node-targeted attacks. This work is concerned with two issues, first, the attacks in the network, and second, the facility location related problems. Concerning the first aspect, several studies have appeared these last years. A part of them relies on ILP models [15]–[18]. Hence, in [18] Li et al. proposed a mixed-integer linear programming (MILP) model that jointly considers controller placement and routing in software-defined networks (SDNs) to improve their resilience against node failures. More recently, in [19] the same authors extend the

model to optimize the placement of primary and backup controllers and the routing paths between them. In [20] Rani et al., investigate the optimal placement of intrusion detection systems in wireless sensor and propose a binary particle swarm optimization (BPSO) algorithm to optimize the placement of intrusion detection systems while considering the network topology and communication range of sensors. Other works using Deep Learning are presented in [21] by Xu et al.

Finally, from optimisation theory point of view, we may cite [4]–[6], [22], [23] and more recently [13] where the problem has been studied for the general equitable and resilient case.

III. Preliminaries

This section is devoted to preliminaries on equity and proportional fairness together with a result that will be very useful in writing down the mathematical formulation of the controller placement problem.

Let us start by recalling formally the notion of equity and its relation to lexicographic optimization as noted in [24], [25]. We recall some definitions on lexicographic ordering, useful for a better understanding of the study. A vector γ is lexicographically greater (resp. lower) than γ' if there exists $s \in \{1, ..., n\}$ such that $\gamma_p = {\gamma'}_p$, for all $p \in \{1, ..., s-1\}$ and $\gamma_s > {\gamma'}_s$ (resp. $\gamma_s < {\gamma'}_s$). A vector γ is lexicographically maximal (resp. minimal) in X if for every vector $\gamma' \in X$, γ is lexicographically greater (resp. lower) than or equal to γ'.

Let $\overrightarrow{\gamma}$ (resp. $\overleftarrow{\gamma}$) be the vector γ with its indices reordered so that the components are in non-decreasing (resp. non-increasing) order. A feasible vector is defined as leximin maximal as follows: A vector $\gamma \in X$ is leximin maximal if for every vector $\gamma' \in X$, $\overrightarrow{\gamma}$ is lexicographically greater than or equal to $\overrightarrow{\gamma'}$. Similarly, one can define leximax minimality as follows: a vector $\gamma \in X$ is leximax minimal if for every vector $\gamma' \in X$, $\overleftarrow{\gamma}$ is lexicographically lower than or equal to $\overleftarrow{\gamma'}$.

Let us look now at the solution methodology. We define $\Gamma \subset \mathbb{R}^m$ as the set of vectors γ for which the following set is non-empty:

$$\{f_i(x) \geq \gamma_i; \quad i \in 1, ..., m, x \geq 0, x \in \mathbb{R}^n\}. \tag{1}$$

We say that γ is feasible if $\gamma \in \Gamma$. Then, computing a leximin maximal vector for the system of inequalities (1) when $f_i(x)$ are linear is relatively easy as shown by the method in [26] or in [6], [24], [25] and in references therein. Then, one can compute a leximin maximal vector among the feasible vectors by solving a sequence of at most m linear programs. At iteration i one computes the highest value that can take the i^{th} smaller component of the solution vector.

Similar results can be drawn for the leximax minimal case.

Let us consider some strictly increasing function ϕ and the system composed of functions $\phi \circ f_i$. Recall that the operator $\circ$ stands for the function composition operator. It can be easily shown that the following result holds [26].

Proposition 1. *Let ϕ be a strictly increasing function in $\mathbb{R}$. A vector γ feasible for* (1) *is leximin maximal if and only if the vector $(\phi(\gamma_1), \ldots, \phi(\gamma_m))$ is leximin maximal for the corresponding system composed of functions $\{\phi \circ f_i, i \in M\}$.*

IV. Problem modeling

The problem studied in this paper concerns the controller location in a network subject to node attacks. This problem has been recently investigated in depth in [14] and a method using linear programming is presented. We will tackle the problem from a different angle: we intend to propose a probabilistic oriented method which ensures equitable protection from attack nodes. We assume that we are given a list of attacks collected in a representative historic of such events. This historic is of primary importance as it allows to define the main parameters used in the model, namely probability covering.

