Proposition d'un modèle d'évaluation de la confiance pour la détection des attaques dans l'Internet des Objets Social

Wafa Abdelghani*, Florence Sèdes**
Corinne Amel Zayani*,** Ikram Amous***

* Université Paul Sabatier,Toulouse, France
** Université de Sfax,Sfax, Tunisie

1 Introduction

L'intégration de la composante sociale dans l'Internet des Objets a donné naissance à l'Internet des Objets Social (SIoT) (Geetha (2016)). Dans ce type d'environnement, les participants sont en compétition pour offrir une variété de services attrayants. Certains d'entre eux ont recours à des comportements malveillants afin de propager des services de mauvaise qualité et lancent des attaques de confiance. Les attaques de confiance citées dans la littérature sont : Self-Promoting Attack (SPA), Bad Mouthing Attack (BMA), Ballot Stuffing Attack (BSA) et Discriminatory Attack (DA) (voir Bao et al. (2013); Abdelghani et al. (2018)) Le rôle d'un modèle d'évaluation de la confiance consiste à assurer le bon fonctionnement du système, en bloquant ce type d'attaque. Il est principalement composé de : (i) L'étape de composition qui consiste à choisir les facteurs qui permettant de mesurer la confiance ; et (ii) L'étape d'agrégation qui consiste à choisir une méthode pour combiner ces facteurs. Pour ce, la majorité des travaux utilise la moyenne pondérée (Nitti et al. (2012); Bao et al. (2013)) qui ne permet pas de détecter tous les types d'attaques.

2 Modèle d'évaluation de la confiance

Nous proposons de nouveaux facteurs permettant de décrire et de quantifier les différents comportements opérant dans les systèmes IoT.

— La réputation : permet de quantifier la renommée d'un utilisateur dans le réseau.
— L'honnêteté : permet d'indiquer si les votes d'un utilisateur reflètent son opinion réelle.
— La qualité du fournisseur : reflète la qualité des services fournis par l'utilisateur.
— La similarité : est calculée en fonction de différents attributs tels que les profils, les centres d'intérêt, et vise à révéler les attaques de type SPA.
— La fréquence des votes : varie par exemple quand un utilisateur lance une attaque contre un autre et vote à plusieurs reprises.
— L'expérience directe : fait référence à l'avis d'un utilisateur sur ses interactions passées avec un autre.
— La tendance des votes : permet de détecter l'attaque DA dans laquelle l'utilisateur fournit souvent des votes négatifs.

Pour agréger ces différents facteurs, nous proposons d'utiliser les techniques d'apprentissage automatique. Un utilisateur est considéré comme malveillant s'il tente de réaliser une attaque BMA, BSA, SPA ou DA. L'algorithme d'apprentissage automatique prend en entrée les valeurs des facteurs proposés et renverra en sortie l'une des classes mentionnées (malveillant/ bienveillant).

3 Expérimentations et évaluations

Nous avons experimenté notre modèle sur le jeu de données "Sigcomm [1]". Nous nous sommes comparés aux facteurs les plus utilisés dans la littérature en utilisant (i) la moyenne pondérée, puis (ii) l'apprentissage automatique. Les résultats montrent que les facteurs proposés donnent de meilleurs résultats par rapport aux autres travaux, même dans le cas de l'agrégation avec la moyenne pondérée. Les résultats sont encore meilleurs lorsque nous appliquons la technique d'apprentissage automatique.

4 Conclusion et perspectives

Nous avons proposé un modèle d'évaluation de confiance, capable de détecter les noeuds malveillants. Ce modèle repose sur de nouveaux facteurs, permettant de quantifier le comportement des utilisateurs, ainsi qu'une nouvelle méthode d'agrégation permettant d'analyser ces comportements.

Références

Abdelghani, W., C. A. Zayani, I. Amous, et F. Sèdes (2018). Trust evaluation model for attack detection in social internet of things. In *International Conference on Risks and Security of Internet and Systems*, pp. 48–64. Springer.

Bao, F., I. Chen, et J. Guo (2013). Scalable, adaptive and survivable trust management for community of interest based internet of things systems. In *11th International Symposium on Autonomous Decentralized Systems*, Mexico City, pp. 1–7.

Geetha, S. (2016). Social internet of things. *World Scientific News 41*, 76.

Nitti, M., R. Girau, L. Atzori, A. Iera, et G. Morabito (2012). A subjective model for trustworthiness evaluation in the social internet of things. In *23rd IEEE International Symposium on Personal, Indoor and Mobile Radio Communications, PIMRC 2012, Sydney, Australia, September 9-12, 2012*, Sydney, Australia, pp. 18–23. IEEE.

1. http ://crawdad.org/thlab/sigcomm2009/20120715/