Optimal Cyber-Security Investment in a Dynamic Version of the Gordon-Loeb Model

Giorgia Callegaro[1], Claudio Fontana[1], Caroline Hillairet[2], and Beatrice Ongarato[1]

[1]Department of Mathematics "Tullio Levi Civita", University of Padova, Padova, Italy
[2]CREST, ENSAE Paris, Palaiseau, France

This document is a draft proposal prepared for the 18^{th} Financial Risks International Forum and is intended for confidential use only. The discussant may contact the presenter, Beatrice Ongarato, at beatrice.ongarato@phd.unipd.it, for additional details or to address any questions regarding the content of this proposal.

***Abstract*—The aim of this work is to determine the optimal cyber-security investment strategy for an entity subject to cyber-attacks. Inspired by the Gordon-Loeb model, we assume that the success rate of cyber-attacks depends on the vulnerability of the security system under threat, which can be reduced investing in security measures. We introduce a dynamic version of the Gordon-Loeb setting, by exploiting Hawkes processes to model the attacks' arrival. This dynamic framework is crucial to rapidly react to the changes which characterize cyber-risk. The problem is framed as a Markovian 2-dimensional stochastic control problem with jumps and it is addressed using dynamic programming techniques. The optimal value is characterized by a partial integro-differential equation, solved numerically. The corresponding optimal strategy is explicitly obtained by differentiating the optimal value function.**

I. Introduction

Cyber-risk is today one of the biggest risks on corporate agendas, with "cyber-attacks/data breaches" being ranked first in the top ten list of global risks by the 2023 AON Global Risk Management Survey reports[1]. According to IBM (the study involved 604 organizations impacted by data breaches between March 2023 and February 2024, over 17 industries, 16 countries and regions, with breaches that ranged from 2.100 to 113.000 compromised records) the global average cost of a data breach has raised to almost 5M USD in 2024, more than 10% higher with respect to the previous year[2]. Beyond cyber breaches, a significant source of damage for companies is business interruption, which, as stated in [14], can result in losses of millions of dollars.

Cyber-attacks are a threat to every industry: from healthcare to finance, from government to education, and potentially for every private company. Indeed, the rapid digitalization of recent years has certainly optimized and speeded-up many processes, but at the same time it has introduced new sources of vulnerability. As a result of the widespread use of modern technologies such as cloud computing, big data, AI and blockchain, new types of cyber-attacks are emerging, with an intensity and associated losses that have increased dramatically.

It is urgent and essential that companies adequately protect themselves against cyber-attacks, which otherwise could cause enormous and irreparable damage. The more sophisticated the attacks become, the more we need to sharpen our tools to mitigate them. In literature, see [24], three main approaches for defending against cyber-attacks are:

1. [Data-driven and AI-driven] using big data and machine learning tools, robust detection methods can be developed;
2. [Model-driven] analyzing previous attacks' features, dynamic models can be developed, allowing for forecasting;
3. [Game-theoretic] the original problem is modeled as a game between the attacker and the defender, aiming at maximizing their payoffs. Defensive strategies under different mathematical solution concepts can be developed.

In this work, we take into consideration the second stream, aiming at developing a continuous-time stochastic model which achieves a good balance between the ability to reproduce real-world features of cyber-attacks and a degree of analytical tractability, that allows to determine optimal cyber-security investment strategies, which can be numerically obtained.

A. Optimal security investment

The problem of optimal investment in information security against cyber-risk has been first addressed in the seminal work of Gordon and Loeb, in [10]. Therein, the authors propose a deterministic one-period setup, in which they analyze the optimal investment strategy, trying to optimize a cost-benefit tradeoff. More details about this model will be given in Section II-A. Different extensions of the Gordon-Loeb model have been studied: in [21] the authors revisit the framework adopting a real options approach in a dynamic setting; more recently, in [19] and [20], risk aversion and the possibility of insurance against cyber-risks have been introduced (see also [1] and [18] on cyber-insurance). For a comprehensive overview on the extensions of the Gordon-Loeb model, see [20, Section 2.2.3]. The settings in [19] and [20] do not take into account the stochastic pattern driving the arrival of cyber-attacks over time, hence they are not adequate to study the optimal response strategies. In fact, cyber risk, unlike other sources of business risk, is dynamic and changes over time,

[1]Source: https://www.aon.com/en/insights/reports/global-risk-management-survey/top-risks-facing-financial-institutions.

[2]Source: https://www.ibm.com/reports/data-breach.

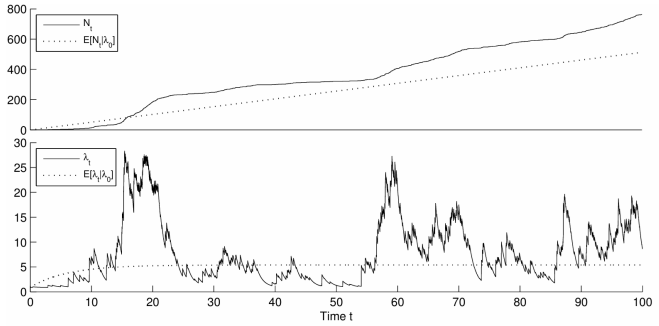


Fig. 1: One Simulated Sample Path of Hawkes process (N, λ), from [9, Section 4].

making it necessary to develop a dynamic response to it. In [21] they work in a dynamic setting, assuming that cyber-threat arrivals are described by a diffusive process.

In our model, which we will define carefully in Section II-B, we consider the overall losses to be driven by a compound counting process, with marks representing losses due to cyber-attacks. This framework is closer to the settings that are typically used in insurance, see e.g. the Cramér-Lundberg model, [8], [15], [16], giving the foundation for a possible extension in this research field.

B. Hawkes processes and cyber-risk

The key feature of our model, as we will clarify Section II-B, is that the number of cyber-attacks arrivals is modeled by Hawkes processes. These processes, first introduced by Alan G. Hawkes in [12], are stochastic processes that count the number of events occurring in a given time interval. Their main characteristic is the "self-exciting" behavior, meaning that the occurrence of an event increases the likelihood of occurrence of further events. Denoting by N the Hawkes process (counting process), which counts the number of attacks, we indicate with λ the associated intensity (hazard rate), which represents the instantaneous probability of an attack to arrive. The self-excitation feature of the Hawkes process N is captured via the intensity λ, given by the stochastic process

$$\lambda_t = \alpha + (\lambda_0 - \alpha)e^{-\xi t} + \beta \sum_{i=1}^{N_t} e^{-\xi(t-\tau_i)}. \qquad (1)$$

The Hawkes parameters can be interpreted as follows:

- $\alpha \geq 0$ is the constant reversion level,
- $\lambda_0 > 0$ is the initial intensity at time $t = 0$,
- $\xi > 0$ is the constant rate of exponential decay,
- $\beta > 0$ is the constant size of self-excited jumps.

We report in Figure 1 an example of simulated path of N and λ, where the clustering behaviour can be clearly observed. The figure is taken from [9, Section 4].

The self-exciting property of Hawkes processes is appropriate to describe the shocks and persistence after shocks that may follow a cyber-attack. This is particularly true taking into account the typical clustering behavior of cyber attacks: for example, the discovery of a software flaw in the IT system of a public administration may lead to an increasing number of attacks in a short time. This intuition has been proven to be true by Baldwin et al. [2], where the threats to ten important Internet services have been analyzed, using data of the SANS (SysAdmin, Audit, Network, and Security) Institute. This was further confirmed by the statistical analysis of Bessy-Roland et al. [4] on the Privacy Rights Clearinghouse database, highlighting the ability of Hawkes models to capture self-excitation and interactions of data-breaches. In this work, the authors prove that Poisson dynamics is not suitable to describe the arrival of data-breaches. Also in the recent work [6], the author calibrates a two-phase Hawkes process with external excitation to a database of cyber-attacks taking into account publication of cyber-vulnerabilities. The three analysis above motivate our assumption of a Hawkes dynamics for cyber-attacks arrivals, see Section II-B.

C. Aim of the work

Consider an entity that is subject to cyber-attacks and assume that the company is sufficiently "large" (e.g., a corporation), so that the threats show a clustered behavior. In the spirit of the Gordon-Loeb model, see [10] and Section II-A, we assume that not all cyber-attacks successfully penetrate the entity's system and that the success rate depends on the vulnerability of the system. To reduce its vulnerability, the entity invests in cyber-security: we aim to study the optimal cyber-security investment.

This paper is organized as follows. In Section II, we briefly present the original Gordon-Loeb model and introduce our dynamic extension. In Section III, we discuss the optimization problem, which determines the optimal cyber-security investment. Later, in Section IV we explain our choice for the parameters and we describe the numerical methods employed to solve the optimization problem. Finally, in Sections V we present some numerical results and discuss their implications.

II. Model

A. The Gordon-Loeb model

The Gordon-Loeb model was first introduced in 2002 by Gordon and Loeb in their seminal work, [10], where they address the problem of optimal investment in information security against cyber-risks. The paper analyzes the optimal amount to invest in IT security to protect a given set of information. In our particular context, we can interpret the set of information as the entity's IT system. Gordon and Loeb assume that an information set (e.g., IT system) is characterized by three parameters:

- p: the probability of a threat occurring,
- ℓ: the loss conditioned on an attack occurring,
- v: the vulnerability defined as the probability that a threat once realized (i.e., an attack) would be successful.

In the Gordon-Loeb model, these parameters are assumed to be constant.

The expected loss from an attack if no investment in security is made is $vp\ell$. The entity can invest a certain amount z in security to reduce its vulnerability. This reduction is

represented by a security breach probability function $S(z, v)$: after an investment z, a threat will penetrate the entity's IT system with probability $S(z, v)$. After investment, the expected loss is given by $S(z, v)p\ell$. Gordon and Loeb require S to satisfy the following:

Assumptions (A).

(A1) $S(z, 0) = 0$ for all z i.e., an invulnerable information set remains invulnerable,

(A2) For all v, $S(0, v) = v$ i.e., if there is no investment in security, then the vulnerability remains unaltered (equal to v),

(A3) S is decreasing and convex w.r.t. z, meaning that $S_z(z, v) < 0$ and $S_{zz}(z, v) > 0$, for all $v \in (0, 1)$ and all z. The monotonicity condition implies that an increasing investment reduces vulnerability, while the convexity condition suggests that the effectiveness of the investment improves as more resources are allocated to security.

Remark 1. *Gordon and Loeb consider two classes of security breach functions, which satisfy Assumptions (A):*

$$S_I(z, v) = \frac{v}{(az + 1)^b} \qquad \textit{and} \qquad S_{II}(z, v) = v^{az+1},$$

for $a, b > 0$.

