République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

جامعة بجاية
Tasdawit n Bgayet
Université de Béjaïa

Université A/Mira de Béjaia
Faculté des Sciences Exactes
Département de Recherche Opérationnelle

Mémoire de Master

En
Mathématiques Appliquées

Option
Modélisation Mathématique et Techniques de Décision

SUJET

Application des jeux Bayésiens dans la sécurité des réseaux ad hoc

Présenté par :

LAMRI Fraoussene & HADDADI Razika

Soutenu le 07 Juillet 2019 devant le jury composé de :

Présidente	Dr S. Boulfekhar	Maître de Conf. A	U. A/Mira Béjaia.
Promotrice	Dr K. Bouibed	Maître de Conf. B	U. A/Mira Béjaia.
Examinateur	Dr N. Khimoum	Maître de Conf. B	U. A/Mira Béjaia.
Examinatrice	Dr A. Anzi	Maître de Conf. B	U. A/Mira Béjaia.

Promotion 2018/2019.

⁕ *Remerciements* ⁕

Nous remercions Dieu (sans Lui rien n'aurait pu être possible) tout puissant de nous avoir accordé santé, courage et la volonté pour accomplir ce modeste travail.

Nous tenons également à remercier notre Promotrice M^{elle} **Karima BOUIBED** pour ses précieux conseils, sa disponibilité et ses encouragements qui nous ont poussés à donner le meilleur de nous-même tout au long de la préparation de ce mémoire.

Nous voudrions également remercier le président et les membres de jury d'avoir accepter de juger notre travail et de consacrer leur temps à la lecture et à la correction de ce mémoire.

Nos remerciements les plus vifs vont tout particulièrement à nos parents et à nos familles.

⁂ *Dédicaces* ⁂

Je dédie ce modeste travail :

A mon source de courage, mes trés chers parents,

A toutes ma famille,

A tous mes professeurs,

A tous mes ami(e)s, et particulièrement : Anis, Celia et Mitcho.

M. ***Lamri fraoussene***

⁕ *Dédicaces* ⁕

Je dédie ce modeste travail :

A mes parents, les deux êtres les plus chers à mon cœur.

A mon grand-père et grand-mère.

A mes frères et sœurs.

A mon ange Wassim.

A ma belle Celia.

A mes ami(e)s.

Mlle. ***Haddadi razika***

TABLE DES MATIÈRES

TABLE DES FIGURES

LISTE DES ABRÉVIATIONS

ENB : Équilibre Nash Bayésien.
EBP : Équilibre Bayésien Parfait.
PAN : Personal Area Network.
LAN : Local Area Network.
MAN : Metropolitan Area Network.
WAN : Wide Area Network.
GAN : Global Area Network.
VPN : Virtuel Private Network.
IEEE : Institue of Electrical and Electronics Engineers.
Wifi : Wireless Fidelity.
MANET : Mobile Ad hoc NETwork.
GSM : Global System for Mobile communications.
UTM : Unified Threat Management.
URL : Uniform Resource Locator.
IDS : Intrusion Detection System.
IPS : Intrusion Prevention System.
HIDS : Host-based Intrusion Detection System.
NIDS : Network Intrusion Detection Systems.
DTN : Delay Tolerant Network.

INTRODUCTION GÉNÉRALE

La théorie des jeux est une discipline mathématique qui étudie les conflits entre plusieurs agents rationnels afin de prédire l'évolution ou de conseiller les individus sur la meilleure stratégie à adopter. Le champ d'application de cette discipline est très vaste. Elle a été appliquée pour la première fois dans les sciences économiques. Par la suite, il a été aperçu que les jeux sont présents dans des domaines aussi inattendus que la biologie, la sociologie ou l'informatique. Depuis son apparition, la théorie des jeux classique a connu un grand intérêt notamment chez les économistes, les sociologues et les philosophes pour pouvoir étudier et analyser le comportement des individus dans la vie réelle. À partir de 1920, la théorie des jeux a été développée principalement par Von Neumann cela dit, avant eux il y'a eu Cournot et Edgeworth qui avaient commencé à travailler dans ce sens. Et en 1944, la théorie des jeux est née "officiellement" avec l'ouvrage fondateur "Theory of Games and Economic Behavior" du mathématicien Von Neumann et de l'économiste Oskar Morgenstern[30]. Cette théorie prend comme hypothèse principale la rationalité forte des individus. Chaque individu cherche à maximiser ses gains personnels en prenant en considération le comportement de ses adversaires. La théorie classique cherche à trouver la meilleure solution pour résoudre les conflits. Dans ce cadre, les théoriciens des jeux ont introduit la notion d'équilibre (Nash notamment). Cette notion peut conduire chaque individu à une situation de non regret, mais elle ne peut pas lui garantir un gain optimal.

Un jeu est une modélisation mathématique d'une situation réelle, sa représentation se fait à base de l'information qui est généralement imparfaite et pleine d'incertitude. En générale, les joueurs ne peuvent pas évaluer avec certitude une ou plusieurs données du jeu. Pour remédier à cette insuffisance de la théorie des jeux, Harsany a introduit les jeux à information incomplète (jeux Bayésiens). Un jeu bayésien est un jeu dans lequel l'information dont dispose chaque joueur sur les caractéristiques des autres joueurs est incomplète. En particulier, on représente ainsi un jeu dans lequel un ou plusieurs joueurs font face à une incertitude quant au gain des autres joueurs. Cette situation impose de spécifier pour chaque joueur des croyances concernant les caractéristiques des autres joueurs. Harsanyi a été le premier à introduire la notion de type. Un type dans le point de vue de Harsanyi, est une sorte d'état d'esprit. Il contient non seulement la croyance du joueur sur l'état de la nature mais aussi sur sa croyance sur la croyance des autres, et la croyance du joueur sur la croyance des autres sur sa croyance, etc. Cependant, Harsanyi [12] et [13] ne donna pas une construction rigoureuse de cette idée. Cela a été fait une vingtaine d'années plus tard par Mertens et Zamir [19].

Dans les réseaux mobiles ad hoc ou MANET (Mobile ad hoc NETwork), aucune infrastructure réseau fixe n'existe, et la gestion est totalement distribuée. Les nœuds peuvent se déplacer aléatoirement, et par conséquent la topologie du réseau change aussi rapidement et aléatoirement. Les nœuds ne peuvent communiquer qu'avec leurs nœuds voisins, de proche en proche, et les nœuds intermédiaires doivent coopérer pour l'acheminement des paquets de données (tous les nœuds jouent le rôle de routeur). Cependant, dû au dynamisme du réseau et à la mobilité des nœuds, ce voisinage change aussi dynamiquement.

Plusieurs difficultés sont rencontrées dans les réseaux ad hoc telles que le problème de routage, la contrainte d'énergie, la bande de fréquence limitée et la sécurité. Les modèles analytiques pour évaluer la performance des réseaux ad hoc ont été rares en raison de la nature distribuée et dynamique de ces réseaux. La théorie des jeux offre une suite d'outils qui peuvent être utilisés efficacement dans la modélisation de l'interaction entre les nœuds indépendants.

On se pose alors les trois questions suivantes :

- Comment modéliser le problème de la sécurité dans les réseaux ad hoc les jeux Bayésiens ?
- Quel est le concept de solution approprié ?
- Quelles sont les étapes de résolution de ce jeu ?

Afin d'apporter des réponses à ces questions, on a procédé comme suit :

Dans le premier chapitre, nous donnerons quelques rappels sur la théorie des jeux classique, ainsi que quelques concepts d'équilibre des jeux non coopératifs sous forme normale notamment l'équilibre de Nash.

Nous enchaînerons avec le second chapitre qui portera sur les principales notions des jeux Bayésien, on a rappelé dans un premier temps les définitions de base des jeux Bayésiens statiques, les stratégies, les gains des joueurs, notamment le concept d'équilibre étudié pour ce type de jeu et quelques exemples d'applications. Puis, nous avons présenté aussi les éléments essentiels des jeux Bayésiens dynamiques plus particulièrement les jeux Bayésiens répétés qui seront utiles pour aborder le quatrième chapitre.

Le troisième chapitre sera consacré en une introduction aux réseaux informatiques en général et aux réseaux ad hoc en particulier où nous présenterons les différentes notions qui leurs sont liées nous passerons ensuite à la définition de la sécurité informatique et ses objectifs ainsi que les techniques de défense et principales attaques. Nous avons cité les objectifs d'utilisation de la théorie des jeux pour modéliser les réseaux ad hoc et différents avantages d'application de cette théorie dans ce domaine.

La contribution essentielle de notre travail sera présentée dans le dernier chapitre. Elle consiste en un modèle permettant de répondre aux besoins des réseaux ad hoc en termes de sécurité. Nous commencerons d'abord par donner une présentation détaillée du modèle où nous appliquerons les jeux Bayésiens pour modéliser le comportement stratégique des nœuds, notre objectif est de déterminer s'il est essentiel de toujours laisser le système IDS fonctionner sans compromis sur son efficacité. Tout d'abord, nous modélisons l'interaction entre le système de détection d'intrusion et un attaquant comme un jeu Bayésien statique . Deuxièmement, nous modélisons ce jeu comme un jeu Bayésien dynamique, où IDS n'a pas de probabilités préalables fixes quant au type de son adversaire et peut mettre à jour ses croyances à la fin de chaque étape du jeu et montrons que ce jeu admet un équilibre Bayésien parfait en stratégies mixtes. Ensuite nous illustrons les résultats de cette étude.

Nous terminons ce mémoire par une conclusion, où nous relaterons les principaux résultats obtenus dans le cadre de notre travail qui se base sur l'approche de la théorie des jeux, ainsi que quelques propositions de travaux futurs à développer.

CHAPITRE 1

GÉNÉRALITÉS SUR LA THÉORIE DES JEUX

1.1 Introduction

La théorie des jeux consiste à étudier les situations de conflits qui peuvent exister entre des agents en interaction. Elle a connu une véritable explosion au cours de ces dernières années aussi bien sur le plan théorique qu'au niveau des applications. Elle est devenue un outil central dans plusieurs disciplines comme l'économie, la biologie, le transport routière et les réseaux informatique , etc...

Ce chapitre sera consacré à la présentation de notions de base de la théorie des jeux et quelques concepts de solutions les plus étudié pour les jeux sous forme normale.

1.2 Qu'est ce qu'un jeu ?

Un jeu est une situation où des agents (les joueurs) sont conduits à faire des choix parmi un certain nombre d'actions possibles et dans un cadre défini à l'avance (les règles du jeu). Les résultats de ces choix constituent une issue du jeu à laquelle est associée un gain pour chacun des participants. Ces résultats ne dépendent pas de la décision d'un seul joueur, mais plutôt de celles de tous les autres avec la possibilité que le hasard intervient.

1.2.1 Composantes d'un jeu

Un jeu est un ensemble de règles qui encadre ou contraint le comportement des joueurs et qui détermine leurs utilités sur la base des actions entreprises. Selon cette terminologie, un jeu suppose une définition claire des règles de comportements des joueurs qui spécifient :

Joueurs : un joueur est une personne physique, une société ou encore la nature, ou bien généralement un preneur de décision, agissant au mieux pour son intérêt selon le principe de la rationalité individuel. Dans un jeu on peut distinguer un ensemble de N joueurs, chacun des joueurs est caractérisé par un indice i, $i = \{1, 2, ..., N\}$ avec $N \geq 2$.

Stratégies : une stratégie est un plan d'actions spécifiant l'ensemble des décisions que doit prendre le joueur au cours du jeu. Il existe différent type de stratégie :

- **Stratégie pure :** une stratégie pure du joueur i est un plan d'action qui prescrit une action de ce joueur pour chaque fois qu'il est susceptible de jouer. On note

par S_i l'ensemble des stratégies pures du joueur i et par s_i une stratégie pure de ce joueur et on note par $s_{-i} = (s_1, ..., s_{i-1}, s_{i+1}, ..., s_N)$ l'ensemble des stratégies de tous les joueurs, sauf la stratégie du joueur i ;

- **Stratégie mixte :** une stratégie mixte pour le joueur i est une distribution de probabilités sur son ensemble de stratégies pures. $\alpha = (\alpha_1, \alpha_2, ..., \alpha_N)$ telle que

$$\alpha_i \geq 0, \forall i = 1, ..., N, \quad \sum_{i=1}^{N} \alpha_i = 1.$$

où α_i est la probabilité que le joueur i joue sa stratégie pure $s_i \in S_i$.
On notera par

$$\Delta_N = \{\alpha = (\alpha_1, \alpha_2, ..., \alpha_N) \in \mathbb{R}^N, \quad \sum_{i=1}^{N} \alpha_i = 1; \alpha_i \geq 0, \forall i = 1, ..., N\}.$$

l'ensemble des stratégies mixtes du joueur i.

- **Stratégie de comportement :** Une stratégie de comportement $\hat{\gamma}^i$ pour le $i^{ème}$ joueur est une application $\hat{\gamma}^i(.) : E^i \to Y$ qui assigne un élément de Y à tout ensemble d'information de E^i tel que

$$\hat{\gamma}^i(\eta^i) \in Y_{\eta^i}, \qquad \forall \eta^i \in E^i.$$

Remarque 1. *Toute stratégie de comportement est une stratégie mixte, mais il existe des stratégies mixtes qui ne sont pas des stratégies de comportement[25].*

Utilité (gain) : pour chaque joueur i correspond une fonction d'utilité u_i

$$u_i : S_1 \times ... \times S_N \longrightarrow \mathbb{R}$$

qui associe un gain pour chaque profil de stratégie $s = (s_1, s_2, ..., s_N)$.

Rationalité : on dit qu'un joueur possède un comportement rationnel s'il est conscient des alternatives et choisit délibérément la stratégie qui lui est le plus favorable parmi son ensemble d'actions.

Si le hasard ou la chance est présente dans le jeu et peut affecter le déroulement du jeu, il est courant de la transformer en un joueur fictif nommé "chance" ou "nature".

1.3 Classification générale des jeux :

La théorie des jeux utilise des approches très variées. Nous pouvons citer, entre autres, les modèles coopératifs ou non coopératifs, les jeux à un seul coup ou répétés, et les jeux à horizon fini ou infini, ainsi que les jeux à information complète et incomplète.
Les jeux sont largement utilisés dans différents domaines et pour modéliser des situations très variée, ceci induit qu'au sein même des différentes classes de jeux énoncées plus haut, il existe plusieurs types et peuvent être classés suivant différents critères :

1.3.1 Selon le comportement des joueurs :

Jeu coopératif : un jeu est dit coopératif si les joueurs peuvent passer entre eux des accords qui les lient de manière contraignante ou leur stratégie est décidée en commun,

afin d'améliorer le gain de tous les joueurs coalisés [21], c'est le cas par exemple, si les joueurs s'accordent sur un contrat, un accord devant une autorité,...etc, où il est prévu une sanction (punition) légale en cas de non-respect du contrat ou de l'accord.

Jeu non coopératif : les jeux non coopératifs correspondent à des situations dans lesquelles chaque joueur arrête seul ses choix stratégiques sans consulter les autres joueurs, et n'offrent pas la possibilité d'une coopération formelle ou liante.

1.3.2 Selon le nombre de coups :

Les choix effectués par les joueurs dans un jeu peuvent être simultanés ou séquentiels. Cette distinction met en évidence deux types de jeux que l'on peut définir comme suit :

Jeux sous forme stratégique (ou normale) :

Le modèle de jeux sous forme stratégique supprime la structure séquentielle de la prise de décision. Quand elle est appliquée à des situations dans lesquelles les preneurs de décisions jouent séquentiellement, elle oblige à supposer que les joueurs choisissent leur stratégie une fois pour toute. Ils sont alors engagés dans cette stratégie et ne peuvent pas la modifier à mesure que le jeu se déroule. Cette modélisation est toutefois très utile pour décrire des situations dans lesquelles les joueurs jouent en même temps.

Définition 1.3.1. ***(Jeu sous forme normale à N joueurs)***
Un jeu sous forme normale est décrit par le jeu

$$\langle \mathbb{N}, \{S_i\}_{i\in\mathbb{N}}, \{u_i\}_{i\in\mathbb{N}} \rangle. \tag{1.1}$$

Où

- $\mathbb{N}$ *est l'ensemble des joueurs.*
- S_i *est l'ensemble des stratégies du joueur* i, $i \in \mathbb{N}$.
- u_i *est la fonction de gain du joueur* i, $i \in \mathbb{N}$.

Exemple 1. ***(Le dilemme du prisonnier)***
Deux suspects d'un crime majeur sont détenus dans des cellules séparées. La police a assez de preuves pour condamner chacun d'entre eux pour des crimes mineurs mais pas assez pour les condamner pour le crime majeur, à moins que l'un d'entre eux ne dénonce l'autre. Si les deux suspects se taisent, ils seront chacun condamnés à un an de prison. Si seulement l'un d'entre eux dénonce l'autre, il sera libéré et utilisé en tant que témoin contre l'autre qui écopera de 10 ans de prison. Enfin si les deux dénoncent, ils passeront chacun 5 ans en prison.
Ce jeu peut être représenté comme un jeu stratégique où :

- *les joueurs sont les deux suspects.*
- *Chacun de deux suspect a le choix entre deux actions : {S : Se taire , D : Dénoncer}.*
- *On suppose que les préférences des joueurs sont uniquement déterminées par les années qu'ils passeront en prison. Ainsi :*
  $u_1(D,S) > u_1(S,S) > u_1(D,D) > u_1(S,D)$
  et $u_2(S,D) > u_2(S,S) > u_2(D,D) > u_2(D,S)$
  Par exemple, on peut spécifier :

$u_1(D,S) = 0, u_1(S,S) = -1, u_1(D,D) = -5, u_1(S,D) = -10.$
Et de manière similaire
$u_2(S,D) = 0, u_2(S,S) = -1, u_2(D,D) = -5, u_2(D,S) = -10$
Il est usuel de représenter un jeu fini à deux joueur sous forme stratégique par le tableau des gains. Le jeu peut alors être représenté comme suit :

Suspect 1 \ Suspect 2	Se taire	Dénoncé
Se taire	(-1 ;-1)	(-10 ;0)
Dénoncé	(0 ;-10)	(-5 ;-5)

TABLE 1.1 – Le dilemme du prisonnier

Jeux sous forme dynamique (extensive) :

La modélisation sous forme extensive est l'un des moyens les plus simples de représenter un jeu. Il s'agit d'un modèle où les joueurs choisissent séquentiellement leurs actions, jusqu'au moment où le jeu est déclaré fini.

Remarque 2. *La représentation par la forme extensive est généralement utilisée pour les jeux séquentiels car l'ordre des coups est clairement décrit.*

Représentation graphique :

Tout jeu sous forme extensive peut être représenté par un arbre (graphe connexe sans cycle) où :

- à chaque nœud terminal correspond un résultat du jeu,
- à chaque nœud non terminal est associé un joueur : arrivé à ce point du jeu, c'est à son tour de jouer,
- Chaque arc représente chacune des actions que ce joueur peut prendre à ce point du jeu.

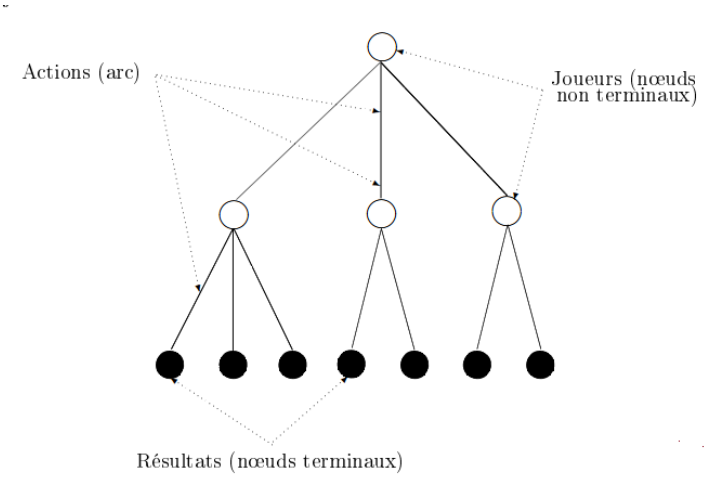

FIGURE 1.1 – L'arbre de la représentation graphique

Exemple 2. *Soit un jeu à deux joueurs, dans lequel chaque joueurs a deux actions possibles : aller à droite ou aller à gauche. Le joueur 1 joue en premier. Chaque joueur préfère être à droite si l'autre y est aussi, sinon il préfère être à gauche.*

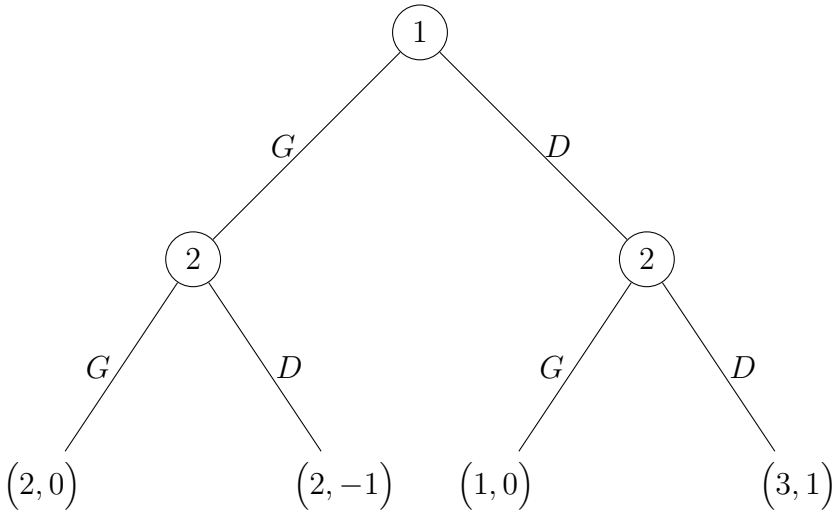

FIGURE 1.2 – Jeu séquentiel

L'introduction du joueur Nature :

Le modèle de jeu sous forme extensive avec information parfaite ne permet pas de rendre compte d'événements aléatoires pouvant intervenir durant le jeu. Cependant, il peut être aisément étendu pour couvrir de telles situations. La définition d'un jeu sous forme extensive avec joueur "Nature" est une variante de la définition précédente dans laquelle :

- la fonction du joueur assigne la "Nature" à certaine sous-séquences (on ajoute un nouveau joueur).
- les probabilités de chacune des actions de la "Nature" sont spécifiées.
- les préférences des joueurs sont définies sur l'ensemble des loteries d'histoires terminales (et non plus sur les histoires terminales elles-mêmes). Pour que l'analyse reste simple, on supposera que les événements aléatoires après une certaine histoire (sous-séquence) sont indépendants des événements aléatoires après les autres sous-séquences.

Exemple 3. *Considérons un jeu à deux joueurs dans lequel le joueur 1 doit d'abord choisir entre les actions A et B. S'il choisit A le jeu s'arrête avec des gains (1,1). Si il choisit B :*

- *avec probabilité 1/2, le jeu s'arrête et les gains sont (3,0).*
- *et avec probabilité 1/2, le joueur 2 peut choisir entre les actions.*
- *C qui donne un gain (0,1).*
- *et D qui donne un gain (1,0).*

Un jeu sous forme extensive qui modélise cette situation peut être représente comme suit :

Où N représente le joueur "Nature" et où les nombres à côté des actions de N représentent la probabilité que cette action soit "choisie".

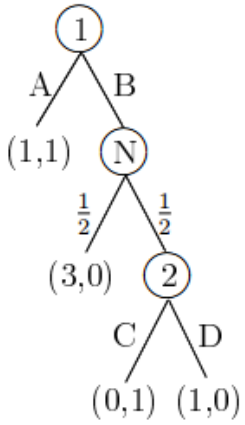

FIGURE 1.3 – Exemple sur l'introduction du joueur Nature

1.3.3 Selon la nature de l'information :

Jeux à information parfaite

Un jeu est à information parfaite, si chaque joueur, au moment de choisir sa stratégie, a une connaissance parfaite de l'ensemble des décisions prises antérieurement par les autres joueurs. La représentation qui semble appropriée à ce type de jeux est la forme extensive[14].

Jeux à information imparfaite

Contrairement au type précédent, ici les joueurs n'interviennent pas les uns après les autres. Autrement dit, les règles du jeu stipulent l'existence de coups simultanés, ce qui revient à introduire une certaine imperfection au niveau de l'information dont disposent les joueurs. La représentation qui apparaît comme la plus appropriée pour chaque coup est la forme normale

Exemple 4. *Chacun des deux joueurs commence par mettre un euro dans le pot. On donne au joueur 1 une carte qui peut être Haute avec probabilité q ou Basse avec probabilité* $(1-q)$*. Il observe la carte mais le joueur 2 ne l'observe pas. Il peut "laisser" ou "monter". Si il "laisse", le joueur 2 prend le pot et le jeu s'arrête. Si le joueur 1 "monte", il rajoute 1 Euro dans le pot et le joueur 2 a le choix entre "passer" et "suivre". Si il passe, le joueur 1 prend le pot. Si le joueur 2 "suit", il ajoute 1 Euro dans le pot et le joueur 1 montre la carte. Si elle est Haute, le joueur 1 prend le pot, sinon le joueur 2 le prend.*
Ce jeu peut être représenté comme suit :

Le joueur 1 a deux ensembles d'information, un contenant l'histoire unique Haute et l'autre contenant l'histoire unique Bas. Le joueur 2 a un ensemble d'information qui consiste en deux histoires : $\{Haute, Monter\}$ *et* $\{Basse, Monter\}$*. Cet ensemble d'information repète le fait que le joueur 2 ne peut pas observer le carte du joueur 1 . Notez ici que la condition qui veut que l'ensemble des actions disponibles après chaque histoire d'un ensemble d'information soit le même est ici satisfaite.*

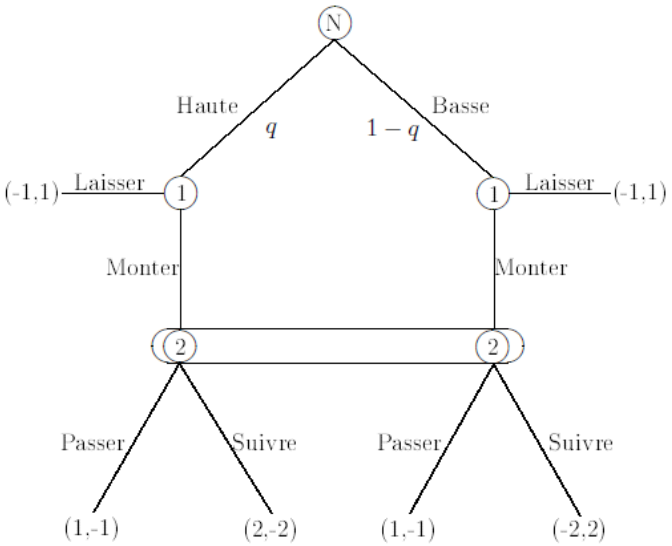

FIGURE 1.4 – La forme extensive avec un coups simultané

Jeux à information complète

Les premiers jeux étudiés par Von Neumann et Morgenstern [30] furent des jeux à information complète. On dit qu'un jeu est à information complète si chaque joueur connaît lors de la prise de décision : l'ensemble des joueurs, l'ensemble de ses stratégies ainsi que l'ensemble des stratégies des autres joueurs et les motivations ou les fonctions objectifs de tous les autres joueurs. Dans ce cas, on dit aussi qu'il y a connaissance commune de la structure du jeu de la part de tous ceux qui y participent [32].

