

PROPOSITION DE SUJET DE THESE



Campagne 2016

Laboratoire L3i

Sujet de la thèse :

Détection et analyse des signaux faibles. Développement d'un framework d'investigation numérique pour un service caché *Lanceurs d'alerte*.

Résumé du travail proposé :

Le sujet de thèse s'inscrit dans le contexte du développement d'une plateforme d'analyse automatique de documents associée à un service caché *lanceurs d'alerte* focalisé sur la révélation de faits/événements/actions en lien avec des problématiques environnementales/écologiques.

Dans le but de traiter de manière automatique les documents textuels révélés par le lanceur d'alerte et portant sur un ou plusieurs faits relatifs à un événement déclencheur, nous proposons de développer un framework d'investigation qui s'appuiera (1) sur une approche Bayésienne non paramétrique de type HDP, afin de regrouper par clustering multi-niveaux, avec un minimum d'*a priori*, les documents portant sur un même fait/thème, et d'extraire des indicateurs horodatés et géoréférencés caractéristiques et significatifs de chaque thème, (2) de confirmer/corréler les informations révélées et les augmenter par un mécanisme hybride agent mining-HDP alimentant un deep neural network; les agents sont chargés d'effectuer des requêtes transversales ou en profondeur à partir des indicateurs précédents sur des réseaux sociaux et spécialisés, (3) de visualisation analytique comme outil d'aide à la mise en perspectives de l'information par la création de représentations visuelles et de tableaux de bord dynamique. Nous souhaitons mettre l'humain au cœur du processus de moissonnage d'information en ligne afin d'offrir des possibilités de « retour de pertinence » et de « renforcement de pistes », par exemple au travers d'un jeu sérieux. Pour des raisons de sécurité, on peut envisager que les interactions à distance (via les mécanismes et services Tor) entre expert et lanceur d'alerte s'effectuent au travers de casques virtuels et à l'aide d'avatars.

Ce framework doit répondre au besoin qu'ont les journalistes/politiques/juristes de se munir d'outils d'investigation (extraction, vérification, corrélation) et de représentation de l'information (synthèse, aide à la décision). Il a pour but de faciliter les expertises indépendantes, protéger les lanceurs d'alerte et aider à la détection des signaux faibles.

Mots clés :

Investigation numérique, détection de signaux faibles, approches Bayésiennes non paramétriques, agent mining, deep learning, visualisation analytique, traitement du signal social, protection des sources, communication interactive immersive

Informations complémentaires :

- **Encadrant(s) :**
 - Michel Ménard (directeur de thèse)
 - Guillaume Chiron et Alain Bouju (co-direction)
- **Thématiques :** Analyse et gestions de contenus
- **Domaine d'application :** Investigation numérique
- **Financement complémentaire envisagé** de type participatif et/ou contrat avec des sociétés éditrices.
- **Cadre de coopération :** collaboratif ou industriel selon le type de financement choisi.
- **Date de début du contrat :** Automne 2016.

Contact: michel.menard@univ-lr.fr, guillaume.chiron@univ-lr.fr, alain.bouju@univ-lr.fr

Contexte de l'étude:

Il existe des situations dans lesquelles l'anonymat est une nécessité légitime difficilement contestable: on peut citer celle des journalistes enquêtant sur des sujets sensibles souhaitant préserver leur identité comme leurs sources, les lanceurs d'alertes.

Un signal faible est une information d'alerte précoce, de faible intensité, pouvant être annonciatrice d'une tendance ou d'un événement important (Igor Ansoff, Economiste).

Une problématique majeure actuelle porte sur notre capacité à prendre des décisions éclairées devant l'augmentation drastique des signaux délivrés par toujours plus de moyens d'information. Des phénomènes de saturation des capacités de nos systèmes de traitement conduisent à des difficultés d'interprétation ou même à refuser les signaux précurseurs de faits ou d'événements. L'utilité de la prise de décision contrainte par des nécessités temporelles oblige un traitement rapide de la masse d'information. Etre capable de détecter dans un délai imposé, les *bons* signaux porteurs de l'information *utile* dans un contexte de stratégie d'anticipation, s'avère être un challenge devenu permanent pour de nombreux acteurs économiques. Il est donc nécessaire de développer, sous la forme de plateformes d'investigation, de nouveaux services d'aide à la décision pour les politiques et les organisations en charge de ces activités. Les prises de décision, qui doivent portées aussi bien sur la crédibilité de la source d'information que sur la pertinence des informations révélées relatives à un événement, nécessitent des algorithmes robustes de détection des signaux faibles, d'extraction et d'analyse de l'information portée par ces derniers, d'ouverture sur un contexte informationnel plus large.