To find the optimal investment, Gordon and Loeb consider a cost-benefit approach. They maximize the Expected Net Benefit of Investment in information Security (ENBIS):

$$\text{ENBIS}(z) = (v - S(z, v))p\ell - z. \tag{2}$$

ENBIS encapsulates the cost-benefit trade-off of security investment. The first term represents the reduction in the expected loss as a result of the investment z in information security (benefit), while the second term subtracts the cost of investing. The optimal investment is given by z^* which satisfies the following first order condition:

$$-S_z(z^*, v)p\ell - 1 = 0$$

Gordon and Loeb show that for the two classes of security breach functions introduced in Remark 1, the optimal security investment is always less than $1/e$ times the expected loss,

$$z^* < \frac{1}{e} v p \ell. \tag{3}$$

B. Our dynamic extension

We aim at extending the Gordon-Loeb model in continuous time and dynamically, taking into account the main characteristics presented in Section II-A.

Let $(\Omega, \mathcal{F}, \mathbb{P})$ be a probability space and $T > 0$ a terminal time. We assume that cyber-attacks arrive according to a Hawkes process $(N_t)_{t\in[0,T]}$, with intensity solving the stochastic differential equation (SDE)

$$\mathrm{d}\lambda_t = -\xi(\lambda_t - \alpha)\,\mathrm{d}t + \beta \mathrm{d}N_t, \quad \lambda_0 > 0, \xi > 0,$$

which can be obtained from (1) by Itô's formula, see [13].

This choice for the attacks' arrivals is justified in Section I-B.

Proposition 1. *Let λ be the process defined in Eq.* (1) *and N the Hawkes process having λ as intensity. Then, their expectations are given by*

$$\begin{aligned}\mathbb{E}[\lambda_t] &= \frac{\alpha\xi}{\xi - \beta} + e^{-(\xi-\beta)(t)}(\lambda_0 - \frac{\alpha\xi}{\xi - \beta}),\\ \mathbb{E}[N_t] &= \int_0^t \mathbb{E}[\lambda_s]\mathrm{d}s\\ &= \frac{\alpha\xi}{\xi - \beta}t - \frac{1}{\xi - \beta}(\lambda_0 - \frac{\alpha\xi}{\xi - \beta})(e^{-(\xi-\beta)t} - 1).\end{aligned}$$

Proof. Refer to [9, Proposition 2.3]. □

We denote the jump times of N by $(\tau_i)_{i\in\mathbb{N}}$. For $t \in [0, T]$, the potential losses generated by all cyber-attacks occurring in the time interval $[0, t]$ are given by a compound Hawkes process:

$$C_t = \sum_{i=1}^{N_t} \eta_i,$$

where $(\eta_i)_{i\geq 1}$ are a family of random variable satisfying the following:

Assumption (B). $(\eta_i)_i$ are i.i.d. positive random variables such that $\eta_i \in L^1(\mathbb{P})$ and $\mathbb{E}[\eta^i] = \bar{\eta}$ for every i and independent with respect to N.

Each random variable η_i represents the loss associated with the i-th attack.

The filtration is $\mathbb{F} := (\mathcal{F}_t)_{t\in[0,T]}$, with $\mathcal{F}_t = \sigma(N_s, s \leq t) \vee \sigma(\eta_{\tau_i}, \tau_i \leq t)$.

In the spirit of the Gordon-Loeb model, we assume that not all threats are successful: if the entity does not make any investment in security, the attacks penetrate the entity's IT system (or not) depending on its vulnerability $v \in (0, 1)$. The actual losses are given by:

$$L_t^0 = \sum_{i=1}^{N_t} \eta_i \cdot B_i^v, \tag{4}$$

where $(B_i^v)_{i\geq 1}$ is a family of i.i.d. Bernoulli random variables such that $B_i^v \sim \text{Be}(v)$, for every i.

Remark 2. *The interpretation of Eq.* (4) *is the following: a cyber-attack attempts to breach the system at time τ_i, with a potential loss η_i. With probability v, the threat penetrates the system (i.e., the attack is successful) and the potential loss becomes an actual loss; otherwise, with probability $(1 - v)$, the threat is rejected by the system and the actual loss is zero.*

Similarly to the Gordon-Loeb model, the entity can invest in cyber-security to reduce its vulnerability. We assume that, at each instant in time, the entity can invest a certain amount z_t. The process $z = (z_t)_{t\in[0,T]}$ is the investment rate and the cumulated investment at time t is given by $\int_0^T z_t\,\mathrm{d}t$. We assume that the control z belongs to the set $\mathcal{Z}$, described in Definition 1.

Definition 1. *We define by $\mathcal{Z}$ the set of admissible strategies:*

$$\mathcal{Z} := \{(z_t)_{t\in[0,T]} \text{ such that } z_t \geq 0, z_t \ \mathbb{F}- \text{ predictable and } \mathbb{E}\left[\int_0^T z_t \mathrm{d}t\right], \mathbb{E}\left[\int_0^T z_t^2 \mathrm{d}t\right] < \infty\}. \tag{5}$$

Given $\tau \in [0,T]$ stopping time adapted to the filtration in $\mathbb{F}$, we denote by $\mathcal{Z}_\tau$ the class $\mathcal{Z}$ restricted to the time interval $[\tau, T]$.

It is reasonable to assume that a more recent investment in security should be more effective than a past one (e.g. due to the obsolescence of technology). To describe this feature, we introduce a decaying rate $\rho > 0$ and define the process H as follows:

$$H_t = H_0 e^{-\rho t} + \int_0^t e^{-\rho(t-s)} z_s \mathrm{d}s. \tag{6}$$

The stochastic differential equation associated to H is

$$\mathrm{d}H_t = (-\rho H_t + z_t)\mathrm{d}t.$$

Analogously to the Gordon-Loeb case, we introduce a probability breach function $S(H_t, v)$, that satisfies the properties listed in Assumptions (A).

Hence, after investing in security, the actual losses of the entity are given by

$$L_t^z = \sum_{i=1}^{N_t} \eta_i \cdot B_i^{S(H_{\tau_i}, v)}, \tag{7}$$

where $(B_i^{S(H_{\tau_i},v)})_{i\geq 1}$ is a family of Bernoulli random variables such that $\mathbb{P}(B_i^{S(H_{\tau_i},v)} = 1 | H_{\tau_i} = h) = S(h, v)$.

Remark 3. *The model we consider for the overall losses, see Eqs.* (4)*,* (7)*, is driven by a compound Hawkes process, with the marks representing losses due to cyber-attacks. We consider marks that depend on the level of information security, so that only a portion of the incoming cyber-attacks will actually generate a loss.*

We prove below some properties of the compound jump processes introduced above.

Proposition 2. *The expectation of the cumulated losses (resp., without and with investment), are given by*

$$\mathbb{E}[L_T^0] = \mathbb{E}\left[\int_0^T v\bar{\eta}\lambda_t \mathrm{d}t\right] = v\bar{\eta}\mathbb{E}[N_T]$$
$$\mathbb{E}[L_T^z] = \mathbb{E}\left[\int_0^T S(H_t, v)\bar{\eta}\lambda_t \mathrm{d}t\right].$$

and

$$\mathbb{E}[L_T^0 - L_T^z] = \mathbb{E}\left[\int_0^T (v - S(H_t, v))\bar{\eta}\lambda_t \mathrm{d}t\right]. \tag{8}$$

Proof. Recall the definition of L_T^0 in Eq. (4), we have that $\eta_i \cdot B_i^v$ are i.i.d. and due to Wald's equation, see [22], we write

$$\mathbb{E}[L_T^0] = \mathbb{E}[\eta \cdot B^v]\mathbb{E}[N_T] = v\bar{\eta}\mathbb{E}[N_T] = v\bar{\eta}\mathbb{E}\left[\int_0^T \lambda_t dt\right]$$

Notice that $(\eta_i \cdot B^{S(H_{\tau_i},v)})_{i\geq 1}$ are not independent; thus Wald's formula does not hold. We then proceed as follows:

$$\begin{aligned}
\mathbb{E}[L_T^z] &= \mathbb{E}\left[\sum_{i=1}^{N_T} \eta_i \cdot B^{S(H_{\tau_i},v)}\right] \\
&= \mathbb{E}\left[\sum_{i=1}^{N_T} \mathbb{E}\left[\eta_i \cdot B^{S(H_{\tau_i},v)} \middle| \mathcal{F}_{\tau_i -} \vee \sigma(N_T)\right]\right] \\
&= \mathbb{E}\left[\sum_{i=1}^{N_T} \bar{\eta} S(H_{\tau_i}, v)\right] = \bar{\eta}\mathbb{E}\left[\int_0^T S(H_t, v) dN_t\right] \\
&= \mathbb{E}\left[\int_0^T S(H_t, v)\bar{\eta}\lambda_t dt\right].
\end{aligned}$$

□

III. The optimization problem

Inspired by the benefit-cost approach presented in Eq. (2), we consider the following problem:
Optimization problem.

$$\sup_{z\in\mathcal{Z}} \mathbb{E}\left[L_T^0 - L_T^z - \left(\int_0^T \delta z_t + \frac{\gamma}{2} z_t^2 \mathrm{d}t\right) + U(H_T)\right]. \tag{9}$$

$$\mathrm{d}\lambda_t = -\xi(\lambda_t - \alpha)\,\mathrm{d}t + \beta \mathrm{d}N_t, \tag{10}$$
$$\mathrm{d}H_t = (-\rho H_t + z_t)\mathrm{d}t, \tag{11}$$

where the set of admissible controls is $\mathcal{Z}$ as defined in Eq. (5). The difference $L_T^0 - L_T^z$ represents the benefit obtained by the entity's when it invests in cyber-security. Differently from the problem in Eq. (2), where they assume a linear cost of investment, we consider a quadratic cost $\delta z_t + \frac{\gamma}{2} z_t^2$, $\delta > 0, \gamma > 0$. This choice is common in stochastic control literature. We also include a utility function $U(H_T)$, assuming U to be increasing and concave. The function U takes into account the efforts made by the entity until time T. In fact, the entity does not end up existing at time T, thus it needs some security investments for the future.

