Mémoire présenté devant le jury de l'EURIA en vue de l'obtention du Diplôme d'Actuaire EURIA et de l'admission à l'Institut des Actuaires

le 25 Septembre 2019

Par : Yannick Bessy-Roland
Titre : Modélisation stochastique individuelle de sinistres cyber

Confidentialité : Non

Les signataires s'engagent à respecter la confidentialité indiquée ci-dessus

Membre présent du jury de l'Institut des Actuaires :
Romain Laïly
Anthony Nahelou
Anne Bontoux
Bastien Potentier
Signature :

Entreprise :
Milliman
Signature :

Membres présents du jury de l'EURIA :
Franck Vermet

Directeur de mémoire en entreprise :
Alexandre Boumezoued
Signature :

Invité :

Signature :

Autorisation de publication et de mise en ligne sur un site de diffusion de documents actuariels
(après expiration de l'éventuel délai de confidentialité)

Signature du responsable entreprise :

Signature du candidat :

EURIA
EURo Institut
d'Actuariat

6, avenue le Gorgeu
CS 93837
29238 Brest Cedex 3

T +33 (0)2 98 01 66 55
euria@univ-brest.fr

Résumé

L'interconnexion des systèmes informatiques entre les entreprises fait des cyberattaques un risque de contagion, or les outils actuariels classiques permettent di□cilement de modéliser ce phénomène, ainsi ce mémoire se penche sur la modélisation de la fréquence des cyberattaques, par les processus dits de Hawkes, dans le cas particulier des violations de données, et ce, d'un point de vue assurantiel. Ces processus permettent notamment de modéliser des phénomènes d'excitation et de dépendance. Après une présentation et une contextualisation du cyber-risque en assurance, les travaux se tournent vers une étude de la capacité des processus de Hawkes à modéliser ce risque dans le cas des violations de données. Il s'ensuit la détermination d'une prime pure, d'assurance et de réassurance, pour une garantie violation de données.

La dernière partie de ce mémoire propose une méthode de provisionnement individuel avec des processus de Hawkes, afin de déterminer un nombre d'IBNR (Incurred But Not Reported). Cela permet de répondre aux limites du cas plus classique Poissonnien qui ne permet pas de modéliser des e□ets de dépendance et d'excitation, tout en profitant des avantages des modèles individuels. Les travaux se penchent tout particulièrement sur une méthode d'estimation de la fonction de vraisemblance qui s'avère incalculable en pratique. Cette dernière partie se clôt avec une application du modèle sur une base recensant des violations de données, qui, comme d'autres risques plus classiques, présentent des délais de déclaration, qui engendrent la présence d'IBNR.

Mots clefs: Processus de Hawkes, Cyber-risque, Micro-level, IBNR, Provisionnement stochastique individuel, Vol de données

Abstract

The interconnection of computer systems between companies makes cyber attacks a risk of contagion, yet traditional actuarial tools make it difficult to model this phenomenon, so this paper examines the modelling of the frequency of cyber attacks, by the so-called Hawkes processes, in the particular case of data breaches, from an insurance point of view. These processes make it possible to model excitation and dependence phenomena. After a presentation and contextualization of cyber-risk in insurance, the work turns to a study of the ability of Hawkes processes to model this risk in the case of data breaches. This results in the determination of a pure insurance and reinsurance premium for a data breach coverage.

The last part of this paper proposes an individual reserving method with Hawkes processes, in order to determine a number of IBNR (Incurred But Not Reported). This makes it possible to respond to the limitations of the more traditional Poissonnian case, which does not allow the modelling of dependence and excitation effects, while taking advantage of the advantages of individual models. The work focuses on a method for estimating the likelihood function that is incalculable in practice. This last part ends with an application of the model on data breaches, which, like other more traditional risks, present reporting delays, which lead to the presence of IBNR.

Keywords: Hawkes processes, Cyber-risk, Micro-level, IBNR, Individual claims reserving, Data breach

Remerciements

En premier lieu je souhaite remercier mon tuteur de stage, Alexandre Boumezoued, pour m'avoir proposé ce sujet passionnant, ainsi que pour ses précieux conseils, cela a été un véritable plaisir de travailler sur ce thème.

Mes remerciements vont également à mon second tuteur Mohamed Benkhalfa pour ses conseils avisés.

Je remercie également ma tutrice EURIA, Madame Isabelle Devine pour son suivi régulier, et ses différents apports qui m'ont beaucoup aidés pour la rédaction de ce mémoire.

Je tiens de la même façon à remercier Charlène Bessy-Roland, Alexis Sorignon, Dimitri Delcaillau ainsi que Alice Launay pour leur relecture.

Finalement je remercie tous ceux qui ont pu contribuer d'une façon ou d'une autre à ce mémoire, je remercie notamment Madame Caroline Hillairet, ainsi que toute l'équipe R&D de Milliman.

Note de synthèse

Bien que la cyber-assurance existe depuis la fin des années 1990, le marché est encore en pleine évolution en Europe avec des montants de primes brutes qui, en 2017, selon Marsh avaient un potentiel de croissance estimé entre 50% et 100% [1]. Le marché attendu pour 2020 serait entre 8 et 10 milliards d'après Morgan Stanley contre 3.5 milliards en 2018 [2]. Le cyber-risque, de par son évolution rapide et sa probabilité de survenance élevée est classé numéro un parmi les risques émergents (d'après le baromètre des risques émergents de la FFA) [3], ce baromètre le place également en deuxième place des opportunités pour le secteur de l'assurance.

Cependant ce risque présente des caractéristiques atypiques en matière de modélisation. D'une part au niveau du coût, avec des éléments souvent immatériels à évaluer, comme le coût d'une perte de réputation, le coût d'une donnée violée, ou encore le coût d'un arrêt de production. D'autre part au niveau de la fréquence, car le fait que la majorité des systèmes soient interconnectés crée un environnement global de risque avec des phénomènes de contagion et de dépendance.

Ce mémoire propose une modélisation de la fréquence et du coût des cyber-risques dans le cas particulier des violations de données. Une attention particulière est accordée à la fréquence qui y est modélisée par des processus de Hawkes, qui permettent de capter des phénomènes de contagion, d'excitation et donc de dépendance.

Deux majeures parties composent ce mémoire, la première consiste à évaluer la capacité des processus de Hawkes à modéliser la fréquence de survenance des violations de données ainsi qu'à la détermination d'une prime pure d'assurance et de réassurance pour une garantie violation de données. La seconde partie s'est penchée sur le développement d'une méthode de provisionnement individuel avec des processus de Hawkes, en présence d'IBNR. L'objectif étant de tenir compte, dans la modélisation, des biais d'observation dûs aux délais de déclaration. L'intérêt est en particulier de pouvoir provisionner des sinistres atypiques qui ne se modélisent pas correctement avec le classique processus de Poisson, le cyber-risque en fait partie.

1. Évoqué par [Orlando *et al.*, 2017]
2. Évoqué dans : http://us.milliman.com/insight/2019/Could-cyber-risk-be-the-next-Big-Short/
3. Baromètre des risques émergents de la FFA : https://www.ffa-assurance.fr/sites/default/files/files/2019/02/20190206_-_barometre_2019_des_risques_emergents.pdf

Présentation de la base de données et motivations

Base de données

Nous avons étudié la base de données publique Privacy Rights ClearingHouse, (PRC), elle recense plus de 9000 violations de données aux États-Unis depuis 2005. Elle contient notamment les dates auxquelles les violations se sont produites, les types d'attaques utilisés, les types d'organisations attaquées, les états concernés ainsi que le nombre de données violées. Nous avons e□ectué des regroupements par types d'attaques ainsi que par types d'organisations, afin de disposer de groupes su□samment robustes pour les études qui suivent, ces regroupements se sont basés sur des critères de similitudes des groupes d'origine. Ces informations sont résumées ci-dessous :

Regroupement	Origine	Description
OTHER	CARD	Fraude impliquant des cartes de paiements, autre que du Hack
OTHER	INSD	Insider : quelqu'un qui a légitimement accès aux données les enfreint intentionnellement (employé, client, sous traitant, etc.)
HACK	HACK	Piratage ou logiciels malveillants
THEFT/LOSS	PHYS	Documents papiers (non électroniques), perdus ou volés
THEFT/LOSS	PORT	Ordinateurs portables, clef USB, smartphones, disques dur etc., perdus ou volés
THEFT/LOSS	STAT	Ordinateur non portable perdu, volé ou accédé de façon inappropriée
DISC	DISC	Divulgation non intentionnelle : par exemple informations di□usées publiquement ou envoyées à la mauvaise personne

Table 1 – Types d'attaques de la PRC

Regroupement	Origine	Description
BUSINESSES	BSF	Entreprises - Services financiers et assurances
BUSINESSES	BSO	Entreprises - Autres
BUSINESSES	BSR	Commerces-Détaillants / Marchands - Comprend le commerce de détail en ligne
OTHERORGA	EDU	Établissements d'enseignement
OTHERORGA	GOV	Gouvernement et armée
OTHERORGA	ONG	Organismes à but non lucratif
MED	MED	Fournisseurs de soins de santé et d'assurance médicale

Table 2 – Types d'organisations de la PRC

Des regroupements ont également été e□ectués pour les États en conservant tels quels les plus représentés, à savoir : California (15.7%), Texas (6.9%) et New-York (6.3%), et en regroupant les autres dans un groupe nommé OTHER. [4]

Motivations

Outre les motivations qui sont de constater que les systèmes sont interconnectés, et présentent donc un risque de contagion, deux motivations quantitatives nous ont dirigés vers les processus de Hawkes :

La première est le rejet de l'hypothèse Poissonnienne, le processus de Poisson étant un processus classique de modélisation. Deux tests ont été e□ectués, un test d'indépendance des inter-temps de survenance (Ljung-Box) ainsi qu'un test d'adéquation des inter-temps à la loi exponentielle (Kolmogorov-Smirnov), les deux hypothèses sont rejetées avec une p-value très faible (<2.2e-16).

La seconde, et principale motivation est la présence d'autocorrélation du nombre d'attaques au sein de la base de données. Plus précisément, en traçant le nombre d'attaques survenues un mois m+1 en fonction du nombre d'attaques survenues dans le mois précédent m, et ce, au sein du même type d'attaque (types cités précedemment) nous obtenons un coe□cient de corrélation linéaire de 0.6548 qui indique donc une corrélation significative.

Parmi les choix possibles pour modéliser un tel phénomène se trouve le processus de Hawkes, outre cet argument, il a été choisi d'une part car il permet également de modéliser des phénomènes d'excitation, et d'autre part car il possède une interprétation naturelle, qui donne de l'information sur le phénomène.

Les processus de Hawkes

Le processus de Hawkes est un processus de comptage, au même titre que le processus de Poisson. Sa caractéristique principale réside dans son intensité conditionnelle, celle-ci représente le risque instantané qu'une attaque survienne, sachant le passé du processus. Plus simplement, l'intensité conditionnelle joue, par exemple, le même rôle que l'intensité du processus de Poisson, la di□érence est qu'elle est conditionnée au passé, et est donc elle-même un processus aléatoire. Le processus de Hawkes la définit de la façon suivante :

$$\lambda(t) = \mu(t) + \int_{]\ 1\ ;t[} \phi(t \quad s) dN_s = \mu(t) + \sum_{T_n < t} \phi(t \quad T_n)$$

Avec $\mu(.)$ et $\phi(.)$ des fonctions déterministes, positives, et $(N_t)_{t\ 0}$ le processus de Hawkes. La propriété auto-excitante réside dans la somme sur les T_n qui sont les temps

4. La base est disponible à l'adresse : https://www.privacyrights.org/data-breaches, elle a récemment fait l'objet d'une étude par [Farkas *et al.*, 2019].

de survenance ordonnés du processus. $\mu(.)$ est un risque de base, indépendant des évènements survenus, en particulier si le noyau ϕ est nul, le processus est un processus de Poisson inhomogène de taux $\mu(.)$.

Le processus de Hawkes s'étend au cas multivarié, en considérant d processus, l'intensité du i-ème processus est définie de la sorte :

$$\lambda^{(i)}(t) = \mu^{(i)}(t) + \sum_{j=1}^{d} \int_{]-1;t[} \phi_{i;j}(t-s) dN_s^{(j)} = \mu^{(i)}(t) + \sum_{j=1}^{d} \sum_{T_n^{(j)} < t} \phi_{i;j}(t - T_n^{(j)})$$

avec $\mu^{(i)} : \mathbb{R}^+ \to \mathbb{R}^+$
$\phi_{i;j} : \mathbb{R}^+ \to \mathbb{R}^+$

Dans ce cas, pour $1 \leq i, j \leq d$, $\phi_{i;j}$ représente l'impact du processus $(N_t^{(j)})_{t \geq 0}$ sur l'intensité $(\lambda_t^{(i)})_{t \geq 0}$ du processus $(N_t^{(i)})_{t \geq 0}$. Ce sont donc non seulement des phénomènes d'auto-excitation qui sont modélisés ($i = j$) mais également d'inter-excitation ($i \neq j$).

Les processus de Hawkes sur une segmentation fine

Modèle

La première application effectuée a consisté en l'étude des capacités prédictives du processus de Hawkes sur une segmentation fine de la base de données. La segmentation retenue est celle qui consiste à croiser les variables type d'attaque, type d'organisation et État, en mettant les segments trop peu représentés dans un segment nommé OTHER. Cela mène à six segments retenus.

L'étude s'est effectuée avec trois types de noyaux différents :
— Noyau 1 : $\phi_{i;j}(a) = \alpha_{i;j} \exp(-\beta_i a)$
— Noyau 2 : $\phi_{i;j}(a) = \alpha_{i;j} \exp(-\beta_{i;j} a)$
— Noyau 3 : $\phi_{i;j}(a) = \alpha_{i;j} a \exp(-\beta_i a)$

L'intensité de fond choisie est un *drift* linéaire : $\mu_i(t) = \mu_{0;i} + \gamma_i t$, afin de prendre en compte d'éventuelles tendances. Cela mène, au total à un nombre de 54 paramètres pour les noyaux 1 et 3, et 84 paramètres pour le noyau 2. Ces modèles sont donc relativement complexes.

Une étude parallèle a été menée, consistant à réduire la complexité du processus en pénalisant la fonction de vraisemblance, afin d'observer s'il est possible d'améliorer les capacités prédictives de cette façon. La pénalisation prend la forme suivante :

$$\log L(\mu, \phi)_{penalise} = \log L(\mu, \phi) + \gamma \sum_{1 \leq i;j \leq d} |\alpha_{i;j}|$$

où $\gamma \geq 0$ est le coefficient de pénalisation et $L(\mu, \phi)$ est la vraisemblance du processus de Hawkes, avec $\mu = (\mu_{i;0}, \gamma_i)_{1 \leq i \leq d}$ et $\phi = (\alpha_{i;j}, \beta_{i;j})_{1 \leq i;j \leq d}$. Cette pénalisation correspond à

une méthode de type Lasso que nous avons privilégiée face à une méthode de type Ridge, car elle permet aux coe□cients pénalisés de prendre exactement la valeur 0. Autrement dit, cela permet au modèle de faire ressortir les interactions principales.

Résultats

Les modèles ont été comparés de la façon suivante : ils ont été calibrés sur la période 2011-2015 pour prédire le nombre d'attaques en 2016, ainsi que sur 2011-2016 pour prédire le nombre d'attaques en 2017. La mesure de comparaison est la somme des valeurs absolues des di□érences, sur chaque segment, entre le nombre prédit et le nombre réel d'attaques. Les résultats sont les suivants :

γ	0	100	600	900	3000	6000
Noyau 1 (2016)	337.6614	280.7602	277.7764	283.5881	973.0103	1135.5217
Noyau 1 (2017)	170.3384	249.4687	240.4258	261.7280	732.0155	792.7558
Noyau 2 (2016)	259.4504	282.2328	202.7125	180.3729	256.7397	430.4255
Noyau 2 (2017)	127.3343	160.8886	159.4488	141.6603	148.1485	346.4559
Noyau 3 (2016)	201.7575	285.1470	262.0646	283.1685	502.2474	1559.1263
Noyau 3 (2017)	165.6958	183.2997	254.2543	172.6621	3168.8662	6402.4315

Table 3 – Somme sur les six segments, des écarts absolus entre l'espérance du nombre d'attaques prédits (en 2016 et 2017) et le nombre réel, en fonction du paramètre de pénalisation γ.

Ces résultats semblent montrer qu'il est di□cile de sélectionner un modèle sur sa capacité prédictive, les meilleurs modèles ne sont en e□et pas les mêmes d'une année sur l'autre. La pénalisation dans certains cas permet bien d'améliorer les capacités prédictives.

Finalement un des meilleurs compromis sur les deux années est le noyau 3 non pénalisé. Les distributions prédites par ce modèle pour l'année 2016 contiennent le réel pour quatre segments sur six. Sur 2017 les distributions contiennent toutes le réel mais pour l'une d'entre elles, au-delà de son quantile 99.5%, ce qui signifie que la valeur réelle est hautement improbable sous ce modèle. Le noyau 3 est également le meilleur compromis en terme de vraisemblance. Les tests statistiques d'adéquation du processus aux données sont en majorité concluants (9 sur 12 acceptés au seuil de 5%). Ces résultats mettent en évidence qu'une excitation latente (noyau 3) représente mieux les données, ce qui n'est pas le cadre exponentiel classique des processus de Hawkes (noyaux 1 et 2). Bien que ces résultats soient encourageants, la complexité du modèle mène à considérer une segmentation moins fine pour les applications qui suivent.

Tarification d'une garantie violation de données

La tarification s'est déroulée en trois temps, le choix d'une segmentation, la détermination du modèle de fréquence ainsi que celle du modèle de coût.

Segmentation : di□érentes segmentations, moins fines que la précédente ont été testées, ces segmentations ont été choisies sur des critères de bon sens (Ex : un type d'attaque = un segment) ainsi que de similitudes statistiques. Elles ont été comparées sur le critère de la validation des tests statistiques d'adéquation des processus de Hawkes. La segmentation retenue est la segmentation par types d'organisations, à savoir les trois segments : MED (médical, santé), BUSINESSES et OTHER, qui n'est rejetée par aucun test à 5%.

Modèle de fréquence : en parallèle du processus de Hawkes, un autre type de modèle de fréquence a été testé, qui consiste à modéliser le nombre journalier d'attaques par une loi binomiale négative pour les deux premiers segments, et par un GLM binomial négatif pour le segment OTHER afin de prendre en compte une tendance dans le temps, qui est évidente graphiquement. Ces modèles ont été choisis parmi plusieurs autres (Poisson, géométrique, etc.), sur des critères de qualité d'ajustement, statistique (test du khi-deux) et graphique (diagrammes quantiles-quantiles).

Modèle de coût : il a pour but de modéliser deux phénomènes : le premier est qu'une attaque n'a pas les mêmes probabilités de violer un certain nombre de données selon le segment, le second est que le coût d'une donnée violée évolue avec le nombre total de données violées. Pour cela des lois continues ont été sélectionnées afin de modéliser le logarithme de la distribution du nombre de données violées par segment (deux lois Gamma et une loi logistique) et un modèle linéaire du type log(Coût total) = a + b log(Nombre de données violées), présent dans la littérature, a été retenu afin de modéliser le second phénomène évoqué ci-dessus.

Résultats : Les distributions prédites du nombre d'attaques par segment, pour 2017, contiennent toutes le réel, et ce pour les deux méthodes (Hawkes et distributions discrètes), hormis la distribution de OTHER dans le cas du GLM binomial négatif. Les primes obtenues dans le cas d'une garantie classique, sont résumées dans le tableau suivant, (le mémoire s'est également intéressé à une garantie plus élevée, accompagnée de réassurance). Les primes sont sensiblement proches excepté sur le dernier segment.

	BUSINESSES	MED	OTHERORGA
Prime pure Hawkes	975.43	5 629.92	759.27
Prime pure distribution discrètes	1048.32	5443.21	453.51

Table 4 – Primes pures obtenues, en dollars

Une comparaison avec des primes réelles met en évidence que celles obtenues ne sont pas dénuées de sens [5], cependant les primes réelles étudiées prennent en compte le chi□re d'a□aires de l'entreprise assurée, ainsi nos primes sont éloignées des primes de référence

5. Des exemples de primes sont donnés sur ce site : https://databreachinsurancequote.com/cyber-insurance/cyber-insurance-data-breach-insurance-premiums

quand le chi□re d'a□aires d'une entreprise est élevé. Prendre en compte ce facteur est une potentielle ouverture pour ce travail, qui pour l'instant considère le risque comme égal au sein d'un même secteur, quelle que soit l'entreprise.

Développement d'une méthode de provisionnement individuel avec les processus de Hawkes

Le principe de cette méthode est le suivant : les sinistres sont supposés survenir à des temps $(T_n)_{n\ 1}$ suivant un processus de Hawkes et sont modélisés de façon jointe avec leurs délais de reporting $(U_n)_{n\ 1}$, qui sont supposés suivre une loi $p_{Uj\mathcal{T}_n}$ (par exemple une loi exponentielle). Nous nous plaçons sur un horizon de temps d'observation $[0, \tau]$. Comme un assureur, en τ, ne peut observer que les temps d'occurrences tels que $T_n + U_n \quad \tau$, cela signifie qu'une partie des sinistres ne sont pas encore connus, ce sont les fameux IBNR (Incurred But Not Reported) qu'il est alors nécessaire de provisionner en fin d'année.

La problématique de cette section apparaît lors de l'écriture de la vraisemblance d'un tel modèle qui a la forme suivante :

$$L(\phi, \mu) = \exp\left(\int_0 \lambda(s) p_{Uj\mathcal{S}}([0, \tau \quad s])\mathrm{d}s \right) \prod_{n=1}^{n_\tau^R} \lambda\left(t_n^R\right) p_{Ujt_n^R}(u_n^R)$$

Cette vraisemblance dépend de λ, qui dépend de tous les temps passés du processus. En prenant les notations $(T_n^{IBNR})_{n\ 1}$ pour les sinistres IBNR et $(T_n^R)_{n\ 1}$ pour les sinistres observés, l'ensemble des sinistres $(T_n)_{n\ 1}$ se décompose en ces deux sous-ensembles, λ se réécrit alors sous la forme :

$$\lambda(s) = \mu(s) + \sum_{T_n < s} \phi(s \quad T_n) = \mu(s) + \sum_{t_n^R < s} \phi(s \quad t_n^R) + \sum_{T_n^{IBNR} < s} \phi(s \quad T_n^{IBNR})$$

Par construction, les IBNR $(T_n^{IBNR})_{n\ 1}$ ne sont pas connus, donc l'intensité λ n'est pas calculable, il en découle que la vraisemblance n'est pas calculable.

Cette section s'est alors orientée vers une méthode d'estimation de cette vraisemblance. La méthode a nécessité plusieurs approximations dans les calculs, di□érents tests ont alors été e□ectués afin de tester sa validité, parmi lesquels le suivant :

Des processus d'IBNR avec Hawkes ont été simulés pour 22 jeux de paramètres connus, puis les paramètres ont été estimés, sur ces simulations, par notre fonction de vraisemblance approchée. Des IBNR ont ensuite été simulés (par une méthode approchée encore une fois) sous ces paramètres. Les résultats sont que 18 distributions simulées sur les 22 cas, contiennent le nombre réel d'IBNR. Cette méthode n'est donc pas dénuée de sens malgré ses approximations.

D'autres tests ont été effectués comme la constatation graphique que le biais lié à l'observation est bien pris en compte, ou encore la mise en comparaison de notre modèle avec un modèle biaisé, en terme d'estimation de paramètres.

Cette section se clôt avec une application sur une base de données réelle (violation de données aux État-Unis), ainsi qu'une comparaison avec la méthode individuelle Poisson et la méthode de Mack. Sur cet exemple le modèle individuel de Hawkes semble un bon compromis entre les deux méthodes en terme de prédiction (distribution qui contient le réel) et de précision (variance peu élevée).

Conclusion

Ce mémoire met en évidence l'intérêt du processus de Hawkes pour modéliser la fréquence des violations de données, notamment avec sa capacité d'ajustement, et de prédiction.

Une méthode de tarification est présentée et semble faire sens en vue des primes réellement observées sur le marché. Cette méthode permet de prendre en compte l'environnement de risque global (phénomènes de contagion entre les entreprises) mais ne s'adapte pas au risque intrinsèque à l'entreprise outre la prise en compte de son secteur d'activité, cela pourrait faire l'objet de travaux futurs, par exemple pour prendre en compte le chiffre d'affaires de l'entreprise. La méthode présente l'avantage d'obtenir des distributions et donc beaucoup d'informations sur le risque (quantiles, variance, etc.).

La méthode de provisionnement développée en dernière partie semble faire sens malgré ses différentes estimations, des futurs travaux seraient de tenter de mieux justifier, et/ou de réduire le nombre de ces estimations. Une telle méthode permet de profiter des avantages des méthodes individuelles face aux méthodes agrégées, et notamment de modéliser des sinistres atypiques en profitant des caractéristiques du processus de Hawkes, les sinistres plus classiques sont également concernés en ce sens que le processus de Hawkes est une généralisation du processus de Poisson.

Les processus de Hawkes présentent toutefois quelques limites, une première limite est le nombre de paramètres qui croît rapidement avec la dimension du processus, une autre limite concerne la sensibilité du processus à la base utilisée, en effet, ce dernier est non seulement influencé par la base de données à travers les paramètres estimés, mais également à travers tout l'historique de la base, qui est pris en compte dans le passé du processus lors des simulations, ainsi la qualité des données est d'importance.

Une dernière limite (qui est également sa force) concerne le caractère inter-dépendant de ce processus. En effet, cela implique que la mauvaise calibration de certain segments influence nécessairement les autres segments.

Summary

Although cyber insurance has been around since the late 1990s, the market is still evolving in Europe with gross premium amounts that, in 2017, according to Marsh, had an estimated growth potential of between 50 percent and 100 percent [6]. The market expected for 2020 would be between 8 and 10 billion according to Morgan Stanley compared to 3.5 billion in 2018 [7]. Cyber-risk, due to its rapid evolution and high probability of occurrence, is ranked number one among emerging risks (according to the FFA Emerging Risk Barometer) [8], this barometer also places it in second place among the opportunities for the insurance sector.

However, this risk has atypical modelling characteristics. On the one hand, at the level of cost, with often intangible elements to be assessed, such as the cost of a loss of reputation, the cost of a violated data, or the cost of a production shutdown. On the other hand, the fact that most systems are interconnected creates a global risk environment with contagion and dependence.

This paper proposes a modeling of the frequency and cost of cyber risks in the particular case of data breaches. Particular attention is paid to the frequency modelled by Hawkes processes, which make it possible to capture phenomena of contagion, excitement and therefore dependence.

Two major parts of this paper are included, the first part is to assess the ability of Hawkes' processes to model the frequency of occurrence of data breaches and to determine a pure insurance and reinsurance premium for a data breach coverage. The second part focused on the development of an individual reserving method with Hawkes processes, in the presence of IBNR. The objective is to take into account, in the modelling, the observation biases due to reporting delays. The interest is in particular to be able to compute reserves for atypical claims that are not modeled correctly with the classic Poisson process, the cyber-risk is one of them.

6. mentioned in [Orlando *et al.*, 2017]
7. mentioned in : http://us.milliman.com/insight/2019/Could-cyber-risk-be-the-next-Big-Short/
8. FFA Emerging Risk Barometer : https://www.ffa-assurance.fr/sites/default/files/files/2019/02/20190206_-_barometre_2019_des_risques_emergents.pdf

Presentation of the database and motivations

Database

We studied the public Privacy Rights ClearingHouse (PRC) database, which has recorded more than 9,000 data breaches in the United States since 2005. It contains in particular the dates on which the breaches occurred, the types of attacks used, the types of organizations attacked, the states concerned and the number of records breached. We have grouped them by type of attack as well as by type of organization, in order to have sufficiently robust groups for the following studies, these groupings were based on criteria of similarities of the origin groups. This information is summarized below :

Grouping	Origin	Description
OTHER	CARD	Fraud involving payment cards, other than Hack
OTHER	INSD	Insider : someone who has legitimate access to the data intentionally violates it (employee, customer, subcontractor, etc.)
HACK	HACK	Hacking or Malware
THEFT/LOSS	PHYS	Paper documents (non-electronic), lost or stolen
THEFT/LOSS	PORT	Laptops, USB sticks, smartphones, hard drives etc., lost or stolen
THEFT/LOSS	STAT	Non-portable computer lost, stolen or accessed inappropriately
DISC	DISC	Unintentional Disclosure : eg information publicly released or sent to the wrong person

Table 5 – Types of PRC Attacks

Grouping	Origin	Description
BUSINESSES	BSF	Companies - Financial Services and Insurance
BUSINESSES	BSO	Companies - others
BUSINESSES	BSR	Retail-Dealers / Merchants - Includes Online Retail
OTHERORGA	EDU	Educational Institutions
OTHERORGA	GOV	Government and Army
OTHERORGA	ONG	Non Profit Organizations
MED	MED	Health Care and Medical Providers

Table 6 – Types of PRC organizations

Groupings have also been made for States, by keeping the most represented, namely : California (15.7%), Texas (6.9%) and New York (6.3%), and by grouping the others in a group called OTHER. [9]

9. The database is available at : https://www.privacyrights.org/data-breaches.

Motivations

In addition to the motivations of considering that the systems are interconnected, and therefore present a risk of contagion, two quantitative motivations have led us towards Hawkes' processes :

The first is the rejection of the Poissonnian hypothesis, the Poisson process being a classic modelling process. Two tests were carried out, an independence test of occurrence inter-times (Ljung-Box) and a test of adequacy of inter-times to the exponential law (Kolmogorov-Smirnov), both hypotheses are rejected with a very low p-value (<2.2e-16).

The second, and the main motivation is the presence of autocorrelation of the number of attacks in the database. More precisely, by drawing the number of attacks that occurred in a month m+1 according to the number of attacks that occurred in the previous month m, and this, within the same type of attack (types mentioned above) we obtain a linear correlation coe□cient of 0.6548 which therefore indicates a significant correlation.

Among the possible choices to model such a phenomenon is the Hawkes process, in addition to this argument, it has been chosen on the one hand because it also allows to model excitation phenomena, and on the other hand because it has a natural interpretation, which gives information about the phenomenon.

Hawkes processes

The Hawkes process is a counting process, as it is the case for the Poisson process. Its main characteristic lies in its conditional intensity, which represents the instantaneous risk of an attack occurring, knowing the past of the process. More simply, conditional intensity plays, for example, the same role as the intensity of the Poisson process, the di□erence is that it is conditioned by the past, and is therefore itself a random process. The Hawkes process defines it as follows :

$$\lambda(t) = \mu(t) + \int_{]\ 1\ ;t[} \phi(t \quad s) dN_s = \mu(t) + \sum_{T_n < t} \phi(t \quad T_n)$$

With $\mu(.)$ and $\phi(.)$ deterministic functions, positive, and $(N_t)_{t\ \ 0}$ the Hawkes process. The self-exciting property lies in the sum of the T_n which are the ordered occurrence times of the process. $\mu(.)$ is a basic risk, independent of the events that occurred, in the particular case where the kernel ϕ is zero, the process is an inhomogeneous Poisson process with a rate of $\mu(.)$.

The Hawkes process extends to the multivariate case, considering d process, the in-

tensity of the i-th process is defined as follows :

$$\lambda^{(i)}(t) = \mu^{(i)}(t) + \sum_{j=1}^{d} \int_{]-1;t[} \phi_{i;j}(t-s) dN_s^{(j)} = \mu^{(i)}(t) + \sum_{j=1}^{d} \sum_{T_n^{(j)} < t} \phi_{i;j}(t - T_n^{(j)})$$

with $\mu^{(i)} : \mathbb{R}^+ \to \mathbb{R}^+$
$\phi_{i;j} : \mathbb{R}^+ \to \mathbb{R}^+$

In this case, for $1 \leq i, j \leq d$, $\phi_{i;j}$ represents the impact of the $(N_t^{(j)})_{t \geq 0}$ process on the $(\lambda_t^{(i)})_{t \geq 0}$ intensity of the $(N_t^{(i)})_{t \geq 0}$ process. It is therefore not only self-excitation phenomena that are modelled ($i = j$) but also inter-excitation phenomena ($i \neq j$).

Hawkes processes on accurate segmentation

Model

The first application carried out consisted in studying the predictive capabilities of the Hawkes process on an accurate segmentation of the database. The segmentation used is the one which consists in crossing the variables type of attack, type of organization and State, and in putting the segments too poorly represented in a segment named OTHER. This leads to six selected segments.

The study was carried out with three different types of kernels :
— Kernel 1 : $\phi_{i;j}(a) = \alpha_{i;j} \exp(-\beta_i a)$
— Kernel 2 : $\phi_{i;j}(a) = \alpha_{i;j} \exp(-\beta_{i;j} a)$
— Kernel 3 : $\phi_{i;j}(a) = \alpha_{i;j} a \exp(-\beta_i a)$

The selected background intensity is a linear *drift* : $\mu_i(t) = \mu_{0;i} + \gamma_i t$, to take into account possible trends. This leads to a total of 54 parameters for kernels 1 and 3, and 84 parameters for kernel 2. These models are therefore relatively complex.

A parallel study was conducted to reduce the complexity of the process by penalizing the likelihood function, in order to observe whether it is possible to improve predictive capabilities in this way. The penalty takes the following form :

$$\log L(\mu, \phi)_{penalized} = \log L(\mu, \phi) + \gamma \sum_{1 \leq i;j \leq d} |\alpha_{i;j}|$$

where $\gamma > 0$ is the penalty ratio and $L(\mu, \phi)$ is the likelihood of the Hawkes process, with $\mu = (\mu_{i;0}, \gamma_i)_{1 \leq i \leq d}$ and $\phi = (\alpha_{i;j}, \beta_{i;j})_{1 \leq i;j \leq d}$. This penalty corresponds to a Lasso method that we have preferred over a Ridge method, because it allows the penalized coefficients to take exactly the value 0. In other words, it allows the model to highlight the main interactions.

Results

The models were compared as follows : they were calibrated over the period 2011-2015 to predict the number of attacks in 2016, as well as over 2011-2016 to predict the number of attacks in 2017. The comparison measure is the sum of the absolute difference, over each segment, between the value of the predicted number and the real number of attacks. The results are as follows :

γ	0	100	600	900	3000	6000
Kernel 1 (2016)	337.6614	280.7602	277.7764	283.5881	973.0103	1135.5217
Kernel 1 (2017)	170.3384	249.4687	240.4258	261.7280	732.0155	792.7558
Kernel 2 (2016)	259.4504	282.2328	202.7125	180.3729	256.7397	430.4255
Kernel 2 (2017)	127.3343	160.8886	159.4488	141.6603	148.1485	346.4559
Kernel 3 (2016)	201.7575	285.1470	262.0646	283.1685	502.2474	1559.1263
Kernel 3 (2017)	165.6958	183.2997	254.2543	172.6621	3168.8662	6402.4315

Table 7 – Sum over the six segments, of the absolute differences between the expected number of predicted attacks (in 2016 and 2017) and the real number, according to the penalty coefficient γ.

These results seem to show that it is difficult to select a model based on its predictive capacity, as the best models are not the same from one year to the next. Penalization in some cases does improve predictive skills.

Finally, one of the best compromises over the two years is the non-penalized kernel 3. The distributions predicted by this model for year 2016 contain the real number of attacks for four out of six segments. Over 2017 the distributions all contain the real number of attacks but one of them, beyond its 99.5% quantile, which means that the real value is highly unlikely under this model. Kernel 3 is also the best compromise in terms of likelihood. The statistical tests of the adequacy of the process to the data are mostly conclusive (9 out of 12 accepted at the 5% threshold). These results show that a latent excitation (kernel 3) better represents the data, which is not the classical exponential framework of Hawkes' processes (kernels 1 and 2). Although these results are encouraging, the complexity of the model leads us to consider a less fine segmentation for the following applications.

Pricing of a data breach guarantee

The pricing process was carried out in three stages : the choice of a segmentation, the determination of the frequency model and the determination of the cost model.

Segmentation : different segmentations, less detailed than the previous one, were tested, these segmentations were chosen on the basis of common sense (e. g. one type of attack = one segment) as well as statistical similarities. They were compared on the basis of the validation of statistical tests of Hawkes' process adequacy. The segmentation used

is the segmentation by type of organization, i.e. the three segments : MED (medical, health), BUSINESSES and OTHER, which is not rejected by any 5% test.

Frequency Model : In parallel with the Hawkes process, another type of frequency model was tested, which consists in modelling the daily number of attacks by a negative binomial law for the first two segments, and by a negative binomial GLM for the segment OTHER to take into account a trend over time, which is graphically obvious. These models were chosen among several others (Poisson, geometric, etc.), based on fit quality, statistics (chi-square test) and graphs (quantile-quantile diagrams).

Cost model : its purpose is to model two phenomena : the first is that an attack does not have the same probabilities of violating a certain number of records according to the segment, the second is that the cost of a data breach changes with the total number of records breached. For this purpose, continuous laws were selected to model the logarithm of the distribution of the number of records breached per segment (two Gamma laws and one logistic law) and a linear model of the type log(Total cost) = a + b log(Number of violated data), present in the literature, was used to model the second phenomenon mentioned above.

Results : The predicted distributions of the number of attacks per segment, for 2017, all contain the real, for both methods (Hawkes and discrete distributions), except the distribution of OTHER in the case of negative binomial GLM. The premiums obtained in the case of a traditional guarantee are summarised in the following table (the master thesis also focused on a higher guarantee, accompanied by reinsurance).

	BUSINESSES	MED	OTHERORGA
Pure Premium (Hawkes)	975.43	5 629.92	759.27
Pure Premium (Discrete distribution)	1048.32	5443.21	453.51

Table 8 – Pures premiums obtained, in dollars

Premiums are significantly close except in the last segment. A comparison with real premiums shows that the ones obtained are not meaningless [10], however, the actual premiums studied take into account the turnover of the insured company, so our premiums are far from the reference premiums when a company's turnover is high. Taking this factor into account is a potential opening for this work, which for the time being considers the risk as equal within the same sector, whatever the company.

10. Examples of premimums are given in the following website : https://databreachinsurancequote.com/cyber-insurance/cyber-insurance-data-breach-insurance-premiums

Development of an individual reserving method with Hawkes processes

The principle of this method is as follows : claims are assumed to occur at times $(T_n)_{n\ 1}$ following a Hawkes process and are modelled together with their reporting times $(U_n)_{n\ 1}$, which are assumed to follow a p_{ujT_n} law (e.g. an exponential law). We place ourselves on a time horizon of observation $[0, \tau]$. As an insurer, in τ, can only observe the times of occurrences such as $T_n + U_n \quad \tau$, it means that some of the claims are not yet known, it is the famous IBNR (Incurred But Not Reported) that it is then necessary to provision at the end of the year.

The problem of this section appears when writing the likelihood of such a model which has the following form :

$$L(\phi, \mu) = \exp\left(\int_0 \lambda(s) p_{Ujs}([0, \tau \quad s])\mathrm{d}s \right) \prod_{n=1}^{n_\tau^R} \lambda\left(t_n^R\right) p_{Ujt_n^R}(u_n^R)$$

This likelihood depends on λ, which depends on all the past events of the process. By taking the notations $(T_n^{IBNR})_{n\ 1}$ for IBNR claims and $(T_n^R)_{n\ 1}$ for observed claims, all claims $(T_n)_{n\ 1}$ is broken down into these two subsets, λ is then rewritten as :

$$\lambda(s) = \mu(s) + \sum_{T_n < s} \phi(s \quad T_n) = \mu(s) + \sum_{t_n^R < s} \phi(s \quad t_n^R) + \sum_{T_n^{IBNR} < s} \phi(s \quad T_n^{IBNR})$$

By construction, the IBNR $(T_n^{IBNR})_{n\ 1}$ are not known, so the intensity λ is not calculable, so it follows that the probability is not calculable.

This section then turned to a method for estimating this likelihood. The method required some approximations in the calculations, di□erent tests were then performed to test its validity, including the following :

IBNR processes with Hawkes were simulated for 22 known parameter sets, and then the parameters were estimated, on these simulations, by our approximate likelihood function. IBNRs were then simulated (by a method approached again) under these parameters. The results are that 18 distributions simulated out of the 22 cases, contain the actual number of IBNR. So this method is not meaningless despite its approximations.

Other tests were carried out such as the graphical observation that the observation bias is well taken into account, or the comparison of our model with a biased model, in terms of parameter estimation.

This section ends with an application on a real database (data breaches in the United States), as well as a comparison with the individual Poisson method and the Mack method. In this example, the Hawkes individual model seems to be a good compromise

between the two methods in terms of prediction (distribution that contains the real) and precision (low variance).

Conclusion

This master thesis highlights the value of the Hawkes process in modelling the frequency of data violations, particularly with its ability to adjust and predict.

A pricing method is presented and seems to make sense in view of the premiums actually observed on the market. This method makes it possible to take into account the global risk environment (phenomena of contagion between companies) but does not adapt to the intrinsic risk of the company in addition to taking into account its sector of activity, this could be the subject of future work, for example to take into account the company's turnover. The method has the advantage of obtaining distributions and therefore a lot of information on risk (quantiles, variance, etc.).

The reserving method developed in the last part seems to make sense despite its different estimates, future work would be to try to better justify, and/or reduce the number of these estimates. Such a method makes it possible to take advantage of the advantages of individual methods over aggregate methods, and in particular to compute reserves for atypical claims by taking advantage of the characteristics of the Hawkes process, more traditional claims are also concerned in the sense that the Hawkes process is a generalization of the Poisson process.

Hawkes processes have some limitations, however, a first limit is the number of parameters that increases rapidly with the size of the process, another limit concerns the sensitivity of the process to the database used, indeed, the latter is influenced not only by the database through the estimated parameters, but also through the entire history of the database, which is taken into account in the past of the process during simulations, so data quality is of importance.

A final limitation (which is also its strength) concerns the interdependent nature of this process. Indeed, this implies that the incorrect calibration of certain segments necessarily influences the other segments.

Table des matières

Table des figures

Introduction

Avec la numérisation de l'économie et le stockage de plus en plus massif de données en ligne, le cyber-risque concerne aujourd'hui la majorité des entreprises. Une certaine prise de conscience de ce risque se fait ressentir à toutes les échelles, d'abord à l'échelle de l'entreprise, mais également dans la réglementation, par exemple sur la protection des données personnelles, et pour finir dans le secteur de l'assurance.

Le marché de la cyber-assurance est en effet encore en pleine expansion, en témoigne la forte croissance des montants de primes ces dernières années. Ce risque, attractif en terme de marché, est cependant peu maîtrisé en terme de modélisation.

Il présente en effet des caractéristiques atypiques, en premier lieu le coût des cyber-attaques concerne des actifs immatériels comme la perte d'exploitation, la perte de réputation ou encore le vol de données. En second lieu ce risque est caractérisé par une absence de frontières géographiques ainsi qu'une interdépendance des systèmes informatiques, à l'échelle de l'entreprise, mais également nationale puis mondiale. Cette caractéristique d'interdépendance se modélise difficilement avec les outils actuariels classiques.

Des travaux théoriques ont été effectués sur ce dernier point, c'est par exemple le cas de [Baldwin *et al.*, 2017] qui modélisent la fréquence des cyber-attaques sur des ports internet avec un processus de diffusion multivarié, pour des fins de cyber-sécurité. Parmi les exemples plus orientés assurance, nous pouvons citer [Maochao et Lei, 2017] qui proposent différentes modélisations basées sur la contagion dans un réseau, dans un but de pricing, ainsi que [Böhme et Kataria, 2006] et [Herath et Herath, 2011], qui modélisent les corrélations au sein d'une entreprise (les ordinateurs sont interconnectés donc leurs risques sont corrélés), ainsi qu'entre les entreprises, à l'aide de copules. Ces travaux nécessitent des informations comme une structure du réseau, le nombre d'ordinateurs connectés entre eux au sein d'une entreprise, le nombre d'ordinateurs infectés ou encore le taux d'infection, ces informations sont en pratique difficiles à obtenir. En parallèle, d'autres travaux se penchent uniquement sur la fréquence des cyber-attaques, c'est le cas de [Edwards *et al.*, 2016] qui modélise le nombre journalier d'attaques aux États-Unis par des lois discrètes.