Jeux a information incomplète

Si l'une des conditions dans la définition précédante n'est pas vérifiée, le jeu est dit à information incomplète (appelé aussi jeu bayésien). Un travail de pionnier a été réalisé par Harsanyi [12], l'auteur montre que si l'on suppose que chaque joueur dispose d'une distribution de probabilités subjectives sur les caractéristiques inconnues des autres joueurs, alors on peut transformer un jeu à information incomplète en un jeu à information complète mais imparfaite. Le système imaginé par Harsanyi pour traduire l'incertitude mathématique est pris en compte par l'introduction d'un évènement lié à la nature qui représente un joueur fictif sans fonction gain qui n'intervient qu'avant le début du jeu.

1.3.4 Autres classes de jeu :

1.3.5 Jeu fini :

Définition 1.3.2. *Le jeu (1.1) est dit fini, si tous les ensemble des stratégies des joueurs sont finis, autrement dit, si* $|S_i| < \infty, \forall i \in \mathbb{N}$.

Définition 1.3.3. *(Jeu fini à deux joueurs)[25]*

Si $\mathbb{N} = 2$, $|S_1| = m < \infty$ *et* $|S_2| = n < \infty$, *on dit que le jeu (1.1) est un jeu fini a deux joueurs. Il est représenté par :*

$$< \mathbb{N}, S_1, S_2, u_1, u_2 > \tag{1.2}$$

Où : S_1 *est l'ensemble constitué d'un nombre fini de* m *stratégies du joueur 1,* S_2 *est l'ensemble constitué d'un nombre fini de* n *stratégies du joueur 2.*
$u_1 : S_1 \times S_2 \to \mathbb{R}$ *est la fonction de gain du joueur 1.*
$u_2 : S_1 \times S_2 \to \mathbb{R}$ *est la fonction de gain du joueur 2.*
$S = S_1 \times S_2$ *est l'ensemble des issues possibles du jeu.*

Définition 1.3.4 (Jeu fini à deux joueurs à somme nulle)**.** *Si dans le jeu fini a deux joueurs défini dans* (1.2) *la somme des gains des deux joueurs est nulle en toute situation du jeu* $(u_1(s) + u_2(s) = 0, \forall s \in S)$, *on dit que le jeu (1.2) est un jeu fini à deux joueurs à somme nulle. Il sera noté par :*

$$< \mathbb{N}, S_1, S_2, u > \tag{1.3}$$

Où : $u = u_1 = -u_2$ *est la fonction que le joueur 1 veut maximiser et que le joueur 2 veut minimiser. Un exemple représentatif nous permettant d'étudier les jeux à somme nulle est le jeu d'enfant : (pierre, feuille, ciseaux). Chacun des deux joueurs doit choisir simultanément une action : pierre, feuille ou ciseaux. Il y a un cycle entre ces trois symboles : la pierre casse les ciseaux, les ciseaux coupent la feuille et la feuille recouvre la pierre. Si les deux joueurs choisissent le même symbole, alors ils font match nul. Sinon, le joueur ayant le symbole le plus fort gagne et l'autre en perd une. Le jeu (pierre, feuille, ciseau) sous sa forme stratégique peut donc être décrit par la matrice suivante :*

Joueur 1 \ Joueur 2	Pierre	Feuille	Ciseaux
Pierre	(0 ;0)	(-1 ;1)	(1 ;-1)
Feuille	(1 ;-1)	(0 ;0)	(-1 ;1)
Ciseaux	(-1 ;1)	(1 ;-1)	(0 ;0)

TABLE 1.2 – Jeu de Pierre, Ciseaux et Papier

Définition 1.3.5 (Jeu fini à deux joueurs à somme non nulle)**.** *Si dans le jeu (1.2) la somme des gains des deux joueurs est non nulle en toute situation du jeu* $(u_1(s) + u_2(s) = constante, \forall s \in S)$, *on dit que le jeu (1.1) est un jeu fini à 2 joueurs à somme non nulle.*

1.3.6 Jeux répétés

Définition 1.3.6. *Un jeu répété est un jeu ordinaire réitéré plusieurs fois de suite. Par jeu ordinaire, nous entendons un jeu statique (joué une seule fois) dans lequel les joueurs choisissent simultanément leurs stratégies, le jeu (1.1) est appelé jeu constituant.*

Définition 1.3.7. *Un jeu répété au sens strict est un jeu répété stationnaire : c'est le même jeu ordinaire appelé jeu constituant qui est répété de période en période.*

Les conditions du jeu ne se modifient pas au cours du temps :

- même nombre de joueurs ;
- mêmes ensembles de stratégies des joueurs ;
- mêmes fonctions de gains ;
- même facteur d'actualisation.

Si l'une des conditions évolue au cours du temps, nous parlerons alors de **super jeu (supergame)**. Un super jeu est donc une séquence de jeux ordinaires qui peuvent différer d'une période à l'autre.

Définition 1.3.8. *Considérons le jeu répété dans lequel les joueurs font face à chaque période au jeu constituant (1.1). La répétition de ce jeu permet aux joueurs de conditionner leurs choix présents et futurs sur les choix passés. Cette interdépendance temporelle peut conduire à des solutions plus coopératives ou plus agressives que celle observées dans le jeu constituant. La répétition élargit l'ensemble des solutions. On définit $s_i(t)$ l'action du joueur $i \in \mathbb{N}$ à la date t. Ainsi, le profil de stratégies sélectionnées par les N joueurs à la date t s'écrit :*

$$s(t) = (s_1(t), ..., s_i(t), ..., s_N(t)) \in S = \prod_{i \in \mathbb{N}} S_i.$$

Définition 1.3.9. *L'histoire du jeu à la date t est donnée par*

$$h(t) = (s(0), s(1), ..., s(t-1)) \in S^t = \prod_{k=0}^{t-1} S.$$

L'histoire du jeu correspond à l'ensemble des actions que les joueurs ont choisi entre la période initiale $k = 0$ et la période $k = t - 1$. Dans un jeu répété, le profil d'actions sélectionné par les joueurs à chaque période crée un nouveau sous-jeu qui est entièrement défini par l'histoire à cette date.

Définition 1.3.10. *Dans un jeu répété, une stratégie pour un joueur $i \in \mathbb{N}$ consiste en une séquence de règles de décision, une par période. Cette stratégie est notée par :*

$$\sigma_i = (\sigma_i(0), \sigma_i(1), \sigma_i(2), ..., \sigma_i(t), ...),$$

où $\sigma_i(t)$ est la règle de décision du joueur $i \in \mathbb{N}$ à la date t : $\sigma_i(t)(.) : S^t \to S_i$.
$\sigma_i(t)(.)$ est une application de S^t vers S_i qui spécifie pour chaque histoire du jeu h_t une action ou une conduite à tenir à la date t.
Ainsi, le joueur $i \in \mathbb{N}$ joue à la date t l'action $\sigma_i(t)(h_t) \in S_i$ s'il a observé une histoire h_t du jeu. On notera :

- $\Omega_{i(t)}$ l'ensemble des règles de décision du joueur i à la date t ;
- $\Omega_i = \Omega_{i(0)} \times \Omega_{i(1)} \times \Omega_{i(2)} \times ...$ l'ensemble des stratégies du joueur $i \in \mathbb{N}$ dans le jeu répété, $\Omega_{i(0)} = S_i$;
- $\sigma = (\sigma_1, ..., \sigma_i, ..., \sigma_N)$ le profil de stratégies du jeu répété ;
- $\sigma(t) = (\sigma_1(t), ..., \sigma_i(t), ..., \sigma_N(t))$ le profil des règles de décision à la période t. On a $\sigma \in \Omega = \prod_{i \in \mathbb{N}} \Omega_i$.

On distingue plusieurs classes de stratégies selon la place que l'histoire occupe dans les règles de décision des joueurs.
A la période t, il observe l'histoire h_t et joue l'action prescrite par sa règle de décision $\sigma_i(t)$. Nous pouvons avoir alors $\sigma_i(t)[h_t^1] \neq \sigma_i(t)[h_t^2]$ pour deux histoires $h_t^1, h_t^2 \in S^t$ différentes. Le gain accumulé escompté du joueur $i \in \mathbb{N}$ avec un facteur d'actualisation $\sigma \in [0,1]$, commun à tous les joueurs, s'écrit :

$$U_i(\sigma) = \sum_{t=0}^{\infty} \sigma^t u_i(\sigma(t)).$$

On notera le jeu infiniment répété avec actualisation (jeu escompté) par :

$$\Gamma^{\infty} =< \mathbb{N}, \{\Omega_i\}_{i\in\mathbb{N}}, \{U_i\}_{i\in\mathbb{N}}, \sigma > . \tag{1.4}$$

1.4 Quelques concepts de solutions pour les jeux non coopératifs :

L'analyse d'un jeu permet de prédire l'équilibre qui émergera si les joueurs sont rationnels. Par équilibre nous entendons une combinaison de stratégies telle qu'aucun des joueurs n'a d'incitation à changer sa stratégie compte tenu des stratégies des autres joueurs. Une fois que l'équilibre est atteint dans un jeu (peu importe la manière dont il a été obtenu), il n'y a aucune raison de le quitter.
La solution idéale correspondrait à un équilibre unique et, dans ce cas, nous pouvons précisément prédire la solution de cette situation conflictuelle. Néanmoins, on a souvent des équilibres multiples et parfois il n'en existe pas [32].

1.4.1 Équilibre de Nash

L'équilibre de Nash doit son nom au mathématicien et économiste américain John F. Nash, qui a introduit ce concept en 1950.

Définition 1.4.1. *[32] Un profil de stratégies $s^* = (s_1^*, ..., s_N^*)$ est un équilibre de Nash en stratégies pures dans le jeu (1.1) si aucun joueur n'a intérêt à changer sa stratégie s_i au moment où les autres joueurs continuent à jouer la stratégie s_i^*, c'est à dire :*

$$u_i(s_i^*, s_{-i}^*) \geq u_i(s_i, s_{-i}^*), \quad \forall s_i \in S_i \quad \forall i \in \mathbb{N}.$$

Définition 1.4.2. *Une situation $s^* = (s_1^*, ..., s_N^*)$ est un équilibre de Nash strict dans le jeu (1.1) ssi :*

$$u_i(s_i^*, s_{-i}^*) > u_i(s_i, s_{-i}^*), \quad \forall s_i \in S_i \quad \forall i \in \mathbb{N}.$$

Définition 1.4.3. *Une situation $\alpha^* = (\alpha_1^*, ..., \alpha_N^*) \in \Delta = \prod_{i=1}^{N} \Delta_i$ est un équilibre de Nash en stratégies mixtes dans le jeu (1.1) ssi :*

$$\tilde{u_i}(\alpha_i^*, \alpha_{-i}^*) \geq \tilde{u_i}(\alpha_i, \alpha_{-i}^*), \quad \forall \alpha_i \in \Delta_i \quad \forall i \in \mathbb{N}.$$

avec α_i la stratégie mixte jouée par le joueur i et α_{-i} est le profil de stratégies mixte joué par tous les joueurs à l'excepté du joueur i et $\tilde{u_i}$ est le gain éspéré de $i^{\text{ème}}$ joueur.

Proposition 1. *[22] Tout équilibre de Nash en stratégies pures est aussi un équilibre de Nash en stratégies mixtes.*

Théoreme 1. *[22] Tout jeu fini admet au moins un équilibre de Nash en stratégies mixtes.*

Définition 1.4.4. *Un profil de stratégies σ^* est un équilibre parfait dans le jeu répété (1.3), si*

i *σ^* est un équilibre de Nash sur l'ensemble du jeu*

$$U_i(\sigma^*) \geq U_i(\sigma_i, \sigma^*_{-i}), \ \ \forall \sigma_i \in \Omega_i, \ \ \forall i \in \mathbb{N}.$$

ii *σ^{*h_t} est un équilibre de Nash pour tout t et toute histoire h_t*

$$U_i(\sigma^{*h_t}) \geq U_i(\sigma_i, \sigma^{*h_t}), \ \ \forall t = 1, 2, ..., \ \ \forall h_t, \ \ \forall \sigma_i \in \Omega_i^{h_t}, \ \ \forall i \in \mathbb{N}.$$

1.4.2 Équilibre en stratégies dominantes

Définition 1.4.5. ***(Dominance) :***

On dit que la stratégie s_i^1 du joueur i domine la stratégie s_i^2 si

$$u_i(s_i^1, s_{-i}) \geq u_i(s_i^2, s_{-i}), \quad \forall s_{-i} \in S_{-i}.$$

Définition 1.4.6. ***(Dominance stricte) :***

On dit que la stratégie s_i^1 du joueur i domine strictement la stratégie s_i^2 si

$$u_i(s_i^1, s_{-i}) > u_i(s_i^2, s_{-i}), \quad \forall s_{-i} \in S_{-i}.$$

Définition 1.4.7. ***(Stratégie dominante) :***

On dit que la stratégie s_i^* est dominante pour le joueur i si elle domine toute stratégie $s_i \in S_i$.

Définition 1.4.8. ***Une stratégie est dominée*** *si elle procure au joueur des gains toujour inférieur à ceux associés à au moins une autre des stratégies possibles. On distingue deux types :*

Une stratégie s_i est ***strictement dominée*** *pour le joueur i s'il existe une stratégie s_i' telle que pour tous les profils S_{-i}*

$$u_i(s_i', s_{-i}) > u_i(s_i, s_{-i}).$$

Une stratégie s_i est ***faiblement dominée*** *pour le joueur i s'il existe une stratégie s_i' telle que pour tous les profils S_{-i}*

$$u_i(s_i', s_{-i}) \geq u_i(s_i, s_{-i}).$$

Définition 1.4.9. ***(Équilibre en stratégies dominantes) :***

Un jeu possède un équilibre en stratégies (strictement) dominantes si pour chacun des joueurs, il existe une stratégie qui domine (strictement) toutes ses autres stratégies, quelles que soient les stratégies des autres joueurs.

Autrement dit, quelles que soient les stratégies des autres joueurs, le gain que j'obtiens en jouant cette stratégie dominante (strictement) sera strictement supérieur à celui obtenu en jouant une autre stratégie.

Chaque joueur jouera donc évidemment sa stratégie dominante et personne n'aura intérêt à dévier de cet équilibre. L'équilibre en stratégie dominante est donc un équilibre de Nash. Lorsqu'il existe (ce qui est assez rare), l'équilibre en stratégies dominantes est unique.

Définition 1.4.10. ***(Équilibre par élimination itérée des stratégies dominées) :***
On dit qu'une stratégie est dominée pour un joueur donné s'il existe au moins une autre stratégie telle que, quelles que soient les stratégies adoptées par les autres joueurs, cette autre stratégie est toujours au moins aussi bonne que la première et strictement meilleure dans au moins l'une des situations. Si chaque joueur est rationnel, suppose que les autres joueurs sont rationnels et suppose que les autres joueurs supposent qu'il est rationnel, alors on peut définir l'équilibre du jeu comme celui qui serait obtenu par l'élimination successive des stratégies dites dominées. L'idée est que chaque joueur peut identifier les stratégies dominées de son adversaire et peut donc réduire le champ des actions, sachant qu'elles ne seront jamais jouées par un joueur rationnel.

1.4.3 Pas d'équilibre, trop d'équilibres

Il est important de noter que tous les jeux n'ont pas toujours un équilibre qui peut être déterminé par une simple exploration de la matrice des gains. D'autre part, certains jeux sont caractérisés par des équilibres multiples.

Exemple 5. ***(La bataille des sexes)***
Certains jeux font intervenir une part de coordination et une part de conflit entre les joueurs. C'est le cas du jeu de la bataille des sexes suivant :

Cas 1 : *Un couple a l'intention d'aller à un spectacle une soirée. L'homme préfère aller voir le combat de boxe tandis que la femme préfère l'opéra. Chacun a intérêt à aller avec l'autre au spectacle qui l'intéresse. Mais si l'homme et la femme vont chacun de son côté au spectacle qui l'intéresse, leurs gains (degré de satisfaction) seront inférieurs à la perspective d'aller avec l'autre même à un spectacle qui ne l'intéresse pas. On suppose qu'ils ne connaissent pas avant de prendre leur décision, le choix de leur partenaire, soit parce que le choix est simultané, soit parce qu'ils ne peuvent pas se voir avant le soir.*

l'homme \ la femme	boxe	opera
boxe	(4 ;2)	(1 ;1)
opera	(0 ;0)	(2 ;4)

TABLE 1.3 – Bataille des sexes

Dans ce jeu, on a deux équilibres : (boxe,boxe), (opera,opera).

Cas 2 :*On reprend le même exemple, mais pour la femme et pour l'homme, être avec l'autre est plus important que le lieu.*

l'homme \ la femme	boxe	opera
boxe	(4 ;2)	(0 ;0)
opera	(0 ;0)	(2 ;4)

TABLE 1.4 – Bataille des sexes

Dans ce jeu aussi, on a deux équilibres : (boxe,boxe), (opera,opera).

Exemple 6. ***(Le dilemme du prisonnier)***
On reprendre l'exemple 1(Le dilemme du prisonnier), dont la matrice des gains est :

Suspect 1 \ Suspect 2	Se taire	Dénoncé
Se taire	(-1 ;-1)	(-10 ;0)
Dénoncé	(0 ;-10)	(-5 ;-5)

TABLE 1.5 – Le dilemme du prisonnier

Dans ce jeu, on a un seul équilibre : (Dénoncé, Dénoncé).

Exemple 7. ***(Le jeu de pile ou face)***

On considère deux joueurs, chacun choisit entre pile (action P) ou face (action F). les stratégies des joueurs sont :

$$S_1 = S_2 = \{P, F\}.$$

Si les choix sont identiques, le joueur 2 donne 1 € au joueur 1 :

$$u_1(P,P) = u_1(F,F) = -u_2(P,P) = -u_2(F,F) = 1.$$

Si les choix diffèrent, le joueur 1 donne 1 € au joueur 2 :

$$u_1(P,F) = u_1(F,P) = -u_2(P,F) = -u_2(F,P) = -1.$$

La matrice des gains sera la suivante :

$$\begin{array}{c} \\ P \\ F \end{array} \begin{array}{c} \begin{array}{cc} P & F \end{array} \\ \begin{pmatrix} (1,-1) & (-1,1) \\ (-1,1) & (1,-1) \end{pmatrix} \end{array}$$

Dans ce jeu, il n'existe pas d'équilibre de Nash en stratégies pures.

Exemple 8. ***(Concurrence à la Cournot)***
Le travail de Augustin Cournot en 1838, en dépit de son ancienneté, consiste aujourd'hui une pierre angulaire de l'organisation industrielle. C'est de cette époque que date sa principale contribution à la théorie des jeux contemporaine et à la théorie d'oligopole dans son célèbre ouvrage recherches sur les principes mathématiques de la théorie des richesses [8] dont il a consacré cinq chapitres des recherches aux structures de marché où les firmes se concurrencent par les quantités. Pour autant, Cournot constitue aujourd'hui une référence incontournable pour de nombreux économistes et théoriciens des jeux qui continuent à développer, dans de nombreux modèles, les démonstrations dont il est l'initiateur. A cet égard, on parle à l'heure actuelle d'équilibre de Cournot-Nash de sorte que l'application de ce concept touche autant l'économie mathématique que l'économie industrielle.
Son modèle célèbre de duopole puis d'oligopole se trouve dans son chapitre VII de son livre [8] proposé de la môme manière par A. Cournot en 1838 fait l'hypothèse que le prix

d'un bien homogène, produit par deux firmes, reste fixe quand ces deux firmes maximisent leurs profits par rapport aux quantités qu'elles désirent produire. Cette concurrence est appelée la concurrence en quantité ou à la Cournot.

***Description du l'oligopole de Cournot**[26]*

Soit un marché d'oligopole constitué de N firmes sur lequel ces dernières se font concurrence pour offrir un produit homogène. La fonction inverse de demande du marché est donnée par $p = P(Q)$ où : p est le prix du marché, $Q = \sum_{i=1}^{N} q_i$ est la quantité totale du produit offerte sur le marché et q_i la quantité produite par la firme i. Cette fonction est supposée non négative $(P(Q) \geq 0; \forall Q)$, deux fois continûment differentiable et elle est strictement décroissante $(P'(Q) < 0; \forall Q)$. Soit $C_i(q_i)$, la fonction de coût de production de la firme i de q_i unités du produit. Cette fonction est supposée : non négative, convexe, deux fois continûment differentiable et non-décroissante. L'objectif de chaque firme i est la maximisation de son profit étant donné la production des autres firmes concurrentes :

$$\Pi_i(q_i, q_{-i}) = P(\sum_{j \in N} q_j)q_i - C_i(q_i) \rightarrow \max_{0 \leq q_i < +\infty}, \ \forall i \in \mathbb{N}. \tag{1.5}$$

où $q_{-i} = (q_1, ..., q_{i-1}, q_{i+1}, ..., q_N)$ est un vecteur de $\mathbb{R}_+^{N-1}$ représente l'offre de chaque firme sauf celle de la i^{me}.

Formellement, la concurrence à la Cournot (ou la concurrence en quantité) est caractérisée par un jeu sous forme normal :

$$j_c =< \mathbb{N}, \{Q_i\}_{i \in \mathbb{N}}, \{\Pi_i\}_{i \in \mathbb{N}} > \tag{1.6}$$

où :

- $\mathbb{N} = \{1...N\}$ *est l'ensemble des firmes qui constituent l'oligopole du Cournot. Une firme quelconque est désignée par l'indice i ; $i \in \mathbb{N}$,*
- $Q_i = [0, +\infty[= \{q_i / 0 \leq q_i < +\infty\}$ *désigne l'ensemble des stratégies de la firme $i \in \mathbb{N}$. Il caractérise les valeurs des quantités admissibles que la firme i est prête à offrir sur le marché,*
- $\Pi_i : \prod_{i=1}^{N} Q_i \subset \mathbb{R}_+^N \rightarrow \mathbb{R}$ *est la fonction de gain de la firme $i \in \mathbb{N}$. Il s'agit donc d'un modèle statique dans le sens où les firmes ne se rencontrent qu'une seule fois sur le marché et elle fixe les quantités simultanément et de manière non coopératif et qu'un commissaire priseur détermine le prix qui égalise l'offre à la demande du marché.*

***L'équilibre du jeu de Cournot**[26]*

Définition 1.4.11. *L'équilibre oligopolistique de Cournot-Nash du jeu (1.5) est un vecteur de quantités $q^c \in \mathbb{R}_+^N$ tel que :*

$$\Pi_i(q^c) = \max_{Q_i = [0, +\infty[} \Pi_i(q_1^c, q_2^c, ..., q_{i-1}^c, q_i, q_{i+1}^c, ..., q_N^c), \ \forall i \in \mathbb{N}.$$

Remarque 3. *D'après cette définition, l'une des premières propriétés de l'équilibre de Cournot est la stabilité dans le sens où une fois l'équilibre est réalisé, aucune des deux firmes n'a intérêt à modifier unilatéralement les quantités qu'elle produit sous peine de voir ses profits diminuer ce qui correspond à un équilibre de Nash.*

La condition d'optimalité du premier ordre du problème (1.4) est donnée par :

$$\frac{\partial \Pi_i(q_i, q_{-i})}{\partial q_i} = P(\sum_{j=1}^{N} q_j) + q_i P'(\sum_{j=1}^{N} q_j) - C_i'(q_i) = 0, \;\; i \in \mathbb{N}.$$

L'équilibre oligopolistique de Cournot, $q^c = (q_1^c, q_2^c, ..., q_N^c)$ où $q_i^c \geq 0$; $i \in \mathbb{N}$, est déterminé par N équations satisfaisant la condition du premier ordre ; $\frac{\partial \Pi_i(q_i, q_{-i})}{\partial q_i} = 0$, $i \in \mathbb{N}$. La $i^{ème}$ équation est appelée la fonction de meilleure réaction (appelée règle de décision optimale en terme de la théorie des jeux) de la firme i ; un concept fondamental introduit par Cournot afin d'expliquer comment le modèle peut être résolu. Elle décrit l'offre optimale, q_i, qui maximise le profit de la firme i étant donné les quantités produites par les autres firmes q_{-i}. Selon Cournot, Elle est définit par :

Définition 1.4.12.

$$R_i(q_{-i}) = \{q_i^* \in Q_i / \Pi_i(q_i^*, q_{-i}^*) = \max_{q_i \in Q_i} \Pi_i(q_i^*)\}, \equiv \{q_i^* \in Q_i / \frac{\partial \Pi_i(q_i^*, q_{-i}^*)}{\partial q_i^*}\}.$$

où $R_i : \prod_{j \in \mathbb{N} \setminus \{i\}} Q_j \to Q_i$. Elle donne la quantité q_i que doit produire la firme i pour chaque niveau de production de ses concurrentes q_{-i}.

Duopole lineaire : *On considère deux firmes sur le marché qui se font concurrence en quantité. Le coût marginale de production est $C_i(q_i) = c_i(q_i)$, la demande inverse du marché est :*

$$p(Q) = \begin{cases} a - Q, & si \;\; Q > 0, \\ 0, & sinon. \end{cases}$$

Avec $Q = q_1 + q_2$, est la quantité offerte sur le marché.

Le profits des deux firmes :

$$\begin{cases} \pi_1(q_1, q_2) = p(q_1 + q_2)q_1 - c_1 q_1, \\ \pi_2(q_1, q_2) = p(q_1 + q_2)q_2 - c_2 q_2, \end{cases}$$

D'où :

$$\begin{cases} \pi_1(q_1, q_2) = [a - (q_1 + q_2)]q_1 - c_1 q_1, \\ \pi_2(q_1, q_2) = [a - (q_1 + q_2)]q_2 - c_2 q_2, \end{cases}$$

Les conditions d'équilibre sont données comme suit :
La condition de 1^{er} ordre :

$$\begin{cases} \frac{\partial \pi_1(q_1, q_2)}{\partial q_1} = a - 2q_1 - q_2 - c_1 = 0, & (1) \\ \\ \frac{\partial \pi_1(q_1, q_2)}{\partial q_2} = a - 2q_2 - q_1 - c_2 = 0, & (2) \end{cases}$$

La condition de 2^{eme} ordre :

$$\begin{cases} \frac{\partial^2 \pi_1(q_1, q_2)}{\partial q_1^2} = -2, \\ \\ \frac{\partial^2 \pi_1(q_1, q_2)}{\partial q_2^2} = -2, \end{cases}$$

De (1) on a $a - 2q_1 - q_2 - c_1 = 0 \Rightarrow 2q_1 = a - q_2 - c_1 \Rightarrow q_1^* = \frac{a - q_2 - c_1}{2}$. (3)

De (2) on a $a - 2q_2 - q_1 - c_2 = 0 \Rightarrow 2q_2 = a - q_1 - c_2 \Rightarrow q_2^* = \frac{a-q_1-c_2}{2}$. (4)

On remplace (3) dans (4) et on aura :

$q_2^* = \frac{a-\frac{a-q_2-c_1}{2}-c_2}{2} \Rightarrow q_2^* = \frac{a+c_1-2c_2}{3}$. (5)

On remplace (5) dans (3) et on aura :

$q_1^* = \frac{a+c_2-2c_1}{3}$.

