République Algérienne Démocratique et Populaire

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université A. Mira de Béjaia

جامعة بجاية
Tasdawit n Bgayet
Université de Béjaïa

Faculté des Sciences Exactes

Département de Recherche Opérationnelle

Mémoire de Master
en
Recherche Opérationnelle

Option : Modélisation Mathématique et Techniques de Décision

Thème

Application des Jeux de Formation de Coalitions dans L'Etude de la Sécurité de la Couche Physique des Réseaux Ad-hoc

Présenté par :

M^{lle} **AIANE Nedjma** M^{r} **CHEBEL Salim**

Devant le jury composé de :

Président	M^{me} **HALIMI**	**M.A.A**	**U. A/Mira Béjaia**
Rapporteur	M^{r} **M. S. RADJEF**	**Professeur**	**U. A/Mira Béjaia**
Examinatrice	M^{me} **DJOUADI**	**M.A.A**	**U. A/Mira Béjaia**
Examinatrice	M^{lle} **BOUHADDI**	**Doctorante**	**U. A/Mira Béjaia**

Promotion 2014 / 2015

Remerciement

Nous remercions le dieu tout puissant de nous avoir donné force et courage pour accomplir cet humble recueil.

Nous tenons à remercier le Professeur RADJEF de nous avoir accordé le privilège d'apporter son aide pour l'accomplissement de notre travail.

Notre reconnaissance a tous ceux qui ont contribués, de près ou de loin à la réalisation du projet et particulièrement à M^{lle} BOUHADDI.

Nos sincères remerciements vont particulièrement à nos parents et à nos familles.

Cet humble recueil est dédié :

A *mes chers parents qui m'ont toujours répondu présent durant toute ma vie.*

A *mes frères et sœur.*

A *mes amis Mourad, Lamine, Nabil.*

A *toutes les personnes qui m'ont apportés de l'aide.*

Salim

Ce modeste travail est dédié :

A *mes chers parents qui m'ont toujours répondu présent durant toute ma vie.*

A *mes frères Abdou, Chérif et ma petite sœur Maya.*

A *mes amis(e).*

A *toutes les personnes qui m'ont apportés de l'aide.*

Nedjma

Table des matières

Table des figures

Liste des notations

$\mathcal{N}$: ensemble des joueurs (utilisateurs).
$\mathcal{M}$: ensemble des destinations.
$\mathcal{K}$: ensemble d'oreilles indiscrètes (espions).
$\mathcal{H}$: ensemble des coordinateurs.
$\mathcal{P}$: ensemble des profits de stratégies.
N : nombre de joueurs (émetteurs).
M : nombre de récepteurs.
K : nombre d'espions.
He : nombre de coordinateurs.
m_i : désigne la destination d'un émetteur i.
X_i : ensemble des stratégies du joueur $i \in \mathcal{N}$.
f_i : fonction d'utilité du i^{eme} joueur.
V : fonction caractéristique.
S : une coalition.
T : une structure de coalitions.
ϕ : valeur de Shapley.
Γ : jeu Gamma.
Δ : jeu Delta.
σ : profil de stratégies.
ρ : règle d'ordre.
$P(Q)$: fonction inverse de demande du marché.
R_j : fonction de réaction de la firme j.
$\mathcal{P}_i$: ensemble de niveau de puissance de transmission du joueur (émetteur) i.
L : nombre de niveaux de puissance de transmission.
$\mathcal{P}$: ensemble des profils de stratégies.
$C(P_i)$: taux de secret entre le nœud i utilisant le niveau de puissance P_i et son coordinateur $h \in \mathcal{H}$.
C_h^i : capacité du canal entre le nœud i et son coordinateur h.
C_k^i : capacité du canal entre le nœud i et l'oreille indiscrète $k \in \mathcal{K}$.

O : fonction de détection des intrus.
$C = \{0, 1\}$: ensemble d'empoisonnement de cachette.
$M = \{0, 1\}$: ensemble d'inondations malveillantes.
$NFP(i)$: nombre de paquets expédiés par un nœud $i \in \mathcal{N}$.
$NR_{\_ack(i)}$: nombre de reconnaissances reçues par le nœud $i \in \mathcal{N}$.
$NRP(i)$: nombre de paquets reçus par le nœud $i \in \mathcal{N}$.
$ENRP(i)$: nombre prévu de paquets à recevoir par le nœud $i \in \mathcal{N}$.
CL : ensemble des classes de sécurités.
SE : ensemble des seuils de différentes classes de sécurité.
$F(\mathcal{N})$: fonction sévérité.
r_i : réputation du nœud $i \in \mathcal{N}$.
δ : nombre de joueurs dans S.
γ : nombre de coalitions possibles dans le MANET.
$S^{'}$: ensemble des coalitions gagnantes.
se_i : seuil d'une classe de sécurité.
Δt : intervalle de temps.
$SD = \{(a, b)/(a, b)\}$: paire de source-destination.
Q_{ab} : nombre de paquets de données transmis entre les deux nœuds a et b.
$P_{ab}(S)$: ensemble des chemins à l'intérieur de la coalition S reliant le nœud a au nœud b.
$t(k)$: fiabilité du chemin k.
P_{ij} : fidélité du chemin (i,j).
D_{ij} : distance entre le nœud i et j.
h_{i,m_i} : gain du canal entre un émetteur $i \in \mathcal{N}$ et une destination $m_i \in \mathcal{N}$.
d_{i,m_i} : la distance entre l'émetteur $i \in \mathcal{N}$ et le récepteur $m_i \in \mathcal{M}$.
μ : un paramètre lié à l'environnement.
θ_{i,m_i} : paramètre généré selon la loi uniforme sur $[0, 2\pi)$ pour chaque émetteur i et sa destination m_i.
$g_{i,k}$: gain du canal entre l'émetteur $i \in \mathcal{N}$ et un espion $k \in \mathcal{K}$.
C_{i,m_i} : taux de secret entre l'émetteur $i \in \mathcal{N}$ et sa destination $m_i \in \mathcal{M}$.
C^d_{i,m_i} : capacité d'information que l'émetteur i peut transmettre à sa destination m_i.
$C^e_{i,k}$: perte de taux de secret pour l'émetteur i causée par l'espion k.
$q_{i,\hat{i}}$: gain de canal entre l'utilisateur i et $\hat{i}$.
σ^2 : variance du bruit.
ν_0 : rapport signal bruit (SNR).
$\tilde{P}$: puissance de transmission.
$\overline{P}_{i,\hat{i}}$: puissance de transmission utilisée lors de la phase d'échange d'information.
P^S_i : puissance de transmission utilisée par la coalition S pour transmettre les données de l'utilisateur i.

h_S : vecteur colonne, représente le canal de "utilisateur-destination".
g_S^k : vecteur colonne, représente le canal de "utilisateur-espion k".
w_S : vecteur colonne, représente le poids de signal.
H : désigne la transposé du conjugué.
$C_{i,m_i}^{S,DF}$: taux de secret de l'utilisateur $i \in S$ après l'utilisation du protocole DF.
R_S : matrice carrée $|S| \times |S|$.
G_S : matrice $(K+1) \times |S|$.
e : vecteur $(K+1) \times 1$.
$V_{i_j}(S)$: profit du j^{me} émetteur $\in S$.
$C_{i_j}(S)$: fonction qui calcule la perte pour l'utilisateur $i_j \in S$.
$\hat{C}_{i,k}^e$: perte causée par l'espion $k \in \mathcal{K}$ lors de la phase d'échange d'information.
Π_0 : structure de coalitions initiale.
Π_c : structure de coalitions courante.
$S_{\Pi_c}(i_j)$: désigne la coalition S auquel i_j appartient dans la structureΠ_c.
Π_f : structure de coalitions finale.

Introduction Générale

La communication est le fondement de toute société humaine, très tôt dans son histoire, l'homme a souhaité dépasser les limites imposées par la portée de sa voix et de sa perception, en inventant divers outils : machines, appareilles et mécanismes qui permettent d'établir la communication, mais le besoin incessant de partager et d'échanger des informations ne cesse d'accroitre, ce qui a fait naitre une nouvelle technologie qui répond de mieux en mieux aux exigences et aux attentes du monde actuel. Cette technologie se nomme réseau Ad-hoc [1], appelée aussi MANET (Mobile Ad-hoc Network).

Un réseau Ad-hoc est une collection de nœuds (terminaux, ordinateurs portables, PDAs, smartphones, capteurs, etc.) mobiles formant un réseau temporaire à topologie variable, doté d'une transmission sans fil appelée ondes radio.
A l'origine, les applications exploitant les réseaux Ad-hoc ont été envisagées principalement pour des situations de crise (par exemple, dans les champs de bataille ou pour des opérations de secours). Bien que cette avancée technologique présente de nombreux avantages, elle présente aussi des inconvénients tel que le problème de sécurité qui est un sujet d'une grande importance et un critère de sélection, à cause de l'utilisation de lien sans fil ce qui facilite considérablement les attaques et engendre des failles dans le système de sécurité. Pour remédier à ce problème, il existe de nombreux travaux incluant la théorie des jeux [6], [15], [19] qui est un outil performant et un moyen qui permet de mieux analyser et étudier le comportement interactif entre les différents nœuds qui constituent le réseau.

La théorie des jeux est apparue au début des années 40, elle vise à analyser des situations d'interaction entre plusieurs agents rationnels et les conséquence de leurs comportements stratégiques. L'apparition des jeux coopératifs et les jeux de formation de coalitions, qui sont inspirés de la réalité, a conduit a un certain renouvellement de la modélisation d'un réseaux Ad-hoc sous forme d'un jeu coopératif où ce dernier offre la

1. Locution latine qui peut être traduite par adéquat ou appropriée. Dans le contexte des réseaux sans fil elle signifie plutôt "créé pour l'occasion".

possibilité de regrouper les nœuds du réseau ayant un objectif commun au sien d'une coalition.

L'objectif de ce mémoire est d'examiner à la lumière de la théorie des jeux, le comportement coopératif qui émerge entre les nœuds afin d'améliorer la sécurité du réseau Ad-hoc.

Notre travail est organisé comme suit :
Le premier chapitre donne un aperçu général sur les environnements mobiles Ad-hoc. Il présente ses applications, ses caractéristiques (changements fréquents de topologie, utilisation limitée de l'énergie, etc.), puis nous aborderons l'aspect sécurité où nous passerons en revue quelques attaques et techniques de défenses.

Le second chapitre sera consacré à la théorie des jeux : entre définition d'un jeu, sa classification, concepts de solutions, les jeux de formation de coalitions et leur condition de stabilité.

Le troisième chapitre, portera sur une synthèse bibliographique des travaux réalisés ces dernière années sur la sécurité des réseaux Ad-hoc via la théorie des jeux.

Quant au dernier chapitre, nous présenterons un modèle qui traite le problème de sécurité des réseaux Ad-hoc où nous serons amenés à implementer un algorithme de formation de coalitions, et faire une comparaison d'utilité moyenne (taux de secret) entre deux approches coopérative et non coopérative ce qui constitue l'essentielle de notre contribution.