Ce mémoire propose une modélisation de la fréquence des attaques, dans le cas

particulier des violations de données, avec des processus dits de Hawkes. Ces processus permettent notamment de modéliser des e□ets d'excitation et de dépendance, sans pour autant définir explicitement une structure de réseau. Ce type de processus a déjà été utilisé dans le cadre de la cyber-sécurité par exemple par [Baldwin *et al.*, 2017] et [Peng *et al.*, 2016]. Nous n'avons pas connaissance de travaux dans cette direction dans le cadre de l'assurance, qui est un cadre relativement di□érent.

Ce document est composé de trois grandes parties, la première présente le cyber-risque, d'abord d'un point de vue général puis d'un point de vue assurantiel. Les deux autres parties tentent de répondre à la problématique de modélisation, dans le cas particulier des violations de données, et ce sur trois aspects de la chaîne d'assurance à savoir la tarification, la réassurance, ainsi que le provisionnement. Les modélisations utilisées permettent également de déterminer des quantiles à horizon un an dans le cadre d'un modèle interne Sovabilité II.

Plus en détail, après la présentation du cyber-risque, la seconde partie de ce mémoire concerne l'application des processus de Hawkes pour modéliser la fréquence des violations de données, avec notamment la détermination d'une prime d'assurance et de réassurance pour une garantie de ce type. L'approche proposée a pour objectif de prendre en compte les particularités de ce risque, bien entendu en matière de fréquence, mais également en matière de coût, avec une étude du coût d'une donnée violée.

Pour finir, la dernière partie vient compléter la précédente en se plaçant dans le cadre du provisionnement. Elle se penche sur le développement d'une méthode de provisionnement individuel avec des processus de Hawkes afin de déterminer le nombre d'IBNR (Incurred But Not Reported), et ce, dans le but de s'émanciper du cadre Poissonien plus classique, qui ne permet pas de profiter de certaines particularités comme la dépendance et l'excitation. L'avantage de ces modèles est en particulier de prendre en compte le biais d'observation généré par le fait que les sinistres observés sont généralement ceux qui ont un faible délai de déclaration. L'intérêt d'un modèle utilisant les processus de Hawkes étant de pouvoir provisionner des sinistres atypiques tout en profitant des avantages des méthodes individuelles. Le processus de Hawkes est également légitime en ce sens qu'il est une généralisation du processus de Poisson.

Les travaux se portent principalement sur une méthode d'estimation de la fonction de vraisemblance qui s'avère incalculable de par sa construction. Après le développement, et des tests autour de cette méthode, cette dernière partie se clôt avec une application sur le cas des violations de données. En e□et, comme les sinistres non-vie plus classiques, les violations de données présentent un délai entre leur survenance et leur déclaration à l'assureur. Ce délai provient principalement du délai nécessaire pour se rendre compte qu'une violation a été subie, il génère naturellement des IBNR.

Chapitre 1

Le cyber-risque

1.1 Introduction

Le cyber-risque peut se définir comme suit : « une atteinte aux données numériques détenues et/ou gérées par une organisation (entreprise, association, collectivité locale, administration) que celles-ci lui appartiennent ou qu'elles lui soient confiées par des tiers, ainsi que les conséquences d'une atteinte au système d'information » [1].

Ces dernières années, ce risque se fait de plus en plus remarquer du grand public avec notamment de très grosses cyber-attaques comme les cas NotPetya ou encore WannaCry [2] en 2017, qui ont touché des centaines de milliers d'ordinateurs à travers le monde.

En réalité, il n'est pas si récent : les premières vagues de cybercriminalité sont apparues avec la prolifération des courriels dans les années 80, poursuivies par d'autres vagues dans les années 90 avec le développement des navigateurs Web. À partir des années 2000 la cybercriminalité a augmenté de manière explosive, avec la création des réseaux sociaux ainsi que le stockage de plus en plus massif de données. La cybercriminalité est devenue une activité organisée, avec des gangs ainsi qu'une véritable industrie criminelle.

Le cyber-risque est aujourd'hui classé numéro un parmi les risques émergents (risques qui se développent ou évoluent, caractérisés par une forte incertitude) par les assureurs, devant le risque climatique et le risque de crise du système financier. Tenant compte de la probabilité d'occurrence de ce risque ainsi que son impact élevé, il est prévu qu'il restera classé comme tel pour les cinq prochaines années. [3]

Ce chapitre présente le cyber-risque autour de deux parties, la première décrit les grandes caractéristiques de ce risque d'un point de vue général et la seconde s'intéresse au cyber-risque et ses caractéristiques dans le monde de l'assurance.

---

1. Définition qui apparaît dans une présentation de KPMG sur la cyber-assurance en 2017 : https://www.institutdesactuaires.com/global/gene/link.php?doc_id=10471&fg=1
2. Ces cas sont détaillés par la suite.
3. Baromètre des risques émergents (FFA) : https://www.ffa-assurance.fr/presse/communique-de-presse/deuxieme-edition-du-barometre-des-risques-emergents-pour-assurance

1.2 Présentation générale

Cette section a pour but de présenter le cyber-risque, ses acteurs et ses principales caractéristiques, sans rentrer dans des considérations techniques.

1.2.1 Manifestations et motivations des cyber-attaques

Trois principaux objectifs peuvent motiver une cyber-attaque :

— Le rançonnage : l'attaquant bloque l'accès à un logiciel ou à des données et exige en échange une rançon. Le concept est apparu dans les années 80 avec le paiement d'une rançon par courrier. Aujourd'hui la rançon est réclamée par carte de crédit ou cryptomonnaie.

— La fuite de données et l'espionnage : le but de l'attaquant est de voler des données. Cela peut être des données personnelles, numéros de cartes de crédit, données de santé, données sensibles etc.

— Le sabotage : le but du sabotage est d'altérer ou de supprimer de façon illicite un programme informatique ou des données.

Pour atteindre ces objectifs, di□érents types d'attaques sont utilisés, parmi les plus courants nous retrouvons :

— Malware : logiciel spécialement conçu pour perturber, endommager ou obtenir un accès non autorisé à un système informatique, en général ce nom évoque en majorité :
  — le virus : *"automate autoréplicatif à la base non malveillant, mais aujourd'hui souvent additionné de code malveillant, conçu pour se propager à d'autres ordinateurs en s'insérant dans des logiciels légitimes, appelés « hôtes » "* (définition wikipédia) ;
  — le spyware : *"logiciel malveillant qui s'installe dans un ordinateur ou autre appareil mobile, dans le but de collecter et transférer des informations sur l'environnement dans lequel il s'est installé, très souvent sans que l'utilisateur en ait connaissance"* (définition wikipédia).
— Man-in-the-middle : l'attaquant intercepte secrètement les communications entre deux parties qui pensent communiquer directement entre elles.
— Zero-day : exploitation d'une vulnérabilité dans un navigateur ou une application avant que celle-ci ne soit corrigée.
— Denial-of-service (DOS) : attaque ayant pour but de rendre un serveur, un service ou une infrastructure indisponible. L'attaquant envoie une multitude de requêtes afin de saturer la bande passante ou d'épuiser les ressources système.
— Phishing : le but est de faire croire à la victime qu'elle fait face à un tier de confiance afin de lui soutirer des informations sensibles. Cela peut être fait via un faux site internet ou l'envoie d'un document, le plus souvent un mail, paraissant fiable.

Les motivations des attaquants peuvent être diverses, par exemple une motivation financière, du militantisme (politique, sociétal..) on parle alors de "Hacktivistes", les objectifs peuvent également être militaires, ou encore compétitifs (vols d'information chez les concurrents), finalement, il existe également du terrorisme cyber.

Le rapport de Verizon "2019 Data Breach Investigations Report", basé sur l'étude de plus de 40 000 incidents de sécurité informatique étudie à la fois les violations de données et les incidents (rançonnage/sabotage, incidents qui touchent un actif numérique). Il met notamment en évidence les informations suivantes :

Concernant les violations de données : les motivations principales de ces attaques sont financières (71% des attaques ont cette motivation), 25% des violations sont tout de même motivées par l'avantage stratégique et correspondent donc à de l'espionnage. Les attaquants sont dans la plupart des cas (aux alentours de 75%) des individus externes, et assez régulièrement des individus internes à l'organisation (aux alentours de 20%). Toujours concernant les violations de données, l'utilisation de Malwares semble concerner environ 30% des attaques (stable entre 2013 et 2018), le social engineering (manipulation, escroquerie) semble quant à lui être de plus en plus utilisé en passant de 17% en 2013 à 35% en 2018, le phishing en fait une grande partie (plus de 80%).

Ce rapport se penche également sur les incidents (ex : sabotage/rançonnage décrits ci-dessus) : presque 60% sont des attaques DOS, les ransomwares quant à eux concernent moins de 10% des attaques.

1.2.2 Réglementations

Ces deux dernières décennies le cyber-risque s'est fait de plus en plus présent et menaçant, en parallèle un cadre réglementaire en terme de cyber-sécurité s'est crée. De façon générale, deux grandes catégories de régulations se distinguent :

— une première partie a pour but d'obliger les entreprises à posséder un niveau de sécurité minimum afin de protéger leurs systèmes et informations contre les cyber-attaques.
— une seconde partie concerne les obligations de notification en cas de violation de données, sous certaines conditions.

Cette section explicite chronologiquement, les principales réglementations qui ont été mises en place en matière de cyber-sécurité, aux États-Unis ainsi qu'au sein de l'union européenne.

Aux États-Unis : les trois principaux règlements au niveau fédéral ont été établis dès 1996 (Loi sur la portabilité et la responsabilité en matière d'assurance maladie), 1999 (Gramm-Leach-Blieley) et 2002 (sécurité intérieure). Ces règlements obligent les organisations de soin de santé, les institutions financières et les agences fédérales à protéger leurs systèmes d'information.

A l'échelle des États, la Californie a adopté une loi sur la notification des violations de données en 2003. La plupart des États ont par la suite créés leur propre loi de notifi-

cation en suivant la loi originale de Californie qui déclare que les violations doivent être signalées si "*des informations d'identification personnelles sensibles ont été acquises ou sont raisonnablement considérées comme ayant été acquises par une personne non autorisée, et sont raisonnablement susceptibles de causer un préjudice important aux personnes concernées*." En particulier, ces lois imposent une notification aux résidents concernés par la violation de données, ainsi qu'à certains organismes, notamment au procureur général de l'État sous certaines conditions (par exemple un nombre minimum de résidents a□ectés). Une grande partie des États ont promulgués leurs lois avant 2010, South-Dakota ainsi que l'Alabama ont promulgués les derniers leurs lois de notification en 2018, les 50 états ont donc maintenant une loi de notification.

En parallèle, depuis plusieurs années, le congrès Américain a proposé de nombreux projets de lois visant à élargir la réglementation sur la cybersécurité, ainsi qu'à criminaliser les cyber-attaques. Parmis les actions principales (et récentes) du gouvernement, nous pouvons citer la création en 2015 d'une agence dédiée à la cybersécurité (CTIIC), la directive CISA promulguée en 2015, qui encourage l'échange entre le secteur privé et le gouvernement fédéral d'information autour du cyber-risque (les menaces et les mécanismes de défense), le plan d'action national en cybersécurité annoncé en 2016 (CNAP, budget de plus de 19 milliards de dollards en 2017) ainsi que le projet de loi SHIELD ACT en 2017 afin de renforcer la cybersécurité à New York.

Concernant l'Union Européenne : en 1995 la directive 95/46/CE sur la protection des données personnelles, visait à harmoniser la protection en matière de données personnelles et imposait par exemple de devoir prendre des mesures pour assurer un niveau de sécurité minimum dans le traitement de données.

Le règlement de 2004 numéro 460/2004 du Parlement européen et du Conseil a été à l'origine de la création de l'ENISA (European Union Agency for Network and Information Security), un centre d'expertise avec pour vocation d'aider les pouvoirs à trouver des solutions pour lutter contre les menaces cyber.

En 2016 la directive NIS est entrée en vigueur, son objectif principal est de créer un niveau de cyber sécurité plus élevé dans l'union européenne.

Pour finir, le règlement général sur la protection des données (RGPD), adopté en 2016 et directement applicable en 2018, vient remplacer la directive 95/46/CE. Son but est d'instaurer une norme unique en matière de protection des données au sein de l'UE. En particulier, il s'applique à une entité si elle est responsable du traitement de données personnelles établies sur le territoire de l'Union européenne, ou qui cible directement des résidents européens, que l'entité soit européenne ou non. Comme dans les règlements qui l'ont précédé, il rend obligatoire la notification d'une violation de données portant atteinte aux droits et libertés de personnes résidant dans l'Union européenne. Une particularité de la RGPD réside dans la sévérité de ses amendes, qui peuvent atteindre 20 millions d'euros, ou 4% du chi□re d'a□aire annuel d'une entité.

Finalement, des réglementations existent depuis plus de 20 ans en matière de cybersécurité, mais la création de réglementations s'est faite, et se fait encore, très active, et

ce, car le risque évolue lui même très rapidement. Étant donné que les systèmes sont de plus en plus inter-connectés et que l'économie est de plus en plus informatisée, il est de plus en plus nécessaire de former un environnement global, et homogène, de sécurité, car une faille de sécurité dans un système peut engendrer une contagion dans d'autres systèmes.

1.2.3 Exemples de cyberattaques

Le cas Bangladesh Bank : en mai 2015 quatre comptes bancaires sont ouverts dans une banque aux Philippines. Neuf mois plus tard, trente-cinq virements sont demandés par la Bangladesh Bank (environ 950 Millions de dollars), à destination de cette banque des Philippines, via le réseau bancaire SWIFT.

90% de ces virements seront annulés par manque de précision, sur les 10 % restant, soit 101M de dollars, 81M arriveront sur les quatre comptes (frauduleux) aux Philippines. Quelques jours plus tard ces quatre comptes sont vidés massivement.

Le cas Equifax : Equifax est une des plus grandes sociétés d'évaluation de cote de crédit aux États-Unis (elle évalue la solvabilité et la capacité de remboursement d'une personne ou d'une entreprise souhaitant accéder au crédit à la consommation).

En 2017 cette société a été victime d'une violation de données, les attaquants ont eu accès, entre mai et juillet aux données concernant plus de 147 Millions d'américains en utilisant une vulnérabilité logicielle, cette dernière avait été annoncée et un correctif était disponible deux mois avant la violation.

Les données violées permettaient notamment de l'usurpation d'identité : noms, adresses, dates de naissance, numéros de sécurité sociale. Des numéros de cartes de crédit ainsi que des dossiers de crédits ont également été exposés.

Equifax s'est vu assigné plus de 2500 plaintes de consommateurs, ainsi que des recours collectifs nationaux et internationaux et des actions en justices par des villes et gouvernements américains.

Cette société a accepté un arrangement avec les régulateurs des États-Unis pour au final débourser entre 575 et 700 millions de dollars pour les victimes, les États et les organismes de réglementation américains. Cela mène à une perte totale, estimée à 1.4 milliards de dollars, qui incluent des frais généraux, des coûts de sécurité des données, des frais juridiques ainsi que des charges de responsabilité. La conséquence financière est en fait plus lourde, étant donné l'e□et de perte de réputation, ou encore la dégradation de la perspective de notation Moody's, qui est passée de stable à négative.

L'attaque NotPetya : en 2017, en Ukraine, un ransomware (logiciel ayant pour but le rançonnage décrit en 1.2.1) s'est propagé en utilisant une mise à jour d'un logiciel de comptabilité utilisé par plusieurs entreprises (M.E.Doc). Son code présentait des similitudes avec d'autre cas déja vécus, y compris le cas Wannacry qui peu de temps avant a infecté plus de 200 000 ordinateurs à travers 150 pays). Tout types d'entreprises ont été touchés, du site du gouvernement jusqu'aux ordinateurs de la centrale de Tchernobyl (qui entre autre permettent de suivre le niveau de radioactivité).

La propagation a rapidement dépassé les frontières et a concerné l'Europe, touchant par exemple Maerks (transporteur maritime danois) ou Nivea en Allemagne, ainsi que les États-Unis, touchant par exemple Merck (Pharmaceutique). Au total environ 2000 organisations auraient été touchées.

En particulier le logiciel bloque l'ordinateur infecté, cela à causé di□érents problèmes, notamment des arrêts de production ou des usines immobilisées/ralenties.

Le coût total s'élèverait à plus de dix milliards de dollars, avec, pour certaines multinationales, des coûts à hauteur de 200-300 millions pour Saint-Gobain, Maersk, Merk ou encore FedeX.

1.3 Le cyber-risque dans le monde de l'assurance

Cette section présente le cyber-risque en assurance, une première partie concerne le marché de la cyber assurance et la seconde les caractéristiques assurantielles techniques.

1.3.1 Un marché en construction

Malgré le fait que la cyber-criminalité existe depuis quelques dizaines d'années, l'adaptation à ce risque est encore en construction (ceci est encore plus vrai en Europe qu'aux Etats-Unis), la cyber-assurance fait partie des diverses possibilités dont disposent les entreprises pour réduire l'impact d'une cyber-attaque et est en ce sens un outil de cybersécurité.

Cette section évoque di□érents faits qui semblent montrer que le marché de la cyberassurance est encore en construction, notamment à travers la prise de conscience croissante du risque par les entreprises, l'évolution rapide de la taille du marché, ainsi que le manque de maîtrise de ce risque.

1.3.1.1 Le manque de préparation des entreprises

Dans le rapport annuel de l'assureur Hiscox le degré de préparation de plusieurs entreprises aux cyber-attaques a été mesuré : environ trois quart de ces dernières a été classé comme « cyber-débutant ». Plus en détail, en se basant sur les rapports Risk : Value du NTT security des dernières années, qui sont construits à partir des témoignages d'entreprises (aux alentours du millier de témoignages chaque année), di□érents aspects de la gestion de ce risque par les entreprises ressortent :

Tout d'abord, les évolutions sont faibles en terme de politique de sécurité et de système de gestion de crise. En 2017 seuls 56% possèdent une politique de cybersécurité, ce nombre gagne ensuite un pourcent pour chacune des années suivantes (2018-2019). De la même façon, moins de la moitié des entreprises sur ces trois années possèdent un plan de réaction face à une cyber attaque.

Ensuite, l'investissement dans la sécurité informatique, après avoir monté entre 2015 et 2017, stagne depuis, avec une part d'environ 15% du budget IT et entre 16 et 18 % du budget d'exploitation.

À cela s'ajoute le fait que les entreprises interrogées ne semblent, en majorité, pas se sentir concernées par la RGPD [4]. En 2017, soit un an avant l'entrée en vigueur, un quart des entreprises américaines interrogées se sentait concerné, 26% en Australie ainsi que 29% à Hong-Kong. En réalité la RGPD concerne une entreprise du moment qu'elle traite les données d'un ressortissant européen. En 2018 puis 2019, pas d'évolution, avec seulement un tiers des interrogés qui pensent avoir à faire à la RGPD. Pourtant la réglementation fait en quelque sorte partie des cyber-risques pour les entreprises car elle peut générer des sanctions financières lourdes en cas de manquement aux obligations en terme de cyber-sécurité (cf la partie "Union Européenne" de la Section 1.2.2).

Cette faible progression dans la gestion du cyber-risque par les entreprises n'est pas en adéquation avec l'évolution du risque, en effet, le nombre de vulnérabilités informatiques découvertes est passé de 6 477 en 2016 à 16 555 en 2018, le temps moyen pour se remettre d'une attaque est passé de 57 jours en 2018 à 66 en 2019, et le coût pour se remettre d'une violation, en pourcentage du revenu, a augmenté ces trois dernières années passant de 9.9% en 2017 à 12.7% en 2019.

1.3.1.2 Vers une prise de conscience du risque

Malgré le manque d'investissement en sécurité informatique, il semble y avoir une prise de conscience du cyber-risque par les entreprises. En 2017, 57% des responsables interrogés étaient convaincus qu'ils subiraient un jour une violation de données. En 2019, sur les 5 risques que les entreprises interrogées pensent avoir à faire durant les 12 prochains mois, 3 concernent le cyber-risque.

Les entreprises prennent donc peu à peu conscience du cyber-risque, et craignent notamment, en cas d'attaque, une perte de confiance du client, une baisse de la réputation, et ensuite des conséquences financières. Pourtant, les divers moyens pour lutter contre ce risque n'augmentent pas rapidement (budget risque, plan d'intervention, politique de sécurité, discussions aux assemblées, etc.). Au-delà de la nécessité d'une prise de conscience de la responsabilité de tous les employés, et de créer et diffuser une culture de la cyber-sécurité afin que tout le monde se sente concerné (aujourd'hui encore, beaucoup pensent que la sécurité relève uniquement du service IT), ce sont les moyens qui pourraient être une barrière, avec 43% des interrogés qui déclarent ne pas avoir les ressources nécessaires pour mettre en place un tel système. Tout ceci indique qu'il reste encore une marge de progression en terme de cyber-sécurité et potentiellement, d'investissement dans la cyber-assurance, le rapport Risk : Value 2019 du NTT Security indique en effet que moins de la moitié (48%) des entreprises étudiées a souscrit une cyber-assurance.

4. Le règlement n° 2016/679, dit **Règlement Général sur la Protection des Données**, est un règlement de l'Union européenne qui constitue le texte de référence en matière de protection des données à caractère personnel.

1.3.1.3 Une opportunité de marché

L'article Cyber insurance survey de [Orlando *et al.*, 2017], fait ressortir les point suivants concernant le marché de la cyber-assurance :

Des cyber-assurances sont apparues dans les années 1990 en étant proposées pour accompagner l'achat de logiciels. Une des premières cyber-assurance en tant que telle (contre le Hack) est apparue vers 1998. Par la suite, ce type d'assurance s'est développé, pour aujourd'hui concerner 50 à 60 assureurs rien qu'entre les États-Unis, les Bermudes ainsi que Londres.

La croissance du marché de la cyber assurance semble être liée à la survenance de grandes cyberattaques sensibilisant ainsi à la fois l'o□re et la demande en cyber assurance. Cette croissance est également stimulée par la réglementation, ceci s'est par exemple observé par une forte augmentation des polices d'assurances suite à la création de la loi de notification sur les violations de données en Californie (2003).

Cette croissance, bien qu'un peu moins forte que prévue aux États-Unis, reste très importante, une étude de Betterley Risk a montré que le montant de primes brutes concernant la cyber-assurance était de 2 milliards en 2014 (contre 1.3 en 2013), et semblait croître de 10 a 25 % par an. D'après l'assureur Chubb, 17 assureurs vendaient de la cyber-assurance en 2007, générant ainsi 350 millions de primes à l'année. Il y en aurait 65 en 2018, générant ainsi 3.5 milliards de primes à l'année. Le marché attendu pour 2020 serait entre 8 et 10 milliards d'après des analystes de Morgan Stanley.

Le marché en Europe est bien moins important (moins de 10% du marché mondial, en particulier 9 entreprises sur 10 souscrivant une cyber-assurance seraient américaines) avec moins de 150 millions de montant de primes brutes estimé en 2017, cependant le potentiel de croissance est estimé entre 50% et 100% par année d'après Marsh.

De plus en plus de très grosses entreprises souscrivent une cyber-assurance, cela est en partie dû aux évènements majeurs de 2017 (WannaCry et NotPetya évoqués en 1.2.3) qui ont accélérés la prise de conscience, au-delà, il semblerait que le marché possède encore un potentiel de croissance car comme cité ci-dessus il reste encore beaucoup d'entreprises qui n'ont pas encore contracté d'assurance de ce type (cela concerne beaucoup les PME). Ceci vient placer le cyber-risque en deuxième position dans le classement des opportunités pour le secteur de l'assurance [5].

1.3.1.4 Maîtrise du risque en assurance

Un dernier point soulignant que le marché de la cyber-assurance est encore en construction concerne le manque de maîtrise actuel de ce risque, en e□et :

Le cyber-risque est un risque encore méconnu dans le sens où le marché de l'assurance ne dispose pas de dizaines d'années d'expérience, contrairement à d'autres risques. Bien que des assurances pour des cyber-risques soient apparues aux États-Unis vers la fin des

5. Baromètre des risques émergents de la FFA : https://www.ffa-assurance.fr/sites/default/files/files/2019/02/20190206_-_barometre_2019_des_risques_emergents.pdf

années 90, les cyber-risques d'il y a dix ans ne sont plus les mêmes aujourd'hui. Ceci est dû à l'évolution très rapide ces dernières décennies de la place du numérique dans notre économie, ainsi qu'à la sophistication et à la création de nouvelles cyber-attaques au même rythme qu'évolue la technologie. À cela il faut ajouter le manque de données disponibles. Il y a donc aujourd'hui, en assurance, des di□cultés techniques concernant ce risque. En particulier autour de la tarification et de l'identification des risques (ces aspects seront plus développés dans la section suivante). Des di□cultés d'adaptation pourront également apparaître à l'avenir si les réglementations sur la cyber-assurance, encore peu fournies aujourd'hui, évoluent.

1.3.2 Caractéristiques assurantielles

Cette section détaille les spécificités techniques du cyber-risque en assurance.

1.3.2.1 Asymétrie d'information

Bien que cette problématique soit présente dans beaucoup de champs de l'assurance, elle est particulièrement présente dans le cyber-risque.

Afin d'assurer correctement une entreprise, l'assureur doit déterminer son exposition au risque. Pour cela il est nécessaire de connaître les di□érentes protections informatiques que possède l'entreprise. Cependant, il est possible de posséder certaines protections, sans les maintenir à jour régulièrement. Au-delà, comme évoqué précédemment, la sécurité découle d'un processus, d'un ensemble de bonnes pratiques plutôt que de simples logiciels de protections installés. Cela peut être di□cile à évaluer pour l'assureur. Il existe donc une forte asymétrie d'information sur le réel niveau de sécurité entretenu et celui connu par l'assureur.

1.3.2.2 Identification du risque

Une particularité actuelle de la cyber-assurance est la di□culté à identifier les risques.

Ceci est dû d'une part au manque de données, en e□et, les données publiques sur les cyber-attaques sont rares, cela est en partie causé par le fait que les entreprises sont réticentes à di□user ces informations par peur de perte de réputation, mais également par le jeune âge de ce risque, peu de données ont donc été collectées. Deuxièmement cette di□culté à identifier le risque est due à son évolution constante, ainsi qu'à la nécessité d'identifier clairement quels risques sont pris en compte, et quels risques ne le sont pas, dans une couverture cyber.

Un des dangers actuels pour les assureurs est le risque dit (cyber) silencieux, ce risque correspond à la non exclusion de la couverture du cyber-risque dans le cadre de polices d'assurances plus traditionnelles. Par exemple un piratage informatique peut mener à des dommages matériels (accidents de trains etc..), dans ce cas le risque est-il pris dans une couverture cyber ? Est-ce que ce risque a été pris en compte dans la tarification de la couverture plus classique ? Il y a donc une prise de conscience nécessaire sur le fait

que l'exposition au cyber pour un assureur est plus importante que la seule exposition relative aux contrats cyber.

1.3.2.3 Évaluation quantitative du risque

Au-delà de la difficulté à identifier clairement l'exposition au risque, il reste difficile de donner un coût à une cyberattaque. En effet, selon les différents types de cyberattaques, il peut être très difficile d'évaluer la perte, par exemple dans le cas d'une attaque DOS qui bloque les systèmes de l'entreprise, comment évaluer le coût de la perte d'exploitation ? Dans le cas d'une violation de données, comment évaluer le coût d'une donnée violée ? Plus généralement, comment évaluer le coût d'une perte de réputation ? Les cyberattaques provoquent des pertes sur des actifs plus abstraits qu'une perte matérielle, encore une fois le manque de données est un problème majeur pour l'évaluation de leurs impacts.

1.3.2.4 Le cyber-risque en tant que risque de contagion

Une partie de la difficulté à donner un coût aux cyberattaques est la présence de dépendances fortes entre les expositions des entreprises. La plupart des modèles actuariels utilisés ne sont pas adaptés à ces hypothèses de dépendance. Le risque est que les assureurs tarifient individuellement leurs couvertures cyber, sans prendre en compte ces dépendances.

Ces dépendances sont encore plus marquées par le fait qu'il n'y a aucune frontière géographique concernant une cyberattaque, ces attaques peuvent se faire à des milliers de kilomètres de la cible, elle sont également accentuées par l'homogénéité des systèmes informatiques, en effet beaucoup d'entreprises utilisent les mêmes logiciels, les mêmes systèmes d'exploitation, les mêmes fournisseurs, cela implique que les failles sont probablement les mêmes dans tous les systèmes. Au-delà, les données sont de plus en plus stockées numériquement, les systèmes sont de plus en plus interconnectés ; l'économie s'est numérisée de plus en plus ces dernières décennies.

Toutes ces dépendances font du cyber-risque un risque potentiellement systémique, qui pourrait se comparer, en terme de gravité, au risque de catastrophe naturelle, en particulier, certaines attaques ont des coûts extrêmement élevés. Ces dépendances et ces coûts extrêmes font qu'il est particulièrement difficile de tarifer ce risque.

Chapitre 2

Modélisation du cyber risque par les processus de Hawkes

Ce chapitre à pour objectif la détermination d'une prime pure pour une assurance violations de données. Cela nécessite une étude de la fréquence des attaques, ainsi que du coût, un point d'attention est porté sur la fréquence des cyberattaques pour laquelle nous avons utilisé des processus de Hawkes.

La première partie présente la base de données qui a été étudiée avec quelques statistiques descriptives (section 2.1).

Une seconde partie se penche sur nos motivations à appliquer les processus de Hawkes afin de modéliser la fréquence des violations de données, ainsi que sur le formalisme de ces processus (sections 2.2 et 2.3).

La troisième partie de ce chapitre a un double intérêt : étudier le calibrage de processus de Hawkes sur une segmentation fine (donc avec beaucoup de dimensions) dans un but d'interprétation des paramètres et donc de compréhension des tendances sous-jacentes dans les violations de données.

En parallèle, le second intérêt est d'étudier si le fait de réduire la complexité du processus en pénalisant la fonction de vraisemblance, peut permettre d'améliorer les capacités prédictives, et capacités d'ajustement des processsus de Hawkes sur ces données (sections 2.4 et 2.5).

Enfin, la quatrième et dernière partie consiste en la détermination d'une prime pure pour un contrat couvrant les violations de données aux États-Unis, ainsi que la détermination d'un quantile de la distribution de perte associée (section 2.6).

2.1 Présentation de la base de données

2.1.1 Description générale

Cette étude s'est portée sur la Privacy Rights Clearinghouse Database. La Privacy Rights Clearinghouse est une organisation à but non lucratif crée en 1992, son objectif est de protéger la vie privée en responsabilisant les individus et en plaidant pour un changement positif.

En particulier cette organisation met à disposition une base de données qui recense des violations de données aux États-Unis depuis 2005. Les violations dont elle dispose sont celles qui ont été recensées à des agences gouvernementales ainsi que rapportées par les médias. En ce sens c'est une base de confiance.

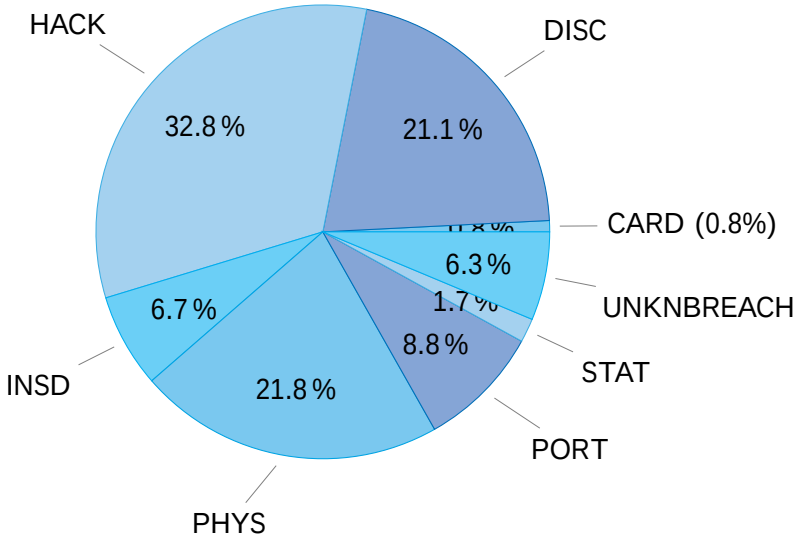
Les variables à disposition sont les suivantes :

— Date made public : la date à laquelle la violation a été déclarée
— Compagny : le nom de l'entreprise qui a subi la violation
— City : la ville dans laquelle se situe l'entreprise
— State : l'état dans lequel se situe l'entreprise
— Type of breach : le type d'attaque subie (HACK ; THEFT/LOSS ; etc.)
— Type of organization : le type/secteur d'entreprise qui a subi l'attaque (HEALTH ; BUSINESSES ; etc.)
— Total records : le nombre de données violées
— Description of Incident : une description de ce qu'il s'est passé
— Information source : la source dont provient l'information
— Year of breach : l'année durant laquelle s'est déroulée la violation
— Latitude
— Longitude

2.1.2 Statistiques descriptives

Afin de mieux comprendre le comportement de la fréquence des violations de données et dans une optique de segmentation future, voici quelques statistiques descriptives effectuées sur la période 2010-2019, les paragraphes qui suivent sont portés sur la colonne "Origine" des tableaux qui accompagnent les graphiques, qui correspond à la classification de la base telle quelle, l'étude des regroupements est e□ectuée en 2.1.3 :

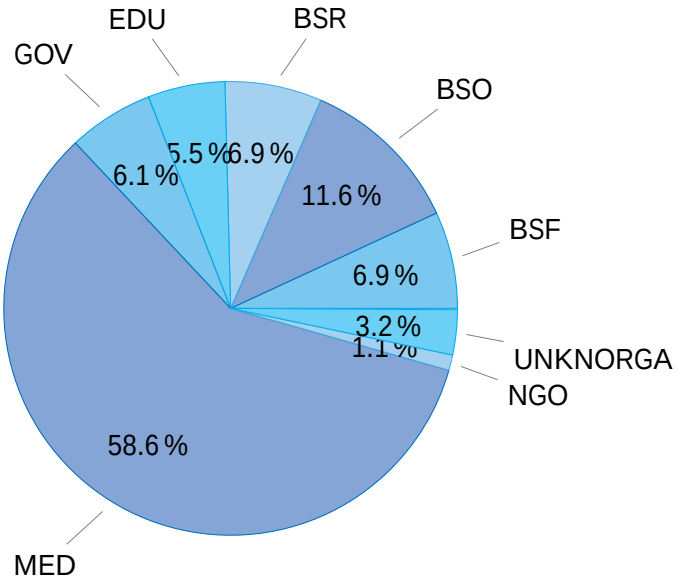
La Figure 2.1 représente les pourcentages de présence des types d'attaques référencées dans la base : trois grandes classes d'attaques se démarquent HACK, DISC et PHYS et représentent ensembles plus de 74% de la base. En particulier, parmi les violations de données, il est remarquable de constater que 21.1% proviennent d'une divulgation non intentionnelle. De la même façon 21.8% des violations concernent des documents physiques.



Regroupement	Origine	Description
OTHER	CARD	Fraude impliquant des cartes de paiements, autre que du Hack
OTHER	INSD	Insider, quelqu'un qui a légitimement accès aux données les enfreint intentionnellement (employé, client, sous traitant, etc.)
HACK	HACK	Piratage ou logiciels malveillants
THEFT/LOSS	PHYS	Documents papiers (non électroniques), perdus ou volés
THEFT/LOSS	PORT	Ordinateurs portables, clef USB, smartphones, disques dur etc, perdus ou volés
THEFT/LOSS	STAT	Ordinateur non portable perdu, volé ou accédé de façon inappropriée
DISC	DISC	Divulgation non intentionnelle par exemple informations di□usées publiquement ou envoyées à la mauvaise personne
	UNKNBREACH	Non déterminé

Figure 2.1 – Diagramme circulaire des types d'attaques - Origine représente la classification initiale de la base - Regroupement représente notre classification

La Figure 2.2 représente les pourcentages de présence des types d'organisations attaquées : elle met en évidence que la très grande majorité des organisations attaquées sont des organisations du secteur médical. Ceci est probablement lié au fait que des données médicales sont plus valorisables par la suite (revente sur le marché noir, etc.) que certaines données comme des données de carte de crédit, cela s'explique par le caractère non périsable des données médicales contrairement à d'autres données (une carte bancaire peut aisément être bloquée, changée etc..). Ensuite ce sont les diverses entreprises et commerces qui sont les plus représentés, en constituant ensembles près de 26% de la base.



Regroupement	Origine	Description
BUSINESSES	BSF	Entreprises - Services financiers et assurances
BUSINESSES	BSO	Entreprises - Autres
BUSINESSES	BSR	Commerces-Détaillants / Marchands - Comprend le commerce de détail en ligne
OTHERORGA	EDU	Établissements d'enseignement
OTHERORGA	GOV	Gouvernement et armée
OTHERORGA	ONG	Organismes à but non lucratif
MED	MED	Fournisseurs de soins de santé et d'assurance médicale
	UNKNORGA	Non déterminé

Figure 2.2 – Diagramme circulaire des types d'organisations attaquées - Origine représente la classification initiale de la base - Regroupement représente notre classification

La répartition des attaques référencées par État, présente en Annexe A, est hétérogène. Le maximum concerne la Californie qui recense 1117 attaques, certains États ont beaucoup moins d'attaques référencées comme le Montana (25 attaques), le North Dakota (10 attaques) ou encore le New Hampshire (30 attaques). Une partie non négligeable des États est entre 100 et 200 attaques comme l'Indiana (170) et le New Jersey (123). Certaines localisations comme Tokyo ou Berlin concernent les organisations dont le siège se trouve probablement en dehors des États-Unis. Ces localisations sont en général rares et ne comportent qu'un seul recencement.

En se penchant sur les lois de notification de violations de données évoquées en 1.2.2, nous pouvons remarquer que toutes n'ont pas été promulguées avant 2010. En particulier, nous pouvons noter la Floride (2014), l'Alabama (2018), le nouveau-Mexique (2017) ou encore le Kentucky (2014). Ces états ont tout de même des recensements, mais la non-obligation de notifier ces attaques avant leur promulgation peut jouer sur la perception de

la fréquence des attaques dans ces États. En revanche, c'est tout de même une majorité des États qui a promulgué ses lois de notification avant 2010, c'est pourquoi, avec cet argument ainsi que pour des considérations de nombre su□sant de données, nous avons décidé d'e□ectuer nos études à partir de 2010.

2.1.3 Regroupements

Les études qui suivront nécessitent des groupes su□samment représentés, la segmentation actuelle n'est pour l'instant pas satisfaisante à ce niveau. Pour cette raison nous avons e□ectué les regroupements suivants en prenant en compte les similitudes entre certaines variables. Nous avons décidé de regrouper les types d'attaques : PHYS, PORT et STAT dans une nouvelle catégorie nommée THEFT/LOSS. De la même manière, nous avons regroupé CARD et INSD dans une nouvelle catégorie nommée OTHER. Ces catégories représentent respectivement 32.3 % et 7.5 % de la base de données.

Concernant les types d'organisations, avec les mêmes arguments, nous avons regroupé BSF, BSO et BSR dans une catégorie nommée BUSINESSES. NGO, EDU et GOV sont quant à eux placés dans une catégorie OTHERORGA. Ce qui mène à une représentation de 25.5% et 12.8% de la base de données totale.

Pour terminer, nous souhaitons étudier si cela fait sens de prendre en compte une dimension géographique dans le cadre du cyber-risque. Étant donné que le nombre d'attaques rapporté par état est très hétérogène comme expliqué dans le dernier paragraphe de la Section 2.1.2, nous avons créé un groupe principal nommé OtherStates (66.8%) et avons conservé les 3 États les plus représentés en dehors de ce groupe, c'est-à-dire : California (15.7%), Texas (6.9%) et New-York (6.3%).

2.2 Etat de l'art et motivations

2.2.1 Motivations au sein de la Privacy Rights Clearinghouse Database

Les sections qui suivent présentent les faits qui nous motivent à utiliser des processus de Hawkes afin de modéliser la fréquence des cyber-attaques.

2.2.1.1 Rejet de l'hypothèse Poissonnienne

Un outil de modélisation actuarielle classique, pour modéliser une fréquence de survenance est le processus de Poisson homogène de paramètre λ *2* R_+. Il est donc naturel de commencer par tester si le processus de Poisson homogène peut être un bon candidat pour modéliser la fréquence des violations de données.

Ce processus a la particularité de posséder des accroissements indépendants qui suivent une loi exponentielle de paramètre λ. Des tests d'adéquation possibles sont par exemple un test de Kolmogorov-Smirnov pour tester la validité exponentielle, un test de Ljung-Box afin de tester l'hypothèse d'indépendance. Ces tests peuvent être accompagnés de vérifications grahiques.

	Ljung-Box	Kolmogorov-Smirnov
p-value	< 2.2e-16	< 2.2e-16

Table 2.1 – Tests d'adéquations processus de Poisson homogène

Les p-values des tests, en Table 2.1 sont très faibles, les deux tests sont rejetés. Le diagramme quantile-quantile de l'échantillon face à la loi exponentielle, ainsi que les autocorrélations en Figure 2.3 nous confortent dans cette idée, les quantiles des deux distributions sont loins d'êtres alignés, et beaucoup de pics de corrélation dépassent le seuil en bleu, qui indique une corrélation significative.

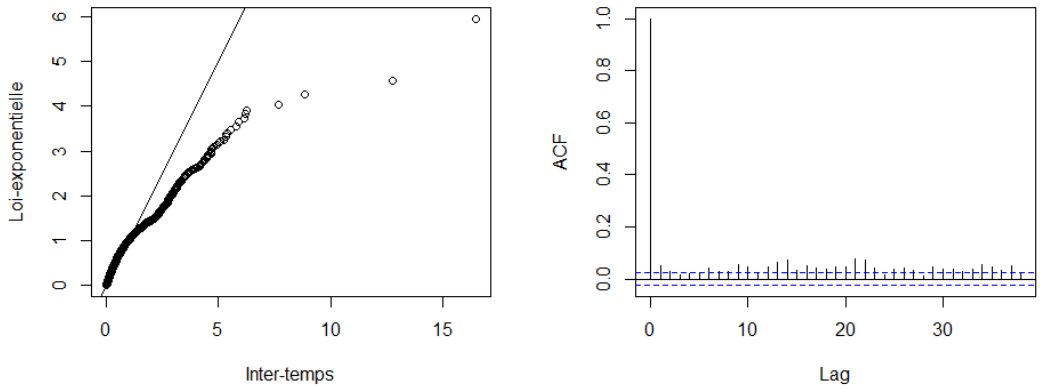


Figure 2.3 – Diagramme quantile-quantile entre la loi exponentielle et les inter-temps de la PRC (gauche) - Fontion d'autocorrélation des inter-temps de la PRC (droite)

2.2.1.2 Présence d'autocorrélation

Une première motivation pour appliquer les processus de Hawkes est la présence d'autocorrélation dans le nombre d'attaques. En effet en traçant le nombre d'attaques survenues dans un mois, en fonction du nombre d'attaques survenues dans le mois précédent, et ce, par type d'attaques, nous obtenons la figure 2.4.

Elle met en évidence un coefficient de corrélation linéaire de 0.6548 qui indique une claire autocorrélation du nombre d'attaques par type d'attaques.

Le même phénomène s'observe en figure 2.5 en croisant les variables, types d'attaques et types d'organisations attaquées.

