A game theoretic approach of a virus-antivirus competing game

Yassine Mehmouden

July 2024

Contents

1 Introduction

Nowadays, malware attacks are really common, in 2023, according to *Statista*, there were no fewer than 6.06 billion of these attacks worldwide[1]. Understanding malware attacks and finding the best answer to them is a challenge every company or organization faces today. It is this idea that led us to the present paper. Since attacks can be really different from each other and the way to answer them too, it is interesting to see what is the best option for each camp, even if we will focus the study on the defensive aspect of the confrontation. Hence, we can see this opposition as a game and use game theory to study it.
For this purpose, we model the situation with an attacker and a defender, having each one their set of strategies, playing a game where both of them want to have the best pay-off. Employing simulations, our goal is to analyze this game to eventually detect equilibria or even solutions.
The remainder of this paper is structured as follows. Section 2 presents the modeling of the game and details the different strategies. Results and analyses are given in section 3. Finally, section 4 presents a conclusion.

2 Presentation of the game

As said in the introduction, we model the situation by a game. The first player is the attacker, his goal is to attack a network with a virus. The network is modeled by a graph where the vertices are the devices and the edges are the links between them. The attacker chooses a propagation method for the virus which will be discussed below and aims to maximize his pay-off. We will consider two pay-off functions for the attacker, we will detail them further. The defender's goal is the opposite of the attacker's. He wants to defend the network, and for this purpose, he can put a budget for the defense. The higher the budget, the quicker the response to the attack. We consider for the defender two pay-off functions like for the attacker, they will be discussed below, but, unlike the attacker's, the defender's pay-off functions take into consideration the budget used in the defense process. We chose to study this perspective because it is more relevant in our case, as we especially study the defensive aspect of this attack.

2.1 Games rules

At the beginning of the game, the attacker injects the virus into one node of the network and chooses one propagation strategy. The virus proliferates in the network, and when more than 5% of the network's nodes are infected, we consider that the defender detects the virus. Even if before the number of infected devices reached this threshold, the defender could have doubts about whether the malware was due to a deliberate attack or not, he is now sure that he has to act to defend the network. So, he decides on a budget for the defense and the setting up of a solution. This budget is directly linked to the waiting time before the injection of an antivirus into the network, as we will see below. After this time, the antivirus can be injected into the network and diffused. But at each time step, one node having the antivirus can only diffuse it to one of its neighbors. We call this *a unicast diffusion*. Once a node has the antivirus, he cannot be infected by the virus again, our model is then a kind of SIR compartmental model where there are susceptible, infected, and recovered nodes. So, after the introduction of the antivirus, during each time step, the nodes, in a random order, can propagate the antivirus, propagate the virus, or do nothing. The game ends when there is no longer any infected node in the network.

2.2 Virus strategies

As discussed before, the virus can use different propagation strategies, these strategies affect the number of neighbors an infected node will infect during each time step. We detail the strategies :

[1] https://www.statista.com/statistics/873097/malware-attacks-per-year-worldwide/

1. unicast propagation: an infected node infects one of its neighbors (if possible) during each time step.

2. broadcast propagation: an infected node infects all its susceptible neighbors during each time step.

3. chaotic propagation: an infected node can infect one or all of its susceptible neighbors randomly, i.e. it infects only one susceptible neighbor with a probability of 0.5, otherwise it infects all of them.

4. sneaky propagation: an infected node infects only one susceptible neighbor during each time step until a decrease in the number of infected nodes, after which, it adopts a broadcast propagation, i.e. it infects all its susceptible neighbors at each time step.

All the propagation strategies are variants and combinations of the unicast and the broadcast strategies. These strategies permit drawing attention to different behaviors of the virus, for example, the sneaky virus that will proliferate discreetly until discovered and then will attack intensely the network or the broadcast virus that will proliferate aggressively during the whole attack, etc.