D'où l'équilibre de Nash est le vecteur $(q_1^*, q_2^*) = (\frac{a+c_2-2c_1}{3}, \frac{a+c_2-2c_1}{3})$ et les profits des deux firmes sont donnés comme suit :

$$\pi_1(q_1^*, q_2^*) = [\frac{a + c_2 - 2c_1}{3}]^2.$$
$$\pi_2(q_1^*, q_2^*) = [\frac{a + c_1 - 2c_2}{3}]^2.$$

1.5 Conclusion

Dans ce chapitre, nous avons résumé les notions de base de la théorie des jeux, ainsi que un bref aperçu sur les concepts de solutions des jeux non coopératifs sous forme normale. Nous avons exposé aussi quelques exemples célèbres en théorie des jeux.

CHAPITRE 2

SUR LES JEUX BAYÉSIENS

2.1 Introduction

Un jeu bayésien est un jeu dans lequel l'information dont dispose chaque joueur sur les caractéristiques des autres joueurs est incomplète. En particulier, on représente ainsi un jeu dans lequel un ou plusieurs joueurs font face à une incertitude quant au gain des autres joueurs. Cette situation impose de spécifier pour chaque joueur des croyances concernant les caractéristiques des autres joueurs. Du fait de l'hypothèse de rationalité, ces croyances prennent la forme d'une distribution de probabilités sur toutes les caractéristiques possibles. Partant d'une distribution a priori, les joueurs actualisent leurs croyances en fonction des choix faits par l'autre joueur, en utilisant la règle de Bayes, d'où la dénomination de ces jeux.

2.2 Jeux statique à information incomplète

Dans cette section, nous présentons formellement la démarche introduite par Harsanyi [12] et qui consiste à considérer que la caractéristique θ_i est la réalisation d'une variable aléatoire et représente le résultat du mouvement d'un nouvel agent appelé la Nature. Cette approche des jeux statiques à information incomplète consiste à considérer que la Nature joue en premier lieu et procède au tirage aléatoire du type $\theta_i \in \Theta_i$ du joueur i. La valeur de θ_i est révélée (observée) seulement au (par) le joueur i qui devient donc son information privée. Les autres joueurs n'observent pas θ_i . Avec cette approche, on définit un jeu Bayésien dont le déroulement est le suivant :

1. Il existe, avant tout début de jeu, une fonction de distribution (croyances) à priori $p(\theta)$ donnant les probabilités jointes des types $\theta = (\theta_1, ..., \theta_n)$. Cette distribution à priori est une connaissance commune à tous les joueurs ;
2. Le jeu commence par le mouvement de la Nature qui procède au tirage aléatoire du vecteur $\theta = (\theta_1, ..., \theta_n)$ distribué selon $p(\theta)$;
3. La Nature révèle le type θ_i au seul joueur i ;
4. Connaissant $p(\theta)$ et θ_i , chaque joueur i peut en déduire des croyances à posteriori $p_i(\theta_{-i}/\theta_i)$ sur la valeur θ_{-i} des types des autres joueurs.

5. Chaque joueur choisit une stratégie de son espace S_i . Ce choix se fait en fonction du type θ_i révélé par la Nature, d'où l'on peut écrire $s_i(\theta_i)$.
6. Chaque joueur i reçoit un gain qui dépend non seulement du profil de stratégies pures $s = (s_1, ..., s_n)$, mais également de sa caractéristique privée $\theta_i \in \Theta_i$. Elle prend donc la forme de l'espérance d'utilité $E_{\theta_{-i}}[u_i(s_i, s_{-i}; \theta_i)]$ [13].

Remarquons que l'hypothèse selon laquelle la distribution jointe à priori $p(\theta)$ est connaissance commune est une hypothèse forte. Elle est à la base de l'existence des probabilités subjectives (à posteriori) $p_i(\theta_{-i}/\theta_i)$.
En introduisant un joueur fictif, la Nature, une situation de jeu statique à information incomplète est réinterprétée comme étant un jeu dynamique à information imparfaite. En effet, lorsque la Nature choisit (tire de façon aléatoire) la caractéristique (type) θ_i , les autres joueurs ne peuvent observer ce choix. Ils ne connaissent donc pas la totalité de l'histoire du jeu. Cette extension du jeu par sa transformation en un jeu en information imparfaite permet d'appliquer la technique standard de la théorie des jeux, notamment le concept de l'équilibre de Nash, sous réserve d'une nouvelle définition des concepts de stratégies et d'utilité.

Pour déterminer l'espérance de gain liée au choix d'une stratégie, les joueurs doivent spécifier les probabilités $p_i(\theta_{-i}/\theta_i)$, ce qui nécessite le recours à la formule de Bayes. Dans l'approche de Harsanyi, connaissant son type θ_i et la distribution jointe $p(\theta)$, chaque joueur peut estimer la probabilité des types θ_{-i} des autres joueurs en se référant à la formule de Bayes :

$$p_i(\theta_{-i}/\theta_i) = \frac{p(\theta_{-i}/\theta_i)}{p(\theta_i)} = \frac{p(\theta_{-i}/\theta_i)}{\sum_{\theta_i \in \Theta_i} p(\theta_{-i}/\theta_i)}.$$

La formule de Bayes permet de réviser les probabilités (croyances) après avoir observé un évènement donné. Pour expliciter cette formule (de Bayes), on utilise le schéma suivant qui représente deux ensembles (évènements) A et B non disjoints

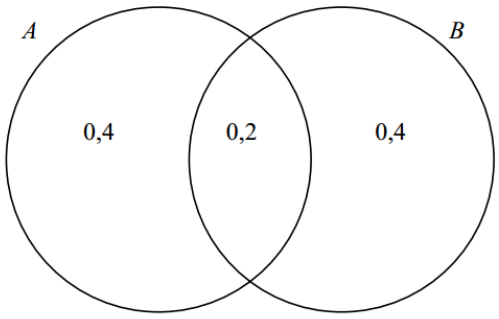

FIGURE 2.1 – Schéma représentatif de la formule de Bayes

Etant donné que $p(A) = 0,6, p(B) = 0,6$ et $p(A \cap B) = 0,2$; on a $p(A/B) = \frac{p(A \cap B)}{p(B)} = \frac{0.2}{0.6} = \frac{1}{3}$.

Dans un jeu statique en information incomplète, le joueur i connaît son type θ_i mais est incertain sur les types $\theta_{-i} = (\theta_1, ..., \theta_{i-1}, \theta_{i+1}, ..., \theta_n)$ des autres joueurs. Avec l'introduction dans le jeu à information incomplète, la fonction d'utilité du joueur i de type $\theta_i \in \Theta_i$ est reformulée ainsi : $p_i(s_1, ..., s_n; \theta_i)$. Le joueur i dispose de croyances à posteriori sur les types θ_{-i}, croyances résumées dans la distribution de probabilité $p_i(\theta_{-i}/\theta_i)$. Lorsque les

types θ_i sont indépendants, les distributions de probabilité $p_i(\theta_{-i}/\theta_i)$ ne dépendent plus de θ_i et dans ce cas, les croyances à posteriori du joueur i s'écrivent $p_i(\theta_{-i})$. Nous obtenons ainsi la définition suivante d'un jeu statique à information incomplète.

2.2.1 Jeux Bayésiens statiques :

Harsanyi [12] a été le premier à introduire la notion de type. Un type dans le point de vue de Harsanyi, est une sorte d'état d'esprit. Il contient non seulement la croyance du joueur sur l'état de la Nature mais aussi sur sa croyance sur la croyance des autres, et la croyance du joueur sur la croyance des autres sur sa croyance, etc. Cependant, Harsanyi ne donna pas une construction rigoureuse de cette idée. Cela a été fait une vingtaine d'années plus tard par Mertens et Zamir [19]. Les ingrédients du modèle de Harsanyi standard sont les suivants :

Définition 2.2.1. *(Jeu Bayésien)*
Un jeu Bayésien peut être décrit par un 6-tuplet [4] :

$$G = (\mathbb{N}; \{\Theta_k\}_{k\in\mathbb{N}}; p; \{A_k\}_{k\in\mathbb{N}}; \{S_k\}_{k\in\mathbb{N}}; \{U_k\}_{k\in\mathbb{N}});$$

où :

- $\mathbb{N} = \{1, ..., N\}$ *est l'ensemble des joueurs, avec* N *le nombre total de joueurs.*
- Θ_k *est l'ensemble des types du joueur* k *et* $\Theta = \Theta_1 \times ... \times \Theta_N$ *est l'ensemble des profils de types.*
- p *est une distribution de probabilités à priori sur le profil de types* $\theta = (\theta_1, ..., \theta_N)$ *et* $\theta_k \in \Theta_k$ *avec* $k \in \mathbb{N}$.
- A_k *est l'ensemble des actions possibles pour un joueur* $k \in \mathbb{N}$ *et* $A = (A_1 \times ... \times A_N)$ *est l'ensemble des profils d'actions.*
- S_k *est l'ensemble des stratégies pures possibles pour le joueur* $k \in \mathbb{N}$. *Une stratégie pure d'un joueur* k *est obtenue par l'application* $s_k : \Theta_k \to A_k$ *associant pour chaque type* $\theta_k \in \Theta_k$, *une action* $a_k \in A_k$ *qu'elle soit choisie par le joueur* k *lorsque son type est* θ_k. *Soient* $S = S_1 \times ... \times S_N$ *l'ensemble des profiles de stratégies. Nous définissons un profile de stratégie comme la fonction* $s : \Theta \to A$ *telle que* $\forall\theta = (\theta_1, ..., \theta_N) \in \Theta$, $s(\theta) = (s_1(\theta_1), ..., s_k(\theta_k), ..., s_N(\theta_N))$.
- U_k *est la fonction d'utilité du joueur* $k \in \mathbb{N}$ *telle que* $U_k : S \times \Theta \to \mathbb{R}$. *De plus, les types possibles, la distribution de probabilités et les fonctions d'utilités sont supposées être une connaissance commune pour tous les joueurs.*

2.2.2 Les stratégies dans un jeu Bayésien :

Rappelons qu'une stratégie est un plan d'actions complet spécifiant les actions possibles du joueur en toute circonstance où il peut avoir à intervenir. Cette définition de la stratégie est en fait similaire à celle des jeux dynamiques. Selon le déroulement du jeu défini plus haut, à l'étape 2, la Nature révèle à chaque joueur i son type θ_i. Ainsi, une stratégie (pure) du joueur i doit spécifier une action pour chaque type possible que pourrait lui révéler la Nature. Nous obtenons ainsi la définition de la notion de stratégie.

• **La stratégie pure dans un jeu Bayésien :**

Définition 2.2.2. *Dans le jeu Bayésien G, une stratégie pure contingente du joueur i est la fonction $s_i(\theta_i)$ qui, pour chaque type possible $\theta_i \in \Theta_i$, spécifie une action $s_i \in S_i$ que le joueur i choisira si le type θ_i venait à être tiré par la Nature. L'ensemble des stratégies pures possibles $\tilde{S}_i$ du joueur i est donc l'ensemble de toutes les fonctions $s_i(\theta_i)$.*

Exemple 9. *Si les actions possibles du joueur 1 sont A et B et ses types possibles sont θ_H et θ_L , alors l'ensemble de (toutes) ses stratégies $s_i(\theta_i)$ est :*

$\tilde{s_1} = A$ *si* θ_H *et* A *si* θ_L ;

$\tilde{s_2} = A$ *si* θ_H *et* B *si* θ_L ;

$\tilde{s_3} = B$ *si* θ_H *et* A *si* θ_L ;

$\tilde{s_4} = B$ *si* θ_H *et* B *si* θ_L ;

On a donc $\tilde{S}_i = (\tilde{s_1}, \tilde{s_2}, \tilde{s_3}, \tilde{s_4})$ *dont le cardinal est 4.*

• **La stratégie mixte dans un jeu Bayésien :**

Une stratégie mixte α_i du joueur i dans le modèle Bayésien est une application qui associe à chaque $\theta_i \in \Theta_i$ une probabilité $\alpha_i(\theta_i) \in \Delta((\theta_i))$. Si le type d'un joueur est θ_i alors il va jouer la stratégie $\alpha_i(\theta_i)$. Si les joueurs autres que i jouent le profil α_{-i}, alors le joueur i de type θ_i espère obtenir le gain suivant (en supposant pour simplifier que tout est fini) :

$$u_i((\alpha_i(\theta_i), \alpha_{-i}), \theta_i) = \sum_{\theta_{-i} \in \Theta_{-i}} p_{\theta_i}(\theta_{-i}) \sum_{i \in \mathbb{N}} \prod_{j \in \mathbb{N}} \alpha_j(\theta_j)(s_j) u_i(s, \theta).$$

où $\theta = (\theta_i, \theta_{-i})$.

2.2.3 L'espérance de gain dans un jeu Bayésien

Dans un jeu Bayésien, $\theta_i \in \Theta_i$ est une information privée du joueur i. On dit que θ_i est le type du joueur i. Il est observé uniquement par le joueur i. Pour tous les autres joueurs, θ_i est une variable aléatoire. Le gain du joueur i pour le profil de stratégies $s = (s_1(\theta_1), ..., s_n(\theta_n)) = (s_i(\theta_i), s_{-i}(\theta_{-i}))$ la forme de l'espérance de gain :

$$\tilde{u_i}(s_1^*(\theta_1), s_n^*(\theta_n)) = E_{\theta \in \Theta}[u_i(s_1^*(\theta_1), s_n^*(\theta_n), \theta_i)] = \sum_{\theta \in \Theta} P(\theta) u_i(s_1^*(\theta_1), s_n^*(\theta_n), \theta_i).$$

où : $P(\theta) = P(\theta_1, ..., \theta_n)$ est la probabilité jointe de $\theta = (\theta_1, ..., \theta_n)$.
Le jeu Bayésien G est ainsi mise sous la forme normale suivante :

$$\tilde{G} = (\mathbb{N}, \tilde{S}_1, ..., \tilde{S}_n, \tilde{u}_1, ..., \tilde{u}_n).$$

Remarque 4. *Si le jeu Bayésien sous forme normale $\tilde{G}$ est un jeu fini, c'est- à-dire si l'ensemble des joueurs et les ensembles de stratégies s_i sont finis, alors on peut appliquer le théorème de Nash. Pour un tel jeu fini, il existe donc un équilibre de Nash, possiblement en stratégies mixtes.*

2.2.4 Équilibre de Nash Bayésien

La démarche proposée par Harsanyi pour analyser les jeux statiques à information incomplète consiste à considérer ces derniers comme des jeux dynamiques à information imparfaite faisant intervenir un joueur fictif intervenant à la première étape du jeu, la Nature. Pour appliquer le concept de l'équilibre de Nash à un tel jeu, on commence par le mettre sous la forme normale. Cela nécessite l'introduction d'une nouvelle définition de la notion de stratégie qui est en fait similaire à celle introduite pour les jeux dynamiques. Nous obtenons ainsi l'équilibre de Nash Bayésien qui est un concept d'équilibre défini pour la classe des jeux simultanés (statiques) à information incomplète. Comme indiqué par Harsanyi, un jeu à information incomplète peut être analysé en considérant que le centre d'activité est soit le joueur soit les différents types de joueur. Harsanyi qualifie la première approche de player-centered interprétation et la seconde de type-centered interprétation. En les utilisant de façon appropriée, ces deux approches s'avèrent être équivalentes. Dans le cadre d'un tel jeu, l'équilibre Bayésien de Nash est défini comme suit :

Définition 2.2.3. *Un équilibre de Nash Bayésien pour le jeu Bayésien G est un profil de stratégies pures $(s_1^*(\theta_1), ..., s_n^*(\theta_n))$ qui soit un équilibre de Nash du jeu sous forme normale $\tilde{G}$. Le profil de stratégies pures $(s_1^*(\theta_1), ..., s_n^*(\theta_n))$ est donc un équilibre de Nash Bayésien si pour tout $i = 1, ..., n$ on a :*

$$\tilde{u_i}(s_i^*(\theta_i), s_{-i}^*(\theta_{-i})) \geq \tilde{u_i}(s_i(\theta_i), s_i^*(\theta_{-i})) \qquad \forall s_i(\theta_i) \in \tilde{S_i}$$

Soit si :

$$\sum_{\theta} p(\theta)\tilde{u_i}(s_i^*(\theta_i), s_{-i}^*(\theta_{-i}), \theta_i) \geq \sum_{\theta} \tilde{u_i}(s_i(\theta_i), s_i^*(\theta_{-i}), \theta_i) \qquad \forall s_i(\theta_i) \in \tilde{S_i}$$

Définition 2.2.4. *(Equilibre de Nash Bayésien)*
Un profil de stratégies $s^* = (s_1^*, ..., s_N^*) \in S$ est un équilibre de Nash Bayésien pour le jeu G, si :

$$\forall k \in \mathbb{N}, \forall s_k \in S_k, \forall \theta_k \in \Theta_k, u_k^B((s_k^*, s_{-k}^*), \theta_k) \geq u_k^B((s_k, s_{-k}^*), \theta_k).$$

Définition 2.2.5. *D'après la Définition 2.2.4, un profil de stratégies mixtes α est un équilibre Bayésien si pour tout i et pour tout type $\theta_i \in \Theta_i$ on a :*

$$u_i((\alpha_i(\theta_i), \alpha_{-i}), \theta_i) = \max_{\tilde{\alpha}_i \in \Delta(S_i(\theta_i))} u_i(\tilde{\alpha}_i, \alpha_i, \theta_i).$$

En d'autres termes, le profil de stratégies $(s_1^*(\theta_1), ..., s_n^*(\theta_n))$ est un équilibre de Nash du jeu G Bayésien où chaque agent maximise son utilité espérée conditionnelle à ses croyances sur le type des autres agents. L'équilibre Bayésien est donc moins exigeant que l'équilibre de Nash en information complète puisque les joueurs ne maximisent leur utilité qu'en espérance.

Remarque 5. *Il est important de remarquer que dans la forme normale d'un jeu, le joueur i doit spécifier une action pour chaque type θ_i possible et cela même s'il connaît son type. En effet, du fait de l'existence de l'interdépendance stratégique entre les joueurs, le choix du joueur i dépend du choix des autres joueurs. Or, ces derniers ignorent le type θ_i du joueur i. Ils doivent donc considérer toutes les stratégies possibles pour les différents types du joueur i. Le jeu doit donc spécifier les stratégies du joueur i pour tous les θ_i possibles. Cette définition de la stratégie permet d'appliquer le concept de l'équilibre de Nash pour un jeu Bayésien, ce qui donne l'équilibre de Nash Bayésien.*

Remarque 6. *En l'absence ou dans le cas d'une multiplicité d'équilibres de Nash Bayésiens dans l'espace des stratégies pures, le jeu peut se résoudre dans l'espace des stratégies mixtes ou de comportement. Par une stratégie mixte pour un joueur $k \in \mathbb{N}$, nous entendons une application $\tilde{s_k} : \Theta_k \to \Delta(S_k)$ qui assigne pour chaque type du joueur k, $\theta_k \in \Theta_k$, une distribution de probabilités sur l'ensemble des stratégies S_k. Soit $\bar{s_k} : \Theta_k \times S_k \to [0,1]$ l'application qui assigne pour le joueur k avec le type $\theta_k \in \Theta_k$, une probabilité de jouer la stratégie $s_k \in S_k$. La fonction d'utilité attendue (ou le gain espéré) pour le joueur k, sachant son type $\theta_k \in \Theta_k$, les types des autres joueurs $\theta_{-k} \in \Theta_{-k}$, sa stratégie mixte $\tilde{s_k} \in \Delta(S_k)$ et les stratégies de comportement des autres joueurs $\tilde{s_{-k}} \in \Delta(S_{-k})$ est :*

$$\tilde{u_k^B}((\tilde{s}_k, \tilde{s}_{-k}), \theta_k) = \sum_{\theta_{-k}} p(\theta_k/\theta_{-k}) \tilde{u}_k((\tilde{s}_k, \tilde{s}_{-k}), (\theta_k, \theta_{-k})).$$

où :

$$\tilde{u_k^B}((\tilde{s}_k, \tilde{s}_{-k}), (\theta_k, \theta_{-k})) = \sum_{s \in S} \prod_{l \in \mathbb{N}} \bar{s_l}(\theta_l, s_l) u_k(s, \theta).$$

Alors, un équilibre de Nash Bayésien est un équilibre de Nash du jeu attendu dans lequel chaque joueur $k \in \mathbb{N}$ tente de maximiser son utilité attendue pour un type donné. Cet équilibre suggère qu'aucun type d'un joueur ne peut avoir un meilleur gain en changeant unilatéralement sa stratégie.

Théoreme 2. *Si tous les ensembles (des joueurs, types et actions) sont finis alors le modèle Bayésien admet un équilibre Bayésien en stratégies mixtes [12].*

2.3 Illustration de l'équilibre de Nash Bayésien :

Pour illustrer l'équilibre de Nash Bayésien, nous allons présenter les deux exemples suivants :

Exemple 10. ***(Duopole de Cournot avec asymétrie de l'information)***
On peut modifier le modèle de duopole de Cournot en introduisant l'asymétrie de l'information en considérant par exemple que la firme 1 a une incertitude quant au coût marginal c_2 de la firme 2. Elle estime que celui-ci peut être égal à c_H (coût élevé) ou c_L (coût faible) avec respectivement les probabilités α et $(1-\alpha)$. Pour la firme 1, la firme 2 peut donc avoir l'une des deux différentes fonctions de gain (profit) possibles, soit :

$$\pi_2(q_1, q_2; c_H) = q_2.[(a - q_1 - q_2) - c_H].$$

$$\pi_2(q_1, q_2; c_L) = q_2.[(a - q_1 - q_2) - c_L].$$

La firme 2 connaît la valeur de son coût marginal et donc n'a aucune incertitude sur sa propre fonction de gain.
On peut par exemple considérer que la firme 2 n'a aucune incertitude quand à c_1, la valeur du coût marginal de la firme 1. Par conséquence, pour la firme 2, la fonction de gain de la firme 1 demeure inchangée, soit

$$\pi_1(q_1, q_2; c_1) = q_1.[(a - q_1 - q_2) - c_1].$$

On dira que l'espace des types de la firme 2 est $\Theta_2 = \{c_L, c_H\}$ et l'espace des types de la firme 1 est $\Theta_1 = \{c_1\}$.

A titre de simplification, considérons que $\theta_1 = a - c_1 = 1$, c'est à dire qu'il n'existe aucune incertitude relative au coût c_1 de la firme 1. En d'autres termes, la firme 2 dispose d'une information complète sur la firme 1. Par contre, la firme 1 n'est pas certaine de la valeur de $\theta_2 = a - c_2$ de la firme 2, c'est à dire du coût c_2 de la firme 2. Elle a seulement des croyances à posteriori sur θ_2 résumées dans les probabilités suivantes :

$$p(\theta_2 = \frac{3}{4}) = \frac{1}{2} \ et \ p(\theta_2 = \frac{5}{4}) = \frac{1}{2}.$$

Lorsque $\theta_2 = \frac{3}{4}$, la firme 2 est dite du type c_H (coût élevé) et lorsque $\theta_2 = \frac{5}{4}$, la firme 2 est dite du type c_L (coût faible).
Le duopole ainsi d'ecrit est un jeu Bayésien à deux joueurs. L'équilibre de Nash Bayésien est le vecteur de stratégies $(q_1^*, q_2^{H^*}, q_2^{L^*})$ où q_1^* est la quantité optimale choisie par la firme 1, $q_2^{H^*}$ la quantité optimale choisie par la firme 2 lorsque celle-ci est du type c_H et $q_2^{L^*}$ la quantité optimale choisie par la firme 2 lorsque celle-ci est du type c_L.
La firme 2 choisit une quantité optimale en fonction de son type (c_H ou c_L), ce qui s'exprime par la fonction $(q_2^*(\theta_2))$. Cette quantité satisfait le programme de maximisation suivant :

$$max \ \pi_2 = q_2(\theta_2 - (q_1 + q_2)).$$

La condition du premier ordre, nécessaire et suffisante, de ce programme implique que :

$$q_2^*(\theta_2) = \frac{\theta_2 - q_1}{2}.$$

Cette condition d'équilibre s'écrit également comme suit :

$$q_2^{H^*} = \frac{\frac{3}{4} - q_1}{2} \ et \ q_2^{L^*} = \frac{\frac{5}{4} - q_1}{2}.$$

La firme 1 choisit la quantité optimale q_1 en fonction de ses croyances sur la valeur de θ_2, c'est à dire celle qui maximise son espérance de profit, soit :

$$max \ \pi_1 = \frac{1}{2}[q_1(1 - (q_1 + q_2^H))] + \frac{1}{2}[q_1(1 - (q_1 + q_2^L))].$$

La condition du premier ordre, nécessaire et suffisante, de ce programme implique que :

$$q_1^* = \frac{2 - (q_2^H + q_2^L)}{4}.$$

L'équilibre de Nash Bayésien du jeu s'obtient par la combinaison des trois conditions d'équilibre, soit :

$$q_1^* = \frac{2 - (q_2^{H^*} + q_2^{L^*})}{4} = \frac{2 - (\frac{\frac{3}{4} - q_1}{2} + \frac{\frac{5}{4} - q_1}{2})}{4}.$$

$$q_1^* = \frac{1}{3}.$$

Ceci implique que :

$$q_2^{H^*} = \frac{\frac{3}{4} - q_1^*}{2} = \frac{5}{24}.$$

$$q_2^{H^*} = \frac{\frac{5}{4} - q_1^*}{2} = \frac{11}{24}.$$

L'équilibre Bayésien est donc le vecteur de stratégies suivantes :

$$(q_1^*, q_2^{H^*}, q_2^{L^*}) = (\frac{1}{3}, \frac{5}{24}, \frac{11}{24}).$$

Exemple 11. ***(Le dilemme du Shérif)***
Un Shérif est face à un suspect, nous supposons que les deux individus sont armés et sont face à face l'un de l'autre avec leur arme en main. Chacun d'eux doit décider si il doit ouvrir le feu ou non. Nous supposons que le Shérif ignore si le suspect armé est un Innocent ou un Criminel. Le Shérif est alors confronté à une situation où l'information sur son adversaire est incomplète lors de sa prise de décision. Le Shérif préférerait tirer si le suspect tire et de ne pas tirer si son adversaire ne tire pas. Le suspect Criminel préférerait tirer même si le Shérif ne fait rien au risque d'être capturé si il ne tire pas. Quant au suspect Innocent, il préférera ne pas tirer même si le Shérif tire. La modélisation de cette situation peut se faire sous forme de jeu Bayésien sur le type du suspect où les caractéristiques du jeu sont définies comme telles :

- ***Les joueurs :*** *d'une part nous avons le suspect armé et d'une autre le Shérif* $\mathbb{N} = \{Suspect, Shérif\} = \{i, j\}$,
- ***Les types des joueurs :*** *le suspect dispose de deux types;* $\Theta_i = \{Criminel, Innocent\}$. *Le Shérif dispose d'un seul type,* $\Theta_j = Normal$,
- ***Les stratégies :***
  - *L'ensemble de stratégies du suspect lorsque son type est* $\theta_i = Criminel$ *est* $A_i = \{Tirer, Ne\ pas\ Tirer\}$ *et lorsque son type est* $\theta_i = Innocent$, *son ensemble de stratégies est un singleton* $A_i = \{Ne\ pas\ Tirer\}$.
  - *L'ensemble des actions disponibles pour le Shérif est* $A_j = \{Tirer, Ne\ pas\ Tirer\}$.
- ***La fonction de croyance à priori :*** $p_j : \Theta_i \to [0, 1]$. *Le Shérif distribue des probabilités sur l'ensemble des types du suspect, avec* μ_0 *la probabilité que le suspect soit de type criminel et* $(1 - \mu_0)$ *pour qu'il soit de type innocent.*
- ***Les fonctions d'utilité :*** *les utilités possibles pour les deux joueurs sont décrites dans les deux tableaux suivants, chaque tableau pour un type particulier du suspect.*

$Type\ 1 : \theta_i = Criminel$

Stratégies	Tirer	Ne pas tirer
Tirer	(0,0)	(2,-1)
Ne pas tirer	(-2,-1)	(-1,2)

$Type\ 2 : \theta_i = Innocent$

Stratégies	Tirer	Ne pas tirer
Ne pas tirer	(-2,-2)	(0,1)

TABLE 2.1 – Forme stratégique du jeu du Dilemme du Shérif.