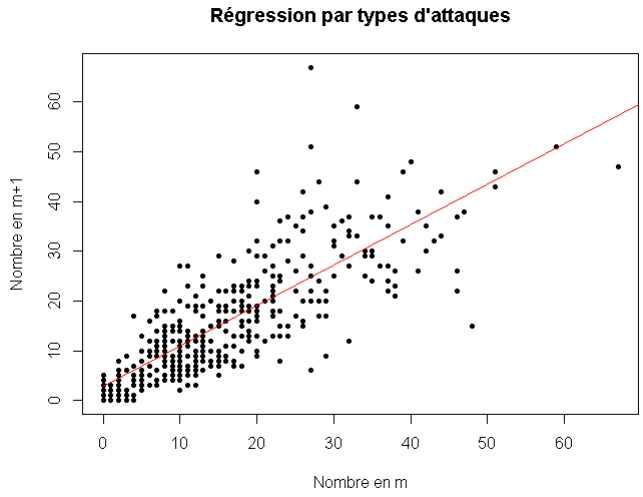


Figure 2.4 – Régression du nombre d'attaques d'un mois sur le précédent - par types d'attaques - R^2 = 0.6548

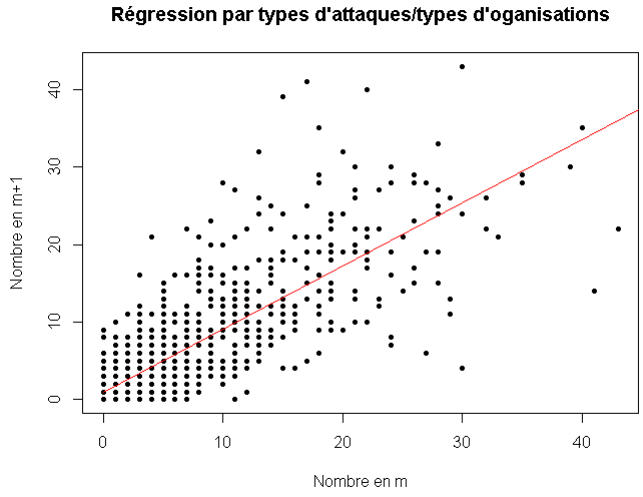


Figure 2.5 – Régression du nombre d'attaques d'un mois sur le précédent - par types d'attaques et types d'organisations - R^2 = 0.6637

Pour générer de l'autocorrélation, deux choix naturels sont le processus de Cox, et le processus de Hawkes, le processus de Hawkes permet également de prendre en compte des e□ets d'excitations, qui semblent faire sens dans le cadre du cyber-risque, par exemple, une faille logicielle découverte engendrera probablement beaucoup d'attaques en peu de temps. Un autre exemple est la contagion d'un virus au sein d'autres ordinateurs.

2.2.2 Les processus de Hawkes pour modéliser les cyber-attaques dans la littérature

Au-delà du fait que le cyber-risque est un risque de contagion, dans le sens où les attaques se propagent à travers les systèmes connectés, fait qui pourrait mener à ces phénomènes d'autocorrélation, d'auto-excitation et de contagion dans les attaques observées, quelques articles ont motivé notre utilisation des processus de Hawkes.

Tout d'abord les travaux de [Edwards *et al.*, 2016] portés sur l'étude de la fréquence et de la gravité des cyberattaques sur une base de données. Ces travaux ont mené à considérer la loi binomiale négative afin de modéliser le nombre journalier de cyberattaques. Une loi binomiale négative peut provenir d'un mélange de lois de Poisson, plus précisément d'une loi de Poisson avec un paramètre stochastique suivant lui même une loi Gamma. Cette modélisation nous amène, dans le cadre d'une approche micro-level, à considérer un processus de Cox (processus de Poisson avec intensité stochastique) qui pourrait générer ces résultats au niveau macro. Le processus de Cox peut générer de l'autocorrélation, c'est également le cas des processus de Hawkes. Ces derniers ont en fait déjà été utilisés pour la modélisation du cyber-risque.

Notamment par [Baldwin *et al.*, 2017] qui ont porté leur étude sur la modélisation jointe du nombre d'attaques sur différents ports. Un port est un accès par lequel peut s'effectuer une attaque (Oracle, SQL, DNS, etc.). Le nombre d'attaques est modélisé par un vecteur de diffusion à sauts dont chaque composante i suit l'équation différentielle stochastique suivante :

$$\frac{\mathrm{d}X_{i;t}}{X_{i;t}} = u_i \mathrm{d}t + \sqrt{V_{i;t}}\mathrm{d}W^X_{i;t} + Z_{i;t}\mathrm{d}N_{i;t}$$

avec $W^X_{i;t}$ un mouvement Brownien, $V_{i;t}$ une intensité stochastique, $Z_{i;t}$ la taille des sauts, et $N_{i;t}$ un processus de Hawkes.

Les résultats mettent en évidence (à travers les paramètres du processus de Hawkes) un effet de contagion entre les différents ports (un effet d'inter-excitation) ainsi qu'un effet d'auto-excitation au sein de chaque port. Donc de la dépendance dans le temps et de la dépendance entre chaque ports. Cela semble justifier l'approche par les processus de Hawkes.

Ces processus ont également été utilisés par [Peng *et al.*, 2016] pour modéliser les risques extrêmes dans le cadre du cyber-risque avec un processus ponctuel d'intensité :

$$\lambda(t, x_t \mid F_t) = \lambda_g(t \mid F_t) f(x_t \mid F_t)$$

Avec x_t qui correspond au dépassement de valeur d'un certain seuil, f correspond à une densité provenant de la théorie des valeurs extrêmes. Et pour la composante temporelle $\lambda(t, x_t \mid F_t)$ différentes formes ont été testées dont celle de Hawkes, cette dernière sera décrite en détail dans la Section 2.3 qui suit .

Les résultats de ces di□érentes publications soulignent qu'il peut être pertinent d'utiliser les processus de Hawkes pour modéliser la fréquence des évènements cyber. Cela motive notre tournure vers ces processus, cependant les travaux précédents ont été réalisés dans le cadre de la cyber-sécurité plutôt que celui de la cyber-assurance. En particulier les données concernent un très grand nombre d'attaques sur quelques heures, sur des ports internet.

Pour notre étude, nous souhaitons nous placer dans le cadre d'une compagnie d'assurance qui modélise le cyber-risque. Les données sont donc sensiblement di□érentes puisqu'elles ne concernent que les attaques qui ont abouti, et ce à l'échelle de l'année. A notre connaissance il n'y a pas encore eu de travaux dans cette direction.

2.3 Les processus de Hawkes

Avec les arguments du chapitre précédent, nous avons décidé de modéliser la fréquence des cyber-attaques avec des processus de Hawkes. Ce chapitre présente une grande partie du cadre formel utilisé pour les modélisations qui suivront tout au long du mémoire.

Il présente en premier lieu les processus ponctuels, puis le cas particulier des processus de Hawkes, d'abord en une dimension (processus monovarié) puis en multi-dimensions (processus multivarié).

Par la suite, des algorithmes de simulations sont détaillés, puis, la fonction de vraisemblance, qui permettra d'estimer les paramètres de tels processus sur des données, est présentée. Pour conclure cette partie, des méthodes de qualité d'ajustement sont décrites.

2.3.1 Les processus ponctuels

Cette section permet de placer les processus de Hawkes dans le cadre plus général des processus ponctuels, elle définit notamment le concept d'intensité conditionnelle qui est indispensable à la compréhension de l'intéret du processus de Hawkes.

2.3.1.1 Intérêt et définition

Les processus ponctuels sont des processus pour lesquels une réalisation consiste en un motif de points dans un certain espace. Cet espace peut par exemple être la droite réelle R et ainsi représenter le temps, dans quel cas la réalisation du processus peut être interprétée comme des temps d'occurrences ou temps d'arrivée d'un phénomène aléatoire, par exemple les temps d'arrivée d'une file d'attente. Un autre exemple courant est le cas où cet espace est R^n, n 1, cela permet de représenter de façon jointe plusieurs informations, par exemple sur R^3 un processus ponctuel peut représenter des positions aléatoires dans l'espace.

Avant de définir mathématiquement le processus ponctuel, rappelons la définition d'une mesure de comptage, pour la suite nous nous plaçons sur un espace métrique S séparable, localement compact, muni de sa tribu borélienne $B(S)$.

Definition 2.3.1. Une mesure μ est dite de comptage si pour tout ensemble B borné (défini ici comme inclus dans un compact) : $\mu(B) < 1$ et $\mu(B)$ 2 N

Toute mesure de comptage μ sur S peut être écrite comme une somme de diracs :

$$\mu = \sum_{i=1}^{K} K_i \delta_{x_i} \tag{2.1}$$

avec : 0 K 1 et $0 < K_i < 1$ des entiers, et les x_i appartiennent à S. Les K_i sont les multiplicités des x_i.

Nous pouvons maintenant définir le processus ponctuel en tant que mesure aléatoire de comptage :

Definition 2.3.2. Notons M l'ensemble des mesures de comptage sur S. Munissons le de la tribu M qui est la plus petite tribu qui rend les applications μ 7 ! $\mu(B)$ mesurables, pour tout B mesurable.

Un processus ponctuel est une application mesurable d'un espace de probabilité vers (M, M).

Nous parlerons de processus ponctuel simple dans le cas ou toutes les multiplicités K_i sont égales à 1 presque sûrement, dans ce cas le lien avec un motif de point est évident à travers la représentation 2.1, le motif correspond aux x_i chargés par la mesure.

Par la suite nous ne serons concernés que par des processus ponctuels simples.

2.3.1.2 Intensité conditionnelle d'un processus ponctuel simple

Dans cette section nous nous plaçons dans le cadre de processus ponctuels simples sur R, ils peuvent donc être interprétés comme des temps d'arrivée d'un phénomène aléatoire.

Nous définissons maintenant un élément essentiel pour caractériser de tels processus : le processus d'intensité conditionnelle. Pour cela introduisons le processus de comptage :

$$N_t = N([0,t]) = \sum_{n \quad 1} 1_{(T_n \quad t)}$$

Où les $(T_n)_{n \quad 1}$ sont les temps d'arrivée (ordonnés) de notre phénomène aléatoire. Ce processus compte simplement le nombre de survenances de notre phénomène aléatoire jusqu'au temps actuel t.

Definition 2.3.3. Considérons un espace probabilisé (, F, P). Soit N un processus de comptage, le processus d'intensité conditionnelle associé λ est définit comme suit :

$$\lambda(t) = \lim_{h \,!\, 0} \mathsf{E}\left[\frac{N(t+h) \quad N(t)}{h} j F_t\right] = \lim_{h \,!\, 0} \frac{1}{h} \mathsf{P}\left[N(t+h) \quad N(t) > 0 j F_t\right] \quad , t \quad 0.$$

Avec F_t qui représente l'information disponible sur le processus de Hawkes jusqu'au temps t (non inclus). [1]

Cette intensité conditionnelle représente le risque qu'un évènement survienne dans l'intervalle infinitésimal $[t, t + dt[$. Elle est souvent notée $\lambda(t)$, par abus de notation, sans a□cher son conditionnement.

2.3.2 Les processus de Hawkes monovariés

Nous pouvons maintenant présenter le processus de Hawkes, commençons par le processus de Hawkes monovarié (c'est-à-dire en une dimension).

Le processus de Hawkes monovarié peut être défini comme un processus de comptage auto-excitant dont l'intensité a la forme :

$$\lambda(t) = \mu(t) + \int_{[0;t[} \phi(t - s) dN_s = \mu(t) + \sum_{T_n < t} \phi(t - T_n)$$

avec $\mu : \mathbb{R}^+ \to \mathbb{R}^+$
$\phi : \mathbb{R}^+ \to \mathbb{R}^+$

La somme dans l'intensité est responsable de la propriété d'auto-excitation, la fonction ϕ étant positive, chaque temps passé T_n contribue positivement à l'intensité au temps actuel t.

Le noyau ϕ représente l'évolution de cette influence au cours du temps. Il peut prendre beaucoup de formes di□érentes selon ce qui est modélisé.

- Un premier noyau classique est un noyau strictement décroissant, qui correspond au cas où un évènement passé a de moins en moins d'influence sur le risque présent au fur et à mesure que le temps passe, par exemple cela permet de modéliser les répliques sismiques. C'est le cas du noyau utilisé dans le modèle ETAS d'origine (Epidemic Type Aftershock Sequence) de la forme $\phi(a) = \frac{K}{(c+a)^p}$ avec c, a, p des constantes, ou encore du noyau exponentiel, qui de part ses avantages en termes de calculs (noyau markovien, etc.) est le plus étudié dans la littérature, avec $\phi(a) = \alpha \exp(-\beta a)$.
- Nous pouvons également imaginer que ce noyau représente le taux de fertilité d'un individu au cours de sa vie, dans quel cas il aura une forme d'abord croissante puis décroissante au-delà d'un certain âge. C'est par exemple le cas du noyau à retard de la forme $\phi(a) = \alpha a \exp(-\beta a)$ avec α, β des constantes, ou encore du noyau de Rayleigh, défini comme, $\phi(a) = \alpha a \exp(-\beta a^2)$

1. En particulier, le processus $(\lambda(t))_{t \geq 0}$ est N-prévisible

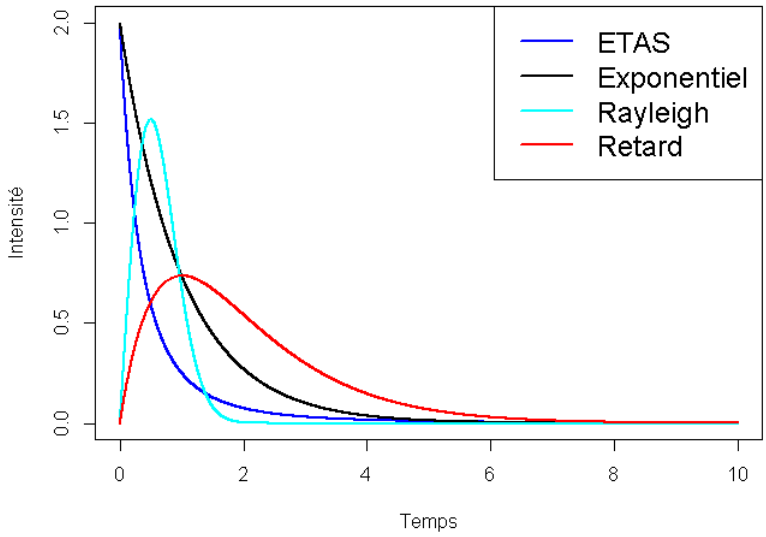


Figure 2.6 – Évolution de différents noyaux au cours du temps

Un cas très particulier est celui où le noyau ϕ est nul, dans ce cas le processus de Hawkes n'est autre qu'un processus de Poisson général d'intensité $\mu(t)$. La figure 2.6 représente un exemple de l'évolution de la valeur des noyaux cités précédemment, pour un jeu de paramètres fixés.

La fonction μ, déterministe, représente l'intensité, donc le risque, de base du processus, sans prendre en compte l'influence des évènements extérieurs.

Cette propriété d'excitation, semblable aux phénomènes de réaction en chaîne, engendre des clusters (au sens groupements d'attaques, par exemple visibles graphiquement, voir figures 2.9 et 2.10) dans la trajectoire d'un processus de Hawkes dans le sens où, dans des périodes d'excitation, des évènements sont plus probables de survenir et donc d'augmenter encore le risque d'avoir de nouveaux évènements. A contrario, dans le cas inverse, des périodes de faibles intensités apparaissent. D'où l'apparition de "groupements" dans les arrivées des évènements (les "clusters"), ainsi que de périodes de faible activité.

Ces processus ont été introduits la première fois par [HAWKES, 1971], ils ont connu un intérêt particulier en sismologie, afin de modéliser les répliques sismiques, mais ils ont également des applications en finance, en neurosciences ou encore en mathématiques des populations.

2.3.2.1 Représentation en population des processus de Hawkes

Une autre façon intuitive de comprendre le processus de Hawkes, est de le considérer d'un point de vue population, en tant que processus de naissance, la description est la suivante :

Considérons un processus de naissance avec immigration qui suit les règles suivantes :

- Les arrivées des immigrants suivent un processus de Poisson in-homogène de taux $\mu(t)$;
- Chaque immigrant génère des naissances selon un processus de Poisson inhomogène, avec un taux $\phi(a)$ où a est l'âge de l'immigrant ;
- Chaque individu engendré engendre lui même des naissances au même taux ϕ.

[Boumezoued, 2016b] montre que le processus résultant est un processus de Hawkes d'intensité : $\lambda(t) = \mu(t) + \sum_{T_n<t} \phi(t \quad T_n)$.

2.3.2.2 Exemples et interprétation des paramètres avec deux noyaux

Dans la suite de ce mémoire nous appliquerons les processus de Hawkes dans les cas particuliers où le noyau à la forme : $\phi(a) = \alpha \exp(\quad \beta a)$ et $\phi(a) = \alpha a \exp(\quad \beta a)$, que nous appellerons noyau exponentiel et noyau à retard. La valeur de a s'interprète comme l'âge d'un évènement, en a=0 c'est la survenance de l'évènement, l'évolution de la valeur du noyau au cours du temps correspond à l'évolution de l'impact d'un évènement sur l'intensité au cours du temps.

La manière dont évolue cet impact découle d'un rapport de force entre les deux paramètres α et β. Le noyau exponentiel atteint son maximum en 0 qui vaut α et est strictement décroisant. Le noyau à retard est croissant, atteint son maximum en $\frac{1}{\quad}$, qui vaut $\quad \exp(\quad 1)$ puis décroît.

Le premier noyau correspond donc à une excitation instantanée de l'intensité lors de la survenance d'un évènement. Le second correspond à une excitation progressive. Intuitivement le paramètre α est responsable de l'excitation et le paramètre β de la disparition de cette excitation.

2.3.2.3 Influence du paramètre β

Ci-dessous, en Figure 2.7, les graphiques représentent la valeur des noyaux au cours du temps, avec α = 1 et β qui prend les valeurs 1.5 et 4.

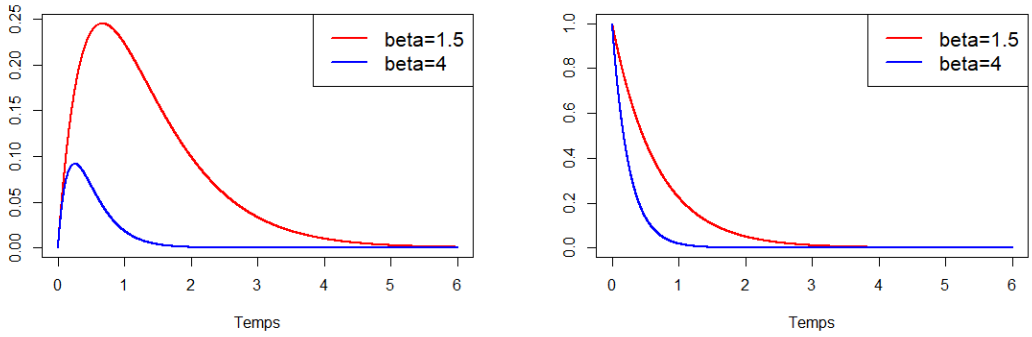


Figure 2.7 – Impact de β - à gauche le noyau à retard - à droite le noyau exponentiel

Plus β est élevé plus l'intensité décroît rapidement pour les deux noyaux. Remarquons également que, pour le noyau à retard, l'intensité maximale est a□ectée par β, elle est plus faible, et est atteinte plus tôt, avec un β élevé.

2.3.2.4 Influence du paramètre α

Le paramètre α correspond au paramètre d'excitation. En figure 2.8, l'évolution de la valeur des noyaux pour β = 2 et α qui prend les valeurs 0.5 et 1.5.

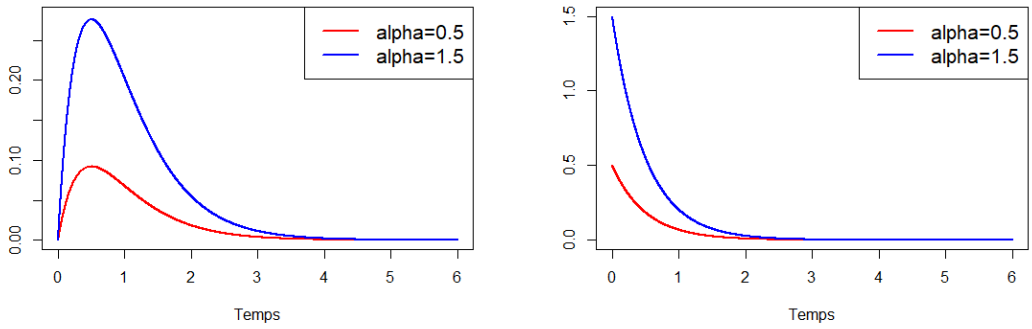


Figure 2.8 – Impact de α sur l'intensité

Pour le noyau exponentiel, seule la valeur maximale change, la décroissance est la même. Pour le noyau à retard, l'instant ou le maximum est atteint ne change pas, en revanche plus α est élevé plus le maximum est élevé.

2.3.2.5 Intensités et leur processus

Finalement voici un exemple de processus de Hawkes ainsi que de son intensité, pour chaque noyau.

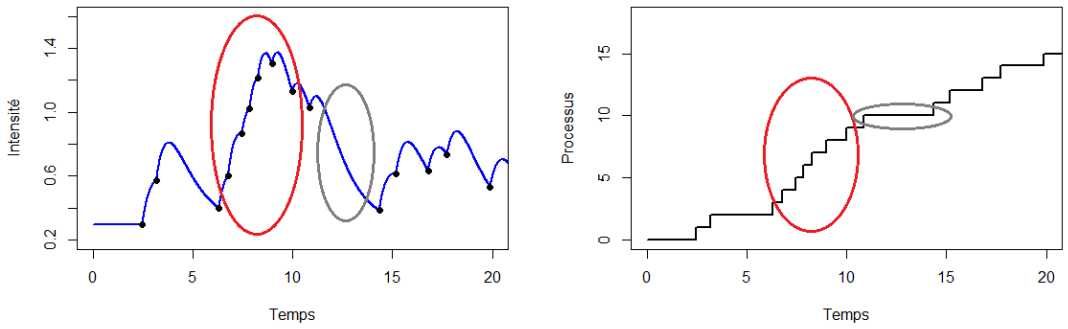


Figure 2.9 – Processus de Hawkes (droite) et son intensité (gauche) avec le noyau à retard

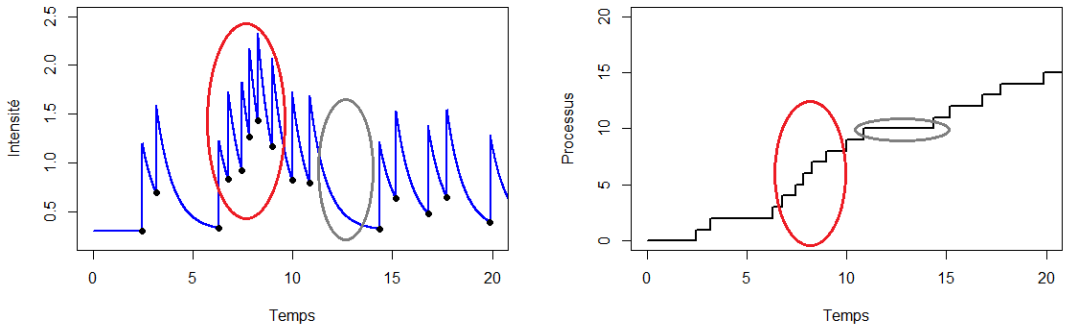


Figure 2.10 – Processus de Hawkes (droite) et son intensité (gauche) avec le noyau exponentiel

Dans les deux cas, nous retrouvons les motifs types du processus de Hawkes cités précédemment à savoir des périodes de forte activité (en rouge) ainsi que des périodes peu actives (en gris).

2.3.3 Les processus de Hawkes multivariés

Ce type de processus s'étend au cas multi-dimensionnel. Ceci permet, au-delà de la propriété d'auto-excitation, de modéliser des e□ets d'inter-excitation.

Considérons d processus de comptage : $(N_t^{(1)})_{t\ 0}, (N_t^{(2)})_{t\ 0}, ...(N_t^{(d)})_{t\ 0}, d\ 2$ N , définits comme :

$$N_t^{(j)} = N^{(j)}(t) = \sum_{n\ 1} 1_{(T_n^{(j)}\ t)}, j\ 2\ f1, .., dg$$

Où les $(T_n^{(j)})_{n\ 1}$ sont les temps d'arrivée (ordonnés) d'un phénomène aléatoire.
Le processus de Hawkes multivarié définit l'intensité $(\lambda_t^{(i)})_{t\ 0}$ du processus $(N_t^{(i)})_{t\ 0}, i\ 2\ f1, ..., dg$ de la façon suivante :

$$\lambda^{(i)}(t) = \mu^i(t) + \sum_{j=1}^{d} \int_{[0;t[} \phi_{i;j}(t \quad s) dN_s^{(j)} = \mu^i(t) + \sum_{j=1}^{d} \sum_{T_n^{(j)} < t} \phi_{i;j}(t \quad T_n^{(j)})$$

avec $\mu^{(i)} : R^+ \quad ! \ R^+$
$\phi_{i;j} : R^+ \quad ! \ R^+$

La fonction $\mu^{(i)}$ représente l'intensité de base, déterministe, du processus $(N_t^{(i)})_{t\ 0}$, c'est son intensité sans prendre en compte les autres évènements.

La double somme représente l'influence des évènements passés de tous les processus, sur l'intensité actuelle du processus $(N_t^{(i)})_{t\ 0}$. En particulier, chaque évènement passé, de chaque processus vient exciter l'intensité du processus $(N_t^{(i)})_{t\ 0}$. C'est cette partie de l'intensité qui force le phénomène d'auto-excitation ($i = j$) ainsi que d'inter-excitation ($i \neq j$).

Le noyau $\phi_{i;j}$ représente l'influence des évènements passés du processus $(N_t^{(j)})_{t\ 0}$ sur l'intensité du processus $(N_t^{(i)})_{t\ 0}$.

2.3.3.1 Exemple dans le cas exponentiel

Par exemple dans le cas du noyau exponentiel, l'intensité prend la forme suivante pour $1 \quad i \quad d$:

$$\lambda^{(i)}(t) = \mu^{(i)}(t) + \sum_{j=1}^{d} \int_{[0;t[} \phi_{i;j}(t \quad s) dN_s^{(j)} = \mu^{(i)}(t) + \sum_{j=1}^{d} \sum_{T_n^{(j)} < t} \alpha_{i;j} \exp(\ \beta_{i;j}(t \quad T_n^{(j)}))$$

Cette fois-ci :
— les $\alpha_{i;j}$ sont la valeur du saut de l'intensité $\lambda^{(i)}$ lors d'un saut du processus $(N_t^{(j)})_{t\ 0}$
— les $\beta_{i;j}$ correspondent à la vitesse de décroissance de l'impact de ce saut sur $(\lambda_t^{(i)})_{t\ 0}$

— $\mu^{(i)}$ correspond au taux de base du processus $(N_t^{(i)})_{t\ 0}$

Ci-dessous, en Figure 2.11 la représentation de l'intensité d'un processus de Hawkes bivarié avec : μ_1 = 1.2, μ_2 = 1 et $\alpha_{1;1}$ = 2, $\alpha_{1;2}$ = 0, $\alpha_{2;1}$ = 0.5, $\alpha_{2;2}$ = 1.5 et $\beta_{1;1}$ = 4, $\beta_{1;2}$ = 8, $\beta_{2;1}$ = 2, $\beta_{2;2}$ = 8

L'intensité du processus 1 en bleu, celle du processus 2 en rouge. Les points bleus correspondent aux sauts de l'intensité déclenchés par un saut du processus 1, les rouges ceux déclenchés par un saut du processus 2. Comme $\alpha_{2;1}$ est nul, le processus deux ne fait jamais sauter l'intensité du processus 1, mais la réciproque est fausse. Nous pouvons remarquer une décroissance plus rapide d'un saut de l'intensité 2 déclenché par le processus 2, qu'un saut que l'intensité 2 déclenché par le processus 1, cela traduit $\beta_{2;2} > \beta_{2;1}$

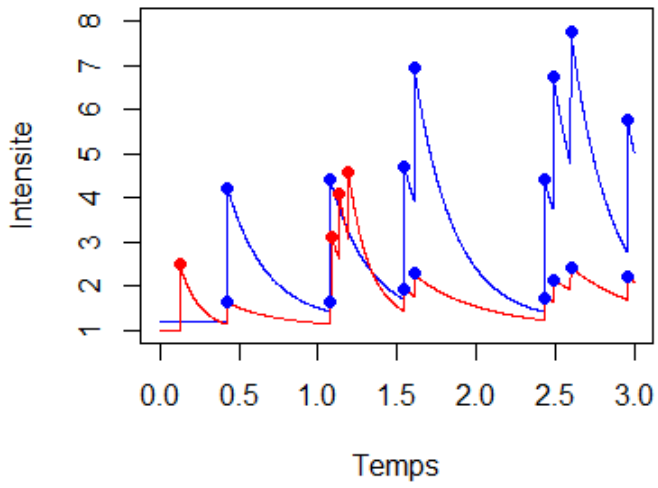


Figure 2.11 – Intensité d'un processsus de Hawkes bivarié

2.3.4 Simulation des processus de Hawkes

Les processus de Hawkes ont été présentés formellement, il est maintenant question de leur application, notamment comment simuler des processus de Hawkes, comment estimer leurs paramètres et comment vérifier s'ils sont adaptés à nos données.

Une méthode de simulation du processus de Hawkes est basée sur la simulation de processus de Poisson inhomogènes, les paragraphes suivants expliquent ces deux méthodes, une description plus détaillée est par exemple faite par [Chen, 2016].

2.3.4.1 L'algorithme de *Thinning* de Lewis

Une façon de simuler des trajectoires d'un processus de Poisson inhomogène est d'utiliser l'algorithme dit de *Thinning*, proposé par [Lewis et Shedler, 1978]. L'algorithme est basé sur le théorème suivant :

En considérant un processus de Poisson homogène d'intensité λ, observé sur une période $[0, T]$, et en notant ses n_T temps d'arrivée observés $t_1, ..., t_{n_T}$. Supposons que chaque temps t_k est supprimé avec une probabilité 1 $\lambda(t_k)/\lambda$, où $\lambda(.)$ est une fonction d'intensité (déterministe, positive) telle que pour 0 t T nous avons $\lambda(t)$ λ, alors les temps conservés forment une réalisation d'un processus de Poisson inhomogène d'intensité $\lambda(t)$ sur $[0, T]$.

Pour générer une réalisation d'un processus de Poisson inhomogène d'intensité $\lambda(.)$ connaissant une borne λ, l'algorithme consiste donc à simuler des temps d'arrivée d'un processus de Poisson homogène d'intensité λ, (par exemple en simulant des temps d'inter-arrivées selon des lois exponentielles indépendantes de paramètre λ), chaque temps est ensuite sélectionné comme expliqué ci-dessus. L'algorithme en pseudo-code est en Annexe B.

Ci-dessous, en Figures 2.12 et 2.13 un exemple de simulation d'un processus de Poisson inhomogène d'intensité linéaire : $\lambda(t)$ = 0.03 + 0.1 t sur l'intervalle $[0, 20]$, avec comme choix de borne : $\lambda(20)$ qui vaut 2.03.

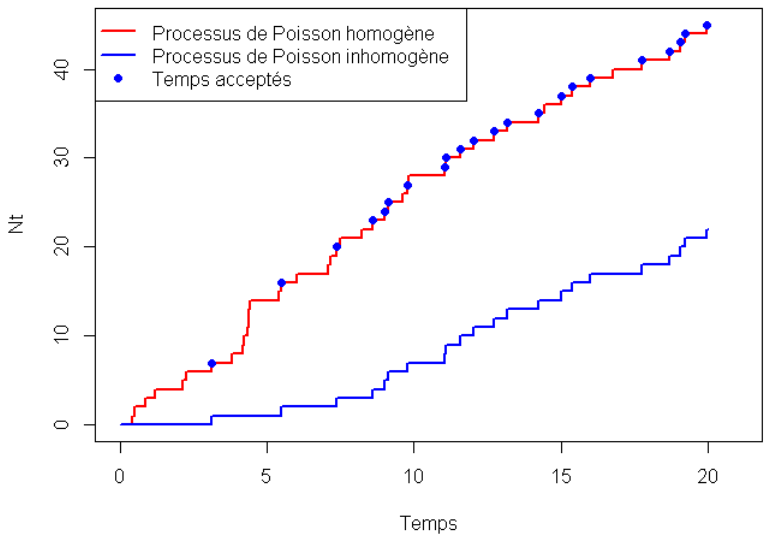


Figure 2.12 – Exemple de simulation d'un processus de Poisson inhomogène - partie 1

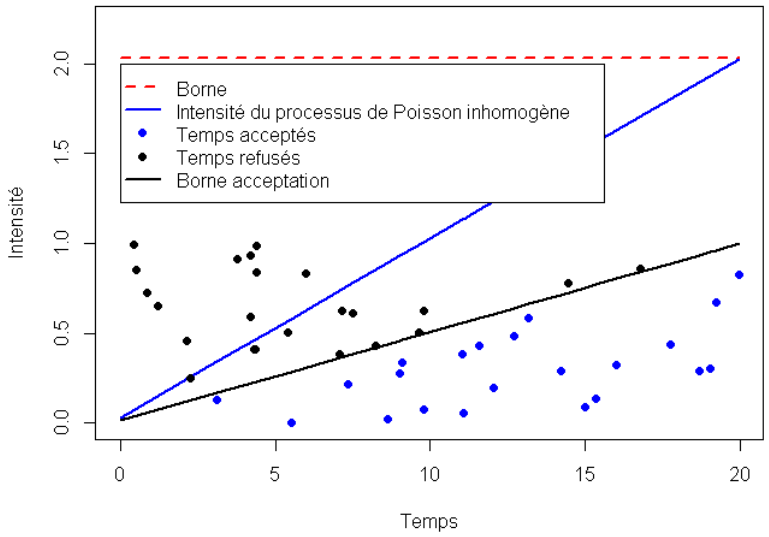


Figure 2.13 – Exemple de simulation d'un processus de Poisson inhomogène - partie 2

Notons que, à mesure que le temps augmente, les temps d'arrivée du processus de Poisson homogène ont de plus en plus tendance à être acceptés, ceci vient de l'intensité linéaire strictement croissante du processus que nous souhaitons simuler. En particulier plus le temps s croît plus les tests de la forme $D \quad \lambda(s)/\lambda$ (cf algorithme en Annexe B) ont de chances d'être acceptés car le rapport $\lambda(s)/\lambda$ ne fait que croître.

Ces tests sont visibles sur l'image inférieure, chaque point correspond à une réalisation de la loi uniforme sur $[0,1]$, le test, pour un temps s, est accepté si le point est inférieur à la borne d'acceptation (en noir) $\lambda(s)/\lambda$.

2.3.4.2 L'algorithme de *Thinning* modifié d'Ogata

[Ogata, 1981] propose un algorithme permettant de simuler un processus ponctuel, connaissant son intensité conditionnelle. En particulier cela fonctionne pour le processus de Hawkes. Il fonctionne selon la remarque suivante : entre deux temps d'arrivée successifs T_k, T_{k+1}, l'intensité du processus de Hawkes est déterministe.

En se basant sur cette remarque, supposons que nous avons simulé les k premiers temps : $t_1, ..., t_k$, d'un processus de Hawkes d'intensité $\lambda_{Hawkes}(s)$. Nous connaissons l'intensité du processus en t_k, et jusqu'au prochain temps T_{k+1} l'intensité est déterministe, nous pouvons alors simuler le prochain temps d'inter-arrivée $T_{k+1} \quad t_k$ avec l'algorithme de Lewis, comme étant le premier temps d'arrivée d'un processus de Poisson inhomogène démarrant en $t_0 = t_k$, d'intensité déterministe $\lambda_{Poisson}(t) = \lambda_{Hawkes}(t), t \quad t_k$.

Une fois le temps t_{k+1} généré, il su□t de mettre à jour l'intensité du processus de Hawkes en prenant en compte son influence (par exemple la faire sauter dans le cas

exponentiel) puis de recommencer cet algorithme.

Un point important est de mettre à jour la borne λ de l'algorithme de Lewis à chaque début d'intervalle t_k, t_{k+1}.

La figure 2.14 représente le principe de l'algorithme dans le cadre de la simulation d'un processus de Hawkes monovarié avec noyau exponentiel.

L'extrémité gauche de chaque flèche noire représente le lancement d'une simulation d'un processus de Poisson inomogène avec pour intensité l'intensité décroissante du processus de Hawkes sur ce segment. L'extrémité droite représente la survenance du premier temps de ce processus de Poisson inhomogène simulé. Cela correspond à une survenance de notre processus de Hawkes, et provoque donc un saut dans son intensité. La borne (en rouge) est donc mise à jour, puis le même algorithme est e□ectué.

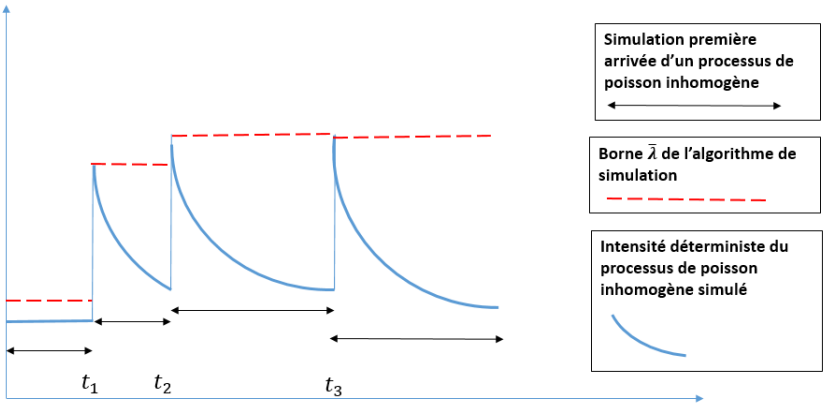


Figure 2.14 – Simulation d'un processus de Hawkes

La procédure de Thinning peut également se faire avec le point de vue population, voir par exemple [Boumezoued, 2016a].

2.3.4.3 Simulation d'un processus multivarié

Pour finir, il est possible de simuler des processus de Hawkes multivariés, cette fois, l'algorithme se base sur le principe qui suit :

Considérons un processus de Hawkes multivarié de dimension d, $(N_t^{(1)})_{t\ 0}, ...(N_t^{(d)})_{t\ 0}$, d 2 N . En simulant un processus d'intensité $\lambda(t) = \sum_{i=1}^{d} \lambda^{(i)}(t)$ et en associant une marque M_i 2 f1, ..., dg à chaque saut T_i nous obtenons une suite $(T_n, M_n)_{n\ 1}$. Si la marque associée à T_n est la marque M_n 2 f1, ..., dg telle que :

$$P(M_n = i) = \frac{\lambda^{(i)}(T_n)}{\sum_{j=1}^{d} \lambda^{(j)}(T_n)}$$

alors pour $i \in \{1,...,d\}$ le processus des temps ordonnés : $\{T_n : M_n = i\}$ est un processus de Hawkes d'intensité $\lambda^{(i)}$.

L'algorithme de simulation d'un processus de Hawkes multivarié consiste donc à simuler un processus monovarié avec l'algorithme d'Ogata, et à associer à chaque temps une marque, avec les probabilités décrites ci-dessus.

Les deux derniers algorithmes, en pseudo-code, sont en Annexe B. Le choix de la borne λ y est également discuté dans le cadre des noyaux utilisés dans ce mémoire.

Remarque : En utilisant le fait que l'algorithme d'Ogata se base sur les temps passés pour simuler les temps futurs, il est possible de simuler le prolongement d'un processus de Hawkes qui aurait généré tous les temps d'un historique passé dont nous disposons, pour cela il suffit de démarrer l'algorithme, non pas avec un historique vide mais avec un historique de temps passés générés qui correspond à l'historique dont nous disposons. Cela signifie que lors de nos applications nous pourrons simuler des processus de Hawkes qui contiennent dans leur passé, l'historique dont nous disposons.

2.3.5 Fonction de vraisemblance

Par la suite, nous calibrerons des processus de Hawkes sur des données en utilisant la méthode du maximum de vraisemblance. Pour obtenir l'expression de la vraisemblance, nous partons de la vraisemblance générale d'un processus ponctuel en une dimension, dont le détail est donné en Annexe C.1.

En reprenant les mêmes notations, à savoir : supposons que nous avons observé les m temps $(t_n)_{1 \leq n \leq m}$ sur l'intervalle d'observation $[0,t]$, il ne reste plus qu'à remplacer l'intensité du processus ponctuel par celle d'un processus de Hawkes pour finalement obtenir :

$$\log L(\mu,\phi) = \int_0^t \mu(s)\mathrm{d}s \quad \int_0^t \sum_{t_n<s} \phi(s \quad t_n)\mathrm{d}s + \sum_{n=1}^{m} \log\left(\mu(t_n) + \sum_{k=1}^{n \quad 1} \phi(t_n \quad t_k)\right) \quad (2.2)$$

Dans le cas multivarié, supposons que nous sommes en dimension d et que nous observons les temps $((t_n^i)_{1 \leq n \leq m_i})_{1 \leq i \leq d}$ sur $[0,t]$, alors nous avons pour fonction de vraisemblance :

$$\log L\left((\mu_i)_{1 \leq i \leq d}, (\phi_{i;j})_{1 \leq i;j \leq d}\right) = \sum_{i=1}^{d} \log L^{(i)}\left(\mu_i, (\phi_{i;j})_{1 \leq j \leq d}\right) \quad (2.3)$$

(Voir par exemple [Daley et Vere-Jones, 2003]), avec pour $1 \leq i \leq d$

$$\log L^{(i)}\left(\mu_i, (\phi_{i;j})_{1 \leq j \leq d}\right) = \int_0^t \lambda^{(i)}(s)\mathrm{d}s + \sum_{n=1}^{m_i} \log\left(\lambda^{(i)}(t_n^{(i)})\right) \quad (2.4)$$

qui correspond à la log-vraisemblance du processus $(N_t^{(i)})_{t\ 0}$ avec les temps observés $\left(t_n^{(i)}\right)_{1\ n\ m_i}$. Il ne reste plus qu'à remplacer les intensités $\lambda^{(i)}$ par leur expression donnée en 2.3.3 pour obtenir l'expression finale de la log-vraisemblance d'un processus de Hawkes multivarié :

$$\begin{aligned}\log L(\mu,\phi) = & \sum_{i=1}^{d}\int_0^t \lambda^{(i)}(s)\mathrm{d}s + \sum_{i=1}^{d}\sum_{n=1}^{m_i}\log\lambda^{(i)}(t_n^{(i)}) \\ = & \sum_{i=1}^{d}\int_0^t\left(\mu^{(i)}(s) + \sum_{j=1}^{d}\int_0^s \phi_{i;j}(s\quad u)\mathrm{d}N_u^{(j)}\right)\mathrm{d}s \\ & + \sum_{i=1}^{d}\sum_{n=1}^{m_i}\log\left(\mu^{(i)}(t_n^{(i)}) + \sum_{j=1}^{d}\int_0^{t_n^{(i)}}\phi_{i;j}(t_n^{(i)}\quad s)\mathrm{d}N_s^{(j)}\right)\end{aligned} \tag{2.5}$$

En pratique (pour coder la vraisemblance), il faut réécrire la vraisemblance comme suit :

$$\begin{aligned}\log L(\mu,\phi) = & \sum_{i=1}^{d}\int_0^t\left(\mu^{(i)}(s) + \sum_{j=1}^{d}\sum_{t_k^{(j)}<s}\phi_{i;j}(s\quad t_k^{(j)})\right)\mathrm{d}s \\ & + \sum_{i=1}^{d}\sum_{n=1}^{m_i}\log\left(\mu^{(i)}(t_n^{(i)}) + \sum_{j=1}^{d}\sum_{t_k^{(j)}<t_n^{(i)}}\phi_{i;j}(t_n^{(i)}\quad t_k^{(j)})\right)\end{aligned} \tag{2.6}$$

La complexité de calcul apparaît sous cette forme. Dans le cas particulier du noyau exponentiel, il est possible de l'écrire sous une forme récursive pour accélérer les calculs, voir par exemple [Jaisson, 2015].

