# Asymmetric Centrality Game against Network Epidemic Propagation

Arnold Willie Kouam Kounchou, Yezekael Hayel, Serge Olivier Tsemogne Kamguia, Gabriel Deugoué, Charles Kamhoua

# Asymmetric Centrality Game against Network Epidemic Propagation

Willie KOUAM[1,2][0000−0002−6804−868X], Yezekael HAYEL[2][0000−0003−3891−3916], Gabriel DEUGOUÉ[1][0000−0003−1015−0902], Olivier TSEMOGNE[4][0000−0002−0989−3269], and Charles KAMHOUA[3][0000−0003−2169−5975]

[1] University of Dschang, Dschang, Cameroon
willie.kouam@alumni.univ-avignon.fr
agdeugoue@yahoo.fr
[2] CERI/LIA, Avignon Université, France
yezekael.hayel@univ-avignon.fr
[3] DEVCOM Army Research Laboratory, USA
charles.a.kamhoua.civ@army.mil
[4] IMT Atlantique, Brest, France
olivier.tsemogne@gmail.com

**Abstract.** The Mirai botnet network epidemic discovered in 2016 falls into the category of numerous epidemics propagated by attackers over a network to gain control over multiple devices. This particular epidemic has been employed in some of the most extensive and widespread distributed denial of service (DDoS) attacks [24]. To take control of numerous devices, the attacker's strategy consists of injecting malicious code from an infected device into one or more vulnerable neighboring devices. This initiates a conflict, as the defender attempts to restrict the attacker's influence and control. Intelligent and rational agents (defender and attacker) thus engage in a conflictual interaction, constantly competing for optimal strategies within the network. Their objective is to gain control over the most crucial devices, which are identified using *centrality measures*. Nevertheless, an agent's perception of the significance of devices may vary due to factors such as variations in roles, information accessibility, available resources, and diverse viewpoints on risks, issues, or opportunities [8]. Consequently, the agents involved in the process may hold different views regarding the significance of devices, resulting in the utilization of different centrality measures. The significance of considering these variations in centrality measures, as well as the impact on each agent's objective, is emphasized by our analysis. Hence, we propose a non-zero-sum game model to identify the optimal centrality measure for each agent in the context of controlling an epidemic spread. Our model also provides the NE (Nash Equilibrium) strategy profile for agents at each stage of the game. Numerical experiments show that, by taking into account these differences in centrality measures and using our game model, defenders effectively limit the impact of epidemics caused by malicious attackers.

**Keywords:** Epidemic network · Cyber deception · Centrality measure · Non-zero-sum game

5

[5]DISTRIBUTION A. Approved for public release: distribution unlimited.

## 1 Introduction

Networks have become an essential part of our daily lives, ranging from social networks to transportation networks, and even cyber networks. One of the critical challenges in these networks is controlling epidemics that spread through them [16]. The spread of epidemics in a network is commonly due to an agent attempting to compromise devices in the network through a cyber-attack, which spreads like a virus, infecting other devices in the network. To prevent this, various techniques have been developed, including the use of game theory [9,25,26]. However, motivated by propagation scenarios involving two main agents, one of which aimed to eventually compromise the system, we take into consideration a wide range of games wherein the attacker and the defender's interactions are dynamic, involve uncertainty, and could extend over a long period of time. In recent years, game theory has emerged as a powerful tool to model and analyze the strategic interactions between agents in such networked systems and has been applied in many fields, including cyber security [5].

In the field of game theory for cyber security, the problem of epidemic control has become increasingly important due to the rise of epidemics caused by malicious intelligent and rational agents, who generally have complete information about the state of the network. Due to the attacker's informational advantage, a variety of deception techniques have been developed to safeguard the network. Deception is a cyber defense mechanism that aims to intentionally misguide the cyber attacker by hiding true information or presenting false information to attackers, in order to prevent or at least to reduce damages from cyber attacks [22]. One important cyber deception technique under uncertainty is the use of tools such as honeypots to mislead attackers and detect attacks [1]. Therefore, the authors of [21], employing honeypot placement as a defense technique, recently proposed a one-sided partially observable stochastic game framework for determining an optimal strategy for both the attacker and defender in the context of network epidemic problems. However, the proposed value iteration (VI) algorithm presents a major problem related to scalability (24 nodes in the context of lateral movement problems with lower dimensional states and belief spaces). Meanwhile, the epidemic control problem generally applies to networks with numerous devices and, henceforth, requires more efficient tools. To address this issue, the authors of [23] modeled the epidemic control problem as a game between two players who make decisions based on centrality measures, which are measures of a device's importance or influence in a network. Nonetheless, the study only examines the scenario where both agents use the same centrality measures from the outset of the game. In practice, however, agents may hold varying perspectives and levels of knowledge regarding the significance of devices within a network. Due to the asymmetry of the agents' knowledge, they may have divergent preferences regarding the centrality measures they choose, as these decisions are influenced by the information available to each of them.

Exploring the scenario in which agents use distinct centrality measures holds significant importance for various reasons. Firstly, different centrality measures capture various aspects of a device's significance in a network [15]. Due to agents' lack of awareness of each other's methods, they may have distinct opinions on which nodes are the most important. Secondly, agents may have varying preferences for using different centrality measures due to factors like implementation complexity and impact on the network. For instance, one agent may prefer degree centrality for its simplicity, while another agent may favor betweenness centrality for its consideration of the network's overall structure. Finally, the use of different centrality measures may lead to different decisions and outcomes, affecting the effectiveness of epidemic control strategies. Studying the impact of different centrality measures on agents' decisions and strategies can help us understand how information and

objectives influence decision-making and the resilience of epidemic control strategies to errors or inaccuracies in centrality measures.

This article thus presents a new approach to the centrality game on a network using a cyber deception technique. The proposed game is asymmetric, with two players making decisions based on their respective centrality measures. The game is modeled as a two-player non-zero-sum game on a graph, where the nodes represent devices in the network, and the edges represent attacks using specific vulnerabilities. The attacker sequentially chooses from any infected node, adjacent and susceptible nodes to attack keeping his position secret from the defender. On his side, the defender chooses edges that will act as honeypots, to detect and counteract unauthorized use of information systems; the proposed model considers several factors. First, each player chooses his or her centrality measure at the start of the game, and this choice is common knowledge. Second, the attacker does not observe all the actions of the defender after a given time slot. Third, the detection of transmission means that the defender cures the infected node, the source of the transmission. Moreover, although the nodes lack intelligence and rationality, they have the potential to make decisions based on their current state. During each time slot, a node has the potential to transition from a Susceptible to a Resistant state or from an Infected to a Susceptible state, but the exact probabilities of these changes are only known to the defender. This assumes that a time slot of the game consists of two stages: the stage of *strategic interactions* and the stage of *random transitions.* We thus propose four key contributions for improving the scalability of the proposed solution:

- a two-player non-zero-sum infinite horizon stochastic game is studied in which no player observes the opponent's actions,
- a coupled system in which two players act strategically and a set of nodes react to their individual states,
- an investigation of the impact of different centrality measures on agents' strategies and the game outcome,
- an examination of the effects of network topology and parameter settings on the game outcome.

Our results highlight the importance of taking into account the heterogeneity in agents' perspectives when designing strategies for epidemic control problems in networks.

## 2 Related work

A common cause of epidemic spread in networks is the attempt by an agent to compromise the computers in the network through a cyber attack, with various goals such as distributed denial of service (DDoS). Indeed, DDoS follows the furtive preliminary recruitment of devices into a zombie army called a botnet [12]. A report by [11] revealed that during the period between April 2013 and May 2014, DDoS attacks affected 38% of companies that provide financial services or operate online services for the public. The mathematical modeling of epidemics borrows fundamental notions from epidemiology in that the population is divided into compartments and the name of the epidemic is derived from the possible compartments and the possible transitions of an individual between compartments. Thus, several epidemic models can be distinguished, namely SIS, SIR, etc. The concept of Nash equilibrium has been used in several works including various epidemic models to determine a profile of equilibrium strategies between conflicting agents. For example, the NE concept is used in [19] and [20] to stop the spread of SIS epidemics in a decentralized manner and to optimize influence in competitive contexts. To compare the advantages of centralized and

decentralized protection of a network against threats, Trajanovski, Hayel, et al. [19] discuss the price of anarchy (PoA) in a single community, bipartite, and multi-community networks. They prove the existence of the Nash equilibrium and outline a reinforcement learning algorithm to find the NE in pure strategies. However, like several other authors, they did not include strategic defense mechanisms as deception schemes, despite their effectiveness in contexts with asymmetric information and an attacker's advantage. Several deception methods exist in the literature related to network security. In [17] numerous deception techniques have been proposed for network security, such as impersonation, delays, fakes, camouflage, false excuses, and social engineering because traditional cybersecurity approaches face a continual cycle of detecting and responding to new threats and vulnerabilities. Therefore, game models are more elaborated and computers can examine the huge number of possible threat scenarios in cyber systems better than humans. However here, no one is guaranteed to have information dominance in terms of intelligence and accessibility. Hence the importance of game theory for cyber security. Because of these observations, the authors of [21] employed a $SIR$-type game model integrating game theory and cyber deception for epidemics. Indeed, they modeled the problem as a partially observable stochastic game on a graph in which the defender aims to optimize the placement of honeypots to mislead the attacker as much as possible. However, the proposed approach presents problems related to the scalability with the size and complexity of the proposed Heuristic Search Value Iteration (HSVI) algorithm [10].