2.3 Defense budget

When the defender detects the attack, he decides on a defense budget, which represents the money/resources the defender is ready to pay to contain the attack. As said earlier, the budget is directly linked to the time for setting up the solutions, i.e. the number of time steps between the detection of the virus and the injection of the antivirus into the network.
This relation is represented by the Δ function:

$$\Delta(K) = \begin{cases} 500 \text{ if } K = 0 \\ round(\frac{200}{K}) \text{ otherwise} \end{cases}$$

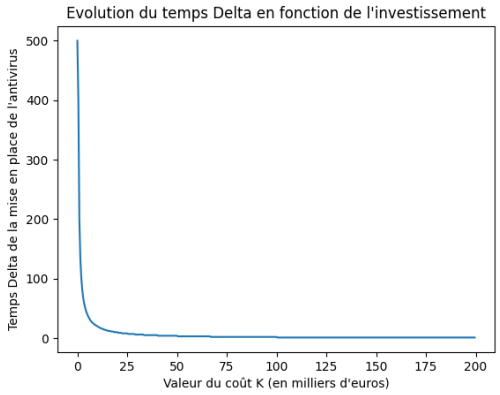


Figure 1: Delta function for the games of this paper

This function returns the number of steps between the detection of the virus and the injection of the antivirus. It takes as parameter K, the investment in thousands of euros here, but another unit can be chosen.
The larger the investment, the fewer the waiting steps
The values presented here have been chosen according to the graph used for the simulations that can be seen in part 3, they must be adapted if the chosen graph is different.

2.4 Pay-off functions

We use two pay-off functions for both the attacker and the defender. These functions will help us analyze a game's outcome and evaluate the efficiency of each strategy.

2.4.1 Attacker's pay-off

First, for the attacker, we consider two pay-off functions :

- The virus prioritizes the accumulated number of infected nodes during the attack, we then can express the pay-off function u_A, if we note s a strategy vector where $s = (c_A, K)$, $c_A \in U, B, C, S^2$ (c_A is the propagation strategy chosen by the attacker, and K is the value of the defender's investment) :

$$u_A(s) = \sum_{t=0}^{T} n_i(t, s)$$

  Where T is the total number of time steps of the attacks and $n_i(t, s)$ the number of infected nodes at the time step t when using the strategy vector s.

- The virus prioritizes the number of steps where the number of infected nodes is near the "epidemic peak", i.e. the maximal number of infected nodes during a time step. Say, the epidemic peak of the infection is $n_{\max}$ and is obtained at step $t_{\max}$, then :

$$u'_A(s) = \rho(s) \cdot \sum_{t=t_{\max}+1}^{T} \delta(n_i(t, s) \geq tol \cdot n_{\max})$$

  Where $tol \in [0, 1]$ is the tolerance of the gap between the max and the number of infected nodes, $\rho(s)$ is the epidemic peak when the strategy vector s is used, and
  $\delta(n_i(t, s) \geq tol \cdot n_{max}) = \begin{cases} 1 \text{ if } n_i(t, s) \geq tol \cdot n_{\max} \\ 0 \text{ otherwise} \end{cases}$.
  We consider only the time steps before the max because, before the start of the decrease of the number of infected nodes, the attacker cannot know that he reached the maximum, hence if he planned an attack after infecting a maximal number of nodes, he will only do this attack after the start of the decline.

These two pay-off functions will permit us to evaluate the attacks from different perspectives and do different games.

2.4.2 Defender's pay-off

As for the attacker, we will also consider two pay-off functions for the defender. As explained earlier, we take into consideration the investments as well as another feature of the attack in these functions because the defender's goal is to defend the network without spending too much. So we consider two functions:

- The defender wants to minimize the epidemic peak. Say there are N nodes in the graph, so n devices in the network, ρ is the epidemic peak, α and β are two coefficients, then we can express the defender's pay-off u_D when the strategy vector $s = (c_A, K)$ is used:[3]

$$u_D(c_A, K) = \alpha \cdot \rho(s) + \beta \cdot \frac{K \cdot 1000}{N}$$

[2] U: unicast, B: broadcast, C: chaotic, S: sneaky. See part 2.2.

[3] As said before, K is in thousands of euros, hence the "1000". Also, we want to minimize the cost per device, hence the N.