2.3.6 Méthodes de comparaison des calibrages

Dans ce chapitre nous allons calibrer di□érents processus de Hawkes sur des données réelles, afin de comparer les di□érents modèles testés, nous nous sommes basés sur trois critères :

- La valeur de la fonction de vraisemblance
- La somme des écarts absolus entre les prédictions (moyennes) et le nombre d'attaques réel
- Des tests statistiques de qualité d'ajustement

Les deux derniers points ne sont pas triviaux et nécessitent d'être détaillés.

2.3.6.1 Détermination de l'espérance du Processus de Hawkes non stationnaire pour la prédiction moyenne

Afin de déterminer la prédiction moyenne sans simulations (ce qui permet un grand gain de temps) nous devons au préalable déterminer l'espérance du processus de Hawkes.

Nous avons décidé de faire ce calcul dans le cas général où le processus n'est pas stationnaire. Rappelons que le processus de Hawkes multivarié avec noyau exponentiel définit l'intensité $(\lambda_t^{(i)})_{t\ 0}$ du processus $(N_t^{(i)})_{t\ 0}, i\ 2\ f1,...,dg$ de la façon suivante :

$$\lambda^{(i)}(t) = \mu^i(t) + \sum_{j=1}^{d} \int_{[0;t[} \phi_{i;j}(t \quad s) dN_s^{(j)} = \mu^{(i)}(t) + \sum_{j=1}^{d} \sum_{T_n^{(j)} < t} \alpha_{i;j} \exp(\ \beta_{i;j}(t \quad T_n^{(j)}))$$

$$\text{avec} \begin{cases} \mu^{(i)} : \mathsf{R}^+ \quad ! \ \mathsf{R}^+ \\ (\alpha_{i;j})_{1\ i;j\ d} \ 2\ \mathsf{R}_+^{d\ d} \\ (\beta_{i;j})_{1\ i;j\ d} \ 2\ \mathsf{R}_+^{d\ d} \end{cases}$$

Une méthode pour calculer les moments du processus de Hawkes non stationnaire (avec des noyaux plus généraux que l'exponentiel) est explicitée dans le cas monovarié par [Boumezoued, 2016b]. Nous reprenons ici les mêmes arguments adaptés au cas multivarié pour déterminer l'espérance du processus de Hawkes dans le cas exponentiel.

La pyramide des âges :

La mesure aléatoire $Z_t^{(i)}(\mathrm{d}a), i\ 2\ f1,..,dg$ définit comme :

$$Z_t^{(i)}(\mathrm{d}a) = \int_{(0;t]} \delta_{t\ s}(\mathrm{d}a) \mathrm{d}N_s^{(i)} = \sum_{n=1}^{N_t^{(i)}} \delta_{t\ T_n^{(i)}}(\mathrm{d}a)$$

compte les individus du processus $(N_t^{(i)})_{t\ 0}$ d'âge $\mathrm{d}a$ au temps t. Un intérêt de cette mesure est de l'intégrer contre une fonction f en définissant :

$$hZ_t^{(i)}, fi = \int_{\mathsf{R}^+} f(a) Z_t^{(i)}(\mathrm{d}a) = \int_{(0;t]} f(t \quad s) \mathrm{d}N_s^{(i)}$$

par exemple cela permet de représenter $N_t^{(i)}$ avec $N_t^{(i)} = hZ_t^{(i)}, 1i$ ou encore l'intensité du processus $(N_t^{(i)})_{t\ 0}$ par :

$$\lambda^{(i)}(t) = \mu^{(i)}(t) + \sum_{j=1}^{d} hZ_t^{(j)}, \phi_{i;j} i$$

Pour les calculs qui suivent nous utiliserons la propriété suivante :

Propriété : Pour toute fonction dérivable $f : \mathsf{R}_+ \ ! \ \mathsf{R}$ nous avons :

$$hZ_t^{(i)}, fi = f(0) hZ_t^{(i)}, 1i + \int_0^t hZ_s^{(i)}, f^{\emptyset} i \mathrm{d}s$$

En particulier, le premier terme de cette expression fait référence aux sauts correspondant à l'arrivée d'individus d'âge zéro, le second terme, quant à lui, illustre le phénomène de vieillissement. Pour une démonstration de cette propriété voir [Boumezoued, 2016b], Lemme 1.

Dynamique générale

Considérons le vecteur :

$$X_t = \left(hZ_t^{(1)}, 1i, ..., hZ_t^{(d)}, 1i, hZ_t^{(1)}, \phi_{1;1}i, ..., hZ_t^{(1)}, \phi_{d;1}i, ..., hZ_t^{(d)}, \phi_{1;d}i, ..., hZ_t^{(d)}, \phi_{d;d}i\right)$$

et étudions sa dynamique. En particulier intéressons nous à la dynamique de $hZ_t^{(j)}, \phi_{i;j}i$ pour 1 i, j d, en gardant en tête que $\phi_{i;j}$ représente l'influence de $(N_t^{(j)})_{t\ 0}$ sur l'intensité de $(N_t^{(i)})_{t\ 0}$, et donc que $hZ_t^{(j)}, \phi_{i;j}i$ représente l'influence des évènements de $(N_t^{(j)})_{t\ 0}$, au temps t, sur l'intensité de $(N_t^{(i)})_{t\ 0}$.

$$hZ_t^{(j)}, \phi_{i;j}i = \phi_{i;j}(0)N_t^{(j)} + \int_0^t hZ_s^{(j)}, \phi_{i;j}^0 i\mathrm{d}s = \phi_{i;j}(0)N_t^{(j)} \quad \beta_{i;j}\int_0^t hZ_s^{(j)}, \phi_{i;j}i\mathrm{d}s \tag{2.7}$$

En di□érenciant nous obtenons :

$$\mathrm{d}hZ_t^{(j)}, \phi_{i;j}i = \phi_{i;j}(0)\mathrm{d}N_t^{(j)} \quad \beta_{i;j}hZ_t^{(j)}, \phi_{i;j}i\mathrm{d}t \tag{2.8}$$

Maintenant, posons $g_{i;j}(t) = \mathrm{E}\left[hZ_t^{(j)}, \phi_{i;j}i\right]$ et passons à l'espérance sur (2.8) en utilisant le fait que $\mathrm{E}[\mathrm{d}N_t^{(j)}] = \mathrm{E}[\lambda^j(t)]\mathrm{d}t$:

$$\begin{aligned}\mathrm{dE}\left[hZ_t^{(j)}, \phi_{i;j}i\right] &= \phi_{i;j}(0)\mathrm{E}\left[\lambda^{(j)}(t)\right]\mathrm{d}t \quad \beta_{i;j}\mathrm{E}\left[hZ_t^{(j)}, \phi_{i;j}i\right]\mathrm{d}t \\ &= \phi_{i;j}(0)\mathrm{E}\left[\mu^{(j)}(t)\mathrm{d}t + \sum_{k=1}^{d} hZ_t^{(k)}, \phi_{j;k}i\mathrm{d}t\right] \quad \beta_{i;j}g_{i;j}(t)\mathrm{d}t\end{aligned} \tag{2.9}$$

Finalement, en utilisant le fait que la mesure de Lebesgues ne charge pas de points nous obtenons :

$$g_{i;j}^0(t) = \phi_{i;j}(0)\mu^{(j)}(t) + \phi_{i;j}(0)\sum_{k=1}^{d} g_{j;k}(t) \quad \beta_{i;j}g_{i;j}(t) \tag{2.10}$$

Maintenant étudions l'espérance de : $hZ_t^{(k)}, 1i$ pour 1 k d, en rappelant que $hZ_t^{(k)}, 1i = N_t^{(k)}$:

$$\begin{aligned}\mathrm{dE}\left[hZ_t^{(k)}, 1i\right] &= \mathrm{E}\left[\mathrm{d}N_t^{(k)}\right] = \mathrm{E}\left[\lambda_t^{(k)}\right]\mathrm{d}t \\ &= \mathrm{E}\left[\mu^{(k)}(t) + \sum_{l=1}^{d} hZ_t^{(l)}, \phi_{k;l}i\right]\mathrm{d}t\end{aligned} \tag{2.11}$$

Ce qui nous donne, en posant $g_k(t) = \mathrm{E}\left[\langle Z_t^{(k)}, 1\rangle\right]$:

$$g_k'(t) = \mu^{(k)}(t) + \sum_{l=1}^{d} g_{k;l}$$

En considérant le vecteur : $G(t) = \left(g_1(t), ..., g_d(t), g_{1;1}(t), ..., g_{1;d}(t), ..., g_{d;1}(t), ..., g_{d;d}(t)\right)$ ce système peut se réecrire sous la forme :

$$G'(t) = AG(t) + B$$

B est définit comme suit :
Pour 1 i d, $[B]_i = \mu^{(i)}(t)$
Pour $d+1$ i d^2+d tel que $i = ad+b$, $a,b \in \mathbb{N}$, $[B]_i = \phi_{a;b}(0)\mu^{(b)}(t)1_{b>0} + \phi_{a\ 1;d}(0)\mu^{(d)}(t)1_{b=0}$

A est définie comme suit :
Pour 1 m d : $[A]_{m;n} = 1$ si $md+1$ n $md+d$, et 0 sinon.
Pour $d+1$ m d^2+d tel que $m = ad+b, a,b \in \mathbb{N}$: si $b > 0$,
$[A]_{m;n} = \phi_{a;b}(0)$ si $bd+1$ n $bd+d$
$[A]_{m;n} = \beta_{a;b}$ pour $n = ad+b$ et
$[A]_{m;n} = \phi_{a;b}(0)$ $\beta_{a;b}$ pour $n = ad+b$ si $bd+1$ $ad+b$ $bd+d$
Si $b = 0$ $[A]_{m;n} = \phi_{a\ 1;d}(0)$ si d $d+1$ n d $d+d$
$[A]_{m;n} = \beta_{a\ 1;d}$ pour $n = d$ $d+b$ et
$[A]_{m;n} = \phi_{a\ 1;d}(0)$ $\beta_{a\ 1;d}$ pour $n = d$ $d+b$ si d $d+1$ $ad+d$ d $d+d$

Finalement, une solution de ce système linéaire a la forme :

$$G(t) = G(t_0)\exp(A(t - t_0)) + \int_{t_0}^{t} \exp(A(t - s))B(s)\mathrm{d}s$$

Les d premières coordonnées de ce vecteur G correspondent aux espérances des d dimensions du processus de Hawkes, les exponentielles de matrice sont calculées numériquement.

Remarque 1 : La démonstration se reprend de la même façon pour obtenir des espérances conditionnelles plutôt que des espérances. Cela permettra par la suite d'obtenir des prédictions en tenant compte du passé.

Remarque 2 : L'esprit reste le même pour calculer l'espérance dans le cas du noyau à retard, il suffit d'effectuer les mêmes calculs en ajoutant dans le vecteur X_t les termes $\langle Z_t^{(j)}, \alpha_{i;j}\exp(-\beta_{i;j}a)\rangle$ pour $1 \leq i,j \leq d$.

2.3.6.2 Tests de qualité d'ajustement

Toujours en considérant notre processus de Hawkes multivarié de dimension d :

$(N_t^{(1)})_{t\ 0}, (N_t^{(2)})_{t\ 0}, ...(N_t^{(d)})_{t\ 0}, d$ *2* N , et en notant $(T_k^{(i)})_{k\ 1}$ les temps de saut du processus $(N_t^{(i)})_{t\ 0}$ avec i *2 f*1, ..., d*g*

Les tests d'ajustements que nous avons utilisés sont basés sur la propriété suivante :

Propriété :

Définissons pour k 1 :

$$\tau_k^{(i)} = \int_0^{T_k^{(i)}} \lambda^{(i)}(t)\mathrm{d}t$$

Avec comme convention $T_0^{(i)}$ = 0 i *2 f*1, ..., d*g*. Alors les $(\tau_k^{(i)})_{k\ 1}$, peuvent être interprétés comme des temps transformés, et sont les temps de sauts d'un processus de Poisson homogène d'intensité 1.

Cela permet d'e□ectuer des tests sur nos processus de Hawkes calibrés, en notant $\widehat{\lambda}(t)$ l'intensité estimée, si le processus sous-jacent est bien un processus de Hawkes avec cette intensité, les temps

$$\theta_k^{(i)} = \tau_k^{(i)} \quad \tau_{k\ 1}^{(i)},\ k \quad 1$$

sont indépendants et distribués selon une loi exponentielle de paramètre 1. Nous réaliserons donc par la suite des tests d'indépendance, par exemple avec un test de Ljung-Box, ainsi que des tests d'adéquation à la loi exponentielle, par exemple avec un test de Kolmogorov-Smirnov.

2.4 Un premier calibrage sur deux types d'attaques

2.4.1 Choix du modèle

Cette partie a un double objectif : en premier lieu se rassurer sur la capacité des Hawkes à s'ajuster sur ce type de données, et en second lieu montrer l'intéret d'un *drift* dans le taux de base $\mu(t)$.

Pour cela nous avons calibré un processus de Hawkes bivarié sur deux des types d'attaques les plus représentées à savoir THEFT/LOSS ainsi que DISC, qui ont été évoqués en section 2.1. Le calibrage a été e□ectué sur la période 2011-2016 dans le but de prédire le nombre d'attaques sur 2017.

Deux calibrages di□érents ont été e□ectués avec le noyau exponentiel qui a été décrit en Section 2.3.2.2, en choisissant pour simplifier $\beta_{i;j} = \beta_i$, 1 i, j 2.

Le premier calibrage considère $\mu_i(t) = \mu_i$ 0 pour tout temps t *2* R et 1 i 2.

Le second calibrage considère un *drift* : $\mu_i(t) = \mu_{i;0} + \gamma_i t$ avec $(\mu_{i;0}, \gamma_i)$ *2* R_+ R pour tout temps t *2* R et 1 i 2.

L'intérêt de considérer un *drift* est de tenter de capter les tendances plus ou moins évidentes qui apparaissent dans la fréquence des cyber-attaques au cours du temps en Figures 2.15 et 2.16.

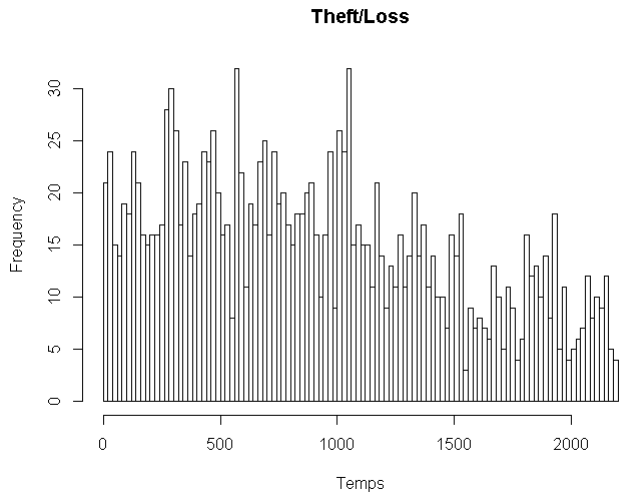


Figure 2.15 – Histogramme du nombre d'attaques de type THEFT/LOSS au cours du temps - période 2011/2016 - Échelle de temps journalière

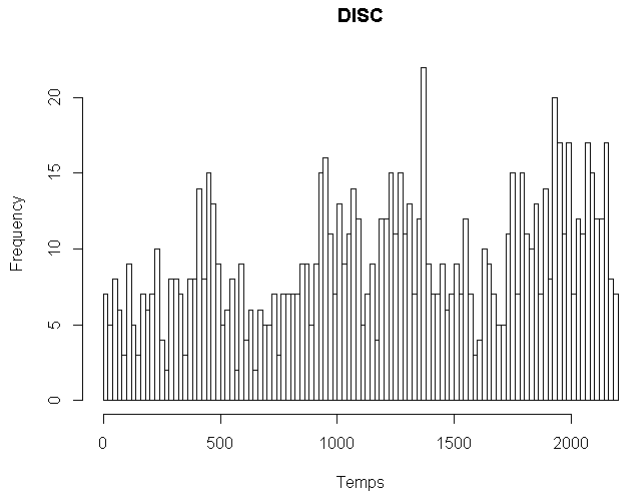


Figure 2.16 – Histogramme du nombre d'attaques de type DISC au cours du temps - période 2011/2016 - Échelle de temps journalière

2.4.2 Calibrage et simulations

L'estimation des paramètres s'est e□ectuée par la méthode du maximum de vraisemblance. La log-vraisemblance du processus de Hawkes n'étant pas toujours une fonction concave selon le noyau choisi (ce qui est le cas dans les prochaines parties), l'algorithme de Nelder-Mead, un algorithme de type simplexe, a été utilisé. Cet algorithme nécessite seulement de pouvoir évaluer la fonction étudiée, sans devoir évaluer de dérivée. Une deuxième motivation pour utiliser cet algorithme est que la fonction R constrOptim permet d'utiliser l'algorithme de Nelder-Mead sous contraintes linéaires. Ces contraintes sont nécessaires, d'une part pour forcer les paramètres $(\alpha_{i;j})_{1 \ i;j \ 2}$, $(\beta_i)_{1 \ i \ 2}$ et $(\mu_{i;0})_{1 \ i \ 2}$, à être positifs, et d'autre part pour contraindre le terme $\mu_{i;0} + \gamma_i t$ à être positif également, pour t appartenant à une période choisie, par exemple la période de calibrage. Cette dernière contrainte permet de ne pas avoir d'intensité négative sur une période choisie.

Une fois les paramètres calibrés, 10 000 trajectoires du processus ont été e□ectuées pour l'année 2017. A ce stade le passé est pris en compte deux fois lors des simulations, tout d'abord, comme tout modèle qui est calibré, le passé est pris en compte dans les paramètres qui ont été estimés. Ensuite le processus de Hawkes simulé est le prolongement d'un processus de Hawkes qui a pour temps de survenances passés, l'historique dont nous disposons, ce point a été évoqué dans la remarque en 2.3.4.3.

2.4.3 Analyse des résultats

Les histogrammes des nombres d'attaques prédits sont en en Figure 2.17 pour le premier calibrage, et en Figure 2.18 pour le second calibrage. Il apparaît que le premier calibrage (sans *drift*) n'est pas capable de prédire correctement la distribution des attaques à un an (notamment sur THEFT/LOSS), contrairement au calibrage avec *drift*.

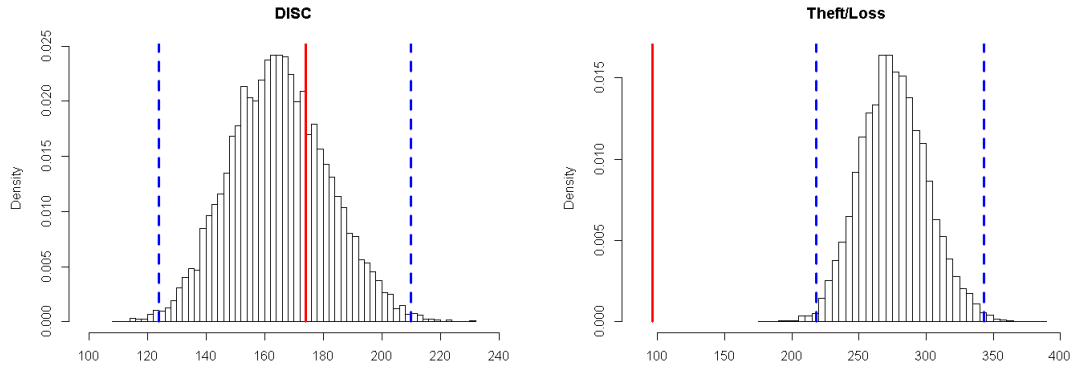


Figure 2.17 – Prédictions premier calibrage pour les attaques de type DISC et THEFT/LOSS - En rouge le réel - En bleu les quantiles à 0.5% et 99.5% des simulations

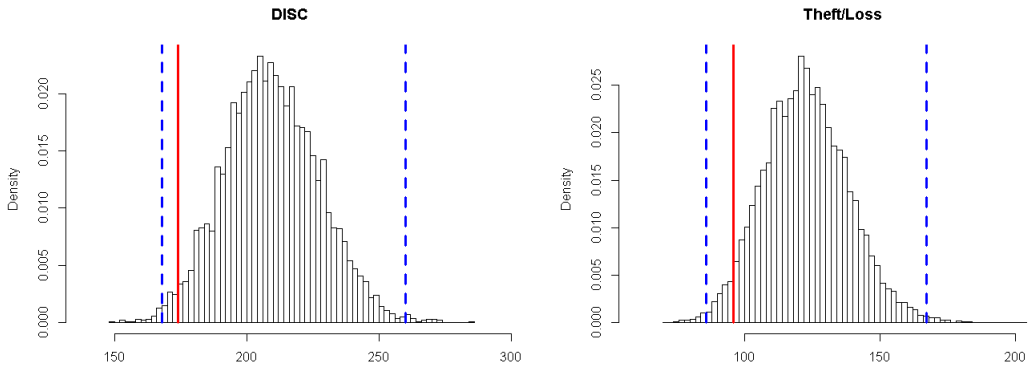


Figure 2.18 – Prédictions second calibrage pour les attaques de type DISC et THEFT/LOSS - En rouge le réel - En bleu les quantiles à 0.5% et 99.5% des simulations

Les tests statistiques cités en 2.3.6.2, à savoir un test d'indépendance (Ljung-Box) et un test d'adéquation avec la loi exponentielle de paramètre 1 (Kolmogorov-Smirnov), sur les inter-temps transformés ne sont pas concluants à 5% pour THEFT/LOSS sous le premier modèle (p-value<0.05), en revanche, sous le second modèle, tous les tests sont acceptés. Ces résultats sont respectivement en Tables 2.2 et 2.3.

	Ljung-Box (Lag=4)	Kolmogorov-Smirnov
DISC	0.0843	0.1325
THEFT/LOSS	0.0039	0.0327

Table 2.2 – Tests d'adéquations premier calibrage

	Ljung-Box (Lag=4)	Kolmogorov-Smirnov
DISC	0.5277	0.2725
THEFT/LOSS	0.1760	0.9597

Table 2.3 – Tests d'adéquations second calibrage

Ces tests sont e□ectués avec un retard de 4 dans tout le mémoire. Le retard peut faire varier le résultat du test, globalement le fait d'augmenter le retard dégrade la p-value.

Finalement, sur cet exemple, le processus de Hawkes semble valide statistiquement, et permet de prédire correctement la distribution future du nombre d'attaques.

2.5 Les processus de Hawkes sur une segmentation fine

Afin d'être en mesure de traiter tous les cas de violations de données, il est nécessaire de se calibrer sur la base de données entière et non de se restreindre à certains segments comme dans l'étude précédente. Di□érents choix sont alors possibles concernant la segmentation. Nous souhaitons dans cette section, commencer par évaluer la capacité prédictive des processus de Hawkes sur une segmentation fine. Cela permet également de profiter d'une compréhension plus fine des interactions potentielles entre les di□érents types d'attaques, et donc une meilleure compréhension du risque.

Bien qu'un avantage du processus de Hawkes réside dans l'interprétation naturelle de ses paramètres comme évoqué en 2.3.2.2, le nombre de paramètres, donc la complexité, augmente rapidement avec la dimension du processus, ceci est dû aux paramètres (d'interactions) des noyaux $(\phi_{i;j})_{1 \ i;j \ d}$ dont le nombre évolue en $O(d^2)$, avec d 2 N la dimension du processus.

Une trop grande complexité peut entraver la capacité prédictive du modèle, par exemple parce que l'augmentation du nombre de paramètres vient augmenter l'erreur d'estimation de ces derniers. Une grande complexité peut également rendre di□cile l'interprétation du modèle.

Afin d'éviter les problèmes cités ci-dessus, nous tentons de réduire la complexité du processus en pénalisant la fonction de vraisemblance avec les paramètres d'interaction, et étudions la qualité d'ajustement et de prédiction du modèle en fonction de cette pénalisation. Ce travail a été réalisé avec di□érents noyaux.

2.5.1 Vraisemblance pénalisée

Une façon de réduire la complexité du processus consiste à réduire la puissance des interactions, c'est-à-dire les valeurs des paramètres d'excitations $(\alpha_{i;j})_{1 \ i;j \ d}$. Une première manière de le faire réside dans une pénalisation de la fonction de vraisemblance, par la norme L^2 du vecteur des paramètres concernés. Cette pénalisation correspond à une méthode de type Ridge, elle permet de réduire les plages de valeurs que peuvent prendre les paramètres pénalisés. Une seconde méthode consiste en une pénalisation de la vraisemblance par la norme L^1, elle se distingue de la méthode Ridge (norme L^2) car elle permet aux paramètres pénalisés de prendre exactement la valeur 0. Nous retenons cette méthode, avec pour objectif que le modèle soit forcé à faire ressortir les interactions principales sous cette nouvelle contrainte.

Cela revient à minimiser l'opposée de la log-vraisemblance comme suit :

$$\log L(\mu, \phi)_{penalise} = \log L(\mu, \phi) + \gamma \sum_{1 \ i;j \ d} |\alpha_{i;j}|$$

où γ 0 est le coe□cient de pénalisation et $L(\mu, \phi)$ est la vraisemblance du processus de Hawkes, avec $\mu = (\mu_{i;0}, \gamma_i)_{1 \ i \ d}$ et $\phi = (\alpha_{i;j}, \beta_{i;j})_{1 \ i;j \ d}$. L'idée est ensuite de tester

différentes valeurs de ce coefficient et d'observer la façon dont les paramètres réagissent.

2.5.2 Segmentation

La segmentation la plus fine que nous pouvons réaliser, à partir des trois variables explicatives Type d'attaque, Type d'organisation attaquée et Localisation (State) est la segmentation croisant toutes les modalités de ces variables. Le nom des groupes est de la forme : Type d'organisation & Type d'attaque & Etat. Afin de conserver des groupes suffisamment robustes au calibrage, nous avons conservé tels quels, tous les croisements possédant plus de 200 attaques. Les autres croisements ont été rassemblés dans un groupe nommé OTHER. Une exception a également été faite pour le croisement MED & OTHER & OTHER [2] qui a été mis dans ce dernier groupe, bien qu'il possède plus de 200 attaques, ce choix est motivé par une forte irrégularité de ce croisement sur la période d'intérêt.

Finalement la segmentation retenue contient six groupes et est résumée ci-dessous, dans la table 2.4.

Groupe	Nombre d'attaques
OTHER (1)	2046
MED & DISC & OTHER (2)	497
BUSINESSES & HACK & OTHER (3)	386
MED & HACK & OTHER (4)	472
MED & THEFT/LOSS & CALIFORNIA (5)	214
MED & THEFT/LOSS & OTHER (6)	943

Table 2.4 – Segmentation PRC - 2016

La figure 2.19 représente la fréquence des attaques pour chaque segment sur la période de calibration (2011-2016). A première vue, les tendances sont très différentes, ce qui nous conforte dans l'idée que la segmentation fait sens. En se basant sur le premier calibrage de la section 2.2.1, nous incluerons un *drift* dans nos modèles afin de tenter de capter ces tendances.

Il est également remarquable de constater que sur cette figure certains motifs très irréguliers apparaissent parfois pendant quelques mois ou années, c'est par exemple le cas pour le segment MED & HACK & OTHER qui comprend une forte excitation entre 1100 et 1500 jours avant de retomber sur un niveau bien plus faible. Il est donc nécessaire de se calibrer sur une grande période pour ne pas calibrer uniquement sur un motif particulier et avoir des prédictions très éloignées de la réalité.

2. Les groupes OTHERORGA et OtherStates évoqués en Section 2.1.3 seront simplement notés OTHER dans la suite des études.

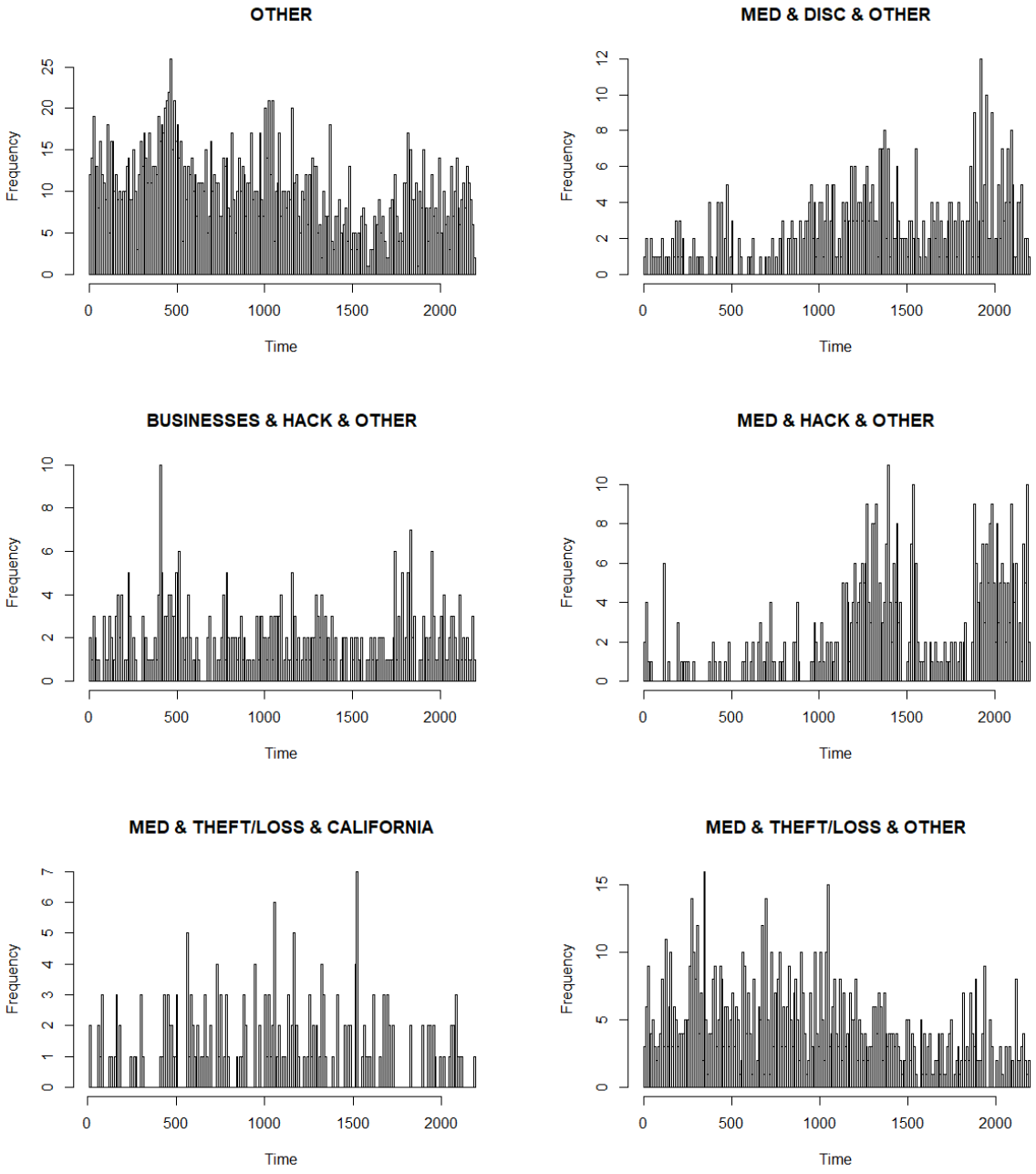


Figure 2.19 – Fréquence des attaques sur la période de calibrage (2011-2016)

2.5.3 Résultats

Le calibrage avec la fonction de vraisemblance pénalisée a été réalisé pour les paramètres de pénalisation suivants : $\gamma \in \{0, 100, 600, 900, 3000, 6000\}$, ainsi qu'avec trois noyaux différents, en considérant notre processus de Hawkes multivarié de dimension d, avec les mêmes notations que précédemment, pour $i, j \in \{1, .., d\}$ les noyaux testés sont les suivants :

- Noyau 1 : $\phi_{i,j}(a) = \alpha_{i,j} \exp(-\beta_i a)$. Il correspond au noyau exponentiel évoqué précédemment, avec une excitation instantanée $\alpha_{i;j}$, potentiellement différente pour tous les groupes. En revanche, l'influence de tous les groupes $j \in \{1, ..., d\}$ sur un groupe $i \in \{1, .., d\}$ décroît à la même vitesse β_i.
- Noyau 2 : $\phi_{i,j}(a) = \alpha_{i,j} \exp(-\beta_{i,j} a)$. Même cas que le noyau 1 mais l'influence de tous les groupes décroît à une vitesse $\beta_{i;j}$ de façon potentiellement différente.
- Noyau 3 : $\phi_{i,j}(a) = \alpha_{i,j} a \exp(-\beta_i a)$. Il correspond au noyau à retard évoqué précédemment, le délais avant l'excitation maximale de l'intensité d'un groupe i, causée par un évènement du groupe j est le même, $\frac{1}{i}$, quelque soit le groupe $j \in \{1, ..., d\}$.

L'intensité de fond, comme discuté précédemment, sera un *drift* linéaire : $\mu_i(t) = \mu_{0;i} + \gamma_i t$. Ce qui mène, au total à un nombre de 54 paramètres pour les noyaux 1 et 3, et 84 paramètres pour le noyau 2.

Les résultats étudiés qui suivent sont les analyses décrites en Section 2.3.6 "Méthodes de comparaisons". Nous rappelons que nous calibrons en maximisant la fonction de vraisemblance (où, ici, en minimisant l'opposée de la log-vraisemblance). Nous avons étudié les calibrages 2011-2015 ainsi que 2011-2016 et leurs prédictions respectives 2016 et 2017.

2.5.3.1 Calibrage

Les valeurs des vraisemblances en Table 2.5, bien qu'affectées par les pénalisations, restent correctes jusqu'à une pénalisation de 900.

	0	100	600	900	3000	6000
Noyau 1 (2011-2015)	6513.19	6375.83	6990.89	7385.11	13261.36	15799.48
Noyau 1 (2011-2016)	7639.44	7755.28	8421.69	8874.91	15143.42	17833.19
Noyau 2 (2011-2015)	6171.78	6278.31	6519.87	6673.23	8340.74	9563.34
Noyau 2 (2011-2016)	7516.43	7647.73	7959.91	8142.27	9835.47	11152.66
Noyau 3 (2011-2015)	6152.92	6528.24	6998.68	7407.18	10914.03	16016.69
Noyau 3 (2011-2016)	7484.55	7888.62	8253.16	8914.18	35829.76	78405.08

Table 2.5 – Valeurs des opposées des fonctions de log-vraisemblances en fonction de la pénalisation - la ligne supérieure correspond au coefficient γ de pénalisation.

Le noyau trois qui possède le même nombre de paramètres que le noyau 1 a une bien

meilleure vraisemblance (non pénalisée), cela nous indique que les données sont mieux représentées par cette excitation "latente" par opposition à une excitation instantanée. Plus en détail, les paramètres $(\beta_i)_{1 \ i \ 6}$ en Annexe E sont de l'ordre de 5-6, l'échelle de temps étant journalière, l'excitation maximale provoquée par un évènement est atteinte au bout de 4 ou 5 heures, dans ce modèle. La vraisemblance est également meilleure sous le modèle 3 (excitation latente, 54 paramètres) que le modèle 2 (excitation instantanée, 84 paramètres).

Les tests d'adéquation des trois modèles non pénalisés (sur la période 2011-2016), en Tables 2.6, 2.7 et 2.8 montrent qu'il est di□cile de valider les douze tests, ceux relatifs à l'adéquation à la loi exponentielle sont dans la grande majorité des cas validés, ce sont les tests d'indépendance qui sont plus sensibles.

	Ljung-Box (Lag=4)	Kolmogorov-Smirnov
OTHER (1)	0.0159	0.0503
MED & DISC & OTHER (2)	0.0000	0.5546
BUSINESSES & HACK & OTHER (3)	0.4677	0.5558
MED & HACK & OTHER (4)	0.0000	0.0024
MED & THEFT/LOSS & California (5)	0.0944	0.1146
MED & THEFT/LOSS & OTHER (6)	0.0029	0.0733

Table 2.6 – Tests d'adéquation modèle 1

	Ljung-Box (Lag=4)	Kolmogorov-Smirnov
OTHER (1)	0.2514	0.0865
MED & DISC & OTHER (2)	0.0000	0.1300
BUSINESSES & HACK & OTHER (3)	0.1051	0.5966
MED & HACK & OTHER (4)	0.0000	0.0361
MED & THEFT/LOSS & California (5)	0.3809	0.5669
MED & THEFT/LOSS & OTHER (6)	0.0250	0.6341

Table 2.7 – Tests d'adéquation modèle 2

	Ljung-Box (Lag=4)	Kolmogorov-Smirnov
OTHER (1)	0.7461	0.9060
MED & DISC & OTHER (2)	0.0327	0.5173
BUSINESSES & HACK & OTHER (3)	0.5815	0.3363
MED & HACK & OTHER (4)	0.0000	0.0370
MED & THEFT/LOSS & California (5)	0.0599	0.4246
MED & THEFT/LOSS & OTHER (6)	0.0794	0.5379

Table 2.8 – Tests d'adéquation modèle 3

Il est possible que des facteurs exogènes non pris en compte entraînent ces corrélations.

Finalement, le modèle 3 est de nouveau le plus performant avec la plupart de ses tests qui sont validés à 5%, au seuil de 3% seul un test est rejeté.

2.5.3.2 Prédictions

La table 2.9 met en évidence qu'une pénalisation semble pouvoir améliorer les capacités prédictives du modèle, dans une certaine mesure, c'est par exemple le cas pour les noyaux 1 et 2 pour l'année 2016. En revanche, il semble di□cile de sélectionner un modèle en se fiant à sa capacité prédictive observée, en e□et les meilleurs prédictions de 2017 ne sont pas réalisées par les meilleurs modèles de 2016.

	0	100	600	900	3000	6000
Noyau 1 (2016)	337.6614	280.7602	277.7764	283.5881	973.0103	1135.5217
Noyau 1 (2017)	170.3384	249.4687	240.4258	261.7280	732.0155	792.7558
Noyau 2 (2016)	259.4504	282.2328	202.7125	180.3729	256.7397	430.4255
Noyau 2 (2017)	127.3343	160.8886	159.4488	141.6603	148.1485	346.4559
Noyau 3 (2016)	201.7575	285.1470	262.0646	283.1685	502.2474	1559.1263
Noyau 3 (2017)	165.6958	183.2997	254.2543	172.6621	3168.8662	6402.4315

Table 2.9 – Somme des écarts absolus entre l'espérance du nombre d'attaques prédits (en 2016 et 2017) et le nombre réel, sur les six segments.

Un modèle qui semble être un bon compromis en terme de prédiction sur les deux années est, encore une fois, le noyau 3 sans pénalisation, les histogrammes de prédictions pour ce cas sont en Annexe D. Le modèle semble avoir des di□cultés à prédire correctement les six segments sur l'année 2016, les résultats sont meilleurs sur l'année 2017 sauf pour un segment. Ces di□cultés peuvent provenir de di□érents facteurs, tout d'abord la capacité de l'algorithme d'optimisation en grande dimension. Ensuite le fait d'inclure un *drift* n'est pas toujours une amélioration, si le modèle capte une tendance qui n'est que passagère, dans le *drift*, cela risque de fausser les prédictions, à cela s'ajoute le fait qu'un modèle interdépendant est très sensible aux erreurs, dans le sens où, si un segment n'est pas correct, cela influence nécessairement tous les autres segments. Pour finir comme pour tout modèle, il existe de nombreux facteurs exogènes dans la réalité, qui ne sont pas pris en considération.

2.5.4 Interprétation

En prenant en compte les résultats précédents, le modèle 3 semble le plus adapté pour analyser les paramètres du processus. Une interprétation possible est la suivante :

L'intensité de base μ_0 est la plus élevée pour les groupes 1 et 6 ce qui traduit simplement le fait qu'il sont plus représentés. Ce lien n'est pas toujours vérifié, par exemple, les groupes 2 et 4 semblent plus devoir leur nombre d'attaques aux phénomènes d'excitations que le groupe 3 car ils sont plus représentés mais ne présentent pas un plus grand taux de base ($\mu_{0;2} < \mu_{0;3}$ et $\mu_{0;4} < \mu_{0;3}$).

Concernant les *drifts*, le modèle semble avoir capté les tendances visibles en Figure 2.19, elles sont toutes croissantes ($\gamma > 0$) sauf pour les segments 2 et 4. Les segments 2 et 5 ont des tendances très peu marquées, ce qui correspond également aux histogrammes en figure 2.19.

La matrice des excitations en Table E.3 représente la valeur des excitations maximales. Pour 1 i, j d, le coe□cient $_{i;j}$ représente la valeur maximale de l'influence d'un évènement du groupe j, sur l'intensité du groupe i. Cette influence maximale est en e□et atteinte après un certain temps, comme précisé en 2.3.2.2, car nous considérons ici le noyau à retard. La table E.3 montre une forte auto-excitation des groupes 2 et 4, ce qui correspond à la remarque faite dans le paragraphe sur l'intensité de base, c'est également le cas pour le groupe 5 ($_{i;i} >> \mu_{0;i}$ pour $i = 2, 4$ et 5). Le groupe OTHER est le moins auto-excité ($_{1;1} < \mu_{0;1}$). Les di□érents types d'attaques pour le secteur médical semblent s'inter-exciter, les attaques de type HACK et DISC ont un clair impact sur l'intensité de l'autre, elles excitent également les attaques de type THEFT/LOSS. En revanche les attaques de type THEFT/LOSS ne semblent pas avoir un grand impact sur les deux autres.

Concernant les coe□cients $(\beta_i)_{1 \ i \ 6)}$ ils sont tous du même ordre de grandeur hormis pour le groupe BUSINESSES & HACK & OTHER qui est plus élevé, cela signifie que le phénomène d'excitation est moins fort, et moins long pour ce groupe.

Ces résultats sont une interprétation possible des paramètres, mais ces phénomènes d'excitation, qui sont des phénomènes de causalité dans le modèle, ne reflètent pas nécessairement une causalité dans la réalité, mais plutôt de corrélation, autrement dit, les paramètres ne permettent pas d'a□rmer qu'un certain type d'attaque influe sur un autre dans la réalité.

2.5.5 Conclusion

Finalement, cette segmentation présente plusieurs limites pour une application actuarielle, ces limites découlent principalement de sa complexité : les temps de calculs sont longs, la capacité prédictive reste limitée, et les tests statistiques sont d'autant plus di□ciles à justifier dans leur totalité qu'ils sont nombreux.

En prenant en compte ces remarques, nous nous tournerons vers une segmentation plus agrégée dans les sections qui suivent.

2.6 Tarification d'une garantie violation de données

L'objectif de cette section est d'expliciter une méthode qui permet de déterminer une prime pure pour une garantie violations de données, à l'aide de l'approche classique : prime = fréquence coût. Elle se déroule en quatre parties, la première concerne le choix d'une segmentation sur le modèle de fréquence, la seconde concerne la modélisation de la fréquence, par le modèle de Hawkes, mais également par des modèles plus simplistes, la troisième partie concerne la modélisation du coût d'une violation de données, enfin la quatrième et dernière partie se porte sur la détermination et la comparaison des primes entre les différents modèles utilisés.

2.6.1 Choix d'une segmentation

Afin de déterminer des primes adaptées au mieux à l'entreprise assurée nous souhaitons segmenter la base de données. En effet la Figure 2.19 laisse penser que les risques ne sont pas les mêmes selon le type d'entreprise assuré ou le type d'attaque considéré. Par ailleurs, l'étude précédente montre qu'une segmentation trop fine n'est pas la plus viable à la fois en prédictions mais également statistiquement.