Chapitre 1

Réseaux Ad-hoc

1.1 Introduction

Aujourd'hui, les réseaux sans fil ont connu une forte expansion et sont de plus en plus populaires du fait de leur facilité de déploiement. L'évolution rapide de la technologie dans le domaine de la communication sans fil, a permis aux usagers munis d'unités de calcul portables d'accéder à l'information à n'importe quel moment depuis n'importe quel endroit. Cet environnement n'astreint plus l'usager à une localisation fixe, mais lui permet une libre mobilité tout en assurant sa connexion avec le réseau. Il offre des solutions ouvertes pour fournir des services essentiels là où l'installation d'infrastructures n'est pas possible. Les réseaux sans fil sont généralement classés selon deux catégories : les réseaux sans fil avec infrastructure fixe qui utilisent généralement le modèle de la communication cellulaire et les réseaux sans fil sans infrastructure fixe, appelés aussi réseaux Ad-hoc.

- **Réseaux avec infrastructure :** un nœud peut se connecter directement avec les nœuds qui se trouvent dans la même station de base.
- **Réseaux sans infrastructure :** un nœud peut se connecter directement avec les autre nœuds qui se trouvent dans son rayon de transmission.

Ce chapitre sera consacré à la présentation d'une classe particulière de réseaux sans infrastructure, sur laquelle est portée notre étude, qui est la classe des réseaux Ad-hoc. Nous passerons en revue leurs applications, caractéristiques ainsi que leurs faiblesses en terme de sécurité et nous citerons quelques attaques et techniques de défense.

1.2 Réseaux Ad-hoc

Un réseau mobile Ad-hoc, ou bien appelé MANET (Mobile Ad-hoc Network), est une collection de nœuds (terminaux, ordinateurs portables, PDAs, smartphones, capteurs$\cdots$,) mobiles qui interagissent et coopèrent pour bénéficier ou bien offrir des services. Un nœud

dans un réseau Ad-hoc peut à la fois communiquer directement avec d'autres nœuds ou servir de relais. Un relais est utilisé pour communiquer dans la situation où les nœuds se trouvent hors de portée radio les uns des autres. Ces réseaux sont dits Ad-hoc dans la mesure où ils ne nécessitent pas d'infrastructure.
Le mode de fonctionnement "Ad-hoc" se distingue du mode "infrastructure" du fait que dans ce dernier mode de communication les nœuds communiquent entre eux via un point d'accès appelé aussi base, qui peut être relié à un réseau fixe. La figure suivante montre la différence d'utilisation des réseaux sans fil en mode infrastructure fixe et en mode Ad-hoc.

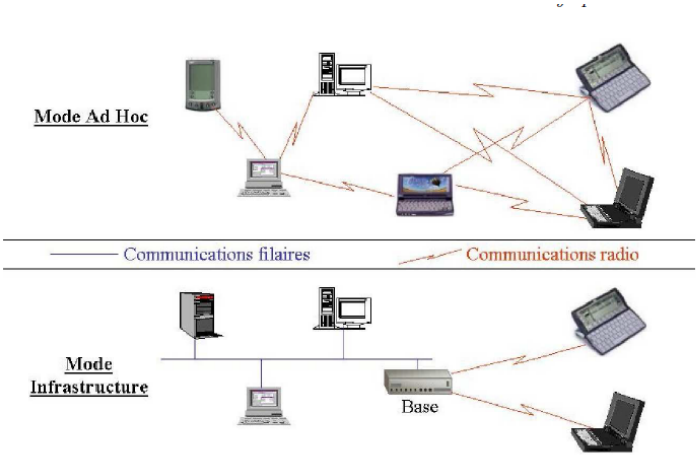

FIGURE 1.1 – Mode Ad-hoc / Mode infrastructure.

1.2.1 Modélisation mathématique 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 (les unités ou les hôtes mobiles) du réseau et E_t modélise l'ensemble des connexions qui existent entre ces nœuds à l'instant t qui sont les liens réseau. Si $e = (u, v)$ appartient à E_t, cela signifie que les nœuds u et v sont en mesure de communiquer directement à l'instant t.

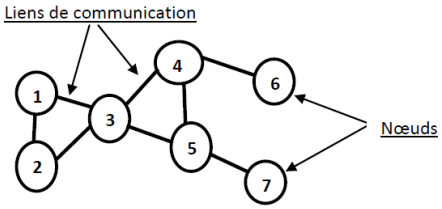

FIGURE 1.2 – Modélisation d'un réseau Ad-hoc.

1.2.2 Applications

Les domaines d'application des réseaux Ad-hoc sont nombreux, nous pouvons citer à titre d'exemple les applications suivantes [26] :

- **Domaine militaire :** Lors des interventions en milieu hostile, il peut être difficile ou trop encombrant d'utiliser un réseau à infrastructure. Les réseaux sans fil sont parfaitement bien adaptés à ce type d'environnement.
- **Services d'urgence :** Lors des catastrophes d'origine naturelle comme un tremblement de terre, feux, inondation $\cdots$, les réseaux sans fil, par leurs capacités et leurs rapidités de déploiement, permettent aux différentes équipes de secours d'établir rapidement des liaisons et d'échanger des informations.

- **Domaine commercial :** Pour un paiement électronique distant ou pour l'accès mobile à internet, ou bien servir de guide en fonction de la position de l'utilisateur.

1.2.3 Caractéristiques

Les réseaux Ad-hoc se caractérisent par :

- **Topologie dynamique :** les raisons principales du changement de topologie sont dues à la mobilité des nœuds, les interférences, le bruit, la puissance de transmission, la direction de l'antenne et le mécanisme de mise en veille pour la préservation de l'énergie [22].
  La figure ci-dessous illustre le changement de topologie.

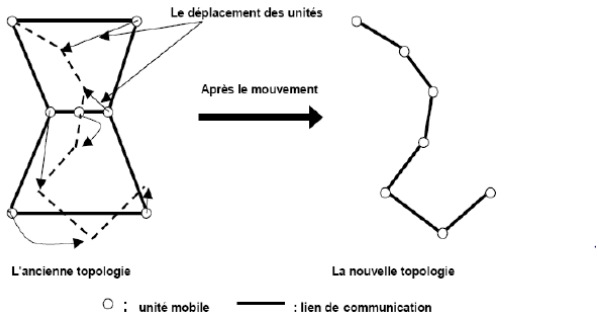

FIGURE 1.3 – Le changement de topologie des réseaux Ad-hoc.

- **Contrainte d'énergie :** les nœuds dans les réseaux Ad-hoc sont alimentés par des batteries dont les capacités sont limitées. Par conséquent, elles ne peuvent pas satisfaire les demandes d'énergie des nœuds pour un fonctionnement normal durant une période de temps raisonnable.

– **Sécurité limitée :** les réseaux Ad-hoc sont plus touchés par le manque de sécurité que les réseaux filaires classiques. Cette vulnérabilité est due essentiellement à la nature du médium de propagation sans fil qui rend possible certaines attaques, par exemple l'écoute clandestine [1].

1.2.4 Avantages et inconvénients des réseaux Ad-hoc

Parmi les avantages des réseaux Ad-hoc, nous citons :

– le déploiement dans un environnement quelconque ;
– le faible coût d'exploitation du réseau dû à l'absence d'infrastructure ;
– la souplesse d'utilisation des réseaux Ad-hoc.

Même si les réseaux Ad-hoc jouissent de nombreux avantages, cependant plusieurs contraintes restent encore à traiter. Nous citons à titre d'exemple :

– les possibilités de communication limitées en raison de la connectivité ;
– la sécurité dans les réseaux Ad-hoc est difficile à contrôler ;
– la faible autonomie des batteries constitue un frein à une utilisation longue du terminal et à la mise en place de nouveaux services.

1.2.5 Routage dans les réseaux Ad-hoc

Définition 1.1

Généralement, le routage est une méthode d'acheminement des informations à la bonne destination à travers un réseau de connexion donné. Le problème de routage consiste, pour un réseau dont les arcs, les nœuds et les capacités sur les arcs sont fixés, à déterminer un acheminement optimal des paquets (messages) à travers le réseau au sens d'un certain critère de performance. Le problème consiste à trouver l'investissement de moindre coût en capacités minimales et de réserves qui assure le routage du trafic minimal et garantit sa survabilité en cas de panne d'arc ou de nœud.

La figure suivante illustre le chemin optimal reliant la source à la destination.

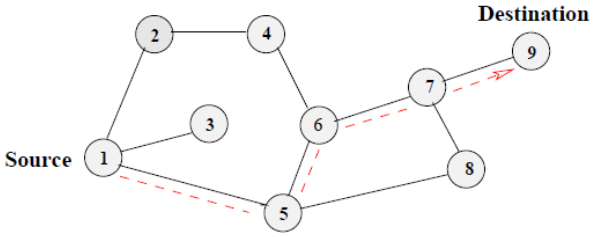

FIGURE 1.4 – Chemin entre la source et la destination dans le routage.

Une bonne stratégie de routage utilise ce chemin pour transmettre les paquets entre les deux nœuds. Pour être réellement opérationnel dans un environnement mobile, le protocole de routage prend en compte trois phases :

1. **Découverte de l'information de routage :** cette étape permet de connaitre les éléments nécessaires sur la topologie utilisée pour choisir un chemin qui peut atteindre le nœud de destination.
2. **Choix du chemin :** après la collecte des informations obtenues, le protocole de routage peut choisir une route en fonction de certains critères, par exemple : le nombre minimum de sauts, économie d'énergie···
3. **Maintenance des routes :** la topologie des réseaux Ad-hoc n'arrête pas d'évoluer avec le temps. Les routes sont dans l'obligation de changer à cause de la mobilité des nœuds, le protocole de routage doit prendre en compte ces changements et met à jour les nouvelles routes qui apparaîssent et d'autres qui disparaissent.

Nous distinguons trois familles de protocoles de routages Ad-hoc [4] :

Protocoles proactifs

Ces protocoles sont basés sur la même stratégie de routage que dans les réseaux filaires, qui est l'existence de tables de routage au niveau de chaque nœud. Les deux principales méthodes utilisées sont la méthode *état de lien* "Link state" et la méthode *vecteur de distance* "Distance vector".

Protocoles réactifs

Ces protocoles créent et maintiennent les routes selon le besoin. La différence avec les protocoles proactifs est que la taille des tables de routage stockée en mémoire est moins importante.

Protocoles hybrides

C'est une hybridation des deux derniers protocoles, ils tirent les avantages des protocoles réactifs et proactifs.

1.3 Vulnérabilités des réseaux Ad-hoc

Définition 1.2

Une vulnérabilité est une faiblesse ou une faille dans le système de sécurité qui peut être exploitée par un attaquant [35].
Le principal problème ne se situe pas au niveau du support physique, mais principalement dans le fait que tous les nœuds sont équivalents et potentiellement nécessaires pour le fonctionnement du réseau.
La première vulnérabilité de ces réseaux est liée à la technologie sans fil, nous pouvons citer :

- **Vulnérabilité du canal :** dans un réseau Ad-hoc, un message peut être écouté ou une fausse information peut être injectée dans le réseau sans avoir accès aux composantes du réseau.

- **Vulnérabilité du nœud :** le fait que les nœuds aient la possibilité de se déplacer dans des endroits non protégés peut facilement les rendre victimes d'une attaque.

- **Absence d'infrastructure :** un réseau Ad-hoc est supposé être opérationnel sans infrastructure fixe, mais cela rend les solutions de sécurité classiques, basées sur les autorités de certification, inapplicables.