IV-A Model description

To model our problem, we can use a graph $G(N, M, A)$ with a set of nodes $N = 1, ..., n$ representing candidate controller locations, a set of nodes $M = 1, ..., m$ representing locations that should be covered, and a set A of directed links. In our problem M and N coincide. A link from node $i \in N$ to node $j \in M$ indicates that a controller at node i monitors node j. If there is no link from node i to node j, then a controller at i does not monitor j. In particular, we consider a link only when the distance between i and j is less than a known threshold. We assume K (primary or backup) controllers available to be placed in the candidate locations to protect the selective locations. We take into consideration a probabilistic version of the problem, where the effective covering of node j by node i is represented by a random variable a_{ij}. More specifically, this variable a_{ij} is a Bernoulli random variable that takes value 1 with a given probability p_{ij}. Therefore, the probability that a controller at node i monitors node j is represented by p_{ij}. This value is potentially computed by considering the different attacks that has already happened in the past. Another assumption made is that the random variables $a_{ij}, i \in N, j \in M$ are independent and the models developed in this study require this condition. By assuming this, the calculations are much facilitated as it may be seen later on. It can be noticed that $p_{ij} = p_{ji}$, while the case when some node i cannot monitor node j is depicted by absence of link from i to j in the graph representation. On top of above we add a few additional assumptions:

- A list S of attacks s is given. It represents a realistic data collected or simulated.
- A future attack is not known but we assume known the maximal number of nodes simultaneously affected by an attack.

IV-B An example

In the following we show how the p_{ij} values are computed. We are given a small size networks composed of 8 nodes (Fig. 1-6). There are considered three specific attacks (a, b, and c). Each attack affects three nodes shown as dotted in

the figures. Each attack disrupt the attacked nodes and may disconnect the network as shown for each case. We examine for each node separately its connected nodes in the after-attack resulting network. Hence, we may notice that node A remains connected to B only once while with C and D there are respectively 3 and 1 times. All this allows to compute the probability covering for node A to nodes B, C, D as shown in Fig. 7.

Following above, we compute p_{ij} as

$$p_{ij} = \frac{\sum_{s \in S} a_{ij}^s}{|S|} \quad i \in N, j \in M$$

where S gives the list of attacks s, each of them being composed of a set of nodes under attack. We assume that some node may monitor any node that can be reached. Then, a_{ij}^s is counted as 1 any time i remains connected to j in case of attack s and 0 otherwise.

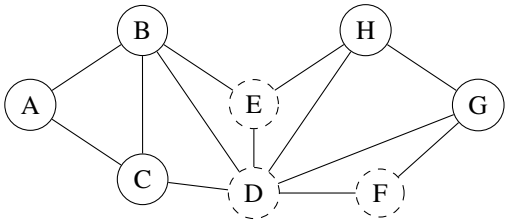

Figure 1: Case a)

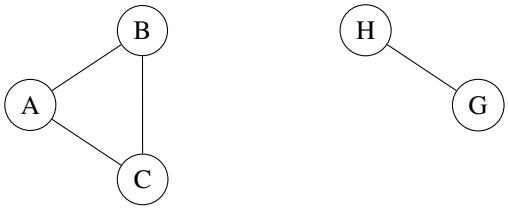

Figure 2: Case a) after attack

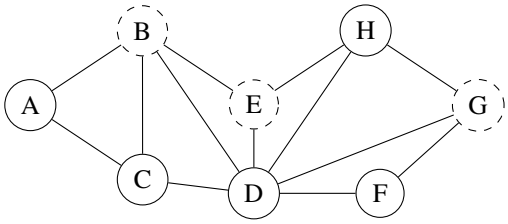

Figure 3: Case b)