Pour cette raison différentes segmentations, moins fines, explicitées en Annexe F, ont été considérées. Elles ont été choisies sur des critères de bon sens (par exemple un segment par type d'attaque), cela concerne les segmentations 1 et 2, mais également sur des critères de similitudes statistiques. En particulier nous avons étudié les trois premiers moments des distributions des inter-temps de survenance, sur les croisements Type d'organisation et Type d'attaque, cette étude est résumée en table F.1, et a donné lieu aux segmentations 3 (obtenue via un K-means sur ces critères) et 4 (sur décision, sans K-means).

Les segmentations ont été comparées avec leurs test de qualité d'ajustement avec le modèle de Hawkes, et ce avec les trois noyaux utilisés précédemment. Il ressort de ces tests que la segmentation sur laquelle les modèles s'ajustent le mieux est la segmentation 1. En particulier pour le noyau 2 tous les tests sont acceptés (les calibrages ont été effectués en considérant des taux de base avec *drift*, comme dans l'étude précédente), ce qui en fait un modèle justifiable statistiquement.

2.6.2 Modèle de fréquence

2.6.2.1 Modèle de Hawkes

Les histogrammes de fréquence sur notre segmentation, n'affichent pas de tendance particulière sur les segments MED et BUSINESSES. Pour cette raison le modèle a été re-calibré avec un taux de base constant pour ces segments, le *drift* est conservé pour le dernier segment car celui-ci affiche une claire tendance décroissante. Le but de cette opération est d'optimiser nos prédictions, car en captant une fausse tendance, le modèle peut s'écarter de la réalité. Avec ces considérations, en comparant encore une fois les trois noyaux, le modèle qui possède les meilleurs tests statistiques est celui avec le noyau 1 : $\phi_{i;j}(a) = \alpha_{i;j} \exp(-\beta_i a)$ (les deux autres ont au moins un test de rejeté). La Table

2.10 montre que tous les tests sont acceptés à 5%, hormis le test d'indépendance pour BUSINESSES, qui est accepté à 4%.

	Ljung-Box (Lag=4)	Kolmogorov-Smirnov
BUSINESSES	0.0418	0.6853
MED	0.2595	0.0924
OTHERORGA	0.3038	0.3372

Table 2.10 – Tests d'adéquation du noyau 1

Nous utiliserons ce modèle pour modéliser la fréquence des cyber-attaques.

2.6.2.2 Distributions discrètes

L'article de [Edwards *et al.*, 2016] cité dans la Section 2.2.2 met en évidence la bonne adéquation de la loi binomiale négative sur la fréquence journalière d'attaques, l'étude à été réalisée sur la PRC sur la période 2005-2015 pour les violations dont le nombre de données violées est connu. En se basant cette étude, nous avons calibré différentes lois discrètes sur le nombre journalier d'attaques (Poisson, Géométrique, Binomiale négative), pour les secteurs BUSINESSES ainsi que MED c'est en effet la loi binomiale négative qui se calibre le mieux. En particulier, nous retenons un calibrage avec les données de la période 2011-2015 qui fournit de bonnes p-values avec le test de Kolmogorov-Smirnov (0.0998 pour MED et 0.9766 pour BUSINESSES. En ajoutant l'année 2016 le test est rejeté pour le secteur MED bien que la comparaison graphique soit très correcte). Les comparaisons graphiques des lois empiriques et théoriques sont en Annexe G.

Afin de tenir compte d'une tendance pour la fréquence du nombre d'attaques de OTHERORGA, comme cela a été fait dans le modèle de Hawkes, un modèle linéaire généralisé a été calibré, avec comme variable explicative le temps. Un GLM Poisson et un GLM binomial négatif ont été considérés. Pour les distinguer, ils ont été calibrés jusqu'à 2015 puis comparés en terme de MSE sur 2016, les deux modèles donnent presque le même MSE (Mean square Error : 59.73 pour le négatif binomial et 59.68 pour le Poisson). C'est le modèle binomial négatif qui a été retenu, d'une part afin de profiter de sa plus grande variance lors des prédictions et d'autre part car c'est le modèle qui a été retenu pour les deux autres secteurs.

Les histogrammes de prédictions de ces 2 modèles (Hawkes versus Distributions discrètes) sont en Annexe H. Les deux modèles contiennent le réel entre leurs quantiles à 99.5%, sauf le modèle GLM pour OTHERORGA, qui sous estime le nombre réel. Sur cet exemple le modèle de Hawkes semble plus intéressant car sa distribution est plus étendue. En particulier le modèle de Hawkes sur cet exemple serait plus adapté dans le cadre de la détermination d'un quantile pour un modèle interne.

2.6.2.3 Probabilité de subir une attaque

La probabilité de subir une attaque sera approchée par le rapport entre le nombre d'attaques prédit dans un secteur et le nombre d'entreprises de ce secteur aux États-Unis, cette approche se base sur l'hypothèse que toutes les violations de données aux États-Unis sont présentes dans la PRC. Cette hypothèse peut sembler forte, mais tenant compte de l'obligation de notification des violations aux États-Unis (au-delà de 500 données violées en général), et tenant compte du fait que la base est régulièrement mise à jour, elle ne semble pas dénuée de sens. Une seconde hypothèse est utilisée avec cette approche, qui est celle de considérer que toutes les entreprises ont la même probabilité d'être attaquées dans un secteur, cela n'est pas exacte, par exemple les rapports laissent entendre que les petites et moyennes entreprises sont des cibles faciles, car ont peu de moyens en cyber-sécurité. Il serait éventuellement possible de prendre en considération de tels facteurs, comme la taille de l'entreprise ou son chi□re d'a□aire, dans le modèle.

Le bureau du recensement des États-Unis [3] propose di□érents rapports concernant le nombre d'entreprises sur le territoire. Le nombre total d'entreprises est en 2017 de 5 954 684, cependant nous considérons que le risque se porte peu sur les entreprises de très petites tailles, nous ne considérerons ainsi que les entreprises de taille supérieure à 20 personnes, cela concerne 10.9 % de la base (les très petites entreprises sont très nombreuses mais une grande partie n'emploie personne, en réalité ce ne sont pas des Businesses [4]).

Le bureau du recensement fournit un détail du nombre d'entreprises par secteur pour l'année 2016, c'est ce rapport qui sera utilisé à défaut d'en avoir un autre, il permet de déterminer le nombre d'entreprises des secteurs MED, BUSINESSES, ainsi que EDU (éducation) qui fait partie du segment OTHERORGA. Concernant les organisations gouvernementales (GOV dans le segment OTHER) un rapport de 2017, qui recense ces organisations sur toutes les échelles (comtés, villes, États, districts, etc.) est disponible. En considérant que le taux de petites entreprises est le même dans tous les secteurs nous obtenons les résultats suivants :

	BUSINESSES	MED	OTHERORGA
Nb entités concernées	747 047	97 651	101 502

Table 2.11 – Nombre d'entreprises exposées par secteur

Nous n'avons pas considéré les ONG dans OTHERORGA qui normalement y sont présentes, ce choix est motivé par le fait que très peu d'ONG concernent la base (environ 1.1%) mais elles sont présentes en très grand nombre sur le territoire des États-Unis (1.5 millions estimés) à défaut de posséder une information sur leur taille pour ne considérer que les plus importantes, nous préférons les écarter du décompte, sans quoi la probabilité

3. https://www.census.gov
4. https://www.theguardian.com/business/2018/sep/23/how-many-small-businesses-us-census-bureau-wrong

de subir une attaque serait drastiquement réduite.

2.6.3 Modèle de coût

Le Ponemon Institute mène des recherches sur des sujets de protection des données, de confidentialité et de technologies de sécurité des données. Il a pour objectif une meilleure compréhension par les entreprises de ces sujets et donc une meilleure façon de gérer ces problématiques. Il publie notamment, chaque année, un rapport sur le coût des violations de données, basé sur le témoignage d'entreprises (plusieurs centaines pour le rapport de 2019). Ce rapport explicite les di□érentes tendances dans les coûts des violations de données, par exemple les coûts moyens par pays, par type d'organisation mais également les facteurs influant sur les coûts, comme le temps mis pour détecter la violation, ou la taille de l'entreprise.

La PRC possède comme variable, le nombre de données violées lors d'une violation, cette information n'est pas disponible pour toutes les attaques mais cela en concerne tout de même 3393 sur la période 2011-2016. Pour évaluer le coût d'une violation de données, il est alors possible de prendre en compte cette information de deux façons grâce au rapport du Ponemon Institute de 2019, la première est d'utiliser le coût moyen d'une donnée violée par type d'organisation et la seconde est de créer une loi du coût marginal d'une donnée violée en fonction du nombre total de données violées. Nous avons sélectionné la seconde méthode car la première se restreint aux violations inférieures ou égales à 100 000 données, ce qui, nous le verrons par la suite, est très restrictif. De la même façon, à la vue du rapport, le nombre de données violées a un fort impact sur le coût marginal d'une donnée violée, considérer une simple moyenne ne permet pas de prendre en compte cet e□et.

2.6.3.1 Coût marginal d'une donnée violée

En Tables 2.12 et 2.13, les moyennes disponibles, extraites du rapport Cost Of Data Breach 2019 pour calibrer une loi du coût marginal d'une donnée violée en fonction du nombre total de données violées. La première concerne les violations de taille moyenne, la seconde celles qui sont dénommées "Mega breaches", avec un très grand nombre de données violées.

	1	2	3	4
Nb données violées	5000	17500	37500	75000
Coût total (en millions)	2.2	3.3	4.7	6.4
Coût d'une donnée violée	440.00	188.57	125.33	85.33

Table 2.12 – Coûts moyens des violations de données de tailles moyenne

Il apparaît une claire tendance décroissante du coût marginal d'une donnée violée, cela peut-être dû à la présence de coûts fixes pour traiter une violation de donnée, qui

	1	2	3	4	5	6
Nb données violées	10^6	10^7	20^7	30^7	40^7	50^7
Coût total (en millions)	42.0	163.0	225.0	309.0	345.0	388.0
Coût d'une donnée violée	42.00	16.30	11.25	10.30	8.63	7.76

Table 2.13 – Coût moyens des "Mégas" violations de données

sont donc plus amortis avec plus de données violées.

Pour prendre en compte cette tendance, Jay Jacobs (2014) propose un modèle du type :

log(Coût total) = a + b log(Nb données violées) avec a, b des constantes, cependant son étude ne concerne que des violations de taille inférieure à 100 000 données.

[Farkas *et al.*, 2019] propose un modèle du type :

log(Coût total) = $a + b$ log(log(Nb données violées)) pour tenter de mieux prendre en compte la décroissance dans les "Mégas" violations.

En calibrant les deux modèles par les moindres carrés, le modèle de Jacobs apparaît être celui qui capte au mieux la tendance des données. En e□et, la somme de ses erreurs au carré vaut 0.19 contre 0.72 pour l'autre modèle. Huit points sur dix sont mieux approchés par ce modèle. Nous avons donc choisi le modèle log-log, qui a pour coe□cients : a = 9.242 et b = 0.595. Ci-dessous, la représentation du coût total d'une attaque en fonction du nombre de données violées, avec en bleu le modèle log-log(log) et en rouge le modèle sélectionné, qui donne des coûts extrêmes plus élevés.

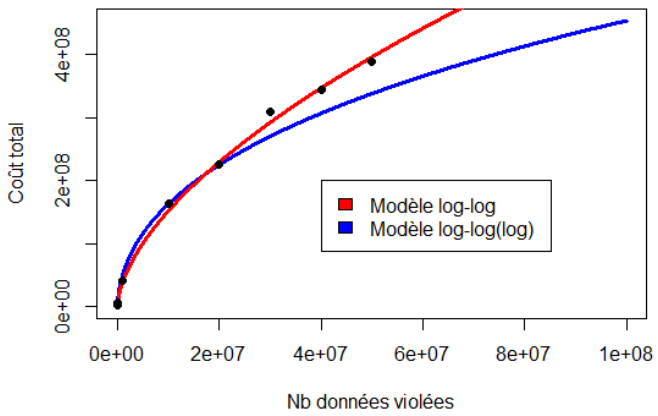


Figure 2.20 – Évolution du coût total d'une violation de données en fonction du nombre de données violées - les points correspondent aux données du Ponemon Institute

2.6.3.2 Les coûts pris en compte

Un avantage des données du rapport Cost Of Data Breach (2019) est que les coûts estimés sont basés sur les di□érents coûts engendrés par une violation de données, parmi lesquels :

- Détection et gestion : cela concerne par exemple les coûts relatifs à l'investigation, la communication, l'audit ou encore la gestion de crise ;
- Notification : les coûts nécessaires pour la notification/communication aux particuliers concernés ainsi qu'au régulateur (par exemple nécessité d'engager un prestataire, etc.) ;
- Coûts post-violation : cela concerne par exemple les amendes potentielles ou les coûts légaux, si la responsabilité est mise en jeu ;
- Coût de la perte d'exploitation : ces coûts sont ceux relatifs à l'arrêt potentiel d'activité subit pendant un certain temps ou à la perte de réputation ainsi que la perte de clientèle.

Les coûts utilisés dans notre étude sont donc relativement complets, ce qui permet de proposer une assurance elle-même complète.

2.6.3.3 Nombre de données violées

Sur la période 2011-2016 nous disposons de 430, 2575 et 388 nombre de données violées, respectivement, pour les secteurs BUSINESSES, MED et OTHERORGA. Étant donné la très grande échelle des valeurs (de une donnée violée à 3 milliards, qui correspond à l'attaque sur Yahoo en 2013), il n'est pas possible de calibrer une seule distribution sur les données. Une première solution est d'utiliser la théorie des valeurs extrêmes mais le nombre de données dans deux groupes (BUSINESSES et OTHERORGA) n'est pas su□sant. En revanche, en passant au logarithme sur le nombre de données violées il est possible de reconnaître des distributions.

Un fait remarquable est l'aspect des distributions avant 500 données violées, en e□et, la distribution semble être coupée en deux, au niveau de 500 données violées ($\log(500) = 6.2$), comme c'est le cas pour le secteur MED en Figure 2.21.Ce phénomène est probablement causé par le fait qu'une grande partie des réglementations de notifications aux États-Unis obligent à notifier à l'autorité une violation de plus de 500 données. Cette séparation, plus nette pour les secteurs MED et OTHERORGA, est acceptée par le test de Kolmogorov-Smirnov comme suivant une loi uniforme pour ces deux secteurs. Pour le secteur BUSINESSES la séparation n'est pas nécessaire pour calibrer une loi.

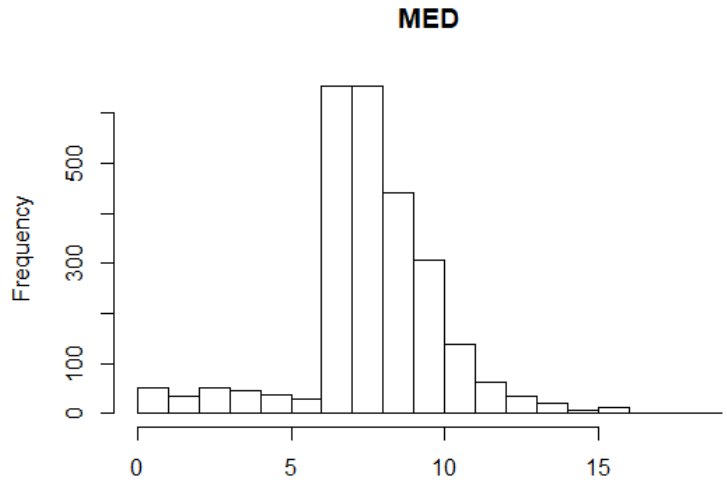


Figure 2.21 – Distribution du log(Nb données violées) par attaques - secteur MED

Toujours en étudiant le logarithme, di□érentes distributions ont été testées sur la seconde partie des données pour MED et OTHERORGA, ainsi que sur la totalité des données pour BUSINESSES, parmi lesquelles les lois de Weibull, Cauchy, Normale, Gamma et Logistique. Les lois retenues, sur un critère graphique et statistique (test de Kolmogorov-Smirnov) sont la loi Gamma (BUSINESSES, p-value de 0.246), la loi logistique (MED, p-value de 0.087) et la loi gamma (OTHERORGA, p-value de 0.978).

Les graphiques d'adéquation sont en Annexe I, globalement les adéquations sont correctes hormis quelques écarts au niveau des quantiles extrêmes.

2.6.4 Détermination de la prime pure

2.6.4.1 Garantie

Pour cet exemple nous nous plaçons dans le cas d'une garantie violations de données pour les entreprises situées aux États-Unis, tous types de causes confondus. La garantie portera sur tous les coûts relatifs à la violation, comme précisé précédemment.

Nous allons estimer un tarif pour une garantie "moyenne" ainsi qu'un tarif pour une garantie avec un plafond élevé.

Nous choisissons d'inclure une franchise à hauteur de 500 données volées ce qui équivaut, avec notre modèle, à une franchise de 417 660 418 000 $. Cette franchise a un double objectif, le premier est de profiter des avantages classiques des franchises, comme par exemple lutter contre l'aléa moral et le second est de n'utiliser que les parties des distributions de nombre de données violées les plus fiables (comme il n'y a pas toujours d'obligation de notification avant 500 données cette partie est plus obscure).

Nous choisissons également d'inclure, une limite de garantie qui correspond au quantile 80% de la distribution empirique du nombre de données volées pour le premier tarif, et au quantile 95% pour le second tarif. Ne pas mettre de limite de garantie pourrait mener à une prime considérablement élevée car le fait de modéliser à l'échelle logarithmique notre nombre de données volées peut mener à des nombre simulés très élevés. En effet une loi continue comme la loi gamma calibrée sur le secteur BUSINESSES peut générer par simulation, bien qu'avec faible probabilité, des nombres à hauteur de 30, qui, passés à l'exponentielle sont gigantesques, et bien plus élevés que le nombre maximum observé avec nos données (3 milliards), cela pourrait fausser la moyenne.

Pour finir, nous profitons de disposer d'un modèle stochastique pour calculer une prime de réassurance non proportionnelle, pour cela nous considérons un contrat de réassurance qui récupère le risque au-delà d'une certaine valeur pour chaque segment, dans le cas de la garantie "élevée".

Tous ces éléments, exprimés en millions de dollars, sont résumés dans la Table 2.14.

	Plafond tarif 1	Plafond tarif 2	Seuil réassurance tarif 2
MED	2.5	7.5	5
OTHERORGA	4.6	30	20
BUSINESSES	13	300	100

Table 2.14 – Plafonds des tarifs et seuils de réassurance, par type d'organisation - en million de dollars

2.6.4.2 Résultats

Les coûts moyens ont été estimés sur la base de 10 millions de simulations, et sont exprimés avec leur erreur à 95%. Les nombres d'attaques prédits correspondent à l'espérance du processus de Hawkes conditionnée par le passé du processus, (Nb attaques prédit 1) ainsi que le nombre d'attaques moyen prédit par les distributions discrètes (Nb attaques prédit 2), ce dernier est calculé sur la base de 100 000 simulations et est fourni avec l'erreur à 95%. Les résultats sont en Tables 2.15 et 2.16.

	BUSINESSES	MED	OTHERORGA
Coût moyen	3 897 589 3103	1 189 381 521	1 793 923 1114
Nb attaques prédit 1	186.96	462.23	42.96
Nb attaques prédit 2	200.93 0.1	446.90 0.19	25.66 0.03
Nb entités concernées	747 047	97 651	101 502
Fréquence 1	$2.50*10^{-4}$	$4.73*10^{-3}$	$4.23*10^{-4}$
Fréquence 2	$2.69*10^{-4}$	$4.58*10^{-3}$	$2.53*10^{-4}$
Prime pure 1	975.43	5 629.92	759.27
Prime pure 2	1048.32	5443.21	453.51

Table 2.15 – Primes pures avec le tarif 1

	BUSINESSES	MED	OTHERORGA
Coût moyen	22 082 497 39371	1 645 128 1151	3 944 739 4413
Coût moyen réassureur	16 206 894 39342	551 297 1169	1 702 749 4183
Nb attaques prédit 1	186.96	462.23	42.96
Nb attaques prédit 2	200.93 0.1	446.90 0.19	25.66 0.03
Nb entités concernées	747 047	97 651	101 502
Fréquence 1	$2.50*10^{4}$	$4.73*10^{3}$	$4.23*10^{4}$
Fréquence 2	$2.69*10^{4}$	$4.58*10^{3}$	$2.53*10^{4}$
Prime pure 1	5 526.49	7 787.20	1 669.58
Prime pure 2	5 939.43	7 528.93	997.2415
Prime pure réassurance 1	4 056.025	2 609.56	720.68
Prime pure réassurance 2	4 359.10	2 523.01	430.46

Table 2.16 – Primes pures avec le tarif 2

D'après securityMetrics[5] une prime d'assurance violation de données peut varier de 650$ à 120 000 $. Le site databreachinsurancequote[6] donne des exemples de primes d'assurance selon le type d'entreprise, quelques exemple sont cités en Annexe J en les re-classant selon notre segmentation (nous n'avons pas d'exemples pour le secteur OTHERORGA qui concerne l'éducation et le gouvernement).

Nos primes sont de façon générale, plus faibles que celles citées en exemple, cela s'explique d'une part par le fait que nous avons des primes pure, qui par définition ne contiennent pas de chargements. Ensuite, les primes en Annexe J peuvent fortement varier selon le chi□re d'a□aire de l'entreprise, c'est un facteur que nous n'avons pas pris en compte. Pour finir, notre exposition est discutable, l'information sur le nombre d'entreprises et le choix de celles que nous considérons sont sensibles, par exemple [Pons, 2014], obtient des probabilités plus élevées avec une méthode semblable, sur l'année 2011.

2.6.5 Limites

Sur l'année 2017 le modèle réussi à prédire des distributions qui contiennent le réel dans des quantiles acceptables (c'est-à-dire que selon le modèle, le nombre réel n'est pas improbable). Cependant, il arrive que cela ne soit pas toujours le cas sur des années à fortes, ou faibles sinistralité. Par exemple, en recalibrant les modèles jusqu'à 2015 pour prédire l'année 2016, les résultats, basés sur 10 000 (Hawkes) et 100 000 (modèle 2) simulations sont en Table 2.17 (cette fois c'est le noyau 3 qui se calibre le mieux).

Une première observation est que les prédictions par les lois binomiales négatives sont très proches de celles avec les Hawkes. Ensuite, les segments BUSINESSES et OTHERORGA ont des résultats aussi acceptables que dans l'application précédente.

5. https://www.securitymetrics.com/blog/cyber-breach-insurance-how-much-does-it-cost
6. https://databreachinsurancequote.com/cyber-insurance/cyber-insurance-data-breach-insurance-premiums

	BUSINESSES	MED	OTHERORGA
Minimum méthode 1	130	329	20
Minimum méthode 2	132	332	12
Moyenne méthode 1	189	437	46
Moyenne méthode 2	201	447	36
Réel	192	569	
Quantile 99.5 méthode 1	232	524	68
Quantile 99.5 méthode 2	244	529	53
Maximum méthode 1	258	572	80
Maximum méthode 2	280	596	67

Table 2.17 – Prédictions année 2017

En revanche, pour le segment MED, bien que le réel se situe dans les distributions prédites, il est au-delà du quantile 99.5% ce qui suggère que sous ces modèles, le nombre réel avait moins de 0.5% de chances de se produire. De façon générale il est di□cile d'avoir le réel toujours bien placé dans les distributions, car le nombre d'attaques d'une année sur l'autre peut énormément varier. Pour avoir des prédictions plus sures, il faudrait utiliser une distribution (encore plus) étendue.

Chapitre 3

Développement d'une méthode de provisionnement individuel avec les processus de Hawkes

3.1 Introduction

Le provisionnement individuel a été introduit formellement, parmi les premières fois par [Arjas, 1989], [Jewell, 1989], [Norberg, 1993] et [Hesselager, 1994]. Bien qu'introduit au même moment que les travaux de [Mack, 1993] sur les méthodes de provisionnement stochastiques basées sur les triangles de liquidation, il est aujourd'hui bien moins populaire. Cela est en majeure partie dû à la simplicité d'utilisation et de compréhension des modèles agrégés basés sur les triangles.

Cependant, la modélisation individuelle pour le provisionnement a, au travers des publications, su montrer ses avantages, qui sont pour la plupart de combler les inconvénients des méthodes agrégées. Elle permet en premier lieu d'e□ectuer une séparation naturelle et sans ambiguïté des sinistres IBNR (Incured But Not Reported) et RBNS (Reported But Not Settled). En second lieu, elle permet d'éviter la perte d'information due à l'agrégation des données dans un triangle, et en ce sens de profiter d'une information plus fine. Au-delà, son intérêt par rapport aux méthodes agrégées est d'être plus flexible, à savoir pouvoir prendre en compte des tendances complexes dans le développement des sinistres ainsi que des paiements. Une fois calibré, le modèle donne de l'information sur l'évolution des facteurs de risque et peut donc devenir un outil de gestion et d'analyse du risque. Finalement un avantage majeur, qui découle de cette flexibilité, est de pouvoir, encore une fois, palier à un inconvénient des méthodes agrégées à savoir qu'il est parfois di□cile pour ces dernières de justifier proprement les hypothèses sous-jacentes au modèle utilisé.

Une grande partie des articles sur ce sujet a poursuivi les premières études sur les modèles individuels en reprenant leur cadre d'introduction, qui est, une modélisation de la sinistralité suivant un processus de Poisson inhomogène (marqué). Cependant, ce type de processus ne permet pas de modéliser des e□ets de dépendance temporelle. C'est pourquoi certains se sont penchés vers d'autres types de modèles utilisant des processus

plus complexes. Nous pouvons citer [Badescu *et al.*, 2016] qui utilisent un processus de Cox, [Wüthrich, 2018] quant à lui, s'est tourné vers des méthodes de machine learning.

Dans ce mémoire nous nous intéressons, toujours dans le cadre du provisionnement individuel, à l'utilisation de processus de Hawkes. Rappelons que ces processus, introduits la première fois par [HAWKES, 1971], ont la particularité de modéliser des phénomènes d'auto-excitation et induisent donc des dépendances temporelles complexes. Ils sont une généralisation du processus de Poisson et en ce sens, un candidat idéal pour s'émanciper de ce cadre plus classique.

Après avoir introduit le cadre formel du provisionnement individuel avec des processus de Hawkes, ce travail se penche tout particulièrement sur une méthode d'estimation de la fonction de vraisemblance, étant donné que cette dernière s'avère, sous ce modèle, incalculable car dépendante des IBNR (non observés). Une fois la méthode et ses limites testées, une application dans le cadre du cyber-risque est e□ectuée.

3.2 Le modèle individuel

Nous reprenons le cadre d'étude définit par [Boumezoued et Devineau, 2017], en l'adaptant aux processus de Hawkes. Ce cadre est le suivant :

Nous considérons que les sinistres surviennent à des temps $(T_n)_{n\ 1}$ suivant un processus de Hawkes et modélisons de façon jointe ces temps de survenance ainsi que leurs délais de reporting $(U_n)_{n\ 1}$ qui sont supposés suivre une loi $p_{uj T_n}$. Nous nous plaçons sur un horizon de temps d'observation $[0, \tau]$.

Comme un assureur, en τ, ne peut observer que les temps d'occurrence tels que $T_n + U_n \quad \tau$, cela signifie qu'une partie des sinistres ne sont pas encore connus : ce sont les fameux IBNR qu'il est alors nécessaire de provisionner en fin d'année.

Commençons par e□ectuer la distinction entre les temps d'occurence survenus et observés $(T_n^R)_{n\ 1}$ et les survenus mais non observés $(T_n^{IBNR})_{n\ 1}$ (*Reported* vs *Incurred But Not Reported*). Cette distinction se fait très naturellement avec cette modélisation, par les ensembles :

$$I^R(\tau) = \{(T_n, U_n) \text{ tels que } T_n + U_n \quad \tau\}$$
$$I^{IBNR}(\tau) = \{(T_n, U_n) \text{ tels que } T_n + U_n > \tau\}$$

Nous pouvons maintenant nous intéresser aux processus respectifs représentant ces temps d'occurrences. L'intérêt de connaître le processus des temps observés (en particulier son intensité), est de pouvoir écrire une vraisemblance par rapport à ce seul processus de temps observés. Cela permet d'éviter le biais qui aurait été inclus dans une vraisemblance simple (par vraisemblance simple il est entendu une vraisemblance classique, ne prenant pas en compte le phénomène : observé versus IBNR). En e□et, par construction, les temps

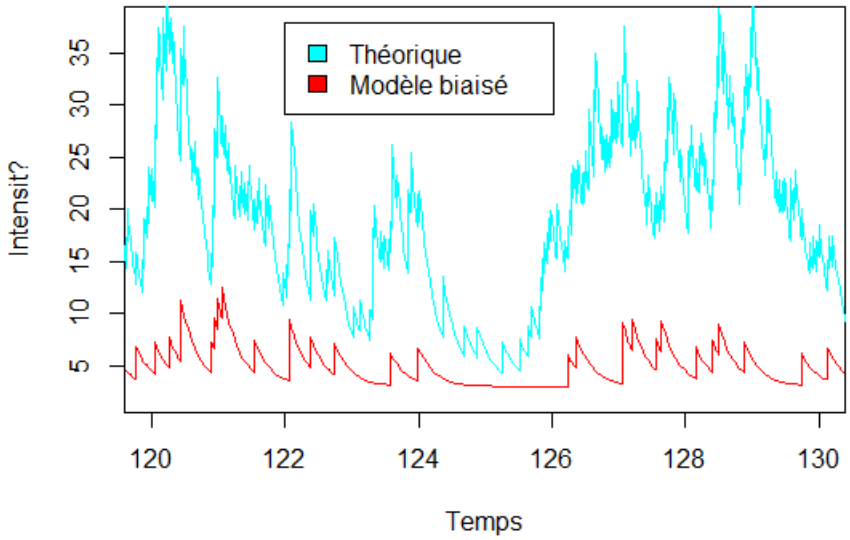


Figure 3.1 – Intensité d'un processus de Hawkes complet en cyan - intensité biaisée (qui ne saute qu'aux temps observés

observés sont ceux qui ont en général de faibles délais de reporting. Ne pas prendre en compte cette information mènerait à une estimation de la loi de délais moins lourde qu'en réalité, ainsi qu'à une fréquence sous-estimée. Graphiquement, une vraisemblance simple sur le processus de Hawkes correspondrait à considérer l'intensité rouge sur la Figure 3.1 alors que l'intensité réelle est celle en Cyan. Les sauts de l'intensité réelle qui ne sont pas e□ectués par l'intensité biaisée (rouge) correspondent aux survenances d'IBNR.

Afin de déterminer l'intensité du processus des temps observés, nous allons utiliser les mesures aléatoires de Poisson et en particulier une propriété de martingalité qui leur permet de représenter des processus ponctuels.

3.2.1 La mesure ponctuelle de Poisson

Définition : Une mesure ponctuelle de Poisson, notée $M(\mathrm{d}s, \mathrm{d}\theta)$, définie sur $\mathrm{R}^+ \quad E$, de mesure intensité $m(\mathrm{d}s, \mathrm{d}\theta) = \mathrm{d}s\mu_s(\mathrm{d}\theta)$, avec μ une mesure sigma-finie, est une mesure aléatoire à valeur dans N *[f+ 1 g* qui vérifie les propriétés suivantes :

- Pour tous ensembles mesurables et disjoints $B_1, ..., B_n$ de $\mathrm{R}^+ \quad E$ les variables aléatoires $M(B_1), ..., M(B_n)$ sont indépendantes
- Pour tout ensemble mesurable B de $\mathrm{R}^+ \quad E$, la variable aléatoire $M(B)$ suit une

distribution de Poisson de paramètre : $\lambda = m(B)$

— $M(0 \quad E) = 0$

Sous cette définition la mesure ponctuelle de Poisson définit une mesure de comptage sur $\mathbb{R}^+$ dans le sens où, pour tout $t > 0$ nous avons $M(ftg \quad E)$ *2* $f0, 1g$.

Par la suite nous utiliserons régulièrement la propriété de martingalité suivante :

Propriété : Soit M une mesure ponctuelle de Poisson, en notant (G_t) la filtration canonique engendrée par M, $P(G_t)$ la tribu prévisible associée, et E la tribu sur E. Si la fonction $f(s, y)$ est $P(G_t) \quad E$ mesurable et telle que, $8t \quad 0$:

$$\int_0^t \int_E jf(s, y)jm(\mathrm{d}s, \mathrm{d}y) < 1$$

alors nous avons le résultat suivant :

$$\int_0^t \int_E f(s, y)M(\mathrm{d}s, \mathrm{d}y) \quad \int_0^t \int_E f(s, y)m(\mathrm{d}s, \mathrm{d}y)$$

est une martingale locale.

3.2.2 Détermination des processus d'intensité séparés

Nous pouvons maintenant utiliser cette propriété de la mesure ponctuelle de Poisson pour utiliser la représentation dite de *Thinning* de notre processus $(T_n, U_n)_{n \ 1}$ d'intensité $\lambda(t)\mathrm{d}tp_{Ujt}(\mathrm{d}u)$ avec $\lambda(t)$ le processus d'intensité du processus de Hawkes. Le principe est le suivant :

Soit $M(\mathrm{d}t, \mathrm{d}u, \mathrm{d}\theta)$ une mesure ponctuelle de Poisson sur $(\mathbb{R}^+)^3$ de mesure intensité $m(\mathrm{d}t, \mathrm{d}u, \mathrm{d}\theta) = \mathrm{d}t\mathrm{d}u\mathrm{d}\theta$, en prenant la mesure :

$$N(\mathrm{d}t, \mathrm{d}u) = \int_0^1 1 \quad {}_{(t)p_{Ujt}(u)} M(\mathrm{d}t, \mathrm{d}u, \mathrm{d}\theta)$$

nous avons bien une mesure d'intensité $n(\mathrm{d}t, \mathrm{d}u) = \lambda(t)\mathrm{d}tp_{Ujt}(\mathrm{d}u)$, pour s'en convaincre nous pouvons utiliser la propriété de martingalité de la mesure de Poisson M sachant que l'intensité $\lambda(t)$ est mesurable par rapport à la tribu prévisible $P(G_t)$:

$$\begin{aligned}
&\int_0^t \int_{\mathbb{R}^+} f(s, u)N(\mathrm{d}s, \mathrm{d}u) \quad \int_0^t \int_{\mathbb{R}^+} f(s, u)n(\mathrm{d}s, \mathrm{d}u) \\
&= \int_0^t \int_{\mathbb{R}^+} \int_{\mathbb{R}^+} f(s, u)1 \quad {}_{(s)p_{Ujs}(u)} M(\mathrm{d}s, \mathrm{d}u, \mathrm{d}\theta) \quad \int_0^t \int_{\mathbb{R}^+} f(s, u)\lambda(s)p_{Ujs}(u)\mathrm{d}s\mathrm{d}u \\
&= \int_0^t \int_{\mathbb{R}^+} \int_{\mathbb{R}^+} f(s, u)1 \quad {}_{(s)p_{Ujs}(u)} M(\mathrm{d}s, \mathrm{d}u, \mathrm{d}\theta) \quad \int_0^t \int_{\mathbb{R}^+} \int_{\mathbb{R}^+} f(s, u)1 \quad {}_{(s)p_{Ujs}(u)} m(\mathrm{d}s, \mathrm{d}u, \mathrm{d}\theta)
\end{aligned}$$

Cette dernière ligne donne immédiatement, par la propriété précédente, une martingale.

Nous pouvons de la même façon vérifier que : $N_t = N([0,t],\mathsf{R}^+)$ est bien un processus d'intensité $\lambda(t)$ en effet :

$$\int_0^t \int_{\mathsf{R}^+} \int_{\mathsf{R}^+} \mathbb{1}_{(s)p_{Ujs}(u)} M(\mathrm{d}s,\mathrm{d}u,\mathrm{d}\theta) \quad \int_0^t \int_{\mathsf{R}^+} \int_{\mathsf{R}^+} \mathbb{1}_{(s)p_{Ujs}(u)} m(\mathrm{d}s,\mathrm{d}u,\mathrm{d}\theta)$$
$$= N_t \quad \int_0^t \lambda(s)\mathrm{d}s$$

est bien une martingale. Cette façon de représenter le processus est la représentation de *Thinning* dans le sens où l'obtention de notre processus se fait via la sélection de certains points de la mesure aléatoire de Poisson.

Interessons nous maintenant à l'intensité des $(T_n^R)_{n\ 1}$. La mesure représentant les couples (T_n, U_n) observés est : $N^R(\mathrm{d}t,\mathrm{d}u) = \mathbb{1}_{t+u} \quad N(\mathrm{d}t,\mathrm{d}u)$, en remarquant encore une fois que :

$$N^R([0,t],\mathsf{R}^+) \quad \int_0^t \int_{\mathsf{R}^+} \mathbb{1}_{s+u} \quad \lambda(s)p_{Ujs}(u)\mathrm{d}u\mathrm{d}s$$
$$= N^R([0,t],\mathsf{R}^+) \quad \int_0^t \lambda(s)p_{Ujs}(0,\tau \quad s)\mathrm{d}s$$

est une martingale, nous avons désormais l'intensité pour les temps d'occurrence des évènements observés : $\lambda^R(t) = \lambda(t)p_{Ujt}([0,\tau \quad t])$. En reprenant les calculs avec $N^{IBNR}(\mathrm{d}t,\mathrm{d}u) = \mathbb{1}_{t+u} \quad N(\mathrm{d}t,\mathrm{d}u)$ nous avons également l'intensité du processus des IBNR : $\lambda^R(t) = \lambda(t)p_{Ujt}(]\tau \quad t,\ \infty[)$.

3.3 La fonction de vraisemblance

3.3.1 Forme de la fonction de vraisemblance

Supposons que nous disposons d'observations $(t_n^R)_{n=1}^{n_\tau^R}$ et des délais associés $(u_n^R)_{n=1}^{n_\tau^R}$. Avec n^R le nombre d'occurrences rapportées jusqu'à τ.
Notons :

- $H_n = \{T_1^R = t_1^R, ..., T_n^R = t_n^R\}$.
- $\mathsf{P}\big(. \mid (T_n^{IBNR})_{n\ 1}\big)$ la probabilité sachant l'information des $(T_n^{IBNR})_{n\ 1}$ au cours du temps, c'est-à-dire connaissant pour tout temps t l'ensemble $\{T_n^{IBNR}, T_n^{IBNR} \leq t\}$, ensemble que nous noterons H_t^{IBNR}.

En se basant sur le calcul de la fonction de vraisemblance d'un processus ponctuel en Annexe C, nous pouvons écrire la fonction de vraisemblance des sinistres observés (nous utilisons la notation P par abus de langage, en réalité nous faisons plutôt référence à une densité) :

$$
\begin{aligned}
&\mathrm{P}\left(\delta 1 \quad n \quad n^R, T_n^R = t_n^R, U_n^R = u_n^R, \text{ et } N^R = n^R \mid (T_n^{IBNR})_{n\ 1}\right) \\
&= \mathrm{P}\left(N^R = n^R \mid H_{n_\tau^R}\right) \prod_{n=1}^{n_\tau^R} \mathrm{P}\left(T_n^R = t_n^R \mid H_{n\ 1}, H_{t_n^R}^{IBNR}\right) \mathrm{P}\left(U_n^R = u_n^R \mid T_n^R = t_n^R\right) \\
&= \exp\left(\int_{t_{n_\tau^R}^R}^{} \lambda^R(s)\mathrm{d}s \right) \prod_{n=1}^{n_\tau^R} \lambda^R\left(t_n^R\right) \exp\left(\int_{t_n^R\ 1}^{t_n^R} \lambda^R(s)\mathrm{d}s \right) \frac{p_{U|t_n^R}(u_n^R)}{p_{U|t_n^R}([0,\tau \quad t_n^R])} \\
&= \exp\left(\int_0^{} \lambda^R(s)\mathrm{d}s \right) \prod_{n=1}^{n_\tau^R} \lambda^R\left(t_n^R\right) \frac{p_{U|t_n^R}(u_n^R)}{p_{U|t_n^R}([0,\tau \quad t_n^R])} \\
&= \exp\left(\int_0^{} \lambda(s) p_{U|s}([0,\tau \quad s])\mathrm{d}s \right) \prod_{n=1}^{n_\tau^R} \lambda\left(t_n^R\right) p_{U|t_n^R}(u_n^R),
\end{aligned}
$$

Finalement la log-vraisemblance, que nous noterons : $L(\phi, \mu)$ a la forme suivante :

$$
\begin{aligned}
\mathrm{L}(\phi,\mu) = & \int_0^{} \lambda(s) p_{U|s}([0,\tau \quad s])\mathrm{d}s + \sum_{n=1}^{n_\tau^R} \left\{ \ln\left(\lambda\left(t_n^R\right)\right) + \ln\left(p_{U|t_n^R}(u_n^R)\right) \right\} \\
= & \int_{t_{n_\tau^R}^R}^{} \lambda(s) p_{U|s}([0,\tau \quad s])\mathrm{d}s + \sum_{n=1}^{n_\tau^R} \int_{t_n^R\ 1}^{t_n^R} \lambda(s) p_{U|s}([0,\tau \quad s])\mathrm{d}s \qquad (3.1) \\
& + \sum_{n=1}^{n_\tau^R} \ln(\lambda(t_n^R)) + \sum_{n=1}^{n_\tau^R} \ln(p_{U|t_n^R}(u_n^R)).
\end{aligned}
$$

Cette vraisemblance prend en compte le biais d'observation provenant du fait que seul les temps rapportés sont observés.

3.3.2 Approximation par l'espérance conditionnelle

Un fait remarquable dans cette fonction de vraisemblance est que même si nous avons fait l'e□ort de l'écrire par rapport aux seuls temps observés, elle dépend en réalité des temps non observés, ceci est dû à la caractéristique auto-régressive du processus de Hawkes. Plus précisément, étant donné que dans l'écriture de la vraisemblance :

$$
\lambda(s) = \mu(s) + \sum_{T_n < s} \phi(s \quad T_n) = \mu(s) + \sum_{t_n^R < s} \phi(s \quad t_n^R) + \sum_{T_n^{IBNR} < s} \phi(s \quad T_n^{IBNR})
$$

nous ne pouvons calculer $\lambda(s)$ car les $(T_n^{IBNR})_{n\ 1}$ ne sont pas observés. Par conséquent il n'est pas non plus possible de calculer $L(\phi, \mu)$. En réalité cette fonction de vraisemblance est une variable aléatoire qui dépend des $(T_n^{IBNR})_{n\ 1}$.

Une première idée pour palier à ce problème est d'estimer cette fonction de vraisemblance en calculant son espérance conditionnelle sachant tout le passé connu :

$$\mathsf{E}\,[L(\phi,\mu)] := \mathsf{E}\big[L(\phi,\mu)\ j\ (T_k^R = t_k^R)_{k=1}^{n_\tau^R}\big]$$

Obtenir cette espérance serait idéal dans le sens où elle permet d'utiliser toute l'information disponible sur le processus. Cependant, cela mène à évaluer des termes du type :

$$\mathsf{E}\big[\lambda(s)\ j\ (T_k^R = t_k^R)_{k=1}^{n_\tau^R}\big], s \quad \tau$$

et nécessite, pour mener le calcul à son terme, de connaître la loi du processus conditionnée par la position exacte de certains temps futurs. Cette loi se révèle trop complexe à déterminer dans le cadre d'un processus de Hawkes. En e□et, étant donné que l'intensité stochastique du processus dépend de tous les temps passés, connaître la position d'une occurrence future influence de façon complexe le processus d'intensité passé.