Exploiting the result in Eq. (8), we can compute the expectation of $L_T^0 - L_T^z$. Moreover, we can divide all terms in Eq. (9) by δ, obtaining an equivalent problem, with a small abuse of notation.
Equivalent problem.

$$\sup_{z\in\mathcal{Z}} \mathbb{E}\left[\int_0^T \left[(v - S(H_t, v))\bar{\eta}\lambda_t - z_t - \frac{\gamma}{2} z_t^2\right] \mathrm{d}t + U(H_T)\right]. \tag{12}$$
$$\begin{aligned}
\mathrm{d}\lambda_t &= -\xi(\lambda_t - \alpha)\,\mathrm{d}t + \beta \mathrm{d}N_t \\
\mathrm{d}H_t &= (-\rho H_t + z_t)\mathrm{d}t.
\end{aligned}$$

From now on, we focus on the problem in Eq. (12). First of all, we introduce the following notation:

- $H_s^{t,h,z}$ is the process H evaluated at time $s > t$, starting at time t, with initial value h and associated to the control z. In particular,

$$H_s^{t,h,z} = h + \int_t^s (-\rho H_v^{t,h,z} + z_v)\mathrm{d}v,$$

i.e.

$$H_s^{t,h,z} = he^{-\rho(s-t)} + \int_t^s e^{-\rho(s-v)} z_v \mathrm{d}v. \tag{13}$$

- $\lambda_s^{t,\lambda}$ is the process H evaluated at time $s > t$, starting at time t, with initial value λ,

$$\lambda_s^{t,\lambda} = \lambda - \xi \int_t^s (\lambda_v^{t,\lambda} - \alpha)\mathrm{d}v + \beta \int_t^s \mathrm{d}N_v^{\lambda}.$$

i.e.

$$\lambda_s^{t,\lambda} = \alpha + (\lambda - \alpha)e^{-\xi(s-t)} + \beta \int_t^s e^{-\xi(s-v)} \mathrm{d}N_v^{\lambda}.$$

- J is the revenue function, i.e. the function we aim at maximizing given the initial state (t, λ, h):

$$J(t,\lambda,h;z) = \mathbb{E}\left[\int_t^T \Big[(v - S(H_s^{t,h,z}, v))\bar{\eta}\lambda_s^{t,\lambda} - z_s - \frac{\gamma}{2} z_s^2\Big]\mathrm{d}s + U(H_T^{t,h,z})\right].$$

Consequently, we define the value function as

$$V(t,\lambda,h) = \sup_{z \in \mathcal{Z}_t} J(t,\lambda,h;z), \tag{14}$$

where $\mathcal{Z}_t$ has been introduced in Definition 1.

We now make the following standing assumption:

Assumptions (C). The Dynamic Programming Principle holds, analogously to [5, Theorem 2.2.1]: for all (t, λ, h) in $[0, T) \times \mathbb{R}_{>0} \times \mathbb{R}_{\geq 0}$ and for all families of bounded stopping times $\{\theta^z, z \in \mathcal{Z}\}$ we have

$$V(t,\lambda,h) = \sup_{z \in \mathcal{Z}_t} \mathbb{E}\left[\int_t^{\theta^z} \Big[(v - S(H_s^{t,h,z}, v)\bar{\eta})\lambda_s^{t,\lambda} - z_s - \frac{\gamma}{2} z_s^2\Big]\mathrm{d}s + V(\theta^z, \lambda_{\theta^z}^{t,\lambda}, H_{\theta^z}^{t,h,z})\right].$$

As a further assumption, we require that the function V defined in Eq. (14) to be at least $\mathcal{C}^1$, i.e., continuous and differentiable with continuous derivative in all its arguments.

Theorem 1. *Under Assumptions (C), V solves the following partial integral differential equation*

$$\begin{aligned} &\frac{\partial V}{\partial t} - \xi(\lambda - \alpha)\frac{\partial V}{\partial \lambda} - \rho h \frac{\partial V}{\partial h} + \lambda(V(t,\lambda+\beta,h) - V(t,\lambda,h)) \\ &+ (v - S(h,v))\bar{\eta}\lambda + \max\left\{0, \frac{\frac{\partial V}{\partial h} - 1}{\gamma}\right\}\left(\frac{\partial V}{\partial h} \right. \\ &\left. - 1 - \frac{\gamma}{2}\max\left\{0, \frac{\frac{\partial V}{\partial h} - 1}{\gamma}\right\}\right) = 0, \\ &V(T,\lambda,h) = U(h). \end{aligned} \tag{15}$$

Moreover, the optimal control is given by

$$z^* = \begin{cases} 0 & \text{if } \frac{\partial V}{\partial h} \leq 1 \\ \frac{\frac{\partial V}{\partial h} - 1}{\gamma} & \text{otherwise}. \end{cases} \tag{16}$$

Proof. From the Dynamic Programming Principle and being V sufficiently smooth by Assumptions (C), we find that V solves the following Hamilton Jacobi Bellmann equation, see [5, Theorem 2.2.2.], [3, Section 5.2, Eqs. (38a), (38b)]:

$$\begin{aligned} 0 &= \sup_{z \in \mathcal{Z}} \frac{\partial V}{\partial t} - \xi(\lambda - \alpha)\frac{\partial V}{\partial \lambda} - \rho h \frac{\partial V}{\partial h} \\ &\quad + z\frac{\partial V}{\partial h} + \lambda(V(t,\lambda+\beta,h) - V(t,\lambda,h)) \\ &\quad + (v - S(h,v))\bar{\eta}\lambda - z - \frac{\gamma}{2}z^2 \\ &= \frac{\partial V}{\partial t} - \xi(\lambda - \alpha)\frac{\partial V}{\partial \lambda} - \rho h \frac{\partial V}{\partial h} \\ &\quad + \lambda(V(t,\lambda+\beta,h) - V(t,\lambda,h)) \\ &\quad + (v - S(h,v))\bar{\eta}\lambda + \sup_{z \in \mathcal{Z}}\left(z\frac{\partial V}{\partial h} - z - \frac{\gamma}{2}z^2\right). \end{aligned}$$

The supremum is given by

$$\sup_{z \geq 0}\left(z\frac{\partial V}{\partial h} - z - \frac{\gamma}{2}z^2\right) = \begin{cases} 0 & \frac{\partial V}{\partial h} \leq 1, \\ \frac{1}{2\gamma}\left(\frac{\partial V}{\partial h} - 1\right)^2 & \text{otherwise} \end{cases}$$

and it is reached for the optimal control as defined in Eq. (16). □

Remark 4. *The interpretation of the optimal control in Eq. (16) is the following: it is worth to invest if the benefit we obtain by doing so is larger than the marginal cost.*

Let us now state some properties of the value function V as defined in Eq. (14).

Proposition 3. *If $h_1 < h_2$, then*

$$V(t,\lambda,h_1) < V(t,\lambda,h_2).$$

Proof. Let $h_1 < h_2$, then for every fixed control z, for every time $s > t$

$$H_s^{t,h_1,z} < H_s^{t,h_2,z} \text{ a.e..}$$

The inequality can be simply derived from Eq. (13). Since $S(h,v)$ is decreasing in h, see Assumption (A), $-S(h,v)$ is increasing in h. The function U is increasing in h by hypothesis, thus it follows:

$$\begin{aligned} J(t,\lambda,h_1;z) &= \mathbb{E}\left[\int_t^T \Big[(v - S(H_s^{t,h_1,z}, v))\bar{\eta}\lambda_s^{t,\lambda} - z_s - \frac{\gamma}{2}z_s^2\Big]\mathrm{d}s + U(H_T^{t,h_1,z})\right] \\ &< \mathbb{E}\left[\int_t^T \Big[(v - S(H_s^{t,h_2,z}, v))\bar{\eta}\lambda_s^{t,\lambda} - z_s - \frac{\gamma}{2}z_s^2\Big]\mathrm{d}s + U(H_T^{t,h_2,z})\right] \\ &\leq V(t,\lambda,h_2). \end{aligned}$$

In particular, taking z as the optimal control for the initial values (λ, h_1) at time t, we get the result. □

Proposition 4. *If $0 < \lambda_1 < \lambda_2$, then*

$$V(t, \lambda_1, h) < V(t, \lambda_2, h).$$

Proof. For $s > t$, $\lambda_s^{t,\lambda_2} - \lambda_s^{t,\lambda_1}$ is a strictly positive process, see [17, Proof Proposition 3.1]. Thus $\lambda_s^{t,\lambda_2} > \lambda_s^{t,\lambda_1}$ almost everywhere. For every fixed $z, h \geq 0$, the quantity $(v - S(H_s^{t,h,z}, v))\bar{\eta}$ is non-negative, thus

$$\begin{aligned} J(t, \lambda_1, h; z) &= \mathbb{E}\left[\int_t^T \left[(v - S(H_s^{t,h,z}, v))\bar{\eta}\lambda_s^{t,\lambda_1} - z_s \right.\right. \\ &\qquad \left.\left. - \frac{\gamma}{2} z_s^2\right] \mathrm{d}s + U(H_T^{t,h,z})\right] \\ &< \mathbb{E}\left[\int_t^T \left[(v - S(H_s^{t,h,z}, v))\bar{\eta}\lambda_s^{t,\lambda_2} - z_s \right.\right. \\ &\qquad \left.\left. - \frac{\gamma}{2} z_s^2\right] \mathrm{d}s + U(H_T^{t,h,z})\right] \\ &\leq V(t, \lambda_2, h). \end{aligned}$$

Taking z as the optimal control for the initial values (λ_1, h) at time t, we get that V is increasing in λ. □

Proposition 5. *The value function is bounded from below, in particular*

$$\begin{aligned} V(t, \lambda, h) \geq (v - S(h, v))\bar{\eta}\left(\frac{\alpha\xi}{\xi - \beta}(T - t) - \frac{1}{\xi - \beta}\left(\lambda \right.\right. \\ \left.\left. - \frac{\alpha\xi}{\xi - \beta}\right)(e^{-(\xi-\beta)(T-t)} - 1)\right) + U(h). \end{aligned}$$

Proof. Since $V(t, \lambda, h) \geq J(t, \lambda, h, z)$ for each $z \geq 0$, we write $V(t, \lambda, h) \geq J(t, \lambda, h, 0)$. The bound then follows. In particular, we refer to Proposition 1 to obtain the expectation of $\lambda_s^{t,\lambda}$. □

IV. Methods

A. Parameters' choice

The parameters chosen to perform the numerical analysis are in Table I, II, III. We denote this set by *standard set of parameters* and we will use them unless otherwise stated.

S	v	a	b
S_I	0.65	$1 \cdot 10^{-5}$	1

TABLE I: Security breach function.

λ	α	ξ	β	λ_0
	2.7	1.5	0.9	2.7

TABLE II: Hawkes intensity.

The parameters for the security breach function, Table I, are analogous to those in [20], which are themselves slight variations of those in [10] and [18]. We choose the security breach function S as S_I in Remark 1, considering the h entry to be expressed in k$. Under this assumption, S_I becomes:

$$S_I(h, v) = \frac{v}{(az \cdot 10^3 + 1)^b}.$$

We refer to Figure 2 for a grafic representation of the security breach function in terms on h.

