

Adaptation d'un modèle de langage à une tâche de traduction pour des systèmes de sécurité basés sur les intentions

Master Recherche - Équipe SOTERN

1 CONTEXTE

Les réseaux basés sur les intentions ont été introduits par la RFC 9315 [1] et ont comme objectif de mettre l'accent sur les intentions d'un administrateur plutôt que les moyens de configuration d'un réseau. Par exemple un administrateur pourrait vouloir exprimer : « Les utilisateurs du département Ressources Humaines doivent pouvoir s'échanger des données de manière sécurisée. ». Cette intention doit alors pouvoir être transcrite dans une configuration du réseau et des équipements.

Depuis une décennie, les avancées des travaux sur les modèles de langage, et en particulier les larges (en anglais *LLM (Large Language Model)*, par exemple chatGPT pour OpenAI, Llama pour Facebook), permettent d'exprimer sous une forme condensée de l'entrée donnée au réseau et partir de cette donnée rend la tâche de traduction vers autre chose plus simple à apprendre).

Il n'existe pas encore de modèle de langage permettant d'effectuer la traduction depuis le langage naturel vers une description de réseau ou de politique de sécurité. Cependant, si cela existait, des problématiques seraient encore non résolues, la tâche de traduction langage naturel \rightarrow politique de sécurité du réseau permet-elle de garantir une correspondance exacte ?

2 ÉTAT DE L'ART ET OBJECTIFS

Les réseaux basés sur les intentions et les problématiques associées sont décrits dans [2]. La tâche de reconnaissance de l'intention de l'utilisateur et de sa traduction dans un langage dédié aux intentions peut-être vue comme une tâche de traduction entre deux langages et des LLM ont pu être adaptés pour réaliser ces traductions[3]. D'autres travaux ont permis de montrer la faisabilité d'une traduction automatique entre des configurations d'équipement par l'utilisation de modèles de langage [4].

Utiliser le langage naturel comme langage d'entrée utilisateur est parfaitement compatible avec l'esprit des réseaux basés sur les intentions tels que décrit dans la RFC9315. Cependant, le langage d'expression des intentions, doit à la fois être assez expressif pour rendre compte de l'expression de l'intention en langage naturel, et être assez descriptif pour pouvoir être traduit automatiquement dans un langage de politique de sécurité. Le langage de référence utilisé dans la littérature est NILE [5] utilisant des réseaux de neurones sequence-to-sequence pour réaliser la traduction du langage de haut niveau vers le langage NILE et proposent une plateforme complète dans [6] (la présentation vidéo est disponible¹). Cependant, le langage NILE étant prévu pour être étendu, n'est pas forcément complet du point de vue de la sécurité du réseau (il n'y a que la notion de filtrage qui est actuellement utilisé).

Un corpus aligné de phrases en anglais et de traductions dans le langage NILE a été généré en 2024. L'**objectif principal** du stage est de proposer une méthodologie permettant d'adapter un modèle de langage LLM et d'évaluer cet apprentissage dans le cadre d'une tâche de traduction « zero shot ».

La méthodologie de travail du stage repose sur non seulement une approche pratique (développement des outils d'apprentissage si besoin et d'inférence des réseaux de neurones) mais aussi une approche théorique (méthodologie d'évaluation et de comparaisons des traductions).

Les travaux réalisés dans le cadre de ce stage pourront faire l'objet d'un article qui sera soumis à une relecture par les pairs dans le domaine de la cybersécurité des réseaux.

BIBLIOGRAPHIE

- [1] A. Clemm, L. Ciavaglia, L. Z. Granville, et J. Tantsura, « Intent-Based Networking - Concepts and Definitions ». [En ligne]. Disponible sur: <https://www.rfc-editor.org/info/rfc9315>

¹<https://www.usenix.org/conference/atc21/presentation/jacobs>

- [2] A. Leivadreas et M. Falkner, « A Survey on Intent-Based Networking », *IEEE Commun. Surv. Tutorials*, vol. 25, n° 1, p. 625-655, 2023, doi: [10.1109/COMST.2022.3215919](https://doi.org/10.1109/COMST.2022.3215919).
- [3] W. Zhu *et al.*, « Multilingual Machine Translation with Large Language Models: Empirical Results and Analysis ». 2023.
- [4] C. Wang, M. Scazzariello, A. Farshin, S. Ferlin, D. Kostić, et M. Chiesa, « NetConfEval: Can LLMs Facilitate Network Configuration? », *Proc. ACM Netw.*, vol. 2, n° CoNEXT2, juin 2024, doi: [10.1145/3656296](https://doi.org/10.1145/3656296).
- [5] A. Jacobs, R. Pfitscher, R. Ferreira, et L. Granville, « Refining Network Intents for Self-Driving Networks », 2018, p. 15-21. doi: [10.1145/3229584.3229590](https://doi.org/10.1145/3229584.3229590).
- [6] A. S. Jacobs *et al.*, « Hey, Lumi! Using Natural Language for Intent-Based Network Management », in *2021 USENIX Annual Technical Conference (USENIX ATC 21)*, USENIX Association, juill. 2021, p. 625-639. [En ligne]. Disponible sur: <https://www.usenix.org/conference/atc21/presentation/jacobs>