Notre alternative est de nous tourner vers une estimation par une espérance contenant un peu moins d'informations. Nous profitons de l'écriture par intervalle sous la forme (3.1) pour éviter le problème discuté ci-dessus, et ce, en estimant chaque terme par une espérance adaptée :

$$\text{Les termes : } \int_{t_{n\ 1}^R}^{t_n^R} \lambda(s) p_{Ujs}([0,\tau \quad s])\mathrm{d}s \text{ ainsi que : } \ln(\lambda(t_n^R))$$

$$\text{seront estimés par : } \mathsf{E}_{n\ 1}\Big[\int_{t_{n\ 1}^R}^{t_n^R} \lambda(s) p_{Ujs}([0,\tau \quad s])\mathrm{d}s\Big] \text{ et : } \mathsf{E}_{n\ 1}\big[\ln(\lambda(t_n^R))\big]$$

$$\text{Avec pour définition : } \mathsf{E}_{n\ 1}[.] := \mathsf{E}\big[.\ j\ (T_k^R = t_k^R)_{k=1}^{n\ 1}\big]$$

Notre vraisemblance est finalement estimée par la formule suivante :

$$\begin{aligned} L(\phi,\mu) \quad & \int_{t_{n_\tau^R}^R}^{} \mathsf{E}_{n_\tau^R}\big[\lambda(s)\big] p_{Ujs}([0,\tau \quad s])\mathrm{d}s + \sum_{n=1}^{n_\tau^R} \int_{t_{n\ 1}^R}^{t_n^R} \mathsf{E}_{n\ 1}\big[\lambda(s)\big] p_{Ujs}([0,\tau \quad s])\mathrm{d}s \\ & + \sum_{n=1}^{n_\tau^R} \mathsf{E}_{n\ 1}\big[\ln(\lambda(t_n^R))\big] + \sum_{n=1}^{n_\tau^R} \ln(p_{Ujt_n^R}(u_n^R)) \end{aligned} \tag{3.2}$$

Il reste à estimer le terme $\mathsf{E}_{n\ 1}\big[\ln(\lambda(t_n^R))\big]$, par exemple avec la méthode Delta :

$$\mathsf{E}_{n\ 1}\big[\ln(\lambda(s))\big] \quad \ln(\mathsf{E}_{n\ 1}\big[\lambda(s)\big]) \quad \frac{Var_{n\ 1}\big[\lambda(s)\big]}{2\mathsf{E}_{n\ 1}\big[\lambda(s)\big]^2} \tag{3.3}$$

3.3.2.1 Calcul des espérances

Intéressons nous maintenant au calcul du terme $E_{n-1}[\lambda(s)]$ pour $s \in]t_{n-1}^R, t_n^R]$ avec $n-1$ fixé.

Nous effectuerons la suite des calculs en se plaçant dans le cas classique où la fonction ϕ est de la forme : $\phi(s) = \alpha \exp(-\beta s)$.

$$
\begin{aligned}
E_{n-1}[\lambda(s)] &= \mu(s) + E_{n-1}\Big[\sum_{T_k<s} \phi(s-T_n)\Big] \\
&= \mu(s) + E_{n-1}\Big[\sum_{T_k-t_{n-1}^R} \phi(s-T_k)\Big] + E_{n-1}\Big[\int_{t_{n-1}^R}^{s} \phi(s-v)dN_v\Big] \\
&= \mu(s) + E_{n-1}\Big[\sum_{T_k<t_{n-1}^R} \phi(s-T_k)\Big] + \phi(s-t_{n-1}^R) + E_{n-1}\Big[\int_{t_{n-1}^R}^{s} \phi(s-v)dN_v\Big] \qquad (3.4) \\
&= \mu(s) + \exp(-\beta(s-t_{n-1}^R))\Big(E_{n-1}\big[\lambda(t_{n-1}^R)\big] - \mu(t_{n-1}^R)\Big) + \phi(s-t_{n-1}^R) \\
&+ E_{n-1}\Big[\int_{t_{n-1}^R}^{s} \phi(s-v)dN_v\Big]
\end{aligned}
$$

Avec :

$E_{n-1}\Big[\int_{t_{n-1}^R}^{s} \phi(s-v)\mathrm{d}N_v\Big]$

$E_{n-1}\Big[\int_{t_{n-1}^R}^{s} \phi(s-v)\mathrm{d}N_v^{IBNR}\Big]$ (Nous effectuons cette approximation pour prendre en compte le fait que sur $]t_{n-1}^R, t_n^R[$ il n'y a pas d'occurences observées.) (*)

$=E_{n-1}\Big[\int_{t_{n-1}^R}^{s} \phi(s-v)\lambda^{IBNR}(v)\mathrm{d}v\Big]$ (Cette étape n'est pas immédiate, son détail apparaît en Annexe K)

$=E_{n-1}\Big[\int_{t_{n-1}^R}^{s} \phi(s-v)\lambda(v)p_{Uj|v}(\tau-v, 1)\mathrm{d}v\Big]$

$= \int_{t_{n-1}^R}^{s} \phi(s-v)E_{n-1}[\lambda(v)]p_{Uj|v}(\tau-v, 1)\mathrm{d}v$

L'expression (3.4) devient donc :

$$
\begin{aligned}
E_{n-1}[\lambda(s)] &= \mu(s) + \exp(-\beta(s-t_{n-1}^R))\Big(E_{n-1}[\lambda(t_{n-1}^R)] - \mu(t_{n-1}^R)\Big) + \phi(s-t_{n-1}^R) \\
&+ \int_{t_{n-1}^R}^{s} \phi(s-v)E_{n-1}[\lambda(v)]p_{Uj|v}(\tau-v, 1)\mathrm{d}v
\end{aligned}
\qquad (3.5)
$$

En posant $g_{n\ 1}(s) = \mathsf{E}_{n\ 1}[\lambda(s)]$ et en dérivant l'expression (5) nous obtenons :

$$g'_{n\ 1}(s) = \mu'(s) \quad \beta \exp(\ \beta(s \quad t^R_{n\ 1})\Big(\mathsf{E}_{n\ 1}[\lambda(t^R_{n\ 1})] \quad \mu(t^R_{n\ 1})\Big) \quad \beta\phi(s \quad t^R_{n\ 1}) + \frac{\partial}{\partial s}\Big[\int_{t^R_{n\ 1}}^{s} \phi(s \quad v)\mathsf{E}_{n\ 1}[\lambda(v)p_{Ujv}(\tau \quad v, 1)]\mathrm{d}v\Big]$$

En remarquant que :

$$\frac{\partial}{\partial s}\Big[\int_{t^R_{n\ 1}}^{s} \phi(s \quad v)\mathsf{E}_{n\ 1}[\lambda(v)]\mathrm{d}v\Big]$$

$$= \phi(0)p_{Ujs}(\tau \quad s, 1)\mathsf{E}_{n\ 1}[\lambda(s)] + \int_{t^R_{n\ 1}}^{s} \phi'(s \quad v)\mathsf{E}_{n\ 1}[\lambda(v)p_{Ujv}(\tau \quad v, 1)]\mathrm{d}v$$

$$= \phi(0)p_{Ujs}(\tau \quad s, 1)\mathsf{E}_{n\ 1}[\lambda(s)] \quad \int_{t^R_{n\ 1}}^{s} \beta\alpha \exp(\ \beta(s \quad v))\mathsf{E}_{n\ 1}[\lambda(v)p_{Ujv}(\tau \quad v, 1)]\mathrm{d}v$$

Le passage à la ligne suivante provient de l'expression de l'intégrale isolée dans (3.5)

$$= \phi(0)p_{Ujs}(\tau \quad s, 1)\mathsf{E}_{n\ 1}[\lambda(s)] \quad \beta\Big(\mathsf{E}_{n\ 1}[\lambda(s)] \quad \Big(\mu(s) + \exp(\ \beta(s \quad t^R_{n\ 1}))(\mathsf{E}_{n\ 1}[\lambda(t^R_{n\ 1})] \quad \mu(t^R_{n\ 1})) + \phi(s \quad t^R_{n\ 1})\Big)\Big)$$

Nous obtenons finalement :

$$g'_{n\ 1}(s) = g_{n\ 1}(s)(\phi(0)p_{Ujs}(\tau \quad s, 1) \quad \beta) + \mu'(s) + \beta\mu(s) \tag{3.6}$$

La forme de la solution de cette équation différentielle linéaire du premier ordre est la suivante :

$$g_{n\ 1}(s) = \mathsf{E}_{n\ 1}[\lambda(s)]$$

$$= e^{\int_{t^R_{n\ 1}}^{s}(\ (0)p_{Ujv}(\quad v; 1) \quad)\mathrm{d}v}\Big(K + \int_{t^R_{n\ 1}}^{s} (\mu'(v) + \beta\mu(v))e^{\ \int_{t^R_{n\ 1}}^{v}(\ (0)p_{Ujx}(\quad x; 1) \quad)\mathrm{d}x}\mathrm{d}v\Big)$$

Avec K déterminé par les conditions initiales, c'est-à-dire :

$$K = \mathsf{E}_{n\ 1}[\lambda(t^R_{n\ 1}+)] := \mathsf{E}_{n\ 2}[\lambda(t^R_{n\ 1})] + \alpha$$

Nous pouvons alors calculer par récurrence les termes de l'approximation de la vraisemblance (3.2).

Remarque 1 : L'approximation faite en (*) est importante : pour que le passage de $\mathrm{d}N_v$ à $\mathrm{d}N^{IBNR}_v$ soit exact il aurait fallu conditionner jusqu'à l'évènement $fT^R_n = t^R_n g$. Cependant, ce conditionnement ne permet pas le passage de $\mathrm{d}N^{IBNR}_v$ à $\lambda^{IBNR}(v)\mathrm{d}v$ qui

suit (*), et qui est détaillé en Annexe K. En particulier, dans la preuve, sous un conditionnement jusqu'à $fT_n^R = t_n^R g$, Z n'est plus mesurable par rapport à $P(G_t)$.

Remarque 2 : Il est possible de reprendre nos calculs en prenant soin de ne pas e□ectuer l'approximation (*) (c'est- à-dire sans ajouter l'information qu'il n'y a que des IBNR sur chaque intervalle considéré). Dans ce cas, nous aboutissons à la dynamique suivante :

$$g^{\emptyset}(s) = g(s)(\phi(0) \quad \beta) + \mu^{\emptyset}(s) + \beta\mu(s) \tag{3.7}$$

Deux choses sont remarquables sur ce résultat :

— Premièrement, cette dynamique aurait été la même si les calculs avaient été faits avec une simple espérance (pour le vérifier, le calcul se reprend très simplement). Ceci est dû au fait que le conditionnement s'arrête au début de l'intervalle, la seule donnée qui change étant la condition initiale.

— Deuxièmement, cette dynamique est semblable à (3.6) hormis le fait que, dans le cas où $\phi(0) < \beta$, le facteur de décroissance est plus marqué avec notre équation (3.6) que celui de l'équation (3.7) car nous avons : $\phi(0)p_{Ujs}(\tau \quad s, 1) \quad \beta \quad \phi(0) \quad \beta$. De la même façon, dans le cas où $\phi(0) > \beta$, le facteur de croissance est moins marqué (et peut même être négatif) dans notre équation (3.6) que dans (3.7).

  Ceci vient caractériser le fait que l'équation (3.6) prend en compte l'information que sur $]t_{n\ 1}^R, t_n^R[$ il n'y a pas de présence de temps rapportés mais uniquement des IBNR (grâce a (*)), alors que l'équation (3.7) considère que les deux types de temps peuvent être générés.
  Naturellement, la tendance moyenne de l'intensité à croître est moins marquée avec moins d'évènements.

Interprétation du résultat : Le passage en (*) a été forcé afin de prendre en compte le fait que sur chaque intervalle seuls des IBNR sont en mesure de survenir et donc de faire sauter l'intensité. Ceci peut donner le sentiment que l'espérance conditionnelle calculée est celle d'un processus de Hawkes qui e□ectivement n'a pour saut que des IBNR entre deux temps rapportés. En réalité, nous avons un peu moins d'informations, car en (3.5) l'espérance sous l'intégrale ne conditionne pas cette information. Cette espérance prend en compte que les deux types d'évènements peuvent survenir. Nous n'avons ni $E_{n\ 1}$, ni E telles qu'elles ont été définies. Notre formule $g_{n\ 1}$ est une sorte de compromis entre les deux.

Finalement le calcul de nos espérances conditionnelles s'e□ectue en pratique de la manière récursive suivante :

— $g_0(t_1^R)$ est calculé avec comme condition initiale $\mu = E[\lambda(0)]$ car il n'y a pas de saut en zéro.

— De façon récurrente, $g_{n\ 1}(t_n^R)$ est calculé avec comme condition initiale $g_{n\ 1}(t_{n\ 1}^R+) = g_{n\ 2}(t_{n\ 1}^R) + \alpha$, ce qui correspond à prendre notre approximation précédente et à ajouter artificiellement le saut correspondant à l'occurrence $t_{n\ 1}^R$.

3.4 Validité du modèle dans un cadre classique

Le modèle contenant plusieurs approximations, il est nécessaire de vérifier empiriquement si les résultats restent cohérents avec ce qui est souhaité en terme de modélisation, à savoir réduire le biais de calibrage généré par la présence d'IBNR.

Afin de vérifier si le passage (*) a du sens, les premières applications ont été effectuées pour tester les modèles découlant des calculs avec et sans l'approximation (*). C'est-à-dire, le modèle que nous appellerons modèle 1 qui découle de l'équation différentielle (3.7) ainsi que le modèle 2 qui découle de l'équation différentielle (3.6).

3.4.1 Modèle

Ces premiers tests ont été effectués dans un cadre classique, le processus de Hawkes a pour intensité :

$$\lambda(s) = \mu + \int_0^s \alpha \exp(-\beta(s-u))\mathrm{d}N_u, (\mu,\alpha,\beta) \in (\mathrm{R}^+)^3$$

Et les délais seront modélisés avec un modèle exponentiel de paramètre θ, dont la densité est $f(x) = \theta \exp(-\theta x)$.

3.4.2 Calculs de g

Sous le modèle 1 la fonction g se calcule explicitement et a la forme suivante, pour s appartenant à $]t_{n\ 1}^R, t_n^R]$:

$$g_{n\ 1}(s) = \exp\left((\alpha-\beta)(s-t_{n\ 1}^R)\right)\left(K_1 + \frac{\beta\mu}{(\alpha-\beta)}\right) - \frac{\beta\mu}{(\alpha-\beta)}$$

avec $K_1 = g_{n\ 2}(t_{n\ 1}^R) + \alpha$.

Sous le modèle 2, une intégration numérique a été effectuée pour le calcul de g car l'équation différentielle ne possède pas de solution explicite.

Le terme d'ordre deux dans l'approximation 3.3 est pour l'instant ignoré car les approximations effectuées ne permettent pas de connaître la loi réelle qui est sous-entendue par le modèle.

3.4.3 Validité de l'approche par espérance conditionnelle

3.4.3.1 Aspect graphique

Le premier intérêt des espérances conditionnelles est d'approcher $\lambda(s)$ qui nous est inconnu. Pour vérifier si cette approche a du sens, nous avons simulé un processus de

Hawkes connaissant ses paramètres, puis tracé son intensité réelle (= théorique), notre estimation de l'intensité par g (= modèle IBNR), ainsi que l'intensité biaisée :

$$\lambda_{biais}(s) = \mu + \sum_{T_n^R < s} \alpha \exp(\beta(s - T_n^R))$$

Cette méthode a été e□ectuée pour di□érents jeux de paramètres. Les tendances générales se retrouvent dans l'exemple donné à travers les Figures 3.2, 3.3 et 3.4. La première figure concerne le modèle 1, sans l'approximation (*), les deux autres figures correspondent au modèle 2, avec en 3.4 un zoom sur la période de fin d'observation, où se situe la majorité des IBNR.

Graphiquement, il semble que le modèle 2 qui e□ectue l'approximation (*) :

$$E_{n-1}\left[\int_{t_n^R}^{s} \phi(s-v)\mathrm{d}N_v\right] \quad E_{n-1}\left[\int_{t_n^R}^{s} \phi(s-v)\mathrm{d}N_v^{IBNR}\right] \tag{3.8}$$

permette une meilleure estimation de $\lambda(s)$ par $E_{n-1}[\lambda(s)]$.

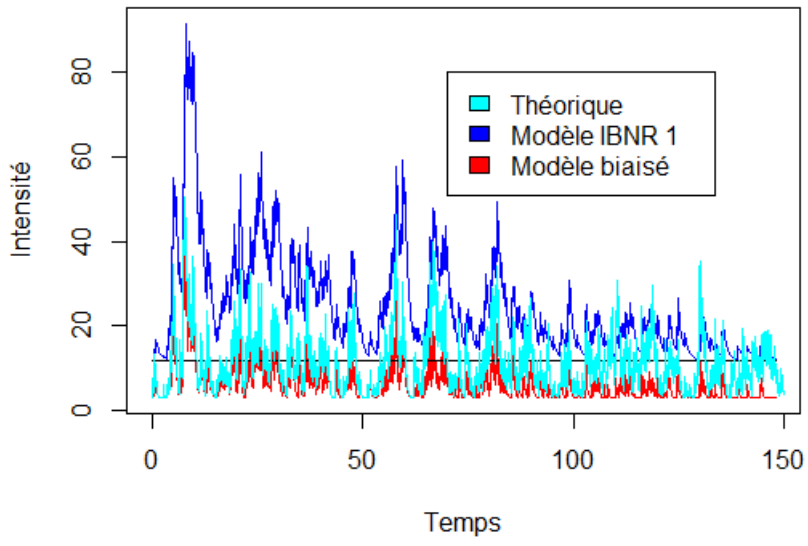


Figure 3.2 – Comparaison modèle 1

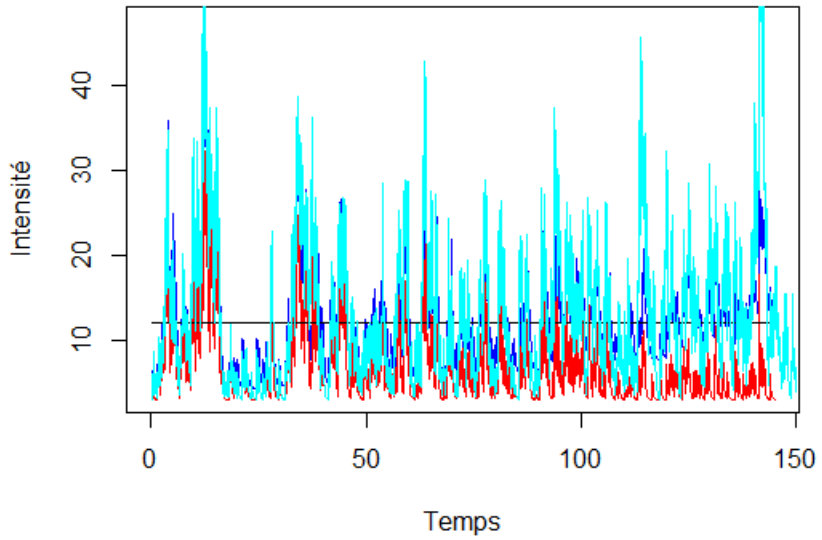


Figure 3.3 – Comparaison modèle 2

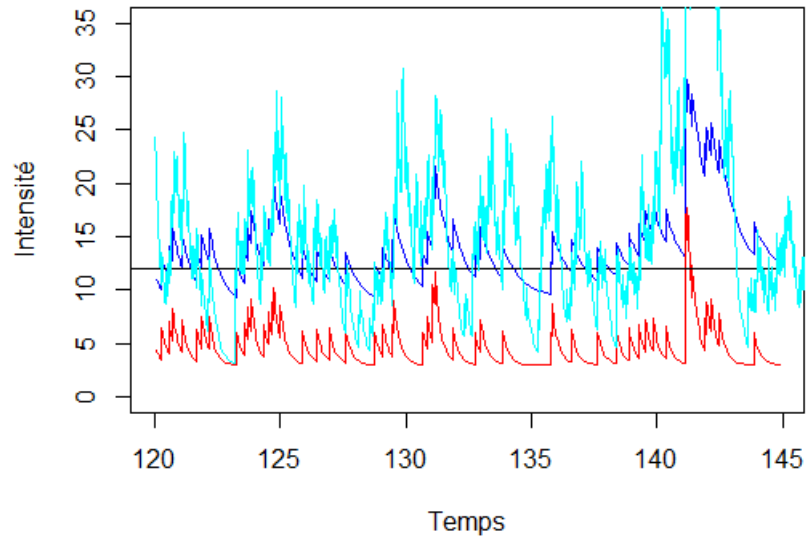


Figure 3.4 – Comparaison modèle 2 (Zoom)

En effet, l'intensité estimée (bleue) est plus proche de l'intensité réelle (cyan) sous le modèle 2, là où le modèle 1 la surestime toujours. En particulier, en zoomant (Figure 3.4) vers les temps longs (là où le processus est susceptible d'avoir des IBNR), nous pouvons observer que le modèle 2 permet bien de rehausser l'intensité estimée pour la rapprocher de l'intensité réelle, alors qu'un calcul par un modèle de Hawkes simple (rouge) donnerait une intensité biaisée, plus faible.

Le modèle 1 semble moins fiable pour estimer par la suite les paramètres avec une optimisation. En effet sous ce modèle, nous pouvons observer que la forme de g ne lui permet pas de descendre en dessous de l'intensité moyenne $\frac{\alpha}{1-\frac{\alpha}{\beta}}$ (tracée en noir) une fois qu'elle l'a dépassée. D'autant plus que dans la grande majorité des tests elle surestime toujours l'intensité réelle, ce qui n'est pas contre-intuitif car sans l'approximation (*), comme évoqué dans la remarque 2, la dynamique de g sur un intervalle est celle d'une espérance simple. Cela signifie que dans cette dynamique, il n'est pas considéré que seul un type d'évènement puisse survenir entre deux temps observés. Pourtant nous faisons tout de même sauter l'intensité aux temps observés, naturellement nous surestimons l'intensité moyenne réelle. Dans la suite des résultats nous ne nous intéresserons qu'au modèle 2.

3.4.3.2 Validité de l'approximation

Étant donné les différentes approximations, comme précisé précédemment, la fonction g_{n-1} ne correspond ni à E_{n-1} ni à E comme nous les avons définies. Comme ces espérances conditionnelles sont difficiles à calculer et à simuler nous n'avons pas de benchmark direct de comparaison. En revanche, notre méthode de calcul explicitée dans le paragraphe "Interprétation du résultat" est proche au fait de baser nos calculs sur le processus $(\widetilde{T_n})_{n-1}$ qui suit cette définition :

- Sur l'intervalle $[0, t_1^R[$ seuls des IBNR T_n^{IBNR} surviennent
- Le comportement sur chaque intervalle $[t_{n-1}^R, t_n^R[$ est le suivant :
  - l'intensité de départ est l'intensité moyenne calculée sur l'intervalle précédent $E_{n-1}\left]t_{n-2}^R, t_{n-1}^R\right]$ plus un saut α
  - Seuls des IBNR surviennent sur chaque intervalle

Il est possible de générer des simulations d'arrivées d'IBNR, avec ce comportement, en adaptant l'algorithme d'Ogata détaillé en section 2.3.4.2 et en Annexe B.

Comme nous savons qu'entre deux temps rapportés il n'y a que des IBNR, l'idée est de les simuler sur cet intervalle que nous notons : $]t_{n-1}^R, t_n^R]$. Pour ce faire nous utilisons la même logique que l'algorithme d'Ogata appliquée avec l'intensité des IBNR : $\lambda^{IBNR}(t) = \lambda(t)p_{Ujt}(0, \tau - t)$.

Nous pouvons alors, grâce à ces simulations, calculer l'espérance empirique de l'intensité du processus décrit ci-dessus E_{n-1}, en chaque temps t_n^R et la comparer à notre valeur $g_{n-1}(t_n^R)$.

La méthode est la suivante : considérons que nous avons la réalisation d'un processus

de temps observés $(T_k^R)_{k=1}^{n_\tau^R}$. En notant $\widetilde{\lambda}$ l'intensité du processus décrit ci-dessus. En prenant comme notation :

$$\mathbb{E}_{n-1}[\lambda(t_n^R)] = \frac{1}{M}\sum_{k=1}^{M}\widetilde{\lambda^{(k)}}(t_n^R)$$

la moyenne empirique sur M simulation de $\widetilde{\lambda}(t_n^R)$.

La méthode pour calculer empiriquement $\mathbb{E}_{n-1}[\lambda(t_n^R)]$ est la suivante :

— Utiliser l'algorithme de génération d'IBNR sur l'intervalle $]t_{n-1}^R, t_n^R]$ avec pour intensité de départ $\mathbb{E}_{n-2}[\lambda(t_{n-1}^R)] + \alpha$

— calculer l'intensité $\widetilde{\lambda^{(k)}}(t_n^R)$ qui découle de cette trajectoire :

$$\begin{aligned}\widetilde{\lambda^{(k)}}(t_n^R) &= \left(\widetilde{\lambda^{(k)}}(t_{n-1}^R) + \alpha - \mu\right)\exp(-\beta(t_n^R - t_{n-1}^R)) + \mu \\ &\quad + \sum_{t_{n-1}^R < T_k^{IBNR} < t_n^R}\phi(t_n^R - T_k^{IBNR}) \\ &= \left(\mathbb{E}_{n-2}[\lambda(t_{n-1}^R)] + \alpha - \mu\right)\exp(-\beta(t_n^R - t_{n-1}^R)) + \mu \\ &\quad + \sum_{t_{n-1}^R < T_k^{IBNR} < t_n^R}\phi(t_n^R - T_k^{IBNR})\end{aligned}$$

— Effectuer les deux points précédents un grand nombre M de fois puis calculer : $\mathbb{E}_{n-1}[\lambda(t_n^R)]$ définit ci-dessus.

Le graphique ci-dessous représente les quantiles à 95% des erreurs relatives de $g_{n-1}(t_n^R)$ par rapport à l'estimation empirique $\mathbb{E}_{n-1}[\lambda(t_n^R)]$ sur 22 jeux de paramètres. Pour vérifier la validité de la formule, nous avons considéré, pour $s \in]t_{n-1}^R, t_n^R]$, la condition initiale : $g_{n-1}(t_{n-1}^R+) = \mathbb{E}_{n-2}[\lambda(t_{n-1}^R)] + \alpha$, c'est-à-dire l'intensité de départ qui sert pour le calcul de $\mathbb{E}_{n-1}[\lambda(t_n^R)]$, afin de pouvoir comparer les deux formules.

Le principe est le suivant : chaque point correspond à un jeu de paramètres qui a généré une simulation d'un processus de Hawkes associé (horizon de temps 150). Sur cette simulation, nous avons calculé : $\left(\mathbb{E}_{n-1}[\lambda(t_n^R)]\right)_{n=1}^{n_\tau^R}$ à partir de 5000 simulations à l'aide de l'algorithme d'Ogata. Ensuite nous avons représenté sur le graphique le quantile à 95% de la distribution des erreurs relatives, c'est-à-dire le quantile empirique à 95% de :

$$\left(\left|\frac{\mathbb{E}_{n-1}[\lambda(t_n^R)] - g_{n-1}(t_n^R)}{\mathbb{E}_{n-1}[\lambda(t_n^R)]}\right|\right)_{n=1}^{n_\tau^R}$$

le but étant qu'il soit le moins élevé possible.

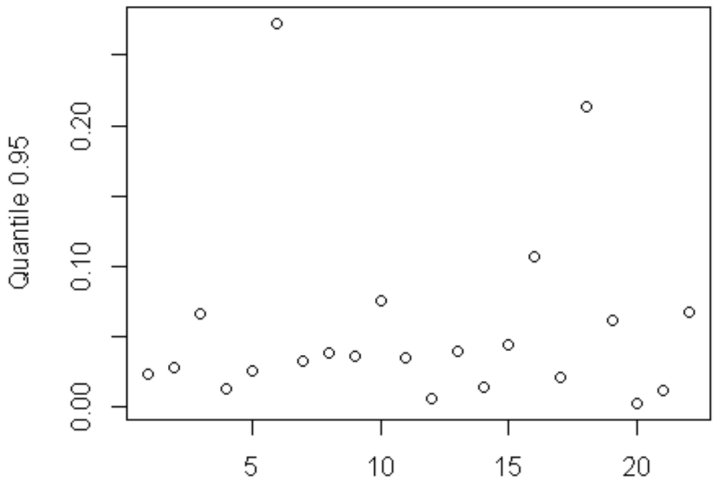


Figure 3.5 – Quantiles 95% des erreurs relatives

Mis à part trois jeux de données, les quantiles à 95% sont tous inférieurs à 10%. Cela signifie que plus de 95% des termes $E[\ _1[\lambda(t_n^R)]$ sont approchés par notre fonction $g_{n\ 1}(.)$ en t_n^R avec une erreur inférieure à 10%. De plus, 15 jeux de données ont des quantiles inférieurs à 5%, ces éléments semblent indiquer que notre formule $g_{n\ 1}$ a bien du sens.

3.4.4 Estimations et impact du paramètre θ

3.4.4.1 Estimations

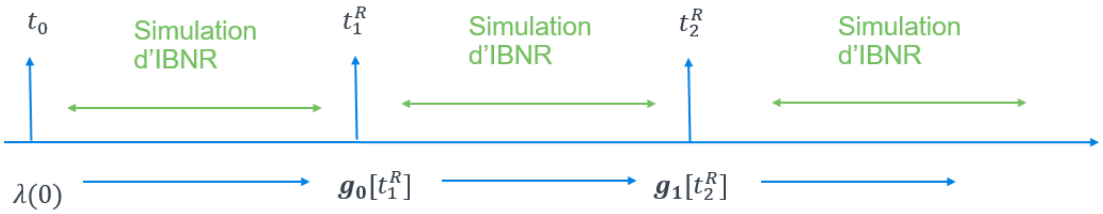
La vraisemblance approchée a été testée sur 22 jeux de paramètres. Pour chacun d'entre eux une simulation du processus a été générée puis les paramètres ont été estimés par la vraisemblance approchée (sans biais) ainsi que par la vraisemblance d'un Hawkes simple et d'une loi exponentielle simple (vraisemblances séparées donc biaisées).

Les résultats des estimations ainsi que les erreurs relatives d'estimation sont en Annexe L. Nous pouvons remarquer que les paramètres estimés étudiés de façon isolée ne sont pas toujours meilleurs avec la vraisemblance sans biais. En revanche le nombre moyen d'IBNR théorique obtenu avec les paramètres estimés par la vraisemblance sans biais est dans la plupart des cas (17/22) plus proche du nombre moyen théorique réel qu'avec les paramètres estimés avec biais. Et dans tous les cas testés, ce nombre est supérieur à celui obtenu avec les paramètres biaisés, donc plus prudent.

3.4.4.2 Prédictions du nombre d'IBNR

Grâce à l'algorithme de simulation évoqué précedemment, il nous est possible de générer des simulations d'arrivées d'IBNR. Comme nous savons qu'entre deux temps rapportés il n'y a que des IBNR, l'idée est de les simuler sur cet intervalle que nous notons : $]t_{n\ 1}^{R}, t_n^R]$. L'intensité exacte $\lambda(.)$ n'étant pas connue, l'algorithme est initialisé sur chaque intervalle avec l'intensité :

$$\lambda^{IBNR}(t_{n\ 1}^{R}+) \quad (g_{n\ 2}(t_{n\ 1}^{R}) + \alpha)p_{Ujt_{n\ 1}^{R}}(0, \tau \quad t_{n\ 1}^{R})$$



ci-dessous les nombres d'IBNR réels de nos 22 simulations, avec les quantiles empiriques (provenant de 2000 simulations) à 5% et 95%. Les paramètres utilisés sont les paramètres estimés précédemment, ici toutes les erreurs de notre méthode sont donc prises en compte dans les résultats.

	1	2	3	4	5	6	7	8	9	10	11
Quantile 5%	54	53	9	4742	9	386	45	26	206	55	65
Nombre réel	61	77	18	5128	12	177	65	36	212	59	77
Quantile 95%	84	84	22	4967	24	474	71	48	259	96	122
	12	13	14	15	16	17	18	19	20	21	22
Quantile 5%	76	124	7	99	4	64	279	113	5250	31	65
Nombre réel	100	134	7	126	6	57	235	127	5378	32	95
Quantile 95%	106	167	18	138	16	94	361	160	5488	52	102

Table 3.1 – Nombres d'IBNR estimés

18 cas sur 22 ont un nombre réel d'IBNR compris entre les deux quantiles prédits, ce qui signifie que notre méthode fait sens, malgré ses approximations à divers niveaux.

3.4.4.3 Impact du paramètre θ

Le paramètre θ joue un rôle sur le nombre d'IBNR, plus il est grand moins il y a d'IBNR. Cela amène à se poser la question de l'intérêt de notre approximation de la vraisemblance dans le cas où ce paramètre est assez grand, en e□et dans ce cas il y a peu d'IBNR donc la question se pose du choix entre la vraisemblance du Hawkes simple,

certes baisée (mais peu car peu d'IBNR) mais non approximée, et notre approximation sans biais. Pour illustrer ce phénomène, nous avons estimé les paramètres de dix jeux de données simulés, en ne faisant varier que theta. Les valeurs de theta et le pourcentage théorique moyen d'IBNR sont les suivants :

	1	2	3	4	5
theta	0.0250	0.0555	0.08611	0.11667	0.1472
Pourcentage d'IBNR	0.2604	0.1200	0.0774	0.05714	0.0453
	6	7	8	9	10
theta	0.1778	0.2083	0.2389	0.2694	0.3000
Pourcentage d'IBNR	0.0375	0.0320	0.0279	0.0247	0.0222

Table 3.2 – Évolution de theta

En Annexe M, les graphiques des erreurs relatives des prédictions du nombre moyen d'IBNR. c'est-à-dire l'erreur entre le nombre obtenu avec les paramètres réels, et celle obtenue avec les paramètres estimés. Avec en rouge les résultats avec les paramètres estimés biaisés, en bleu les résultats avec les paramètres estimés par notre méthode sans biais. En particulier, nous pouvons observer que lorsque le nombre d'IBNR est élevé (theta faible), notre méthode a toujours une meilleure performance que l'estimation biaisée. Cet écart se réduit avec le nombre d'IBNR, cependant pour tous les jeux de paramètres testés sauf deux, notre méthode reste meilleure ou égale, jusqu'à un taux d'IBNR de 2.2%.

3.5 Une application au cyber-risque

3.5.1 Description de la base de données

3.5.1.1 Provenance

En section 1.2.2 nous avons discuté des obligations de notifications en terme de violations de données, aux États-Unis, l'avantage de ces lois de notification est qu'il est possible de trouver des bases de données publiques pour plusieurs états, recensant les attaques, avec en particulier la date de survenance de l'attaque et la date de notification de l'attaque. L'écart entre ces deux dates peut provenir de délais administratifs, ainsi que du délai nécessaire pour se rendre compte qu'une violation de données a été subie. Dans le rapport Cost Of Data Breach (2018), ce délai est estimé en moyenne à 197 jours.

Le modèle a été appliqué sur la base de données concernant l'état de l'Indiana, en se penchant sur les années 2016-2017 pour se calibrer et ensuite prédire le nombre d'IBNR sur cette période.

3.5.1.2 Analyse et motivations

En analysant la base de données, quelques faits motivent l'utilisation de notre modèle de provisionnement avec des processus de Hawkes :

En observant la Figure 3.6, l'histogramme des délais met en évidence que plus de la moitié des délais dépassent 42 jours, quelques délais "extrêmes", supérieurs à 300 jours sont également présents. Ces délais longs, associés à des sinistres qui surviennent en fin de période d'observation, peuvent engendrer la présence d'IBNR sur cette même période.

Par ailleurs, la forme de l'histogramme des délais nous oriente vers la loi exponentielle, en restant conscient que la queue de distribution des délais est probablement plus lourde à cause des délais aux alentours de 300-400 jours.

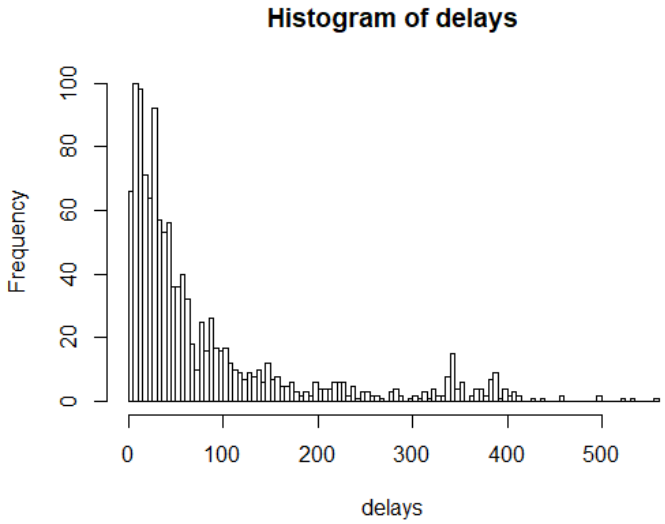


Figure 3.6 – Histogrammes des délais (base Indiana) sur la période 2016-2017

De la même façon, l'histogramme des temps d'occurrence rapportés (3.7) semble indiquer la présence d'IBNR, une chute des occurrences rapportées est en e□et observée sur les dates proches de la fin d'observation. Ceci peut être dû au fait que des sinistres sur cette période n'ont pas encore été déclarés.

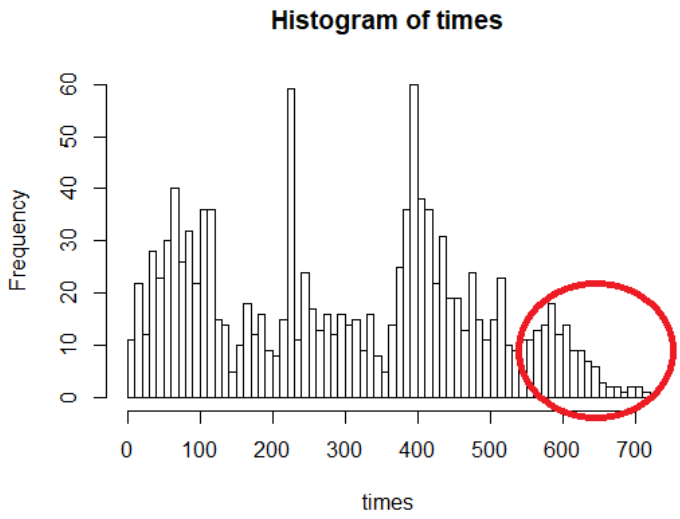


Figure 3.7 – Histogrammes des survenances (base Indiana) sur la période 2016-2017

Concernant l'utilisation de processus de Hawkes pour modéliser la fréquence, le tracé du nombre d'attaques survenues dans un mois en fonction du nombre d'attaques survenues dans le mois qui le précède, Figure 3.8, met en évidence un phénomène de forte autocorrélation, avec un coe□cient R^2 de 0.84. Ceci est une première motivation pour l'utilisation des processus de Hawkes.

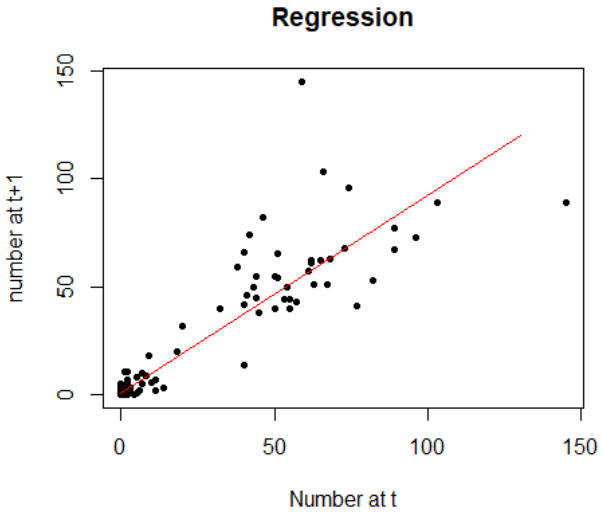


Figure 3.8 – Tracé du nombre d'attaques dans un mois t + 1 en fonction du nombre d'attaques du mois précédent t

3.5.2 Adéquation des modèles

Pour tester et comparer visuellement l'adéquation des modèles nous pouvons utiliser la propriété que nous avons utilisée précédemment, à savoir : Si un processus ponctuel a pour intensité conditionnelle $\lambda(t)$ alors en transformant ses temps t_i d'occurrences en τ_i avec :

$$\tau_i = \int_0^{t_i} \lambda(t)\mathrm{d}t$$

la suite $(\tau_i)_{i\ 1}$ est une réalisation d'un processus de Poisson homogène de paramètre 1.

Il est alors possible de vérifier graphiquement si certaines données sont aberrantes étant donné le modèle en traçant le nombre cumulé d'évènements en fonction de la suite $(\tau_i)_{i\ 1}$ ainsi que les intervalles de confiance à 95% de ces valeurs.

Ces graphiques présents en Figures 3.9 et 3.10 indiquent que les données sont plus vraisemblables sous le modèle individuel Hawkes que le classique modèle individuel Poisson.

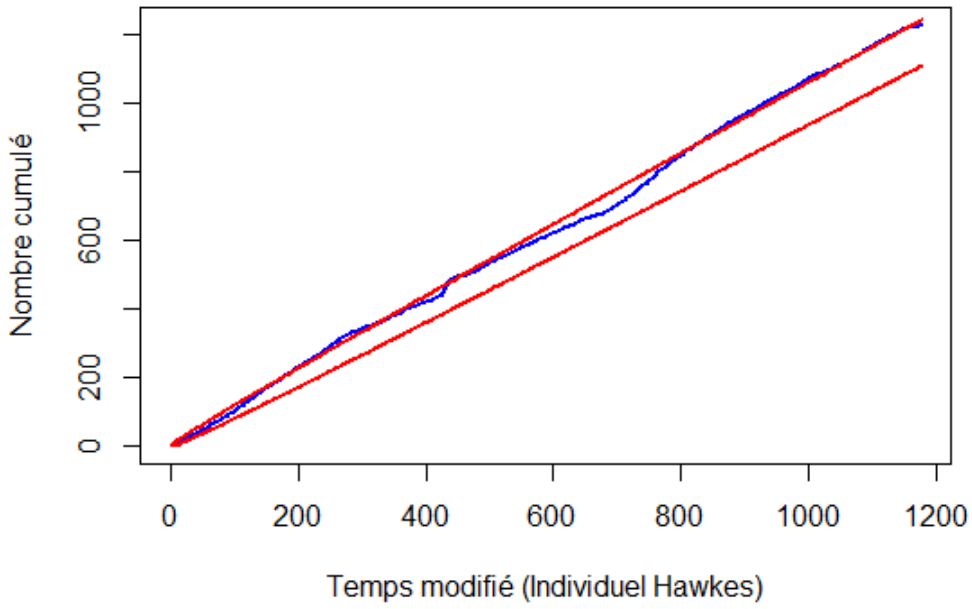


Figure 3.9 – Tracé du processus de comptage en fonction des temps modifiés - Hawkes

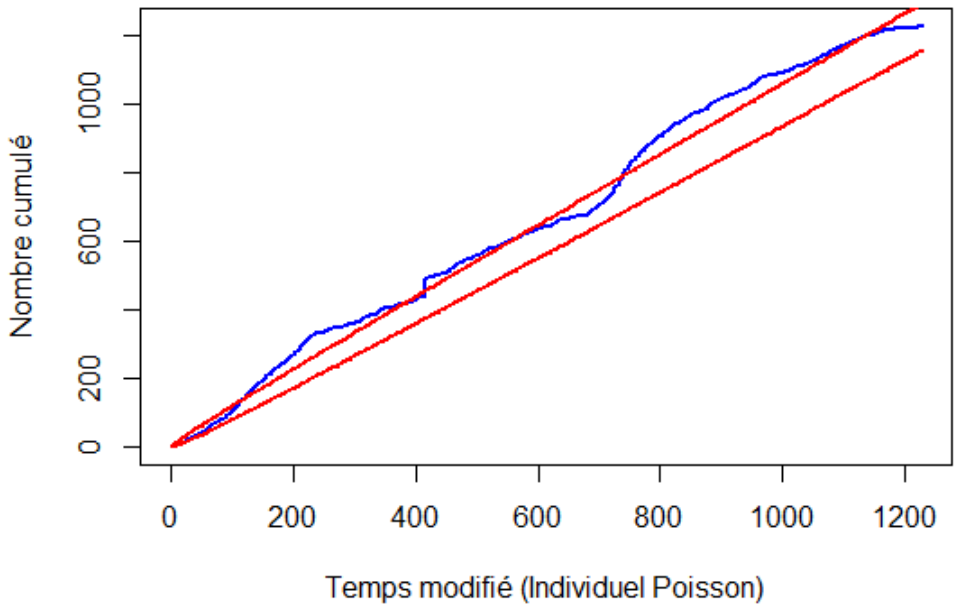


Figure 3.10 – Tracé du processus de comptage en fonction des temps modifiés - Poisson

Une méthode plus statistique consiste à e□ectuer un test de Kolmogorov-Smirnov sur les temps d'attentes entre deux occurrences (supposés suivre une loi exponentielle de paramètre 1 après transformation du temps). Ce test, présent en Table 3.3 indique que seul le modèle de Hawkes est accepté (à 5%).