Pour chercher l'équilibre de Nash Bayésien de ce jeu, nous le transformons en un jeu à information complète mais imparfaite en introduisant un joueur fictif qui est la Nature. La représentation de la forme extensive de ce jeu transformé est donnée par la figure suivante :

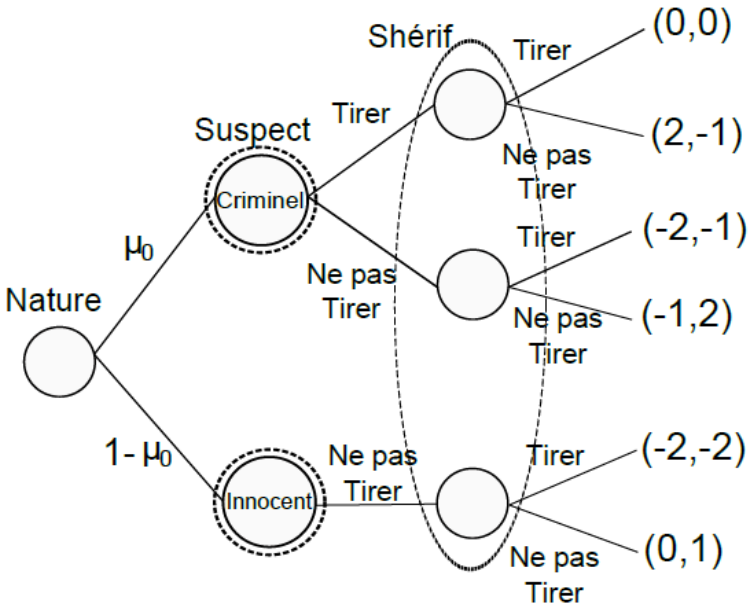

FIGURE 2.2 – Forme extensive du jeu du dilemme du Shérif.

Dans la Figure 2.2, les cercles en pointillés avec un seul noeud de décision signifient que le joueur i connaît le résultat du tirage aléatoire de la Nature (le joueur connaît son type). Quant au cercle en pointillés avec trois noeuds de décision signifie que lorsque le joueur j s'apprête à choisir une stratégie, il ne connaît pas le type du joueur i et peut se retrouver dans l'ensemble d'information à trois éléments sans savoir à quel élément il se trouve au juste.

Dans ce jeu, deux stratégies contingentes au type du suspect sont disponibles pour le premier joueur, qui sont :

- $s_i^1 = (Tirer\ si\ Criminel, Ne\ pas\ Tirer\ si\ Innocent)$;
- $s_i^2 = (Ne\ pas\ Tirer\ si\ Criminel, Ne\ pas\ Tirer\ si\ Innocent)$.

Quant au second joueur, comme il n'a qu'un seul type, ses deux stratégies sont indépendantes de son type, et sont :

- $s_j^1 = Tirer$;
- $s_j^2 = Ne\ pas\ Tirer$.

Nous analysons l'équilibre de Nash Bayésien ENB du jeu en considérant les deux stratégies de chacun des deux joueurs. Nous pouvons déjà éliminer la stratégies Ne pas Tirer du joueur i si il est de type Criminel car elle est strictement dominée par la stratégie Tirer. Si ce joueur est de type Innocent, il choisira son unique stratégie qui est Ne pas Tirer. De ce fait, il nous reste deux issues possibles qui peuvent être des équilibres de Nash Bayésiens, à savoir s_i^1, s_j^1 et s_i^1, s_j^2. Dans un premier temps, le profil de stratégie s_i^1, s_j^1 constitue un ENB ssi :

$$\begin{cases} u_i^B((s_i^1, s_j^1), \theta_i) \geq u_i^B((s_i^2, s_j^1), \theta_i), & \forall \theta_i \in \Theta_i. \\ u_j^B((s_i^1, s_j^1)) \geq u_j^B((s_i^1, s_j^2)). \end{cases}$$

Lorsque le joueur i joue sa stratégie dominante s_i^1 les gains du joueur j en jouant ses stratégies s_j^1 et s_j^2 sont respectivement :

$$u_j^B(s_i^1, s_j^1) = \mu_0(0) + (1 - \mu_0)(-2). \tag{2.1}$$

$$u_j^B(s_i^1, s_j^1) = \mu_0(-1) + (1 - \mu_0)(1). \tag{2.2}$$

La stratégie s_j^1 est la stratégie dominante du joueur j, si :

$$u_j^B((s_i^1, s_j^1)) \geq u_j^B((s_i^1, s_j^2)).$$

$$\Longrightarrow 2\mu_0 - 2 \geq 1 - 2\mu_0 \Longrightarrow \mu_0 \geq \frac{3}{4}.$$

Lorsque $\mu_0 \geq \frac{3}{4}$ la stratégie dominante du joueur j est s_j^2
Par conséquent, si la croyance à priori du Shérif sur le type de son adversaire est plus grande que $\frac{3}{4}$,il choisira la stratégie Tirer, sinon, il choisira de Ne pas Tirer.

2.4 Jeux Bayésiens répétés :

Nous abordons maintenant la classe des jeux Bayésiens dynamiques. Dans cette classe de jeux, on étudie l'issue de l'interaction des joueurs en l'existence simultanée de deux difficultés. En premier lieu, au moins l'un des joueurs ne dispose pas de toute l'information pertinente concernant les caractéristiques des autres joueurs (information incomplète). En second lieu, le jeu est dynamique, ce qui peut donner aux joueurs lors du déroulement du jeu la possibilité d'extraire de nouvelles informations à partir de l'observation des actions passées. Chaque joueur peut donc réviser ses croyances sur l'autre joueur et ce dernier doit en tenir compte lors du choix de son action. Ainsi, dans un jeu dynamique à information incomplète ou imparfaite, il existe non seulement une interaction entre les stratégies des joueurs mais également une interaction entre stratégies et croyances. Pour cela, les croyances des joueurs prennent un rôle central dans le concept d'équilibre approprié à cette classe de jeux. La définition formelle du jeu Bayésien répété est donnée comme suit :

Définition 2.4.1. *(Jeu Bayésien répété)*
Un jeu Bayésien répété est décrit par un 6-tuplet [4] :

$$\mathcal{G}_{\mathcal{R}} = (\mathbb{N}; \{\Theta_k\}_{k\in\mathbb{N}}; p; \{A_k\}_{k\in\mathbb{N}}; \{\Sigma_k\}_{k\in\mathbb{N}}; \{\mu_k\}_{k\in\mathbb{N}}; \{U_k^R\}_{k\in\mathbb{N}});$$

où :

- $\mathbb{N}$ *est l'ensemble des joueurs du jeu composé de N joueurs, Θ_k est l'ensemble des types possibles du joueur $k \in \mathbb{N}$ et p est une distribution de probabilités initiale sur les profils de types $\Theta = \prod_{k=1}^{N} \Theta_k$*
- *A_k est l'ensemble des actions disponibles pour le joueur $k \in \mathbb{N}$. Une action à l'instant t_q du joueur k est notée $a_k(t_q) \in A_k$ $q \geq 0$. Nous notons par $a(t_q) = (a_1(t_q), ..., a_N(t_q))$ un profil d'actions joué par les N joueurs à l'instant t_q. Pour $q \geq 1$, soit $h(t_q) = (a(t_0), a(t_1), ..., a(t_{q-1}))$ la séquence des profils d'actions joués avant t_q. Nous nous référons à une histoire du jeu répété jusqu'à l'instant t_q comme $h(t_q) \in H(t_q)$. $H(t)$ est l'ensemble de toutes les histoires possibles du jeu jusqu'à l'instant t_q. Nous supposons que le jeu démarre à la période t_0, avec $H(t_0) = \emptyset$.*

- Σ_k *est l'ensemble des stratégies de comportement du joueur* $k \in \mathbb{N}$. *Soit* $\Delta(A_k)$ *l'ensemble des distributions de probabilités possibles sur l'ensemble des actions de joueur* k. *Une stratégie de comportement du joueur* k *est une application* $\sigma_k : H(t_q) \times \Theta_k \to \Delta(A_k)$, *associant à chaque histoire possible* $h(t_q) \in H(t_q)$ *et type* $\theta_k \in \Theta_k$, *une distribution de probabilités sur les actions du joueur* k. *Soit* $\bar{\sigma}_k : H(t_q) \times \Theta_k \times A_k \to [0,1]$ *une application qui assigne au joueur* k, *une probabilité de jouer à l'instant* t_q *l'action* $a_k(t_q) \in A_k$, *sachant* $h(t_q) \in H(t_q)$ *et* $\theta_k \in \Theta_k$. *Soit* $\sigma = (\sigma_1, ..., \sigma_N) \in \Sigma = \prod_{k=1}^{N} \Sigma_k$ *un profil de stratégies de comportement qui peut être écrit, également, comme* (σ_k, σ_{-k}) *où* σ_k *la stratégie de comportement jouées par* k *et* σ_{-k} *est les stratégies de comportement jouées par tous les joueurs à l'excepté du joueur* k.
- μ_k *est la croyance à posteriori du joueur* k *définie comme une probabilité conditionnelle que les types de ses adversaires soient* θ_{-k}, *sachant l'histoire* $h(t_q) \in H(t_q)$ *et le type* $\theta_k \in \Theta_k$. *Nous notons la croyance à posteriori du joueur* k *par* $\mu_k(\theta_{-k}/h(t_q), \theta_k)$.
- $U_k^R((\sigma_k, \sigma_{-k})/h(t_q), \theta_k)$ *est la fonction d'utilité du joueur* $k \in \mathbb{N}$ *qui décrit son gain jusqu'à l'instant* tq ; $q \geq 0$, *sachant l'histoire* $h(t_q)$, *son type* $\theta_k \in \Theta_k$, *sa stratégie de comportement* $\sigma_k \in \Sigma_k$ *et les stratégies de comportement des autres joueurs* σ_{-k}, *telle que :*

$$U_k^R((\sigma_k, \sigma_{-k})/h(t_q) = \sum_{\tau=0}^{q} \tilde{U}_k^B((\sigma_k, \sigma_{-k})/h(t_\tau, \theta_k, \mu_k(./h(t_\tau, \theta_k)$$

où

$$\tilde{U}_k^B((\sigma_k, \sigma_{-k})/h(t_q, \theta_k, \mu_k(./h(t_q, \theta_k) = \sum_{\theta_{-k}} \mu_k(\theta_{-k}/h(t_q), \theta_k) \tilde{U}_k((\sigma_k, \sigma_{-k})/h(t_q, (\theta_k), \theta_{-k})).$$

avec

$$\tilde{U}_k(\sigma/h(t_q), \theta) = \sum_{a(t_q) \in A} \prod_{l \in \mathbb{N}} \bar{\sigma}_l(a_l(t_q)/h(t_q), \theta) U_k(a(t_q)/h(t_q), \theta).$$

2.5 Jeux de signalisation de base :

Les jeux de signalisation se réfèrent à une classe de jeux à deux joueurs à information incomplète dans laquelle un seul joueur est informé seulement.

2.5.1 Description du jeu

Un jeu de signalisation basique, dans sa forme la plus simple, est défini comme suit :

- **Joueurs :**il existe trois joueurs en tout
  - Joueur 1 : est l'expéditeur, avec un ensemble d'informations privées ;
  - Joueur 2 : est le récepteur dont l'ensemble d'information est connu de tous ;
  - Joueur 0 : est un joueur fictif, la Nature qui tire le type θ de l'expéditeur à partir d'un ensemble Θ de types.
- **Stratégies :** chacun des deux joueurs, 1 et 2, dispose d'un ensemble de stratégies S_1 et S_2 respectivement :
  - $S_1 = \{s_1^1, s_2^1, ..., s_{n_1}^1\}$;
  - $S_2 = \{s_1^2, s_2^2, ..., s_{n_2}^2\}$;

où
s_j^i :représente la j^{eme} stratégie du i^{eme} joueur et n_1, n_2 représentent le nombre total de stratégies des joueurs 1 et 2, respectivement. L'espace des stratégies mixtes sont Δ_{n_1} et Δ_{n_2} avec les vecteurs de probabilités α^1 et α^2 respectivement. Le joueur 1 observe l'information concernant son type θ et choisit une action $s_i^1 \in S_1$. Le joueur 2, dont le type est connu de tous, observe s_i^1 et choisit une action $s_i^2 \in S_2$. Avant le début du jeu, le second joueur possède des croyances sur le type, θ , du joueur 1 à base desquelles il attribue une probabilité $p(\theta)$ pour chacun des types θ.

La stratégie du joueur 1 est une distribution de probabilité $p(./\theta)$ sur les actions s_i^1 pour chaque type θ , quant à la stratégie du joueur 2 est une distribution de probabilités $p(./s_i^1)$ sur les actions s_i^2 pour chaque stratégie s_i^1 du joueur 1.

- **Utilité :** après que les deux joueurs aient pris leurs actions dans leurs espaces de stratégies respectifs, les utilités sont attribuées selon ces deux actions ainsi que le type de l'expéditeur choisi par la nature. La fonction d'utilité de chacun des joueurs est définie de la manière suivante :

$$u_i : S_1 \times S_2 \times \Theta \to \mathbb{R}, \;\; i = 1, 2.$$

L'utilité du joueur 1 en choisissant la stratégie $\sigma_1(./\theta)$ et que le joueur 2 joue $\sigma_2(./s_i^1)$ est :

$$u_1(\sigma_1, \sigma_2, \theta) = \sum_{i=1}^{n_1} \sum_{j=1}^{n_2} \sigma_1(s_i^1/\theta)\sigma_2(s_2^j/s_i^1)u_1(s_i^1, s_j^2, \theta) \tag{2.3}$$

L'utilité du joueur 2 à la stratégie $\sigma_2(./\theta)$, lorsque le joueur 1 joue $\sigma_1(./\theta)$ est :

$$u_2(\sigma_1, \sigma_2, \theta) = \sum_{\theta} p(\theta)(\sum_{i=1}^{n_1} \sum_{j=1}^{n_2} \sigma_1(s_i^1\theta)/\sigma_2(s_2^j/s_i^1)u_1(s_i^1, s_j^2, \theta)) \tag{2.4}$$

Le récepteur met à jour ses croyances, $p(\theta)$, sur le type de l'expéditeur et à base son choix d'action s_i^2 sur la distribution à posteriori $\mu(./s_i^1)$ sur Θ. L'équilibre Bayésien parfait, que nous définirons ci-dessous, dicte que l'action du joueur 1 notée $\sigma_1^*(./\theta)$ dépend de son type. En connaissant $\sigma_1^*(./\theta)$ et en observant s_i^1 , le joueur 2 peut utiliser la règle de Bayes afin de mettre à jour $p(.)$ et $\mu(./s_i^1)$.

Définition 2.5.1. *(Equilibre Bayésien parfait)*
un équilibre Bayésien parfait (EBP) est une combinaison de stratégies et un ensemble de croyances μ tels qu'à chaque nœud du jeu :

- *Les stratégies dans le reste du jeu sont des meilleures réponses aux stratégies spécifiées par l'équilibre et étant données les croyances d'équilibre,*
- *Les croyances à chaque nœud sont rationnelles, étant données les connaissances fournies par le jeu jusqu'à ce point, elles sont actualisées selon la règle de Bayes quand cela est possible, à partir des croyances à priori et des actions observées des autres joueurs, sous l'hypothèse qu'ils jouent leur stratégie d'équilibre. La première condition correspond à la rationalité séquentielle. La seconde condition impose la cohérence des croyances avec les stratégies. La règle de Bayes doit être appliquée en accord avec les actions précisées dans les stratégies d'équilibre, en tenant compte du fait que pour chacun des nœuds contenus dans un ensemble d'information, la probabilité d'être atteint dépend des stratégies d'équilibre des joueurs qui jouent avant ce nœud.*

2.5.2 Croyances et révision Bayésienne :

On appelle révision Bayésienne, ou bien le calcul des probabilités à posteriori, ce processus par lequel un joueur incertain sur le type des autres joueurs incorpore l'information qu'il reçoit et modifie ses croyances, c'est à dire la distribution du ou des paramètres inconnus. Pour la mise à jour des croyances, nous faisons recours à la formule de Bayes. Dans l'approche de Harsanyi, un joueur donné $k \in \mathbb{N}$ connaissant son type θ_k, et la distribution jointe $p(\theta)$, ainsi que les actions choisies à l'instant t_q, chaque joueur peut estimer la probabilité des types θ_{-k} des autres joueurs en se référant à la formule de Bayes :

$$\mu_k(\theta_l/(h(t), a_l(t))) = \frac{\mu_k(\theta_l/(h(t))P(a_l(t)/h(t), \theta_l))}{\sum_{\hat{\theta}_l} \mu_k(\hat{\theta}_l/(h(t))P(a_l(t)/h(t), \hat{\theta}_l)}.$$

La formule de Bayes permet de réviser les probabilités (croyances) après avoir observé un événement donné qui est dans notre cas correspond au profil de stratégies joué par les autres joueurs à l'instant t_q.

2.5.3 L'importance des croyances dans le concept d'équilibre d'un jeu Bayésien dynamique :

L'interaction entre stratégies et croyances est ainsi au cœur de la résolution d'un jeu Bayésien dynamique. Le concept d'équilibre approprié pour cette classe de jeux est l'équilibre de Nash Bayésien parfait, ou tout simplement équilibre Bayésien parfait. L'équilibre Bayésien parfait est une synthèse entre l'équilibre Bayésien des jeux à information incomplète et l'équilibre parfait des jeux dynamiques. Mais, l'équilibre Bayésien parfait n'est pas seulement cette synthèse car les joueurs peuvent réviser leurs croyances durant le déroulement du jeu. Nous avons vu que dans un jeu dynamique , le principe de rationalité séquentielle implique qu'un équilibre du jeu est également un équilibre dans tous les sous-jeux de l'équilibre (perfection en sous-jeux). L'introduction du principe de rationalité séquentielle a pu ainsi permettre d'écarter les équilibres de Nash non raisonnables. Mais, lorsque le jeu dynamique est à information incomplète (ou imparfaite), le principe de rationalité séquentielle peut être insuffisant.

Les croyances des joueurs aux ensembles d'information atteints à l'équilibre (appartenant au sentier d'équilibre) deviennent un élément explicite de l'équilibre. Ce concept d'équilibre est basé sur deux exigences :

- **Principe de rationalité séquentielle :** En tout point du jeu (ensembles d'information singletons ou non), les joueurs choisissent des actions optimales (maximisation de l'espérance de gain) étant données les croyances sur les actions choisies jusqu'à ce point du jeu.
- **Cohérence des croyances :** les croyances doivent être consistantes avec les stratégies jouées à cet équilibre.

2.6 Conclusion

Ce chapitre avait pour objectif de rappeler dans un premier temps les définitions de base des jeux Bayésiens statiques, les stratégies, les gains des joueurs, notamment le concept d'équilibre étudié pour ce type de jeux, ainsi que quelques exemples d'applications. Puis, nous avons présenté aussi les éléments essentiels des jeux Bayésiens dynamiques plus particulièrement les jeux Bayésiens répétés qui seront utiles pour aborder le quatrième chapitre.

CHAPITRE 3

RÉSEAUX INFORMATIQUES ET CONCEPTS DE SÉCURITÉ

3.1 Introduction

La sécurité informatique est de nos jours devenue un problème majeur dans la gestion des réseaux informatiques ainsi que pour les particuliers toujours plus nombreux à se connecter à Internet. La transmission d'informations sensibles et le désir d'assurer la confidentialité de celles-ci est devenue un point primordial dans la mise en place de réseaux informatiques. Dans ce chapitre, nous allons parler de la sécurité informatique, de ses objectifs ainsi que des différentes menaces.

3.2 Réseau informatique

Un réseau informatique est un ensemble d'éléments matériels reliés entre eux dans le but de permettre aux utilisateurs de partager des ressources et d'échanger des informations sous forme numérique dont l'intérêt est de diminuer les coûts grâce au partage des données et des périphériques.

A l'origine, la connexion entre les différents éléments du réseau se faisait via des câbles et des fils, mais à travers le temps, le besoin à plus de mobilité et à pouvoir partager ou échanger de l'information à tout moment, en utilisant des dispositifs mobiles, a fait naître une nouvelle technologie des réseaux sans fil.

Aujourd'hui, les réseaux sans fil sont de plus en plus populaires du fait de leur facilité de déploiement. Ces réseaux jouent un rôle crucial au sein des réseaux informatiques. Ils offrent des solutions ouvertes pour fournir la mobilité ainsi que des services essentiels là où l'installation d'infrastructures n'est pas possible.

3.2.1 Un aperçu des différents réseaux informatiques

Les réseaux sont mis en place dans le but notamment de transférer des données d'un système à un autre ou de fournir des ressources partagées comme par exemple les serveurs, les bases de données ou une imprimante sur le réseau. Il est possible selon la taille et la portée du réseau informatique de différencier et de catégoriser les réseaux. Voici ci-dessous les principales catégories de réseaux informatiques :

- Personal Area Network (PAN) ou réseau personnel,
- Local Area Network (LAN) ou réseau local,
- Metropolitan Area Network (MAN) ou réseau métropolitain,
- Wide Area Network (WAN) ou réseau étendu,
- Global Area Network (GAN) ou réseau global.

La connexion physique qui relie ces types de réseau peut être câblée (filaire) ou bien réalisée à l'aide de la technologie sans fil. Bien souvent les réseaux de communication physique constituent le fondement de plusieurs réseaux logiques, appelés VPN (Virtuel Private Network, ou réseau privé virtuel en français). Ceux-ci utilisent un moyen de transmission physique commun, par exemple un câble de fibre optique et, lors du transfert des données, sont assignés à des réseaux virtuels logiquement différents au moyen d'un logiciel de VPN créant un tunnel (ou logiciel de tunneling).

3.3 Réseau wifi

La norme Wifi (Wireless Fidelity) est le nom commercial donné à la norme IEEE (Institue of Electrical and Electronics Engineers) 802.11. Grâce aux normes Wifi, il est possible de créer des réseaux locaux sans fil. En pratique, le Wifi permet de relier des ordinateurs portables, des machines de bureau,...

3.4 Réseau ad hoc

Un réseau mobile ad hoc, appelé aussi MANET (Mobile Ad hoc NETwork), est un ensemble autonome et coopératif de noeuds mobiles qui se déplacent et communiquent de manière autonome par une transmission sans fil appelée ondes radio qui ne suppose pas d'infrastructure préexistante. Un noeud peut à la fois communiquer directement avec d'autres noeuds ou servir de relais. Un relais permet à des noeuds se trouvant hors de leur rayon de transmission les uns des autres de communiquer. Ces réseaux sont dits ad hoc dans la mesure où ils ne nécessitent pas d'infrastructure fixe. Ils peuvent exister temporairement pour répondre à un besoin ponctuel de communication.

3.4.1 Modélisation d'un réseau ad hoc

Un réseau ad hoc peut être modélisé par un graphe $G^t = (V^t, E^t)$, où :

- V^t représente l'ensemble des nœuds (i.e. les unités ou les hôtes mobiles) du réseau.
- E^t modélise l'ensemble des connections qui existent entre ces nœuds.

Si $e = (u, v) \in E^t$, cela veut dire que les nœuds u et v sont en mesure de communiquer directement à l'instant t [9].

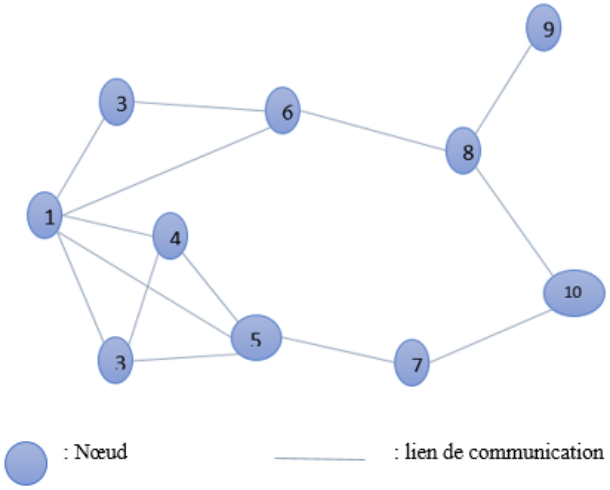

FIGURE 3.1 – Modélisation d'un réseau ad hoc par un graphe

3.4.2 Caractéristiques des réseaux ad hoc :

- **Description :** Un réseau ad hoc est donc constitué d'entités, mobiles, qui communiquent entre elles. Chaque entité communique directement avec sa voisine. Pour communiquer avec d'autres entités, il lui est nécessaire de faire passer ses données par d'autres qui se chargeront de les acheminer. Ainsi, le fonctionnement d'un réseau ad hoc le différencie notablement d'un réseau comme le réseau GSM (Global System for Mobile communications).
- **Liens asymétriques :** En théorie, les liens sont symétriques car on a un affaiblissement du signal inversement proportionnel à la distance entre l'émetteur et le récepteur. Mais en pratiques ils sont asymétriques. On peut noter un déphasage dû aux multiples réflexions du signal sur différents obstacles. De plus, la route inverse n'est pas forcément la même que la route directe.
- **Sécurité limitée :** Vu les contraintes précédentes, les méthodes de sécurité (cryptage,... etc.) sont réduites ce qui augmente le risque d'attaques ou de piratage. En effet, les réseaux mobiles ad hoc sont considérés comme étant très fragiles en matière d'attaques en tout genre. Lorsqu'une station émet des données, toute unité équipée d'un dispositif d'écoute (ici les cartes WiFi) a la possibilité d'intercepter ces données. Les pirates informatiques peuvent donc intercepter les données d'une manière directe en utilisant des antennes pirates (car les données circulent par voie hertzienne) ou bien obliger une station à consommer une bonne partie de ses ressources d'énergie en l'inondant de toutes sortes de requêtes inutiles.
- **Contraintes sur la bande passante :** Les réseaux sans fil se basant sur le partage des médiums de communication, alors la bande passante réservée à un hôte sera relativement modeste. Ceci implique des liens sans fil à capacité variable. Pour les réseaux ad hoc, les messages vont être cryptés. Nous avons également des clés « de groupe ». Nous savons que seules les stations en possession de clé peuvent décrypter les messages. Les mécanismes mis en place doivent permettre aux stations qui se sont déconnectée de pouvoir récupérer la ou les clés permettant les décryptages lors de leur reconnexion [11].

3.4.3 Avantages et inconvénients des réseaux ad hoc

Les réseaux ad hoc ont des avantages et des inconvénients, dans ce qui suit, nous citons quelques-unes des avantages.