According to some authors, the globality of the proposed solution in the previous approach may be responsible for these limitations, as it does not consider the topology of the considered graph. Therefore, [23] proposed an approach in which the agents pose their actions taking into account the influence of the nodes in the graph, influence measured through various centrality measures [2]. The authors of [23] demonstrated that their model is a game of centralities thresholds, and provided the necessary conditions for obtaining a Nash equilibrium. However, these results were based on the assumption that the two agents in conflict act according to the same centrality measure, which is not always the case in real-world situations. Indeed, in most cyber security problems, the protagonists do not have identical information and resources. As a result of this asymmetry, there can be an asymmetry in their perceptions of a node's importance within the graph. The selection of the centrality measure is thus influenced, resulting in agents eventually opting for different centrality measures.

## 3 General model description

In this game, there are two sides: the attacker, who controls the malware and wants to infect as many devices in the network as possible, and the defender, who wants to stop or reduce the infection. The devices in the network will make a decision based on their own state. As the game progresses, different stages will occur, and we'll explain each one in more detail. So, in summary, it's a battle between the attacker and defender to control the network, and the network devices will make a probabilistic decision based on their current state.

### 3.1 Problem description

The attacker tries to infect a maximum number of devices in the network to reach a minimum threshold that will allow her to launch her attack. She can do this because some devices have weak points that can be easily taken advantage of. For example, many devices use default passwords that don't change for a long time, so they are more likely to be hacked, due to the relatively limited

range of default passwords. Knowing the status of each device through frequent probes enables the attacker to infect and compromise the system to spread the malware. To prevent this spread, we suggest the defender deploy a patch for infected devices and use a cyber deception technique. An Intrusion Detection System (IDS) installed on certain network edges can identify code transmissions and nullify them, but this defensive action could reveal the defender's countermeasures to the attacker. To conceal the defensive measure, we propose that the defender allows the code to reach its target, revealing to the attacker that the device is infected, and then disinfects the device before the attacker's subsequent probe. The tool thus used is called an *intrusion-proof system (IPS)* in the following. It can detect malicious connectivity attempts and automatically install patches on infected devices that are sources of the malware propagation attempt. Additionally, users of infected or vulnerable devices can choose to accept the patch or customize their password, and the defender is informed of their decision. The probabilities of infected devices accepting patches and vulnerable devices customizing passwords are known only to the defender and are not reported to the attacker.

### 3.2 System model

This section provides a detailed description of the interactions between the attacker and the defender in the context of an epidemic spread. The model takes into consideration three main factors: the conflicting interests of the two parties, the dynamic spread of the virus through the network, and the response of each device depending on its current state. To distinguish between the strategic interactions of the players and the internal state transitions of the devices, the model assumes that the game is divided into time slots, with each time slot comprising two stages: the strategic stage (the first stage) and the reactive stage (the second stage).

#### 3.2.1 Time slot description

A time slot in this framework involves two distinct stages: firstly, the strategic actions of the attacker and defender, and secondly, the probabilistic moves/reactions of the devices, which depend on their current state, i.e., internal state transitions of the devices.

**Strategic stage:** The two players (attacker and defender) make their actions, which result in an intermediate state $a(z)_i$ for each device $i$ of the network.

- *Attacker:* Assuming perfect information about the state of each device in the network at every time slot, the attacker is the strategic and rational agent who spreads malware through the network by silently propagating it from each infected device to adjacent susceptible devices. However, the attacker may not want to transmit the malware to all susceptible neighbors of each infected device, as doing so could expose the infected devices and raise the defender's suspicions.
- *Defender:* In order to limit the spread of the malware, the defender acts strategically by using IPSs to monitor a limited number of edges at each time slot. Whenever a malware transmission is detected on edge, the defender cures the two devices involved in the transmission (i.e., the source device and the target device). The defender's choice of IPS locations is not revealed to the attacker; these IPSs are only available for a single time slot, and the interaction between the attacker and defender is repeated at each time interval.
- It should be noted that each player's actions are influenced by the centrality measure he/she has chosen to evaluate the influence of the network devices. After establishing the action profile, the

system enters an intermediate state $a\,(z)$, indicating the beginning of the second stage within the current time slot.

**Reactive stage:** During the second stage of a time slot, each device has the ability to take an action that can result in a change of its internal state. The transition depends on the device's current state and the specific self-restoration process used. An infected device can perform tasks such as updating software or running a malware scan to eliminate the threat with probability $\alpha$, and then transition to the susceptible state. Alternatively, a susceptible device can choose with probability $\rho$, to install an immunization mechanism to become resistant. Regardless of the action taken, each device $i$ will transition from the intermediate state $a(z)_i$ to a final state $z_i^{'}$, as depicted in figure 1. Not being informed of these transition probabilities, the attacker cannot infer the defender's actions, since an infected device may become susceptible due to either an IPS or its own decision.

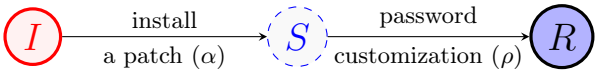
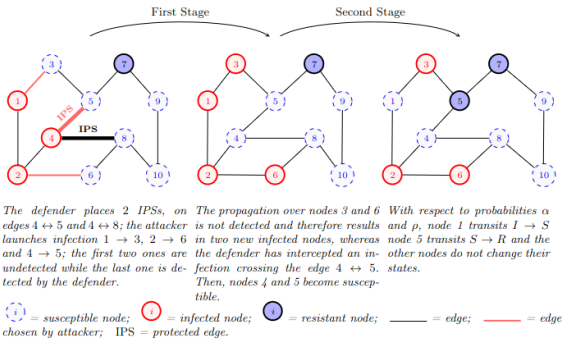
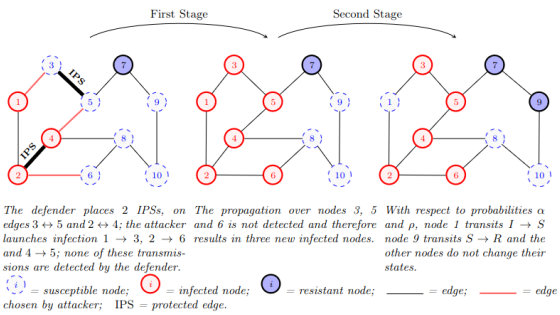



Fig. 1: Possible state transitions of a node depending on the decision taken.

**Illustration of a time slot sequence:** We present a hypothetical situation for our game with two different scenarios. In the first one $(a)$, both agents use degree centrality, while in the second scenario $(b)$, the defender uses betweenness centrality and the attacker uses degree centrality. In each scenario, the attacker selects from any infected node the susceptible neighbor with the highest centrality value. Meanwhile, the defender chooses two nodes with the highest centrality values to protect.




(a) A time slot of the game: a possible scenario with 10 devices when both defender and attacker use *degree centrality*.




(b) A time slot of the game: a possible scenario with 10 devices when the defender uses *betweenness centrality* and the attacker uses *degree centrality*.

After explaining the sequence of events within a given time slot, the following section focuses on describing the *asymmetric game* model. This model is used to determine the optimal strategies of the attacker and defender at each time slot. It should be noted that, in our context, a player's optimal strategy comprises two key components. The first one is the selection of the centrality measure, and the second one is the computation of the optimal probability distribution associated with it. In the following, we refer to the centrality measure used by the defender as $c^d$ and the centrality measure used by the attacker as $c^a$. Furthermore, we assume that the centrality measure used by each player is common knowledge information.

### 3.3 Definition of the asymmetric centrality game

Without loss of generality, we focus on the defender's goal of minimizing and the attacker's goal of maximizing the number of infected devices at each time slot. Considering the fact that only the attacker knows the state of the system at each time slot, which is private information for her, the *asymmetric centrality game* is the *non-zero sum Bayesian game* defined by the tuple $\mathcal{G} = \left(G, N, Z, A = A_1 \times A_2, \alpha, \rho, \mathcal{O}, \mathcal{R}_d, \mathcal{R}_a, b^0\right)$, where:

- $G = (V, E)$ is a non-directed graph representing the network where $V = \{1, 2, 3, ..., |V|\}$ is the set of nodes and $E \subseteq \{e \in 2^{|V|}, |e| = 2\}$ is the set of edges,
- $N$ is the set of players: the defender (player 1) and the attacker (player 2),
- The network at time $t$ is the sub-graph of the network at time $t-1$, consisting of non-resistant nodes, i.e. at time $t$, $V = V \setminus R^{t-1}$ (where $M^{t-1}$ represents the set of nodes of type $M$ at the end of time slot $t-1$),
- $Z$ is the set of possible states of the network and each state $z$ is defined by, $z = (z_i)_{i=1}^{|V|}$; where $z_i = \begin{cases} S & \text{if node } i \text{ is susceptible} \\ I & \text{if node } i \text{ is infected} \end{cases}$; for all $i \in V$. The attacker knows the state of the network while the defender has to update his belief at each time slot $t$,
- The set $A_1$ refers to the actions available to the defender, which involve selecting up to $h$ edges to deploy IPSs. The defender lacks knowledge about the state of the network at each time $t$, so all edges in the set $\mathbb{S} = E \cap (V \times V)$ are potentially usable by the attacker. However, since $\mathbb{S}$ may be quite large, the defender should limit his field of action by playing over the set $\mathbb{S}_b$ at each time $t$, referred to as the **defender's critical zone**. This set is defined by $\mathbb{S}_b = \bigcup_{z \in \text{supp}(b)} \mathbb{S}_z$ where $\mathbb{S}_z = \{(i,j) \in I^t \times S^t : \{i,j\} \in E\}$ and $\text{supp}\,(b) = \{z \in Z \mid b\,(z) \neq 0\}$ is the support of the belief $b$ over the network state. Then, the defender's actions space is accordingly, $A_1 = \begin{cases} \mathcal{P}_h\,(\mathbb{S}_b) \text{ if } |\mathbb{S}_b| > h \\ \left\{2^{\mathbb{S}_b}\right\} \quad \text{otherwise} \end{cases}$,
- The set of actions available to the attacker is denoted as $A_2$. To perform an action, the attacker selects a set $T_i$ of adjacent susceptible nodes from any infected node $i$, as the targets for propagating the malware. The attacker strategically avoids targeting the same susceptible node from different infected sources to minimize the likelihood of detection, as doing so would not yield any additional benefit. Thus, an action $a_2$ for the attacker at time $t$ can be represented as a tuple $T = (T_i)_{i \in I^t} \equiv \bigcup_{i \in I^t} T_i^{'}$, with $T_i^{'} = \{\{i,j\}, j \in T_i\}$ that satisfy the properties: $\begin{cases} \forall i \in I^t, & T_i \subseteq S^t \\ \forall i \in I^t, \forall j \in T_i, & (i,j) \in \mathbb{S}_z \\ \forall k,l \in I^t, & k \neq l \implies T_k \cap T_l = \emptyset \end{cases}$,
- $\mathcal{O}$ represents the set of observations made by the defender, which depends on the state of each node at the end of each time slot. The defender observes a node if its state changes from $I$ to $S$ or from $S$ to $R$. When there is no observation for the defender, then $o_i = \mathfrak{X}$. A defender's observation profile can thus be defined as a tuple $o(z, a, z') = (o_i)_{i \in V}$, with $o_i \in \{z_i', \mathfrak{X}\}$, $\forall i \in V$,
- $\mathcal{R}_d$ is the defender's reward and $\mathcal{R}_a$ the attacker's one at each time slot, $b^0$ is the defender's initial belief.

## 4 Asymmetric centrality game solution

Every agent aims to hold the most crucial positions within the graph. To achieve this, each agent focuses on nodes with high centrality values from their individual perspective ($c^a$ for the attacker and $c^d$ for the defender). The model's outcome thus depends on the centrality of each node, which rewards the defender if a node transits from an infected to a susceptible or resistant state, while the attacker benefits from infecting a node.

### 4.1 Players' rewards associated with an action profile

When an action profile $(W,T) \in A_1 \times A_2$ is implemented, the centrality value of any node is rewarded to the defender, if the node transits from infected to susceptible or resistant, or to the attacker, if the node transits from susceptible to infected. Table 1 displays the expected partial reward for both players, which includes the centrality value of node $i$ according to both the defender's and attacker's centrality measures, denoted as $c_i^d$ and $c_i^a$ respectively.

| | | ATTACKER: Propagate $i \to j$? | |
|---|---|---|---|
| | | Propagate $(\{i,j\} \in T)$ | No propagate $(\{i,j\} \notin T)$ |
| DEFENDER: Watch $\{i,j\}$? | Watch $(\{i,j\} \in W)$ | $c_i^d,\ -c_i^a$ | 0 |
| | No watch $(\{i,j\} \notin W)$ | $-(1-\alpha)\,c_j^d,\ (1-\alpha)\,c_j^a$ | 0 |

Table 1: The players expected reward resulting from a joint action $(W,T)$ on one edge $\{i,j\}$.

At a given state $z$, the rewards associated to an action profile $(W,T) \in A_1 \times A_2$ are assigned to the defender and attacker as follows:

$$\mathcal{R}_d(W,T) = \sum_{\substack{\{i,j\}\in\mathbb{S}_z \\ \{i,j\}\in W \\ j\in T_i}} c_i^d - \sum_{\substack{\{i,j\}\in\mathbb{S}_z \\ \{i,j\}\notin W \\ j\in T_i}} (1-\alpha)\,c_j^d = \sum_{\substack{\{i,j\}\in\mathbb{S} \\ \{i,j\}\in W \\ j\in T_i}} c_i^d - \sum_{\substack{\{i,j\}\in\mathbb{S} \\ \{i,j\}\notin W \\ j\in T_i}} (1-\alpha)\,c_j^d,$$

$$\mathcal{R}_a(W,T) = \sum_{\substack{\{i,j\}\in\mathbb{S}_z \\ \{i,j\}\notin W \\ j\in T_i}} (1-\alpha)\,c_j^a - \sum_{\substack{\{i,j\}\in\mathbb{S}_z \\ \{i,j\}\in W \\ j\in T_i}} c_i^a = \sum_{\substack{\{i,j\}\in\mathbb{S} \\ \{i,j\}\notin W \\ j\in T_i}} (1-\alpha)\,c_j^a - \sum_{\substack{\{i,j\}\in\mathbb{S} \\ \{i,j\}\in W \\ j\in T_i}} c_i^a.$$

Indeed, for all $\{i,j\} \in \mathbb{S} \setminus \mathbb{S}_z$, we never get $j \in T_i$.

### 4.2 Players' rewards associated with a strategy profile

Denote by $\Pi_i$ the strategy space for player $i$. Let's consider mixed strategies $\pi_1 \in \Pi_1$ for the defender and $\pi_2 : Z \longrightarrow \Delta(A_2) \in \Pi_2$ for the attacker.

• *Defender's reward:* The expected reward of the defender with belief $b \in \Delta(Z)$ associated to the strategy profile $\pi = (\pi_1, \pi_2)$ is $\mathcal{R}_d(\pi|b) = \sum_{z \in Z} b(z)\, \mathcal{R}_d(\pi|z)$, where

$$\begin{aligned}
\mathcal{R}_d(\pi|z) &= \sum_{(W,T) \in A_1 \times A_2} \pi_1(W)\, \pi_2(T|z)\, \mathcal{R}_d(W,T), \\
&= \sum_{\substack{\{i,j\} \in \mathbb{S} \\ (W,T) \in A_1 \times A_2 \\ \{i,j\} \in W \\ j \in T_i}} \pi_1(W)\, \pi_2(T|z)\, c_i^d + \sum_{\substack{\{i,j\} \in \mathbb{S} \\ (W,T) \in A_1 \times A_2 \\ \{i,j\} \notin W \\ j \in T_i}} \pi_1(W)\, \pi_2(T|z)\, (\alpha - 1)\, c_j^d, \\
&= \sum_{\{i,j\} \in \mathbb{S}} \pi_1(i,j)\, \pi_2(i,j|z) \left( c_i^d + (1-\alpha)\, c_j^d \right) - \sum_{\{i,j\} \in \mathbb{S}} (1-\alpha)\, \pi_2(i,j|z)\, c_j^d,
\end{aligned}$$

$\pi_1(i,j) = \sum_{\substack{W \in A_1 \\ \{i,j\} \in W}} \pi_1(W)$ and $\pi_2(i,j|z) = \sum_{\substack{T \in A_2 \\ j \in T_i}} \pi_2(T|z)$ being respectively the probabilities that the defender watches edge $\{i,j\}$ and the attacker targets node $j$ from node $i$ at state $z$. Therefore,

$$\begin{aligned}
\mathcal{R}_d(\pi|b) &= \sum_{z \in Z} b(z) \Bigg( \sum_{\{i,j\} \in \mathbb{S}} \pi_1(i,j)\, \pi_2(i,j|z) \left( c_i^d + (1-\alpha)\, c_j^d \right) - \sum_{\{i,j\} \in \mathbb{S}} (1-\alpha)\, \pi_2(i,j|z)\, c_j^d \Bigg) \\
&= \sum_{\{i,j\} \in \mathbb{S}} \pi_1(i,j)\, \varphi_d(i,j|b,\pi_2) - \sum_{\{i,j\} \in \mathbb{S}} \psi_d(i,j|b,\pi_2)
\end{aligned}$$

where, $\varphi_d(i,j|b,\pi_2) = \pi_2(i,j|b) \left( c_i^d + (1-\alpha)\, c_j^d \right)$ is the defender's expected profit in case of detected virus transmission from $i$ to $j$, $\psi_d(i,j|b,\pi_2) = (1-\alpha)\, \pi_2(i,j|b)\, c_j^d$ is the marginal loss of the defender in case of malware transmission from nodes $i$ to $j$, and $\pi_2(i,j|b) = \sum_{z \in Z} \pi_2(i,j|z)\, b(z)$ is the marginal probability that the attacker spreads the virus from $i$ to $j$ knowing $b$.