Nous proposons dans cette thèse de porter notre action sur deux points essentiels : la détection des signaux faibles et l'extraction de l'information véhiculée par ces derniers. Notre objectif concerne donc la détection de signaux précurseurs dont la présence attenante dans un espace de temps et de lieux donnés anticipe l'avènement d'un fait observable. Cette détection est facilitée par l'information précoce délivrée par un lanceur d'alerte sous la forme de documents. Ils exposent des faits avérés, unitaires et ciblés, mais aussi partiels, relatifs à un événement déclencheur. Le lanceur d'alerte délivre une information non encore décelable/apparente sur les réseaux sociaux et spécialisés. Elle permet de dessiner le contour des signaux faibles à venir sur les réseaux, facilitant ainsi leur détection et l'extraction de l'information portée par ceux-ci.

Description du sujet :

La procédure d'investigation proposée repose sur la détection des signaux faibles présents sur les réseaux. Elle combine algorithmes de fouille de données et visualisation analytique. Elle est facilitée par la connaissance des patterns révélés par le lanceur d'alerte. L'information est estimée à partir (1) des indicateurs révélés par le lanceur d'alerte, (2) des données portées par les signaux faibles, et (3) du comportement des signaux financiers ayant trait aux événements. Les smart data (révélées par le lanceur d'alerte et par les signaux financiers) permettent de mieux cibler le data mining lors des phases de détection des signaux faibles et d'exploration sur les réseaux. Pour le développement du framework d'investigation, trois actions sont entreprises.

Action 1. Analyse automatique de contenus avec un minimum d'*a priori* et identification des informations pertinentes.

Afin de traiter de manière automatique les documents textuels révélés par le lanceur d'alerte et portant sur un ou plusieurs faits relatifs à l'événement déclencheur, nous proposons de développer des outils d'analyse qui s'appuieront sur une approche Bayésienne non paramétrique de type HDP (e.g. MLC-HDP), afin de :

- regrouper les documents portant sur un même fait/thème; le clustering MLC-HDP permet, à partir de vecteurs descripteurs construits sur les documents, de relier ensemble avec un minimum *d'a priori* tous les documents relatifs à un même thème. Ces thèmes, que nous supposons relatifs à l'événement déclencheur, seront découverts simultanément grâce au clustering multi-niveaux (montée en sémantique). Cet outil pourra par exemple s'appuyer sur les mots les plus représentatifs des documents et regrouper ces derniers lorsque ceux-ci partageront suffisamment de mots similaires;

- d'extraire des indicateurs et leurs attributs relatifs à chaque thème (lexique de descripteurs textuels, triplet "personne/lieu/fait"). On peut citer, par exemple comme indicateurs, les personnes morales et physiques, auxquelles sont attribuées des descripteurs de plusieurs niveaux :

- trajectoire ou localisation,
- représentativité: occurrence par document, par thème,
- rayonnement : mesures décrivant les relations avec les autres indicateurs;

- d'évaluer la cohérence intrinsèque des informations déterminée à partir des seuls documents.

Action 2. Agrégation de connaissances. Enrichissement de l'information.

L'objectif est d'utiliser des outils de corrélation avancés et de les appliquer sur de grands ensembles de données de manière transverse (réseaux sociaux, sites spécialisés concernés par le contexte d'événements). Le challenge est ici, en tant qu'investigateur, d'arriver à confirmer les informations révélées, et les augmenter. L'approche que nous souhaitons adopter est du type *agent mining* qui utilise, conjointement aux approches *multi-agents*, des méthodes de *découverte de la connaissance* et de *data mining*. Chaque agent est chargé d'effectuer des requêtes construites à partir d'indicateurs détectés précédemment. Il contribue à une stratégie de découverte qui se veut être un compromis entre coût de recherche et connaissance extraite des sites. Chaque agent possède sa stratégie locale: à partir des premiers résultats de sa requête (effectuée sur un ou plusieurs moteurs de recherche, avec un sous-ensemble d'indicateurs) et des informations apportées par les autres agents, doit-il continuer à explorer le site visité en explorant des liens internes (analyse en profondeur), doit-il modifier les termes, les sources et les objectifs de sa requête (exploration transverse) ? Il est donc nécessaire de proposer une approche optimisant les performances de collaboration, la fusion des informations acquises et la gestion des conflits en s'appuyant sur des modèles biologiques (fourmis, abeilles) exploratoires par renforcement/oubli de pistes.

Les requêtes construites en associant plusieurs indicateurs ont pour objectif d'extraire de l'information complémentaire à l'information révélée, corréler, renforcer ou affaiblir les indicateurs détectés. Les résultats de ces requêtes seront analysés à partir des fonctionnalités suivantes: surveillance de mots clés particuliers (associés aux indicateurs), nombre de liens trouvés vérifiant la présence de l'ensemble des indicateurs présents dans la requête, mise en avant des expressions les plus utilisées autour des mots clés ou indicateurs.