Avantages des réseaux ad hoc :

Les réseaux ad hoc mobiles sont utilisés généralement dans toute application ou, le déploiement d'une infrastructure réseau filaire est trop contraignant, soit à cause de la difficulté de la mise en place, ou à cause de la durée d'installation qui peut être longue. Possédant des caractéristiques particulières comparées aux autres réseaux sans fils, les réseaux MANET peuvent donc être un atout considérable dans de nombreuses situations pour les raisons suivantes :

- **Adaptation :** la propriété sans fil offre plus de flexibilité au réseau. En éliminant les connexions filaires, les réseaux MANETs s'adaptent facilement aux changements dans la configuration du réseau.
- **Facilité de déploiement :** l'absence de câblage donne plus de souplesse et permet de déployer un réseau ad hoc facilement et rapidement. Les réseaux MANETs peuvent être déployés dans un environnement quelconque permettant, ainsi, d'économiser tout le temps de déploiement et d'installation du matériel nécessaire.
- **Coûts :** le déploiement d'un réseau ad hoc ne nécessite pas d'installer des stations de base. Les mobiles sont les seules entités physiques nécessaires pour déployer un tel réseau. Ceci se traduit par une réduction significative des coûts de mise en place du réseau. Consommation énergétique : les portées de communication peuvent être largement réduites en mode ad hoc, ce l'a permet d'économiser beaucoup d'énergie. Extensibilité du réseau : l'une des propriétés les plus importantes d'un réseau ad hoc est la possibilité de l'étendre, et d'augmenter sa taille très facilement, sans nécessiter trop de moyens. Pour ce faire, il suffit de procéder à quelques configurations au niveau du nouveau nœud pour que ce dernier fonctionne au sein du réseau.
- **Permet la mobilité :** les réseaux MANET permettent une certaine mobilité à leurs nœuds. De ce fait, ces derniers peuvent se déplacer librement à condition de ne pas s'éloigner trop les uns des autres pour garder leur connectivité.
- **Tolérance aux pannes :** dans un réseau MANET, les seuls éléments pouvant tombé en panne sont les terminaux eux-mêmes. De manière globale, si une station qui sert au routage tombe en panne, elle peut être remplacée par une autre, et seul le possesseur de cette station en sera affecté. Autrement dit, il n'y a pas de panne pénalisante.

Inconvénients d'un réseau ad hoc :

Les réseaux ad hoc mobiles ne présentent pas seulement des avantages, mais aussi des inconvénients [20] :

- **Topologie non prédictible :** la topologie dynamique due aux déplacements des nœuds rend son étude très difficile.
- **Capacités limitées :** la consommation d'énergie dans un réseau ad hoc dépend de la portée de communication des nœuds. Plus la portée est importante, plus les communications demandent de l'énergie. Il faut donc trouver un compromis entre les deux pour assurer la connectivité du réseau.

- **Taux d'erreur important :** un taux d'erreur important dû aux collisions pourraient survenir si le nombre de nœuds qui partagent le même medium est important.
- **Sécurité :** les réseaux ad hoc ne permettent pas d'utiliser un matériel spécifique pour empêcher les accès non autorisés, ce qui fait que la confidentialité de l'information échangée entre les nœuds peut ne pas être garantie.
- **Absence d'infrastructure :** un MANET se distingue des autres réseaux mobiles par la propriété d'absence d'infrastructure préexistante. Les nœuds mobiles sont eux-mêmes responsables de l'établissement et le maintien de la connectivité du réseau.
- **Autonomie des nœuds :** chaque terminal est un nœud autonome. Il peut fonctionner d'une part comme étant un nœud ordinaire et, d'autre part, comme étant un routeur qui a pour fonction de router l'information qu'il reçoit d'une source vers une destination.
- **Routage Multi-sauts :** dans un MANET, un terminal peut communiquer avec n'importe quel autre terminal à l'intérieur du réseau. Ces terminaux agissent en tant que routeurs et se chargent de relayer les messages en passant via un ou plusieurs nœuds intermédiaires.
- **Liaison à débits variables et bande passante limitée :** les liaisons radio présentent des débits variables et ont généralement une bande passante de capacité limitée, inférieure à celle des liaisons filaires. La demande sur les applications dépasse souvent la capacité du réseau, et cette demande ne cessera de croître avec l'augmentation des traitements multimédias et des applications basées sur les réseaux.
- **Sécurité physique limitée :** de leur nature, les réseaux sans fil sont très sensibles aux attaques extérieures. Cela se justifie par les contraintes et limitations physiques qui font que le contrôle des données transférées doit être réduit.

3.4.4 Domaines d'application des réseaux mobiles ad hoc

Les réseaux ad hoc ne nécessitent pas d'infrastructure pour fonctionner. De ce fait, ils sont facilement mis en œuvre et ne nécessitent aucun coût supplémentaire lié à l'installation. La mobilité des nœuds n'étant plus dépendante d'un point fixe, ces réseaux sont facilement extensibles et peuvent couvrir de longues distances. Tous ces avantages en font le mode prisé pour les applications militaires ou lors des catastrophes naturelles où il n'y a pas d'infrastructure au service des équipements [10] :

- **Le domaine militaire :** Il adopte une recherche plus intensive pour obtenir les meilleures performances. Un réseau ad hoc doit pouvoir être employé à la demande, fonctionner sans infrastructure de communication préexistante et bien sûr tolérer la mobilité. Il doit aussi garantir des échanges fiables et de qualité, car de plus en plus les informations échangées sur le champ de bataille comportent des images et des vidéos.
- **Les services d'urgence :** Ils peuvent être utilisés pour la mise en communication d'unités de secours, lorsqu'une catastrophe naturelle (telle qu'un tremblement de terre, une inondation) a détruit les infrastructures de télécommunications et que l'établissement d'une liaison satellite pour chaque entité en communication représente un coût trop élevé.
- **Des applications civiles :** Outre les applications scientifiques et militaires, des applications civiles ont commencé à tirer profit des caractéristiques des réseaux ad

hoc . Ils peuvent être utilisés pour la mise en place instantanée d'un réseau reliant plusieurs ordinateurs entre eux. Ils s'avèrent particulièrement utiles lors de l'organisation d'événements tels que des colloques afin de proposer un réseau de partage de l'information.

- **Applications commerciales :** Les réseaux ad hoc sont utilisés pour un gain électronique distant en utilisant l'accès mobile à l'internet.
- **Le travail collaboratif et les communications dans des entreprises ou bâtiments :** dans le cadre d'une réunion ou d'une conférence par exemple.
- **Réseaux de senseurs :** Les capteurs, chargés de mesurer les propriétés physiques des environnements (comme la température, la pression...), sont dispersés (le plus souvent lâchés d'un avion ou d'un hélicoptère) par centaines, voire par milliers sur le site, effectuent leurs mesures et envoient les résultats à une station par l'intermédiaire d'un routage ad hoc à travers le réseau.
- **Le cadre informatique :** Dans le cadre de l'informatique, les réseaux ad hoc peuvent servir à établir des liens entre ses différents composants. Dans ce cas, on parle non plus de LAN (Local Area Network), mais de PAN (Personnal Area Network).

Les applications potentielles des réseaux ad hoc sont nombreuses. Par exemple, nous pouvons penser qu'un groupe de personnes avec des ordinateurs portables lors d'une conférence qui souhaite échanger des fichiers peut rapidement mettre en place un réseau ad hoc sans avoir recours à une infrastructure supplémentaire. Les réseaux ad hoc sont idéals dans des zones où un tremblement de terre ou d'autres catastrophes naturelles ont détruit les infrastructures de communication [22]. D'une façon générale, les réseaux ad hoc sont utilisés dans toute application où le déploiement d'une infrastructure réseau filaire est trop contraignant, soit parce qu'il est difficile à mettre en place, soit parce que la durée d'installation du réseau ne justifie pas de câblage à demeure.

3.4.5 Principales catégories de communications

La communication dans les réseaux ad hoc est soumise à divers phénomènes qui caractérisent les communications par onde radio. La plus connue est une forte atténuation du signal avec la distance, qui empêche deux hôtes trop éloignés l'un de l'autre de communiquer ensemble. Pour fonctionner correctement, un réseau ad hoc doit requérir deux grandes fonctions :

- Le routage : dont le but est de trouver un chemin possible entre deux hôtes donnés.
- Le transport qui consiste à acheminer les paquets le long d'un chemin prédéfini.

Dans cette section, nous donnons un type transport nommé diffusion ensuite nous présentons brièvement le routage et sa difficulté.

Diffusion

La diffusion ou l'inondation consiste à transmettre un paquet dans le réseau entier. Un nœud qui initie l'inondation envoie le paquet à tous ses voisins directs. De même, si un nœud quelconque du réseau reçoit le paquet, il le rediffuse à tous ses voisins. Ce comportement se répète jusqu'à ce que le paquet atteigne tous les nœuds du réseau . Le mécanisme de diffusion est utilisé généralement dans la première phase du routage plus exactement dans la procédure de découverte des routes, et cela dans le cas où le nœud source ne connaît pas la localisation exacte de la destination.

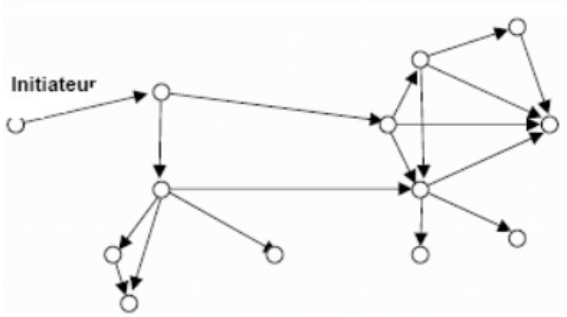

FIGURE 3.2 – Le mécanisme de diffusion

Routage :

Le routage est une méthode à travers laquelle on fait transiter une information donnée depuis un certain émetteur vers un destinataire bien précis. Le problème de routage ne se résume pas seulement à trouver un chemin entre les deux nœuds du réseau, mais encore à trouver un acheminement optimal[6].Par exemple, si on suppose que les coûts des liens sont identiques, le chemin indiqué dans la Figure 3.4 est le chemin optimal reliant la station source et la station destination. Une bonne stratégie de routage utilise ce chemin dans le transfert des données entres les deux stations.

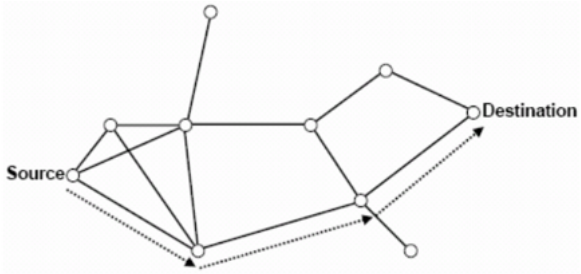

FIGURE 3.3 – Le chemin utilisé dans le routage entre la source et la distination

Le problème qui se pose dans le contexte des réseaux ad hoc est l'adaptation de la méthode d'acheminement utilisée avec le grand nombre d'unités existant dans un environnement caractérisé par de modestes capacités de calcul et de sauvegarde et de changements rapides de topologies. Il semble donc important que toute conception de protocole de routage doit étudier les problèmes suivants :

- La minimisation de la charge du réseau,
- Offrir un support pour pouvoir effectuer des communications multipoints fiables,
- Assurer un routage optimal,
- Offrir une bonne qualité concernant le temps de latence.

3.5 Sécurité informatique

La sécurité informatique est l'ensemble des moyens techniques, organisationnels, juridiques et humains nécessaire et mis en place pour conserver, rétablir et garantir la sécurité

du système d'information. Assurer la sécurité du système d'information est une activité du management du système d'information. « Le système d'information représente un patrimoine essentiel de l'organisation, qu'il convient de protéger. La sécurité informatique consiste à garantir que les ressources matérielles ou logicielles d'une organisation sont uniquement utilisées dans le cadre prévu » [24].

3.5.1 Objectifs et principaux services de la sécurité informatique

La sécurité d'un système informatique a pour objectif la protection des informations contre toutes divulgations, altération ou destruction. C'est pourquoi, nous pouvons distinguer plusieurs types d'enjeux [18] :

- **Confidentialité :** Seules les personnes autorisées ont accès aux informations qui leur sont destinées. Tout accès indésirable doit être empêché.
- **Authentification :** Les utilisateurs doivent prouver leur identité par l'usage de code d'accès. Il ne faut pas mélanger identification et authentification : dans le premier cas, l'utilisateur n'est reconnu que par son identifiant, tandis que dans le deuxième cas, il doit fournir un mot de passe ou un élément que lui-seul connaît. Cela permet de gérer les droits d'accès aux ressources concernées et maintenir la confiance dans les relations d'échange.
- **Intégrité :** Assurer que les informations n'ont pas été altérées par des personnes non autorisées.
- **Disponibilité :** Le système doit fonctionner sans faille durant les plages d'utilisation prévues, garantir l'accès aux services et ressources installées avec le temps de réponse attendu .

3.5.2 Terminologie de la sécurité informatique

La sécurité informatique utilise des termes propres à elle. De manière à bien comprendre ce rapport, il est nécessaire d'en définir certains :

- **Vulnérabilité :** Dans le domaine de la sécurité informatique, une vulnérabilité ou faille est une faiblesse dans un système informatique, permettant à un attaquant de porter atteinte à l'intégrité de ce système, c'est-à-dire à son fonctionnement normal, à la confidentialité et l'intégrité des données qu'il contient.
  Ces faiblesses conduisent à l'exploitation des ressources informatiques par des menaces dans le but de les compromettre et cela peut causer des pertes importantes.
  Ces vulnérabilités sont la conséquence des imp erfections dans la conception, la mise en œuvre ou l'utilisation d'un composant matériel ou logiciel du système.
- **Les attaques :** une attaque est l'exploitation d'une vulnérabilité d'un système informatique susceptible de lui causer des dommages. Il peut y avoir plusieurs attaques pour une même vulnérabilité mais toutes les vulnérabilités ne sont pas exploitables.
  Les attaques peuvent à première vue être classées en 2 grandes catégories :
  Attaques passives : consistent à écouter sans modifier les données ou le fonctionnement du réseau. Elles sont généralement indétectables mais une prévention est possible.

Attaques actives : consistent à modifier des données ou des messages, à s'introduire dans des équipements réseau ou à perturber le bon fonctionnement de ce réseau. Noter qu'une attaque active peut être exécutée sans la capacité d'écoute. De plus, il n'y a généralement pas de prévention possible pour ces attaques, bien qu'elles soient détectables.

- **Contre-mesures :** ce sont les procédures ou techniques permettant de résoudre une vulnérabilité ou de contrer une attaque spécifique.
- **Menaces :** ce sont des adversaires déterminés et capables de monter une attaque en exploitant une vulnérabilité.
- **Intrusions :** on appelle intrusion l'ensemble des actions non autorisées ou l'abus d'utilisation d'un système informatique qui ont pour but de compromettre l'intégrité, la confidentialité ou la disponibilité d'une ressource. Ces actions de franchissement d'un accès non-autorisé ou de manipulation d'une ressource, peuvent être menées par un individu externe n'ayant aucun privilège sur les ressources d'un système, ou par un individu interne qui outrepasse ses privilèges.

3.6 Mécanismes de défense

Afin d'assurer la sécurité d'un système informatique, il existe plusieurs mécanismes. D'une manière globale, la sécurité d'un système informatique peut être comparée à une chaîne de maillons plus ou moins résistants. Elle est alors caractérisée par le niveau de sécurité du maillon le plus faible.

3.6.1 Politique de sécurité

La politique de sécurité est donc l'ensemble des orientations suivies par une entité en termes de sécurité. À ce titre, elle se doit d'être élaborée au niveau de la direction de l'organisation concernée, car elle concerne tous les utilisateurs du système pour qu'ils puissent utiliser le système informatique en toute confiance.

Après une étude des risques et avant de mettre en place des mécanismes de protection, il faut préparer une politique à l'égard de la sécurité. C'est elle qui fixe les principaux paramètres, notamment les niveaux de tolérance et les coûts acceptables.

Définir une politique de sécurité revient à :

- Élaborer des règles et des procédures, installer des outils techniques dans les différents services de l'organisation (autour de l'informatique).
- Définir les actions à entreprendre et les personnes à contacter en cas de détection d'une intrusion.
- Sensibiliser les utilisateurs aux problèmes liés à la sécurité des systèmes d'informations.
- Préciser les rôles et responsabilités.

3.6.2 Moyens techniques

De nombreux moyens techniques peuvent être mis en oeuvre pour assurer une sécurité du système informatique. Il convient de choisir les moyens nécessaires, suffisants et justes. Voici une liste non exhaustive de moyens techniques pouvant répondre à certains besoins en termes de sécurité informatique :

- **Contrôle des accès au système informatique**
  En vérifiant les droits d'accès d'un acteur dans le système soit par mot de passe, ou autres dispositifs d'identification.
- **Surveillance du réseau**
  - Sniffer ou analyseur de paquets : est un logiciel pouvant lire ou enregistrer des données transitant par le biais d'un réseau local non-commuté. Il permet ainsi la résolution de problèmes réseaux en visualisant ce qui passe à travers l'interface réseau, mais peut également servir à effectuer de la rétro-ingénierie réseau à des buts d'interopérabilité, de sécurité ou de résolution de problèmes.
  - Système de détection d'intrusion : repère les activités anormales ou suspectes sur le réseau. Ne détecte pas les accès incorrects mais autorisés par un utilisateur légitime. Mauvaise détection : taux de faux positifs, faux négatifs .
- **Sécurité applicative**
  - Séparation des privilèges : est un principe qui dicte que chaque fonctionnalité ne doit posséder que les privilèges et ressources nécessaires à son exécution, et rien de plus.
  - Audit de code : est une pratique consistant à parcourir le code source d'un logiciel, en identifiant ses points de vulnérabilité, afin de s'assurer du respect de règles précises .
  - Rétro-ingénierie : est l'activité qui consiste à étudier un objet pour en déterminer le fonctionnement interne ou la méthode de fabrication .
- **Emploi de technologies ad hoc**
  - Pare-feu : un élément (logiciel ou matériel) du réseau informatique contrôlant les communications qui le traversent. Il a pour fonction de faire respecter la politique de sécurité du réseau, celle-ci définissant quels sont les communications autorisées ou interdites .
  - UTM : Unified threat management (en français : gestion unifiée des menaces) est un terme utilisé pour décrire des pare-feu réseau qui possèdent de nombreuses fonctionnalités supplémentaires qui ne sont pas disponibles dans les pare-feux traditionnels. Parmi les fonctionnalités présentes dans un UTM, outre le pare-feu traditionnel, on cite généralement le filtrage anti-spam, un logiciel antivirus, un système de détection ou de prévention d'intrusion (IDS ou IPS), et un filtrage de contenu applicatif (filtrage URL).
  - Anti-logiciels malveillants (antivirus, anti-spam, anti-logiciel espion) : Un antivirus est un logiciel conçu pour identifier, neutraliser et éliminer des logiciels malveillants .
- **Cryptographie**

  La cryptographie est une des disciplines de la cryptologie dont le but est de protéger des messages assurant ainsi la confidentialité, l'authenticité et l'intégrité en utilisant souvent des clés .
  - Authentification forte : est une procédure d'identification qui requiert la concaténation d'au moins deux facteurs d'authentification. Par exemple : Un mot de passe et une empreinte biométrique .

- Chiffrement : aussi appelé cryptage, est en cryptographie le procédé grâce auquel on peut rendre la compréhension d'un document impossible à toute personne qui n'a pas la clé de (dé)chiffrement.

3.6.3 Principaux composants et mode de fonctionnement des IDSs

Les systèmes de détection d'intrusion fonctionnent comme ceci : surveiller les données qui circulent dans le réseau, chercher des intrusions dans le système et initier une réponse appropriée (e.g. contacter l'administrateur du système, démarrer des représailles automatiques, etc.).

IDS (Intrusion Detection System)

Un système de détection d'intrusions est un processus de surveillance des événements se trouvant dans un système d'ordinateurs ou du réseau. Il permet de détecter en temps réel et de façon continue des tentatives d'intrusion. Une fois que l'IDS est installé et configuré, il interagit avec l'environnement dans lequel il est implanté de façon à pouvoir le protéger d'éventuelles intrusions. Durant la phase de détection, il capte l'information via une source de donnée, il l'analyse et il transmet les résultats de l'analyse à l'opérateur qui agit en conséquence, selon qu'il y ait ou pas d'attaques. Il existe trois types de systèmes de détection d'intrusion :

- **Systèmes de détection des intrusions de type hôte (HIDS) :** ces systèmes sont en fait les premiers systèmes mis en œuvre pour la détection d'intrusion. Ils analysent exclusivement les données concernant le nœud où l'IDS est installé.
  Toute décision prise est basée sur les informations recueillies au niveau de ce nœud. Ces IDSs utilisent deux types de source pour fournir une information sur l'activité : les fichiers logs (fichier qui enregistre toute activité sur un système en veille) et les traces d'audit (paquets entrant/sortant du nœud, etc.). Cette technologie permet de déterminer l'impact d'une attaque sur le nœud concerné.
- **Systèmes de détection des intrusions réseaux (NIDS) :** ces systèmes sont mis en œuvre pour la protection des réseaux. Ils visent à intercepter et analyser les paquets qui circulent dans le réseau pour déterminer si une attaque a lieu.
  Toutes les communications dans le réseau sans fil sont menées dans l'air et un nœud peut entendre le trafic passant à partir d'un nœud voisin (le mode promiscuité). Par conséquent, les NIDSs des nœuds peuvent mutuellement vérifier le trafic du réseau et examiner individuellement chaque paquet.
- **Systèmes de détection des intrusions hybrides :** ces IDSs hybrides rassemblent les caractéristiques de chacun des HIDSs et des NIDSs. En effet, un IDS hybride peut écouter le traffic qui lui est exclusivement destiné comme il peut également écouter le traffic du réseau et cela en fonction du rôle qu'il joue dans le réseau ou de sa configuration. Les avantages émanant de ces IDSs hybrides sont la réduction de fausses alertes et une meilleure corrélation de données d'observation et d'analyse.

3.6.4 Défis des IDSs dans les MANETs

La mise en place des systèmes de détection d'intrusion dans les réseaux ad hoc doivent inévitablement faire face aux contraintes liées directement aux caractéristiques de ces

réseaux. En effet, la conception et la mise en œuvre des IDSs devraient tenir compte des restrictions liées aux ressources et à l'environnement du réseau de telle sorte que l'implémentation d'un IDS sur un nœud ne le rende pas plus vulnérable qu'il ne l'est déjà. Il est donc important de considérer les différents compromis, qui entourent l'installation des IDSs, entre les performances souhaitées et les limitations des réseaux ad hoc.

- **Compromis sur la sécurité :** Une sécurité maximale est souhaitée dans un environnement décentralisé et distribué mais n'est, hélas, pas envisageable. En effet, pour augmenter la précision de la détection d'intrusion, il est nécessaire, voire indispensable, de mettre plus de ressources au profit de l'IDS comme par exemple augmenter le nombre de paquets à analyser. Cependant, la capacité de traitement de l'IDS représente une limite. En réalité, lorsque le trafic sur le lien dépasse la capacité de traitement de l'IDS, ce dernier laisse passer des paquets potentiellement dangereux qui ne seront pas analysés. Par ailleurs, dans plusieurs cas, la capacité de détection d'un IDS est limitée par sa mémoire, autrement dit, sa capacité à se souvenir, dans le temps, d'événements ayant eu lieu sur plusieurs hôtes pour pouvoir les corréler entre eux. Bien que la détection de certaines attaques ne nécessite pas que le système se "souvienne" de plusieurs événements, certaines nécessitent que le système conserve en mémoire des états précédents pour la détection de certaines intrusions. Pour cette raison, il est important de chercher un compromis entre les ressources déployées, les capacités de calcul et la précision de détection de telle sorte à ne pas altérer la sécurité du réseau.
- **Compromis sur l'énergie :** Déployer un grand nombre de systèmes de détection d'intrusion sur la totalité des nœuds du réseau et augmenter la fréquence d'utilisation de ces IDSs, donnerait une détection d'intrusion plus efficace, des résultats en temps réel et augmenterait la sécurité. Nonobstant, cela épuiserait les ressources du réseau et diminuerait la durée de vie de ce dernier. Il faudrait alors chercher à trouver un compromis qui allierait le nombre d'IDSs à activer sur le réseau ainsi que la fréquence de leur activation à un coût en ressources relativement bas.

Métriques d'évaluation des IDSs :

Lors de la conception d'un modèle de détection d'intrusion, il est important de s'intéresser à un ensemble de métriques qui quantifie le niveau de sécurité et utilise au mieux les ressources telles que la consommation d'énergie et l'espace de stockage. Ces indicateurs de performance permettent à un administrateur réseau de choisir le meilleur système de détection d'intrusion et une optimisation de l'emplacement des IDSs dans le réseau. En conséquence, les métriques suivantes sont considérées comme des caractéristiques importantes pour une bonne conception d'un modèle de détection d'intrusion :

- **Taux de détection :** représente le pourcentage de détection d'attaques sur le nombre total d'attaques.
- **Taux de faux positifs :** constitue le rapport entre le nombre des connexions normales classées comme étant une anomalie sur le nombre total des connexions normales.
- **Taux de faux négatifs :** à l'inverse du taux de détection, cette métrique est définie par le rapport des fausses détections d'attaques sur le nombre total d'attaques.
- **Consommation d'énergie :** cette métrique mesure l'énergie consommée par chaque IDS et l'énergie totale du modèle IDS qui est définie comme étant la somme de l'énergie consommée par chaque IDS installé sur les nœuds du réseau.

3.7 Pourquoi appliquer la théorie des jeux aux réseaux ?

La théorie des jeux peut être utilisée dans tous les domaines où interviennent des questions de compétition stratégique. Cela va de l'économie à l'étude du réseau routier. La percée de cette théorie dans les réseaux de télécommunication (Networking Engineering Games) date des années 1990. Un nouveau domaine d'étude a émergé autour du routage, du contrôle de flux, du contrôle d'accès et de puissance, et de la sécurité du réseau. L'intérêt de la théorie des jeux pour la conception même des réseaux s'est imposé avec la multiplication d'opérateurs concurrents et la compétition accrue entre fournisseurs de service, fournisseurs de contenus et fabricants d'équipements pour les réseaux. Un grand nombre de problèmes intéressant la théorie des jeux ont surgi avec le succès des téléphones mobiles. Celle-ci permet en particulier d'étudier et de concevoir des réseaux autonomes, comme les DTN (dont les connexions se font par proximité et non par un opérateur), en tenant compte des fortes contraintes liées aux ressources énergétiques limitées de ces appareils. Autrement dit, pour plus d'une décennie, la théorie des jeux a été utilisée comme un outil pour étudier les différents aspects des réseaux informatiques et de télécommunications, principalement appliquée à des problèmes dans les réseaux filaires traditionnels. Durant ces dernières années, il y'a eu un regain d'intérêt de la théorie des jeux aux réseau sans fil pour analyser leurs performance.

3.7.1 Avantages de la théorie des jeux dans les réseaux ad hoc

D'autre part, la théorie des jeux offre des avantages pour l'analyse des réseaux ad hoc. Nous mettons en évidence trois d'entre eux :

- Analyse de systèmes distribués : la théorie des jeux permet d'étudier l'existence, l'unicité et la convergence vers un point de fonctionnement en régime permanent lorsque les noeuds du réseau effectuent des adaptations indépendantes. Par conséquent, il sert comme un outil puissant pour une analyse rigoureuse des protocoles distribués.
- Souvent dans les jeux des réseaux ad hoc, les décisions des noeuds à une couche particulière sont faites avec l'objectif d'optimiser la performance des autres couches. Avec une formulation appropriée de l'espace des actions, l'analyse par la théorie des jeux peut donner un aperçu des approches pour une optimisation optimale.
- Conception des systèmes d'incitation à la coopération entre les noeuds.