- **Vulnérabilité du mécanisme de routage :** l'opération du routage est complètement distribuée et requiert la coopération de chaque nœud dans le réseau.
  Cette coopération peut être considérée comme un point vulnérable pour mener les différentes attaques.

- **Changement dynamique de topologie :** dans les réseaux mobiles Ad-hoc, le changement de la topologie requiert un protocole de routage sophistiqué ce qui est un défi additionnel pour la sécurité. Une difficulté particulière réside dans le fait qu'une information de routage incorrecte peut être générée par un nœud malicieux ou bien cela peut être le résultat d'un changement de topologie et il est difficile de distinguer entre les deux cas.

1.4 Sécurité dans les réseaux Ad-hoc

Le service de sécurité dans un réseau mobile Ad-hoc n'est pas différent de ceux des autres réseaux. Le but est de protéger l'information des attaques et des mauvais comportements. Pour faire face à ses menaces, la sécurité des réseaux se base sur un certain nombre de services [5]. Les principaux services que doit offrir un mécanisme de sécurité sont décrits comme suit :

- **Disponibilité :** la disponibilité vise à assurer que le système soit bien prêt à l'emploi. Elle le protège également contre les menaces qui peuvent causer sa perturbation, y compris la non-disponibilité des services, le vol des données et la destruction du matériel.
- **Authentification :** l'authentification permet d'assurer que la communication d'un nœud à un autre est authentique, en d'autres termes s'assurer qu'il n'y a pas de nœud malveillant masqué.
- **Confidentialité :** ce principe permet de s'assurer que le message ne peut être compris que par la source et la destination, en utilisant par exemple un type de codage.
- **Intégrité :** l'intégrité consiste à garantir la non-modification des données envoyées à sa destination durant la communication par des nœuds malicieux, c'est-à-dire qu'un message envoyé de A vers B n'est pas modifié par un autre nœud malicieux C.
- **Non répudiation :** ce service permet de garantir qu'aucun des correspondants ne pourra nier la transaction, c'est-à-dire indiquer que des actions ou bien des événements ont bien eu lieu.

1.5 Attaques dans les réseaux Ad-hoc

L'utilisation des liens sans fil facilite considérablement les attaques contre les réseaux Ad-hoc. En effet, étant donné que les transmissions radio sont effectuées dans l'air, ce qui facilite l'écoute. Il suffit qu'un attaquant soit dans le champ de transmission d'un nœud pour pouvoir intercepter les communications de ce dernier, contrairement aux réseaux filaires où l'attaquant doit avoir un accès physique au réseau ou bien de se connecter aux câbles.

En outre, à cause des limitations du support, les communications peuvent facilement être perturbées : une fois que l'intrus a accès au réseau, il peut intercepter facilement les données transmises et les modifier, puis les retransmettre ou bien perturber les communications avec un bruit.

1.5.1 Les types d'attaques

La figure ci-dessous illustre que les attaques peuvent être une interruption, interception, modification ou fabrication lors de la transmission des données.

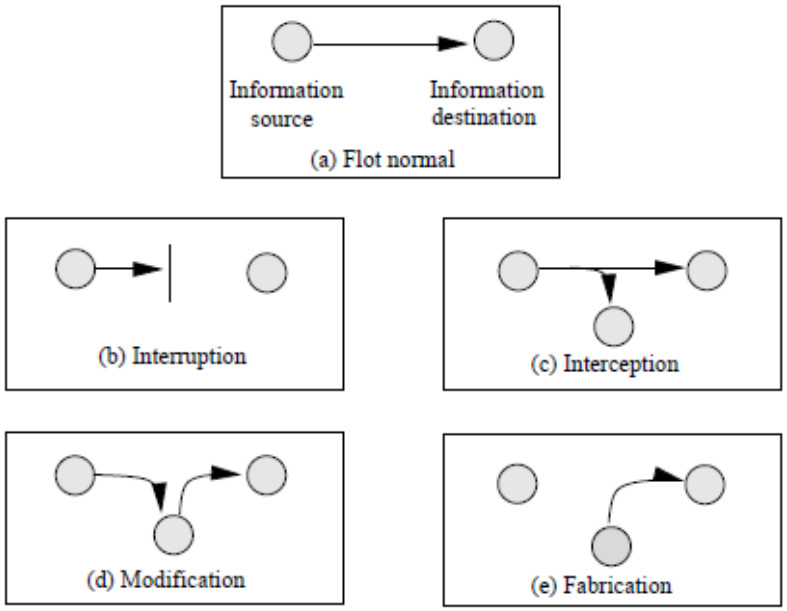

FIGURE 1.5 – Attaques de sécurité

- **Interruption :** un système est détruit ou devient non disponible, c'est une attaque contre la disponibilité.
- **Interception :** intercepter les données, c'est une attaque de confidentialité, par exemple : écoute clandestine.
- **Modification :** modifier les messages, c'est une attaque d'intégrité.
- **Fabrication :** la fabrication des messages et l'insertion de ces messages dans le réseau, c'est une attaque d'authentification.

Définition 1.3

Dans les réseaux mobiles Ad-hoc, un nœud malicieux n'est qu'une unité mobile malveillante, ayant pour but d'écouter clandestinement le trafic, ou bien lancer des attaques qui perturbent le fonctionnement correct d'un réseau. Par exemple, inonder un nœud et modifier le contenu d'une information.

1.5.2 Classification des attaques

Le succès d'une attaque dépend de la vulnérabilité du système et de l'inefficacité des contres-mesures. Les attaques peuvent être classées par leur source (interne ou externe), par leurs effets (passive ou active).

- **Attaques externes :** les attaques externes sont lancées par des nœuds qui n'appartiennent pas au réseau. Nous supposons que l'intrus a accès à toutes les communications entre chaque paire de nœuds légitimes. Par conséquent, il pourra lire, modifier, supprimer, insérer ou envoyer un ancien message.
- **Attaques internes :** les attaques internes sont lancées par des nœuds qui appartiennent au réseau. Par conséquent, il pourra par exemple : modifier le chemin ou supprimer des routes.
- **Attaques passives :** dans ce type d'attaques, l'attaquant n'interrompt pas le protocole de routage, mais tente de découvrir des informations valables en captant le trafic de routage.
- **Attaques actives :** dans ce type d'attaques, l'attaquant participe activement dans la perturbation du fonctionnement du réseau. Il peut supprimer des messages ou modifier des paquets transités dans le réseau.

1.5.3 Taxinomie des attaques

- **Le trou noir (Blackhole) :** c'est un type d'attaque de routage, où un nœud malveillant tente d'exploiter les failles des protocoles de routage afin de se faire élire comme faisant partie du plus court chemin vers le nœud dont il veut intercepter les paquets. Il pourra donc recevoir les paquets destinés à ses victimes et les supprimer afin de réaliser un déni de service.
- **Le trou ver :** cette attaque nécessite la participation d'au moins deux nœuds pour se réaliser, l'objectif est de créer un tunnel entre eux afin de réaliser un raccourci (wormhole) dans le réseau. Une fois le tunnel créé, les deux attaquants encapsulent les messages reçus et les échangent à travers le tunnel, en privant donc les nœuds intermédiaires de recevoir les messages de contrôle du routage.
- **Attaques par déni de service (Sleep Deprivation) :** l'attaquant peut simplement perturber le fonctionnement d'un protocole de routage. L'attaquant peut, par exemple, envoyer de fausses informations de routage : envoyer de faux paquets de contrôle, mentir sur quelques métriques de routage, falsifier les tables de routage.
- **Attaque Sybille :** l'attaque Sybille est définie initialement comme le fait qu'un nœud malveillant (Sybil node) parvienne à posséder illégitimement plusieurs identités et simule un ensemble de nœuds associés à ces identités. Par la suite, plusieurs

variantes sont apparues dans différentes situations. Elle est considérée comme une attaque très difficile à détecter [2].

1.6 Techniques de défense

La sécurité dans les réseaux Ad-hoc est difficile à contrôler, En effet, l'absence d'infrastructure rend ces réseaux sensibles aux problèmes de sécurité. Parmi les concepts de sécurité existant, nous citons :

- **Cryptographie :** la cryptographie est l'art de coder l'information, elle répond aux besoins suivants : confidentialité, intégrité, authenticité et non répudiation. Elle est basée sur le chiffrement qui consiste à transformer une donnée (texte, message, $\cdots$) afin de la rendre incompréhensible par une personne autre que celui qui a créé le message et celui qui en est le destinataire.
  La fonction permettant de retrouver le texte clair à partir du texte chiffré s'appelle le déchiffrement. On distingue deux systèmes :
  - Systèmes symétriques : on utilise une même clé pour le chiffrement et le déchiffrement.
  - Systèmes asymétriques : chaque personne possède 2 clés distinctes (une privée et une publique).
- **Proxy :** un serveur proxy est un serveur informatique qui a pour fonction de relayer des requêtes entre un poste client et un serveur. Les serveurs proxys sont notamment utilisés pour assurer les fonctions suivantes :
  - la journalisation des requêtes ;
  - la sécurité du réseau local ;
  - le filtrage et l'anonymat.
- **Antivirus :** les antivirus sont des programmes capables de détecter la présence de virus sur un ordinateur, ainsi que de nettoyer celui-ci dans la mesure du possible si jamais un ou plusieurs virus sont trouvés. Nettoyer signifie supprimer le virus du fichier sans l'endommager. Mais parfois, ce nettoyage simple n'est pas possible.
- **Firewall (Pare-feu) :** un pare-feu est un logiciel qui vérifie les informations provenant d'internet ou d'un réseau, puis les empêche d'accéder à l'ordinateur ou les y autorise.
  Un pare-feu aide à empêcher les utilisateurs ou les logiciels malveillants d'accéder à un ordinateur via un réseau ou internet. Il peut également empêcher un ordinateur d'envoyer des éléments logiciels nuisibles à d'autres ordinateurs.

Le schéma suivant illustre la façon dont un pare-feu fonctionne :

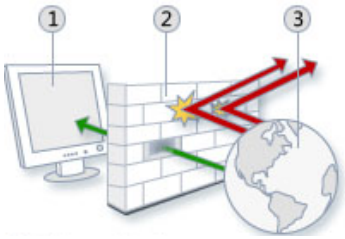

FIGURE 1.6 – Le fonctionnement d'un pare-feu

- 1 un ordinateur.
- 2 un pare-feu.
- 3 internet.

1.7 Couche physique

Dans ce travail, nous nous sommes intéressés à la sécurité des réseaux Ad-hoc, en particulier, la sécurité de la couche physique. Pour cela, on introduit quelques concepts liés à cette dernière.

La couche physique, est la première couche du modèle OSI [1]. Cette couche assure les techniques d'émission et de réception de données.

• Les attaques reliées à la couche physique
- Espionnage (eavesdropping) : consiste à écouter les données transmises entre un émetteur et un récepteur, cette attaque, est considéré comme une attaque passive.
- Déni de service défini dans la section (1.5.3).