Action 3. Visualisation analytique. Mise en perspective de l'information par la création de représentations visuelles et de tableaux de bord dynamique. Boucle de pertinence.

La visualisation analytique, troisième étape du traitement, doit permettre une représentation synthétique et interactive des résultats obtenus afin d'aider les experts à s'approprier l'information. Les résultats bruts apportés par des algorithmes de data mining nécessitent en effet, pour une meilleure compréhension des relations complexes entre les données multi-dimensionnelles, des outils de visualisation mettant en évidence les corrélations dynamiques entre données et événements. L'objectif premier est donc de proposer des diagrammes mieux adaptés à l'interaction et à la visualisation des données. Le second objectif est de mettre l'humain au sein du processus de moissonnage d'information en ligne afin d'offrir des possibilités de « retour de pertinence » et de « renforcement de pistes », par exemple au travers d'un jeu sérieux. On peut imaginer un environnement graphique 3D où circulent et interagissent des entités (images, étiquettes, cartes, dates). Les utilisateurs (Expert et Lanceur d'alerte) peuvent interagir avec ces entités afin d'en

modifier le comportement global et orienter la recherche et la modélisation de l'information dans une direction souhaitée.

Pour des raisons de sécurité, on peut envisager que les interactions à distance (via les mécanismes et services Tor) entre expert et lanceur d'alerte s'effectuent au travers de casques virtuels et à l'aide d'avatars. Expert et lanceur d'Alerte, situés en des lieux différents, peuvent en effet vouloir échanger lors des investigations. La visualisation analytique doit prendre alors en compte les spécificités de ces systèmes (résolution, visualisation 360), susceptibles d'être utilisés dans ce contexte où les sources d'information et l'information elle-même doivent être protégées.

Prérequis et contraintes particulières :

- Pour le déploiement du framework d'investigation numérique, l'architecture envisagée s'appuierait sur Talend, qui fournit une plateforme sur Apache Spark pour l'intégration et la diffusion des données, et sur les plateformes Gama ou NetLogo pour la partie SMA.
- La plateforme d'hébergement du service caché utilise le mécanisme de "service caché" du réseau TOR et la plateforme Globaleaks (<https://globaleaks.org/>) dont le code a fait l'objet de plusieurs audits (voir aussi l'initiative GoLeaks, <http://www.nextinpact.com/news/97876-goleaks-plateforme-pour-lanceurs-dalerte-dans-grand-ouest.htm>).
- Connaissances des langages Matlab, Python et R.

Références bibliographiques :

- Analysis of weak signals for detecting lone wolf terrorists. Brynielsson, J. and Horndahl, A. and Johansson, F. and Kaati, L. and Martenson, C. and Svenson, P. Intelligence and Security Informatics Conference (EISIC), pp. 197-204, Aug 2012.
- A Hierarchical Dirichlet Process Model with Multiple Levels of Clustering for Human EEG Seizure Modeling. Drausin Wulsin, Brian Litt et Shane T. Jensen. Proceedings of the 29th International Conference on Machine Learning (ICML-12), pp. 57-64, New York, NY, USA, 2012.
- Time series analysis on stock market for text mining. Correlation of economy news. Sadi Evren Seker, Cihan Mert, Khaled Al-Naami, Nuri Ozalp, and Ugur Ayan. International Journal of Social Sciences and Humanity Studies. Vol. 6, No.1, pp. 69-90, 2014.
- On the Decision Structures and Knowledge Discovery for ANP Modeling. Lawrence W.Lan, Weil-Wen Wu, Yu-Ting Lee. International Journal of Intelligence Science. Vol. 3, pp. 15-23, 2013.
- Interactive Sensing and Decision Making in Social Networks. Vikram Krishnamurthy, Omid Namvar Gharehshiran, Maziyar Hamdi. J. Found. Trends Signal Process. 7, 1-2, 1-196. 2014
- Système complet d'acquisition vidéo, de suivi de trajectoires et de modélisation comportementale pour des environnements 3D naturellement encombrés. Application à la surveillance apicole. Guillaume Chiron. Thèse de l'université de La Rochelle. Ecole Doctorale S2IM. 28 novembre 2014.
- Extraction d'opinions appliquée à des critères. Duthil, B., F. Troussel, G. Dray, P. Poncelet, et J. Montmain (2012). In Y. Lechevallier, G. Melançon, et B. Pinaud (Eds.), EGC, Volume RNTI-E-23 of Revue des Nouvelles Technologies de l'Information, pp. 483-488. Hermann- Éditions.