Séminaire Mathématique de Béjaïa (LaMOS)
Volume 18, 2020, pp. 107 - 110

6

Jeux Bayésiens et applications

Bouibed K.

Research Unit **LaMOS** (Modeling and Optimization of Systems) and Faculty of Exact Sciences, Bejaia University, Bejaia 06000, Algeria

Résumé Jeux Bayésiens (également connus sous le nom des jeux à informations incomplètes) sont des modèles de situations de décisions interactives où les décideurs (joueurs) n'ont que des informations partielles sur les données de jeu et sur les autres joueurs. Ce travail présente quelques applications des jeux Bayésiens dans les réseaux informatiques, notamment l'interaction entre les fournisseurs de services (les serveurs) et les clients inconnus et la modélisation de problèmes de sécurité dans les réseaux Ad Hoc.

Mots clés : Jeux Bayésiens, Jeux de sécurités, Reseaux Ad Hoc.

6.1 Définition d'un jeu Bayésien

Definition 1 *[2] Un jeu statique Bayésien est donné par :*

$$(J_B) = \langle\ I,\ (A_i)_i,\ (\Theta_i)_i,\ (f_i)_i,\ P\ \rangle, \tag{6.1}$$

- *avec $I = \{1, ..., i, ..., n\}$ est l'ensemble des joueurs,*
- *Θ_i est l'ensemble de types du joueur i, le type $\theta_i \in \Theta_i$ (appelé aussi caractéristique, état d'information,...) résume l'information dont dispose le joueur i avant de jouer. $\theta = (\theta_1, ..., \theta_i, ...\theta_n)$ de $\Theta = \prod_{i=1}^{n} \Theta_i$ représente donc l'information totale dont disposeraient les joueurs s'ils la mettaient en commun.*
- *Une distribution de probabilité a priori P sur Θ.*
- *L'ensemble des actions A_i, la fonction d'utilité (gain) f_i définie sur $A \times \Theta$ avec $f_i(a, \theta)$ est le niveau d'utilité atteint par le joueur i si les actions $a = (a_1, ..., a_i, ..., a_n)$ ont été choisies et si les types sont $\theta = (\theta_1, ..., \theta_i, ..., \theta_n)$.*

Un jeu Bayésien est la donnée d'une famille des jeux paramétrés par les types des joueurs et une distribution a priori sur ces types lors du jeu. Une valeur précise de θ est réalisée mais en général les joueurs ne savent pas exactement laquelle.
Ces jeux tiennent leur nom de l'application de la règle de Bayes. Ainsi, les jeux à information incomplète sont de ce fait transformés en des jeux à information imparfaite.

6.1.1 Déroulement du jeu selon Harsanyi

Harsanyi a considéré que la caractéristique θ_i est la réalisation d'une variable aléatoire et représente le résultat du choix d'un nouvel agent (joueur) appelé Nature.
D'abord, la nature fait un tirage de tous les types $\theta_1, ..., \theta_i, ..., \theta_n$ selon la distribution commune

$P(\theta_1, ..., \theta_i, ..., \theta_n)$ et le type tiré θ_i est communiqué au joueur i de manière confidentielle. Ensuite, chaque joueur choisit son action en fonction de son type et de la probabilité.
Avec cette approche on définit un jeu Bayésien qui se déroule comme suit :

1. La nature procède au tirage aléatoire du vecteur $\theta = (\theta_1, ..., \theta_i, ...\theta_n)$ par la fonction de distribution jointe à partir de laquelle le tirage est effectué. $P(\theta)$ est une connaissance commune à tous les joueurs ;
2. La nature révèle le type θ_i au seul joueur i. En connaissant P et θ_i, chaque joueur i peut en déduire des croyances $P_i(\theta_{-i} \ / \ \theta_i)$ sur la valeur θ_{-i} du type des autres joueurs en faisant appel à la règle de Bayes :

$$P_i(\theta_{-i} \ / \ \theta_i) \ = \frac{P(\theta_{-i},\ \theta_i)}{P(\theta_i)} = \frac{P(\theta_{-i},\ \theta_i)}{\sum\limits_{\theta_{-i}} P(\theta_{-i},\ \theta_i)},\ (P(\theta_i) \neq 0);$$

3. Chaque joueur choisit une action de son espace A_i, ce choix se fait en fonction du type θ_i ;
4. Chaque joueur i reçoit un paiement qui depent non seulement du profil de stratégies pures $x = (x_1, ..., x_i, ..., x_n)$ mais également de sa caractéristique privée $\theta_i \in \Theta_i$ elle prend donc la forme $f_i(x_i,\ x_{-i}, \theta_i)$.

6.2 Application des jeux Bayésiens à la sécurité des réseaux informatiques

L'interaction entre le fournisseur de services (le serveur) et un client inconnu est modélisée par un jeu Bayésien dynamique à deux joueurs. En considérant deux types de clients, les clients malveillants et les clients normaux. Le jeu Bayésien proposé (appelé jeu de sécurité (JS)) à deux joueurs : un serveur s et un client c [1].
On considère deux types ($\theta_c = 0$, désigne un client régulier et $\theta_c = 1$, désigne un client malveillant où un attaquant) pour les clients de serveur, le type de serveur est toujours $\theta_s = 0$, le joueur s a deux stratégies (défendre et ne pas défendre) et le joueur c a aussi deux stratégies (attaquer et ne pas attaquer). La nature des communications entre le serveur et le client est répétée et jouée aux temps $t = 0, 1, 2, ..., T$. Différents paquets sont envoyés par le client au serveur et vice versa. Chaque paquet et les réponses peuvent être considérés comme une étape du jeu de sécurité (JS). Les gains des deux joueurs sont donnés comme suit