• *Attacker's reward:* The expected reward of the attacker associated with the strategy profile $\pi = (\pi_1, \pi_2)$, when the defender's belief is $b \in \Delta(Z)$, is given by $\mathcal{R}_a(\pi|b) = \sum_{z \in Z} b(z)\, \mathcal{R}_a(\pi|z)$.

$$\begin{aligned}
\mathcal{R}_a(\pi|z) &= \sum_{(W,T) \in A_1 \times A_2} \pi_1(W)\, \pi_2(T|z)\, \mathcal{R}_a(W,T) \\
&= \sum_{\substack{\{i,j\} \in \mathbb{S} \\ (W,T) \in A_1 \times A_2 \\ \{i,j\} \notin W \\ j \in T_i}} \pi_1(W)\, \pi_2(T|z)\, (1-\alpha)\, c_j^a - \sum_{\substack{\{i,j\} \in \mathbb{S} \\ (W,T) \in A_1 \times A_2 \\ \{i,j\} \in W \\ j \in T_i}} \pi_1(W)\, \pi_2(T|z)\, c_i^a, \\
&= \sum_{\{i,j\} \in \mathbb{S}} \pi_2(i,j|z) \left( (1-\alpha)\, c_j^a - \pi_1(i,j) \left( (1-\alpha)\, c_j^a + c_i^a \right) \right),
\end{aligned}$$

Therefore,

$$\mathcal{R}_a(\pi|b) = \sum_{z\in Z} b(z) \sum_{\{i,j\}\in\mathbb{S}} \pi_2(i,j|z) \left( (1-\alpha)\, c_j^a - \pi_1(i,j) \left( (1-\alpha)\, c_j^a + c_i^a \right) \right),$$
$$= \sum_{\{i,j\}\in\mathbb{S}} \pi_2(i,j|b)\, \varphi_a(i,j|\pi_1),$$

where $\varphi_a(i,j|\pi_1) = (1-\alpha)\, c_j^a - \pi_1(i,j) \left( (1-\alpha)\, c_j^a + c_i^a \right) = \left( 1 - \pi_1(i,j) \right) (1-\alpha)\, c_j^a - \pi_1(i,j)\, c_i^a$ is the expected reward of the attacker in case she targets the node $j$ from $i$ and $\pi_2(i,j|b) = \sum_{\{i,j\}\in\mathbb{S}} \pi_2(i,j|z)\, b(z)$ has the same interpretation as above.

Furthermore, at each time slot, the main goal for every player is to optimize his payoff by considering the strategy his opponent has chosen. This means that each player aims to play the strategy that best responds to his opponent's strategy.

### 4.3 Players solution approach

• **Defender solution approach:** Suppose the attacker has a strategy denoted as $\pi_2 \in \Pi_2$. A strategy $\pi_1 \in \Pi_1$ employed by the defender is considered as the optimal response to $\pi_2$ if it maximizes the reward $\mathcal{R}_d(\pi|b) = \sum_{\{i,j\}\in\mathbb{S}} \pi_1(i,j)\, \varphi_d(i,j|b,\pi_2) - \sum_{\{i,j\}\in\mathbb{S}} \psi_d(i,j|b,\pi_2)$.

In addition, knowing the strategy $\pi_2$ allows us to determine the coefficients $\varphi_d(i,j|b,\pi_2)$ and $\psi_d(i,j|b,\pi_2)$ for all $\{i,j\} \in \mathbb{S}$. Once these coefficients are fixed, the maximum payoff for the defender can be obtained by maximizing $\sum_{\{i,j\}\in\mathbb{S}} \pi_1(i,j)\, \varphi_d(i,j|b,\pi_2)$. To achieve this maximum payoff, the defender should focus on the top $h$ edges of $\mathbb{S}_b$ according to their rank value $r(i,j|b,\pi_2) = 1 + |\{\{x,y\} \in \mathbb{S}_b : \varphi_d(x,y|b,\pi_2) > \varphi_d(i,j|b,\pi_2)\}|$, and set $\pi_1(i,j) = 0$ for the remaining edges. In other words, $\pi_1$ best responds to $\pi_2$ if $\pi_1(i,j) = 0$ whenever $r(i,j|b,\pi_2) > h$, i.e., if $\pi_1(i,j) = 0$ for all $\{i,j\}$ not in the set $\mathrm{SL}_d(\pi_2) = \{\{x,y\} \in \mathbb{S}_b : r(x,y|b,\pi_2) \leqslant h\}$ of the $h$ top-ranked edges of $\mathbb{S}_b$ according to $\varphi_d(\cdot|b,\pi_2)$. $\mathrm{SL}_d(\pi_2)$ is called *short list* of the defender, best responding to the attacker's strategy $\pi_2$. It is important for the defender to choose a pseudo probability distribution $\pi_1$ over $\mathbb{S}_b$ that is consistent with some probability distribution over $A_1$.

• **Attacker solution approach:** In the same way, an attacker's strategy $\pi_2 \in \Pi_2$ is considered as the best response to a defender's strategy $\pi_1 \in \Pi_1$ when the reward $\mathcal{R}_a(\pi|b) = \sum_{\{i,j\}\in\mathbb{S}} \pi_2(i,j|b)\, \varphi_a(i,j|\pi_1)$ is maximized. The maximum reward for a fixed defender's strategy $\pi_1$ and thus, fixed coefficients $\varphi_a(i,j|\pi_1)$ and $b(z)$ is achieved when $\pi_2(i,j|z) = 0$ in any possible state $z$ (i.e., $b(z) \neq 0$) where $\varphi_a(i,j|\pi_1)$ is not maximal. In other words, for all possible states $z \in Z$, $\pi_2(i,j|z) = 0$ if $\{i,j\} \notin \mathrm{SL}_a(\pi_1) = \{\{x,y\} \in \mathbb{S} : \forall \{u,v\} \in \mathbb{S}, \varphi_a(x,y|\pi_1) \geqslant \varphi_a(u,v|\pi_1)\}$, which is referred to as the *short list* of the attacker best responding to the defender's strategy $\pi_1$. This implies that at state $z$, the attacker may only transmit the virus from each infected node $i$ to a susceptible neighbor $j$ if $\varphi_a(i,j|\pi_1)$ is equal to the maximum possible value.

### 4.4 Nash equilibria properties

A strategy profile $\pi^* = (\pi_1^*, \pi_2^*)$ is a Nash equilibrium if and only if each player best responds to his/her opponent's strategy and no player can unilaterally change his strategy. The short lists of players associated with their best responses as defined above satisfy the following proposition:

**Proposition 1.** *Suppose that* $\mathrm{SL}_d(\pi_2^*) \neq \mathbb{S}$ *then, the shortlist of the defender is a subset of the short list of the attacker, i.e.,* $\mathrm{SL}_d(\pi_2^*) \subseteq \mathrm{SL}_a(\pi_1^*)$.

This means that the defender does not need to worry about the attacker's insignificant target in advance unless he wants to monitor all edges of the graph.

*Proof.* Suppose that $\mathrm{SL}_d(\pi_2^*) \neq \mathbb{S}$ and take any $\{i,j\} \notin \mathrm{SL}_a(\pi_1^*)$. Then, for all $z \in Z$, $\pi_2^*(i,j|z) = 0$ and $\varphi_d(i,j|b,\pi_2^*) = \sum_{z\in Z} b(z)\,\pi_2^*(i,j|z)\left(c_i^d + (1-\alpha)\,c_j^d\right) = 0$. In this case, $\{i,j\}$ is minimally ranked according to $\varphi_d(\cdot|b,\pi_2^*)$ because $\varphi_d(u,v|b,\pi_2^*) \geqslant 0$, $\forall\{u,v\} \in \mathbb{S}$. Since $\mathrm{SL}_d(\pi_2^*) \neq \mathbb{S}$, at least one edge $\{x,y\} \in \mathbb{S}$ is not $h$ top-ranked according to $\varphi_d(\cdot|b,\pi_2^*)$.

As $\varphi_d(x,y|b,\pi_2^*) \geqslant 0 = \varphi_d(i,j|b,\pi_2^*)$, we conclude that $\{i,j\}$ is not h top-ranked according to $\varphi_d$ i.e., $\{i,j\} \notin \mathrm{SL}_d(\pi_2^*)$. ∎

The previous inclusion relation between the short lists (proposition 1) leads us to the following proposition, which shows that our game is actually a game of thresholds.

**Proposition 2.** *1. For all* $\{k,l\} \in \mathrm{SL}_a(\pi_1^*)\backslash\mathrm{SL}_d(\pi_2^*)$, $\{i,j\} \in \mathrm{SL}_d(\pi_2^*)$, *and* $\{u,v\} \in \mathbb{S}\backslash\mathrm{SL}_a(\pi_1^*)$, *it holds:* $\begin{cases} c_j^a \geqslant c_l^a > c_v^a \\ c_j^a > c_l^a \iff \pi_1^*\{i,j\} > 0 \end{cases}$.

*2. For all couples* $\{k,l\},\{k',l'\} \in \mathrm{SL}_a(\pi_1^*) \setminus \mathrm{SL}_d(\pi_2^*)$, *it holds:* $c_l^a = c_{l'}^a$.

This implies that, at Nash equilibrium,

- The objective of the defender is to safeguard nodes with centrality values that exceed a specific threshold $\theta_1$. Similarly, the attacker's goal is to target nodes with centrality values not lower than another threshold $\theta_2$. Moreover, the specific values of *these thresholds are determined based on the centrality measure employed by the attacker.*

- From the attacker's perspective, all the nodes that the defender should leave unprotected have the same centrality values.
  However, note that this proposition does not state that $\mathrm{SL}_2(\pi_1^*) \setminus \mathrm{SL}_1(\pi_2^*)$ is a non-empty set.

