Bibliographic work

Wireless LAN transmitter location under the threat of jamming attacks

Erik Cembreros, Josu Barrutia and Julen Beristain

Euskal Herriko Unibertsitatea

1 Problem explanation

1.1 Context

The objective of this paper[1] is to determine the optimal design of a wireless access point array while considering the potential for jamming attacks. We aim to create a resilient WLAN by strategically placing the access points to withstand jamming. In the subsequent sections, we will use a tri-level multi-period mixed-integer (TL-MIP) model approach to maximize the overall network performance.

Wireless technology plays a significant role in many companies and organizations, making it a target for malicious actors who may exploit its vulnerabilities, such as jamming. The loss of an access point can disrupt connections for multiple users, which can have a detrimental impact on the business or organization.

2 Problem description

The problem model consists in a set of access points (each with a maximum number of connections), a set of possible locations for these access points, a set of jammers, and a set of possible locations for these jammers. There are also demand points that can establish a connection to an access point if two conditions are met:

- The access point must not be at maximum capacity.
- The connection cannot fall within the radius of a jammer.

The problem needs to be solved under the following condition: the set of jammers must be optimally placed to minimize network connectivity, while the access points should be placed in the best possible locations to mitigate the attack. Neither the jammers nor the access points know the locations of the demand points, as the demand points may relocate over time in an attempt to improve their connectivity. When an access point is jammed, the demand points that were connected to it should try to establish a new connection with an access point that can satisfy the previous conditions. The attackers should aim to bottle-neck the network by placing jammers in a way that forces the access points to reach their maximum capacity.

3 Mathematical Model

A Tri-Level Multi-Period Mixed-Integer Programming [TL-MIP] model is used to represent the problem; i.e., a mathematical model with three parts, each corresponding to different decision maker entities (access points, jammers and demand points, in that order) where the decisions made to optimize the objective of each level depends on the previous level in the hierarchy. It has also a temporal variable, and demand points and jammers are allowed to relocate between time

periods. It also has both real and integer parameters and variables, more concretely, decision variables (booleans).

The TL-MIP is split in the next three stages:

$$Z_1 = Max\, W(y) \tag{1a}$$

subject to:

$$\sum_{j \in J} w_j = m \tag{1b}$$

$$w_j \in \{0,1\}\ \forall j \in J \tag{1c}$$

where

$$W(y) = Min\ Z_2 \tag{2a}$$

subject to:

$$\sum_{k \in K} y_{klt} \leq 1\ \forall l \in L, t \in T \tag{2b}$$

$$\sum_{l \in L} y_{klt} \leq 1\ \forall k \in K, t \in T \tag{2c}$$

$$\sum_{n \in P_k} y_{nl(t+1)} \leq 1 - y_{klt}\ \forall k \in K, l \in L, t \in T \tag{2d}$$

$$y_{ktl} \in \{0,1\}\ \forall k \in K, l \in L, t \in T \tag{2e}$$

where

$$Z_2 = Max \sum_{i \in I} \sum_{j \in J} \sum_{t \in T} S_{ijt} x i j t \tag{3a}$$

subject to:

$$\sum_{j \in A_{it}} x_{ijt} = 1\ \forall i \in I, t \in T[\alpha_{it}] \tag{3b}$$

$$\sum_{i \in I} x_{ijt} \leq c w_j\ \forall j \in J, t \in T[\beta_{jt}] \tag{3c}$$

$$x_{ijt} \leq 1 - \sum_{k \in K} \sum_{l \in L} D_{ijklt}\, y_{klt}\ \forall i \in I, j \in J, t \in T[\gamma_{ijt}] \tag{3d}$$

In the stage (1) (access points' point of view), the objective function ($1a$) maximizes the total signal strength (as we will see in its dependencies ($2a$) and ($3a$)), while the constraint ($1b$) requires all the access points to be placed.

In the stage (2) (jammers' point of view), the objective function ($2a$) minimizes the total signal strength (obtained from Z_2 ($3a$)). The constraints ($2b$) and ($2c$) force at most a single jammer to be in each location. On the other hand, ($2d$) prevents jammers to relocate further than distance R in a single time instance change.

In the stage (3) (demand points' point of view), the objective function ($3a$) maximizes the signal strength. The constraint ($3b$) assures that each demand point can only be connected to a single access point (to a real one or to a fictional dummy one with null signal strength). ($3c$) ensures that the capacity of the access points is not overcome. Finally, ($3d$) forces the interdicted connections to have null signal strength. For the last three constraints their dual variables have been annotated.

The demand points' distribution is calculated using a two-dimensional spatial Poisson process (reassigning the distribution in each time period), where the space is divided in cells and the probability of having some amount of demand points is proportional to the relation of the surface of each cell and the total one.