3.7.2 Challenges de l'application de la théorie des jeux aux réseaux ad hoc

L'utilisation de la théorie des jeux pour l'analyse des performances des réseaux ad hoc n'est pas sans défis. Nous soulignons trois domaines particulièrement difficiles :

- Hypothèse de la rationalité

La théorie des jeux est fondée sur l'hypothèse que les joueurs agissent de façon rationnelle, dans le sens que, chaque joueur dispose d'une fonction objectif qu'il cherche à optimiser compte tenu des contraintes imposées sur ses choix d'actions par les conditions du jeu. Bien que les noeuds d'un réseau ad hoc puissent être programmés pour agir d'une manière rationnelle, l'état stationnaire résultant d'un

comportement rationnel n'a pas besoin d'être socialement souhaitable. En effet, une contribution majeure de la théorie des jeux, c'est qu'elle montre formellement que la rationalité individuelle ne conduit pas nécessairement à des états optimaux.

- La complexité des modèles

La nature dynamique des réseaux ad hoc conduit à des imperfections (bruit) dans les actions d'un noeud. Ces imperfections doivent être modélisées avec des jeux assez complexes à information imparfaite. En outre, la modélisation des modèles de canaux sans fil et les interactions entre les protocoles au niveau des différentes couches implique une analyse mathématique complexe et, parfois, non linéaire.

- Choix des fonctions d'utilité

Il est difficile de modéliser comment un noeud évalue les différents niveaux de performance et quels sont les compromis qu'il est prêt à faire. Le problème est exacerbé par un manque de modèles analytiques qui mappent les actions disponibles de chaque noeud à la métrique des couches supérieures telle que le débit.

3.8 Modélisation des réseaux ad hoc comme jeux :

Les réseaux ad hoc, comme tout autre type de réseaux, peuvent être des cibles de maintes attaques qui peuvent causer des dommages et ainsi dégrader leurs performances. Pour contrer ces attaques, tous les nœuds composant ce réseau devront être équipés d'un IDS. Ainsi, une situation d'interaction se crée entre l'IDS, dont le but est de protéger le réseau, et l'attaquant qui cherche à compromettre la sécurité de ce réseau et la théorie des jeux fournit des outils pour étudier l'interaction entre des joueurs dans une société. Pour cela, elle a été suggérée pour modéliser l'interaction entre un attaquant et un IDS dans différents types de réseau.
Cette similitude entre les composants de la théorie des jeux et les éléments d'un réseau ad hoc est illustrée dans les trois points suivant :

- Joueurs : nœuds dans le réseau,

- Stratégies : action liée à la fonctionnalité à étudier (la puissance de transmission, sélection de la forme d'onde, l'accès au medium, expédition des paquets,...),

- Fonction d'utilité : les performances du réseau (le débit, la durée de vie,...).

D'une manière générale, nous pouvons modéliser un réseau ad hoc par le jeu sous forme normale suivant : :

$$G =< \mathbb{N}, \{S_i\}_{i\in\mathbb{N}}, \{U_i\}_{i\in\mathbb{N}} > .$$

tel que :

- $\mathbb{N} = \{1, ..., N\}$: est l'ensemble des nœuds.
- $S_i \in \{S_1, ..., S_n\}$: est l'ensemble de stratège de $i^{ème}$ nœud.
- U_i : est la fonction d'utilité du $i^{ème}$ nœud.

3.9 Conclusion

Dans ce chapitre, nous avons présenté les réseaux informatiques, essentiellement les réseaux mobile ad hoc. La sécurité et les différents types de menaces ont fait l'objet de nombreuses études. Nous avons cité plusieurs mécanismes de sécurité d'un système informatique et particulièrement l'utilisation de la théorie des jeux pour modéliser les réseaux ad hoc et différents avantages d'application de cette théorie dans ce domaine.

CHAPITRE 4

JEUX BAYÉSIENS POUR LA DÉTECTION D'INTRUSION DANS LES RÉSEAUX AD HOC

4.1 Introduction

Le problème de sécurité dans les réseaux ad hoc a longtemps été l'un des soucis majeurs lors de la conception d'un réseau. Plusieurs approches ont été mises en avant dans le but de empêcher les menaces qui pèsent sur ce type de réseaux. Dans le chapitre précédent, nous avons présenté l'une de ces approches qui est la théorie des jeux et qui a pris place dans différents travaux de sécurité avec laquelle une modélisation complète est effectuée.

L'objectif de ce chapitre est de présenter notre modèle de sécurité pour les réseaux ad hoc, en exposant les différentes étapes qui le constituent.

4.2 Travaux connexes

Un cadre théorique de jeu est adapté à la modélisation de problèmes de sécurité tels que la prévention d'intrusion et la détection d'intrusion. Un exemple de modèle de jeu de prévention d'intrusion est présenté par Liu et Zang [16], où les auteurs proposent une approche de la théorie de jeux pour déduire l'intention, les objectifs et les stratégies de l'attaquant. Dans le contexte de la détection d'intrusion, plusieurs approches se basant sur la théorie des jeux ont été proposées pour les réseaux , les réseaux WLAN (Wireless Local Area Network), les réseaux de capteurs et les réseaux ad hoc. Kodialam et Lakshman [15] ont utilisé la théorie de jeux pour modéliser le problème de détection d'intrusion. Pour cela ils ont proposé un jeu à somme nulle entre deux acteurs : le fournisseur de services et l'intrus. Une intrusion réussie survient lorsqu'un paquet malveillant atteint la cible souhaitée. Dans le jeu, l'objectif de l'intrus est de choisir un chemin particulier entre le nœud source et le nœud cible, et l'objectif du fournisseur de services est de déterminer un ensemble de liens sur lesquels un échantillonnage doit être effectué afin de détecter l'intrusion. Essentiellement, le jeu est formulé comme un jeu à somme nulle à deux joueurs, dans lequel le fournisseur de services essaie de maximiser son gain, qui est défini par la probabilité de détection, et d'autre part, l'intrus tente de minimiser la probabilité de être détecté. La solution optimale pour les deux joueurs est de jouer à la stratégie du jeu minmax. La limitation de ce jeu réside dans l'hypothèse d'une connaissance parfaite, ce qui implique que l'intrus dispose de nombreuses informations sur le réseau et est en mesure

de choisir le chemin optimal pour jouer à la stratégie minmax. En général, l'utilisation d'un jeu à somme nulle pour modéliser le problème de la détection d'intrusion présente une limite, c'est-à-dire que le coût de l'intrusion et le coût de la détection sont supposés être des produits strictement concurrentiels. Ce n'est évidemment pas vrai dans la plupart des cas. Par exemple, dans [15], le coût d'échantillonnage sur plusieurs liaisons est beaucoup plus élevé que le coût d'envoi d'un paquet malveillant sur un chemin particulier.

Alpcan et Basar [8] ont présenté un jeu de détection d'intrusion dans les réseaux de capteurs virtuels distribués, où chaque agent du réseau dispose de capacités de détection imparfaites. Ils modélisent l'interaction entre le ou les attaquants et l'IDS sous la forme d'un jeu à somme non nul et non coopératif avec deux versions : la version finie et la version à noyau continu. Dans leur modèle, à côté du ou des attaquants et de l'IDS, un troisième joueur «fictif» est ajouté au jeu pour représenter la sortie du réseau de capteurs lors d'une attaque spécifique, qui est une distribution de probabilité fixe définie comme le rapport de la probabilité de détection (c-à-d. déclencher une alerte) au niveau du capteur cible sur la somme des probabilités de détection de tous les capteurs du réseau. Les auteurs suggèrent ensuite une fonction de coût au jeu de sécurité du noyau continu, qui est paramétré par cette distribution de probabilité. Néanmoins, l'attaquant et l'IDS essayant tous deux de minimiser leurs coûts en fonction de la fonction de coût, cela implique que les deux joueurs ont connaissance de la probabilité de détection de chaque capteur (par rapport à l'attaque spécifique) dans l'ensemble du réseau pendant le parcours du jeu.

Un jeu à deux joueurs, non coopératif et à somme non nulle, a également été étudié par Agah et al. [26] et Alpcan et Basar [3] pour résoudre les problèmes de défense et d'attaque dans les réseaux de capteurs. Comme dans notre jeu de défense et d'attaque à une étape décrit à la Section 4.3, la stratégie optimale de chaque joueur dépend uniquement de la fonction de gain de l'adversaire, et le jeu est supposé avoir des informations complètes. Cependant, comme nous l'avons souligné précédemment, cette hypothèse a des limites dans un réseau réel.

La plupart des solutions théoriques des jeux proposées précédemment pour les réseaux ad hoc se concentrent sur la modélisation de la coopération et de l'égoïsme du réseau (par exemple [31], [5], [23], [29]). Dans ces jeux, chaque nœud choisit de transférer ou non un paquet en fonction de son coût (consommation d'énergie), de ses avantages (débit du réseau) et de la collaboration offerte au réseau par les voisins. Chacune de ces œuvres essaie de montrer qu'en appliquant des mécanismes de coopération, un nœud égoïste qui ne respecte pas les règles aura un faible débit en retour du réseau.

Bouhaddi [4] a traité le problème de sécurité dans un réseau MANET, en considérant des objectifs contradictoires entre un nœud potentiellement malveillant et un IDS basé sur une coalition de défense. Elle a repris le modèle de détection d'intrusion basé sur les jeu Bayésiens statiques en donnant la possibilité aux nœuds du réseau de mettre à jour leur croyance de manière continuelle en considérant le jeu Bayésien répété infiniment. L'objectif de cette contribution est de trouver l'utilisation optimale de deux modes de détection d'intrusion, à savoir un mode collaboratif et un mode non-collaboratif, qui minimise la consommation des ressources du MANET tout en préservant sa sécurité. Elle a modélisé son mécanisme d'activation de l'IDS à travers un jeu Bayésien répété entre un nœud émetteur potentiellement malveillant et une coalition de défense. Chaque entité vise à maximiser son gain : l'attaquant tente de violer les propriétés de sécurité du réseau sans être détecté, tandis que la coalition de défense tente de maximiser ses capacités de défense avec une contrainte sur la dépense des ressources en utilisant l'IDS. En effet, la coalition de défense a le choix entre deux modes d'activation de l'IDS. Un

mode d'activation collaboratif avec un taux de détection élevé et une dépense de ressources significative et un mode d'activation non-collaboratif avec un taux de détection et une dépense de ressources plus faible. Elle a ensuite construit le système de croyance et élaboré les règles de décision optimales pour les deux joueurs correspondant à l'équilibre Bayésien parfait après avoir démontré son existence.

Dans ce travail, nous utilisons un jeu Bayésien dynamique pour modéliser les interactions entre l'attaquant et le défenseur dans des réseaux ad hoc. Cela permet aux deux joueurs de choisir leurs stratégies optimales en fonction du profil de l'histoire d'actions et de leurs croyances quant aux types des adversaires, et ainsi de surmonter les limites du jeu statique à une étape.

4.3 Modèle du jeu Bayésien statique de détection d'intrusion

Considérons un réseau ad hoc plat avec un nombre fixe de N nœuds dans le réseau. On suppose qu'un nœud en défense est équipé d'un IDS. En fonction de la capacité de l'IDS, le nœud en défense peut détecter un nœud attaquant dans le voisinage ou n'importe quel nœud du réseau. Les auteurs dans [28] ont modélisé l'interaction entre l'IDS et l'attaquant par un jeu Bayésien à deux joueurs, dont les composants sont :

- **Joueurs :** Le jeu se déroule entre deux joueurs : Un joueur est un nœud potentiellement *attaquant*, désigné par i. L'autre joueur est un nœud en défense $défenseur$, noté j.
- **Les types :** Le joueur i possède deux types :
  - Type *malveillant* noté par $\theta_i = 0$;
  - Type *régulier* noté par $\theta_i = 1$,

  Ces types représentent l'information privée de l'attaquant que l'IDS ignore. Le joueur j possède un seul type qui est *régulier*, $\theta_j = 0$, et il est connu par les deux joueurs i et j .
- **Stratégies :** Le joueur i dispose des informations personnelles sur son type, qui sont soit malveillantes, désignées par $\theta_i = 0$, soit régulières désignées par $\theta_i = 1$. En d'autres termes, le caractère *malveillant* du joueur i est inconnu du $défenseur\ j$. Le joueur i possède des stratégies pour chacun de ces types.
  - *malveillant* **:** dans ce cas, l'ensemble de stratégies du joueur i est composé de deux stratégies :
    $$A_i = \{Attaquer, Ne\ pas\ attaquer\},$$
    est l'ensembles des stratégies du joueur i
  - *régulier* **:** ici le joueur i possède une seul stratégie (c'est à dire adopter un comportement normal) :
    $$A_i = \{Ne\ pas\ attaquer\}.$$
    Ces deux stratégies sont choisies avec des probabilités μ et $(1-\mu)$, respectivement.
  - Joueur j ($défenseur\ j$) à deux stratégies pures :
    $$A_j = \{Surveiller,\ Ne\ pas\ surveiller\},\ .$$
    Le $défenseur\ j$ est de type *régulier* noté $\theta_j = 0$. Le type de $défenseur\ j$ est bien connu des deux joueurs.

Les deux joueurs choisissent leurs stratégies simultanément au début du jeu, en supposant une connaissance commune du jeu (coûts et croyances).

Où : Pour avoir les profits des deux joueurs, i et j, pour chaque stratégie possible, on a besoin de définir les gains et les pertes qui leur sont associés :

- α : représente le taux de détection (c'est-à-dire le taux réel positif) de l'IDS avec $\alpha \in [0, 1]$.
- β : représente le taux de fausse alarme (c'est-à-dire le taux de faux positif) de l'IDS avec $\beta \in [0, 1]$.
- w : est la valeur de sécurité du défenseur j.
- c_a : représente le coût d'une attaque du joueur i durant toute la période avec $c_a > 0$.
- c_m : représente le coût de surveillance pour le joueur j durant toute la période et $c_m > 0$.

Il est raisonnable de supposer que $w > c_a, c_m$, sinon l'attaquant n'a aucune raison d'attaquer et le défenseur n'a aucune incitation à surveiller.

Remarque 7. *Dans un réseau aux ressources limitées, le coût de la surveillance c_m peut être défini en fonction de la consommation d'énergie associée aux activités de surveillance ; le coût d'attaque c_a peut être défini en fonction de la consommation d'énergie par rapport aux activités d'attaque.*

- **Gains :** Les gains des deux joueurs sont :
  - Type *malveillant* $\theta_i = 0$:
    - Pour la combinaison de stratégies (*Attaquer*, *Surveiller*), le gain du $défenseur\ j$ est le gain attendu de la détection de l'attaque moins le coût de surveillance en c_m.
    - Pour la combinaison de stratégies (*Attaquer*, *Ne pas surveiller*), le gain du $défenseur\ j$ est $-w$ et celui du joueur i de type *malveillant* i est son gain de succès moins le coût d'attaque,
    - Le gain attendu de la détection de l'attaque dépend de la valeur de α, qui est $\alpha w - (1 - \alpha)w = (2\alpha - 1)w$. Notez que $1 - \alpha$ est le taux de faux négatif. En revanche, le gain du joueur i de type *malveillant* est la perte du $défenseur\ j$, qui est $(1 - 2\alpha)w$. Ainsi, le gain du joueur i est son gain moins le coût d'attaque.
    - Pour les deux autres combinaisons de stratégie, lorsque le joueur i joue la stratégies *Ne pas attaquer*, son gain est toujours égal à 0. Dans les deux cas, le gain du $défenseur\ j$ est égal à 0 s'il décide de *Ne pas surveiller*, et il a un coût de contrôle c_m et une perte attendue $-\beta w$ due aux fausses alarmes s'il surveille.

    Donc le jeu Bayésien statique de ce modèle est défini comme suit :

Définition 4.3.1. *(Jeu d'attaquant/défenseur)*

$$G = (\mathbb{N}; \{\Theta_k\}_{k\in\mathbb{N}}; p; \{A_k\}_{k\in\mathbb{N}}; \{S_k\}_{k\in\mathbb{N}}; \{U_k\}_{k\in\mathbb{N}});$$

où :

- $\mathbb{N} = \{i, j\}$ *est l'ensemble des joueurs, où* i *représente un joueur attaquant(nœud potentiellement attaquant) et* j *représente le défenseur (un nœud en défense),*
- $\Theta_i = \{0, 1\}$ *est l'ensemble des types du joueur* i *et* $\Theta_j = \{0\}$ *est l'ensemble singleton représente le type du joueur* j *et* $\Theta = \Theta_i \times \Theta_j$ *est l'ensemble des profils de types avec la valeur 0 représente le type malveillant et 1 représente le type régulier .*
- p *est une distribution de probabilités à priori sur le profil de types. Nous posons* μ_0 *comme la probabilité à priori pour que le joueur* i *soit de type malveillant* $(\theta_i = 0)$*.*
- A_i *: l'ensemble de stratégies du joueur* i *est composé de deux stratégies :*

  $$A_i^1 = \{Attaquer, Ne\ pas\ attaquer\},$$

  et

  $$A_i^2 = \{Ne\ pas\ attaquer\}.$$

  et

  $$A_j = \{Surveiller, Ne\ pas\ surveiller\},$$

  A_j*est l'ensemble de stratégies du joueur* j*, et* $A = A_i \times A_j$ *est l'ensemble des profils d'actions.*
- S_i *(respectivement* S_j*) est l'ensemble des stratégies pures possibles pour le joueur* i*,(respectivement le joueur* j *). Une stratégie pure d'un joueur* i *est obtenue par l'application* $s_i : \Theta_i \to A_i$ *associant pour chaque type* $\theta_i \in \Theta_i$*, une action* $a_i \in A_i$ *qu'elle soit choisie par le joueur* i *lorsque son type est* θ_i*. Soient* $S = S_i \times S_j$ *l'ensemble des profiles de stratégies. Nous définissons un profile de stratégies comme la fonction* $s : \Theta \to A$*. Par conséquent, l'ensemble des stratégies pures des deux joueurs sont :*
  Pour le type Malveillant du joueur i *:*

  - s_i^1 *: Attaquer ;*
  - s_i^2 *: Ne pas attaquer ;*
  - s_j^1 *: Surveiller ;*
  - s_j^2 *: Ne pas surveiller ;*

  Pour le type régulier du joueur i *:*

  - s_i^2 *: Ne pas attaquer ;*
  - s_j^1 *: Surveiller ;*
  - s_j^2 *: Ne pas surveiller ;*

- *$\tilde{U}_i$ (respectivement $\tilde{U}_j$) :$S \times \Theta \to \mathbb{R}$ est la fonction d'utilité du joueur i (respectivement j),du joueur attaquant (respectivement la fonction d'utilité du joueur défenseur). Les gains des deux joueurs sont définis dans les Tableaux 4.1 et 4.2*

Les profits des deux joueurs i et j, l'attaquant et l'IDS, pour le type Malveillant du joueur i, $\theta_i = 0$, sont résumés dans le tableau suivant :

$Type\ 1 : \theta_i = Malveillant$

	s_j^1	s_j^2
s_i^1	$(1-2\alpha)w - c_a, (2\alpha - 1)w - c_m)$	$(w - c_a, -w)$
s_i^2	$(0, -\beta w - cm)$	$(0, 0)$

TABLE 4.1 – Les gains des deux joueurs si le types d'attaquant est Malveillant.

- Type régulier $\theta_i = 1$:
  Le défenseur j reçoit 0 s'il décide de ne pas surveiller, et a un coût de surveillance c_m et une perte attendue à cause de la fausse alarme, $-\beta w$, s'il surveille.
  Donc les profits des deux joueurs i et j, l'attaquant et l'IDS, pour le type régulier du joueur i, $\theta_i = 1$, sont résumés dans le tableau suivant :

$Type\ 2 : \theta_i = Régulier$

	s_j^1	s_j^2
s_i^2	$(0, -\beta w - c_m)$	$(0, 0)$

TABLE 4.2 – Les gains des deux joueurs si le types d'attaquant est Régulier.

4.3.1 Analyse de l'équilibre de Nash Bayésien

L'objectif des deux joueurs est de maximiser les gains attendus (espéré) selon le principe de la rationalité individuel.

Supposons que le défenseur j attribue une probabilité à priori $\mu_0 \in [0, 1]$ au joueur i étant malveillant. La figure 4.1 illustre la forme extensive du jeu Bayésien statique. Dans cette figure, le nœud N représente un nœud «Nature», qui détermine le type du joueur i.

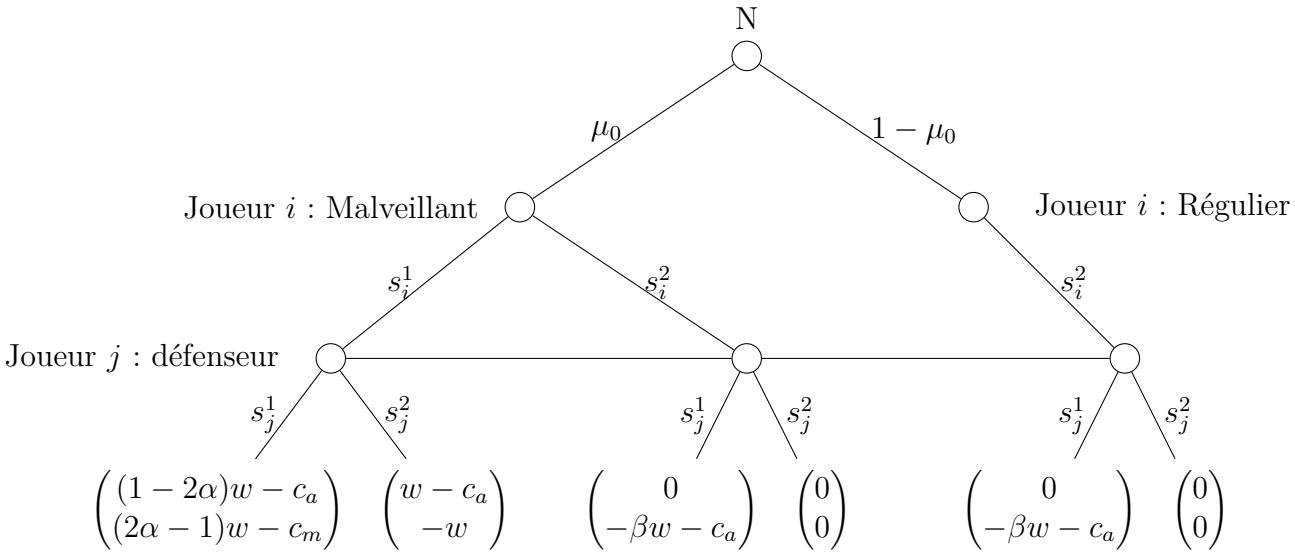

FIGURE 4.1 – La forme extensive du jeu Bayésien statique.

Dans ce qui suit, nous analysons l'équilibre de Nash Bayésien en partant du principe que μ_0 est une connaissance commune, c'est-à-dire que le joueur i connaît la croyance du défenseur j de μ_0.

- Si le joueur i joue sa paire de stratégie pure (*Attaquer* si *malveillante*,*Ne pas attaquer* si *régulier*), le gain attendu du défenseur j jouant sa stratégie pure $Surveiller$ est :

$$U_j(Surveiller) = \mu_0((2\alpha-1)w - c_m) - (1-\mu_0)(\beta w + c_m),$$

et son gain attendu de jouer sa stratégie pure $Ne\ pas\ surveiller$ est :

$$U_j(Ne\ pas\ surveiller) = -\mu_0 w.$$

Donc, si $U_j(Surveiller) > U_j(Ne\ pas\ surveiller)$, ou si $\mu_0 > \frac{(1+\beta)w+c_m}{(2\alpha+\beta-1)w}$, la meilleure réponse du joueur j est de jouer son action $Surveiller$. Cependant, si le défenseur j joue $Surveiller$, *Attaquer* ne constituera pas la meilleure réponse pour le type malveillant du joueur i, et il jouera par contre $Ne\ pas\ attaquer$ à la place. Par conséquent, ((*Attaquer* si malveillant, $Ne\ pas\ attaquer$ si régulier), $Surveiller$, μ_0) n'est pas un équilibre de Nash Bayésien (ENB). Toutefois, si $\mu_0 < \frac{(1+\beta)w+c_m}{(2\alpha+\beta-1)w}$, la meilleure réponse pour le défenseur j est $Ne\ pas\ surveiller$ et donc ((*Attaquer* si malveillante, $Ne\ pas\ attaquer$ si régulière), $Ne\ pas\ surveiller$, μ_0) est un ENB en stratégies pures pour le jeu G.

- Si le type du joueur est malveillant joue sa stratégie pure $Ne\ pas\ attaquer$, la stratégie dominante du défenseur j consiste à jouer $Ne\ pas\ surveiller$, quel que soit μ_0. Cependant, si le défenseur j joue $Ne\ pas\ surveiller$, la meilleure réponse pour le type du joueur malveillant i est de jouer *Attaquer*, ce qui se réduit au cas précédent. Donc la stratégie ((*Ne pas attaquer* si malveillant, $Ne\ pas\ attaquer$ si régulièr), $Ne\ pas\ surveiller$) n'est pas un ENB.
- Nous avions précédemment montré qu'il n'existait pas ENB en stratégies pures pour le jeu lorsque $\mu_0 > \frac{(1+\beta)w+c_m}{(2\alpha+\beta-1)w}$. Un équilibre de Nash Bayésien en stratégies mixtes est dérivé comme suit. Soit p la probabilité avec laquelle le joueur i joue son action

Attaquer et q la probabilité avec laquelle le défenseur j joue *Surveiller*. Le gain attendu du défenseur j en jouant l'action *Surveiller* est

$$U_j(Surveiller) = p\mu_0((2\alpha - 1)w - c_m) - (1-p)\mu_0(\beta w + c_m) - (1-\mu_0)(\beta w + c_m).$$

Et le gain attendu du défenseur j jouant *Ne pas surveiller* est

$$U_j(Ne\ pas\ surveiller) = -p\mu_0 w.$$

En imposant $U_j(Surveiller) = U_j(Ne\ pas\ surveiller)$, nous obtenons que le joueur du type malveillant dont la stratégie d'équilibre est de jouer à *Attaquer* avec une probabilité $p^* = \frac{\beta w + c_m}{(2\alpha+\beta)w\mu_0}$ et de la même manière, en imposant $U_i(Attaquer) = U_i(Ne\ pas\ attaquer)$, nous obtenons que la stratégie d'équilibre du défenseur j consiste à jouer à *Surveiller* avec une probabilité $q^* = \frac{w - c_a}{2\alpha w}$. Ainsi, la paire stratégie ((p^* si malveillant, *Ne pas attaquer* si régulière), q^*, μ_0) est un ENB en stratégie mixte.

En résumé, le jeu Bayésien statique n'a pas de ENB en stratégies pures si $\mu_0 > \frac{(1+\beta)w + c_m}{(2\alpha+\beta-1)w}$, mais il admet un ENB en stratégies mixtes ((p^* si malveillant, *Ne pas attaquer* si régulière), q^*, μ_0). C'est-à-dire que si le défenseur j croit suffisamment en la méchanceté du joueur i, $\mu_0 > \frac{(1+\beta)w + c_m}{(2\alpha+\beta-1)w}$, il existe un ENB en stratégies mixtes pour lequel le défenseur j joue *Surveiller* avec la probabilité q^*, et le joueur i joue son action *Attaquer* avec la probabilité p^* s'il est malveillant et joue *Ne pas attaquer* s'il est régulièr. Nous voyons également que si le défenseur j croit très mal que le joueur i est malveillant $\mu_0 < \frac{(1+\beta)w + c_m}{(2\alpha+\beta-1)w}$, un ENB en stratégies pures ((*Attaquer* si malveillant, *Ne pas attaquer* si régulièr), *Ne pas surveiller*, μ_0) existe. C'est-à-dire qu'il existe un ENB en stratégies pures pour lequel le défenseur j joue sa stratégie pure *Ne pas surveiller*, et le joueur i joue sa stratégie pure *Attaquer* si malveillant et *Ne pas attaquer* si régulièr.