*Proof.* From $\{k,l\} \notin \mathrm{SL}_d(\pi_2^*)$, it comes $\pi_1^*(k,l) = 0$. From $\{k,l\} \in \mathrm{SL}_a(\pi_1^*)$, it comes that $\varphi_a(k,l|\pi_1^*) = (1-\alpha)\,c_l^a$ is maximal. This point leads to the second statement of the proposition 2 because, taking $\{k',l'\} \in \mathrm{SL}_a(\pi_1^*) \setminus \mathrm{SL}_d(\pi_2^*)$, implies $\varphi_a(k',l'|\pi_1^*) = (1-\alpha)\,c_{l'}^a$ is maximal too, and then, $(1-\alpha)\,c_{l'}^a = (1-\alpha)\,c_l^a$, i.e., $c_l^a = c_{l'}^a$.

Note that $\{u,v\} \notin \mathrm{SL}_a(\pi_1^*)$, and from proposition 1, $\{u,v\} \notin \mathrm{SL}_d(\pi_2^*)$ so, $\pi_1^*(u,v) = 0$. In this case, $\varphi_a(u,v|\pi_1^*) = (1-\alpha)\,c_v^a$ and, since $\varphi_a(k,l|\pi_1^*) = (1-\alpha)\,c_l^a$ is maximal, it comes $(1-\alpha)\,c_l^a > (1-\alpha)\,c_v^a$ and, consequently, $c_l^a > c_v^a$.

In addition, the maximality of $\varphi_a(k,l|\pi_1^*)$ also applies to $\{i,j\}$ and, therefore $(1-\alpha)\,c_j^a - \pi_1^*(i,j)\left(c_i^a + (1-\alpha)\,c_j^a\right) = (1-\alpha)\,c_l^a$. Then, $\pi_1^*(i,j)\left(c_i^a + (1-\alpha)\,c_j^a\right) = (1-\alpha)\left(c_j^a - c_l^a\right)$. The positivity of $c_j^a - c_l^a$ relies on that of $c_i^a + (1-\alpha)\,c_j^a$, thus $c_j^a \geqslant c_l^a$. ∎

Since we have demonstrated that players act in accordance with centrality thresholds, it is evident that these thresholds have a direct impact on players' optimal responses. The proposition 3 provides a more specific characterization of shortlists $\mathrm{SL}_d(\pi_2^*)$ and $\mathrm{SL}_a(\pi_1^*)$ by taking into account these centrality thresholds.

**Proposition 3.** *For some centrality values $\theta_1$ and $\theta_2$, it holds:*

1. $\mathrm{SL}_d(\pi_2^*) = \{\{i,j\} \in \mathbb{S}_b : c_j^a \geqslant \theta_1\}$; $\quad \mathrm{SL}_a(\pi_1^*) = \{\{i,j\} \in \mathbb{S} : c_j^a \geqslant \theta_2\}$;
2. $\begin{cases} \text{For some } \{i,j\} \in \mathrm{SL}_d(\pi_2^*), \text{ it holds } c_j^a = \theta_1 \text{ and } \pi_1^*(i,j) \neq 0, \\ \text{For some } \{k,l\} \in \mathrm{SL}_a(\pi_1^*), \text{ it holds } c_l^a = \theta_2 \text{ and } \pi_2^*(k,l|b) \neq 0; \end{cases}$
3. $\theta_2 \leqslant \theta_1$. *In particular, if $\theta_2 < \theta_1$, then no centrality value can lie in the space $]\theta_2, \theta_1[$.*

*Proof.* Consider $\theta_k = \min_{\{\text{source,target}\} \in \mathrm{SL}_p\left(\pi_{-k}^*\right)} c_{\text{target}}^a$, for $(k,p) \in \{(1,d),(2,a)\}$.

By this definition, $c_j^a \geqslant \theta_k$ for any $\{i,j\} \in \mathrm{SL}_p\left(\pi_{-k}^*\right)$. Conversely, on the one hand, take any $\{k,l\} \in \mathbb{S}$ such that $c_l^a \geqslant \theta_2$. The minimum value $\theta_2$ is attained for some $\{k',l'\} \in \mathrm{SL}_a(\pi_1^*)$. Then, from the inequality $c_l^a \geqslant c_{l'}^a$ and proposition 2.1, it comes $\{k,l\} \in \mathrm{SL}_a(\pi_1^*)$ (indeed, suppose $\{k,l\} \in \mathbb{S} \setminus \mathrm{SL}_a(\pi_1^*)$, we have, $c_l^a < c_{l'}^a$). Similarly, take any $\{i,j\} \in \mathbb{S}$ such that $c_j^a \geqslant \theta_1$. With the same reasoning, we get $\{i,j\} \in \mathrm{SL}_d(\pi_2^*)$. Point 1 is proven.

For the proof of point 2, since $\theta_k = \min_{\{\text{source,target}\} \in \mathrm{SL}_p\left(\pi_{-k}^*\right)} c_{\text{target}}^a$, for $(k,p) \in \{(1,d),(2,a)\}$, they are attained for some $\{i,j\} \in \mathrm{SL}_d(\pi_2^*)$ and $\{k,l\} \in \mathrm{SL}_a(\pi_1^*)$ respectively.

Since $\mathrm{SL}_d(\pi_2^*) \subseteq \mathrm{SL}_a(\pi_1^*)$ and the definition of $\theta_k$, $k = 1,2$, we have $\theta_2 \leqslant \theta_1$ (and more specifically $\theta_2 < \theta_1$ iff $\mathrm{SL}_d(\pi_2^*) \subset \mathrm{SL}_a(\pi_1^*)$). Moreover, let's assume that there is $\{u,v\} \in \mathrm{SL}_a(\pi_1^*)$ and $\{i,j\} \in \mathbb{S}$ such that $\theta_2 = c_v^a$ and $c_j^a \in ]\theta_2, \theta_1[$. In this case, $\{i,j\}, \{u,v\} \in \mathrm{SL}_a(\pi_1^*) \setminus \mathrm{SL}_d(\pi_2^*)$; by proposition 2.2 $c_j^a = \theta_2$, which is absurd. Point 3 is proven. ∎

Once a factual definition of short lists of players is provided, it becomes apparent that they are determined by *centrality thresholds that are established based solely on the centrality measure of the attacker*. The following section aims to elucidate the mathematical properties that determine these thresholds and emphasize the associated optimal strategy for each player.

## 5 Nash equilibria analysis

It is assumed that the players are playing a strategy profile $\pi^* = (\pi_1^*, \pi_2^*)$ that is a Nash equilibrium. Additionally, the defender holds a belief $b$ about the network state. This means that the set of possible strategies that each player can choose from, denoted by $\mathrm{supp}(\pi_k^*)$, are contained within their respective short lists, denoted by $\mathrm{SL_p}\left(\pi_{-\mathrm{k}}^*\right)$, $(k,p) \in \{(1,d),(2,a)\}$, which are determined by their individual thresholds $\theta_k$. In this section, based on the definition of the attacker's shortlist $\mathrm{SL_a}(\pi_1^*)$, we denote by $s$ the maximum value of $\varphi_a$ under the Nash equilibrium, i.e., $s = \max_{\{i,j\} \in \mathbb{S}} \varphi_a(i,j|\pi_1^*)$.

**Proposition 4.** *1. The probability of the defender placing an IPS on any edge $\{i,j\} \in \mathbb{S}_b$ is expressed as:*

$$\begin{cases} \{i,j\} \in \mathrm{SL_a}(\pi_1^*) \iff \varphi_a(i,j|\pi_1^*) = s \text{ and } \pi_1^*(i,j) = \dfrac{(1-\alpha)\, c_j^a - s}{c_i^a + (1-\alpha)\, c_j^a} \\ \{i,j\} \notin \mathrm{SL_a}(\pi_1^*) \Longrightarrow \varphi_a(i,j|\pi_1^*) < s \text{ and } \pi_1^*(i,j) = 0 \end{cases}.$$

2. *Mathematically speaking, the total probability of protection for every edge in $\mathbb{S}_b$ is equal to the number of IPSs that the defender has. This is represented by the equation:* $\sum_{\substack{\{i,j\}\in\mathbb{S}_b \\ c_j^a \geqslant \theta_1}} \pi_1^*(i,j) = h.$
3. *The highest value $s$ that the attacker tries to achieve when making her decision is expressed as:*

$$s = (1-\alpha)\frac{\left(\sum_{\substack{\{i,j\}\in\mathbb{S}_b \\ c_j^a \geqslant \theta_1}} \frac{c_j^a}{c_i^a + (1-\alpha)\, c_j^a}\right) - \frac{h}{1-\alpha}}{\sum_{\substack{\{i,j\}\in\mathbb{S}_b \\ c_j^a \geqslant \theta_1}} \frac{1}{c_i^a + (1-\alpha)\, c_j^a}}.$$

*Proof.* 1. The comparison of $\varphi_a(i,j|\pi_1^*)$ and $s$ is according to the definition of the attacker's shortlist $\mathrm{SL_a}(\pi_1^*)$. On the one hand, if $\{i,j\} \in \mathrm{SL_a}(\pi_1^*)$ then,
$s = (1-\alpha)\, c_j^a - \pi_1^*(i,j)\left(c_i^a + (1-\alpha)\, c_j^a\right) \iff \pi_1^*(i,j) = \frac{(1-\alpha)c_j^a - s}{c_i^a + (1-\alpha)c_j^a}$.
On the other hand, if $\{i,j\} \notin \mathrm{SL_a}(\pi_1^*)$ then, $\{i,j\} \notin \mathrm{SL_d}(\pi_2^*)$; the assertion 1 is proven.

