



Filtre de spam

POURMOHAMMAD Maryam, CHABANE Djamila, HAJEB Ghamdan
Département d'Informatique

➤ Le but de notre application ?

L'objectif de notre travail est de réaliser une application qui tournera en tâche de fond en attente de réception de nouveaux courriers. Après réception du courrier, notre application va démarrer une série de traitements de filtrage qui déterminera la catégorie à appliquer au courrier ; spam ou simple courrier.

➤ C'est quoi un spam ?

Un spam est un courrier électronique indésirable que l'on reçoit dans notre boîte mail (pourriel en français) et dont l'expéditeur est inconnu, ce sont des courriers publicitaires ou commerciaux.

Parmi tous les courriels que nous recevons, en 2010 il est estimé que 81% d'entre eux sont considérés comme spam¹. L'utilisateur doit alors prendre le temps de les lire et de les supprimer. Il s'agit d'une véritable pollution de la boîte mail de l'utilisateur qui se trouve fortement ennuyé par ce genre de messages.

On reconnaît un spam selon les éléments suivants : un message publicitaire et/ou promotionnel, des jeux, des concours, des lots incroyables à gagner, des loteries, des promesses impossibles, des messages vous demandant de verser de l'argent, des messages courts ne contenant qu'une adresse URL, des services de pornographie ou les médicaments (les messages non désirés) comme les produits de « dopage sexuel » ou des hormones utilisées dans la lutte contre le vieillissement.

➤ Mais pourquoi spammer ?

L'envoi de spam est pratiqué par de nombreuses personnes, le principal but étant de faire de la publicité, cependant, ils existent également des personnes qui pratiquent cette activité pour embêter leur monde.

➤ Comment les spammeurs collectent ils les adresses mail ?

Les spammeurs peuvent récupérer les adresses e-mails des victimes de plusieurs façons:

- Ils peuvent acheter des listes d'adresses e-mail fournies par quelques fournisseurs de service Internet (e-mail, FAI, forum, etc.)
- Il existe également des outils qui permettent de récupérer des adresses e-mails automatiquement comme **les aspirateurs d'e-mails (spambot)** qui parcourent le réseau et scannent les sites à la recherche du signe @ ou de l'expression **mailto** qui indique la présence d'une adresse mail dans le code source d'une page web
- Ils peuvent aussi pratiquer le piratage de site professionnel ou de fournisseur de service Internet afin de récupérer toutes les adresses e-mails de leurs membres. Ils peuvent pirater des adresses e-mails de particuliers et utiliser leurs carnets d'adresses de façon récursive !

¹ <http://www.arkantos-consulting.com/revue-de-presse/20090807-etude-emailing-prospective-2009-2013.php>

- Il existe d'autres logiciels qui testent toutes les combinaisons d'adresses d'un même nom de domaine en envoyant des messages à ces adresses. Ils attendent alors les notifications d'erreurs de livraison du domaine attaqué. Ils en déduisent alors les adresses fonctionnelles et se constituent ainsi une liste à laquelle ils enverront ensuite leurs spam.

➤ Pourquoi l'Anti spam ?

L'anti spam ou le filtrage est une méthode qui permet de trier le courrier électronique reçu. Ce tri consiste à supprimer tous les courriers non désirés (pourriels) et à autoriser tous les courriers désirés (courriels). Pour procéder au filtrage, il existe plusieurs techniques de filtrages, par exemple :

- Filtres Bayésien : cette méthode consiste à calculer la probabilité qu'un message soit un spam ou non en utilisant la méthode du mathématicien Thomas Bayes.
- Filtrage par mots clés : un autre moyen de filtrage de spam est de parcourir des e-mails à la recherche des mots clés sur lesquels on doute par exemple le mot « sexe », « argent » ou « jeu ».
- Filtrage de serveur expéditeur : cette méthode permet de bloquer des adresses, des domaines ou des serveurs définis dans une liste noire par l'administrateur de système.
- Etc.

➤ Quelle méthode avons-nous choisie ?

Il est très important de choisir la bonne méthode de filtrage. Après l'étude des différentes techniques existantes, le choix le plus judicieux est la méthode Bayésienne. Cette méthode permet de découper le message en plusieurs parties afin de les comparer avec des spam connus. Il permet ensuite de donner des poids aux différentes parties du message. Si le poids total des différentes parties est assez élevé (plus que 90%), la méthode le considère alors comme spam.

➤ Présentation de notre projet

Nous avons réalisé une application qui met en pratique le filtrage Bayésien expliqué ci-dessus. Notre application se compose de 2 grandes parties, l'une qui sera utilisée comme boîte de réception de courriers et qui réalisera le filtrage des courriers entrant et une autre partie qui sera utilisée pour l'envoi de courrier.

À la réception de courriers, une étape d'analyse va se mettre en route. Pendant que l'application réalise le traitement de filtrage sur le courrier entrant, il sera également possible de recevoir d'autres courriers.

Pour analyser le contenu du courrier, le filtre Bayésien va décomposer le contenu du courrier en une liste de composants. Pour pouvoir réaliser la probabilité par rapport au contenu des courriers, l'application a besoin d'une liste de mots ou d'expressions relationnelles qui seront déjà connues, par exemple, des mots comme **Viagra** ou des expressions relationnelles comme **Viaagraaa**, qui figurent sur la plus part des courriers spam de ce genre.

Nous allons donc définir ces listes dans une base de données afin qu'elles soient utilisées par notre application pour la comparaison avec le contenu des nouveaux courriers entrant et ainsi calculer la probabilité (selon le théorème de Bayes) que les courriers soient du spam ou pas. L'utilisateur pourra également définir certains courriers comme spam à partir de la boîte de réception, tout simplement en les cochant et en catégorisant **spam**.

Une fois que l'application aura terminé sa tâche de filtrage, le courrier reconnu comme spam sera mis en évidence dans la boîte de réception afin d'alerter l'utilisateur.