Remarque 8. *Le modèle présenté dans cette section modélise le cas où il n'existe qu'une seule attaque et donc l'IDS réagit qu'une seule fois, nous pourrions considérer le cas où les attaques se répètent ce qui amène l'IDS à réagir à chacune d'elles, dans ce cas l'application d'un jeu Bayésien dynamique (répété) serait adéquate.*

4.4 Modèle du jeu Bayésien dynamique de détection d'intrusion

Le modèle présenté précédemment se base sur un jeu Bayésien statique qui se déroule en une seule étape pour lequel le défenseur maximise ses gains en se basant sur une croyance antérieure bien arrêtée concernant la malveillance de son adversaire. En raison de la difficulté d'attribuer des probabilités à priori précises aux types du joueur i, nous étendons le jeu Bayésien statique à un jeu Bayésien dynamique, dans lequel le défenseur met à joue ses croyances en fonction de l'évolution du jeu.

Nous supposons que le jeu Bayésien statique est joué à plusieurs reprises dans chaque période t_k, où $k = 0, 1, ...$ Un intervalle de T secondes peut être sélectionné pour chaque étapes du jeu. Nous considérons que le jeu a un horizon infini car en général tout nœud n'aura pas l'information sur le moment où son nœud voisin quittera le réseau. Les gains

des joueurs dans chaque étape du jeu sont les mêmes que dans le jeu statique précédent, et nous supposons qu'il n'y a pas de facteur de réduction en ce qui concerne les gains des joueurs. C'est-à-dire que les gains restent les mêmes dans toutes les étapes du jeu. De plus, nous supposons que l'identité des joueurs reste la même tout au long du jeu.

Adaptons les mêmes notations présentées dans le jeu Bayésien statique étudié précédemment. Le type d'un joueur représente son information privée. Le type de défenseur j est *régulier* ($\theta_j = 0$) qui est une connaissance commune. Les joueurs choisissent des actions simultanément au début de chaque étape. La forme détaillée de chaque étape du jeu peut être représentée de la même manière que pour le jeu Bayésien statique.

Supposons qu'au début de chaque étape t_k, le joueur i de type *malveillant* choisit une action $a_i(t_k)$ dans $A_i = \{Attaquer, Ne\ pas\ attaquer\}$, ou le joueur i de type *régulier* choisit sa seul action $Ne\ pas\ attaquer$; le défenseur j choisit une action $a_i(t_k)$ dans son ensemble d'actions $A_j = \{Surveiller, Ne\ pas\ Surveiller\}$. Comme dans les jeux statiques, on peut définir des stratégies mixtes des jeux dynamiques , ces stratégies mixtes dépendent de l'historique du jeu et elles sont nommées stratégies de comportement. Une stratégie de comportement spécifie une distribution de probabilité sur les actions de chaque ensemble d'informations . Nous définissons le profil d'historique des actions réalisées durant les périodes qui précède l'instant t_k, par $h_i^j(t_k)$,

$$h_i^j(t_k) = (a_i^j(t_0), ..., a_i^j(t_{k-1})). \tag{4.1}$$

où $a_i^j(t_k)$ indique l'action du joueur i par rapport au défenseur j à l'étape t_k. Dans ce qui suit, pour simplifier l'exposition, on utilisera un abus de notation et on notera

$$P(\sigma_i(a_i(t_k))) = (Attaquer/\theta_i, h_i^j(t_k)) = p$$

$$P(\sigma_i(a_i(t_k))) = (Ne\ pas\ attaquer/\theta_i, h_i^j(t_k)) = 1 - p$$

$$P(\sigma_j(a_j(t_k))) = (Surveiller/\theta_j, h_j^i(t_k)) = q$$

$$P(\sigma_j(a_j(t_k))) = (Ne\ pas\ Surveiller/\theta_j, h_j^i(t_k)) = 1 - q$$

étant entendu que les stratégies mixtes p et q pour un jeu dynamique dépendront de l'ensemble d'informations actuelles du jeu (l'historique du jeu). Dans l'étapes t_k de jeu , la stratégie de comportement optimal du défenseur j dépend de ses croyances sur les types du joueur i au début de t_k. Dans la première étape de jeu t_0, la croyance du défenseur j selon laquelle le joueur i est malveillant est caractérisée par une probabilité a priori μ_0. Dans les étapes suivantes du jeu dynamique, le défenseur j peut mettre à jour ses croyances à la fin de chaque jeu en fonction de son action observée du joueur i et du profil d'historique des actions du jeu.

Donc le jeu Bayésien dynamique de ce modèle est défini comme suit :

Définition 4.4.1. *(Jeu d'attaquant/défenseur (dynamique))*

$$\mathcal{G}_{\mathcal{R}} = (\mathbb{N}; \{\Theta_k\}_{k\in\mathbb{N}}; p; \{A_k\}_{k\in\mathbb{N}}; \{\Sigma_k\}_{k\in\mathbb{N}}; \{\mu_k\}_{k\in\mathbb{N}}; \{U_k^R\}_{k\in\mathbb{N}});$$

où :

- $\mathbb{N}$, A_k, p , $U_k^R((\sigma_k, \sigma_{-k})|h(t_q), \theta_k)$,$\{\mu_k\}_{k\in\mathbb{N}}$ *:sont définis de la même manière que dans le jeu précédent ;*
- Σ_i *et* Σ_j *sont respectivement les ensembles des stratégies de comportement des joueurs* i *et* j*. Soit* $\Sigma = \Sigma_i \times \Sigma_j$ *l'ensemble des profils de stratégies de comportement, une stratégie de comportement pour le joueur* i*, notée* σ_i *est définie par* $\sigma_i(a_i(t_k)/\theta_i, h_i^j(t_k))$*, où* $h_i^j(t_k)$ *représente le profil d'historique des actions du joueur* i *par rapport à son adversaire* j *au début du l'étape* t_k*. Nous définissons une stratégie de comportement pour le défenseur* j *comme suit :* $\sigma_j(a_j(t_k)/\theta_j, h_j^i(t_k))$*, où* $h_j^i(t_k)$ *représente le profil d'historique d'actions du défenseur* j *par rapport à son adversaire* i *au début du l'étape* t_k*.*

4.4.1 Règle de mise à jour Bayésienne pour les croyances

Nous construisons un système de mise à jour des croyances pour le défenseur j, afin que les croyances du défenseur j puissent être mises à jour de étape t_k à l'étape t_{k+1} du jeu selon la règle de Bayes. Plus précisément, le défenseur j met à jour ses croyances sur les types de son adversaire i à la fin de chaque étape en calculant ses croyances postérieures, définies par $\mu_j(\theta_i/a_i(t_k), h_i^j(t_k))$, où $a_i(t_k)$ représente l'action du joueur i a l'étape t_k, et $h_i^j(t_k)$ représente le profil d'historique des actions du joueur i par rapport au défenseur j. Selon la règle de Bayes, les croyances postérieures du joueur j peuvent être calculées comme suit :

$$\mu_j(\theta_i/a_i(t_k), h_i^j(t_k)) = \frac{\mu_j(\theta_i/h_i^j(t_k))P(a_i(t_k)/\theta_i, h_i^j(t_k))}{\sum_{\tilde{\theta}} \mu_j(\tilde{\theta}_i/h_i^j(t_k))P(a_i(t_k)/\tilde{\theta}_i, h_i^j(t_k))}. \tag{4.2}$$

où $\mu_j(\tilde{\theta}_i/h_i^j(t_k)) > 0$, $h_i^j(t_k) > 0$ et $p(a_i(t_k))/\theta_i, h_i^j(t_k)$ est la probabilité qu'une action soit observée à ce stade du jeu, en fonction du type d'adversaire et de l'historique du jeu.

À partir de l'équation (4.2) , nous voyons que, pour mettre à jour la croyance, lors de la période t_k du jeu, le défenseur j doit d'abord «observer» l'action $a_i(t_k)$.

Du point de vue du défenseur j, l'action (*Attaquer* ou *Ne pas attaquer*) du joueur i à chaque période peut être observée (détectée) par un système de surveillance toujours actif. Comme décrit dans le modèle de jeu statique précédent, la surveillance permanente n'est pas une stratégie qui économise l'énergie. Le défenseur peut utiliser le modèle de jeu statique pour obtenir une meilleure solution. Cependant, bien que chaque étape du jeu soit considéré comme un jeu Bayésien statique, cette solution ne convient pas aux étapes du modèle du jeu Bayésien dynamique, car la mise à jour des croyances oblige le défenseur à observer en permanence les actions de son adversaire à chaque étape du jeu.

4.4.2 Analyse de l'équilibre Bayésien parfait (EBP)

Un jeu Bayésien dynamique est un jeu qui se déroule en plusieurs étapes avec des actions observées et des informations incomplètes.En général, dans un jeu séquentiel, les meilleures réponses des joueurs sont souvent guidées par les menaces suscitées par certaines réactions d'autres joueurs. Pour un jeu Bayésien dynamique , ces menaces dépendent des croyances actuelles, qui peuvent changer à mesure que le jeu évolue. Le concept d'équilibre Bayésien parfait (EBP) définit l'interaction appropriée entre les croyances des utilisateurs sur les types, en fonction d'une sélection d'actions, et les stratégies réelles. EBP exige que les joueurs forment un système complet de croyances sur les types d'opposants à chaque nœud décisionnel atteignable, les mettent à jour conformément à la règle de Bayes et prennent les stratégies de meilleures réponses en utilisant l'équilibre Bayésien normal. EBP demande que le jeu suivant soit optimal pour chaque étape du jeu, c'est-à-dire qu'il soit lié au concept de perfection des sous-jeux.

Dans ce qui suit, nous montrons que le jeu Bayésien dynamique $\mathcal{G}_{\mathcal{R}}$ admet un EBP. Montrons d'abord que les conditions Bayésiennes $B(i) - B(iv)$ et la condition d'équilibre sont satisfaites pour le jeu $\mathcal{G}_{\mathcal{R}}$. Les conditions ci-dessus garantissent le jeu Bayésien $\mathcal{G}_{\mathcal{R}}$ admet un EBP.

Lemme 1. *[17]*
Le jeu $\mathcal{G}_{\mathcal{R}}$ répond aux quatre conditions Bayésiennes $B(i) - B(iv)$:

- $B(i)$ *Les croyances postérieures sont indépendantes et tout les types de joueurs j partagent les mêmes croyance. Même des événements inattendus ne modifieront pas l'hypothèse d'indépendance du type de l'adversaire.*
- $B(ii)$ *La règle de Bayes est utilisée pour mettre à jour les croyances de $\mu_j(\theta_i/h_i^j(t_k))$ à $\mu_j(\theta_i/h_i^j(t_{k+1}))$ chaque fois que possible.*
- $B(iii)$ *Les joueurs ne signalent pas ce qu'ils ne savent pas.*
- $B(iv)$ *Tous les joueurs doivent avoir la même croyance à propos de type d'un autre joueur.*

La preuve du Lemme 1 est plutôt triviale car il s'agit d'un jeu à deux joueurs. En effet,

- $B(i)$ est trivialement satisfait parce que le défenseur j n'a que un seul type.
- À partir du système de mise à jour des croyances proposé, nous voyons que le jeu $\mathcal{G}_{\mathcal{R}}$ satisfait la condition $B(ii)$.
- $B(iii)$ signifie $\mu_j(\theta_i = 1/a_i(t_k), h_i^j(t_k)) = \mu_j(\theta_i = 1/\tilde{a}_i(t_k), h_i^j(t_k))$, si $a_i(t_k) = \tilde{a}_i(t_k)$ (pour le jeu $\mathcal{G}_{\mathcal{R}}$, le signal de l'attaquant fait partie des actions d'attaque, ainsi $B(iii)$ est satisfait).
- Pour la condition $B(iv)$, car dans chaque étape de jeu, seuls deux joueurs sont présents et aucun autre joueur n'influence sur les mises à jour des croyances des deux joueurs.

En substance, le Lemme 1 indique que la mise à jour des croyances de chaque joueur est cohérente dans tous les jeux dynamiques. Partant de l'hypothèse de rationalité des joueurs, la stratégie optimale du défenseur j consiste, à chaque étape, à maximiser ses gains en fonction de ses nouvelles croyances.

Définition 4.4.2. *Dans le jeu $\mathcal{G}_{\mathcal{R}}$, la stratégie de comportement optimal du défenseur j, σ_j^* par rapport à ses croyances $\mu_j(\theta_i/a_i(t_k), h_i^j(t_k))$ du joueur i à la période t_k du jeu satisfait la relation suivante :*

$$U_j((\sigma_i, \sigma_j^*)/\theta_j, h_i^j(t_k), \mu_j(.)) \geq U_j((\sigma_i, \sigma_j')/\theta_j, h_i^j(t_k), \mu_j(.)), \tag{4.3}$$

où σ_j' est une stratégie de comportement alternative du défenseur j, et $h_i^j(t_k)$ est le profil d'historique des actions du joueur i par rapport au défenseur j, $\mu_j(.)$ est l'abréviation de $\mu_j((\sigma_i, \sigma_j^*)/\theta_j, h_i^j(t_k)$ et $U_j(.)$ est le gain attendu du défenseur j sous le profil de stratégies (σ_i, σ_j^*) à la période t_k.

De manière analogue, nous définissons la stratégie optimale de l'attaquant potentiel i comme suit.

Définition 4.4.3. *Dans le jeu $\mathcal{G}_{\mathcal{R}}$ la stratégie de comportement optimal à la période t_k du jeu $\mathcal{G}_{\mathcal{R}}$ de l'attaquant potentiel , i notée par σ_i^*, par rapport à ses croyances $\mu_i(\theta_i/a_j(t_k), h_j^i(t_k))$ vérifie la condition suivante :*

$$U_i((\sigma_i^*, \sigma_j)/\theta_j, h_i^j(t_k), \mu_i(.)) \geq U_i((\sigma_i', \sigma_j)|\theta_j, h_i^j(t_k), \mu_i(.)), \tag{4.4}$$

où σ_i' est une stratégie comportementale alternative du l'attaquant i, et $h_i^j(t_k)$ est le profil historique d'action du défenseur j par rapport à l'attaquant i, $\mu_i(.)$ est l'abréviation de $\mu_i(\theta_i/a_j(t_k), h_j^i(t_k))$, et $U_i(.)$ est le gain attendu du joueur i selon le profil de stratégie (σ_i', σ_j) à la période t_k. Puisque le défenseur j n'a qu'un type, l'équation (4.3) se réduit à

$$U_j((\sigma_i^*, \sigma_j)/\theta_j, h_i^j(t_k)) \geq U_j((\sigma_i', \sigma_j)/\theta_j, h_i^j(t_k)). \tag{4.5}$$

Lemme 2. *[17]*

Le jeu $\mathcal{G}_{\mathcal{R}}$ satisfait à la condition d'équilibre CE pour les jeux Bayésiens dynamiques :

(CE) Pour chaque joueur $l \in \mathbb{N}$, type $\theta_l \in \Theta_l$, la stratégie alternative du joueur l σ_l' et l'historique $h(t_k)$, le gain attendu obtenu en utilisant la stratégie σ_l, noté U_l, satisfait à la condition suivante :

$$U_l(\sigma/h(t_k), \theta_i, \mu(./h(t_k))) \geq U_l((\sigma_l', \sigma_{-l}/h(t_k), \theta_l, \mu(./h(t_k))). \tag{4.6}$$

En substance, la condition CE stipule que la stratégie de comportement de chaque joueur est séquentielle rationnelle dans chaque partie. Par les Définitions 4.4.2 et 4.4.3, étant donné la croyance du défenseur j, μ_j. Le jeu $\mathcal{G}_{\mathcal{R}}$ a une paire de stratégies $\sigma = (\sigma_i^*, \sigma_j^*)$ qui satisfait la formule d'inégalité ci-dessus, la condition CE est donc satisfaite.

Théoreme 3. *[17]*
Le jeu $\mathcal{G}_{\mathcal{R}}$ a un équilibre Bayésien parfait.

Puisque le jeu $\mathcal{G}_{\mathcal{R}}$ satisfait les quatre conditions Bayésiennes $B(i) - B(iv)$ (Lemme 1) et la condition d'équilibre CE (Lemme 2), le jeu a un profil de stratégie (σ, μ), où $\sigma = (\sigma_i^*, \sigma_j^*)$ est un couple de stratégies pour les deux joueurs et $\mu = (\mu_i(\theta_j/h_j^i(t_k)),$ $\mu_j(\theta_i/h_i^j(t_k))$ est le vecteur des croyances pour les deux joueurs. Notez que μ_i n'est pas nécessaire car le type θ_j du défenseur j est toujours *régulier*. Selon la définition de ENB , (σ, μ) est un ENB.

Dans les paragraphes suivants, nous déterminons l'ENB pour chaque étape du jeu dynamique . Nous analysons le jeu dynamique comme un jeu de signalisation Bayésien, dans lequel les actions d'un attaquant potentiel i signalent son type au défenseur j. Etant donné que le défenseur j s'appuie sur un système de surveillance permanent pour déterminer les actions de son adversaire i, qui n'est pas exempt d'erreurs, l'équilibre recherché est toujours un équilibre semi-séparateur. Notez que les deux autres équilibres séparateur et mélangeant, ne s'appliquent pas pour notre jeu. Le cas de l'équilibre séparateur se produit si le type de l'attaquant potentiel i peut être parfaitement déterminé après la signalisation (c.à.d que en observant la stratégie d'équilibre du l'attaquant i, le défenseur j doit pouvoir en déduire son type avec certitude). Et dans le cas de l'équilibre mélangeant, les deux types de défenseur i ne peuvent pas être distingués en fonction de leur comportement, dans le sens que l'observation de la stratégie du l'attaquant i n'apprend rien au défenseur j.

L'équilibre semi-séparateur est donné par les stratégies qui maximisent les gains des deux joueurs, alors qu'aucun des joueurs n'est incité à changer de stratégie. Nous pouvons voir que seul un équilibre en stratégie mixte existe pour chaque jeu dynamique.

Pour déterminer cet équilibre en stratégies mixtes, nous utilisons le principe d'indifférence pour différentes stratégies des joueurs.

A la période t_k, si le défenseur j constate que la stratégie de son adversaire i est *Attaquer*, le gain attendu pour jouer *Surveiller* est

$$U_j(a_j(t_k) = (Surveiller/a_j(t_k)) = Attaquer) = ((2\alpha-1)w-c_m)p+(-\beta w-c_m)(1-p))\mu_j(\theta_i = 1/.)$$

$$+ (-\beta w - c_m)\mu_j(\theta_i = 0/.). \tag{4.7}$$

et son gain attendu pour jouer *Ne pas surveiller* conditionnel à son observation est

$$U_j(a_j(t_k) = (Ne\ pas\ Surveiller/a_j(t_k)) = Attaquer) = -wp\mu_j(\theta_i = 1/.). \tag{4.8}$$

Donc, le joueur i choisit p^* (la probabilité avec laquelle le joueur i joue *Attaquer*) pour garder le défenseur j indifférent entre *Surveiller* et *Ne pas surveiller*. En d'autres termes, p^* est obtenu en définissant les équations (4.7) et (4.8) égales. Par conséquent, nous avons

$$p^* = \frac{\beta w + c_m}{(2\alpha + \beta)w\mu_j(\theta_i = 1/.)}. \tag{4.9}$$

D'autre part, q^* (la probabilité avec laquelle le défenseur j joue *Surveiller*) est sélectionné pour que le joueur i de type malveillant soit indifférent entre ses stratégies *Attaquer* et *Ne pas attaquer*. La condition d'indifférence est donnée comme suit :

$$((1 - 2\alpha)w - c_a)q + (w - c_a)(1 - q)) = 0, \tag{4.10}$$

et la stratégie d'équilibre du défenseur j consiste donc à choisir q^* comme

$$q^* = \frac{w - c_a}{2\alpha w}. \tag{4.11}$$

Le ENB du jeu est donné par $(p^*, q^*, \mu(.))$, avec p^*, q^* et $\mu(.)$ respectivement données par les équations (4.9), (4.11) et (4.2).

Pour voir pourquoi il n'existe pas d'équilibre de stratégie pur pour ce jeu, nous déterminons la meilleure stratégie de réponse (MR) pour les deux joueurs.

$$MR_j = Surveiller \ \ si \ \ p > \frac{\beta w + c_m}{(2\alpha + \beta) w \mu_j(\theta_i = 1/.)}. \tag{4.12}$$

$$MR_i = Attaquer \ \ si \ \ q < \frac{w - c_a}{2\alpha w}. \tag{4.13}$$

Si (4.12) est vérifié $\Rightarrow$ la meilleure reponse de joueur j est $Surveiller$, si $q = 1 \Rightarrow$ (4.13) n'est pas vérifiée $\Rightarrow$ la meilleure réponse de joueur j est $Ne\ pas\ attaquer$, si $p = 0 \Rightarrow$ (4.12) n'est pas vérifiée $\Rightarrow$ donc le joueur j joue son action $Ne\ pas\ surveiller$, $q = 0$. En utilisant l'argument ci-dessus, on voit qu'il n'y a pas d'équilibre en stratégies pures pour le jeu Bayésien dynamique analysée.

4.4.3 Mise à jour des croyances en présence d'erreurs d'observation

Étant donné que le système de surveillance peut inévitablement produire des faux positifs et des faux négatifs, les actions «observées» peuvent ne pas toujours refléter avec exactitude la réalité. Nous intégrons l'effet des erreurs de fausse alarme et de mauvaise détection pour le système IDS en actualisant les croyances en déterminant de manière appropriée les probabilités conditionnelles $P(a_i(t_k)/\theta_i, h_i^j(t_k))$. Plus précisément, en notant avec α_p et β_p le taux de détection et le taux de faux positifs du système de surveillance , respectivement, les probabilités conditionnelles ci-dessus peuvent être mises à jour comme suit :

$$P(a_i(t_k)) = P(Attaquer/\theta_i = 0, h_i^j(t_k)) = (\alpha_p \times p) + \beta_p \times (1 - p). \tag{4.14}$$

$$P(a_i(t_k)) = P(Ne\ pas\ attquer/\theta_i = 0, h_i^j(t_k)) = ((1-\alpha_p) \times p + (1-\beta_p) \times (1-p)). \tag{4.15}$$

$$P(a_i(t_k)) = P(Attaquer/\theta_i = 1, h_i^j(t_k)) = \beta_p. \tag{4.16}$$

$$P(a_i(t_k)) = P(Ne\ pas\ attaquer/\theta_i = 1, h_i^j(t_k)) = (1 - \beta_p). \tag{4.17}$$

Notez que $(1 - \alpha_p)$ représente le faux taux négatif et $(1 - \beta_p)$ représente le vrai taux négatif.

Nous avons utilisé les notations α_p et β_p des équations (4.14) - (4.17) pour différencier le taux de détection α et le taux de faux positifs β définis dans les fonctions de gain du défenseur j.

4.4.4 Exemple d'appliquation

Considérons un jeu d'attaquant/défenseur interagissant sur un nœud n_k. Soit C_{mk} et C_{ak} le coût associé à la surveillance et à l'attaque du nœud n_k. Soit w_k la valeur de l'actif de n_k. Dans les sections précédentes, nous avons donné le ENB du jeu, qui correspond à la combinaison de stratégies $(p^*, q^*, \mu_j(\theta_i))$, où $p^* = \frac{\beta w + c_m}{(2\alpha+\beta) w \mu_0}$ est la probabilité que le

joueur attaquant i joue Attaquer, $q^* = \frac{w-c_a}{2\alpha w}$ est la probabilité que le joueur défenseur j joue Surveiller et $\mu_j(\theta_i)$ est la croyance du joueur j à propos de la malveillance du joueur i donnée par l'équation (4.2) .

Considérons un modèle avec les valeurs suivantes, $\alpha = 0,9178$, $\beta = 0,0025$, $\alpha_p = 0,833$ et $\beta_p = 0,0029$. Soit $w_k = 9,45$ et $C_{ak} = C_{mk} = \frac{w_k}{1000}$. Supposons que la croyance initiale du joueur j sur le fait que le joueur i soit *malveillant* est de 0,5, c'est-à-dire que la valeur initiale de $\mu_0(\theta_i) = 0,5$. Par conséquent, la probabilité que le joueur i joue son stratégie *Attaquer* pour la $1^{ère}$ étape du jeu est $p^* = \frac{0.0019}{\mu_j(\theta_i)} = \frac{0.0019}{0.5} = 0.0038$. De même, la probabilité de *surveillance* $q^* = 0,5442$. Ensuite, nous mettons à jour la croyance malveillante du joueur i dans les conditions suivantes : Si L'action observée du joueur i par le défenseur j est *Attaquer* :

$$\mu_j(\theta_i = 0)(t_1) = \frac{\mu_j(\theta_i = 0)(t_0)P(a_i(t_1) = Attaquer/\theta_i = 0, a_i(t_0))}{\sum_{\tilde{\theta}} \mu_j(\tilde{\theta_i})(t_0)P(a_i(t_k) = Attaquer/\tilde{\theta_i}, a_i(t_0))} = 0.6770.$$

Implémentation sur matlab

À l'aide de Matlab nous avons étudié l'effet de α_p et β_p sur la convergence des croyances postérieures du joueur j.

Dans la Table 4.3 on a fixé le taux $\beta_p = 0.0029$ et nous avons varié le taux α_p . Par contre dans la Table 4.4, nous avons fait l'inverse, nous avons fixé le taux $\alpha_p = 0.833$ nous avons fait varier le taux β_p. Les résultats obtenus sont donnés dans les tableaux suivants :

Iteration / Variable	1	2	3	4	5	6	7	8	9
$\alpha_p = 0.05$	0.0038	0.5159	0.9509	0.9997	0.9998	1.0000	1.0000	1.0000	1.0000
$\alpha_p = 0.1$	0.0038	0.5309	0.9756	0.9993	1.0000	1.0000	1.0000	1.0000	1.0000
$\alpha_p = 0.9$	0.0038	0.6923	0.9986	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000

TABLE 4.3 – Convergence des croyances postérieures du joueur j donnée les observations d'une séquence d'actions d'attaque consécutives sous diverses α.

Iteration / Variable	1	2	3	4	5	6	7	8	9
$\beta_p = 0.001$	0.0038	0.8069	0.9997	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000
$\beta_p = 0.01$	0.0038	0.5685	0.9911	0.9999	1.0000	1.0000	1.0000	1.0000	1.0000
$\beta_p = 0.5$	0.0038	0.5154	0.9493	0.9968	0.9998	1.0000	1.0000	1.0000	1.0000

TABLE 4.4 – Convergence des croyances postérieures du joueur j donnée les observations d'une séquence d'actions d'attaque consécutives sous diverses β.

Nous pouvons distingués trois cas possible selon la relation entre les taux α_p et β_p.