Optimization	δ	γ	$\bar{\eta}$(k$)	$U(h)$	ρ	T
	0.01	0.2	2	$0.02\sqrt{h}$	0.03	0.5

TABLE III: Optimization problem parameters.

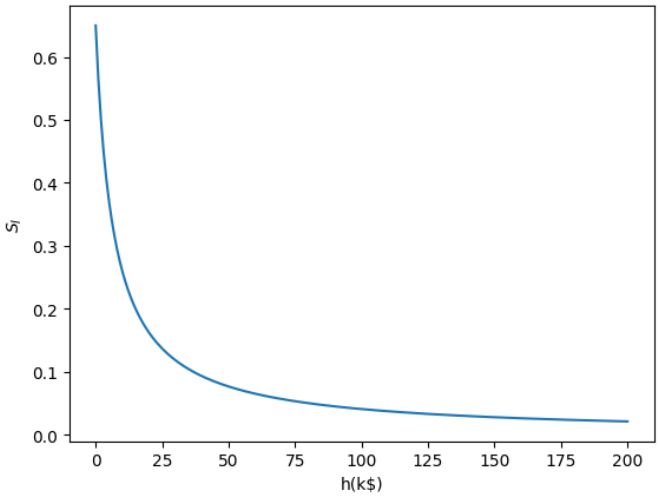


Fig. 2: Security breach functions for the parameters chosen in Table I.

For the Hawkes intensity parameters, see Table II, we choose those in [6]. In [6], the authors calibrate the Hawkes intensity parameters on real data, taken from the Hackmageddon database. This database, updated by Paolo Passeri, collects all the main attacks worldwide, thus it is not perfectly suitable for our scope since we would like to consider only the attacks towards a particular entity. However, due to the unavailability of real data more appropriate to our problem, we believe it is a good starting point to test our model with parameters taken from a real scenario, albeit not perfectly inherent to our context. We refer to [6, Section 4.1.1] for further details on the database.

Remark 5. *In general, observing the dynamics of λ in Eq.* (10) *and the PIDE associated to the optimization problem, Eq.* (15)*, we notice that it is not necessary to specify an initial intensity λ_0. However, to perform some numerical analysis, we will need to take into account the initial intensity λ_0, that we choose equal to α, consistently with [6]. In this case, the equation for λ_t becomes*

$$\lambda_t = \lambda_0 + \beta \sum_{i=1}^{N_t} e^{-\xi(t-\tau_i)}.$$

This choice of λ_0 is influential in:

- *The choice of λ_{max} in Table IV, which depends on the expectation and variance of λ.*
- *The choice of H_0 in Section V-C.*
- *The choice of the Poisson intensities in Section V-D.*
- *The intensity trajectory considered in Section V-D1.*

All other numerical tests are independent from the choice of λ_0.

For the other parameters, we refer to Table III. The linear cost, δ, and the quadratic one, γ, have been chosen after testing the algorithm with different options. In particular, we pick parameters in such a way as to have comparable dimensions between the different elements of the optimization function. We decide to test the algorithm over a half-year time period ($T = 0.5$), as it is a reasonable time window from the entity point of view. Let us stress that shorter maturities are numerically even more stable. As for the average loss associated to cyber-attacks, we opted for $\bar{\eta} = 2\text{k\$}$ We choose a small decay factor ρ, in order to consider a moderate impact of the obsolescence of the technology. We also decided on a square root utility for U, as it is commonly used in optimization problems, being increasing and concave.

B. Numerical scheme for PIDE resolution

To solve the optimization problem, we need to provide a solution to the partial-integro differential equation (PIDE) in Eq. (15). The PIDE can be classified as first-order and non-linear. Due to the great complexity of the problem, we cannot expect to compute explicitly an analytical solution, so we proceed to solve the PIDE numerically. We solve it through the classical method of lines, see [23]. This technique consists in discretizing the PIDE in the space dimensions but not in time and then in integrating the semi-discrete problem as a system of ODEs. In our case, we discretize the (λ, h) dimension with a backward and forward scheme, respectively, and then solve the ODE system with a built-in Python solver. We refer to Algorithm 1 for further details about the application of this scheme in our scenario. We refer to Table IV for the parameters used in the algorithm:

$h_{\min}$	$h_{\max}$	Δh	$\lambda_{\min}$	$\lambda_{\max}$	$\Delta\lambda$
0	100	0.5	2.7	10.8	0.1

TABLE IV: Algorithm 1 parameters.

Algorithm 1 has been implemented in Python. The system of ODEs is solved using the built-in method scipy.integrate.solve_ivp, (https://docs.scipy.org/doc/scipy/reference/generated/scipy.integrate.solve_ivp.html). We compared various ODE solver methods and end up choosing the Radau method. This method is an implicit Runge-Kutta method of the Radau IIA family of order 5, for further details refer to [11].

Remark 6. *Similarly to [7], where they analyse a numerical scheme for solving PIDE in a Lévy setting, we highlight that we need to localize the PIDE in Eq.* (15) *over a bounded domain. In particular, for the integral part arising from the equation of λ, Eq.* (10)*, we extend the function V outside the domain $[\lambda_{min}, \lambda_{max}]$, imposing*

$$V(t, \lambda, h) = V(t, \lambda_{max}, h)$$

for $\lambda > \lambda_{max}$. We choose $\lambda_{max} = \mathbb{E}[\lambda_T] + 7 * \sqrt{Var[\lambda_T]} \approx 10.8$, where 7 is chosen arbitrarily.

Algorithm 1 Numerical scheme for the solution of (15)

1: Choose $\lambda_{\min}, \lambda_{\max}, h_{\min}, h_{\max}$.
2: Discretize $[\lambda_{\min}, \lambda_{\max}]$, $\lambda_0 = \lambda_{\min}, \lambda_N = \lambda_{\max}$, $\lambda_n - \lambda_{n-1} = \Delta\lambda$.
3: Discretize $[h_{\min}, h_{\max}]$, $h_0 = h_{\min}, h_M = h_{\max}$, $h_m - h_{m-1} = \Delta h$.
4: Define $V_{n,m}(t) := V(t, \lambda_n, h_m)$.
5: Approximate the partial derivatives w.r.t. λ

$$\frac{\partial V}{\partial \lambda}(t, \lambda_n, h_m) \approx \frac{V_{n,m}(t) - V_{n-1,m}(t)}{\Delta\lambda},$$
$$\frac{\partial V}{\partial \lambda}(t, \lambda_0, h_m) \approx \frac{V_{1,m}(t) - V_{0,m}(t)}{\Delta\lambda}.$$

6: Approximate the partial derivatives w.r.t. h

$$\frac{\partial V}{\partial h}(t, \lambda_n, h_m) \approx \frac{V_{n,m+1}(t) - V_{n,m}(t)}{\Delta h},$$
$$\frac{\partial V}{\partial h}(t, \lambda_n, h_M) \approx \frac{V_{n,M}(t) - V_{n,M-1}(t)}{\Delta h}.$$

7: Let $\tilde{n} = \frac{\lfloor \beta \rfloor}{\Delta\lambda}$,

$$V(t, \lambda_n + \beta, h_m) \approx V_{(n+\tilde{n}) \wedge N, m}(t).$$

8: Solve using an ODE solver the system given for every n, m by

$$\begin{aligned} V'_{n,m}(t) &= \xi(\lambda_n - \alpha)\frac{V_{n,m}(t) - V_{n-1,m}(t)}{\Delta\lambda} \\ &+ \rho h \frac{V_{n,m+1}(t) - V_{n,m}(t)}{\Delta h} \\ &- \lambda_n (V_{n+\tilde{n}\wedge N, m}(t) - V_{n,m}(t)) - (v - S(h_m, v))\bar{\eta}\lambda_n \\ &- \max\left\{0, \frac{\frac{V_{n,m+1}(t) - V_{n,m}(t)}{\Delta h} - 1}{\gamma}\right\} \left(\frac{V_{n,m+1}(t) - V_{n,m}(t)}{\Delta h} \right. \\ &\left. - 1 - \frac{\gamma}{2} \max\left\{0, \frac{\frac{V_{n,m+1}(t) - V_{n,m}(t)}{\Delta h} - 1}{\gamma}\right\} \right), \\ V_{n,m}(T) &= U(h_m). \end{aligned}$$

C. Optimal control along a trajectory

In Section V-D, we will depict the optimal control with respect to a specific trajectory of the intensity $(\lambda_t(\omega))_{t \in [t_{\text{init}}, T]}$, given a specific initial time t_{init} and initial investment H_{init}. To

Remark 7. *When visualizing the graph for $V(t, \lambda, h)$, varying λ, we will focus only on a subinterval of $[\lambda_{min}, \lambda_{max}]$, as due to domain localization, the value function might be numerically instable for values of λ close to λ_{max}.*

perform this analysis, we proceed as described in Algorithm 2. We will use Algorithm 2 in Section V-D1, specifying the parameters used in the specific scenario, see Table V.

Algorithm 2 Optimal control along a trajectory

Choose $t_{\min}, t_{\max}$, $\lambda_{\min}, \lambda_{\max}$,$h_{\min}, h_{\max}$.
Discretize $[t_{\min}, t_{\max}]$, $t_0 = t_{\min}, t_I = t_{\max}, t_i - t_{i-1} = \Delta t$.
Discretize $[\lambda_{\min}, \lambda_{\max}]$, $\lambda_0 = \lambda_{\min}, \lambda_N = \lambda_{\max}$, $\lambda_n - \lambda_{n-1} = \Delta\lambda$.
Discretize $[h_{\min}, h_{\max}]$, $h_0 = h_{\min}, h_M = h_{\max}$, $h_m - h_{m-1} = \Delta h$.
Solving the PIDE, compute $V(t_i, \lambda_n, h_m)$ and $z^*(t_i, \lambda_n, h_m)$ for $i = 0, \dots, I, n = 0, \dots, N, m = 0, \dots, M$.
Fix a trajectory $\lambda_t(\omega)$.
Consider the initial time $t_{\text{init}} \geq t_{\min}$.
Let $\bar{i} := arg\,min_i\{|t_i - t_{\text{init}}|\}$.
Consider the initial state $H_{t_{\bar{i}}} = H_{\text{init}}$.
for i in $\bar{i}, \dots, I$ **do**
    Consider $k := arg\,min_k\{|\lambda_k - \lambda_{t_i}(\omega)|\}$.
    Consider $j := arg\,min_j\{|h_j - H_{t_i}|\}$
    Define $z^*_{t_i} = z^*(t_i, \lambda_k, h_j)$.
    $H^{t_{\text{init}}, H_{\text{init}}, z^*}_{t_{i+1}}(\omega) = H^{t_{\text{init}}, H_{\text{init}}; z^*}_{t_i}(\omega) - \rho H^{t_{\text{init}}, H_{\text{init}}; z^*}_{t_i}(\omega)\Delta t + z^*_{t_i}\Delta t$
end for

V. Numerical results

In this section, we perform some numerical tests to study the main properties of our model. First, we compute the value function and the optimal control for the standard set of parameters, see Tables I, II, III. Then, we discuss parameter sensitivity. Later, we compare the benefit obtained by implementing the dynamic strategy with respect to the static Gordon-Loeb strategy. We then compare optimal control with a Hawkes' dynamics with an analogous problem formulated under a Poisson's hypothesis. Lastly, we visualize the optimal control along a particular intensity trajectory.