2. A defender's action is to select $h$ edges to protect from his short list $\mathrm{SL_d}(\pi_2^*)$. It is important to remember that for every edge $\{i,j\}$ in the selected list, the value of $\pi_1^*(i,j)$ is equal to the sum of the values of $\pi_1^*(W)$ for all $W \in A_1$ such that $\{i,j\}$ belongs to $W$, i.e. $\pi_1^*(i,j) = \sum_{\substack{W\in A_1 \\ \{i,j\}\in W}} \pi_1^*(W)$.
Then, $\sum_{\substack{\{i,j\}\in\mathbb{S}_b \\ c_j^a \geqslant \theta_1}} \pi_1^*(i,j) = \sum_{\substack{\{i,j\}\in\mathbb{S}_b \\ c_j^a \geqslant \theta_1}} \sum_{\substack{W\in A_1 \\ \{i,j\}\in W}} \pi_1^*(W) = h \sum_{W\in A_1} \pi_1^*(W) = h.$
In fact, since an action consists of $h$ elements, it will be repeated $h$ times in the sum. This leads us to the conclusion shown in assertion 2, which is based on the fact that $\pi_1^*$ represents a probability distribution over the defender's actions set $A_1$.
3. The assertion 3 comes from assertion 2 and the first point of assertion 1.

■

Based on proposition 3, the recommended course of action for the defender in response to the attacker's strategy involves the prior construction of the defender's short list. This process entails the careful selection of the suitable centrality measure to assess the impact of the network nodes. As a result, the defender's optimal strategy can be summarized in two key stages: the selection of the centrality measure and the subsequent computation of the corresponding $\pi_1^*$ optimal strategy.

**Proposition 5.** *At Nash equilibrium, the defender must use the attacker's centrality measure to assess the significance of nodes in the graph. This implies that the defender's decisions are based on the same centrality measure as that of the attacker.*

*Proof.* The defender's best response, represented by the set $\mathrm{SL_d}(\pi_2^*)$ is determined by a centrality threshold based on the attacker's centrality measure (first point of proposition (3)). Moreover, the defender's optimal strategy $\pi_1^*$ on $\mathrm{SL_d}(\pi_2^*)$ is still influenced by the attacker's centrality measure (first assertion of proposition (1)). To put it simply, if the defender wants to play optimally, he needs to take into account the attacker's centrality measure when making decisions. ■

The following proposition allows us to determine at each time $t$, if a given $(\theta_1, \theta_2)$ is a Nash equilibrium:

**Proposition 6.** *1. a) At Nash equilibrium, we have* $\sum_{\substack{\{i,j\}\in\mathbb{S}_b \\ c_j^a \geqslant \theta_1}} \frac{c_j^a - \theta_1}{c_i^a + (1-\alpha)\, c_j^a} \leqslant \frac{h}{1-\alpha}$.

*b) If in particular* $\theta_1 > \theta_2$, *then* $\sum_{\substack{\{i,j\}\in\mathbb{S}_b \\ c_j^a \geqslant \theta_1}} \frac{c_j^a - \theta_2}{c_i^a + (1-\alpha)\, c_j^a} = \sum_{\substack{\{i,j\}\in\mathbb{S}_b \\ c_j^a \geqslant \theta_2}} \frac{c_j^a - \theta_2}{c_i^a + (1-\alpha)\, c_j^a} = \frac{h}{1-\alpha}$.

*2. Assuming that the set* $\mathrm{Last}_h \subseteq \left\{\{i,j\} \in \mathbb{S}_b : c_j^a \geqslant \theta_1\right\}$ *contains the h last-ranked elements of* $\mathbb{S}_b$ *based on their* $\pi_1^*(i,j)$ *values, it follows* $\sum_{\{i,j\}\in \mathrm{Last}_h} \pi_1^*(i,j) \geqslant \frac{h\,(h-1)}{|\mathbb{S}_b| - 1}$.

*3. a) If* $s \leqslant 0$ *then* $\theta_1 = \min_{\{i,j\}\in\mathbb{S}_b} c_j^a$.

*b) If* $s > 0$ *then the attacker infects a susceptible node j if and only if that is for some infected node i, it holds* $\varphi_2(i,j|\pi_1) = s$.

*Proof.* The positivity of $\pi_1^*(i,j)$ for all $\{i,j\}$ in the defender's shortlist implies $(1-\alpha)\, c_j^a \geqslant s$ then $(1-\alpha)\,\theta_1 \geqslant s$ . Moreover,

$$(1-\alpha)\,\theta_1 \geqslant s \iff \theta_1 \geqslant \frac{\left(\sum_{\substack{\{i,j\}\in\mathbb{S}_b \\ c_j^a \geqslant \theta_1}} \frac{c_j^a}{c_i^a + (1-\alpha)\, c_j^a}\right) - \frac{h}{1-\alpha}}{\sum_{\substack{\{i,j\}\in\mathbb{S}_b \\ c_j^a \geqslant \theta_1}} \frac{1}{c_i^a + (1-\alpha)\, c_j^a}} \iff \sum_{\substack{\{i,j\}\in\mathbb{S}_b \\ c_j^a \geqslant \theta_1}} \frac{c_j^a - \theta_1}{c_i^a + (1-\alpha)\, c_j^a} \leqslant \frac{h}{1-\alpha}.$$

In case $\theta_1 > \theta_2$, there exist $\{i,j\} \in \mathrm{SL}_a(\pi_1^*) \setminus \mathrm{SL}_d(\pi_2^*)$, such that $c_j^a = \theta_2$ and then,
$\pi_1^*(i,j) = \frac{(1-\alpha)\, c_j^a - s}{c_i^a + (1-\alpha)\, c_j^a} = \frac{(1-\alpha)\,\theta_2 - s}{c_i^a + (1-\alpha)\,\theta_2} = 0$. So, we get

$$s = (1-\alpha)\,\theta_2 \iff \frac{\left(\sum_{\substack{\{i,j\}\in\mathbb{S}_b \\ c_j^a \geqslant \theta_1}} \frac{c_j^a}{c_i^a + (1-\alpha)\, c_j^a}\right) - \frac{h}{1-\alpha}}{\sum_{\substack{\{i,j\}\in\mathbb{S}_b \\ c_j^a \geqslant \theta_1}} \frac{1}{c_i^a + (1-\alpha)\, c_j^a}} = \theta_2 \iff \sum_{\substack{\{i,j\}\in\mathbb{S}_b \\ c_j^a \geqslant \theta_2}} \frac{c_j^a - \theta_2}{c_i^a + (1-\alpha)\, c_j^a} = \frac{h}{1-\alpha}.$$

Thus, $(1-\alpha)\, c_j^a \geqslant s$ in the general case, and $s = (1-\alpha)\,\theta_2$ in case $\theta_1 > \theta_2$. The assertion 1 is thus proven.

Assertion 2 is a condition that comes from [27], where the authors give the condition to pass from the probability on elements to the probability on the associated sets of size h.
For the proof of 3, suppose $s \leqslant 0$. That is, for any $\{i,j\} \in \mathbb{S}_b$, we get successively:

$$\varphi_a(i,j|\pi_1) \leqslant 0, \iff (1-\alpha)\, c_j^a - \pi_1^*(i,j)(c_i^a + (1-\alpha)\, c_j^a) \leqslant 0,$$

$$\iff \pi_1^*(i,j) \geqslant \frac{(1-\alpha)\, c_j^a}{c_i^a + (1-\alpha)\, c_j^a} > 0, \forall \{i,j\} \in \mathbb{S}_b,$$
$$\iff c_j^a \geqslant \theta_1 \; for \; all \{i,j\} \in \mathbb{S}_b \iff \theta_1 = \min_{\{i,j\} \in \mathbb{S}_b} c_j^a.$$

Suppose on the other hand that $s > 0$. From the definition of the attacker's shortlist, it comes: $\mathcal{R}(\pi^*|b) = \sum_{\substack{\{i,j\} \in \mathbb{S} \\ \varphi_a(i,j|\pi_1^*) \text{ is maximal}}} \pi_2^*(i,j|b)\, \varphi_a(i,j|\pi_1^*) = s \sum_{\substack{\{i,j\} \in \mathbb{S} \\ \varphi_a(i,j|\pi_1^*) = s}} \pi_2^*(i,j|b)$. The maximization of this result imposes the maximization of the $\pi_2^*(i,j|b)$'s value whenever $\varphi_a(i,j|\pi_1^*)$ is maximal. ■

## 6 Numerical illustrations

Communication and information exchange are integral to modern society and, as such, networks have become essential infrastructure. Therefore, protecting these networks against the spread of malicious software is of utmost importance. As we have previously demonstrated, one effective strategy for epidemic propagation in networks is to target the most central devices above a certain centrality threshold. In this section, we present a simulation of the impact of our centrality game on epidemic dynamics, focusing on the scenario of complete information, where the defender has perfect knowledge about the network state. In our experiments, we employ some popular centrality measures described in [3]: degree centrality **(D)**, betweenness centrality **(B)**, eigenvector centrality **(E)**, clustering coefficient centrality **(Clus)**, and closeness centrality **(Clo)**. However, our model is flexible enough to incorporate alternative centrality measures if desired. The simulation has several realizations and a realization ends once all the nodes in the graph have become resistant. Some parameters employed for these simulations are as follows: $\alpha = 0.1$, $\varrho = 0.2$, and 10 IPSs for the defender. The program presents the results of the subsequent metrics upon completion of each realization:

- The epidemic peak (EP), the maximum number of infected nodes reached in the network during a given period;
- The time this peak is attained (TP), i.e., the number of periods it took to reach this peak;
- The time for the control of the epidemic (TC), i.e., the first period at which the number of edges in the stake is not greater than the number of IPSs. From that period onward, the defender prevents any infection;
- The time for the virus extinction (TE), i.e., the period after which there are no more infected nodes in the network.