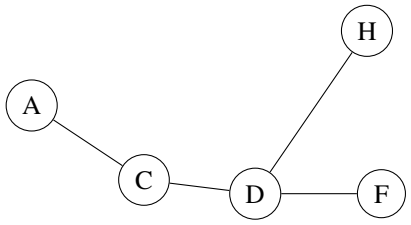

Figure 4: Case b) after attack

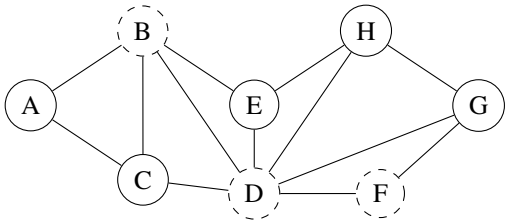

Figure 5: Case c)

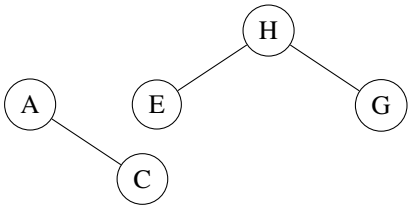

Figure 6: Case c) after attack

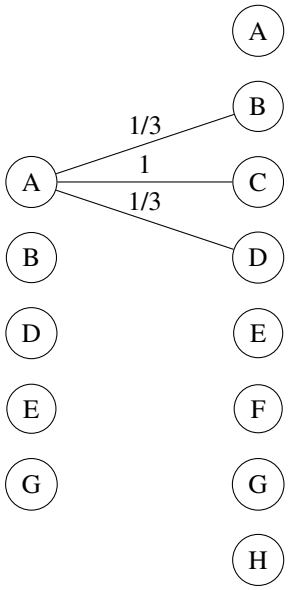

Figure 7: Node A coverage for nodes B, C and D

V. Equitable controller placement

Let binary optimization variable x_i represent whether or not a controller is placed in the node i and $q_j(x)$ denote the probability that node j is not monitored. Following [13], we

obtain the following formulation:

$$\begin{aligned} q_j(x) &= P\left(\sum_{i\in N} a_{ij}x_i < 1\right) \\ &= P\left(a_{ij}x_i < 1, \forall i \in N\right) \\ &= \prod_{i\in N} P\left(a_{ij}x_i < 1\right) \\ &= \prod_{i\in N}(1-p_{ij}x_i) \\ &= \prod_{i\in N}(1-p_{ij})^{x_i} \end{aligned}$$

The above implications are justified by the fact that a_{ij} are binary and independent while variables x_i are binary.
At this stage we aim to maximize the minimum protection, i.e. $q_j(x)$, for the given set of attacks S. This list S is used to compute probability p_{ij} values.

$$\left\{q_j(x) \le \gamma_j,\ j \in M,\ \sum_{i\in N} x_i = K, x \in \{0,1\}^n\right\}, \qquad (2)$$

where one looks for a feasible leximax minimal vector.

As said before, we consider two distinct objective functions, which are the *lexicographic* and the *proportional* one. Let us first focus on the lexicographic case. With respect to the $q_j(x)$ criterion, system (2) can be written as:

$$\left\{q_j(x) \le \gamma_j,\ j \in M,\ \sum_{i\in N} x_i = K, x \in \{0,1\}^n\right\}, \qquad (3)$$

where one looks for a feasible leximax minimal vector γ. The above problem seems hard at first sight since the criteria $q_j(x)$ is clearly non-linear. This is where Proposition I comes into play. We can use the logarithmic function as function ϕ, which combined with the fact that x is a binary solution vector, allows to linearize the functions involved:

$$\log(q_j(x)) = \log\left(\prod_{i\in N}(1-p_{ij})^{x_i}\right) = \sum_{i\in N}(\log(1-p_{ij}))x_i,$$

and system (3) becomes

$$\left\{\sum_{i\in N}(\log(1-p_{ij}))x_i \le \gamma_j,\ j \in M,\ \sum_{i\in N} x_i = K, x \in \{0,1\}^n\right\}$$

Therefore, computing the leximax minimal vector can be done using the approaches shown in [6], [27].