(a) Le joueur c est régulier

Joueur s \ Joueur c	Ne pas attaquer	Attaquer
Ne pas défendre	$(0, 0)$	$(0, 0)$
Défendre	$(-\alpha, -\beta)$	$(-\alpha, -\beta)$

(b) Le joueur c est un attaquant

Joueur s \ Joueur c	Ne pas attaquer	Attaquer
Ne pas défendre	$(-G', G' - \tau')$	$(-G, G - \tau)$
Défendre	$(g' - G' - \alpha, G' - g' - \tau')$	$(g - G - \alpha, G - g - \tau)$

Avec α est le coût de la stratégie défendre, on quantifier la dégradation de service par β.
τ, $\tau^{'}$ les coûts de l'attaquant lorsque il joue respectivement attaquer et ne pas attaquer avec $\tau' \geq \tau$.
G (resp G') est l'information acquise par l'attaquant lorsque il joue attaquer (resp. ne pas attaquer) avec $G \geq G'$, g (resp g') la prévention de la fuite de l'information lorsque l'attaquant joue la stratégie attaquer (resp. ne pas attaquer) avec $g \geq g'$.

L'objectif de l'analyse du jeu de sécurité (JS) est de proposer une probabilité optimale de jouer la stratégie défendre pour le serveur où il est incertain sur le type de son client.

6.3 Jeux Bayésiens pour la détection d'intrusion dans les réseaux mobile Ad Hoc

On considère un réseau Ad Hoc avec N noeud. Chaque noeud défenseur est équipé d'un système de détection d'intrusion (IDS). Le joueur i est un noeud attaquant et le joueur j est un noeud défenseur. Le joueur i a des informations privées sur son type, soit régulier, noté par $\theta_i = 0$, ou malveillant, noté par $\theta_i = 1$. Le défenseur j est du type régulier $\theta_j = 0$. Le type du défenseur j est une connaissance commune des deux joueurs. Le joueur i du type malveillant a deux stratégies pures : attaquer et ne pas attaquer. Le joueur i du type régulier a une stratégie pure : ne pas attaquer. Le joueur j a deux stratégies pures : surveiller et ne pas surveiller [3]. Les gains des deux joueurs sont donnés comme suit

(a) Le joueur i est malveillant

joueur i \ joueur j	Surveiller	Ne pas surveiller
Attaquer	$((1-2\alpha)w - c_a, (2\alpha - 1)w - c_s)$	$(w - c_a, -w)$
Ne pas attaquer	$(0, -\beta w - c_s)$	(0,0)

(b) Le joueur i est régulier

joueur i \ joueur j	Surveiller	Ne pas surveiller
ne pas attaquer	$(0, -\beta w - c_s)$	(0,0)

– où w la valeur de sécurité du défenseur j, $-w$ représente une perte de sécurité dont la valeur est équivalente à un degré de dommages.

- α représente le taux de détection de l'IDS, β représente la fausse alarme de l'IDS avec $\alpha,\ \beta \in [0, 1]$.
- Les coûts des attaques et des surveillances sont indiqués respectivement par c_a et c_s, où $c_a, c_s > 0$ avec $w > c_a, c_s$.
- Soit μ_0 la croyance du joueur j sur le type malveillant du joueur i.

Supposons que μ_0 est une connaissance commune, si la croyance du défenseur j sur le joueur i malveillant est assez élevée : $\mu_0 > \frac{\beta w+c_s}{(2\alpha+\beta)w}$, le jeu Bayésien statique n'a pas d'équilibre en stratégies pures. Mais il possède un équilibre en stratégies mixte $((p^*$, si i est malveillant, ne pas attaquer si i régulier), $q^*,\ \mu_0))$, avec $p^* = \frac{\beta w+c_s}{(2\alpha+\beta)w\mu_0}$ est la probabilité que le noeud malveillant i joue la stratégie attaquer et $q^* = \frac{w-c_a}{2\alpha}$ est la probabilité que le noeud défenseur j joue surveiller. Si la croyance du défenseur j sur le joueur i malveillant est très faible $\mu_0 < \frac{\beta w+c_s}{(2\alpha+\beta)w}$, un équilibre en stratégies pures existe ((attaquer si malveillant, ne pas attaquer si régulière, ne pas surveiller, $\mu_0)$).

L'avantage d'utiliser un modèle du jeu Bayésien statique est que, au lieu d'appliquer une surveillance permanente IDS, le défenseur peut mettre en oeuvre une stratégie selon sa solution d'équilibre Bayésien qui maximise son gain espéré, mais un inconvénient possible dans la pratique est la difficulté d'attribuer des probabilités a priori (μ_0) précises sur le type du joueur i. Pour remédier à ce problème, le modèle a été étendu à un jeu Bayésien dynamique, où le défenseur mit à jour ses croyances selon l'évolution du jeu, c'est à dire le défenseur j mit à jour ses croyances sur les types de son adversaire i à la fin de chaque étape du jeu en calculant ses croyances a postériori en tenant compte de l'histoire du profil d'actions du joueur i.

Références

1. S. Farhang, M.H. Manshaei, M.N. Esfahani and Q. Zhu : A dynamic Bayesian security game framework for strategic defense mechanism design. R. Poovendran and W. Saad (Eds.) : Game Sec 2014, LNCS 8840 319–328, (2014).
2. J.C. Harsanyi : Game with incomplete information played by "Bayesian" players, I. The basic model. Management science 14 :317-334, (1967).
3. Y. Liu, C. Comaniciu and H. Man : A Bayesian game approach for intrusion detection in wireless Ad Hoc networks. Game Nets'06, October14, 2006, Pisa, Italy. Copyright ACM 1-59593-507-X/06/10, (2006).