	Modèle individuel Hawkes	Modèle individuel Poisson
P-Value	0.397	8.47e-14

Table 3.3 – Test de Kolmogorov-Smirnov

3.5.3 Prédictions

L'histogramme des délais permet de constater que les sinistres sont déclarés en grande partie avant 400 jours. Donc les IBNR de la période 2016-2017 devraient être en majorité déclarés lors de 2018-2019. En se basant sur les données disponibles (2018 et une partie de 2019), voici les nombres d'IBNR prédits par le modèle individuel Hawkes, le modèle individuel Poisson, ainsi que le modèle aggrégé, de Mack :

	Individuel Hawkes	Individuel Poisson	Mack	Réel
Nombre IBNR prédit	180	143	183	199

Table 3.4 – Prédictions 1

La prédiction avec le modèle individuel Hawkes correspond à $\mathsf{E}\left[N^{IBNR}\right]$ qui, sous ces hypothèses, se calcule comme suit :

$$
\begin{aligned}
&\mathsf{E}\left[N^{IBNR}\right] \\
=&\mathsf{E}\left[\int_0 \int_0^1 \int_0^1 \mathbf{1}_{\quad (v) p_{Ujv}(u) \mathbf{1}_{v+u>}} \; M(\mathrm{d}v, \mathrm{d}u, \mathrm{d}\theta)\right] \\
=&\mathsf{E}\left[\int_0 \int_0^1 \int_0^1 \mathbf{1}_{\quad (v) p_{Ujv}(u) \mathbf{1}_{v+u>}} \; \mathrm{d}v\mathrm{d}u\mathrm{d}\theta\right] \\
=&\mathsf{E}\left[\int_0 \lambda(v) p_{Ujv}(\tau \quad v, 1)\mathrm{d}v\right] \\
=&\int_0 \mathsf{E}\left[\lambda(v)\right] \exp(\quad \theta \quad (\tau \quad v))\mathrm{d}v \\
=&\frac{\mu}{1 \quad -} \quad \frac{1}{\theta}(1 \quad \exp(\quad \theta\tau))
\end{aligned}
$$

Nous pouvons également simuler des réalisations du nombre d'IBNR pour ces modèles et ainsi comparer leur variance (l'erreur de processus). Pour le modèle individuel Hawkes deux méthodes sont possibles, la première consiste à utiliser l'algorithme de simulation d'IBNR évoqué précédemment, cela permet de tenir compte des temps observés mais c'est une méthode approchée (ci-dessous Hawkes 1). La seconde consiste à simuler des nouvelles trajectoires du processus avec les paramètres estimés et à compter le nombre d'IBNR (ci-dessous Hawkes 2).

Pour le modèle Poissonnien, il est possible de reprendre l'approche précédente, et de déterminer l'intensité du processus d'IBNR qui n'est autre que $\lambda_{Pois}^{IBNR} = \lambda_{Pois} p_{ujt}(\tau \; t, 1)$ avec λ_{Pois} l'intensité du processus de Poisson qui génère les survenances. Nous avons considéré une intensité constante par morceau à l'échelle annuelle.

Le modèle de Mack, quant à lui, a été appliqué avec la fonction MackChainLadder, les simulations n'ont tenu compte que de la variance process (et non de l'erreur d'estimation) afin de comparer les modèles.

En Table 3.5, les résultats basés sur 10 000 simulations.

	Moyenne		Erreur process	Quantile 99.5%	Réel
IBNR individuel (Hawkes 1)	160.3	0.33	17.02	208	199
IBNR individuel (Hawkes 2)	179.91	0.41	20.71	239	199
IBNR individuel Poisson	138.03	0.23	11.68	169	199
Mack	182.76	1.33	67.79	361.98	199

Table 3.5 – Prédiction basées sur 10000 simulations

Les histogrammes de prédictions sont en Figure 3.11.

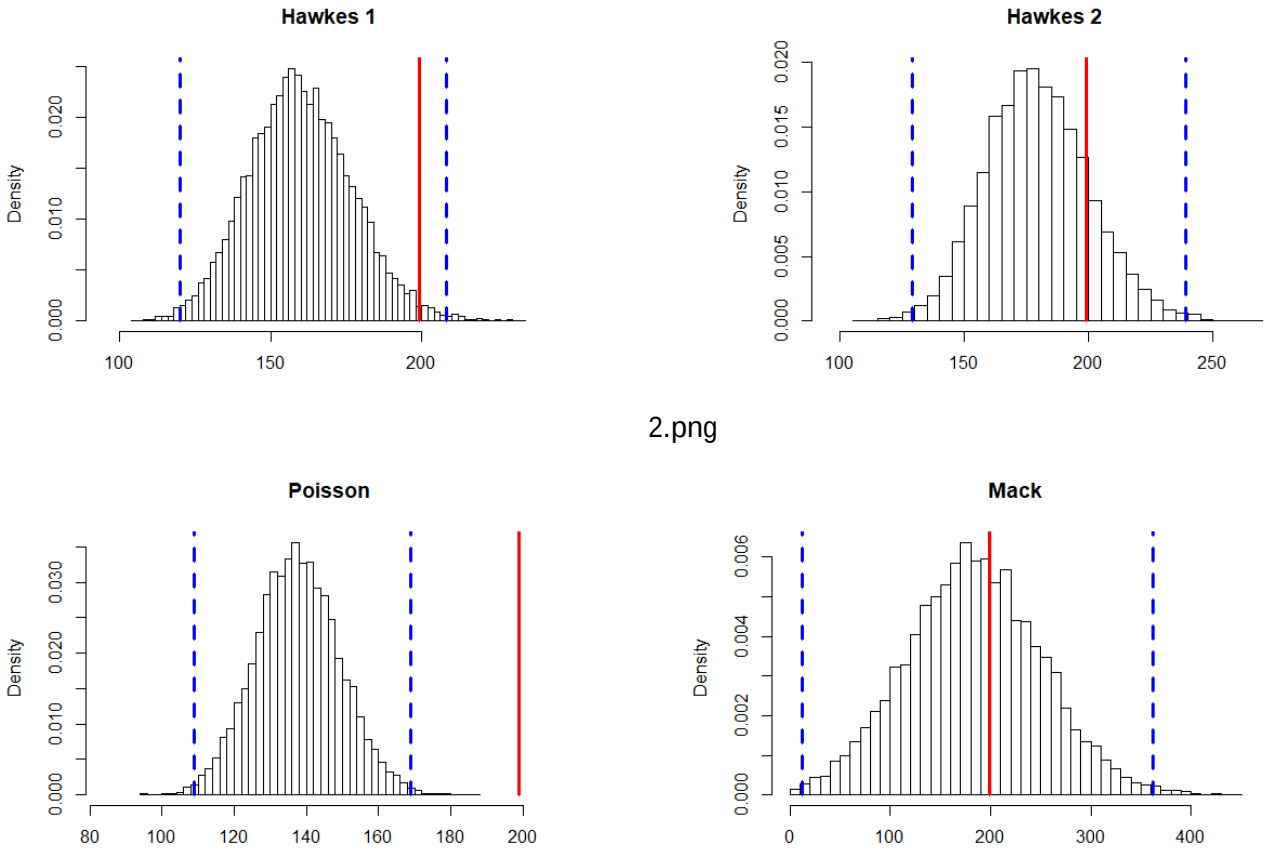


Figure 3.11 – Distribution du nombre d'IBNR prédit - En rouge le nombre réel, en bleu les quantiles à 0.5% et 99.5% de la distribution prédite

Sur cet exemple, les modèles individuels ont une variance plus faible, et permettent donc une prédiction plus précise, c'est leur principal apport par rapport au modèle de Mack, qui fournit une distribution avec une grande variance.

Le modèle de Hawkes apparaît être un bon compromis entre les deux autres modèles, il présente en e□et une faible variance (comme le modèle de Poisson), et contient le réel dans sa distribution (comme le modèle de MACK).

Conclusion

Ce mémoire met en évidence la pertinence des processus de Hawkes comme outil de modélisation de la fréquence des violations de données, et ce, à travers ses capacités interprétatives et prédictives. Ce type de processus permet de prendre en compte des effets de contagion qui sont engendrés par les similitudes logicielles et l'interconnexion des systèmes informatiques entre les entreprises. Ces effets sont traduits de façon naturelle à travers ses paramètres, ce qui en fait, au-delà d'un outil de modélisation, un outil d'analyse du risque.

La méthode de tarification proposée dans ce mémoire permet de prendre en compte l'environnement global de risque entre les entreprises, grâce aux processus de Hawkes. Elle permet également de tenir compte de l'impact du secteur d'activité sur le risque, à travers sa fréquence mais également sa sévérité. Cependant, outre la prise en compte du secteur d'activité, la méthode ne considère pas de facteurs intrinsèques à l'entreprise assurée. Inclure des tels facteurs, comme le chiffre d'affaire (qui est pris en considération dans les primes observables sur le marché), le nombre d'employés, ou encore le nombre d'ordinateurs de l'entreprise, pourrait faire l'objet de futures recherches.

La méthode de provisionnement développée a pour objectif de pouvoir déterminer un nombre d'IBNR pour des sinistres atypiques, qui nécessitent une modélisation par les processus de Hawkes, ces derniers étant une généralisation du processus de Poisson, la méthode concerne également les sinistres plus classiques. Les différents tests semblent montrer que la méthode fait sens malgré les approximations effectuées à divers niveaux. Des travaux futurs pourraient se pencher sur la justification, la maîtrise ou le contournement de ces approximations.

Dans un second temps la flexibilité du modèle peut être améliorée en l'adaptant à des noyaux autres que le classique exponentiel qui a été étudié ici, ainsi qu'en la généralisant au cas multivarié.

De façon générale, toutes les méthodes présentées dans ce mémoire ont l'avantage de pouvoir déterminer des distributions par simulation, cela permet d'obtenir de l'information sur le risque, qui est utile non seulement pour l'analyse, mais également pour le cadre réglementaire du modèle interne solvabilité II.

Le modèle de Hawkes présente toutefois plusieurs limites, la première réside dans le nombre de ses paramètres qui croît rapidement avec la dimension du processus, cela engendre des problématiques de complexité, de temps de calcul, de di□culté d'interprétation ainsi que d'erreur d'estimation.

Une seconde limite concerne sa sensibilité aux données, qui apparaît, comme tout modèle, dans les paramètres estimés, mais également à travers l'historique de données en lui-même qui influence le processus lors des prédictions, ceci est dû à la nature autorégressive de l'intensité.

Une dernière limite concerne l'aspect interdépendant du processus, bien qu'il permette de modéliser des phénomènes complexes de dépendance, cela implique également que la présence de segments mal calibrés influence tous les autres segments négativement.

Annexe A

Répartition de la PRC par états

	Var1	Freq
1	Alabama	70
2	Alaska	22
3	Arizona	129
4	Arkansas	52
5	Beijing	1
6	Berlin	1
7	British Columbia	3
8	Buckinghamshire	2
9	California	1117
10	Cheshire	1
11	Colorado	122
12	Connecticut	109
13	Delaware	16
14	District Of Columbia	104
15	Dublin	1
16	Florida	386
17	Georgia	207
18	Grand Bahama	1
19	Guangdong	1
20	Hawaii	19
21	Idaho	18
22	Illinois	291
23	Indiana	170
24	Iowa	56
25	Kansas	49
26	Kentucky	95
27	London	2
28	Louisiana	50
29	Maine	25
30	Maryland	331
31	Massachusetts	200
32	Michigan	122
33	Minnesota	133

	Var1	Freq
34	Mississippi	29
35	Missouri	131
36	Montana	25
37	Nebraska	33
38	Nevada	46
39	New Hampshire	30
40	New Jersey	123
41	New Mexico	42
42	New York	451
43	Noord Holland	1
44	North Carolina	146
45	North Dakota	10
46	Ohio	193
47	Oklahoma	54
48	Ontario	7
49	Oregon	101
50	Pennsylvania	217
51	Puerto Rico	31
52	Quebec	3
53	Rhode Island	31
54	South Carolina	61
55	South Dakota	11
56	Tennessee	130
57	Texas	489
58	Tokyo	1
59	UNKNSTATE	302
60	Utah	48
61	Vermont	27
62	Virginia	148
63	Washington	169
64	West Virginia	17
65	Wisconsin	84
66	Wyoming	12

Annexe B

Algorithmes de simulation

Ces algorithmes proviennent de [Chen, 2016], avec quelques modifications.

B.1 Algorithme de Lewis

Algorithm 1 Simulation of an inhomogeneous Poisson process with bounded intensity function $\lambda(t)$, on [0, T]

Require: $\lambda(.)$; T
  Initialize $n = m = 0, t_0 = s_0 = 0, \lambda = sup_{0 \ t \ T}\lambda(t)$;
  while $s_m < T$ do
    Generate u uniform(0,1) ;
    Let $w = ln(u)/\lambda$; {w suit une loi exponentielle de paramètre λ}
    Set $s_{m+1} = s_m + w$; {Les s_m sont les temps d'arrivée du processus de Poisson homogène }
    Generate D uniform(0,1) ;
    if $D \quad \lambda(s_{m+1})/\lambda$ then
      $t_{n+1} = s_{m+1}$;{Sélection du temps s_{m+1} avec probabilité $\lambda(s_{m+1})/\lambda$. Les t_n sont les temps d'arrivée du processus de Poisson inhomogène }
      $n = n + 1$;
    end if
    $m = m + 1$;
  end while
  if $t_n \quad T$ then
    return $\{t_k\}_{k=1,:::,n}$
  else
    return $\{t_k\}_{k=1,:::,n \ 1}$
  end if

B.2 Algorithme d'Ogata

Algorithm 2 Simulation of a Hawkes process on [0, T]

Require: $\mu(.)$; $\phi(.)$; T
  Initialize T = ;, s=0, n=0 ;
  while s T do
    Find a bound λ such as $\lambda(t)$ λ for s t T {Typiquement cette borne dépend du passé T, il faut donc la mettre à jour à chaque nouveau temps d'arrivée}
    Generate u uniform(0,1) ;
    Let w = $ln(u)/\lambda$; {w suit une loi exponentielle de paramètre λ}
    Set s = s + w ; {s est le prochain point potentiel du processus de Hawkes}
    Generate D uniform(0,1) ;
    if D $\lambda(s)/\lambda$ then
      n = n + 1 ;
      t_n = s ;{Sélection du temps s avec probabilité $\lambda(s)/\lambda$. Les t_n sont les temps d'arrivée du processus de Hawkes}
      T = T [$f t_n g$
    end if
    m = m + 1 ;
  end while
  if t_n T then
    return $f t_k g_{k=1;:::;n}$
  else
    return $f t_k g_{k=1;:::;n\ 1}$
  end if

Choix des bornes dans les cas utilisés : Le choix de la borne peut permettre d'accélérer l'algorithme, plus cette dernière est faible plus les temps simulés ont de chance d'être acceptés.

Supposons que k temps $t_1, ..., t_k$ sont survenus, l'intensité au temps $s > t_k$, pour le noyau exponentiel avec un *drift* linéaire comme taux de base est $\lambda(s) = \mu_0 + \gamma s + \sum_{i=1}^{k} \alpha \exp(\ \beta(s\ \ t_i))$

La borne λ choisie, pour ce temps s *2*$]t_k, t_{k+1}]$ peut être, la valeur de la somme au dernier temps de saut étant donné que cette partie est strictement décroissante, à laquelle est ajouté la valeur du *drift* à l'horizon T si ce dernier est positif. Si ce dernier est négatif prendre sa valeur au dernier temps t_k permet de réduire la valeur de la borne. Cela donne :

$$\lambda = \mu_0 + (\gamma T)1_{\ >0} + (\gamma t_k)1_{\ <0} + \sum_{i=1}^{k} \alpha \exp(\ \beta(t_k\ \ t_i))$$

Dans le cas d'un noyau de la forme $\phi(a) = \alpha a \exp(-\beta a)$, l'intensité a cette fois la forme : $\lambda(s) = \mu_0 + \gamma s + \sum_{i=1}^{k} \alpha(s - t_i)\exp(-\beta(s - t_i))$. Chaque terme i de la somme atteint sont maximum en $\frac{1}{\beta} + t_i$, qui vaut $-\exp(-1)$. Une façon d'optimiser la borne, au niveau de la somme, est de considérer la valeur maximum du noyau si celle-ci n'a pas été atteinte, et la valeur actuelle sinon (car le noyau est strictement décroissant passé la valeur maximale). Cela mène à une borne :

$$\lambda = \mu_0 + (\gamma T)1_{\gamma > 0} + (\gamma t_k)1_{\gamma < 0} + \sum_{i=1}^{k} \left[\frac{\alpha}{\beta} \exp(-1) 1_{fs < \frac{1}{\beta} + t_i g} + \alpha(s - t_i)\exp(-\beta(s - t_i)) 1_{fs > \frac{1}{\beta} + t_i g} \right]$$

B.3 Algorithme de simulation d'un processus de Hawkes multivarié

Algorithm 3 Simulation of a multivariate Hawkes process of dimension d, on [0, T]

Require: $(\mu_i(.))_{1 \leq i \leq d}$; $(\phi_{i,j}(.))_{1 \leq i,j \leq d}$; T
  Initialize $T^{(1)} = ... = T^{(d)} = \emptyset, s = 0, n_1 = ... = n_d = 0$;
  while $s < T$ **do**
    Find a bound λ such as $\sum_{i=1}^{d} \lambda^{(i)}(t) < \lambda$ for $s < t < T$; {Typiquement cette borne dépend du passé $\left[\bigcup_{i=1}^{d} T_i\right.$, il faut donc la mettre à jour à chaque nouveau temps d'arrivée}
    Generate $u \sim$ uniform(0,1) ;
    Let $w = -\ln(u)/\lambda$; {w suit une loi exponentielle de paramètre λ}
    Set $s = s + w$; {s est le prochain point potentiel du processus de Hawkes}
    Generate $D \sim$ uniform(0,1) ;
    if $D \leq \sum_{i=1}^{d} \lambda^{(i)}(s)/\lambda$ **then**
      $k = 1$;
      while $D\lambda > \sum_{i=1}^{d} \lambda^{(i)}(s)$ **do**
        $k = k + 1$;
      end while
      $n_k = n_k + 1$;
      $t_{n_k}^{(k)} = s$;
      $T^{(k)} = T^{(k)} \cup \{t_{n_k}^{(k)}\}$;
    end if
  end while
  if $t_{n_k}^{(k)} < T$ **then**
    return $T^{(i)}, i = 1, ..., d$;
  else
    return $T^{(1)}, ..., T^{(k)} \setminus \{t_{n_k}^{(k)}\}, ..., T^{(d)}$;
  end if

Choix des bornes dans les cas utilisés :

Supposons que pour 1 i d, k_i temps $\left(t_n^{(i)}\right)_{n=1}^{k_i}$ ont été simulés. L'intensité du processus $(N_t^{(i)})_{t\ 0}$, 1 i d dans le cas exponentiel est de la forme

$$\lambda^{(i)}(s) = \mu_{i;0} + \gamma_i s + \sum_{j=1}^{d}\sum_{k=1}^{k_j} \alpha_{i;j} \exp(\ \beta_{i;j}(s\ \ t_k^{(j)}))$$

pour s plus grand que le dernier temps simulé. Avec les mêmes arguments que pour le cas monovarié (voir ci-dessus), une borne possible, de l'intensité totale, pour ce temps s est :

$$\lambda = \sum_{i=1}^{d}\left[\mu_{i;0} + (\gamma_i T)1_{\ i>0} + (\gamma_i t\ )1_{\ i<0} + \sum_{j=1}^{d}\sum_{k=1}^{k_j} \alpha_{i;j} \exp(\ \beta_{i;j}(t\ \ t_k^{(j)}))\right]$$

avec comme notation t le dernier temps simulé.

Dans le cas du second noyau : $\phi_{i;j}(a) = \alpha_{i;j} a \exp(\ \beta_{i;j} a)$, une borne possible est la suivante :

$$\lambda = \sum_{i=1}^{d}\left[\mu_0^{(i)} + (\gamma_i T)1_{\ i>0} + (\gamma_i t\ )1_{\ i<0}\right.$$
$$\left. + \sum_{j=1}^{d}\sum_{k=1}^{k_j}\left[\frac{\alpha_{i;j}}{\beta_{i;j}} \exp(\ 1)1_{fs<\frac{1}{\beta_{i,j}}+t_k^{(j)}g} + \alpha_{i;j}(s\ \ t_k^{(j)}) \exp(\ \beta_{i;j}(s\ \ t_k^{(j)}))1_{fs>\frac{1}{\beta_{i,j}}+t_k^{(j)}g}\right]\right]$$

Annexe C

Détermination de la fonction de vraisemblance d'un processus ponctuel

Le processus ponctuel en une dimension peut être considéré comme une suite de temps d'arrivée ordonnés : $t_1, ..., t_k ...$. Notons $f(t \mid F_{t_{n-1}})$, la densité conditionnelle du n-ème temps d'arrivée connaissant les temps passés du processus et $F(t \mid F_{t_{n-1}})$ la fonction de répartition associée. Ceci s'interprète comme : la probabilité que le n-ème temps d'arrivée survienne entre t et $t + dt$, connaissant les $n-1$ temps passés est : $f(t \mid F_{t_{n-1}})dt$

Alors la fonction d'intensité conditionnelle définie en 2.3.1.2 se réécrit comme étant :

$$\lambda(t) = \frac{f(t \mid F_{t_n})}{1 - F(t \mid F_{t_n})}, t_n < t \leq t_{n+1}$$

en effet nous avons, pour $t_n < t \leq t_{n+1}$:

$$\begin{aligned}
\frac{f(t \mid F_{t_n})}{1 - F(t \mid F_{t_n})} dt &= \frac{P(t_{n+1} \in [t, t + dt] \mid F_{t_n})}{P(t_{n+1} > t \mid F_{t_n})} \\
&= \frac{P(t_{n+1} \in [t, t + dt], t_{n+1} > t \mid F_{t_n})}{P(t_{n+1} > t \mid F_{t_n})} \\
&= P(t_{n+1} \in [t, t + dt] \mid t_{n+1} > t, F_{t_n}) \\
&= P(t_{n+1} \in [t, t + dt] \mid F_t) \\
&= P(N(t + dt) - N(t) > 0 \mid F_t)
\end{aligned}$$

Nous retrouvons bien l'intensité telle qu'elle a été définie en 2.3.1.2.

En remarquant que

$$\lambda(t) = \frac{f(t \mid F_{t_n})}{1 - F(t \mid F_{t_n})} = -\frac{d}{dt} \log(1 - F(t \mid F_{t_n}))$$

nous avons aisément la relation :

$$f(t \mid F_{t_n}) = \lambda(t) \exp\left(\int_{t_n}^{t} \lambda(s) \mathrm{d}s \right)$$

Nous sommes maintenant en mesure d'écrire la vraisemblance en fonction de l'intensité du processus.

En prenant comme notation $H_n = \{T_n = t_n, ..., T_1 = t_1\}$ avec les conventions $H_0 = ;$ et $T_0 = 0$. Supposons que nous avons observé les m temps $(t_n)_{1 \quad n \quad m}$ sur l'intervalle d'observation $[0, t]$, la fonction de vraisemblance s'écrit comme suit :

$$\begin{aligned}
L(\mu, \phi) &= \mathrm{P}(\text{81} \quad n \quad m, T_n = t_n, \text{ and } T_{m+1} > t) \\
&= \mathrm{P}(T_{m+1} > t \mid H_m) \prod_{n=1}^{m} \mathrm{P}(T_n = t_n \mid H_{n \ 1}) \\
&/ (1 \quad F(\tau \mid H_m)) \prod_{n=1}^{m} f(t_n \mid H_{n \ 1}) \\
&= \exp\left(\int_{T_m}^{t} \lambda(s) \mathrm{d}s \right) \prod_{n=1}^{m} \exp\left(\int_{T_{n \ 1}}^{T_n} \lambda(s) \mathrm{d}s \right) \lambda(T_n) \\
&= \exp\left(\int_{0}^{t} \lambda(s) \mathrm{d}s \right) \prod_{n=1}^{m} \lambda(T_n)
\end{aligned}$$

La log vraisemblance a donc la forme :

$$\log L(\mu, \phi) = \int_0^t \lambda(s) \mathrm{d}s + \sum_{n=1}^{m} \log \lambda(T_n) = \int_0^t \lambda(s) \mathrm{d}s + \int_0^t \log \lambda(s) \mathrm{d}N_s \qquad \text{(C.1)}$$

Annexe D

Prédictions 2016-2017 - Noyau 3

D.1 Noyau 3 - Prédictions 2016

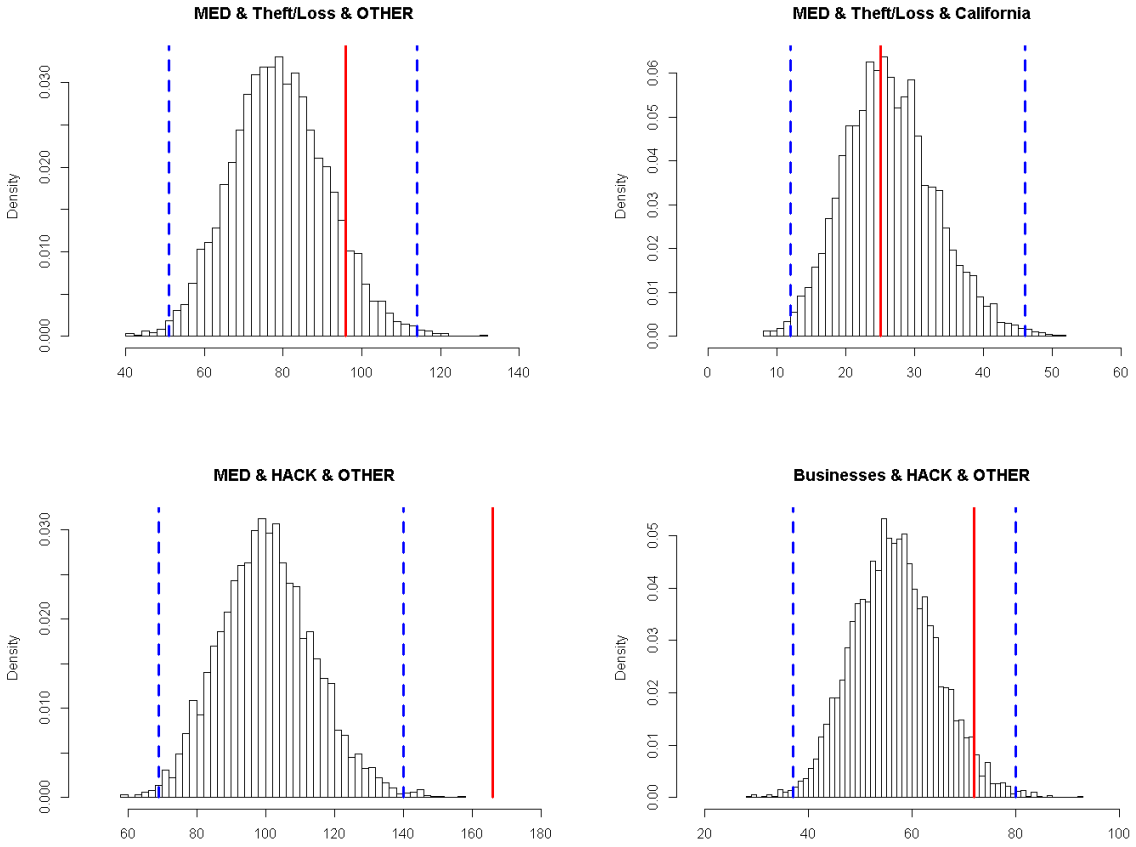


Figure D.1 – Distribution du nombre d'attaques prédit pour 2016 avec le noyau 3, partie 1 - En rouge le nombre réel, en bleu les quantiles à 0.5% et 99.5% de la distribution prédite

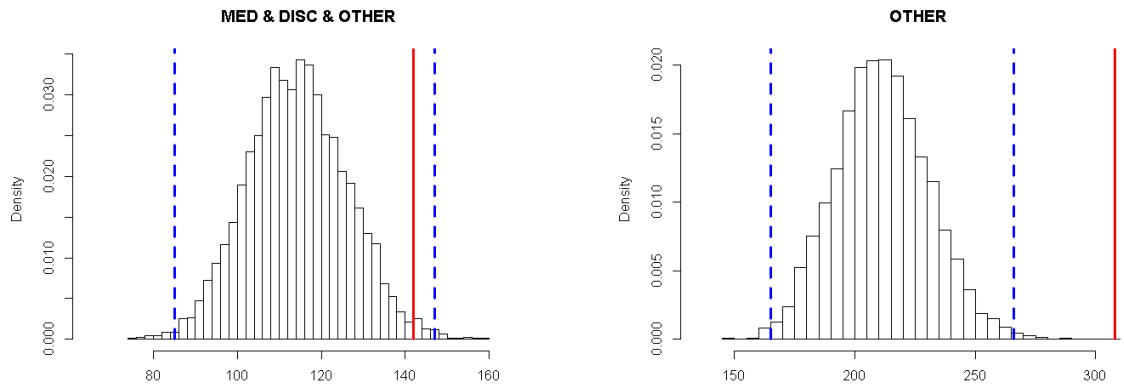


Figure D.2 – Distribution du nombre d'attaques prédit pour 2016 avec le noyau 3, partie 2 - En rouge le nombre réel, en bleu les quantiles à 0.5% et 99.5% de la distribution prédite

D.2 Noyau 3 - Prédictions 2017

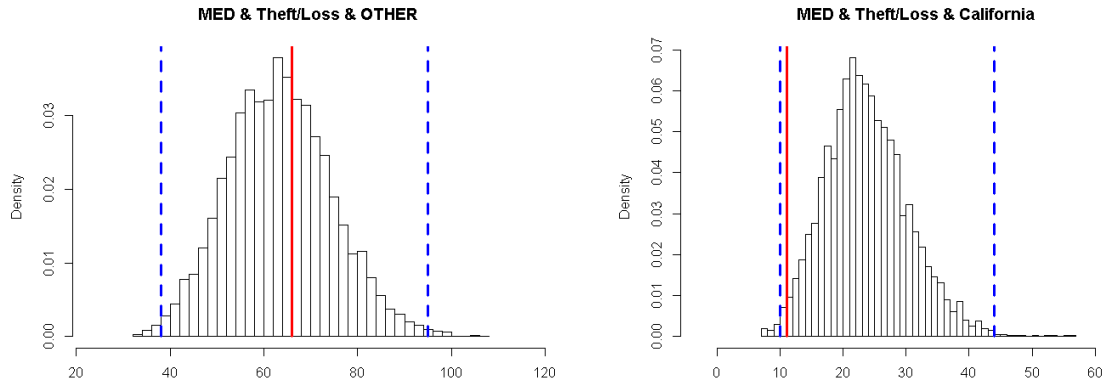


Figure D.3 – Distribution du nombre d'attaques prédit pour 2017 avec le noyau 3, partie 1 - En rouge le nombre réel, en bleu les quantiles à 0.5% et 99.5% de la distribution prédite

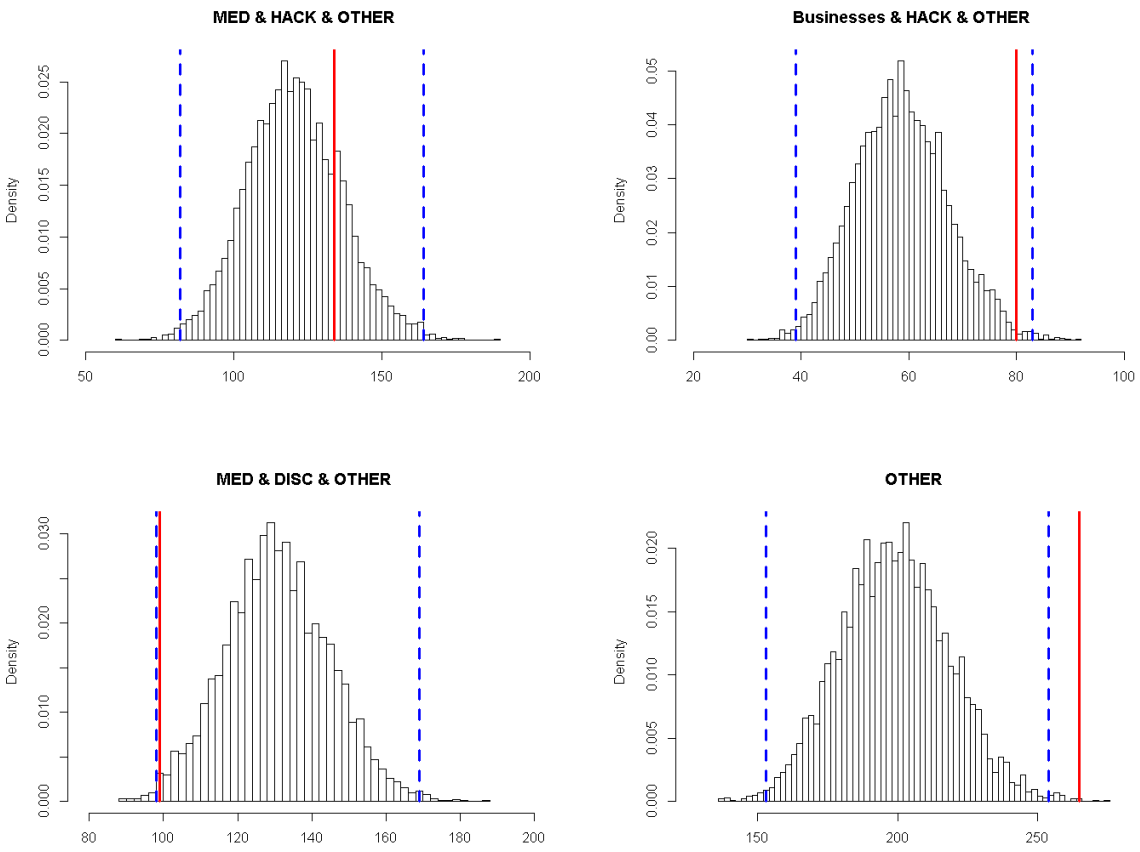


Figure D.4 – Distribution du nombre d'attaques prédit pour 2017 avec le noyau 3, partie 2 - En rouge le nombre réel, en bleu les quantiles à 0.5% et 99.5% de la distribution prédite

Annexe E

Paramètres du modèle 3

	$\mu_{0;i}$
OTHER (1)	0.8694
MED & DISC & OTHER (2)	0.0219
BUSINESSES & HACK & OTHER (3)	0.1223
MED & HACK & OTHER (4)	0.0155
MED & THEFT/LOSS & California (5)	0.0515
MED & THEFT/LOSS & OTHER (6)	0.3553

Table E.1 – Paramètres $(\mu_{0;i})_{1 \quad i \quad 6}$

	1	2	3	4	5	6
1	6.0445	6.0646	4.3587	3.5119	2.5362	2.9487
2	1.4800	6.2759	1.8240	4.7028	3.3100	0.8286
3	1.4471	1.3396	3.1669	1.8420	0.1381	1.1503
4	0.3068	2.8264	1.7419	8.3681	0.3196	0.1188
5	0.3763	0.6154	0.1183	1.1883	7.7952	0.9884
6	2.0294	2.5738	3.1540	1.6299	0.8316	6.7016

Table E.2 – Paramètres $(\alpha_{i;j})_{1 \quad i;j \quad 6}$ - La numérotation correspond aux segments présents dans les autres tableaux (1 = OTHER etc..)

	1	2	3	4	5	6
1	0.4122	0.4136	0.2973	0.2395	0.1730	0.2011
2	0.0791	0.3356	0.0975	0.2515	0.1770	0.0443
3	0.0728	0.0674	0.1593	0.0927	0.0069	0.0579
4	0.0196	0.1807	0.1114	0.5350	0.0204	0.0076
5	0.0232	0.0380	0.0073	0.0733	0.4810	0.0610
6	0.1278	0.1621	0.1987	0.1027	0.0524	0.4221

Table E.3 – Excitations maximales ($_{i;j})_{1 \ i;j \ 6}$ - La numérotation correspond aux segments présents dans les autres tableaux (1 = OTHER etc..)

	β_i
OTHER (1)	5.3941
MED & DISC & OTHER (2)	6.8793
BUSINESSES & HACK & OTHER (3)	7.3128
MED & HACK & OTHER (4)	5.7540
MED & THEFT/LOSS & California (5)	5.9617
MED & THEFT/LOSS & OTHER (6)	5.8402

Table E.4 – Paramètres $(\beta_i)_{1 \ i \ 6}$

	γ_i
OTHER	-2.53e-04
MED & DISC & OTHER &	9.52e-05
BUSINESSES & HACK & OTHER &	-3.56e-06
MED & HACK & OTHER &	9.65e-05
MED & THEFT/LOSS & California &	-7.26e-06
MED & THEFT/LOSS & OTHER &	-1.07e-04

Table E.5 – Paramètres $(\gamma_i)_{1 \ i \ 6}$

Annexe F

Segmentation

F.1 Étude des distributions des inter-temps

	Moyenne	Ecart-type	Skew
BUSINESSES & DISC	14.1050	16.3621	1.8407
BUSINESSES & HACK	3.3810	4.1278	2.7547
BUSINESSES & OTHER	11.6774	20.5858	3.7815
BUSINESSES & THEFT/LOSS	9.6513	12.0743	2.3812
MED & DISC	3.5954	6.0065	5.8813
MED & HACK	4.1514	8.6028	4.6682
MED & OTHER	11.5596	20.2263	5.4667
MED & THEFT/LOSS	1.5512	2.1461	2.2757
OTHERORGA & DISC	11.2589	16.0717	3.8566
OTHERORGA & HACK	9.2555	11.8785	2.4315
OTHERORGA & OTHER	32.2179	55.6419	3.9560
OTHERORGA & THEFT/LOSS	12.4244	22.1758	3.9117

Table F.1 – Caractéristiques des inter-temps par croisement Organisation/Type d'attaque

F.2 Segmentations étudiées

Groupe	Nombre d'attaques (2011-2016)
MED	2803
BUSINESSES	1196
OTHERORGA	598

Table F.2 – Segmentation 1 - Par organisation

Groupe	Nombre d'attaques (2011-2016)
DISC	997
HACK	1528
OTHER	399
THEFT/LOSS	1673

Table F.3 – Segmentation 2 - par Type d'attaques

Groupe	Nombre d'attaques (2011-2016)
BUSINESSES & HACK MED & DISC MED & HACK MED & THEFT/LOSS	3313
BUSINESSES & DISC BUSINESSES & THEFT/LOSS MED &OTHER OTHERORGA & DISC OTHERORGA & HACK	943
BUSINESSES & OTHER OTHERORGA & OTHER OTHERORGA & THEFT/LOSS	341

Table F.4 – Segmentation 3 - obtenue via un regroupement K-means

Groupe	Nombre d'attaques (2011-2016)
BUSINESSES & HACK	699
MED & DISC MED & HACK MED & THEFT/LOSS MED &OTHER	2803
BUSINESSES & DISC BUSINESSES & THEFT/LOSS BUSINESSES & OTHER	497
OTHERORGA & DISC OTHERORGA & HACK	418
OTHERORGA & OTHER OTHERORGA & THEFT/LOSS	180

Table F.5 – Segmentation 4

Annexe G

Distributions discrètes

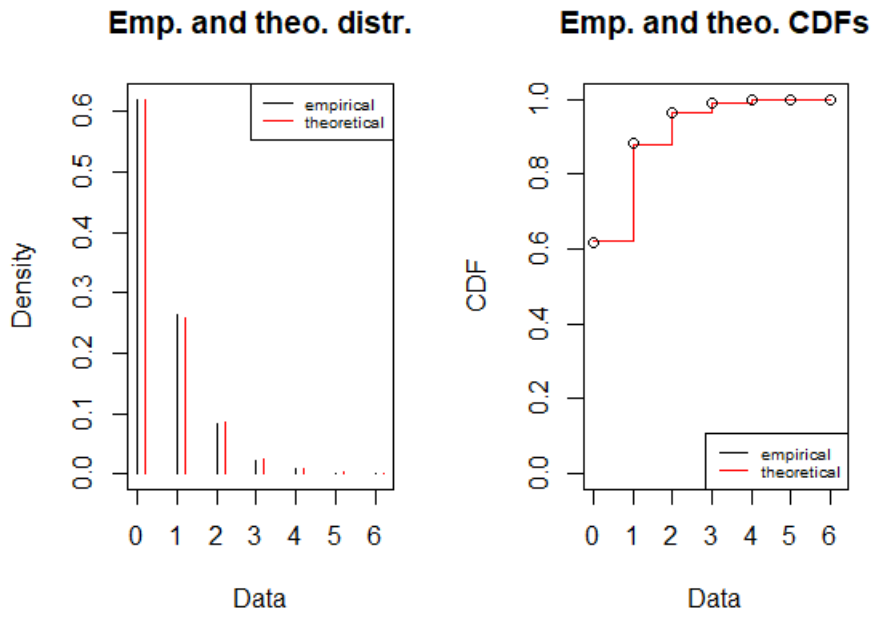


Figure G.1 – Distribution du nombre journalier d'attaques pour le type d'organisation BUSINESSES sur 2011-2015 - comparaison avec la loi binomiale négative

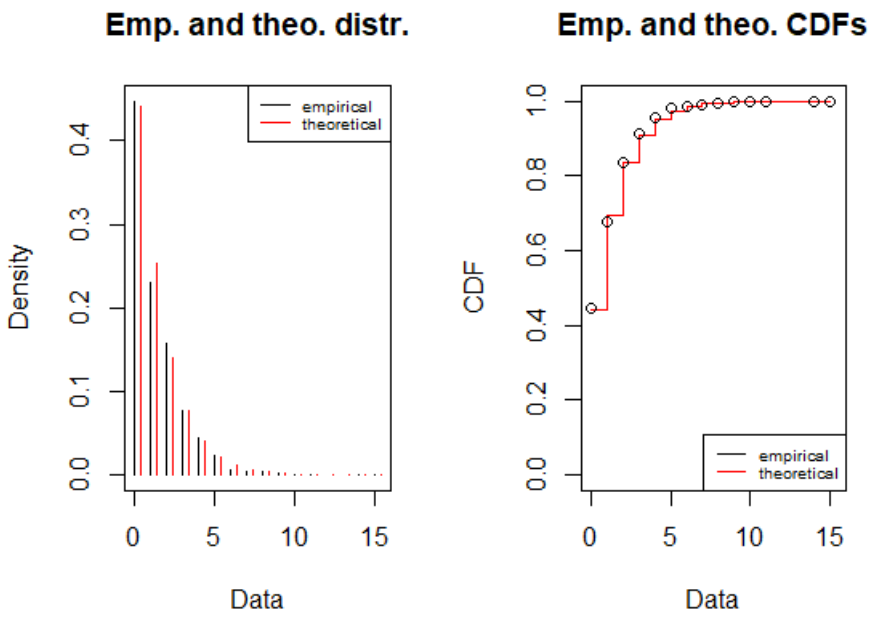


Figure G.2 – Distribution du nombre journalier d'attaques pour le type d'organisation MED sur 2011-2015 - comparaison avec la loi binomiale négative

Annexe H

Prédictions 2017

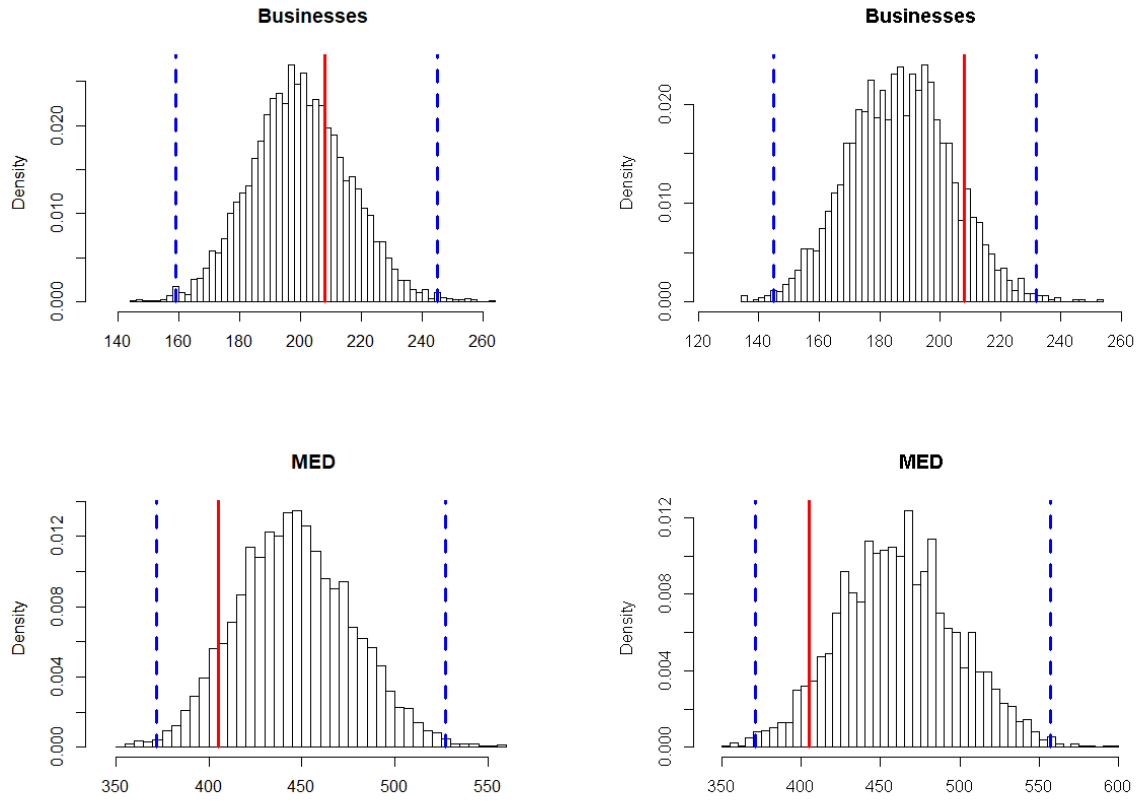


Figure H.1 – Distribution du nombre d'attaques prédit pour 2017 avec le modèle Hawkes à droite et les distributions discrètes à gauche, partie 1 - En rouge le nombre réel, en bleu les quantiles à 0.5% et 99.5% de la distribution prédite.