1.8 Conclusion

Dans ce chapitre, nous avons donné un aperçu général des réseaux sans fil Ad-hoc et nous avons présenté les raisons qui ont poussé à leur apparition. Nous avons également présenté les propriétés les plus importantes de ces réseaux, à savoir l'utilisation de liens sans fil, les changements fréquents de topologie ···

Ces propriétés engendrent de nouvelles problématiques telles que le problème de sécurité qui est un sujet pertinent et nécessite toute l'attention. Afin d'élaborer une solution, nous ferons recours à un outil d'analyse qui est la théorie des jeux.

Dans le prochain chapitre, nous présenterons les notions de base de la théorie des jeux, qui nous serviront à l'étude de la sécurité des réseaux Ad-hoc.

1. Open Systems Interconnection.

Chapitre 2

Concepts de base de la théorie des jeux

2.1 Introduction

Ces dernières années, plusieurs problèmes de sécurité informatique, comme la détection d'intrusions, utilisent la théorie des jeux comme un moyen de modélisation et d'analyse. Cette théorie peut être un moyen élégant pour détecter les interactions existant entre les nœuds du réseau.

En effet, la théorie des jeux est une branche des mathématiques appliquées qui décrit et analyse des situations interactives de décision. Elle procure un ensemble riche d'outils afin d'étudier et de prédire une issue d'interactions complexes entre des entités rationnelles. Ce présent chapitre portera sur la présentation des principales notions de cette théorie et nous mettrons l'accent sur une classe de jeux, qui est les jeux de coalition.

2.2 Bref historique

L'origine de la théorie des jeux remonte aux travaux d'Antoine Augustin Cournot (1838), mais c'est grâce aux travaux de John Von Neumann et Oskar Morgenstern que la théorie des jeux est véritablement considérée comme une nouvelle discipline. En effet, en 1944 ces deux auteurs publient leur célèbre ouvrage "Theory of Games and Economic Behavior" [23], qui détaille la méthode de résolution des jeux à somme nulle qui a été établie par Émile Borel. Dans son ouvrage de 1938 "Applications aux Jeux de Hasard", Borel développe le théorème du Min-Max pour les jeux à somme nulle à deux joueurs, c'est-à-dire les jeux dans lesquels ce que gagne l'un est perdu par l'autre. En 1950, John Forbes Nash établit le fameux concept qui porte son nom (Équilibre de Nash) pour les jeux à somme variable qui généralise les travaux de Cournot.

Même si, au départ, la théorie des jeux a été développée pour des problèmes de sciences économiques, elle est actuellement largement utilisée dans divers domaines comme les sciences politiques, la biologie, la sociologie et très récemment pour les problèmes de

réseaux et de sécurité [33], [24], [30], [31].

2.3 Description d'un jeu et classification

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 intervienne. En ce qui concerne les joueurs, l'hypothèse fondamentale de la théorie des jeux est celle qui stipule que chacun cherche à maximiser ses gains, une hypothèse qui signifie la rationalité. Partant de cette définition générale et en adoptant divers critères de classement, on peut définir plusieurs classes de jeux.

2.3.1 Selon le modèle mathématique utilisé pour les décrire

On distingue :

Jeu sous forme normale ou stratégique

Un jeu sous forme normale est donné par le triplet :

$$J =< \mathcal{N}, \{X_i\}_{i\in\mathcal{N}}, \{f_i\}_{i\in\mathcal{N}} >, \tag{2.1}$$

où :

- $\mathcal{N}$=$\{1,\cdots,N\}$ est l'ensemble des joueurs.
- X_i : est l'ensemble des stratégies du joueur $i \in \mathcal{N}$.
- f_i : X=$X_1 \times \cdots \times X_N \longrightarrow \mathbb{R}$, est la fonction d'utilité du i^{eme} joueur, $i \in \mathcal{N}$.

Jeu sous forme extensive

Un jeu sous forme extensive décrit de manière précise les règles du déroulement du jeu : qui joue, quand, quels sont ses choix et quelle est son information sur le passé de la partie.

Lorsque les règles du jeu stipulent que les joueurs interviennent les uns après les autres, dans un ordre prècis et que le nombre d'actions parmi lesquelles leur choix s'exerce est fini, la représentation qui semble la plus appropriée consiste à tracer un arbre (appelé arbre de Kuhn).

La forme extensive d'un jeu spécifie les données suivantes [28] :

- Les joueurs concernés par le jeu.
- Les moments où chaque joueur aura à jouer.
- Les actions possibles de chaque joueur au moment de jouer.
- L'information dont dispose chaque joueur au moment où il joue.
- Les gains des joueurs pour chacune des combinaisons possibles des actions des joueurs.

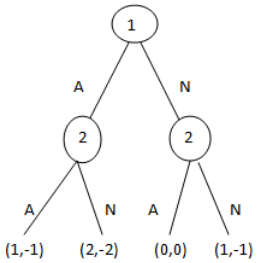

FIGURE 2.1 – Exemple d'un jeu sous forme extensive.

Jeu sous forme coalitionnelle

Un jeu sous forme coalitionnelle est très utilisé pour les jeux coopératifs. Cette représentation consiste à assigner à chaque coalition, l'ensemble des gains qu'elle peut garantir à ses membres.

Un jeu sous forme coalitionnelle est donné par le couple :

$$(\mathcal{N}, V) \tag{2.2}$$

où :

- $\mathcal{N} = \{1, \cdots N\}$ est l'ensemble des joueurs,
- $V : 2^N \longrightarrow \mathbb{R}$ est la fonction caractéristique,
- Pour tout sous-ensemble $S \subseteq \mathcal{N}$, $V(S)$ est le montant que les membres de S peuvent gagner en agissant collectivement.

2.3.2 Selon l'attitude des joueurs face à la coopération

On distingue deux classes principales de jeux : les jeux coopératifs et les jeux non coopératifs.

Jeu coopératif

Un jeu est dit coopératif lorsque les joueurs peuvent passer entre eux des accords qui les lient de manière contraignante avant le déroulement du jeu.
Dans les jeux coopératifs, les actions sont choisies par des coalitions.
Nous allons à présent définir quelques notions liées aux jeux coopératifs.

Définition 2.1

Une coalition est tout sous-ensemble de l'ensemble $\mathcal{N}$ des joueurs.
Une structure de coalitions est une partition notée $T = \{S_1, \cdots, S_L\}$ de l'ensemble $\mathcal{N}$ en coalitions telle que :
$S_l \subseteq \mathcal{N}$, $\forall l = 1, ..., L$.
• $\cup_{l=1}^{L} S_l = \mathcal{N}$.
• $S_l \cap S_j = \emptyset, \qquad \forall l, j \in \{1, ..., L\},\ l \neq j$.

Définition 2.2

Une issue d'un jeu sous forme coalitionnelle $(\mathcal{N}, V)$ est une paire (T, x),
où :
• T : est une structure de coalitions.
• $x = (x_1, \cdots, x_N)$ est un vecteur de paiements, qui distribue les valeurs de chaque coalition de T, tel que :
◦ $x_i \geq 0, \forall i \in \mathcal{N}$.
◦ $\sum_{i \in S} x_i = V(S), \qquad \forall S \in T$.

On distingue deux catégories de jeux :

✠ **Jeux à utilités transférables (UT) :** Les gains sont affectés à chaque coalition qui les divise entre ses membres.
Ces jeux sont aussi connus sous le nom de jeux à fonction de partition (JFP).

✠ **Jeux à utilités non transférables (UNT) :** Les décisions du groupe dépendent des gains qu'elles rapportent à chacun d'eux.

Jeu non coopératif

Un jeu non coopératif correspond à des situations dans lesquelles chaque joueur décide de ses actions individuellement sans consulter les autres joueurs.

2.3.3 Selon la nature de l'information

L'information dont dispose chaque joueur influe beaucoup sur la décision qu'il va prendre, et par conséquent, sur l'évolution du jeu. Il est donc naturel de classer les jeux selon l'information disponible aux joueurs au moment de la prise de décision.

Jeux à information complète / incomplète

Un jeu est dit à information complète, si chacun des joueurs connaît la structure du jeu, c'est-à-dire : l'ensemble des joueurs, les ensembles des stratégies de tous les joueurs, ainsi que leurs fonctions de gain. Chaque joueur sait également que tous les autres joueurs disposent de ces informations.

Le jeu est dit à information incomplète si, au moins, un des joueurs ne connaît pas entièrement la structure du jeu.

Jeux à information parfaite / imparfaite

Un jeu est dit à information parfaite si chacun des joueurs, au moment de choisir son action, a une connaissance parfaite de l'ensemble des décisions prises antérieurement par les autres joueurs. Un jeu est à information imparfaite si au moins un des joueurs ne connaît pas, à un moment du déroulement du jeu, ce qu'a joué un des autres joueurs.

2.3.4 Selon la manière dont les joueurs prennent leurs décisions

Jeux simultanés

On dit qu'un jeu est simultané (statique), si les joueurs décident de leurs actions simultanément.

Jeux séquentiels

On dit qu'un jeu est séquentiel, si les joueurs décident de leurs actions l'un après l'autre.

Remarque

Nous pouvons citer, comme exemple, le jeu de Stackelberg.

2.4 Concepts de solution

2.4.1 Équilibre de Nash

Définition 2.3

Une issue $x^* = (x_1^*, ..., x_N^*) \in X$ est dite équilibre de Nash du jeu sous forme normale (2.1) [13], [38], si aucun joueur $i \in \mathcal{N}$ n'a intérêt à dévier unilatéralement de sa stratégie x_i^* quand les autres joueurs continuent à jouer $x_j^*, j \in \mathcal{N}\backslash\{i\}$. Par conséquent, pour tout joueur $i \in \mathcal{N}$, nous devons avoir :

$$f_i(x_i^*, x_j^*) \geq f_i(x_i, x_j^*), \forall x_i \in X_i.$$

Une issue $x^* \in X$ est un équilibre de Nash strict si :

$$f_i(x_i^*, x_j^*) > f_i(x_i, x_j^*), \forall x_i \in X_i, \ \forall i \in \mathcal{N}$$

Il est possible de déterminer l'équilibre de Nash d'un jeu en utilisant les fonctions de meilleures réponses des joueurs.

2.4.2 Concept du α-noyau

Le α-noyau a été introduit par Aumann [3] en 1961. C'est un ensemble d'issues qui possèdent la propriété d'empêcher la formation des coalitions. Si une issue x est dans le α-noyau et si un certain nombre de joueurs envisagent de former une coalition et de dévier de x, alors le reste des joueurs possèdent au moins une stratégie qui va dissuader au moins un membre de la coalition envisagée d'y faire partie, car il ne pourra pas obtenir plus. Par conséquent, cette coalition ne se formera pas. De façon formelle, on a la définition suivante :

Définition 2.4 [20]

On appelle α-noyau du jeu (2.1) l'ensemble des issues $\overline{x} \in X$ vérifiant la propriété suivante :
pour toute coalition $S \subseteq \mathcal{N}$, $\forall x_S \in X_S$, $\exists y_{-S} \in X_{-S}$ telle que le système suivant :

$$f_i(x_S, y_{-S}) > f_i(\overline{x}), \ \ i \in S$$

n'est pas vérifié.

2.4.3 Concept du noyau

La notion du noyau d'un jeu coopératif a une longue histoire. L'idée de base a été formulée par Edgeworth (1881) dans son examen du commerce [12].