- Another point of view for the defender is to minimize the accumulated number of infected nodes:

$$u'_D(c_A, K) = \alpha \cdot \sum_{t=0}^{T} n_i(t, s) + \beta \cdot \frac{K \cdot 1000}{N}$$

These functions will permit us to do different games where the defender and the attacker have different objectives.

3 Results and analysis

To do the simulations, we use the following graph:

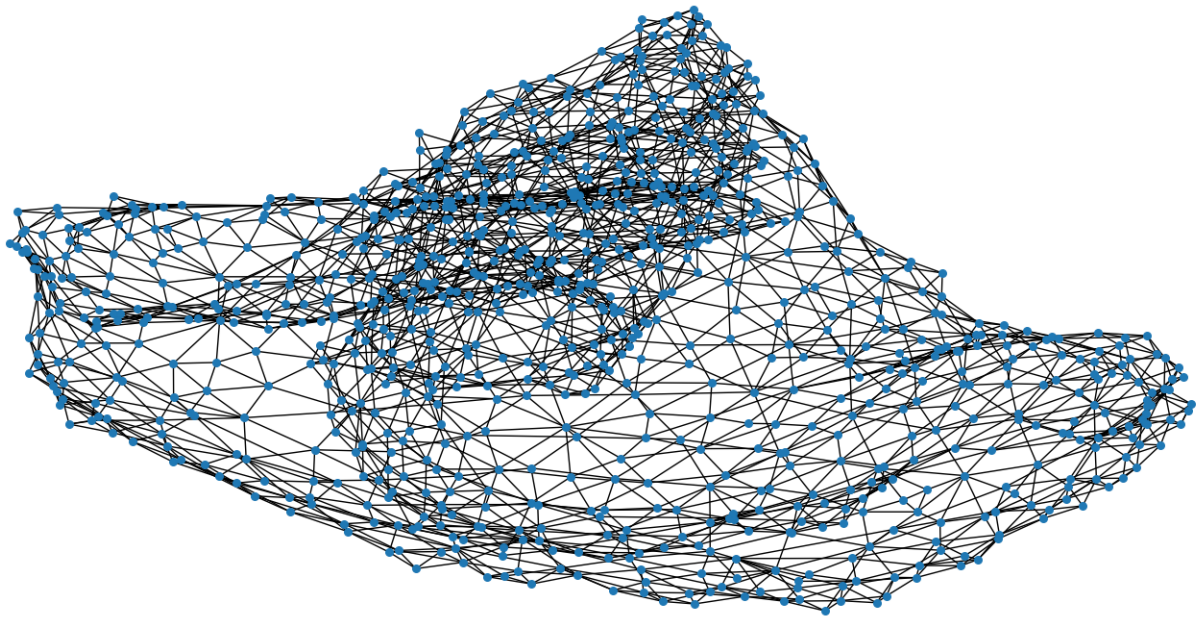


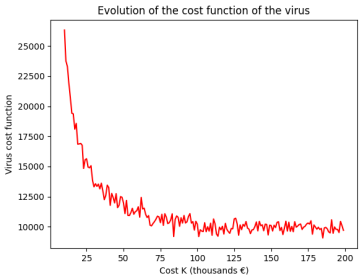
Figure 2: Graph used for the simulations

To obtain this graph, we generated a random number of points between 800 and 1200 (951 points finally), and we took the Delaunay triangulation of these randomly generated points.

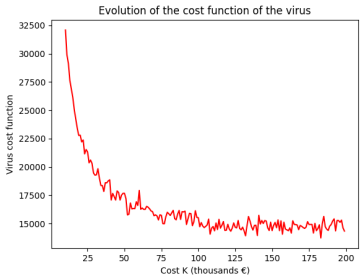
We consider three different games where the pay-off functions will differ. To have the most accurate results, we did 30 simulations for each pair of attacker strategy/defender strategy and we took the average of the simulations' outcomes. For the games, the defender will adopt the following strategies: $K \in \{5k \,|\, k \in [|1, 39|]\}$.