On the other hand, the problem of minimizing the proportional fairness is defined as

$$\sum_{j\in M}\log(q_j(x)). \qquad (4)$$

In view of (4) above, solving the proportional fair controller placement problem amounts to solve

$$\begin{aligned} \min\ & \sum_{j\in M}\sum_{i\in N}(\log(1-p_{ij}))x_i \\ \text{s.t. } & \sum_{i\in N} x_i = K \\ & x_i \in \{0,1\}, \forall i \in N. \end{aligned}$$

Clearly, the above problem is easily tractable as it can be solved in $O(|N||M| + |N|\log|N|)$ by ordering the n coefficients $\{\sum_{j\in M}\log(1-p_{ij}), i \in N\}$ in increasing order and choosing the K first elements.

VI. Numerical results

VI-A Network instances

Two large-scale networks representing North America (Conus) and Europe (Cost) were investigated in this study. The first network has 75 nodes which each node represents a city in North America with their relevant lnks. The second one has 37 nodes representing the Europe's main cities.

VI-B Comparison of lexicographic and proportional fair methods

The attack scenarios examined in this study are built from two distinct sets: the first comes from the predefined attack sets used in [14], and the second is a set of random generated attacks. the predefined attack sets are composed of 12 attacks each with respect to the number of attacks targeted (4, 6, 8 or 10) nodes. Additionally, 12-20 random attacks were introduced, with attack lengths randomly ranging from 3 to 7 nodes. For each scenario, the placement of 2, 3, 4, 5, and 6 controllers was examined, aiming to achieve maximum network coverage. Two distinct methods were employed: the Proportional Fairness method and the Lexicographic Leximax Minimal method. The average coverage across all attacks was computed for each scenario.

We may notice that significant coverage was achieved even with only 2 controllers. The results continued to improve as the number of controllers increased up to 4, after which further increases did not yield substantial improvements. Generally, the Lexicographic method outperformed the Proportional Fairness method in terms of achieving higher coverage, although this is not systematic and the difference between the two methods was not significant.

In table II, we report the numerical results obtained for the second network. As it can be easily noticed, similar conclusion to above may be drawn.

VI-C Comparison with methods of literature

A comparison was made between the proposed methods and the results obtained by the authors of [14]. They have computed the placement of potential controllers for sets of

No. of controllers	Lexico. Avg.	Prop. Fair. Avg.
2	69.435	64.188
3	69.754	67.087
4	69.681	69.739

(a) 4 nodes attacked

No. of controllers	Lexico. Avg.	Prop. Fair. Avg.
2	57.000	57.370
3	69.029	65.471
4	68.696	66.870
5	69.043	67.102
6	68.696	68.623

(b) 6 nodes attacked

No. of controllers	Lexico. Avg.	Prop. Fair. Avg.
2	58.324	58.018
3	62.478	60.649
4	64.946	62.469
5	67.748	65.018
6	68.234	65.198

(c) 8 nodes attacked

No. of controllers	Lexico. Avg.	Prop. Fair. Avg.
2	53.686	55.343
3	55.049	56.726
4	58.451	55.902
5	63.088	57.745
6	65.157	59.686
7	65.690	60.868

(d) 10 nodes attacked

Table I: Results for Network (Conus). We report the relevant averages for both methods with different numbers of controllers.

No. of controllers	Lexico. Avg.	Prop. Fair. Avg.
2	30.028	26.264
3	31.181	25.972
4	31.479	26.278
5	31.917	26.139

(a) 4 nodes attacked

No. of controllers	Lexico. Avg.	Prop. Fair. Avg.
2	27.343	25.196
3	29.951	27.931
4	29.863	27.784
5	31.147	29.265

(b) 6 nodes attacked

No. of controllers	Lexico. Avg.	Prop. Fair. Avg.
2	24.569	24.441
3	26.383	26.697
4	28.402	27.892
5	28.235	27.794
6	28.304	27.490

(c) 8 nodes attacked

No. of controllers	Lexico. Avg.	Prop. Fair. Avg.
2	22.304	22.814
3	23.177	23.755
4	25.275	25.628
5	25.902	24.353
6	26.618	25.324
7	26.912	26.686