Considérons le jeu coopératif à utilité transférable (2.2). Le noyau du jeu (2.2) est constitué de toutes les allocations $x = (x_1, ..., x_N)$ satisfaisant les propriétés suivantes :

- rationalité individuelle : $x_i \geq V(i) \qquad \forall i \in \mathcal{N}$;
- rationalité collective : $\sum_{i\in\mathcal{N}} x_i = V(\mathcal{N})$;
- rationalité coalitionnelle : $\sum_{i\in S} x_i \geq V(S) \qquad \forall S \subseteq \mathcal{N}$.

2.4.4 Valeur de Shapley

La valeur de Shapley [21], [16] pour le jeu $(2, 2)$ est la règle qui assigne à chaque joueur $i \in \mathcal{N}$ un profit donné par la formule suivante :

$$\phi_i = \sum_{S\subseteq\mathcal{N}, i\in S} \frac{(|S|-1)! \times (|\mathcal{N}|-|S|)!}{|\mathcal{N}|!}[V(S) - V(S\backslash\{i\})],$$

où :
$|\mathcal{N}|$ désigne le cardinal de $\mathcal{N}$;
$|S|$ désigne le cardinal de la coalition S ;
$[V(S) - V(S\backslash\{i\})]$ est la contribution marginale du joueur i à la coalition S.

2.5 Jeux évolutionnaires

La théorie des jeux évolutionnaires, est une nouvelle classe de jeux, introduite par John Maynard Smith [34]. L'idée principale, est que ce n'est plus la rationalité de chaque individu qui le pousse à adapter son comportement aux stratégies de ses adversaires, par contre une évolution propre à l'ensemble de la population à laquelle il appartient.

• **Déroulement du jeu**

- Le jeu est joué plusieurs fois entre des individus possédant une rationalité limitée.
- Les joueurs sont tirés de manière aléatoire à partir d'une population qui est un ensemble d'individus qui coexistent dans le même environnement.

• **Les concepts fondamentaux de la théorie des jeux évolutionnaire**

1. Les stratégies Evolutionnairement Stable (ESS)
   Soit une population d'individus notée par ω, on tire d'une manière aléatoire deux individus (joueurs).
   Supposons qu'à l'état initial, l'ensemble d'individus constituant la population adopte tous une même stratégie notée α.
   Le gain d'un individu est noté par $f(\alpha, \alpha)$.

Supposons maintenant, qu'une proportion d'individus notée ξ, adoptent une stratégie mutante [1] notée β, tandis que le reste des individus de la population maintient la stratégie α. Alors l'espérance de gain d'un joueur jouant une stratégie α sera :

$$(1-\xi)f(\alpha,\alpha)+\xi f(\alpha,\beta)=f(\alpha,(1-\xi)\alpha+\xi\beta)$$

Par contre, l'espérance de gain d'un joueur jouant une stratégie β sera :

$$(1-\xi)f(\beta,\alpha)+\xi f(\beta,\beta)=f(\beta,(1-\xi)\alpha+\xi\beta)$$

La stratégie α sera gagnante face à la stratégie mutante β, si :

$$f(\alpha,(1-\xi)\alpha+\xi\beta)>f(\beta,(1-\xi)\alpha+\xi\beta) \tag{2.3}$$

La formule (2.3) fournit la définition d'une ESS.

2. Réplicateur dynamique
Développé par Taylor et Jonker (1978), il décrit un processus de sélection spécifiant comment une population est associée avec différentes stratégies pures dans un jeu qui évolue dans le temps.

2.6 Formation de coalitions

Il existe une littérature variée qui modélise des situations où les joueurs peuvent coopérer [29], cependant deux questions essentielles se posent aux joueurs :
✓ Quelles sont les coalitions qui vont se former et comment vont-elles se former ?
✓ Comment les gains seront répartis entre les coalitions ? Et à l'intérieur de la coalition, c'est-à-dire entre les joueurs de la même coalition ?
Les premiers travaux ont tenté de répondre à la deuxième question, en supposant une structure coalitionnelle déjà en place, comme une donnée exogène du modèle. Par la suite, D'aspermont [9] (1983), Hart et Kurz [17] [18] (1983 et 1984), Bloch [7] (1996), Yi et Shin [32] (1996, 1998), Ray et Vohra [37] (2001), Thoron [36] (2003) expliquent la formations de coalition par des données endogènes du modèle et définissent une classe particulière de jeux appelée jeu de formation de coalitions.

2.6.1 Jeux de formation de coalitions

Nous pouvons classer les jeux de formation de coalitions selon la manière dont les joueurs prennent leurs décisions en deux catégories [33] :

1. Une stratégie mutante est un changement de comportement au cours du temps par rapport au comportement initial.

Jeux simultanés :

•Jeu simple de formation de coalitions

D'Aspermont et al [9] proposent un jeu de formation de coalitions, où les stratégies de chaque joueur est d'annoncer soit "dans" ou bien "dehors". Les joueurs qui annoncent "dans" forment une coalition et ceux qui annoncent "dehors" restent en tant que joueurs indépendants.

Exemple :

Soit $\mathcal{N} = \{A, B, C, D, E\}$ l'ensemble des joueurs.

Les stratégies de chaque joueur :

- A ,B, C annoncent "dans".
- D,E annoncent "dehors".

  La structure de coalitions résultante est : $\{\{A, B, C\}, \{D\}, \{E\}\}$.

•Jeu ouvert d'adhésion

Dans ce jeu, nous disposons d'un ensemble d'adresses noté $A = \{a_1, a_2, ..., a_m\}$, (le nombre d'adresses distinctes doit être supérieur ou égal au nombre de joueurs). Chaque joueur annonce simultanément une adresse. Les joueurs qui annoncent la même adresse vont appartenir à une même coalition.

Exemple :

Considérons un jeu à quatre joueurs $\mathcal{N} = \{1, 2, 3, 4\}$, et $A = \{a_1, a_2, a_3, a_4, a_5\}$ un ensemble d'adresses.

La stratégie X_i du joueur i, $i \in \mathcal{N}$ est de choisir une adresse $a_j \in A$.

- $X_1 \longrightarrow a_1$
- $X_2 \longrightarrow a_1$
- $X_3 \longrightarrow a_3$
- $X_4 \longrightarrow a_5$

La structure de coalitions résultante est : {{1,2}, {3}, {4}}.

•Jeu Γ

Chaque joueur annonce simultanément une liste de joueurs (lui-même y compris) notée S avec qui il veut former une coalition, autrement dit une stratégie de chaque joueur i, $i \in \mathcal{N}$ se ramène à un choix d'un sous ensemble S de $\mathcal{N}$. L'ensemble X_i des stratégies d'un joueur i s'écrit : $X_i = \{S \subseteq \mathcal{N} : i \in S\}$.

Les coalitions qui ont été choisies par chacun de leurs membres seront formées, et les joueurs qui ont fait de mauvais choix se retrouveront seuls.

Formellement :

Considérons une issue $\sigma = (S_1, S_2, ..., S_N) \in \prod_{i \in \mathcal{N}} X_i$ du jeu Γ

Associons à chaque joueur $i \in \mathcal{N}$, l'ensemble T_i^σ défini par :

$$T_i^\sigma = \begin{cases} S_i & si \quad S_l = S_i \quad \forall l \in S_i \quad ; \\ \{i\} & sinon \quad . \end{cases}$$

Exemple

Soit $\mathcal{N}$ ={A,B,C,D,E,F} l'ensemble des joueurs

La stratégie $X_i = S_i$ de chaque joueur i, $i \in \mathcal{N}$:

A $\longrightarrow S_1$={A,B,C}

B $\longrightarrow S_2$={A,B,C}

C $\longrightarrow S_3$={A,B,C}

D $\longrightarrow S_4$={D,C,E}

E $\longrightarrow S_5$={E,D,F}

F $\longrightarrow S_6$={E,D,F}

σ=(S_1, S_2 ,S_3,S_4,S_5 ,S_6)

T_1^σ=T_2^σ=T_3^σ=S_1={A,B,C}

T_4^σ={D}

T_5^σ={E}

T_6^σ={F}

P={{A ,B,C} ,{D},{E},{F}} est la structure de coalitions résultante.

•Jeu Δ

La différence avec le jeu Γ réside dans le fait que si un joueur fait un mauvais choix des membres de sa coalition, en incluant dans sa liste des joueurs qui ne l'ont pas choisi, il ne se retrouvera pas seul, mais va plutôt former une coalition avec les membres de sa liste qui ont fait le même choix que lui. La structure coalitionnelle qui va résulter d'un profit de stratégies $\sigma = (S_1, S_2, ..., S_N)$ sera alors :

P^σ ={$T \subseteq N$:$i, j \in T \Longleftrightarrow S_i$=$S_j$}

Exemple (précédant)

T_1^σ=T_2^σ=T_3^σ=S_1={A,B,C}

T_4^σ={D}

T_5^σ=T_6^σ={E,F}

P={{A ,B,C} ,{D},{E,F}} est la structure de coalitions résultante.

Jeux séquentiels

•Jeu à horizon infini

Bloch [7] propose un jeu séquentiel de formation de coalitions, où il définit d'abord une règle d'ordre notée par ρ, qui est employée pour déterminer l'ordre des joueurs dans le jeu.
Le premier joueur, selon la règle ρ, commence le jeu en proposant la formation d'une coalition S_0 à laquelle il veut appartenir. Chaque membre éventuel répond à la proposition dans l'ordre déterminé par ρ. Si un des joueurs rejette la proposition, il doit faire une contre-offre et proposer une coalition S_1 à laquelle il veut appartenir. Si tous les membres acceptent, la coalition est formée. Tous les membres de S_0 se retirent alors du jeu, et le premier joueur dans N/S_0 recommence le jeu.
La figure suivante décrit le jeu avec trois joueurs.

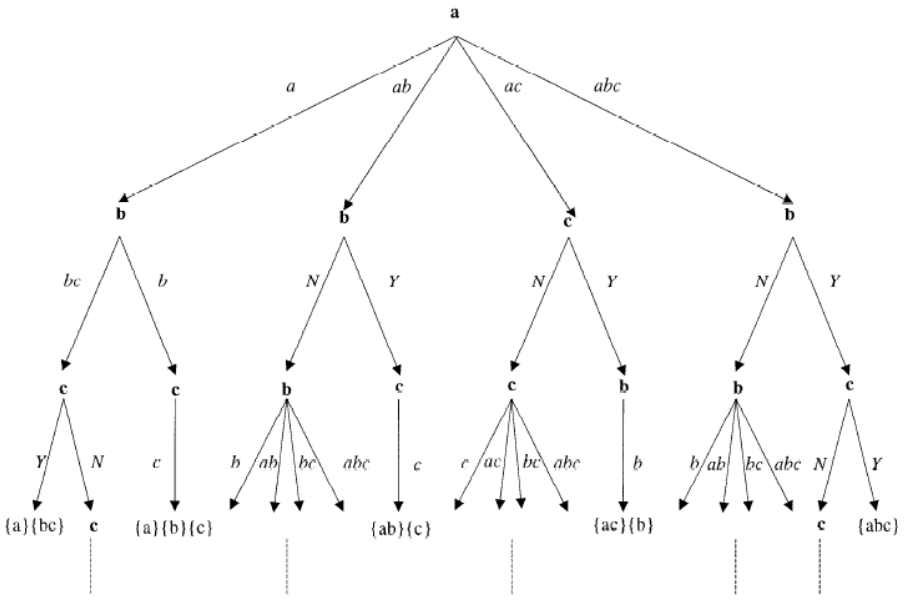

FIGURE 2.2 – Jeu à horizon infini.