3.1 First game

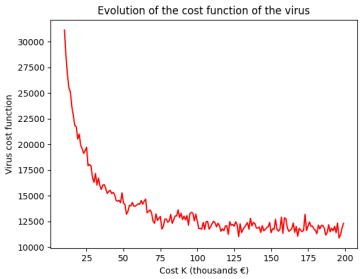
In the first game, we consider that the attacker wants to maximize the accumulated number of infected nodes, and the defender wants to minimize the epidemic peak, so we use the pay-off functions u_A and u_D. For the u_D function, we use the following parameters: $\alpha = 1$, $\beta = 5$, to try to scale the two terms in the function to the same range, so they will be given the same importance.
Here are plotted the pay-off functions of the attacker and the defender for this game:



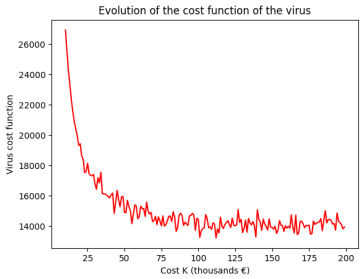
(a) Unicast propagation strategy



(b) Broadcast propagation strategy

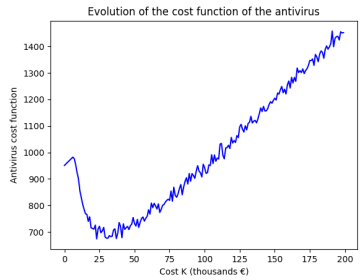


(c) Chaotic propagation strategy

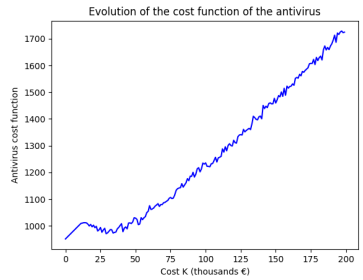


(d) Sneaky propagation strategy

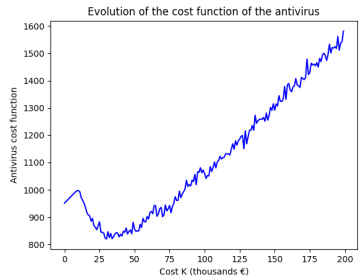
Figure 3: Attacker's pay-off function for all the virus strategies



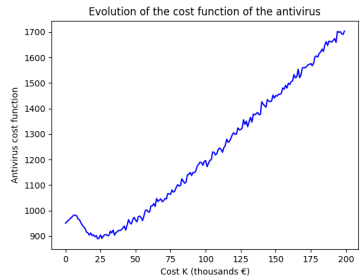
(a) Unicast propagation strategy



(b) Broadcast propagation strategy



(c) Chaotic propagation strategy



(d) Sneaky propagation strategy

Figure 4: Defender's pay-off function for all the virus strategies

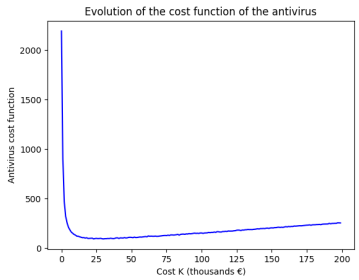
The first thing to analyze in this game is that the strategy $K = 30$ is a dominant strategy for

the defender, indeed, whatever the choice of the attacker, the defender will always minimize his pay-off (because he wants to minimize it) by choosing the strategy $K = 30$. Knowing this, we can resolve the game by proceeding to an iterated elimination of dominated strategies (IESDS), and then eliminate all the attacker's strategies but the *broadcast propagation* one.
So, there is a unique Nash equilibrium in this game, and it is **(B, K = 30)**. As this strategy vector results from an IESDS, it is a Nash equilibrium. Like the same process eliminates all the other strategy vectors, none can also be a Nash equilibrium. So, we have the uniqueness of the Nash equilibrium found here.[4]
This result means that if the defender wants to minimize his pay-off/cost function by giving equal importance to the epidemic peak and his investment, he has to always choose the strategy $K = 30$, meaning that he has to invest $30k€$ in the development of a solution. The attacker, who wants to maximize his pay-off, then just has to choose the best solution to answer this, if we assume that the defender's best solution is known by both players, he will choose the *broadcast propagation* for his virus because it's this propagation that offers to the attacker the best pay-off when the defender uses a defense budget of $30k€$.