(d) 10 nodes attacked

Table II: Results for the Network (Cost). We report the averages number of covered nodes for both methods with different numbers of controllers.

predefined attacks involving 4, 6, 8 and 10 nodes for the network (Conus). In our computation, as previously, we have considered a set of 24 attacks (12 predefined and 12 randomly generated) to compute the p_j values, which are the main parameters used in our methods. Next, we have tested the performance of the solutions obtained with the three methods on the predefined sets of attacks used in [14]. The obtained results with our proposed methods, in terms of coverage, are highly competitive to these obtained in the literature with a negligible difference of 2% observed in the worst-case scenario. On the other hand, one may notice the simplicity of calculations for our method, especially for the proportional fair one.

Nodes attacked	Equitable locations		Method from [14]
	Lexi.	Pr.Fair.	
4	69.75	69.75	69.75
6	47.5	47.5	47.5
8	37.916	37.916	37.916
10	29.25	29.25	30

Table III: 2 Controllers

Nodes attacked	Equitable locations		Method from [14]
	Lexi.	Pr.Fair.	
4	69.75	69.75	70.5
6	68	68	68
8	52.5	52.5	52.5
10	40.667	40.667	40.7

Table IV: 3 Controllers

VII. Conclusion

In this study we have focused on the equitable controller location problem and show how lexicographical optimisation theory may effectively handle the problem of controller placement to face attacks. In the near future we intend to consider more realistic cases assuming that some controllers may be directly impacted by the attacks which leads to the robust resilient controller location problem.

Nodes attacked	Equitable locations		Method from [14]
	Lexi.	Pr.Fair.	
4	70.5	69.75	71
6	68	68	69
8	65.25	65.25	66.7
10	50.917	50.917	51.3

Table V: 4 Controllers

Nodes attacked	Equitable locations		Method from [14]
	Lexi.	Pr.Fair.	
4			
6	69	68	69
8	65.25	65.25	66.7
10	54.333	53.417	54.7

Table VI: 5 Controllers

REFERENCES

[1] R. Church and C. ReVelle, "The maximal covering location problem," *Papers of the Regional Science Association*, vol. 32, no. 1, pp. 101–118, 1974. [Online]. Available: http://dx.doi.org/10.1007/BF01942293

[2] M. R. Garey and D. S. Johnson, *Computers and Intractability: A Guide to the Theory of NP-Completeness*. New York, NY, USA: W. H. Freeman & Co., 1979.

[3] A. Arabani and R. Farahani, "Facility location dynamics: An overview of classifications and applications," *Computers & Industrial Engineering*, vol. 62, no. 1, pp. 408–420, 2012.

[4] T. Ibaraki and N. Katoh, *Resource Allocation Problems: Algorithmic Approaches*. Cambridge, MA, USA: MIT Press, 1988.

[5] G. Laporte, S. Nickel, and F. Saldanha da Gama, *Location Science*. Springer International Publishing, 2015.

[6] H. D. Luss, *Equitable Resource Allocation: Models, Algorithms and Applications*. Hoboken, NJ, USA: John Wiley & Sons, 2012.

[7] A. T. Murray, "Maximal coverage location problem: Impacts, significance, and evolution," *Int. Reg. Sci. Rev.*, vol. 39, no. 1, pp. 5–27, 2016. [Online]. Available: http://dx.doi.org/10.1177/0160017615600222

[8] H. Luss, D. Nace, M. Poss, and M. C. Santos, "Equitable sensor location problems," in *ROADEF 2016*, Compiegne, France, 2016.

[9] W. Ogryczak, "On the lexicographic minimax approach to location problems," *European Journal of Operational Research*, vol. 100, no. 3, pp. 566–585, 1997.

[10] S. S. Savas, M. Tornatore, F. Dikbiyik, A. Yayimli, C. Martel, and B. Mukherjee, "Rascar: Recovery-aware switch-controller assignment and routing in sdn," *IEEE Transactions on Network and Service Management*, vol. 15, no. 4, pp. 1222–1234, 2018.