A. Value function and optimal control

We report in Figure 3, different representations for the value function and the optimal control. In Subfigures 3a, 3d we plot the functions for h fixed, varying t and λ. Consistently with Proposition 3, we observe that the value function is increasing in h. Clearly, a higher cumulative initial investment h leads to a greater benefit, which is represented by a higher value function. On the other hand, the optimal control decreases in h as more money the entity has already invested, the less it should invest later. Both the value function and optimal control are decreasing functions of t. In fact, approaching maturity, the impact of the entity's actions becomes less significant in generating substantial benefits, and thus this causes an overall lower investment. In Subfigures 3b, 3e we plot the functions for λ fixed, varying t and h. We highlight that the value function is increasing in λ, accordingly to Proposition 4. The same holds for the optimal control. A larger λ represents a higher risk that induces a higher benefit, if the entity invests wisely. In terms of optimal control, a larger risk should lead to a higher investment to mitigate it. In Subfigures 3c, 3f, we depict the value function and optimal control for both λ and h fixed, to better visualize their behavior.

B. Parameter sensitivity

In Figure 4, we compare the value function and optimal control for two representative values of ρ, in particular for $\rho = 0$ - no obsolescence in time - and $\rho = 2$ - high obsolescence in time. We observe that a larger ρ generally leads to a smaller value function and a reduced investment. In fact, a high value of ρ forces us to invest later in time. As we go forward in time, we approach maturity and our efforts become less significant as they do not provide much benefit. As a further parameter investigation, we compare the value function and optimal control computed for different values for ξ, $\xi = 1.5, \xi = 20$, i.e., different decaying parameters for the Hawkes intensity. As ξ increases, the Hawkes intensity decays faster after a jump. In Subfigures 5a, 5b, we observe that both the value function and the optimal control are decreasing with respect to ξ. Indeed, the faster the intensity decays, the smaller is the overall risk, thus the entity has a smaller benefit and has to invest less over all.

C. Comparison with a static strategy

As we explained in Section I, cyber-risk is a dynamic type of risk and it is reasonable to implement a dynamic strategy in order to act effectively against these dynamic threats. In particular, we compute the gain obtained by implementing a static strategy with respect to a dynamic one. To be consistent with the original Gordon-Loeb framework, see (3), we consider an initial investment $H_0 \leq \frac{\mathbb{E}[L^0_T]}{e} = \frac{\bar{\eta} v \mathbb{E}[N_T]}{e} = 0.78$ (taking $\bar{\eta} = 2$). In particular, we choose $H_0 = 0.50$. We assume to implement a static strategy as follows: $z^{\text{GL}}_s = H_0\rho$ for every s, such that replacing the control in the equation for H, Eq. (6), we obtain $H^{\text{GL}}_t = H_0$ for all t.

Under these assumptions, we compute

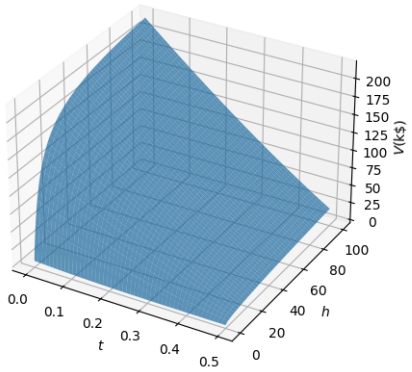
$$\begin{aligned} J(t, \lambda, H_0; z^{\text{GL}}) &= (v - S(H_0, v))\bar{\eta}\mathbb{E}\left[\int_t^T \lambda^{t,\lambda}_s\right] \\ &\quad + (T-t)(-H_0\rho - \frac{\gamma}{2}(H_0\rho)^2) + U(H_0) \\ &= (v - S(H_0, v))\bar{\eta}\left(\frac{\alpha\xi}{\xi-\beta}(T-t) - \frac{1}{\xi-\beta}\Big(\lambda \right. \\ &\quad \left. - \frac{\alpha\xi}{\xi-\beta}\Big)(e^{-(\xi-\beta)(T-t)} - 1)\right) \\ &\quad + (T-t)(-H_0\rho - \frac{\gamma}{2}(H_0\rho)^2) + U(H_0)\,, \end{aligned}$$

where the expectation of the integral of λ follows from a modification of Proposition 1. We define the gain at initial time t, initial state λ as

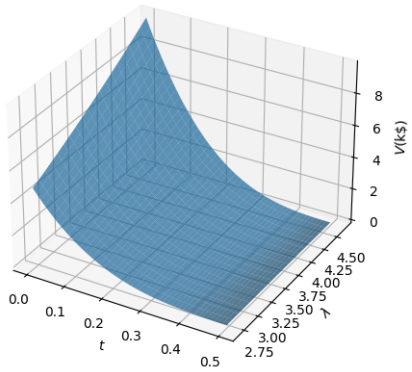
$$\text{gain}^{\text{GL}}(t, \lambda) = V(t, \lambda, H_0) - J(t, \lambda, H_0; z^{\text{GL}}). \tag{17}$$

If we want to evaluate the relative gain, we compute

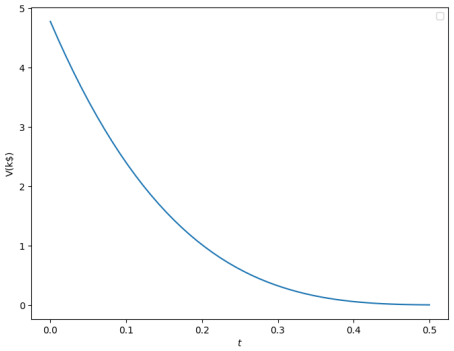
$$\%\text{gain}^{\text{GL}}(t, \lambda) = 100 \cdot \text{gain}^{\text{GL}}(t, \lambda)/V(t, \lambda, H_0). \tag{18}$$



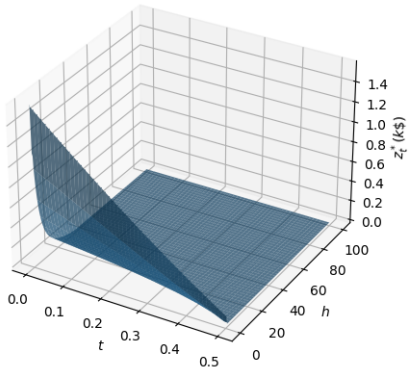
(a) Value function $V(t, \lambda, h)$ for $\lambda = 2.7$.



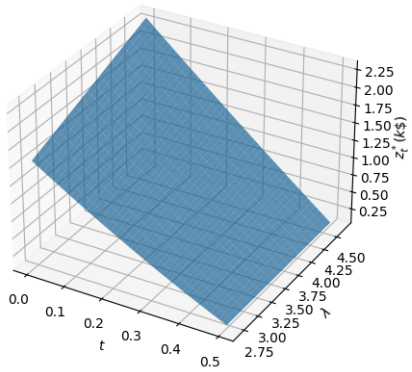
(b) Value function $V(t, \lambda, h)$ for $h = 0$.



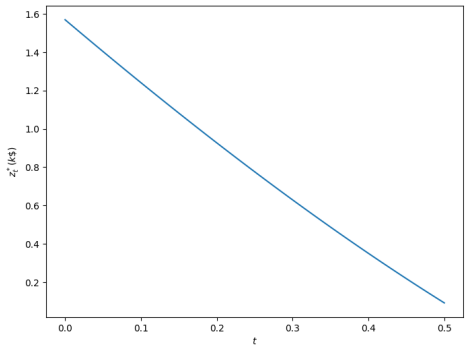
(c) Value function $V(t, \lambda, h)$ for $\lambda = 2.7, h = 0$.



(d) Optimal control $z_t^*(\lambda, h)$ for $\lambda = 2.7$.



(e) Optimal control $z_t^*(\lambda, h)$ for $h = 0$.



(f) Optimal control $z_t^*(\lambda, h)$ for $\lambda = 2.7, h = 0$.

Fig. 3: Value function and optimal control computed with *standard parameters set*, see Tables I, II, III.

We observe in Figure 6 the plots of the gain and of its percentage varying t and λ. We observe that the gain decreases over time and increases over λ. At time 0, we save around $4.7k\$$ when $\lambda = 2.7$ and around $9.6k\$$ when $\lambda = 4.50$, which are respectively the 22% and 28% of the overall benefit.

D. Comparison with Poisson model for arrival of attacks

In this section, we reformulate the optimization problem by choosing as the counting process a Poisson process. We denote by P a Poisson process, i.e., a counting process having constant intensity λ^P. The optimization problem we aim at solving is the same of Eq. (12), but considering a constant intensity rather than a dynamic one. Under the Poisson's hypothesis, the problem becomes deterministic. We denote by $V^P(t, h)$ the value function in this setting, which now solves the PDE:

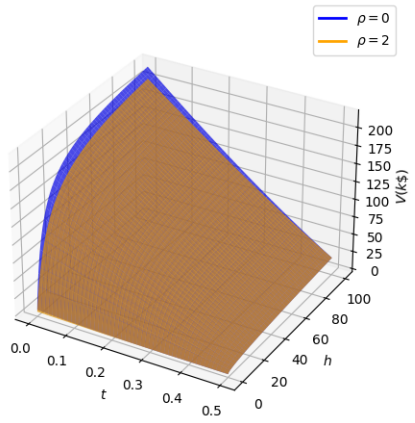
$$\begin{aligned} &\frac{\partial V^P}{\partial t} - \rho h \frac{\partial V^P}{\partial h} + \lambda^P (v - S(h, v))\bar{\eta} \\ &\quad + \max\left\{0, \frac{\frac{\partial V^P}{\partial h} - 1}{\gamma}\right\}\left(\frac{\partial V^P}{\partial h} - 1\right. \\ &\quad \left. - \frac{\gamma}{2}\max\left\{0, \frac{\frac{\partial V^P}{\partial h} - 1}{\gamma}\right\}\right) = 0, \\ &V^P(T, h) = U(h). \end{aligned} \tag{19}$$

The corresponding optimal control is given by

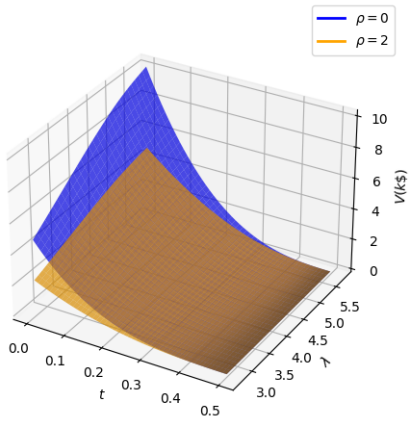
$$z^{P*} = \begin{cases} 0 & \text{if } \frac{\partial V^P}{\partial h} \leq 1 \\ \frac{\frac{\partial V^P}{\partial h} - 1}{\gamma} & \text{otherwise} \end{cases}.$$

We solve the PDE using a similar scheme to that of Algorithm 1.