The objectives of this section can be summarized into two main goals. The first goal is to show how different centrality measures affect the optimal strategies of the players, as previously defined, and identify the most effective centrality measure for the attacker. The second objective consists of the evaluation of the defender's loss if he does not adopt the recommended optimal strategy. To closely mimic real-world scenarios, we conducted our experiments on two prominent network types that have experienced epidemic spread in recent years. The mathematical graph model chosen for the mathematical modeling of each of them was selected on the basis of the main characteristics of the networks developed in [14].

- *Power network (Ukraine power grid hack, December 2015)*: From a physical concept, it is reasonable to conceptualize the power system as a *small-world network* (East China Power Grid [4]). From the perspective of the system comprising networks of varying voltage levels, the power supply and distribution networks at the middle and low voltage levels within cities are strongly interconnected, whereas the transmission networks at higher voltage levels are sparsely connected. From the point of view of the transmission network of the same voltage stage, the network of each region is closely connected, while the network of different regions is sparsely connected. This observation suggests that the power system exhibits the characteristics of a small-world network, characterized by significant local clustering and limited global interconnection [6].
- *Social network (the spread of false information regarding COVID-19 vaccines on social media platforms [18]):* An example is the social network $Twitter$. We have used the *Barabási-Albert* model for its mathematical representation, because of its ability to capture some key features of the latter. The Barabási-Albert model is a preferential growth model that is based on two fundamental principles: continuous network growth (which reflects the fact that social networks are constantly expanding) and preferential attachment (which refers to the fact that new vertices tend to connect to existing vertices that already have many links).

### 6.1 Optimal strategic defense (*OSD*) against optimal strategic attack (*OSA*): best centrality measure for the attacker

We assume that players adopt their optimal strategies as defined above. Since there are several ways to measure the centrality value of a node, the question that arises is therefore as follows: which centrality measure should the attacker use to maximize her payoff (i.e., to maximize the number of infected nodes of the graph)? We therefore study the effectiveness of various centrality measures in identifying critical nodes to attack in the context of epidemic spread. To accomplish this task, we generated:

- a Watts-Strogatz graph with the following characteristics: number of nodes = 1000; degree of each node in the initial graph = 20; probability of modifying each edge = 0.1. Obtaining a graph containing 10000 edges;
- a Barabási-Albert graph with the following characteristics: number of nodes = 1000; number of connection for each node = 15. This results in a graph containing 14775 edges.

Considering that each graph contains 7 infected nodes at the beginning of the game, we performed for each one a simulation containing 100 realizations for every centrality measure mentioned above. We then obtained the following results:

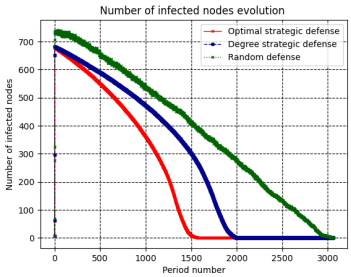
- *Watts-Strogatz graph:* According to the table (2a) given our Watts-Strogatz graph model, *closeness centrality* appears as the best centrality measure for the attacker to infect a maximum number of nodes. Indeed, nodes with high closeness centrality are geographically close to many other nodes in terms of the shortest path length. In the given Watts-Strogatz graph model, the graph structure combines local clustering and short average path lengths. This is achieved through the initial ring structure and the subsequent random rewiring process [14]. As a result, many nodes in the network are relatively close to each other, both in terms of clustering and path lengths. Nodes with higher closeness centrality are likely to be positioned in densely connected areas of the graph, making them potential hubs for spreading the infection.

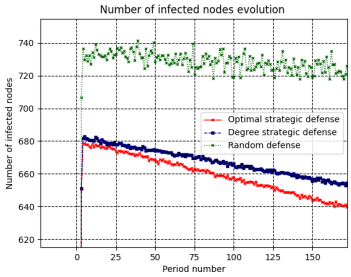
| Watts-Strogatz graph | | | | |
|---|---|---|---|---|
| Metrics/ Measures | EP | TP | TC | TE |
| D | 675.59 | 6 | 1154 | 1359 |
| Clus | 676.23 | 6 | 995 | 1249 |
| B | 533.65 | 9 | 358 | 468 |
| E | 675.35 | 5 | 1041 | 1392 |
| Clo | 678.5 | 8 | 1354 | 1682 |

(a) Average results for optimal strategic defense against optimal strategic attack (both players use the same centrality measure). ***closeness centrality*** *proves ideal for the attacker. The proximity of the epidemic peak for some centrality measures can be attributed to the regular distribution of nodes and the low probability of edge modification, resulting in nodes with almost similar structural properties. Betweenness and closeness differ by* 14.48% *increase at peak.*

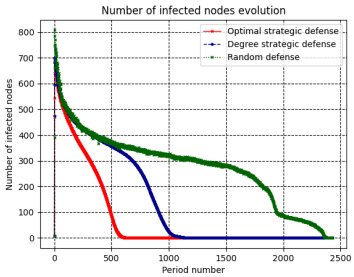
| Barabási-Albert graph | | | | |
|---|---|---|---|---|
| Metrics/ Measures | EP | TP | TC | TE |
| D | 180.04 | 2 | 145 | 266 |
| Clus | 693.93 | 5 | 542 | 692 |
| B | 62.86 | 3 | 92 | 171 |
| E | 196.15 | 2 | 185 | 242 |
| Clo | 561.68 | 9 | 750 | 1067 |

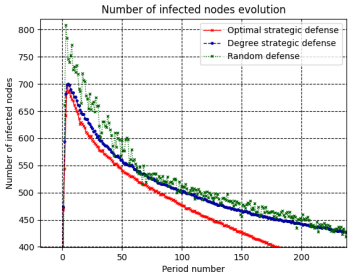
(b) Average results for optimal strategic defense against optimal strategic attack (both players use the same centrality measure). *Since the attacker aims to maximize the number of infected nodes, she will select the* ***clustering coefficient centrality*** *as the metric. The impact of the centrality measure on the expected result is also visible. For example, between closeness centrality and clustering coefficient centrality, there is an increase of* $13,2\%$ *at the epidemic peak.*




(c) Infected nodes variation for the *Watts-Strogatz* graph (with a zoomed-in view highlighting the peaks during the epidemic propagation). *The results show that when the defender deviates from the recommended optimal strategy, the attacker achieves a higher success rate in infecting nodes and a longer time of extinction. Specifically, when the defender employs the DSD strategy, the peak rises to* 682.65*, signifying a noticeable increase of* 0.4%*. Despite the small difference in peak values, this strategy progressively becomes more dangerous for the defender over time. It leads to a greater number of infected nodes and prolongs the time until extinction, taking approximately* 2048 *periods compared to* 1682 *for OSD. For example, at period* 1500*, there is a significant* 28% *surge in infected nodes. In contrast, opting for the RD strategy results in a* 7% *rise at the epidemic peak.*




(d) Infected nodes variation for the *Barabási-Albert* graph (with a zoomed-in view highlighting the peaks during the epidemic). *As announced in the theoretical demonstrations, when the defender does not follow the recommended optimal strategy, the epidemic peak becomes higher. Specifically, when the defender employs the DSD strategy, the peak rises to 700.5, representing a small increase of* 0.6%*. Although the difference between these peaks is small, this strategy becomes increasingly perilous for the defender over time. It results in a higher number of infected nodes and a longer time for the epidemic extinction, taking around* 1216 *periods compared to* 692 *for OSD. For instance, at period number* 500*, there is a significant* 30% *surge in infected nodes. On the other hand, if the RD strategy is chosen, there is a notable* 11% *increase observed at the time of the epidemic's peak.*

- *Barabási-Albert graph:* The *clustering coefficient centrality* is identified as the most effective centrality measure for propagating malware, as shown in table (2b). The Barabási-Albert graph model is a preferential attachment model, where new nodes are more likely to connect to already well-connected nodes. As a result, this model tends to create a scale-free network structure with a few highly connected hub nodes and many low-degree nodes. In a scale-free network, the clustering coefficient tends to be relatively low for most nodes but significantly higher for a few hub nodes. These hub nodes act as highly interconnected clusters, forming the backbone of the network. By targeting nodes with high clustering coefficient centrality, an attacker can exploit these densely connected clusters to infect a maximum number of nodes efficiently.

### 6.2 Sub-optimal defense against optimal strategic attack

We have demonstrated that the defender's optimal strategy requires the adoption of the same centrality measure as the attacker (in our previous simulations, *closeness centrality* for the Watts-Strogatz model and *clustering coefficient centrality* for the Barabási-Albert model). However, in some cases, implementing this strategy in practice can incur high costs (e.g., the time complexity of implementing the attacker's centrality measure). Additionally, the defender may face limitations in terms of resources or sophistication. Therefore, we employed two main strategies as alternatives to the recommended optimal approach:

- The first strategy (*Degree Strategic Defense "DSD"*) involves the defender using the degree centrality (chosen for its computational simplicity) to assess the significance of the graph's nodes. Subsequently, we determined the defender's optimal probability distribution associated with this centrality measure (assuming that the attacker also employs degree centrality).
- The second strategy (*Random Defense "RD"*) is a purely random approach, wherein the defender selects nodes to protect based on a uniform probability distribution. This strategy does not consider any centrality measure.