2.6.2 Conditions de stabilité des coalitions

Il y a deux propriétés fondamentales que doit vérifier une structure de coalitions pour jouir de la stabilité [20], [27].

– **Stabilité intérieure :** une coalition est intérieurement stable, si aucun membre de la coalition n'a intérét à la quitter. Formellement, une coalition S est intérieurement stable, si aucun joueur $i \in S$ n'a intérêt à quitter individuellement S pour rejoindre la frange $\mathcal{N} \backslash S$ des joueurs restants.

Autrement dit, si

$$\forall i \in S, f_i(S) \geq f_i(S\backslash\{i\}),$$

où
$f_i(S)$ est le gain du joueur i en étant dans S,
$f_i(S\backslash\{i\})$ est le gain du joueur i en quittant la coalition S.

– **Stabilité extérieure :** une coalition est extérieurement stable, si aucun joueur en dehors de la coalition n'a intérêt à la rejoindre. Formellement, une coalition S est extérieurement stable, si aucun joueur $i \notin S$ n'a intérêt à rejoindre S.
Autrement dit, une coalition S est extérieurement stable, si

$$\forall i \notin S, f_i(S \cup i) < f_i(S),$$

où
$f_i(S)$ est le gain du joueur i en étant à l'extérieur de S ;
$f_i(S \cup i)$ est le gain du joueur i en rejoignant la coalition S.

Pour illustrer l'utilisation de ces conditions et pour prévoir les coalitions qui vont se former dans un jeu, nous allons étudier l'exemple de l'oligopole de Cournot :

Oligopole de cournot

Considérons un marché composé de trois firmes {1,2,3} produisant un même bien, chacune des firmes doit décider de la quantité à produire. La demande inverse du marché donne le prix de produit comme fonction de la quantité totale mise sur le marché par les trois firmes.
La fonction inverse de demande du marché est donné par :

$$P(Q) = \max(a - Q, 0) \qquad Q = q_1 + q_2 + q_3,$$

où q_j est la quantité produite par les trois firmes $j \in \{1,2,3\}$, a>0 désigne le seuil de saturation du marché, au-delà du quel le produit devient sans valeur sur le marché.

Version non coopérative du jeu

Supposons en premier lieu qu'aucune entente n'est possible entre les firmes, donc nous obtenons un jeu non coopératif :

$$< \mathcal{N}, \{X_j\}_{j\in\mathcal{N}}, \{f_j\}_{j\in\mathcal{N}} >,$$

où :
$\mathcal{N}$ est l'ensemble des joueurs qui sont les trois firmes $\mathcal{N}$=$\{1,2,3\}$;
X_j est l'ensemble des stratégies de la firme j, $X_j = [0, +\infty[$, $j \in \mathcal{N}$.
f_j la fonction de gain de la firme j, représente le bénéfice qu'elle réalisera de la vente de sa production.
Si le coût de production unitaire pour toutes les firmes est c, alors la fonction de gain de la firme j sera :

$$f_j(Q) = q_j[P(Q) - c].$$

On supposera que $c < a$. Pour trouver un équilibre de Nash pour ce jeu, on va construire les fonctions de réaction des trois firmes. La fonction de réaction R_j de la firme j définit, pour des niveaux de production donnés des deux firmes, la meilleure décision de production pour la firme j. Construisons la fonction R_1 :
soient q_2, q_3 les niveaux de production fixés par les firmes 2 et 3 respectivement.

Le prix du marché est alors :
$p(Q) = \max(a - Q, 0) = \max(a - (q_1 + q_2 + q_3), 0)$.
Le profit de la firme 1 sera alors :

$$f_1(q_1) = q_1(a - (q_1 + q_2 + q_3) - c) \qquad (2,4)$$

La maximisation de (2,4), par rapport à q_1, donne une meilleure réponse à la firme 1 qui est :

$$q_1 = \begin{cases} \frac{a-(q_2+q_3)-c}{2}, & \text{si} \quad a - (q_2 + q_3) - c \geqq 0\,; \\ 0, & \text{sinon.} \end{cases}$$

La fonction de réaction de la firme 1 est donnée par

$$R_1(q_2, q_3) = \begin{cases} \frac{a-(q_2+q_3)-c}{2}, & \text{si} \quad a - (q_2 + q_3) - c \geqq 0\,; \\ 0, & \text{sinon.} \end{cases}$$

Les fonctions de réactions des deux autres firmes seront données par :

$$R_2(q_1, q_3) = \begin{cases} \frac{a-(q_1+q_3)-c}{2}, & \text{si} \quad a - (q_1 + q_3) - c \geqq 0\,; \\ 0, & \text{sinon.} \end{cases}$$

$$R_3(q_1,q_2)=\begin{cases}\frac{a-(q_1+q_2)-c}{2}, & \text{si} \quad a-(q_1+q_2)-c\geqq 0\,;\\ 0, & \text{sinon.}\end{cases}$$

Nous pouvons à présent chercher les équilibres de Nash du jeu. En effet, un équilibre de Nash de ce jeu est une situation (q_1,q_2,q_3) vérifiant :

$$\begin{cases} q_1=R_1(q_2,q_3),\\ q_2=R_2(q_1,q_3),\\ q_3=R_1(q_1,q_2).\end{cases}$$

La résulution de ce système conduit à une solution unique :

$$q_1^*=q_2^*=q_3^*=\frac{a-c}{4}$$

Les profits à l'équilibre des trois firmes seront alors :

$$f_1^*=f_2^*=f_3^*=\frac{(a-c)^2}{16}$$

Version coopérative du jeu Supposons à présent que les firmes peuvent coordonner leurs stratégies pour améliorer leurs profits. On s'intéresse à déterminer les coalitions (cartels) qui vont se former et l'issue du jeu en terme de quantités produites par les firmes et les profits réalisés. Supposons que deux firmes : 1 et 2, se regroupent pour constituer un cartel. Elles se comporteront alors comme une seule firme qui a pour objectif de maximiser (f_1+f_2).

Les ensembles des stratégies des deux joueurs sont : $X_{1,2}=X_3=[0,+\infty[$. Leurs fonctions de gain sont respectivement (f_1+f_2) et f_3.

Les fonctions de réaction des deux joueurs (cartel) est donnée par :

$$R_{1,2}(q_3)=\begin{cases}\frac{a-q_3-c}{2}, & \text{si} \quad a-q_3-c\geqq 0\,;\\ 0, & \text{sinon.}\end{cases}$$

La fonction de réaction de la 3ème firme sera :

$$R_3(q_1,q_2)=\begin{cases}\frac{a-(q_1+q_2)-c}{2}, & \text{si} \quad a-(q_1+q_2)-c\geqq 0\,;\\ 0, & \text{sinon.}\end{cases}$$

La résolution de ce système donne :

$$q_1^*+q_2^*=\frac{a-c}{3}, \qquad q_3^*=\frac{a-c}{3}.$$

Donc

$$q_1^*=q_2^*=\frac{a-c}{6}, \qquad q_3^*=\frac{a-c}{3}.$$

Et les profits réalisés :

$$f_1^* = f_2^* = \frac{(a-c)^2}{18} \qquad f_3^* = \frac{(a-c)^2}{9}$$

On s'intéresse à présent au cartel formé par les trois firmes. Leur fonction de gain sera :

$$f(Q) = (f_1 + f_2 + f_3)$$

Donc

$$f(Q) = Q[a - Q - c]$$

Après maximisation de la fonction de gain, la quantité produite par chacune des firmes sera :

$$q_1^* = q_2^* = q_3^* = \frac{(a-c)}{6}$$

Le profit des trois firmes alors :

$$f_1^* = f_2^* = f_3^* = \frac{(a-c)^2}{12}.$$

Stabilité

- **Stabilité interne**

Soit : $i, j, k \in \{1, 2, 3\}$ et $i \neq j \neq k$

1. La grande coalition $\{i, j, k\}$ n'est pas stable intérieurement car,

$$f_i^*\{\{j, k\}, \{i\}\} > f_i^*\{i, j, k\}$$

2. Toutes les coalitions de taille 2 ne sont pas intérieurement stables puisque,

$$f_i^*\{\{i\}, \{j\}, \{k\}\} > f_i^*\{\{i, j\}, \{k\}\}$$

– **Stabilité externe**

1. La grande coalition$\{i, j, k\}$ est stable extérieurement car, il n'existe aucun joueur qui puisse la rejoindre.
2. Toutes les coalitions de taille 2 sont extérieurement stables puisque,

$$f_k^*\{\{i, j\}, \{k\}\} > f_k^*\{i, j, k\}$$

3. Toutes les coalitions de taille 1 sont stables extérieurement puisque,

$$f_k^*\{\{i\}, \{j\}, \{k\}\} > f_k^*\{\{i, k\}, \{j\}\}$$

2.7 Conclusion

Dans ce chapitre, nous avons présenté les notions fondamentales de la théorie des jeux ainsi quelques concepts de solution et nous avons présenté quelques jeux de formation de coalitions. Dans le chapitre suivant, nous allons présenter quelques travaux modélisant le problème de sécurité des réseaux Ad-hoc via la théorie des jeux.

Chapitre 3

Etat de l'art

3.1 Introduction

A l'heure actuelle, le besoin en matière de sécurité est de plus en plus croissant, vue l'émergence de l'outil informatique qui est devenu accessible à un prix abordable, la simplicité d'utilisation des logiciels et l'informatisation des entreprises qui nécessite un réseau sécurisé pour le transfert des données.
Dans ce présent chapitre, nous allons présenter quelques travaux sur l'insertion de la théorie des jeux dans les problèmes de sécurité des réseaux sans fils. Une attention particulière sera accordée aux jeux de formation de coalitions et leurs applications.

3.2 Jeux évolutionnaires dans la sécurité des réseaux sans fils

Il existe dans la littérature diverses méthodes telles que la cryptographie et la détection, développées dans le but de sécuriser les réseaux sans fil. Dans [15], les auteurs proposent une nouvelle approche, qui diffère des méthodes traditionnelles, consistant en l'étude de la sécurité de la couche physique. L'idée principale est de maximiser le taux d'information fiable d'une source à une destination, tout en maintenant les oreilles indiscrètes ignorantes des données à transmettre.

Un jeu non coopératif évolutionnaire de taux de secret est formulé pour prendre en considération l'antagonisme entre la maximisation du taux de secret d'un nœud et la minimisation de la puissance consommée pour la transmission des données.

3.2.1 Le modèle

Le réseau est divisé en clusters, où chaque cluster est composé des nœuds et d'un coordinateur appelé cluster-head. La transmission de données se fait comme suit :

• Dans le premier intervalle de temps (slot), les données capturées par des nœuds appartenant à un même cluster sont transmises au coordinateur.
• Durant le deuxième intervalle de temps, le coordinateur réunit les données et les envoie à la station de base.
Le papier [15] s'est focalisé sur le taux de secret des transmissions entre les nœuds et le coordinateur durant le premier intervalle de temps.