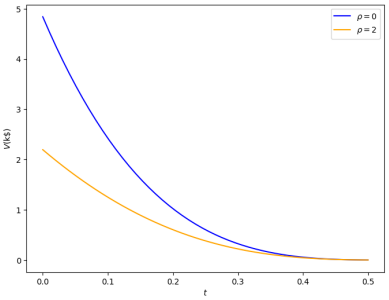
We perform two different comparisons between the Hawkes and Poisson cases



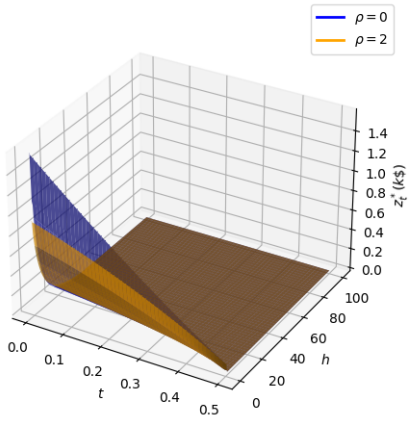
(a) Value function $V(t, \lambda, h)$ for $\lambda = 2.7$.



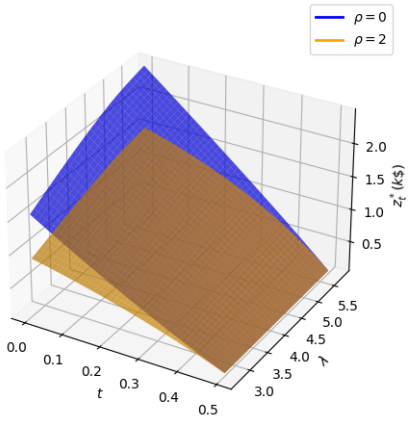
(b) Value function $V(t, \lambda, h)$ for $h = 0$.



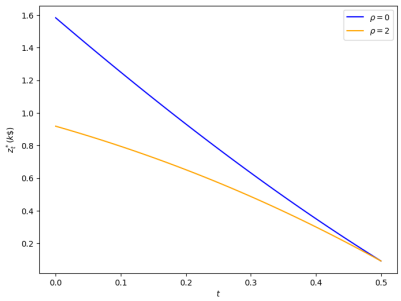
(c) Value function $V(t, \lambda, h)$ for $\lambda = 2.7, h = 0$.



(d) Optimal control $z_t^*(, \lambda, h)$ for $\lambda = 2.7$.

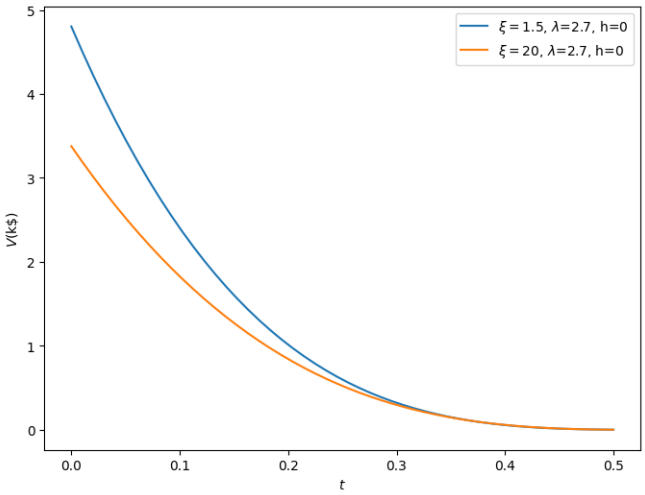


(e) Optimal control $z_t^*(\lambda, h)$ for $h = 0$.

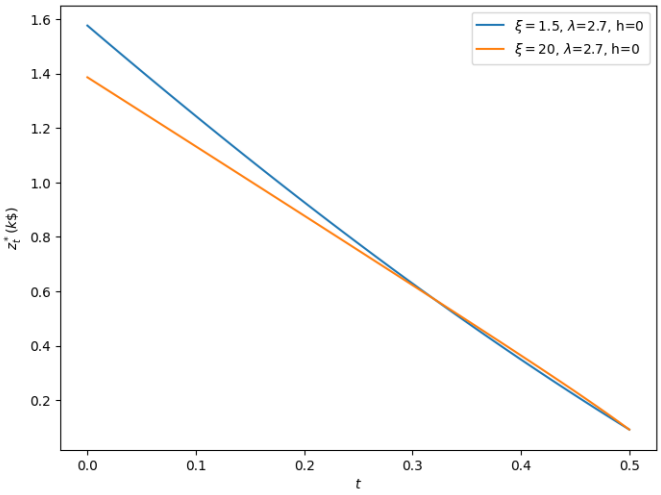


(f) Optimal control $z_t^*(\lambda, h)$ for $\lambda = 2.7, h = 0$.

Fig. 4: Value function and optimal control varying the decaying rate ρ.

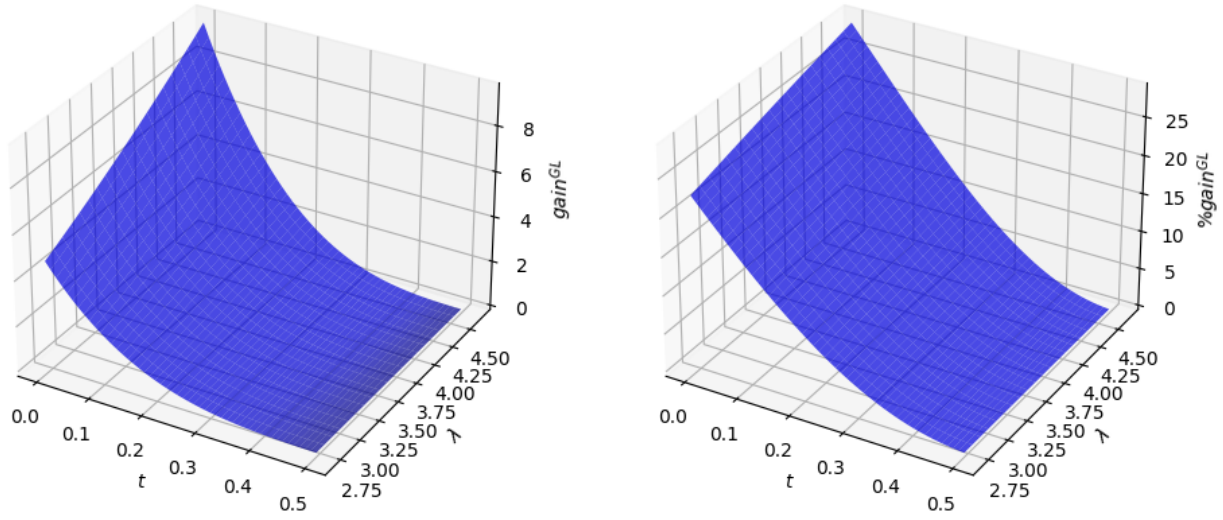


(a) Value function for different ξ, $\lambda = 2.7, h = 0$.



(b) Optimal control for different ξ, $\lambda = 2.7, h = 0$.

Fig. 5: Value function and optimal control varying ξ, for fixed h and λ.



(a) $\text{gain}^{\text{GL}}(t, \lambda)$ (b) $\%\text{gain}^{\text{GL}}(t, \lambda)$

Fig. 6: Gain and percentage of gain with respect to the Gordon-Loeb static strategy, as defined in Eqs. (17), (18).

1) A Poisson process having the same intensity as the Hawkes baseline intensity:

$$\lambda_b^P = \lambda_0 = 2.7. \tag{20}$$

2) A Poisson process P and a Hawkes process N such that

$$\mathbb{E}[P_T] = \mathbb{E}[N_T].$$

In particular, we choose λ_e^P such that

$$\lambda_e^P = \frac{\lambda_0 \xi}{\xi - \beta} + \frac{1}{T(\xi - \beta)}(\lambda_0 - \frac{\lambda_0 \xi}{\xi - \beta})(1 - e^{-\xi T}) = 3.25, \tag{21}$$