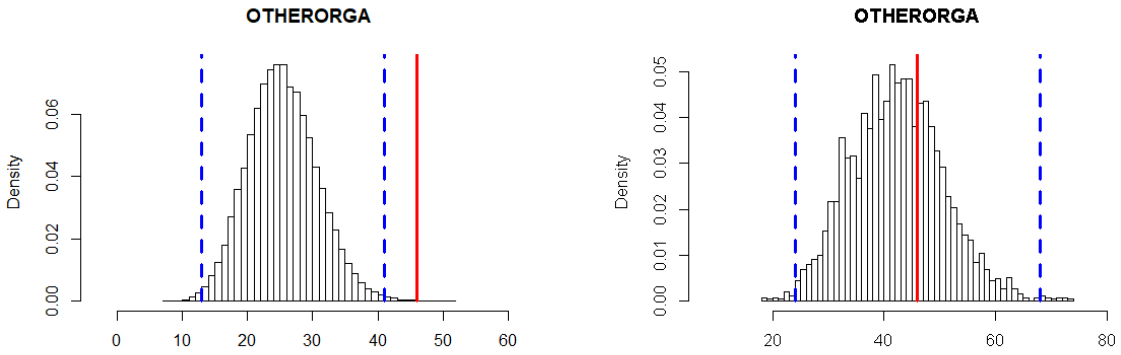


Figure H.2 – Distribution du nombre d'attaques prédit pour 2017 avec le modèle Hawkes à droite et les distributions discrètes à gauche, partie 2 - En rouge le nombre réel, en bleu les quantiles à 0.5% et 99.5% de la distribution prédite.

Annexe I

Distributions du nombre de données volées

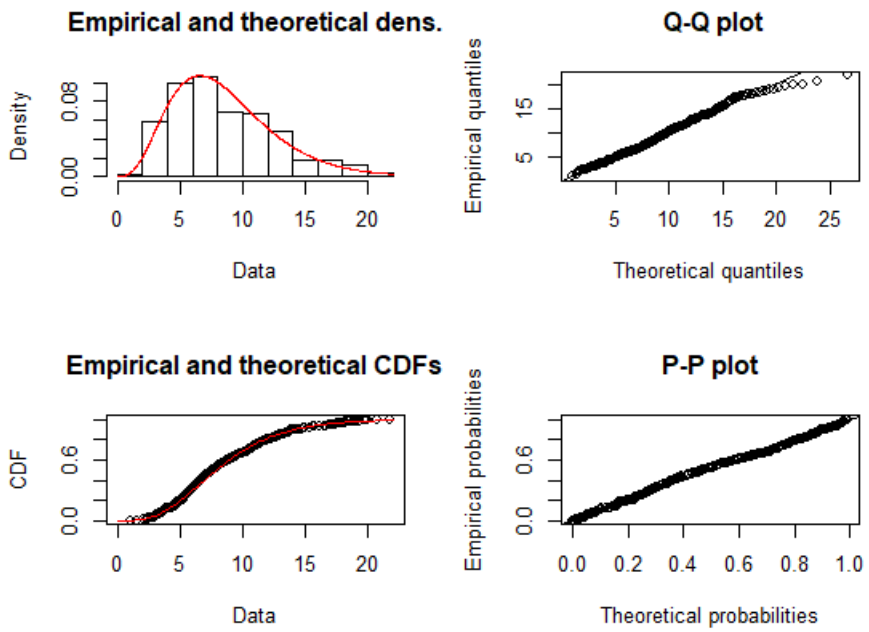


Figure I.1 – Adéquation du log(Nb données violées) avec la loi gamma - secteur BUSINESSES

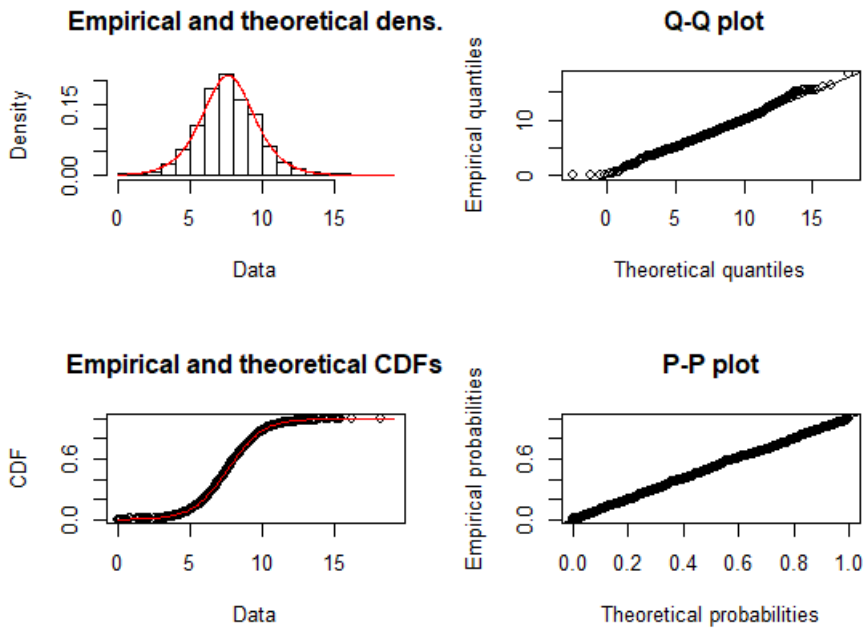


Figure I.2 – Adéquation du log(Nb données violées) avec la loi logistique - secteur MED

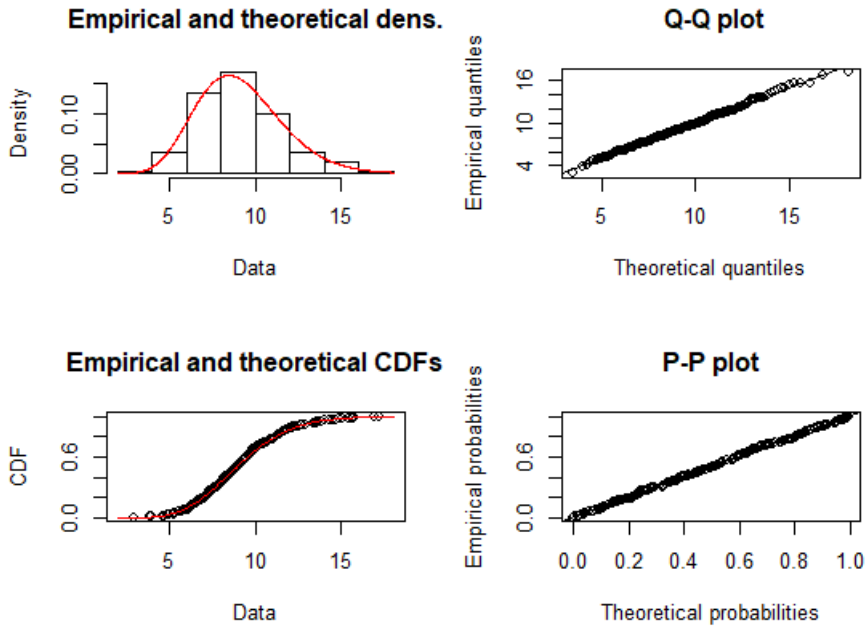


Figure I.3 – Adéquation du log(Nb données violées) avec la loi gamma - secteur OTHE-RORGA

Annexe J

Primes d'assurance violation de données

Activité	Segment	Revenus	Limite	Prime
Fournisseur dans l'énergie solaire	BUSINESSES	130K	2M	1 250
Installations de thermostat	BUSINESSES	50M	5M	8 025
Intégrateur de solutions IT	BUSINESSES	200M	5M	41 500
Conseil en stockage de données	BUSINESSES	1.5M	2M	3 643
Conseil en santé (IT)	MED	150K	1M	3298
Pharmacie en ligne	MED	8M	1M	3 598
Clinique de soins	MED	400K	1M	1 202
Fournisseur Saas en santé	MED	2M	2M	9 398
Société de gestion (pharmacie)	MED	4Md	5M	84 000

Table J.1 – Exemples de primes d'assurance violation de données - les montants sont exprimés en dollars ($)

Annexe K

Détail de calcul

Cette Annexe détaille l'égalité suivante :

$$\mathsf{E}_{n\ 1}\Big[\int_{t_n^R\ 1}^{s}\phi(s\quad v)\mathrm{d}N_v^{IBNR}\Big] = \mathsf{E}_{n\ 1}\Big[\int_{t_n^R\ 1}^{s}\phi(s\quad v)\lambda^{IBNR}(v)\mathrm{d}v\Big] \qquad \text{(K.1)}$$

Cas de l'espérance simple

Cette dernière serait plus évidente dans le cas d'une espérance simple, partant de :

$$N^{IBNR}(\mathrm{d}v,\mathrm{d}u) = N(\mathrm{d}v,\mathrm{d}u)1_{v+u>} = \int_0^1 1_{\quad (v)p_{Ujv}(u)1_{v+u>}}\ M(\mathrm{d}v,\mathrm{d}u,\mathrm{d}\theta)$$

nous avons donc :

$$\mathrm{d}N_v^{IBNR} = \int_0^1\int_0^1 1_{\quad (v)p_{Ujv}(u)1_{v+u>}}\ M(\mathrm{d}v,\mathrm{d}u,\mathrm{d}\theta)$$

Ce qui nous permet d'écrire

$$\int_{t_n^R\ 1}^{s}\phi(s\quad v)\mathrm{d}N_v^{IBNR} = \int_{t_n^R\ 1}^{s}\int_0^1\int_0^1\phi(s\quad v)1_{\quad (v)p_{Ujv}(u)1_{v+u>}}\ M(\mathrm{d}v,\mathrm{d}u,\mathrm{d}\theta) \qquad \text{(K.2)}$$

Et par propriété de la mesure de Poisson, comme la fonction sous l'intégrale est prévisible par rapport à M, nous avons que :

$$\int_0^t\int_0^1\int_0^1\phi(s\quad v)1_{\quad (v)p_{Ujv}(u)1_{v+u>}}\ M(\mathrm{d}v,\mathrm{d}u,\mathrm{d}\theta)$$

$$\int_0^t\int_0^1\int_0^1\phi(s\quad v)1_{\quad (v)p_{Ujv}(u)1_{v+u>}}\ m(\mathrm{d}v,\mathrm{d}u,\mathrm{d}\theta)$$

est une martingale, d'espérance nulle, ce qui nous permet de conclure, en notant :

$$I_{a;b} = \int_a^b\int_0^1\int_0^1\phi(s\quad v)1_{\quad (v)p_{Ujv}(u)1_{v+u>}}\ M(\mathrm{d}v,\mathrm{d}u,\mathrm{d}\theta)$$

$$J_{a;b} = \int_a^b\int_0^1\int_0^1\phi(s\quad v)1_{\quad (v)p_{Ujv}(u)1_{v+u>}}\ m(\mathrm{d}v,\mathrm{d}u,\mathrm{d}\theta)$$

Nous avons :

$$\begin{aligned} &\mathrm{E}(I_{0;s} \quad J_{0;s}) = 0 \\ =&\mathrm{E}(I_{0;t_{n\ 1}^R} \quad J_{0;t_{n\ 1}^R} + I_{t_{n\ 1}^R;s} \quad J_{t_{n\ 1}^R;s}) \\ =&0 + \mathrm{E}(I_{t_{n\ 1}^R;s} \quad J_{t_{n\ 1}^R;s}) \end{aligned} \tag{K.3}$$

Ce qui correspond bien à l'égalité (K.1) sous une espérance simple.

Cas de l'espérance conditionnelle

Cependant dans le cas présent nous sommes sous une espérance conditionnelle. Le raisonnement est alors le suivant : En reprenant (K.2) nous obtenons ,

$$\begin{aligned} &\mathrm{E}_{n\ 1}\Big[\int_{t_{n\ 1}^R}^{s} \phi(s \quad v)\mathrm{d}N_v^{IBNR}\Big] \\ =&\mathrm{E}_{n\ 1}\Big[\int_{t_{n\ 1}^R}^{s}\int_0^1\int_0^1 \phi(s \quad v)1_{\quad (v)p_{Ujv}(u)1_{v+u>}} M(\mathrm{d}v,\mathrm{d}u,\mathrm{d}\theta)\Big] \end{aligned} \tag{K.4}$$

Rappelons que $\mathrm{E}_{n\ 1}[.] = \mathrm{E}[.\ j\ (T_k^R = t_k^R)_{k=1}^{n\ 1}]$.

(1) égalité des espérances conditionnelles : Nous allons montrer que :

$$\begin{aligned} &\mathrm{E}_{n\ 1}\Big[\int_{t_{n\ 1}^R}^{s}\int_0^1\int_0^1 \phi(s \quad v)1_{\quad (v)p_{Ujv}(u)}\mathbb{M}(\mathrm{d}v,\mathrm{d}u,\mathrm{d}\theta)\Big] \\ =&\mathrm{E}_{n\ 1}\Big[\int_{t_{n\ 1}^R}^{s}\int_0^1\int_0^1 \phi(s \quad v)1_{\quad (v)p_{Ujv}(u)}m(\mathrm{d}v,\mathrm{d}u,\mathrm{d}\theta)\Big] \end{aligned} \tag{K.5}$$

Soit une variable aléatoire Z, bornée et mesurable par rapport à la tribu engendrée par les $(T_k^R)_{k=1}^{n\ 1}$ notée $\sigma\big((T_k^R)_{k=1}^{n\ 1}\big)$. En posant :

$$\begin{aligned} X &= \int_A f(y)M(dy) \\ Y &= \mathrm{E}\Big[\int_A f(y)m(dy)j\,\sigma\big((T_k^R)_{k=1}^{n\ 1}\big)\Big] \end{aligned}$$

avec A de la forme $[0,t] \quad E, t\ 2\ \mathrm{R}^+$. M est la mesure aléatoire de Poisson d'intensité m définit sur $\mathrm{R}^+ \quad E$. Z et f sont $P(G_t) \quad E$ mesurables, avec $(G_t)_{t\ 0}$ la filtration canonique engendrée par M, $P(G_t)$ la tribu prévisible associée à G_t, et E une tribu sur

E. Nous allons montrer que $\mathsf{E}[XZ] = \mathsf{E}[YZ]$

$$
\begin{aligned}
&\mathsf{E}[YZ] \\
=&\mathsf{E}\left[Z \quad \mathsf{E}\Big[\int_A f(y)m(dy) | \sigma\big((T_k^R)_{k=1}^{n-1}\big)\Big]\right] \\
=&\mathsf{E}\left[\mathsf{E}\Big[Z \quad \int_A f(y)m(dy) | \sigma\big((T_k^R)_{k=1}^{n-1}\big)\Big]\right] \\
=&\mathsf{E}\Big[\int_A Z \quad f(y)m(dy)\Big] \\
=&\mathsf{E}\Big[Z \quad \int_A f(y)M(dy)\Big] \text{ car Z et f sont } \mathsf{P}(\mathsf{G}_t) \quad E \text{ mesurables} \\
=&\mathsf{E}\Big[Z \quad X\Big]
\end{aligned}
$$

Comme Y est $\sigma\big((T_k^R)_{k=1}^{n-1}\big)$ mesurable cela prouve que :

$$\mathsf{E}\Big[\int_A f(y)M(dy) \, | \, \sigma\big((T_k^R)_{k=1}^{n-1}\big)\Big] = \mathsf{E}\Big[\int_A f(y)m(dy) \, | \, \sigma\big((T_k^R)_{k=1}^{n-1}\big)\Big]$$

Nous avons donc bien, en appliquant ce résultat, :

$$
\begin{aligned}
&\mathsf{E}\Big[\int_{t_n^R \ 1}^{s} \int_0^1 \int_0^1 \phi(s \quad v)1 \quad _{(v)p_{Ujv}(u)} m(\mathrm{d}v, \mathrm{d}u, \mathrm{d}\theta) \ \Big| \ \sigma((T_n^R)_{n=1}^{n-1})\Big] \\
=&\mathsf{E}\Big[\int_{t_n^R \ 1}^{s} \int_0^1 \int_0^1 \phi(s \quad v)1 \quad _{(v)p_{Ujv}(u)} M(\mathrm{d}v, \mathrm{d}u, \mathrm{d}\theta) \ \Big| \ \sigma((T_n^R)_{n=1}^{n-1})\Big]
\end{aligned}
$$

Avec $A =]t_{n \ 1}^R, s]$ R^+ R^+ et $f = \phi(s \quad v)1 \quad _{(v)p_{Ujv}(u)}$

Cela permet de justifier (K.5).

(3) Conclusion : Nous pouvons alors reprendre le calcul de (K.4) :

$$
\begin{aligned}
&\mathsf{E}_{n \ 1}\Big[\int_{t_n^R \ 1}^{s} \int_0^1 \int_0^1 \phi(s \quad v)1 \quad _{(v)p_{Ujv}(u)} 1_{v+u>} \ M(\mathrm{d}v, \mathrm{d}u, \mathrm{d}\theta)\Big] \\
=&\mathsf{E}_{n \ 1}\Big[\int_{t_n^R \ 1}^{s} \int_0^1 \int_0^1 \phi(s \quad v)1 \quad _{(v)p_{Ujv}(u)} 1_{v+u>} \ \mathrm{d}v\mathrm{d}u\mathrm{d}\theta\Big] \\
=&\mathsf{E}_{n \ 1}\Big[\int_{t_n^R \ 1}^{s} \int_0^1 \phi(s \quad v)\lambda(v)p_{Ujv}(u)1_{v+u>} \ \mathrm{d}v\mathrm{d}u\Big] \\
=&\mathsf{E}_{n \ 1}\Big[\int_{t_n^R \ 1}^{s} \phi(s \quad v)\lambda(v)p_{Ujv}([\tau \quad v, 1])\mathrm{d}v\Big]
\end{aligned}
$$

C'est le résultat que nous voulions démontrer.

Annexe L

Estimations de paramètres

L.1 Estimations du paramètre alpha

	Estimation avec biais	Estimation sans biais	Valeur réelle
1	1.1053	1.1722	1.3282
2	0.6459	0.6060	0.7768
3	0.9090	0.9635	1.1294
4	1.8872	2.2744	2.0958
5	1.4366	1.4263	0.8570
6	1.2340	3.3398	2.0991
7	0.9239	1.4912	1.1680
8	1.7031	1.8184	0.7559
9	0.3695	0.8767	0.4896
10	2.0336	2.0736	2.5739
11	2.1057	2.2843	2.6275
12	0.1534	0.0000	0.1031
13	0.9034	0.9402	1.1870
14	0.0000	0.0000	0.2378
15	0.8740	0.8814	1.0406
16	1.5883	1.6610	1.4356
17	0.0226	0.0000	0.3101
18	1.7120	2.2097	2.3241
19	1.0127	1.1095	1.1900
20	1.3354	1.0996	1.0888
21	0.0000	0.0000	0.1470
22	2.0200	2.1298	2.2305

L.2 Estimations du paramètre beta

	Estimation avec biais	Estimation sans biais	Valeur réelle
1	3.6418	6.1104	4.5009
2	1.7127	2.6769	2.3855
3	4.8894	5.3446	3.3120
4	1.9405	2.3467	2.1514
5	21.0698	22.0813	4.6723
6	6.1558	11.4574	4.8313
7	4.0054	12.5995	4.9481
8	22.1815	25.2491	3.3266
9	0.4499	38.5495	1.8803
10	3.4745	4.0790	4.2215
11	2.2015	2.3957	2.6667
12	0.3369	0.3846	2.1648
13	1.4277	2.5111	2.2123
14	3.5907	3.9822	4.9811
15	1.7640	3.7957	3.5053
16	4.5210	4.5702	2.8186
17	0.2170	0.2799	4.0967
18	2.4424	3.7991	3.1700
19	2.0908	2.4412	2.0627
20	1.3602	1.1216	1.1055
21	2.5891	2.2754	3.0619
22	5.0458	6.0369	4.9472

L.3 Estimations du paramètre mu

	Estimation avec biais	Estimation sans biais	Valeur réelle
1	4.1272	5.0592	4.5583
2	2.9516	3.9675	3.4556
3	1.0115	1.0735	0.8140
4	2.5030	4.0861	2.8909
5	1.4529	1.5217	1.2567
6	1.0826	2.9455	1.4030
7	3.7923	4.6311	4.0777
8	2.5284	2.7208	2.2069
9	0.9069	6.3376	4.7987
10	2.1062	2.6784	2.2606
11	0.3810	0.4031	0.4484
12	2.5501	5.2012	4.9383
13	2.9050	5.5149	4.2977
14	0.7884	0.8454	0.7335
15	2.8763	4.8801	4.6780
16	0.4573	0.4634	0.3647
17	2.2392	2.8948	2.5150
18	1.3867	2.6558	1.8790
19	3.5011	4.1304	3.2965
20	3.5553	6.0580	4.9405
21	1.5125	1.6763	1.4578
22	3.5923	4.2225	3.7554

L.4 Estimations du paramètre theta

	Estimation avec biais	Estimation sans biais	Valeur réelle
1	0.0965	0.0890	0.0925
2	0.0836	0.0756	0.0743
3	0.0926	0.0847	0.0899
4	0.0433	0.0294	0.0289
5	0.1022	0.0945	0.0985
6	0.0230	0.0053	0.0109
7	0.0977	0.0900	0.0887
8	0.0880	0.0800	0.0799
9	0.0388	0.0275	0.0290
10	0.0740	0.0667	0.0665
11	0.0886	0.0820	0.0837
12	0.0668	0.0583	0.0576
13	0.0675	0.0592	0.0610
14	0.0796	0.0714	0.0768
15	0.0608	0.0522	0.0525
16	0.0907	0.0815	0.0863
17	0.0474	0.0373	0.0389
18	0.0306	0.0182	0.0206
19	0.0658	0.0574	0.0581
20	0.0666	0.0547	0.0543
21	0.0492	0.0394	0.0449
22	0.0855	0.0779	0.0790

L.5 Nombre moyen d'IBNR théorique

	Nombre moyen avec biais	Nombre moyen sans biais	Nombre moyen théorique
1	61.3934	70.3138	69.9151
2	56.6892	67.8674	68.9466
3	13.4162	15.4589	13.7463
4	2097.9454	4453.8003	3825.4507
5	15.2504	17.2151	15.6201
6	56.9401	429.9347	183.5783
7	50.4498	58.3904	60.1633
8	31.1242	36.6365	35.7396
9	130.3887	232.1481	220.4844
10	68.6595	81.6903	87.1524
11	98.8457	105.7497	365.2750
12	70.0323	89.2073	90.0278
13	117.2015	148.8709	151.9341
14	9.9035	11.8399	10.0260
15	93.8260	121.6321	126.7256
16	7.7768	8.9339	8.6140
17	52.7320	77.2890	69.7136
18	149.7998	325.6101	326.1611
19	103.1678	131.7959	134.0894
20	2931.3503	5638.4583	6046.6815
21	30.7009	42.4328	34.0984
22	70.0759	83.7058	86.5810

Annexe M

Impact du paramètre theta

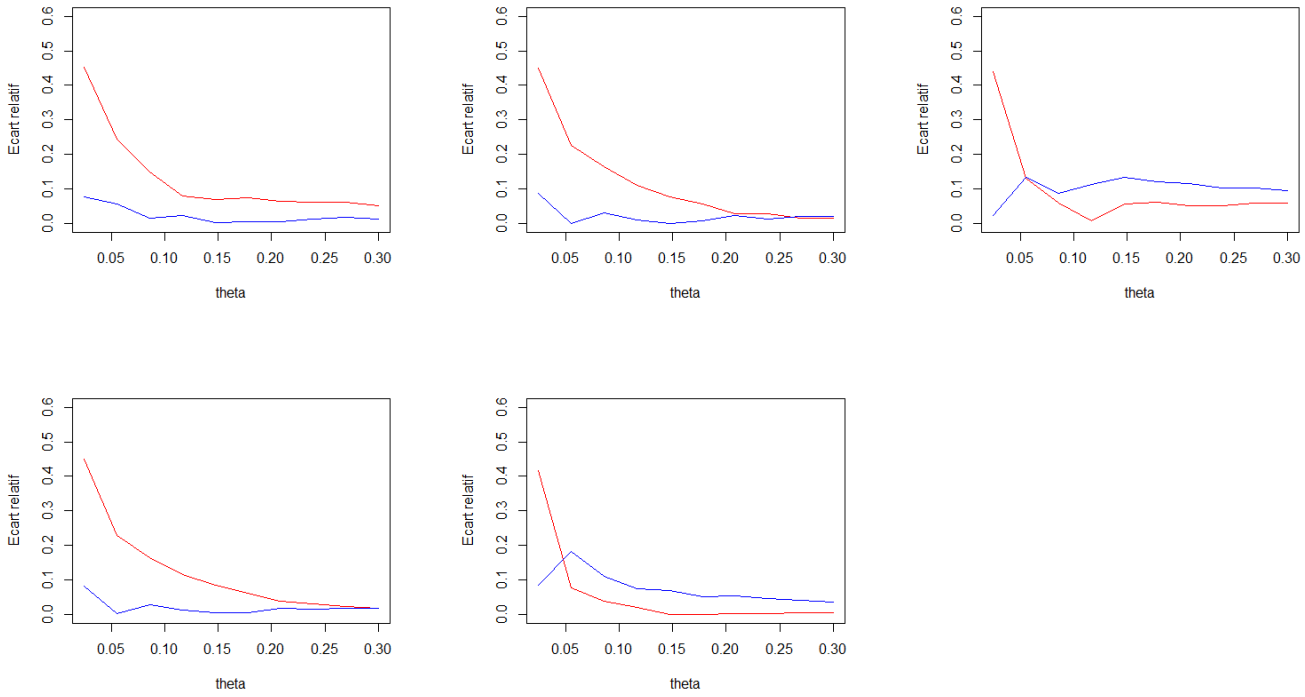


Figure M.1 – Erreur relative du nombre moyen d'IBNR en fonction de theta - en bleu le modèle Hawkes IBNR - en rouge le modèle biaisé - partie 1

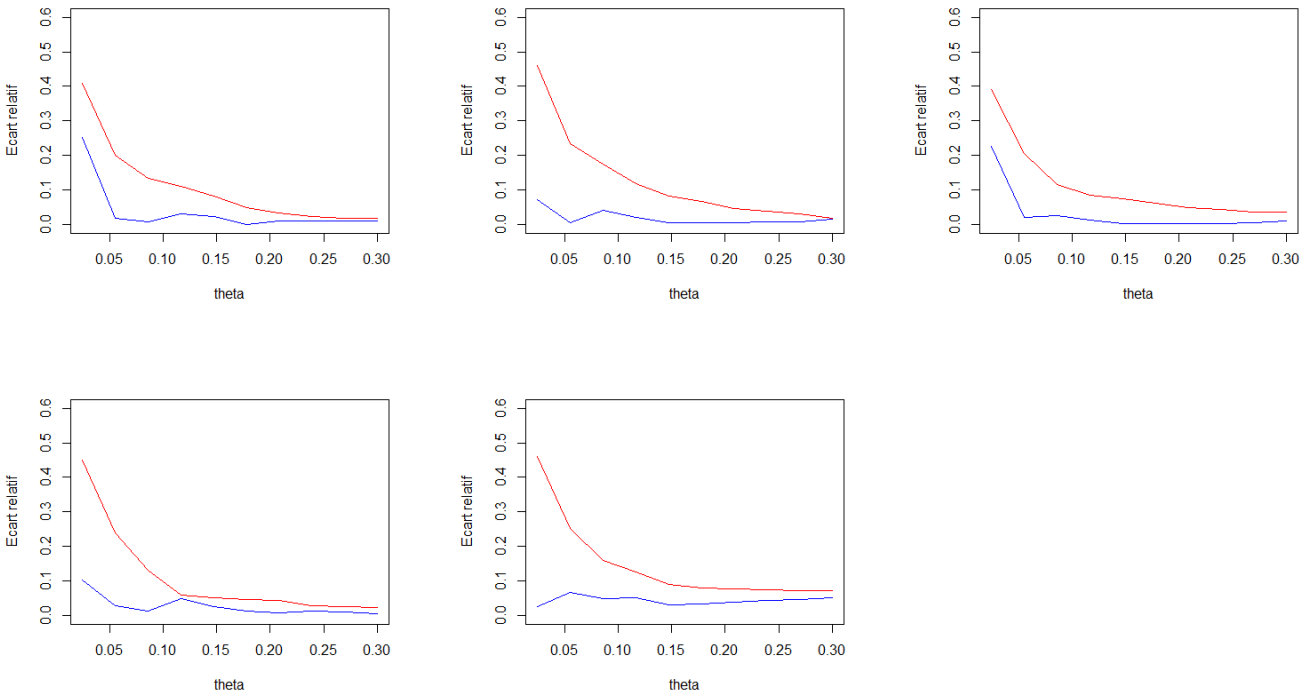


Figure M.2 – Erreur relative du nombre moyen d'IBNR en fonction de theta - en bleu le modèle Hawkes IBNR - en rouge le modèle biaisé - partie 2

Annexe N

Intégrale de l'intensité

Considérons un processus de Hawkes multivarié de dimension d 2 N : $(N_t^{(1)})_{t\ 0}, (N_t^{(2)})_{t\ 0}, ...(N_t^{(d)})_{t\ 0}$ et supposons que sur une période $[0, \tau]$ nous avons observé pour le processus $(N_t^{(i)})_{t\ 0}$ les temps d'occurences $(t_k^{(i)})_{k=1}^n$. Alors l'intégrale de l'intensité, dans le cas où le noyau est exponentiel, entre deux temps observés successifs $t_{k\ 1}^{(i)}$ et $t_k^{(i)}$ est :

$$\int_{t_{k\ 1}^{(i)}}^{t_k^{(i)}} \lambda^{(i)}(t)\mathrm{d}t = \int_{t_{k\ 1}^{(i)}}^{t_k^{(i)}} \Big[\mu^{(i)}(t) + \sum_{j=1}^{d} \sum_{T_u^{(j)} < t} \alpha_{i;j} \exp(\ \ \beta_{i;j}(t \ \ T_u^{(j)})\Big]\mathrm{d}t \tag{N.1}$$

avec :

$$\begin{aligned} &\int_{t_{k\ 1}^{(i)}}^{t_k^{(i)}} \Big[\sum_{j=1}^{d} \sum_{T_u^{(j)} < t} \alpha_{i;j} \exp(\ \ \beta_{i;j}(t \ \ T_u^{(j)})\Big]\mathrm{d}t \\ &= \Big[\sum_{j=1}^{d} \sum_{l=2}^{L} \int_{\widetilde{T_{l\ 1}}}^{\widetilde{T}_l} \sum_{T_u^{(j)} < t} \alpha_{i;j} \exp(\ \ \beta_{i;j}(t \ \ T_u^{(j)})\Big]\mathrm{d}t \end{aligned} \tag{N.2}$$

En notant : $(\widetilde{T_1}, \widetilde{T_2}, ..., \widetilde{T_L}) = (t_{k\ 1}^{(i)}, \widetilde{T_{u;1}}, .., T_{u;\widehat{L}\ 1}, t_{k\ 1}^{(i)})$ où $(\widetilde{T_{u;1}}, .., T_{u;\widehat{L}\ 1})$ est la séquence ordonnée des temps de sauts du processus $N_t^{(j)}$ qui sont arrivés sur $]t_{k\ 1}^{(i)}, t_k^{(i)}[$

L'équation (N.2) devient donc :

$$\begin{aligned} &\Big[\sum_{j=1}^{d} \sum_{l=2}^{L} \int_{\widetilde{T_{l\ 1}}}^{\widetilde{T}_l} \sum_{T_u^{(j)} < t} \alpha_{i;j} \exp(\ \ \beta_{i;j}(t \ \ T_u^{(j)})\Big]\mathrm{d}t \\ &= \Big[\sum_{j=1}^{d} \sum_{l=2}^{L} \sum_{T_u^{(j)}} \sum_{\widetilde{T_{l\ 1}}} \int_{\widetilde{T_{l\ 1}}}^{\widetilde{T}_l} \alpha_{i;j} \exp(\ \ \beta_{i;j}(t \ \ T_u^{(j)})\Big]\mathrm{d}t \\ &= \Big[\sum_{j=1}^{d} \sum_{l=2}^{L} \sum_{T_u^{(j)}} \sum_{\widetilde{T_{l\ 1}}} \frac{\alpha_{i;j}}{\beta_{i;j}} \big(\exp(\ \ \beta_{i;j}(\widetilde{T}_l \ \ T_u^{(j)}) \ \ \exp(\ \ \beta_{i;j}(\widetilde{T_{l\ 1}} \ \ T_u^{(j)})\big) \end{aligned} \tag{N.3}$$

Bibliographie

[Arjas, 1989] Arjas, E. (1989). The claims reserving problem in non-life insurance : Some structural ideas. *ASTIN Bulletin*, 19(2):139–152.

[Bacry *et al.*, 2015] Bacry, E., Mastromatteo, I. et Muzy, J.-F. (2015). Hawkes processes in finance. *Market Microstructure and Liquidity*, 1(01):1550005.

[Badescu *et al.*, 2016] Badescu, A. L., Lin, X. S. et Tang, D. (2016). A marked Cox model for the number of IBNR claims : Theory. *Insurance : Mathematics and Economics*, 69:29–37.

[Baldwin *et al.*, 2017] Baldwin, A., Iffat, G., Ioannidis, C., Pym, D. et Williams, J. (2017). Contagion in cyber security attacks. *Journal of the Operational Research Society*, 68(07):780–791.

[Böhme et Kataria, 2006] Böhme, R. et Kataria, G. (2006). Models and measures for correlation in cyber-insurance. Working Paper, Published in WEIS 2006, preprint on webpage at https ://archive.nyu.edu/bitstream/2451/14997/2/Infosec_ISR_Bohme+Kataria.pdf.

[Boumezoued, 2016a] Boumezoued, A. (2016a). *Micro-macro analysis of heterogenous age-structured populations dynamics. Application to self-exciting processes and demography*. Thèse de doctorat, Paris 6.

[Boumezoued, 2016b] Boumezoued, A. (2016b). Population viewpoint on Hawkes processes. *Advances in Applied Probability*, 48(2):463–480.

[Boumezoued et Devineau, 2017] Boumezoued, A. et Devineau, L. (2017). Individual claims reserving : a survey.

[Bray et Paik Schoenberg, 2013] Bray, A. et Paik Schoenberg, F. (2013). Assessment of point process models for earthquake forecasting. *Statistical Science*, 28:510–520.

[Chen, 2016] Chen, Y. (2016). Thinning algorithms for simulating point processes.

[Çınlar, 2011] Çınlar, E. (2011). *Probability and stochastics*, volume 261. Springer.

[Daley et Vere-Jones, 2003] Daley, D. et Vere-Jones, D. (2003). An introduction to the theory of point processes. vol. i : Elementary theory and methods. 2nd ed. Vol. 1.

[Edwards *et al.*, 2016] Edwards, B., Steven, H. et Forrest, S. (2016). Hype and heavy tails : A closer look at data breaches. *Journal of Cybersecurity*, 2:3–14.

[Fabre-Rudelle, 2018] Fabre-Rudelle, D. (2018). Apport des méthodes d'apprentissage statistique pour le provisionnement individuel en assurance non-vie. Mémoire de D.E.A., ISUP.

[Farkas *et al.*, 2019] Farkas, S., Lopez, O. et Thomas, M. (2019). Cyber claim analysis through generalized pareto regression trees with applications to insurance pricing and reserving.

[Giesecke *et al.*, 2011] Giesecke, K., Kim, B. et Zhu, S. (2011). Monte Carlo algorithms for default timing problems. *Management Science*, 57(12):2115–2129.

[Grigelionis, 1971] Grigelionis, B. (1971). The representation of integer-valued random measures as stochastic integrals over the Poisson measure. *Litovsk. Mat. Sb.*, 11:93–108.

[Haastrup et Arjas, 1996] Haastrup, S. et Arjas, E. (1996). Claims reserving in continuous time ; a nonparametric bayesian approach. *ASTIN Bulletin*, 26(2):139–164.

[HAWKES, 1971] HAWKES, A. G. (1971). Spectra of some self-exciting and mutually exciting point processes. *Biometrika*, 58(1):83–90.

[Herath et Herath, 2011] Herath, H. et Herath, T. (2011). Copula based actuarial model for pricing cyber-insurance policies. *Insurance Markets and Companies*, 2.

[Hesselager, 1994] Hesselager, O. (1994). A markov model for loss reserving. *ASTIN Bulletin*, 24(2):183–193.

[Jaisson, 2015] Jaisson, T. (2015). *Market activity and price impact throughout time scales*. Thèse de doctorat, Ecole Polytechnique.

[Jewell, 1989] Jewell, W. S. (1989). Predicting ibnyr events and delays : I. continuous time. *ASTIN Bulletin*, 19(1):25–55.

[Kerstan, 1964] Kerstan, J. (1964). Teilprozesse Poissonscher prozesse. *Trans. Third Prague Conf. Information Theory, Statist. Decision Functions, Random Processes (Liblice, 1962)*, pages 377–403.

[Khraibani et Khraibani, 2016] Khraibani, Z. et Khraibani, H. (2016). Self-exciting point process to study the evolution of the attack terrorism. *International Journal of Statistics and Applications*, 6:361–367.

[Lewis et Shedler, 1978] Lewis, P. A. W. et Shedler (1978). Simulation of nonhomogeneous Poisson processes by thinning. Rapport technique, Naval Postgraduate School.

[Mack, 1993] Mack, T. (1993). Distribution-free calculation of the standard error of chain ladder reserve estimates. *ASTIN Bulletin*, 23(2):213–225.

[Maochao et Lei, 2017] Maochao, X. et Lei, A. (2017). Cybersecurity insurance : Modeling and pricing. SOA, available at https ://www.soa.org/globalassets/assets/files/research/projects/cybersecurity-insurance-report.pdf.

[Ngoc an dinh, 2012] Ngoc an dinh, g. c. (2012). Mesures de provision cohérentes et méthodes lignes á lignes pour des risques non-vie. Mémoire de D.E.A., ENSAE.

[Norberg, 1993] Norberg, R. (1993). Prediction of outstanding liabilities in non-life insurance. *ASTIN Bulletin*, 23(1):95–115.

[Ogata, 1981] Ogata, Y. (1981). On Lewis' simulation method for point processes. *Information Theory, IEEE Transactions on*, 27(1):23–31.

[Ogata, 1988] Ogata, Y. (1988). Statistical models for earthquake occurrences and residual analysis for point processes. *Journal of The American Statistical Association - J AMER STATIST ASSN*, 83:9–27.

[Orlando *et al.*, 2017] Orlando, A., Marotta, A., Nanni, S., Martinelli, F. et Yautsiukhin, A. (2017). Cyber - insurance survey. *Computer Science Review*, pages 35–61.

[Ozaki, 1979] Ozaki, T. (1979). Maximum likelihood estimation of hawkes' self-exciting point processes. *Annals of the Institute of Statistical Mathematics*, 31(1):145–155.

[Peng *et al.*, 2016] Peng, C., Xu, M., Xu, S. et Hu, T. (2016). Modeling and predicting extreme cyber attack rates via marked point processes. *Journal of Applied Statistics*, 44:1–30.

[Pons, 2014] Pons, F. (2014). Etude actuarielle du cyber-risque. Mémoire de D.E.A., CNAM.

[Pratiwi *et al.*, 2017] Pratiwi, H., Slamet, I., Saputro, D. et , R. (2017). Self-exciting point process in modeling earthquake occurrences. *Journal of Physics : Conference Series*, 855:012033.

[Rasmussen, 2018] Rasmussen, J. G. (2018). Lecture notes : Temporal point processes and the conditional intensity function.

[Reinhart, 2017] Reinhart, A. (2017). A review of self-exciting spatio-temporal point processes and their applications. *Statistical Science*, 33:299–318.

[Rizoiu *et al.*, 2017] Rizoiu, M.-A., Young, L. et Swapnil, M. (2017). *A Tutorial on Hawkes Processes for Events in Social Media*, pages 191–218.

[Wüthrich, 2018] Wüthrich, M. V. (2018). Machine learning in individual claims reserving. *Scandinavian Actuarial Journal*, 2018(6):465–480.