Sémantique Formelle à Deux Joueurs pour Arbres d'Attaque

T. Brihaye[1], S. Pinchinat[2], A. Terefenko[1,2]

[1] Université de Mons, Belgique
[2] Université de Rennes, IRISA, France

Résumé

Les arbres d'attaques sont un formalisme utilisé en sécurité pour l'évaluation de menace en analyse de risque. En 2017, M. Audinot et al. ont introduit une sémantique de chemins sur un système de transition pour les arbres d'attaque. Cette approche ne permet pas de considérer des systèmes avec plusieurs acteurs. Inspiré par ce travail, nous proposons une interprétation à deux joueurs de ce formalisme en généralisant la sémantique de chemins à une sémantique de stratégies. Dans ce cadre, nous montrons que le problème de la vacuité d'un arbre d'attaque est PSPACE*-complet, alors que le problème d'appartenance d'une stratégie à la dénotation d'un arbre est* CONP*-complet.*

Mots-clés

arbre d'attaque, sémantique, arène de jeu, stratégie.

Abstract

Attack trees are a fromalism used in security for the evaluation of threat in risk analysis. In 2017, M. Audinot et al. introduced a path semantics over a transition system for attack trees. This approach does not allow to consider multi-agent systems. Inspired by the latter, we propose a two-player interpretation of this formalism by generalising the path semantics to a strategy semantics. We then show that the emptiness problem for an attack tree is PSPACE*-complete and the membership problem for a strategy to the description of an attack tree is* CONP*-complete.*

Keywords

Attack tree, semantics, game arena, strategy.

1 Introduction

La sécurité est un sujet d'attention croissante dans notre société actuelle pour protéger les ressources critiques de divulgation d'informations, de vol ou de dégâts. Le modèle informel d'arbre d'attaque a été d'abord introduit pas Schneier [3] pour représenter les menaces possibles sur un système informatique. Les arbres d'attaques ont depuis été grandement utilisés dans l'industrie et sont conseillés dans le rapport de l'OTAN de 2008 pour régir l'évaluation des menaces dans l'analyse de risque. Le modèle des arbres d'attaque est un sujet d'intérêt croissant dans la communauté des méthodes formelles avec de nombreuses d'approches différentes (voir le survey [4]).

Le premier modèle formel d'arbre d'attaque introduit dans [3] visait à décrire les attaques possibles sur un système par raffinement de l'objectif principal en sous-objectifs coordonnés soit avec l'opérateur OR soit avec l'opérateur AND. La sémantique sera ensuite augmentée ([1]) avec l'opérateur $SAND$ (pour "AND séquentiel"), qui exprime que les sous-objectifs doivent être atteints dans un ordre donné. En particulier, les auteurs de [1] introduisent une sémantique de chemins sur un système de transition.

Dans notre article [2], notre objectif est de proposer une nouvelle sémantique des arbres d'attaque plus réaliste : nous voulons que nos attaquants soient capables d'adapter leurs actions en fonction de l'environnement, donnant naturellement une sémantique à deux joueurs. Notre approche généralise [1] à un cadre de la théorie des jeux, menant à une sémantique de stratégie. Nous présentons ici un résumé de notre contribution.

2 Syntaxe des arbres d'attaque

Un *arbre d'attaque* est un modèle qui spécifie l'objectif d'un des deux joueur (l'*attaquant*). Etant donné un ensemble de propositions $Prop$, un arbre d'attaque sur $Prop$ est :

- soit une feuille composée d'une unique formule propositionelle ϕ sur $Prop$,
- soit une expression $OP(\tau_1, ..., \tau_n)$ où $\tau_1, ..., \tau_n$ sont des arbres d'attaque et OP est un opérateur parmis OR, AND ou $SAND$.

Nous modélisons un système multi-joueur, par une *arène de jeu concurrente* : un graphe fini sur lequel deux joueurs jouent un jeu de durée non bornée et où ils choisissent une action à chaque tour.

Exemple 2.1. Supposons que l'attaquant essaie de rentrer dans un bâtiment à deux portes d'entrée (d_1 et d_2), sans être vu par le garde qui contrôle l'accès à une des portes. Ce garde peut se déplacer d'une porte à l'autre, mais ne peut pas contrôler les deux portes en même temps. La situation est représentée par l'arène en Figure 1 où, dans chaque état, la première lettre représente la position de l'attaquant (o il est à l'extérieur du bâtiment, d_1 il est à la première porte, et d_2 il est à la seconde porte) et la deuxième lettre représente la position du garde (m il est en mouvement entre les deux portes, d_1 il est à la première porte, et d_2 il est à la seconde porte). Considérons l'ensemble $Prop = \{seen, d_1, d_2\}$ où d_1 et d_2 décrivent la position de l'attaquant et $seen$ est vrai dans les états (d_1, d_1) et (d_2, d_2), c'est-à-dire lorsque garde et le voleur sont à la même porte. L'objectif de l'attaquant est décrit par l'arbre $\tau = OR(d_1 \wedge \neg seen, d_2 \wedge \neg seen)$.