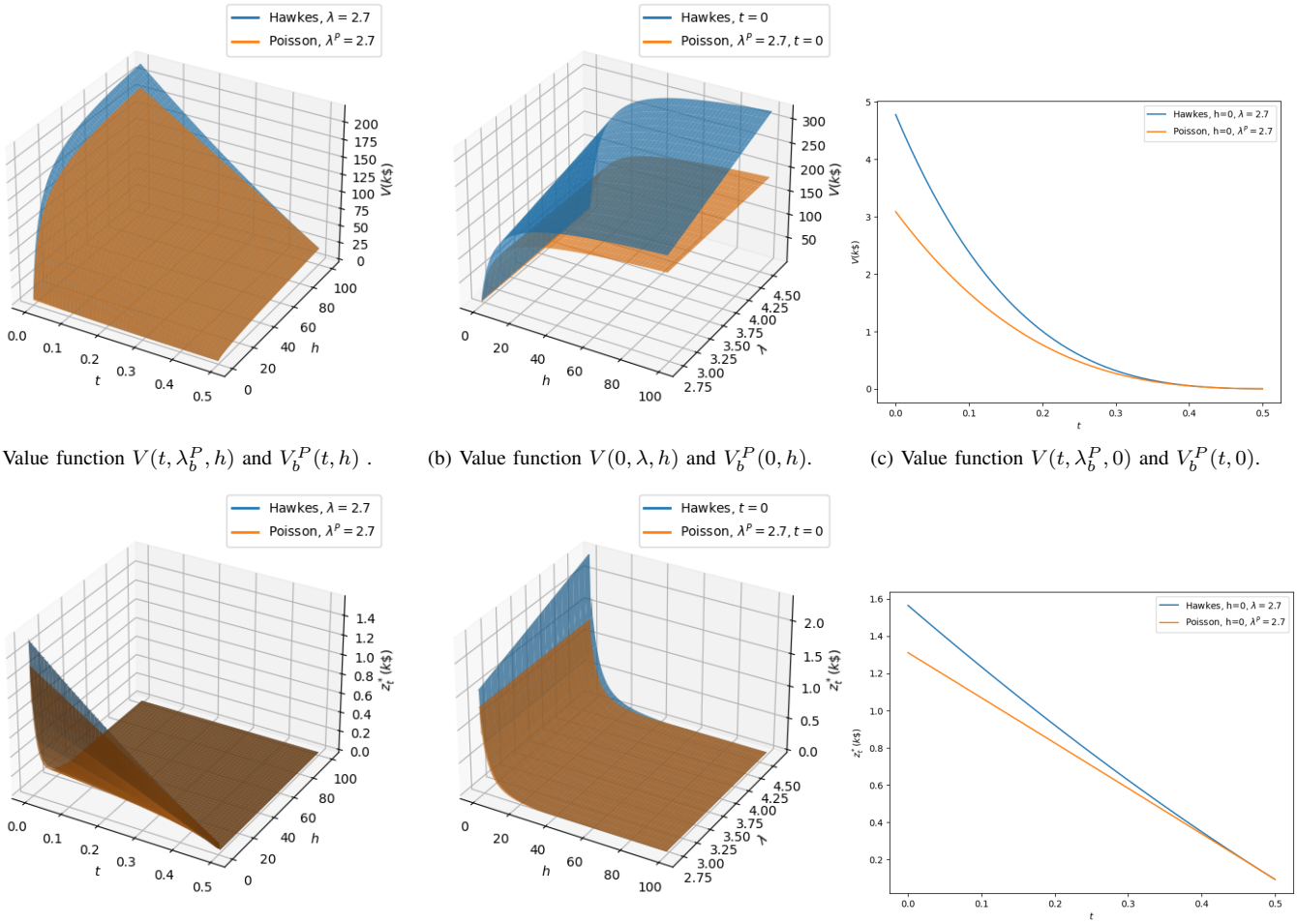
with the parameters choice in Tables II, III.

The first can be interpreted as the case where the entity underestimates the probability of arrival of attacks (e.g. it estimates the number of attacks using data from a non-representative time frame) and assumes it to have a constant behavior. The second experiment represents the case in which the entity estimates correctly the intensity on average, but assumes it to have a constant behavior. We recall the following notation:

- V_b^P is the value function for the Poisson problem, Eq. (19), computed with fixed intensity λ_b^P, as defined in Eq. (20) and z_b^{P*} is the associated optimal control.
- V_e^P is the value function for the Poisson problem, Eq. (19), computed with fixed intensity λ_e^P, as defined in Eq. (21) and z_e^{P*} is the associated optimal control.
- V is the value function associated to the PIDE in Eq. (15) and z^* is the associated optimal control.

For Comparison 1, we refer to Figure 7. In Subfigure 7a, we observe the Hawkes value function $V(t, \lambda, h)$ evaluated in λ_b^P, compared with the Poisson value function $V_b^P(t, h)$ and in Subfigure 7d we depict the corresponding optimal controls. In Subfigures 7b and 7e, we compare the value function and optimal control, varying λ and h at time $t = 0$. Since $V_b^P(0, h)$ does not depend on λ, so we assume it to be constant for every λ. In Subfigures 7c, 7f, we compare the value function and control, fixing $\lambda = \lambda_b^P$ and $h = 0$. We observe that, in the same baseline case, considering Hawkes processes instead of Poisson's causes a larger value function and optimal control. This is reasonable, since $\lambda_t \geq \lambda_b^P$ thus it leads to a larger risk and, consequently, it forces us to invest more due to the higher rate of attack arrival. This result is consistent with the observations in Section V-A.

For Comparison 2, we refer to Figure 8. In Subfigure 8a, we observe the Hawkes value function $V(t, \lambda, h)$ evaluated in λ_e^P, compared with the Poisson value function $V_e^P(t, h)$ and in Subfigure 8d we depict the corresponding optimal controls. In Subfigures 8b and 8e, we compare the value function and optimal control, varying λ and h at time $t = 0$. Since $V_e^P(0, h)$ does not depend on λ, we assume that it is constant for every λ. In Subfigures 8c, 8f, we compare the value function and control, fixing $\lambda = \lambda_e^P$ and $h = 0$. Also in this case, we note that the value function and optimal control, evaluated in λ_e^P are in general larger than the same functions computed for the Poisson case. However, observing Subfigures 8b and 8e, we notice that Hawkes value function and control are close to the Poisson's ones for small values of λ, and the distance between them increases as λ increases. This behavior is interesting as



(a) Value function $V(t, \lambda_b^P, h)$ and $V_b^P(t, h)$.

(b) Value function $V(0, \lambda, h)$ and $V_b^P(0, h)$.

(c) Value function $V(t, \lambda_b^P, 0)$ and $V_b^P(t, 0)$.

(d) Optimal control $z_t^*(\lambda, h)$ for $\lambda = 2.7$.

(e) Optimal control $z_t^*(\lambda, h)$ for $t = 0$.

(f) Optimal control $z_t^*(\lambda, h)$ for $\lambda = 2.7, h = 0$.

Fig. 7: Comparison between Hawkes and Poisson, $\lambda_b^P = 2.7$.

in the case of Comparison 2 it is not always true that $\lambda_t \geq \lambda_e^P$. This result suggests that considering Poisson processes instead of Hawkes processes, i.e., ignoring dynamic intensity, could lead to insufficient investment by the entity, i.e., sub-optimal protection.

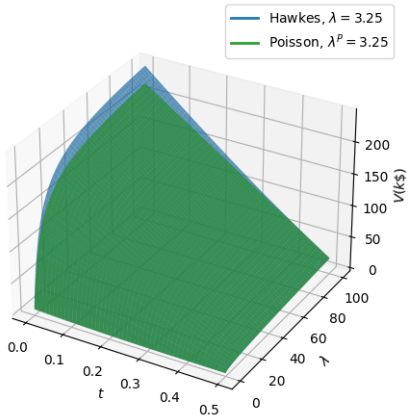
1) Optimal control along a trajectory: As a further numerical experiment, we would like to capture how the optimal control behaves along a particular trajectory of the intensity λ. We refer to Algorithm 2 to show how to associate a specific trajectory $(\lambda_t(\omega))_{t\in[0,T]}$ with the corresponding optimal control. The parameters used to implement Algorithm 2 are the following, specified in Table V

$h_{\min}$	$h_{\max}$	Δh	$\lambda_{\min}$	$\lambda_{\max}$	$\Delta\lambda$	t_{init}	H_{init}	$\lambda_t(\omega)$
0.5	20	0.5	2.7	10.8	0.02	0	2	$\lambda_t(\omega)$

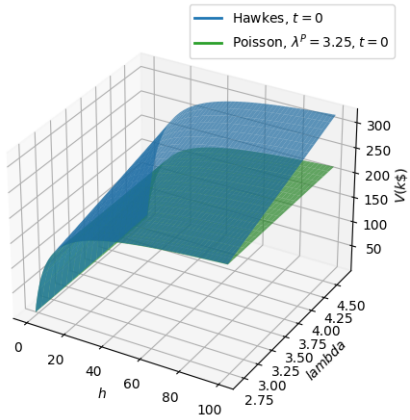
TABLE V: Algorithm 2 parameters for Section V-D1.

In Subfigures 9a, 9c we depict two different trajectories for Hawkes intensity, together with Poisson intensities λ_b^P, λ_e^P, as defined in Section V-D. In Subfigures 9b, 9d we show the corresponding optimal control for the Hawkes' and the Poisson's cases.

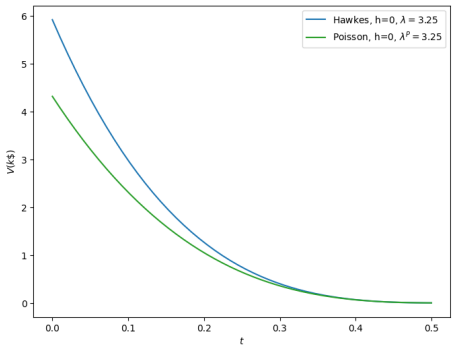
Around the Hawkes' jump times (grey dotted lines), we tipically observe a jump also along the optimal control. The optimal control for Hawkes is always larger than the optimal control for the Poisson process having intensity λ_b^P. This is reasonable since, as claimed in Section V-D, $\lambda_t \geq \lambda_b^P = \lambda_0$. Comparing the optimal control for the Hawkes and Poisson having intensity λ_e^P, we observe that in the beginning, the optimal control for the Hawkes is slightly smaller than the optimal control for the Poisson. However, after the first jump, the optimal control for the Hawkes becomes larger. We highlight in cyan, the time for which $\lambda_t(\omega) > \lambda_e^P$. Whenever $\lambda_t \geq \lambda_e^P$, the optimal control for the Hawkes remains larger than the Poisson's one. Unexpectedly, in Subfigure 9d, we observe that also when $\lambda_t < \lambda_e^P$, we might have that $z^*(t, \lambda_t(\omega), h) > z_e^{P*}(t, h)$.



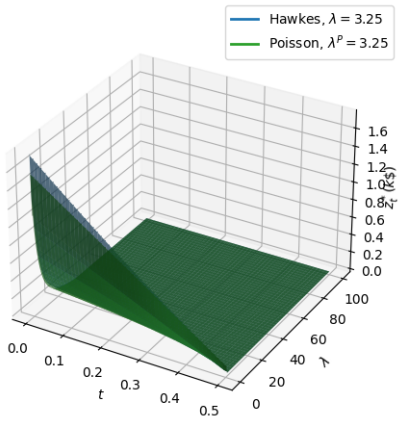
(a) Value function $V(t, \lambda, h)$ for $\lambda = 3.25$.



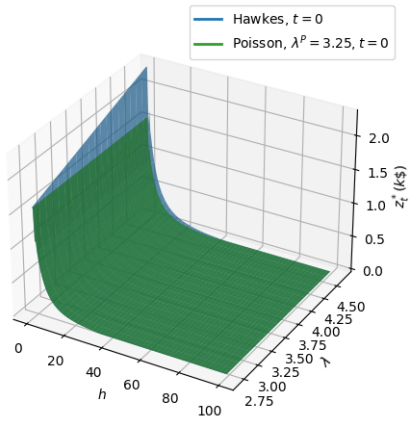
(b) Value function $V(t, \lambda, h)$ for $t = 0$.