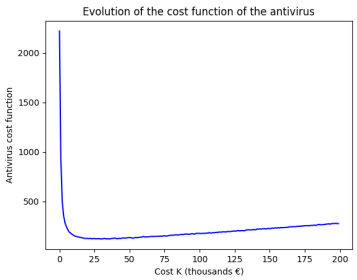
3.2 Second game

In this second game, we consider the same pay-off function for the attacker but now, at his opposite, the defender wants to minimize the accumulated number of infected nodes as well as his investment. We use the pay-off functions u_A and u'_D. We scale appropriately the two terms of u'_D to give them the same importance by using $\alpha = \frac{1}{220}$ and $\beta = 1$.

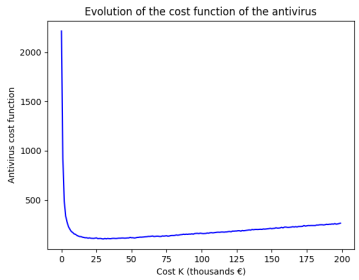
We here plot the pay-off functions of the defender for this game, the attacker's pay-off functions are the same as in the previous part:



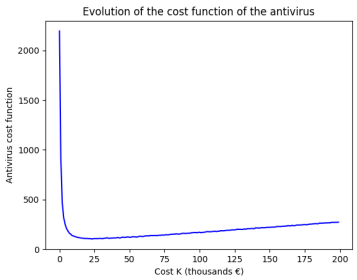
(a) Unicast propagation strategy



(b) Broadcast propagation strategy



(c) Chaotic propagation strategy



(d) Sneaky propagation strategy

Figure 5: Defender's pay-off function for all the virus strategies

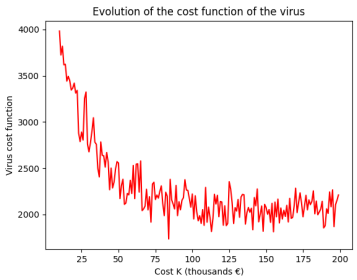
[4]To see more about the links between Nash equilibrium and IESDS, look at the personal page of David Marker, a retired math professor at the University of Illinois at Chicago: https://homepages.math.uic.edu/~marker/stat473-S16/IESDS.pdf

We get the same results that in the first game, we find a unique Nash equilibrium with the strategy vector **(B, K=30)**.
For this second game, nothing changes for both players of the game, the same strategies give the best results.

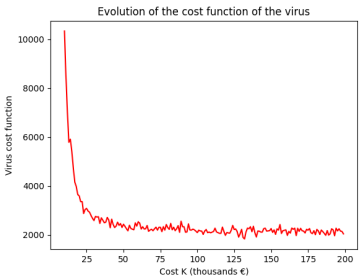
3.3 Third game

For this last game, the attacker wants to maximize the time when the virus is near its peak, and the defender wants to minimize the epidemic peak and his investment as in the first game. So, we use the pay-off functions u'_A and u_D. We choose the following parameters: for u'_A, $tol = 0.9$, so we have a tolerance for the values until 90% of the epidemic peak; for u_D, as for the first game, $\alpha = 1$, $\beta = 5$ to scale the two terms of the pay-off function.

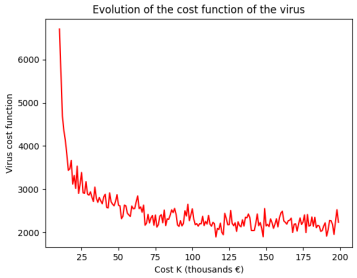
We plot here the attacker's and defender's pay-off functions for this game:



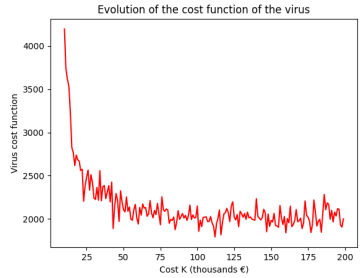
(a) Unicast propagation strategy



(b) Broadcast propagation strategy

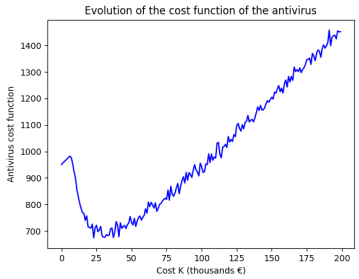


(c) Chaotic propagation strategy

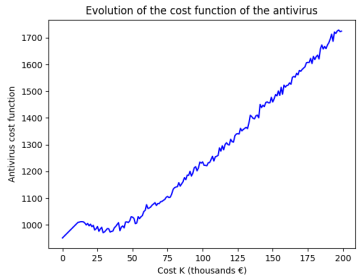


(d) Sneaky propagation strategy

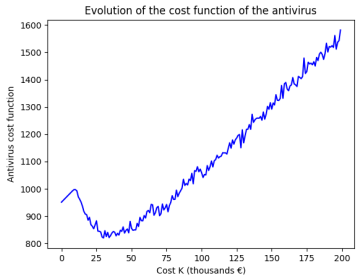
Figure 6: Attacker's pay-off function for all the virus strategies



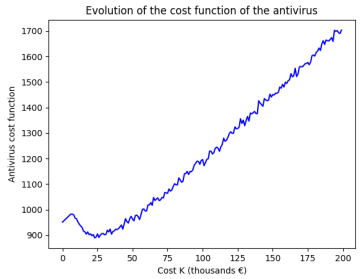
(a) Unicast propagation strategy



(b) Broadcast propagation strategy



(c) Chaotic propagation strategy



(d) Sneaky propagation strategy

Figure 7: Defender's pay-off function for all the virus strategies

As the defender's pay-off is the same as in the first game, these figures are the same as the ones plotted for this game.

For this final game, we again get the result that $K = 30$ is a dominant strategy for the defender. But, by an IESDS now we get that the best strategy for the attacker, knowing this, is the chaotic strategy. So we have a unique Nash equilibrium that is **(C, K=30)**.

3.4 Analysis of the games

In this section, we studied three different games, in which we changed the pay-off functions for the players to see this confrontation from different points of view. A major result is that the strategy $K = 30$ is always the dominant strategy for the defender. All the games studied can be resolved by IESDS, hence, the solutions of the games always include the strategy $K = 30$ for the defender, and for the attacker the best strategy changes. When the attacker wants to maximize the accumulated number of infected nodes, he has to choose the broadcast propagation type, but when he wants to maximize the time when the number of infected nodes is near the epidemic peak, he must choose the chaotic propagation strategy. All these games have a unique Nash equilibrium.
One can wonder why $K = 30$ is always the best strategy. Here is a first observation and a first explanation: When $K = 30$, we have $\Delta(K) = 6$. So, the antivirus solution will be set up 6 time steps after the detection of the infection. With the results obtained in this section, it seems that this period of 6 time steps is the best compromise possible between the investment made by the defender and the waiting time for the antivirus to be set up when using the Δ function presented in section 2.

4 Conclusion

In this work, we study the confrontation between an attacker and a defender in the context of a malware attack on a network. We define a model, using game theory to analyze the game and see what could be the attacks and the answers of the two players. By modeling several pay-off functions and strategies for the players, we can analyze the game from different perspectives both for the attacker and the defender. Thus, while the attacker could seek to maximize the accumulated number of infected devices or the number of step times having good control of the network, the defender wants to minimize his investments while minimizing the effects of the attack: either minimizing the epidemic peak or the accumulated number of infected nodes. For this, the players have different strategies: the attacker can choose the propagation strategy for his virus and the defender can choose his defense budget.
In all three different games studied, we obtained and characterized a unique Nash equilibrium by employing a method of iterated elimination of the dominated strategy (IESDS) and we found a dominant strategy for the defender, i.e. a strategy from which he has no advantage to switch whatever the strategy used by his opponent.
In future works, we could consider using another Δ function inspired by real-life time delay. We could also consider giving roles to some nodes of the network that would affect the propagation and that could even be the target of attacks. Also, adding external factors and hazards to the simulations could be examined.