3.2.2 Le jeu du taux de secret

- **Joueurs**

  Le jeu se déroule entre les nœuds appartenant à un réseau de capteurs sans fil WSN [1] dont l'ensemble des nœuds est noté $\mathcal{N} = \{1, \cdots, N\}$. Les compétitions se font par paire de nœuds.

- **Stratégies**

  Chaque nœud $i \in \mathcal{N}$ a le choix du niveau de puissance de transmission qui peut prendre sa valeur dans l'ensemble $\mathcal{P}_i = \{P_{i1}, P_{i2}, ..., P_{iL}\}$,
  où :
  L : est le nombre de niveaux de puissance.
  $\mathcal{P} = \prod_{i=1}^{N} \mathcal{P}_i$: ensemble des profils de stratégies.

- **Gains**

  Le gain d'un nœud $i \in \mathcal{N}$ qui choisit un niveau de puissance $P_i \in \mathcal{P}_i$ quand son rival choisit un niveau de puissance $P_{\bar{i}} \in \mathcal{P}_{\bar{i}}$ est donné par la fonction suivante :

  $$\mu(P_i, P_{\bar{i}}) = C(P_i) - \alpha P_i, \tag{3.1}$$

  où :

  $$C(P_i) = (C_h^i - \max_{k \in \mathcal{K}} C_k^i)^+, \quad (a)^+ = \max\{a, 0\}$$

  et $C(P_i)$ représente le taux de secret entre le nœud i utilisant le niveau de puissance P_i et son coordinateur $h \in \mathcal{H}$.
  $\mathcal{H} = \{1, \cdots, He\}$: représente l'ensemble des coordinateurs.
  h : représente un coordinateur.
  $\mathcal{K} = \{1, \cdots, K\}$: représente l'ensemble d'oreilles indiscrètes capables d'écouter les données envoyées par un nœud $i \in \mathcal{N}$.
  k : représente une oreille indiscrète.

1. Wireless Sensor Networks.

C_h^i : représente la capacité du canal entre le nœud i et son coordinateur h.
C_k^i : représente la capacité du canal entre le nœud i et l'oreille indiscrète $k \in \mathcal{K}$.

3.2.3 Concept de solution

Le concept de solution utilisé est la Stratégie Evolutionnairement Stable (ESS). Les auteurs ont proposé un algorithme qui décrit le processus itératif qui montre comment les nœuds choisissent de manière adaptative leurs stratégies de niveau de puissance. Ce processus continue jusqu'à ce que l'ESS du jeu de taux de secret soit réalisé. Tous les nœuds trouvent ainsi une solution satisfaisante et aucun nœud ne peut bénéficier de commuter sa stratégie courante de niveau de puissance pendant que les autres maintiennent leurs stratégies inchangées.

Le modèle proposé dans [15] pourrait être étendu en prenant en compte la transmission de données entre le coordinateur et la station de base.

3.3 Une approche coopérative pour analyser des intrusions dans les réseaux Ad-hoc

Un réseau Ad-hoc est susceptible à plusieurs attaques par des nœuds malicieux appelés (intrus). Un intrus peut détruire la communication en annonçant une information fausse de cheminement et en inondant d'autres nœuds avec des cheminements inutiles. Les techniques de défense, comme le chiffrage, ne sont plus suffisantes pour protéger le MANET, il est donc nécessaire d'utiliser un système qui détecte les intrus. La théorie des jeux coopératifs est employée pour analyser la contribution de chaque nœud pour la détection d'une intrusion.

Dans cette section, nous allons présenter une étude [25] proposant un système de détection d'intrusion (IDS) qui se base sur la théorie des jeux coopératifs pour réduire les faux positifs.

3.3.1 Le modèle

Dans [25], un réseau Ad-hoc est modélisé comme un graphe G non orienté $(\mathcal{N}, E)$ où $\mathcal{N} = \{1, \cdots, L\}$ est l'ensemble des nœuds mobiles. Nous décrivons le modèle comme un système distribué, coopératif de détection d'intrusions, où chaque nœud du réseau participe à la détection et à la réaction aux intrusions. Chaque nœud active son IDS pour effectuer localement la collecte des données et la détection d'anomalies. Les auteurs distinguent deux types d'attaques :

- l'empoisonnement de cachette qui peut compromettre l'information dans la table de cheminement en modifiant son contenu ou en supprimant l'information.
- l'inondation malveillante qui consiste à inonder le réseau entier ou quelques nœuds avec une grande masse de donneés conduisant à la consommation des ressources des nœuds victimes d'attaques.

La coopération entre les nœuds mobiles est alors nécessaire pour détecter les intrusions avec un taux faible de faux positifs, chaque nœud $i \in \mathcal{N}$ peut détecter les deux types d'intrusion. Pour cela, on définit une fonction O qui détermine si un nœud a détecté une intrusion :

$$O : \mathcal{N} \to C \times M$$
$$i \in \mathcal{N} \to O(i) = (C_i, M_i)$$

où :
$C = \{0, 1\}$ est l'ensemble des valeurs concernant l'empoisonnement de cachette.
$M = \{0, 1\}$ est l'ensemble des valeurs concernant l'inondation malveillante.
Exemple
si $O(i)$=(1,0), signifie qu'un nœud $i \in \mathcal{N}$ a détecté une attaque d'empoisonnement de cachette.
si $O(i)$=(0,1), signifie qu'un nœud $i \in \mathcal{N}$ a détecté une attaque d'inondation malveilante.

3.3.2 Classes de sécurité de l'IDS

Les fausses alarmes constituent un problème majeur auquel font face les IDS réduisant d'une manière significative leur efficacité. L'objectif principal du papier [25] est d'améliorer l'efficacité du système de détection des intrusions en réduisant le nombre de faux positifs. Pour cela, on définit une fonction f qui calcule la sévérité d'une intrusion :

$$f(.) : \mathcal{N} \to \mathbb{R},$$
$$\forall i \in \mathcal{N}, \qquad f(i) = C_i \frac{NFP(i)}{NR_{\_ack(i)}} \; + \; M_i \frac{NRP(i)}{ENRP(i)}, \tag{3.2}$$

où :

$NFP(i)$ **:** le nombre de paquets expédiés, par le nœud $i \in \mathcal{N}$.

$NR_{\_ack(i)}$ **:** le nombre de reconnaissances reçues par le nœud $i \in \mathcal{N}$.

$NRP(i)$ **:** le nombre de paquets reçus par le nœud $i \in \mathcal{N}$.

$ENRP(i)$ **:** le nombre prévu de paquets que le nœud $i \in \mathcal{N}$ devait reçevoir.

Pour diminuer les faux positifs, on définit un ensemble de classes de sécurité $CL = \{cl_1, ..., cl_k\}$. Ceci permettra de répondre à une intrusion selon la classe à laquelle elle appartiendrait, dépendant de sa sévérité.
On définit $SE = \{se_1, ..., se_{k-1}\}$ les seuils des différentes classes de sécurité.
Un nœud qui suspecte une intrusion calcule sa sévérité à l'aide de la fonction suivante :

$$F(\mathcal{N}) = \sum_{i \in \mathcal{N}} r_i \times f(i). \tag{3.3}$$

où : r_i est la réputation du nœud $i \in \mathcal{N}$.

3.3.3 Le jeu du seuil de sécurité [25]

On considère chaque nœud comme un joueur, une coalition est un sous-ensemble de nœuds, où chaque nœud rapporte au moins un type d'intrusion. Ainsi, chaque nœud dans une coalition S signal un risque dans le MANET. On utilise la valeur de Shapley pour calculer la contribution marginale de chaque nœud dans une coalition.

$$\phi_i(S) = \frac{1}{\delta!} \sum_{\pi \in \Pi_S} F(P_\pi^i \cup \{i\}) - F(P_\pi^i), \tag{3.4}$$

où :
Π_S est l'ensemble des permutations du nœud i dans S,
P_π^i ensemble des nœuds se situant avant le nœud i dans la permutation $\Pi \in \Pi_S$,
δ est le nombre de joueurs dans S,
$F(P_\pi^i \cup \{i\})$ la fonction incluant tous les nœuds dans la permutation se situant avant le nœud i, incluant i.
$F(P_\pi^i)$ la fonction incluant tous les nœuds dans la permutation se situant avant le nœud i, excluant i.

Comme $F(P_\pi^i \cup \{i\}) = \sum_{j \in P_\pi^i \cup \{i\}} r_j \times f(j)$ et $F(P_\pi^i) = \sum_{j \in P_\pi^i} r_j \times f(j)$ alors :

$$\phi_i(S) = \frac{1}{\delta!} \sum_{\pi \in \Pi_S} F(\{i\}), \tag{3.5}$$

donc :

$$\phi_i(S) = F(\{i\}). \tag{3.6}$$

Maintenant, pour calculer la contribution marginale (valeur de Shapley) du nœud $i \in \mathcal{N}$ dans le MANET, nous devrions prendre la moyenne de cette valeur pour les coalitions

possibles, qui est :

$$\phi_i = \frac{1}{\gamma} \sum_{S \subseteq \mathcal{N}, i \in S} F(\{i\}) \tag{3.7}$$

où : γ est le nombre de coalitions possibles dans le MANET.

Les coalitions ayant suffisamment de puissance pour imposer collectivement une décision sont appelés coalitions gagnantes, une coalition est dite gagnante, si sa valeur peut changer le seuil d'une classe de sécurité se_i. Si la valeur d'une coalition est égale à 1, alors elle est gagnante, sinon elle n'est pas gagnante. Ainsi, l'effet du nœud i sur la classe de sécurité cl_i est $\frac{1}{\gamma}|S'|$,
où :
S' est l'ensemble des coalitions gagnantes, i.e

$$\sum_{i \in S'} F(\{S'\}) \geq se_i. \tag{3.8}$$

où :se_i représente le seuil d'une classe de sécurité.

La valeur de Shapley d'un nœud i mesure la contribution relative pour un seuil donné se_i. Par conséquent, on peut ajuster les valeurs des seuils à l'aide des données statistiques afin de réduire les faux positifs. A chaque classe de sécurité correspondrait une réaction spécifique à une intrusion, ceci illustre l'importance de l'analyse de la contribution relative d'un nœud pour décides de la classe de sécurité.

Dans cette section une étude est faite sur la détection d'intrusion afin d'affecté chaque types d'intrusion à sa classe de sécurité. Cette étude est faite à l'aide de la théorie des jeux coopératifs, où les nœuds portant un type d'intrusion coopèrent entre eux en formant des coalitions gagnantes pour influencer sur les classes de sécurité afin de diminuer les faux positifs.

3.4 Un jeu de coalitions pour la sécurité des réseaux sans fils

Il existe de nombreux travaux modélisant le problème de sécurité des réseaux Ad-hoc sous forme d'un jeu coopératif, où les nœuds constituant le réseau forment des coalitions afin de réaliser des objectifs tels que l'identification des nœuds malicieux.
Avant de présenter le modèle de formation de coalitions établi dans [19], nous allons définir quelques notions :

- **Source :** désigne un nœud émetteur qui est à l'origine des paquets de données.
- **Destination :** désigne un nœud récepteur auquel les paquets de données sont destinés.
- **La fiabilité d'un chemin :** est une métrique pour sélectionner une route vers une destination, elle représente une évaluation du chemin.
- **La fidélité d'un chemin :** la fidélité d'un chemin (i,j) est la probabilité qu'un nœud i veut communiquer avec le nœud j.