[11] S. Yang, L. Cui, Z. Chen, and W. Xiao, "An efficient approach to robust SDN controller placement for security," *IEEE Transactions on Network and Service Management*, vol. 17, no. 3, pp. 1669–1682, 2020.

[12] D. Santos, A. de Sousa, C. Mas-Machuca, and J. Rak, "Assessment of connectivity-based resilience to attacks against multiple nodes in sdns," *IEEE Access*, vol. 9, pp. 58 266–58 286, 2021.

[13] M. Santos, H. Luss, D. Nace *et al.*, "Proportional and maxmin fairness for the sensor location problem with chance constraints," *Discrete Applied Mathematics*, 2019.

[14] M. Pioro, M. Mycek, A. Tomaszewski, and A. de Sousa, "On joint primary and backup controllers.placement optimization against node-targeted attacks," in *2022 12th International Workshop on Resilient Networks Design and Modeling (RNDM)*. IEEE, 2022, pp. 1–7.

[15] S. Han, Y. Fang, and C. Wang, "An ilp-based approach for joint primary and backup controllers placement in sdn," *IEEE Access*, vol. 7, pp. 108 246–108 258, 2019.

[16] W. Guo, M. Zhang, J. Wu, and J. Yang, "An ilp model for joint placement of primary and backup controllers in software-defined networks," *IEEE Transactions on Network and Service Management*, vol. 16, no. 1, pp. 84–97, 2019.

[17] S. Wang, H. Liu, Y. Chen, and Y. Chen, "Optimal placement of controllers in software-defined networks using ilp," *IEEE Communications Letters*, vol. 22, no. 8, pp. 1676–1679, 2018.

[18] J. Li, P. Zhang, Y. Wang, B. Liu, and M. Tang, "On the joint optimization of controller placement and routing in software-defined networks," *IEEE Transactions on Network and Service Management*, vol. 15, no. 2, pp. 703–717, 2018.

[19] J. Li, B. Liu, P. Zhang, Y. Wang, and M. Tang, "Towards joint optimization of controller placement and fault tolerance in sdn," *IEEE Transactions on Network and Service Management*, vol. 17, no. 2, pp. 1074–1087, 2020.

[20] K. Rani, I. Chana, A. Singh, and H. Singh, "Optimal placement of intrusion detection systems in wireless sensor networks," *Wireless Personal Communications*, vol. 107, no. 3, pp. 1759–1779, 2019.

[21] J. Xu, P. Li, C. Li, Y. Li, Y. Shang, and H. Huang, "Deep learning-based controller placement for fault-tolerant software-defined networks," *IEEE Transactions on Network and Service Management*, vol. 17, no. 1, pp. 142–155, 2020.

[22] P. Beraldi and A. Ruszczynski, "The probabilistic set covering problem," *Operations Research*, vol. 50, no. 6, pp. 956–967, 2002.

[23] A. Caprara, P. Toth, and M. Fischetti, "Algorithms for the set covering problem," *ANN OPER RES*, vol. 98, no. 1-4, pp. 353–371, 2000.

[24] D. Nace and M. Pioro, "Max-min fairness and its applications to routing and load-balancing in communication networks: a tutorial," *IEEE Commun. Surv. Tutor.*, vol. 10, no. 4, pp. 5–17, 2008.

[25] W. Ogryczak, H. Luss, M. Pioro, D. Nace, and A. Tomaszewski, "Fair optimization and networks: A survey," *Journal of Applied Mathematics*, vol. 2014, pp. 1–25, 2014.

[26] D. Nace and J. B. Orlin, "Lexicographically minimum and maximum load linear programming problems," *Oper. Res.*, vol. 55, no. 1, pp. 182–187, 2007.

[27] W. Ogryczak and T. Sliwinski, "On solving linear programs with the ordered weighted averaging objective," *European Journal of Operational Research*, vol. 148, no. 1, pp. 80–91, 2003.