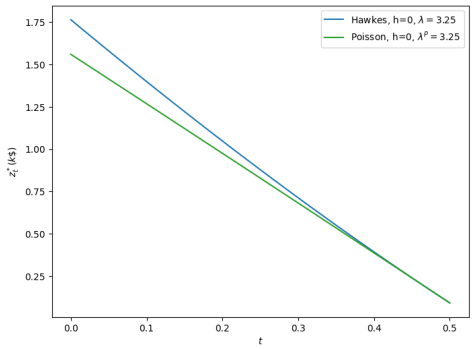
(c) Value function $V(t, \lambda, h)$ for $\lambda = 3.25, h = 0$.



(d) Optimal control $z_t^*(\lambda, h)$ for $\lambda = 3.25$.



(e) Optimal control $z_t^*(\lambda, h)$ for $t = 0$.



(f) Optimal control $z_t^*(\lambda, h)$ for $\lambda = 3.25, h = 0$.

Fig. 8: Comparison between Hawkes and Poisson, $\lambda_e^P = 3.25$.

VI. Conclusions

In this paper, we provide a dynamic version of the Gordon-Loeb model, exploiting instruments such as compound counting processes to describe the overall losses experienced by the entity and Hawkes processes to represent the cyber-attack arrivals. We then formulate an optimization problem which respect the cost-benefit tradeoff proposed in the original Gordon-Loeb setting and solve it with dynamic programming techniques. We characterize the solution via a partial-integro-differential equation that we solve numerically. We then perform some numerical tests, to study the main properties of the optimal investment strategy and to compare our Hawkes setting with a Poisson one. We realize that not considering a dynamic intensity instead of a constant one might leads to a sub-optimal investment rate. Interesting next research directions could be a more detailed investigation of the value function properties in particular the existence of a solution (in a suitable sense) to the PIDE and the verification theorem. As possible future investigation, we would also like to include in the model a utility function and see how it influences the optimal control. Moreover, we would also like to explore a scenario in which the entity may also enter into an insurance contract to cover losses from cyber-attacks. We may then study the optimal allocation of the entity's resources in security and insurance.

References

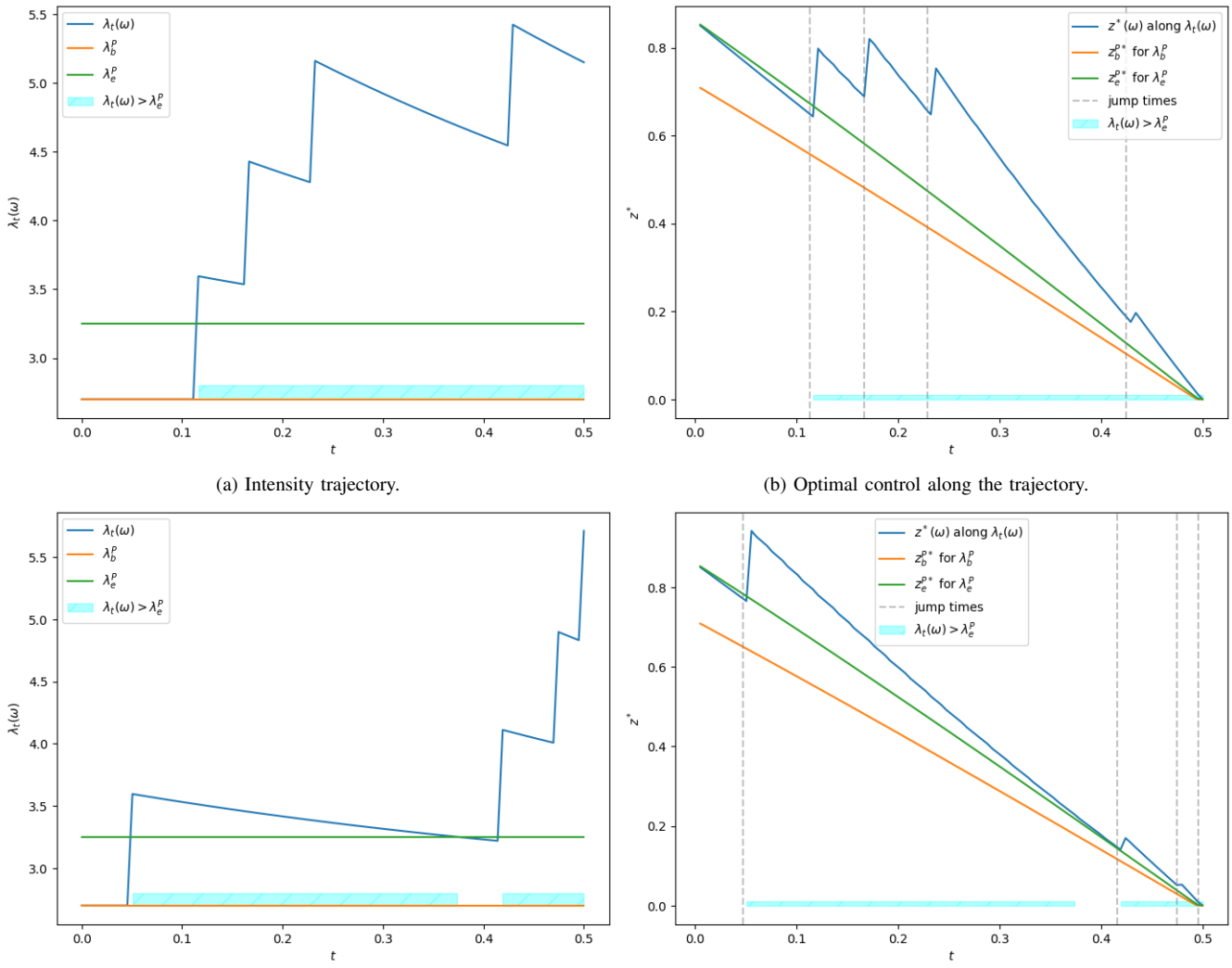
[1] Kerstin Awiszus, Thomas Knispel, Irina Penner, Gregor Svindland, Alexander Voß, and Stefan Weber, *Modeling and pricing cyber insurance: Idiosyncratic, systematic, and systemic risks*, European Actuarial Journal **13** (2023), no. 1, 1–53.

[2] Adrian Baldwin, Iffat Gheyas, Christos Ioannidis, David Pym, and Julian Williams, *Contagion in cyber security attacks*, Journal of the Operational Research Society **68** (2017), no. 7, 780–791.

[3] Alain Bensoussan and Benoit Chevalier-Roignant, *Stochastic control for diffusions with self-exciting jumps: An overview*, Mathematical Control and Related Fields **14** (2024), no. 4, 1452–1476.

[4] Yannick Bessy-Roland, Alexandre Boumezoued, and Caroline Hillairet, *Multivariate Hawkes process for cyber insurance*, Annals of Actuarial Science **15** (2021), no. 1, 14–39.

[5] Bruno Bouchard, *Introduction to stochastic control of mixed diffusion processes, viscosity solutions, and applications in finance and insurance*, Lecture Notes, 2007.



(a) Intensity trajectory.

(b) Optimal control along the trajectory.

(c) Intensity trajectory.

(d) Optimal control along the trajectory.

Fig. 9: Optimal control along a trajectory.

[6] Alexandre Boumezoued, Yousra Cherkaoui, and Caroline Hillairet, *Cyber risk modeling using a two-phase Hawkes process with external excitation*, arXiv preprint arXiv:2311.15701 (2023).

[7] Rama Cont and Ekaterina Voltchkova, *A finite difference scheme for option pricing in jump diffusion and exponential lévy models*, SIAM Journal on Numerical Analysis **43** (2005), no. 4, 1596–1626.

[8] Harald Cramér, *On the mathematical theory of risk*, Skandia Jubilee **4** (1930).

[9] Angelos Dassios and Hongbiao Zhao, *Exact simulation of hawkes process with exponentially decaying intensity*, Electronic Communications in Probability **18** (2013), no. 62, 1–13.

[10] Lawrence A. Gordon and Martin P. Loeb, *The economics of information security investment*, ACM Transactions on Information and System Security (TISSEC) **5** (2002), no. 4, 438–457.

[11] Ernst Hairer, Syvert Paul Nørsett, and Gerhard Wanner, *Solving ordinary differential equations ii: Stiff and differential-algebraic problems*, Solving Ordinary Differential Equations II: Stiff and Differential-algebraic Problems, Springer, 1993.

[12] Alan G. Hawkes, *Spectra of some self-exciting and mutually exciting point processes*, Biometrika **58** (1971), no. 1, 83–90.

[13] Kiyosi Itô, *On a formula concerning stochastic differentials*, Nagoya Mathematical Journal **3** (1951), 55–65.

[14] Philip Low, *Insuring against cyber-attacks*, Computer Fraud & Security **2017** (2017), no. 4, 18–20.

[15] Filip Lundberg, *Approximerad Framställning af Sannolikhetsfunktionen: Återförsäkring af Kollektivrisker*, Ph.D. thesis, Almqvist & Wiksell, 1903.

[16] _____, *Försäkringsteknisk riskutjämning: Teori*, F. Englunds Boktryckeri A.B., Stockholm, 1926.

[17] Vathana Ly Vath, Simone Scotti, et al., *Optimal harvesting under uncertain environment with clusters of catastrophes*, SSRN: https://ssrn.com/abstract=4914119 (2024).

[18] Alessandro Mazzoccoli and Maurizio Naldi, *Robustness of Optimal Investment Decisions in Mixed Insurance/Investment Cyber Risk Management*, Risk analysis **40** (2020), no. 3, 550–564.

[19] Yosra Miaoui and Noureddine Boudriga, *Enterprise security economics: A self-defense versus cyber-insurance dilemma*, Applied Stochastic Models in Business and Industry **35** (2019), no. 3, 448–478.

[20] Henry R.K. Skeoch, *Expanding the Gordon-Loeb model to cyber-insurance*, Computers & Security **112** (2022), 102533.

[21] Ken-ichi Tatsumi and Makoto Goto, *Optimal Timing of Information Security Investment: A Real Options Approach*, Economics of information security and privacy, Springer, 2010, pp. 211–228.

[22] Abraham Wald, *Some Generalizations of the Theory of Cumulative Sums*

of Random Variables, The Annals of Mathematical Statistics **16** (1945), no. 3, 287–293.

[23] Si Yuan, *ODE-oriented semi-analytical methods*, Computational Mechanics in Structural Engineering (1999), 375–388.

[24] Chunming Zhang, Luxing Yang, Jianguo Ren, Chenquan Gan, and Qingyi Zhu, *Mathematical Models for New Types of Cyberattack and Associated Defence Strategies*, Security and Communication Networks (2024), Special Issue.