Implémentation de réseaux récurrents pour la détection d'événements inattendus

Thomas Kastner*,**, Hubert Cardot*, Dominique H. Li*, Nicolas Labroche*

* Université de Tours, LIFAT, EA 6300, Tours, France
prénom.nom@univ-tours.fr,
** Apivia MACIF Mutuelle, France

Notre monde est rempli de processus qui sont de plus en plus capturés et stockés sous forme de bases de données de journaux d'événements. Une telle base contient plusieurs cas, un ensemble d'événements ordonnés composés chacun d'une activité et d'un horodatage. Dans la majorité des applications, l'ensemble des cas peut être généralisé en utilisant un modèle de processus soit défini par un expert, soit extrait automatiquement. Il est nécessaire de connaître le modèle de processus sous-jacent pour évaluer la conformité d'une trace, mais certains modèles peuvent être considérablement complexes, et les experts peuvent avoir du mal à les décrire entièrement même en se basant sur les méthodes d'exploration. De plus, les journaux d'événements peuvent provenir de flux qui doivent être analysés en temps réel. Détecter des anomalies dans ce type de données peut, par exemple, aider à assurer la qualité des données, permettre d'identifier des fraudeurs dans des transactions par carte de crédit ou des réclamations d'assurance. Cela a été étudié pendant de nombreuses années dans le domaine de la fouille de processus (ou "Process Mining"). Nous nous concentrons sur la tâche de détection d'anomalies dans les événements les plus récents d'un cas, c'est-à-dire sur le suffixe d'une trace incomplète. Dans ce contexte, le cas n'est pas terminé, ce qui signifie que d'autres événements peuvent survenir à l'avenir. Enfin, pour presque toutes les applications, l'étiquetage humain est très coûteux, c'est pourquoi il convient d'utiliser des méthodes non supervisées. Ces méthodes sont adaptées pour détecter des observations anormales et ne dépendent d'aucune variable cible.

La tâche de prédiction de l'élément suivant au sein de traces d'événements a été introduite par Evermann et al. (2017) et a été largement étudiée jusqu'à présent (Neu et al. (2022)). Les méthodes neuronales récurrentes peuvent être utilisées pour prédire des événements futurs, car elles s'adaptent à la nature séquentielle des données du journal des événements. La prédiction obtenue peut être exploitée pour générer un score d'anomalie. L'algorithme BiNet présenté par Nolle et al. (2018) utilise les prédictions du type d'événement suivant en utilisant la méthode récurrente GRU pour générer un score d'anomalie. La figure 1 montre une vue d'ensemble de la proposition de BiNet. Nous proposons plusieurs nouveaux scores d'anomalies basés sur les probabilités d'apparition de chaque type d'événement, et nous évaluons un ensemble de caractéristiques liées au modèle de détection d'anomalies et au modèle de prédiction intrinsèque.
Nous expérimentons sur plusieurs jeux de données de l'état de l'art du domaine de la fouille de processus en générant des anomalies synthétiques par permutations d'activités. Nous fournissons ensuite plusieurs indications pour l'utilisation de cette méthodologie dans des cas réels de détection d'anomalie en temps réel dans des journaux d'événements. Premièrement, l'ar-

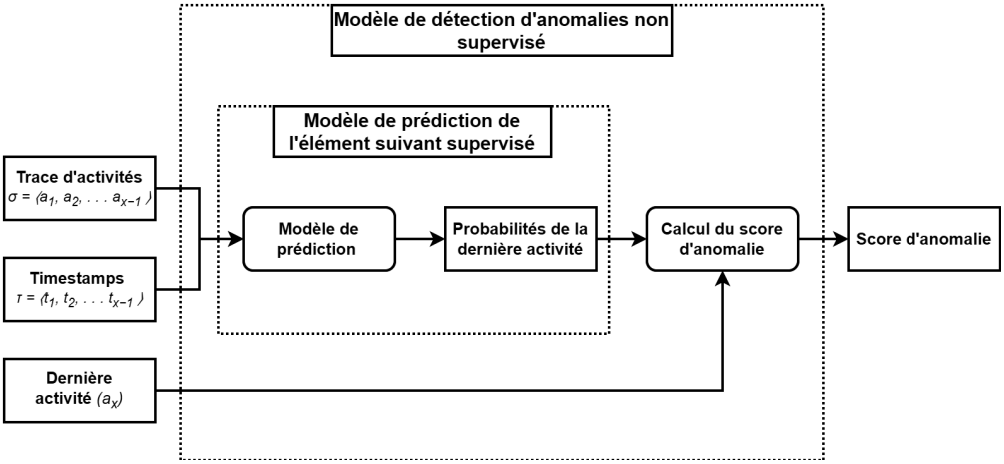

FIG. 1 – *Vue d'ensemble du modèle de détection d'anomalies non supervisé*

chitecture LSTM à une couche semble convenir pour les différents jeux de données de notre benchmark, ce qui est cohérent avec l'état de l'art concernant les méthodes récurrentes de l'apprentissage profond. Deuxièmement, l'exploitation des horodatages sous la forme d'intervalles de temps entre activités semble aussi améliorer les performances de détection des anomalies. Ensuite, une méthode basique de calcul d'anomalie, qui repose sur l'inverse de la probabilité de survenue du type d'événement suivant surpasse les techniques d'anomalie plus complexes. Pour finir, nous vérifions que la présence d'anomalies dans le jeu de données d'entraînement n'impacte pas significativement les résultats de nos expérimentations.
L'ensemble des expérimentations présentées vise à encourager et faciliter la mise en place d'une telle méthode en situation réelle.

Références

Evermann, J., J.-R. Rehse, et P. Fettke (2017). Predicting process behaviour using deep learning. *Decision Support Systems 100*, 129–140.

Neu, D. A., J. Lahann, et P. Fettke (2022). A systematic literature review on state-of-the-art deep learning methods for process prediction. *Artificial Intelligence Review*, 1–27.

Nolle, T., A. Seeliger, et M. Mühlhäuser (2018). Binet : Multivariate business process anomaly detection using deep learning. In M. Weske, M. Montali, I. Weber, et J. vom Brocke (Eds.), *Business Process Management*, Cham, pp. 271–287. Springer International Publishing.