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.