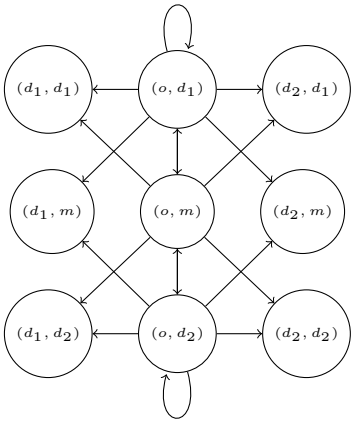

FIGURE 1 – Position du voleur et du garde

3 Sémantique de chemins

Remarquons qu'une arène de jeu peut être vue comme un système de transition $\mathcal{S}$ si on oublie les joueurs. La sémantique de chemins d'un arbre d'attaque τ est une sémantique (1 joueur) consistant en l'ensemble des chemins (suite d'états) du système de transition constituant un scénario favorable pour l'attaquant :

Définition 3.1 ([1])**.** La *sémantique de chemins* $Paths_{\mathcal{S}}(\tau)$ de τ sur le système $\mathcal{S}$ est définie inductivement :

- $Paths_{\mathcal{S}}(\phi)$ est l'ensemble des chemins terminant par un état où ϕ est vrai,
- $Paths_{\mathcal{S}}(OR(\tau_1, ..., \tau_n))$ est l'union des sémantiques des enfants,
- $Paths_{\mathcal{S}}(SAND(\tau_1, ..., \tau_n))$ est la concaténation des sémantiques des enfants,
- $Paths_{\mathcal{S}}(AND(\tau_1, ..., \tau_n))$ est obtenu par shuffle des sémantiques des enfants.

Exemple 3.2. Dans l'Exemple 2.1, la séquence d'états $(o, d_1)(o, m)(d_1, d_2)$ est un chemin dans la sémantique de la feuille $d_1 \wedge \neg seen$. Ce chemin est donc également dans la sémantique de $\tau = OR(d_1 \wedge \neg seen, d_2 \wedge \neg seen)$.

4 Sémantique de stratégies

Obtenir une sémantique compositionnelle représentant les stratégies que notre attaquant peut appliquer pour atteindre son objectif, peu importe le comportement du défenseur n'est pas immédiat, comme le montre l'exemple suivant.

Exemple 4.1. Dans l'Exemple 2.1, il n'existe aucune stratégie, ni pour l'objectif $d_1 \wedge \neg seen$, ni pour l'objectif $d_2 \wedge \neg seen$, puisque le garde peut décider de rester indéfiniment à la même porte. Toutefois, il existe bien une stratégie pour l'objectif $OR(d_1 \wedge \neg seen, d_2 \wedge \neg seen)$: il suffit d'attendre une unité de temps pour voir vers quelle porte le garde va se déplacer et ensuite d'entrer par l'autre porte.

La situation de l'Exemple 2.1 écarte une définition compositionnelle de la semantique de stratégies car nous ne pouvons pas déduire inductivement une sémantique non vide pour un arbre d'attaque alors que ses sous-arbres ont une sémantique vide. Nous utilisons donc la définition suivante.

Définition 4.2. Pour un arbre d'attaque τ, sa sémantique de stratégie $Strat_{\mathcal{G}}(\tau)$ est l'ensemble des stratégies assurant à l'attaquant de jouer des parties (chemins) se trouvant dans $Paths_{\mathcal{S}}(\tau)$.

5 Problèmes de décisions

Nous avons étudié deux problèmes de décisions.

Définition 5.1. Le problème de *non-vacuité* (NV) pour une sémantique fixée d'arbre d'attaque $[\![\cdot]\!]_{\mathcal{G}}$ est le problème de décision suivant :
Entrée : $\mathcal{G}$, une arène de jeu, τ, un arbre d'attaque.
Sortie : Oui si $[\![\tau]\!]_{\mathcal{G}} \neq \emptyset$, Non sinon.

Définition 5.2. Le problème de *l'appartenance* (A) pour une sémantique fixée d'arbre d'attaque $[\![\cdot]\!]_{\mathcal{G}}$ de type X (chemins ou stratégies) est le problème de décision suivant :
Entrée : $\mathcal{G}$, une arène de jeu, τ, un arbre d'attaque et $x \in X$.
Sortie : Oui si $x \in [\![\tau]\!]_{\mathcal{G}}$, Non sinon.

Où $[\![\tau]\!]_{\mathcal{G}}$ fait référence à soit la sémantique de chemins, soit la sémantique de stratégie. Les résultats sont repris dans la table suivante où [2] est notre contribution.

	sémantique de chemin	sémantique de stratégie
NV	NP-**complet** [1] (SMP* et réduction de SAT)	PSPACE-**complet** [2] (algorithme alternant polynomial et réduction de QBF)
A	P [2] (Backward induction)	coNP-**complet** [2] (SMP et réduction de UNSAT)

(*) Small model property.

Ce travail a été en partie soutenu par le Fonds de la Recherche Scientifique - FNRS sous la subvention n°T.0027.21.

Références

[1] Maxime Audinot, Sophie Pinchinat, and Barbara Kordy. Is my attack tree correct ? In *European Symposium on Research in Computer Security*, pages 83–102. Springer, 2017.

[2] Thomas Brihaye, Sophie Pinchinat, and Alexandre Terefenko. Adversarial formal semantics of attack trees and related problems. In Pierre Ganty and Dario Della Monica, editors, *Proceedings of the 13th International Symposium on Games, Automata, Logics and Formal Verification, GandALF 2022, Madrid, Spain, September 21-23, 2022*, volume 370 of *EPTCS*, pages 162–177, 2022.

[3] Bruce Schneier. Attack trees. *Dr. Dobb's journal*, 24(12) :21–29, 1999.

[4] Wojciech Wideł, Maxime Audinot, Barbara Fila, and Sophie Pinchinat. Beyond 2014 : Formal methods for attack tree–based security modeling. *ACM Computing Surveys (CSUR)*, 52(4) :1–36, 2019.