In order to evaluate the correlation in terms of the *maximum number of infected nodes* between these strategies and the optimal one, we have compared each of the defender's strategies with the attacker's optimal strategy. It is worth mentioning that these experiments were conducted on the same graphs used earlier. Unsurprisingly, the results depicted in figures 2c and 2d clearly demonstrate that regardless of whether it is a *Watts-Strogatz* or *Barabási-Albert* graph, following the recommended *optimal strategy* benefits the defender. Moreover, in our context where the attacker aims to maximize the number of infected nodes, employing the *random defense* strategy is strongly discouraged. However, the following observation applies to both the Watts-Strogatz and Barabási-Albert models:

- The defender's *optimal strategy* (OSD), based on clustering coefficient centrality for the *Barabási-Albert* graph and closeness centrality for the *Watts-Strogatz* graph, is initially close to the *degree strategic defense* strategy. Indeed, at the beginning of the game, nodes with a high degree tend to have a high clustering coefficient and high closeness centrality, which aligns with the optimal strategy. However, as time progresses, the DSD strategy primarily focuses on nodes with a high degree which may have a lower clustering coefficient on the one hand and a lower closeness centrality on the other hand. As a result, the two strategies diverge as the infection progresses.

Additionally, in our *Barabási-Albert* graph, it is important to highlight that the betweenness centrality measure is not suitable for the attacker, who obtains *eleven times as many infected nodes* by using the clustering coefficient. This observation can be explained by the fact that:

- Betweenness centrality measures the frequency with which a node lies on the shortest path between two other nodes in a graph. However, in a *Barabási-Albert* graph characterized by preferential connections and high clustering, this measure fails to capture a node's capacity to propagate an epidemic effectively. Nodes possessing high betweenness centrality may not exhibit extensive connectivity or reside within dense clusters, thus limiting their potential for spreading malware.

## 7 Conclusion

The notorious *WannaCry Ransomware attack* that occurred in 2017 was one of the worst attacks that ever had before. WannaCry Ransomware is a type of malicious software that blocks user access to files or systems, holding files or entire devices' hostage using encryption until the victim pays a ransom in exchange for a decryption key, which allows the user to access the files or systems encrypted by the program [13]. Like the latter, many attacks with the same objectives are perpetrated daily. Using their intelligence and rationality, and due to limited resources, many attackers choose the devices to infect based on their influence in the network, which they determine through various centrality measures. [23] addressed and found a solution to the problem when the defender and the attacker use identical centrality measures. This paper generalized the problem by addressing situations where players opt for different centrality measures. We have demonstrated that in a two-player asymmetric network centrality game, where each player takes action according to its centrality measure, the defender, to play optimally, must use the attacker's centrality measure. Based on the simulations conducted in this study, it has been observed that the appropriate centrality measure for the attacker to infect the maximum number of nodes depends on the type of graph. In particular, we have shown that in certain types of graphs, the clustering coefficient centrality is the most effective for the attacker, while in others, the closeness centrality is more appropriate. Our findings have important implications for the epidemic control problem, as they suggest that the choice of centrality measure can significantly impact the effectiveness of control measures. In particular, our results can inform the development of targeted intervention strategies aimed at reducing the spread of infectious diseases. The objective for us is to use these notions of centrality game to solve problems of the *lateral movement* type [7].

## Acknowledgments

The research was sponsored by the U.S. Army Research Office and was accomplished under Cooperative Agreement Numbers W911NF-19-2-0150, W911NF-22-2-0175, and Grant Number W911NF-21-1-0326. The views and conclusions contained in this document are those of the authors and should not be interpreted as representing the official policies, either expressed or implied, of the U.S. Army Research Laboratory or the U.S. Government. The U.S. Government is authorized to reproduce and distribute reprints for Government purposes notwithstanding any copyright notation herein.

## References

1. Anwar, A.H., Kamhoua, C.A., Leslie, N.O., Kiekintveld, C.: Honeypot allocation for cyber deception under uncertainty. IEEE Transactions on Network and Service Management **19**(3), 3438–3452 (2022)
2. Das, K., Samanta, S., Pal, M.: Study on centrality measures in social networks: a survey. Social network analysis and mining **8**, 1–11 (2018)

3. Dey, P., Bhattacharya, S., Roy, S.: A survey on the role of centrality as seed nodes for information propagation in large scale network. ACM/IMS Transactions on Data Science **2**(3), 1–25 (2021)
4. Ding, M., Han, P.: Reliability assessment to large-scale power grid based on small-world topological model. In: 2006 International conference on power system technology. pp. 1–5. IEEE (2006)
5. Do, C.T., Tran, N.H., Hong, C., Kamhoua, C.A., Kwiat, K.A., Blasch, E., Ren, S., Pissinou, N., Iyengar, S.S.: Game theory for cyber security and privacy. ACM Computing Surveys (CSUR) **50**(2), 1–37 (2017)
6. Dong, C., Xiong, X., Xue, Q., Zhang, Z., Niu, K., Zhang, P.: A survey on the network models applied in the industrial network optimization. arXiv preprint arXiv:2209.08294 (2022)
7. Fang, Y., Wang, C., Fang, Z., Huang, C.: Lmtracker: Lateral movement path detection based on heterogeneous graph embedding. Neurocomputing **474**, 37–47 (2022)
8. Funk, S., Salathé, M., Jansen, V.A.: Modelling the influence of human behaviour on the spread of infectious diseases: a review. Journal of the Royal Society Interface **7**(50), 1247–1256 (2010)
9. Hayel, Y., Trajanovski, S., Altman, E., Wang, H., Van Mieghem, P.: Complete game-theoretic characterization of sis epidemics protection strategies. In: 53rd IEEE Conference on Decision and Control. pp. 1179–1184. IEEE (2014)
10. Horák, K., Bošanskỳ, B., Pěchouček, M.: Heuristic search value iteration for one-sided partially observable stochastic games. In: Proceedings of the AAAI Conference on Artificial Intelligence. vol. 31 (2017)
11. Hough, P.: Understanding global security. Routledge (2013)
12. Kolias, C., Kambourakis, G., Stavrou, A., Voas, J.: Ddos in the iot: Mirai and other botnets. Computer **50**(7), 80–84 (2017)
13. Mohurle, S., Patil, M.: A brief study of wannacry threat: Ransomware attack 2017. International Journal of Advanced Research in Computer Science **8**(5), 1938–1940 (2017)
14. Newman, M.E.: The structure and function of complex networks. SIAM review **45**(2), 167–256 (2003)
15. Oldham, S., Fulcher, B., Parkes, L., Arnatkevičiūtė, A., Suo, C., Fornito, A.: Consistency and differences between centrality measures across distinct classes of networks. PloS one **14**(7), e0220061 (2019)
16. Poghosyan, M., Baronchelli, A.: Epidemic spreading on complex networks. Ph.D. thesis (04 2017)
17. Rowe, N.C., Rrushi, J., et al.: Introduction to cyberdeception. Springer (2016)
18. Skafle, I., Nordahl-Hansen, A., Quintana, D.S., Wynn, R., Gabarron, E.: Misinformation about covid-19 vaccines on social media: rapid review. Journal of medical Internet research **24**(8), e37367 (2022)
19. Trajanovski, S., Hayel, Y., Altman, E., Wang, H., Van Mieghem, P.: Decentralized protection strategies against sis epidemics in networks. IEEE Transactions on Control of Network Systems **2**(4), 406–419 (2015)
20. Trajanovski, S., Kuipers, F.A., Hayel, Y., Altman, E., Van Mieghem, P.: Designing virus-resistant, high-performance networks: a game-formation approach. IEEE Transactions on Control of Network Systems **5**(4), 1682–1692 (2017)
21. Tsemogne, O., Hayel, Y., Kamhoua, C., Deugoue, G.: Partially observable stochastic games for cyber deception against network epidemic. In: 11th International Conference GameSec (2020)
22. Tsemogne, O., Hayel, Y., Kamhoua, C., Deugoué, G.: Game theoretic modeling of cyber deception against epidemic botnets in internet of things. IEEE Internet of Things Journal (2021)
23. Tsemogne, O., Kouam, W., Anwar, A.H., Hayel, Y., Kamhoua, C., Deugoué, G.: A network centrality game for epidemic control. In: Decision and Game Theory for Security: 13th International Conference, GameSec 2022
24. Tushir, B., Sehgal, H., Nair, R., Dezfouli, B., Liu, Y.: The impact of dos attacks on resource-constrained iot devices: A study on the mirai attack. arXiv preprint arXiv:2104.09041 (2021)
25. Xiao, K., Zhu, C., Xie, J., Zhou, Y., Zhu, X., Zhang, W.: Dynamic defense against stealth malware propagation in cyber-physical systems: a game-theoretical framework. Entropy **22**(8), 894 (2020)
26. Yu, S., Gu, G., Barnawi, A., Guo, S., Stojmenovic, I.: Malware propagation in large-scale networks. IEEE Transactions on Knowledge and Data Engineering **27**(1), 170–179 (2014)
27. Zaman, A., Marsaglia, G.: Random selection of subsets with specified element probabilities. Communications in Statistics-Theory and Methods **19**(11), 4419–4434 (1990)