- **Cas 1 : si** $\alpha_p = \beta_p$

  On veut étudier le cas où $\alpha_p = \beta_p$

Iteration	1	2	3	4	5	6	7	8	9
	0.0038	0.5010	0.6671	0.7502	0.8002	0.8334	0.8572	0.8751	0.8889
Iteration	10	11	12	13	14	15	16	17	18
	0.9000	0.9091	0.9167	0.9231	0.9286	0.9334	0.9375	0.9412	0.9445
Iteration	19	20	21	22	23	24	25	26	27
	0.9474	0.9500	0.9524	0.9546	0.9565	0.9583	0.9600	0.9615	0.9630
Iteration	28	29	30	31	32	33	34	35	36
	0.9643	0.9655	0.9667	0.9677	0.9688	0.9697	0.9706	0.9714	0.9722
Iteration	37	38	39	40	41	42	43	44	45
	0.9730	0.9737	0.9744	0.9750	0.9756	0.9762	0.9767	0.9773	0.9778

TABLE 4.5 – Convergence des croyances postérieures du joueur j si $\alpha_p = \beta_p$.

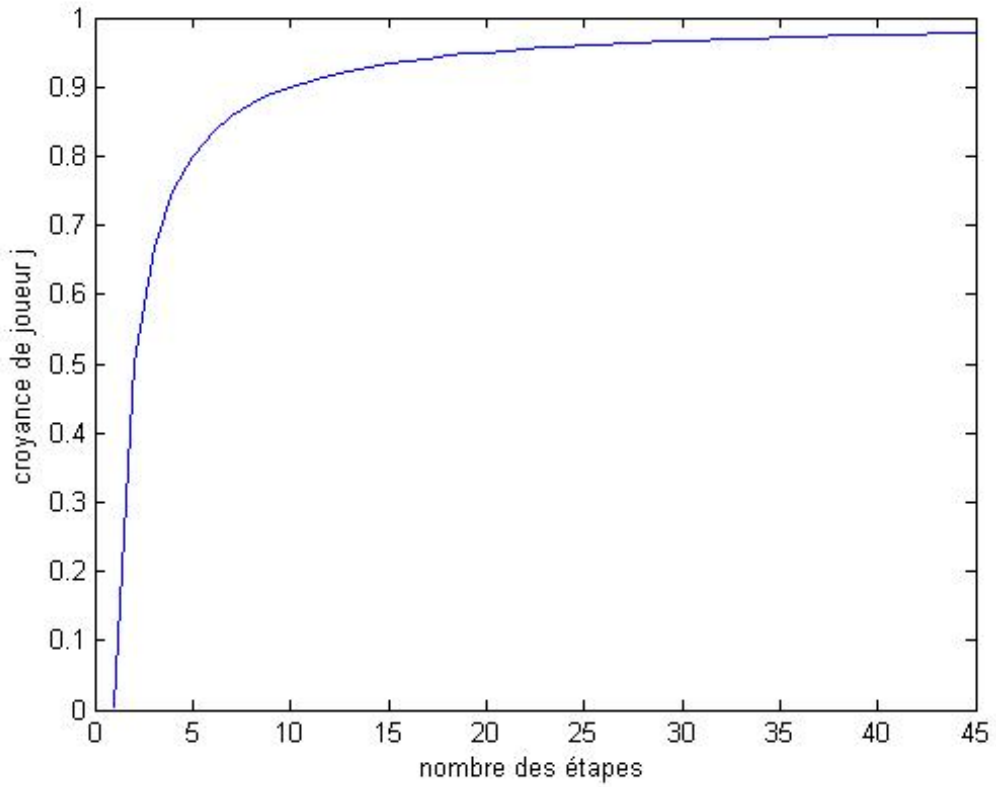

FIGURE 4.2 – Représentation graphique de la convergence des croyances postérieures du joueur j si $\alpha_p = \beta_p$.

- **Cas 2 : si** $\beta_p > \alpha_p$
  Pour $\beta_p = 0.9$ et $\alpha_p = 0.1$

Iteration	1	2	3	4	5	6	7	8	9
	0.0038	0.5001	0.5263	0.5291	0.5294	0.5294	0.5294	0.5294	0.5294
Iteration	10	11	12	13	14	15	16	17	18
	0.5294	0.5294	0.5294	0.5294	0.5294	0.5294	0.5294	0.5294	0.5294

TABLE 4.6 – Convergence des croyances postérieures du joueur j si $\beta_p > \alpha_p$.

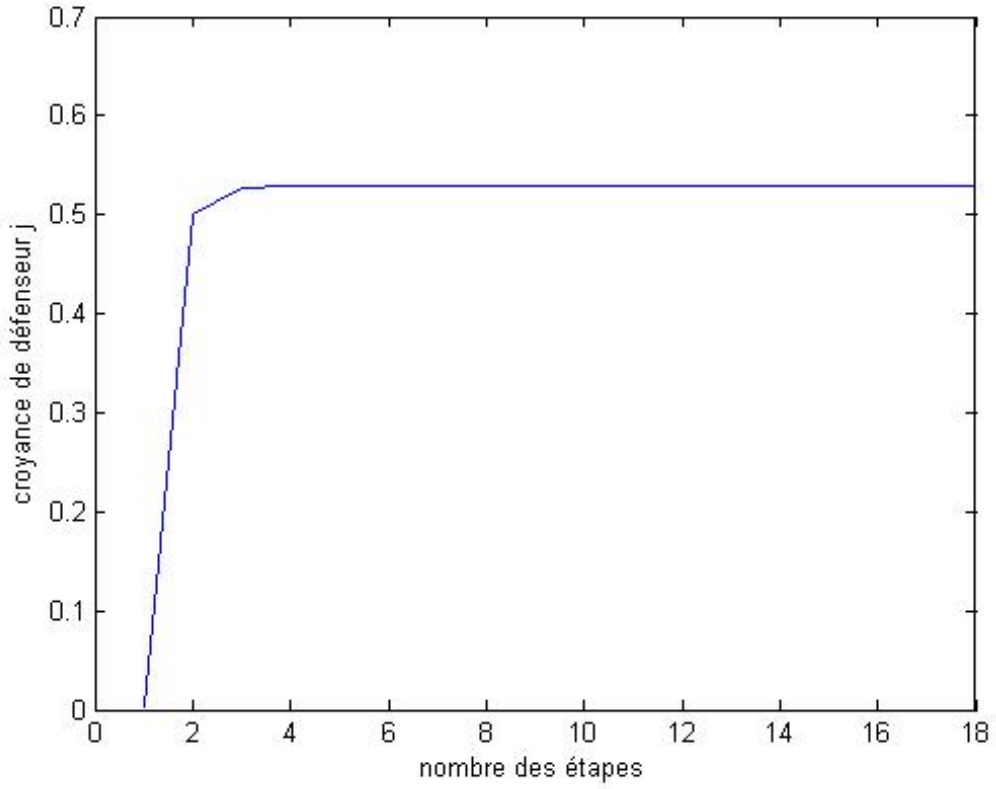

FIGURE 4.3 – Représentation graphique de la convergence des croyances postérieures du joueur j si $\beta_p > \alpha_p$.

Pour $\beta_p = 0.6$ et $\alpha_p = 0.4$

Iteration	1	2	3	4	5	6	7	8	9
	0.0038	0.5006	0.6252	0.6787	0.7066	0.7226	0.7324	0.7385	0.7425
Iteration	10	11	12	13	14	15	16	17	18
	0.7450	0.7467	0.7478	0.7485	0.7490	0.7494	0.7496	0.7497	0.7498

TABLE 4.7 – Convergence des croyances postérieures du joueur j si $\beta_p > \alpha_p$.

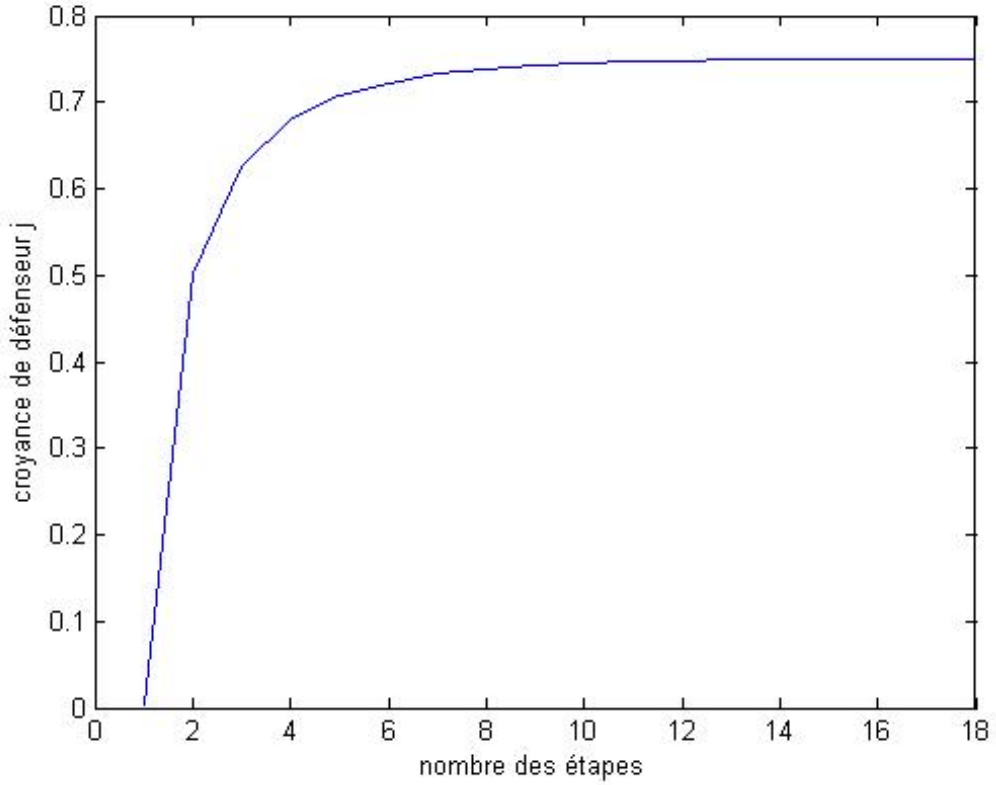

FIGURE 4.4 – Représentation graphique de la convergence des croyances postérieures du joueur j si $\beta_p > \alpha_p$.

- **Cas 3 :si** $\alpha_p > \beta_p$

  Pour $\beta_p = 0.1$ et $\alpha_p = 0.9$

Iteration	1	2	3	4	5	6	7	8	9
	0.0038	0.5084	0.9116	0.9894	0.9988	0.9999	1.0000	1.0000	1.0000
Iteration	10	11	12	13	14	15	16	17	18
	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000

TABLE 4.8 – Convergence des croyances postérieures du joueur j si $\alpha_p > \beta_p$.

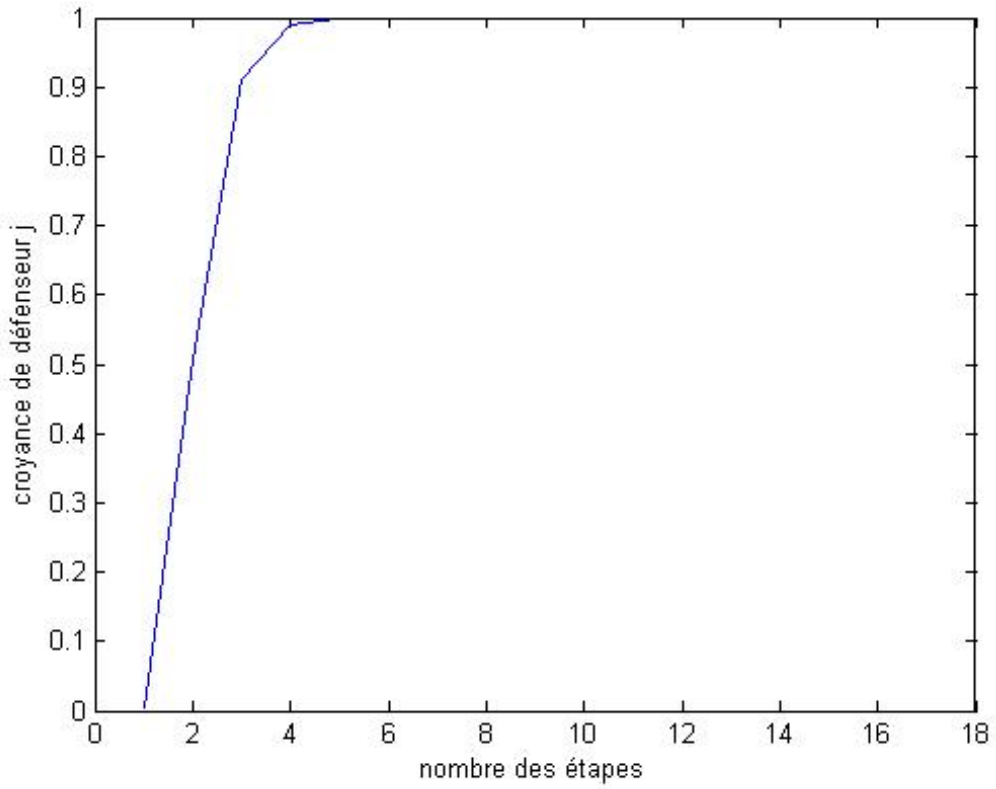

FIGURE 4.5 – Représentation graphique de la convergence des croyances postérieures du joueur j si $\alpha_p > \beta_p$.

Pour $\beta_p = 0.3$ et $\alpha_p = 0.7$

Iteration	1	2	3	4	5	6	7	8	9
	0.0038	0.5022	0.7703	0.8982	0.9557	0.9809	0.9918	0.9965	0.9985
Iteration	10	11	12	13	14	15	16	17	18
	0.9994	0.9997	0.9999	0.9999	1.0000	1.0000	1.0000	1.0000	1.0000

TABLE 4.9 – Convergence des croyances postérieures du joueur j si $\alpha_p > \beta_p$.

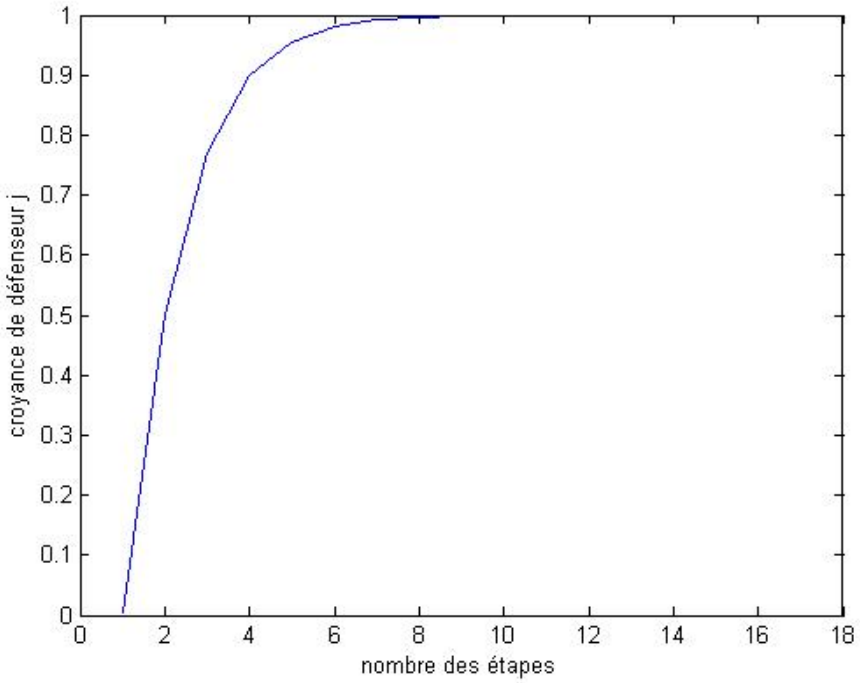

FIGURE 4.6 – Représentation graphique de la convergence des croyances postérieures du joueur j si $\alpha_p > \beta_p$.

4.4.5 Discussion des résultats

- La Table 4.3, montre que plus α_p est élevé, plus la croyance postérieure converge rapidement vers 1. En revanche, la Table 4.4 montre que plus la valeur β_p est basse, plus la croyance postérieure converge plus rapide vers 1. En d'autres termes, la vitesse de convergence de la croyance postérieure du défenseur j augmente avec la précision de détection du système de surveillance.
- De la Table 4.5 et la Figure 4.2 on remarque que si $\alpha_p = \beta_p$ la croyance du défenseur j converge lentement vers 1.
- D'après les Tables 4.6 et 4.7 et leur représentation graphiques données dans les Figures 4.3 et 4.4, nous avons constaté que quand β_p est plus grand que α_p, la croyance ne converge pas vers 1 ou bien si elle converge, elle converge lentement.
- Nous remarquons des Tables 4.8 et 4.9 ainsi que leur représentation graphique (Figure 4.5 et 4.6) que quand α_p est plus grand que β_p la croyance converge vers 1 et plus que α_p est très grand elle converge plus rapidement vers 1.

Donc après avoir observer les résultats, le defenseur j doit se baser sur l'augmentation de taux α_p pour que ses croyances converge plus rapide vers 1 et donc il peut savoir est ce que il va recevoir des attaques ou pas, par conséquent, il peut savoir si il est nécessaire ou pas d'activer son IDS.

4.5 Conclusion

Notre objectif essentiel dans ce chapitre est de voir comment peut-on modéliser un problème de sécurité des réseaux ad hoc par l'approche de la théorie des jeux.
Donc dans un premier temps, nous avons modélisé l'interaction entre le système de détection d'intrusion (IDS) et un attaquant comme un jeu Bayésien statique. Comme dans cette modélisation l'IDS suppose de probabilités préalables fixes quant au type de son adversaire, chose qu'est difficile à réaliser dans la réalité. De plus, les attaques sont répétées à plusieurs reprises, donc cette modélisation n'est pas suffisante ce qui nous a motivé à étendre le jeu Bayésien statique à un jeu Bayésien dynamique. Ce dernier modèle permet au défenseur de mettre à jour ses croyances à propos de type de l'attaquant à la fin de chaque étape du jeu. Par conséquent, l'IDS pourrait fonctionner par intermittence tout en obtenant la même efficacité.

CONCLUSION GÉNÉRALE

Les problèmes de sécurité dans les réseaux ad hoc sont difficiles à résoudre car ces réseaux sont de nature dynamique et sans infrastructure préexistante. Ces caractéristiques empêchent l'utilisation des solutions de sécurité déjà existantes, pour cela l'introduction de la théorie des jeux a été nécessaire afin de cerner l'interaction entre les différents agents du réseau. Quant à la contrainte de l'énergie, les nœuds disposent d'une énergie limitée par la capacité de leur batterie qui est difficilement rechargeable en cours de déploiement.

Dans ce mémoire, nous avons présenté des modèles de la théorie des jeux pour la détection d'intrusion dans les réseaux ad hoc. Nous avons modélisé notre mécanisme d'activation de l'IDS à travers un jeu Bayésien répété entre un nœud attaquant potentiellement malveillant et un défenseur. Chaque entité vise à maximiser son gain : l'attaquant tente de violer les propriétés de sécurité du réseau sans être détecté, tandis que le défenseur tente de maximiser ses capacités de défense avec une contrainte sur la défense des ressources en utilisant l'IDS. Nous avons utilisé le système de croyances pour déterminer les décisions optimales pour les deux joueurs correspondant à l'équilibre Bayésien parfait. Nous avons également montré comment les paramètres du système affectent la vitesse de convergence de la croyance et des stratégies d'équilibre.

Cette étude est loin d'être complète, il est intéressant de la compléter dans plusieurs sens comme par exemple :

- Appliquer d'autres concepts d'équilibre tels que l'équilibre de Nash parfait en sous-jeux et l'équilibre corrélé.
- L'amélioration du taux de détection et en diminuant le taux de faux positifs.

BIBLIOGRAPHIE

[1] A. Agah, S.K. Das, K. Basu, and M. Asadi. "Intrusion detection in sensor networks : A non-cooperative game approach.", In Proceedings of the Third IEEE International Symposium on Network Computing and Applications (NCA 04), pages 343–346, August-September 2004.

[2] T. Alpcan , T. Basar. "A game theoretic analysis of intrusion detection in access control systems.", In Proceeding of the 43rd IEEE Conference on Decision and Control (CDC), December 2004.

[3] T. Alpcan , T. Basar. "A game theoretic approach to decision and analysis in network intrusion detection.", In Proceeding of the 42nd IEEE Conference on Decision and Control (CDC), December 2003.

[4] M. Bouhadi. " Gestion efficace de la sécurité et de l'énergie dans un réseau Ad-hoc : Approche par la théorie des jeux.", Thèse de Doctorat , Université de Bejaia, 2018.

[5] J. Cai , U. Pooch. "Allocate fair payoff for cooperation in wireless ad hoc networks using Shapley value.", In Proceedings of the 18th International Parallel and Distributed Processing Symposium (IPDPS'04), page 219, April 2004.

[6] K. Chait, "Le consensus dans les réseaux ad hoc, Mémoire d'ingéniorat en Informatique.", Université de Bejaia, 2008.

[7] M. Chatterjee, S. K. Das, D. Turgut, " a weighted clustering algorithm for mobile ad hoc networks.", cluster computing, No. 5, page. 193-204, 2002.

[8] A. Cournot. "Recherche sur les principes mathématiques de la théorie des richesses.", Translated by N.T. Bacon as Researches into the Mathematical Principles of the Theory of Wealth. New York : McMillan (1927).

[9] M.Elkoutbi et al. "A New Composite Metric For QoS Satisfying Both Mobility And Bandwidth Constraints In Manets.". In proceedings of African Conference on Research in Computer Science and Applied Mathematics, Côte d'Ivoire,2010.

[10] A. Ephremides, J. E. Wieselthier et D. J. Baker . " A design concept for reliable mobile radio networks with frequency-hopping signaling.", NASA STI/Recon Technical Report , septembre 1988.

[11] C. Johnen, L .H. Nguyen ." Self-stabilizing weight-based clustering algorithm for ad hoc sensor networks.", In Sotiris E. Nikoletseas et José D. P. Rolim, éditeurs : Algorithmic Aspects of Wireless Sensor Networks, Second International Workshop, ALGOSENSORS 2006, Venice, Italy, July 15, 2006, Revised Selected Papers, volume 4240 de Lecture Notes in Computer Science, pages 83-94, 2006.

[12] J.C. Harsanyi. "Games with incomplète information played by bayesian players part.I : The basic model, part.II : Bayesian equilibrium points, part.III : The basic probability distribution of the game.", Management Science, 14-15, 1967-1968.

[13] J.C. Harsanyi. "Games with Incomplete Information. The American Economic Review.", Vol. 85, n° 3. P 291-303,1995.

[14] R. E. Kahn, "The organization of computer resources into a packet radio network" IEEE Trans. Commun, vol. COM-25, no. 1, page. 169-178, Jan. 1977.

[15] M. Kodialam , T.V. Lakshman. "Detecting network intrusions via sampling : A game theoretic approach.", In Proc. IEEE INFOCOM 2003, volume 3, pages 1880–1889, March-April 2003.

[16] P. Liu , W. Zang. "Incentive-based modeling and inference of attacker intent, objectives, and strategies.", In Proceedings of the 10th ACM Conference on Computer and Communications Security (CCS 03), pages 179–189, October 2003.

[17] Y. Liu, C. Comaniciu, H. Man."A Bayesian Game Approach for Intrusion Detection in Wireless Ad Hoc Networks", octobre 2006.

[18] A. Menezes, P. Van orschot, S. Vanstone, " Handbook of Applied Cryptography ", CRC Press, Boca Raton – Florida – États-Unis, 1996.

[19] F. Mertens, Jean et Zamir, Shmuel. "Formulation of Bayesian Analysis for Games With Incomplete Information.", International Journal of Game Theory. 14. 1-29.1985.

[20] N. Mitton ." Auto-organisation des réseaux sans fil multi-sauts à grande échelle.", Thèse de doctorat, INSA de Lyon, Lyon, France, 2006.

[21] H. Moulin. "Théorie des jeux pour l'économie et la politique.", Herman, Paris, 1981.

[22] J. Nash, "Equilibrium Point in N-Person Games.", Proccedings of the National Academy of Sciences, No. 36, pp. 48-49, 1950.

[23] P. Nurmi. "Modelling routing in wireless ad hoc networks with dynamic Bayesian games. In Sensor and Ad Hoc Communications and Networks.", IEEE SECON 2004. First Annual IEEE Communications Society Conference, pages 63–70, October 2004.

[24] J. F. Pillou, " Tout sur les sytèmes d'information ", Paris Dunod, Paris –France, 2006.

[25] M.S. Radjef. "Cours de théorie des jeux.", 1^{er} année Master, Université de Bejaïa, 2018.

[26] C. Shapiro. "Handbook of Industrial Organization.", volume 1, chapter 6 : Theories of Oligopoly Behavior, pages 330-410. Elsevier Science, 1989.

[27] V. Srinivasan, P. Nuggehalli, C-F. Chiasserini, R.R. Rao." An analytical approach to the study of cooperation in wireless ad hoc networks.", IEEE Transsactions on Communications, vol 2 :722–733, March 2005.

[28] H. Sun, H. Wei, "Using Bayesian Game Model for Intrusion Detection in Wireless Ad Hoc Networks.", Int. J. Communications, Network and System Sciences, Vol. 3, No. 7, pp. 602-607, 2010.

[29] A. Urpi, M. Bonuccelli, S. Giordano. "Modelling cooperation in mobile ad hoc networks : A formal description of selfishness.", In WiOpt 03 Workshop : Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks, March 2003.

[30] J.Von Neumann, O. Morgenstern. "Theory of Games and Economic Behavior.", Princeton University Press. 1944.

[31] Y. Xiao, X. Shan, Y. Ren. "Game theory models for IEEE 802.11 DCF in wireless ad hoc networks.", IEEE Radio Communications, 43(3) :S22–S26, March 2005.

[32] M. Yildizoglu, "Introduction à la théorie des jeux", DUNOD, 2003.

RÉSUMÉ

Les réseaux ad hoc sans fil sont en train de devenir un nouveau front de recherche, dans lesquels la sécurité est un problème important. Habituellement, certains nœuds agissent de manière malveillante et sont capables de faire différents types de déni de service (Dos). En raison des ressources limitées, le système de détection d'intrusion (IDS) s'exécute en permanence pour détecter l'intrusion de l'attaquant, ce qui représente un temps système coûteux. Nous avons utilisé les jeux Bayésiens statiques et dynamiques pour modéliser les interactions entre le système de détection d'intrusion et l'attaquant. Nous résolvons le jeu en trouvant l'équilibre Bayésien de Nash et l'équilibre Bayésien parfait. Les résultats de notre analyse montrent que l'IDS pourrait fonctionner par intermittence sans compromettre son efficacité.

Mots clés : Réseaux ad hoc, Jeux Bayésiens, Système de détection d'intrusion, Equilibre de Nash Bayésien .

ABSTRACT

Ad hoc wireless networks are becoming a new research front, in which security is an important problem. Usually, some nodes act maliciously and are able to make different types of denial of service (DOS). Due to limited resources, the Intrusion Detection System (IDS) is always running to detect attacker intrusion, which is costly overhead. We used static and dynamic Bayesian games to model the interactions between the intrusion detection system and the attacker. We solve the game by finding Nash's Bayesian equilibrium and perfect Bayesian equilibrium. The results of our analysis show that the IDS could operate intermittently without compromising its effectiveness.

Key words : Wireless ad hoc networks, Bayesian game, Intrusion system, Bayesian Nash equilibrium.