Although the previously presented model is the basic one, the one that is the best to reflect the problem, the third and the second stages are unified to simplify the computation using the dual of the third stage, fixing the decision variables and relaxing the binary constraint. That

way, the version of the model which is used for the computations is the same expressed before, changing $(2a)$, $(3a)$ and the constraints of the third stage with the objective function $(4a)$ and the constraints $(4b)$:

$$W(y) = Min \sum_{i\in I}\sum_{j\in J}\sum_{t\in T}(\alpha_{it} + c\beta_{ijt} + (1 - \sum_{k\in K}\sum_{l\in L} D_{ijklt}y_{klt})\gamma_{ijt}) \tag{4a}$$

$$\alpha_{it}, \beta_{ijt}, \gamma_{ijt}\ \forall i \in I, j \in J, t \in T \tag{4b}$$

All seen till the moment refers to the non-additive model, where jammers only affect to access and demand points if these last ones are inside the jamming radius (jammers can't work together summing their interference). Because of that, another (more realistic) model, the additive model, is presented too. In this model, the signal strength is $S_{ijt} = P_j G_{ijt}\ :\ G_ijt = (\frac{\omega}{d_{ijt}})^{\eta}$. As we can see, now the signal strength is inversely proportional to the distance. With this expression, the signal to interference plus noise ratio is used with some ω threshold to decide if a connection is established, and the $(3d)$ constraint is modified accordingly. At this point, the problem is reformulated again to transform it to a covering constraint problem and finally the same procedure as with the additive model is used to obtain a two level problem.
[1]

4 Solution Methodologies

Three different methodologies have been used to solve the problem:

1. **Branch-and-Bound**: the classic branch-and-bound for multi-level mixed-integer problems can be directly used to solve the BL-MIP. First, the current optimal solution is initialized with a very low value and the root node is created. Second, the upper bound of the available branches is compared to the current solution to discard those branches that can not improve the solution. Third, a relaxed sub-problem is solved. If the solution contains integers in all the variables with that requirement, it is taken into account; otherwise, new branches are created putting bounds on fractional-valued variables. As said before, if a solution was valid, the next step is to complete the bi-level feasible solution with the lower level, and store it if it is greater than the previous optimal one. Branching and backtracking continues incrementing lower bounds or decrementing upper bounds of each undetermined sub-problem. When there is no more nodes, the current optimal solution is selected.
2. **Implicit enumeration**: seeks to find the optimal solution by means of a search tree. First, set the optimal solution to a very low value and initialize the root node with zero access points ($w_j = 0\ \forall j \in J$). Second, select and remove a node from the set of unprocessed nodes and solve the lower-level problem for the corresponding $w^(m)$ (updating the current optimal solution when it is improved). Then, define the set of suitable locations for new access points. Choose a location from that set and branch with two new nodes, one where the location is set to 1 and the other where it is set to 0. Continue processing until there is no more suitable placement for access points and the set of unprocessed nodes is empty, and choose the final optimal solution.
3. **Dynamic constraint generation for additive model**: a restricted problem in which the set of covers is incomplete is initially considered, and a cutting plane approach is used; i.e., the resolution of the problem begins with a relaxed version of the model and new binary variables u_l are introduced that decide if a given jammer is placed in the cover. Then, the problem is solved for each (i, j, t) demand point, access point and time period triplet, and the optimal one is selected.

[1] All these transformations' strict formulations are skipped because they don't give more insight of the problem.

5 Results analysis

Five AP topologies have been considered to compare their connectivity and how do they affect the placement and movement trends of the jammers. To achieve this the simplified bilevel mixed-integer program [BLMIP] has been used.

The Partite topology had three clusters of APs separated far enough apart that a demand point located between two clusters might not be able to connect to any AP in either cluster. The Perimeter topology distributed APs along the region's perimeter, allowing free movement of demand points and causing them to be separated. The Dense topology featured a central hub with clustered APs, it resembles a critical location which demands constant connectivity. The Spacious topology randomly distributed APs to avoid proximity, resulting in demand points within range of one or two APs. The Median topology had uniformly distributed APs along diagonals and central lines, with clustering in the center, resembling a campus with a central area of high connectivity demand.

For all five topologies, three experiments with 10, 25 and 50 APs, each with a capacity of 15, 5 jammers with jamming radius of 150 feet, and 5 time periods. Each region was 1 square mile. The demand was realized ten times, with 100 demand points, and the results were averaged. This showed that the Spacious and Median topologies were closest to the optimal AP placement.

It was found that AP placement near concentrations of demand points was crucial for ensuring robust network connectivity. However, AP too clustered together give jammers an easier time on severing connections. Therefore, the optimal solution should find a balance between these two factors.

Sensitivity has also been proved, concluding that adding a set of new AP did not improve overall connectivity. Meanwhile, were more jammers to be added to the original problem, the set of new APs would become significantly important.

3a is a generalized utility function considering three aspects: range, unity and tolerance. The comparison of this utility function, both when the jammers were optimally deployed and when they were not, revealed that the Dense and Spacious topologies were the most affected by jammers.

6 Conclusions

The optimal placement of access points is crucial to ensure maximum connectivity for demand points in various environments, including university campuses. This optimal topology will also maximize connectivity in the presence of jammers, considering both non-additive and additive models. Achieving a proper placement requires striking a balance between placing access points near concentrations of demand points and avoiding the formation of clusters. In this regard, the Partite and Median topologies demonstrated greater robustness against jamming attacks when considering utility as total signal strength, number of connections, or tolerance allowance.

While this research considers the placement of both access points and jammers, the placement of demand points has not been taken into account. Considering this would lead to a stochastic problem rather than a deterministic one.

References

1. Schweitzer, D., Medal, H.: Wireless LAN transmitter location under the threat of jamming attacks. Computers and Operations Research **1**06 14-27 (2019)