3.4.1 Modélisation

Les auteurs dans [19] modélisent l'interaction entre les nœuds d'un réseau Ad-hoc par un jeu coalitionnel à utilité transférable, dont les composantes sont :

- **Les joueurs**

  Le jeu se déroule entre les nœuds du réseau.
  Soit $\mathcal{N} = \{1, 2, \cdots, N\}$ l'ensemble de nœuds.

- **La fonction caractéristique**

  V est la fonction caractéristique qui associe à chaque sous-ensemble S, $S \subseteq \mathcal{N}$ un nombre réel $V(S)$ donné par :

$$V(S) = \begin{cases} 0, & \text{si } |S| < 2\,; \\ \frac{1}{\Delta t} \displaystyle\sum_{(a,b)\in SD, a,b\in S} Q_{ab} \cdot \max_{k\in P_{ab}(S)} t(k), & \text{sinon}\,; \end{cases}$$

  où

$$t(k) = \prod_{(i,j)\in k} \frac{P_{ij}}{D_{ij}^2}$$

  Δt : est un intervalle de temps.
  $SD = \{(a,b)/(a,b)$ est une paire de source-destination$\}$.
  Q_{ab} : est le nombre de paquets de données transmis entre les deux nœuds a et b.
  $P_{ab}(S)$: est l'ensemble des chemins à l'intérieur de la coalition S reliant le nœud a au nœud b.
  $t(k)$: la fiabilité du chemin k.

P_{ij} : la fidélité du chemin (i,j).
D_{ij} : la distance entre le nœud i et j.

Le schéma ci-dessous est un exemple de coalition marqué par les paramètres de la fonction caractéristique.

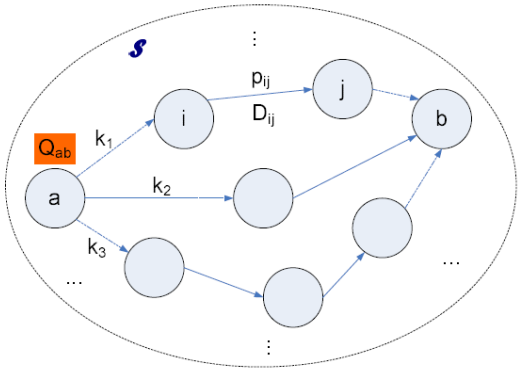

FIGURE 3.1 – La coalition S avec les paramètres de la fonction caractéristique.

Dans chaque coalition, une procédure de découverte du chemin est exécutée entre chaque paire de nœuds (source, destination) et pour chaque chemin possible k entre la source et la destination, il y aura une évaluation de fiabilité $t(k)$. La valeur maximale de $t(k)$ illustre le meilleur service que la coalition peut garantir à la paire (source, destination).
La fidélité du chemin entre le nœud i et le nœud j est obtenue de deux façons :
• **Expérience directe :** le rapport entre le nombre de transmissions réussies sur le nombre total de transmissions.
• **Recommandation indirecte :** Tous les voisins de i donnent leurs opinions à propos de i et j, puis le nœud i combine les avis obtenus et les multiplie par sa propre évaluation à ses voisins, c'est-à-dire que le nœud i donne aussi son avis à propos de ses voisins.

3.4.2 Description du modèle de formation de coalitions

Dans [19], les auteurs définissent un ensemble de règles de jeu, formant un mécanisme menaçant par lequel les nœuds sont incités à coopérer, et ceux qui ne joignent aucune coalition sont susceptibles d'être des nœuds malveillants.
Règles de jeu :

- un nœud joindra une coalition seulement s'il peut obtenir plus de part de profit qu'en restant seul ;
- un nœud déviera de la coalition courante et joint une autre coalition, si cette dernière lui procure un gain meilleur ;

- une coalition refusera d'admettre un nœud, si ce dernier ne peut pas augmenter le profit de la coalition ;
- une coalition exclura un nœud, si ce dernier endommage le profit de la coalition ;
- des nœuds qui finalement n'ont joint aucune coalition seront niés par le réseau.

Le partage de gain à l'intérieur de chaque coalition se fait à l'aide de *la valeur de Shapley*. Un algorithme de formation de coalitions intégrant un protocole de cheminement est établi dans [19]. En utilisant cet algorithme, la taille de la coalition continue à croître jusqu'à ce que la grande coalition est atteinte ou bien tous les mauvais nœuds sont identifiés.

3.5 Jeu coalitionnel et réseaux des agents autonomes

L'article [6] se focalise sur l'avantage de la collaboration des nœuds dans un réseau sans fil afin d'accomplir des objectifs que les nœuds ne peuvent pas réaliser en agissant individuellement ou d'accomplir de meilleurs buts en collaborant, mais la collaboration exige des coûts : par exemple pour transmettre des paquets de données entre un nœud source et un nœud destination. La décision d'expédier ou ne pas expédier les paquets est liée à des contraintes telles que l'énergie. Toutefois un nœud i qui active une liaison avec un de ses voisins, gagnera en ayant accès aux utilisateurs avec lesquels son voisin a activé ses liens. La décision d'activer des liens se base sur le concept de confiance.
Ce conflit a conduit à modéliser l'interaction entre les nœuds du réseau par un jeu coalitionnel à deux étapes :

- Dans la première étape du jeu, les nœuds du réseau (joueurs) jouent par paires et décident de former ou de casser un lien entre eux, ce jeu est répété jusqu'à ce qu'aucun lien n'est ajouté ou supprimé. Dans ce cas, on dit que le réseau a atteint un état stable (les coalitions sont formées).
- Dans la seconde étape, les nœuds appartenant à une même coalition essayent de maximiser leurs profits.

En procédant ainsi, on pourra déterminer des chemins sécurisés basés sur la fidélité des nœuds afin de garantir la sécurité du réseau.

3.6 Conclusion

Ce chapitre a été consacré à une synthèse de la littérature existante sur l'application de la théorie des jeux pour les problèmes de sécurité informatique. Nous avons présenté une application de la théorie des jeux évolutionnaires pour la sécurité des réseaux, et nous avons aussi présenté quelques travaux sur les jeux de formation de coalitions.
Le prochain chapitre sera dédié à la modélisation du problème de sécurité des réseaux Ad-hoc par les jeux coalitionnels.

Chapitre 4

Algorithme de formation de coalitions

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.
Les anciennes techniques de défense ne sont plus à la hauteur, ce qui a poussé des chercheurs à faire des études pour améliorer la sécurité de la couche physique.
Les travaux de Walid Saad et al, [30], [31] (2009, 2010), Lun et al [11](2010), Jingchao [8] (2011), Doaa [10] (2015) visent à augmenter le taux de secret et la quantité de données fiables transmises.

Dans ce chapitre, nous allons présenter une étude [31] qui vise à renforcer la sécurité des réseaux Ad-hoc via la théorie des jeux coopératifs, puis nous allons établir un algorithme de formation de coalitions, et pour finir nous allons interpréter les résultats de cet algorithme pour plusieurs instances afin de tirer un maximum d'informations sur les caractéristiques des structures de coalitions résultantes.

4.2 Modèlisation

Considérons un réseau ayant N émetteurs (par exemple des utilisateurs mobiles) envoyant des données à M récepteurs en présence de K oreilles indiscrètes (espions). On définit $\mathcal{N} = \{1, ..., N\}$, $\mathcal{M} = \{1, ..., M\}$ *et* $\mathcal{K} = \{1, ..., K\}$ comme ensemble des utilisateurs, destinations et d'oreilles indiscrètes respectivement.
Le gain du canal entre un émetteur $i \in \mathcal{N}$ et une destination $m_i \in \mathcal{M}$ est notée par h_{i,m_i}, défini par :

$$h_{i,m_i} = d_{i,m_i}^{-\frac{\mu}{2}} e^{K\theta_{i,m_i}}, \tag{4.1}$$

où :
• m_i : désigne la déstination d'un émetteur i.

• d_{i,m_i} : représente la distance entre l'émetteur $i \in \mathcal{N}$ et le récepteur $m_i \in \mathcal{M}$.
• K : représente le nombre d'espions.
• μ : est un paramètre lié à l'environnement.
• θ_{i,m_i} : est un paramètre généré selon la loi uniforme sur $[0, 2\pi)$ pour chaque émetteur i et sa destination m_i.

On note par $g_{i,k}$ le gain du canal entre l'émetteur $i \in \mathcal{N}$ et un espion $k \in \mathcal{K}$, qui se calcule de la même manière que l'équation (4.1).
Nous considérons que tous les émetteurs sont informés de la présence des espions. Lors de la transmission des informations d'un émetteur $i \in \mathcal{N}$ à une destination m_i, le canal peut être surpris par des espions qui réduisent le taux (capacité) de l'information secrète envoyée. On définit la capacité d'information fiable (secrète) transmise de l'émetteur $i \in \mathcal{N}$ à sa destination $m_i \in \mathcal{M}$ par la formule :

$$C_{i,m_i} = (C^d_{i,m_i} - \max_{1 \leq k \leq \mathcal{K}} C^e_{i,k})^+, \qquad (4.2)$$

où :
• C^d_{i,m_i} : représente la capacité d'information que l'émetteur i peut transmettre à sa destination m_i.
• $C^e_{i,k}$: représente la perte de taux de secret pour l'émetteur i causée par l'espion k.
• $a^+ = max\{a, 0\}$.

Pour améliorer le taux de secret et augmenter la quantité de données fiables, les nœuds (émetteurs) peuvent collaborer en formant des coalitions S. Une fois la coalition S est formée, chaque nœud de S peut coopérer avec ses partenaires dans S en divisant son slot en deux intervalles de temps :

- Dans le premier intervalle de temps, le nœud i annonce ses données aux autres membres de la coalition S.
- Dans le deuxième intervalle de temps, les membres de la coalition S exécutent la technique de beamforming [1]. Ainsi, tous les membres de S transmettent les informations du nœud i par le relais [2] à sa destination m_i.

Dans la phase d'échange d'information les membres de la coalition utilisent des protocoles avant d'exécuter la technique du Beamforming, parmi ces protocoles on cite :

1. Le beamforming, aussi appelé filtrage spatial ou formation de faisceaux, est une technique de traitement de signal utilisée dans les réseaux pour la transmission ou la réception directionnelle de signaux.
2. Dispositif pour retransmettre un signal et l'amplifier.

• Le protocole (Amplify and Forward) noté AF : dans ce protocole le signal que les membres de la coalition reçoivent sera expédié tel qu'il est à sa destination.

• Le protocole (Decode and Forward) noté DF : ce protocole exige plus de traitement car le signal reçu par les membres de la coalition sera décodé pour enlever le bruit puis le recoder avant de l'expédier à sa déstination.

Dans la suite de notre travail, nous allons utiliser le protocole DF.

Le but d'une approche coopérative est d'annuler le signal aux espions, c-à-d imposer $C^e_{i,k} = 0, \forall\, k \in \mathcal{K}$, par conséquent améliorer le taux de secret.

La figure ci-dessous illustre ce modèle pour $N = 9$ émetteurs, $M = 2$ destinations et $K = 2$ oreilles indiscrètes.

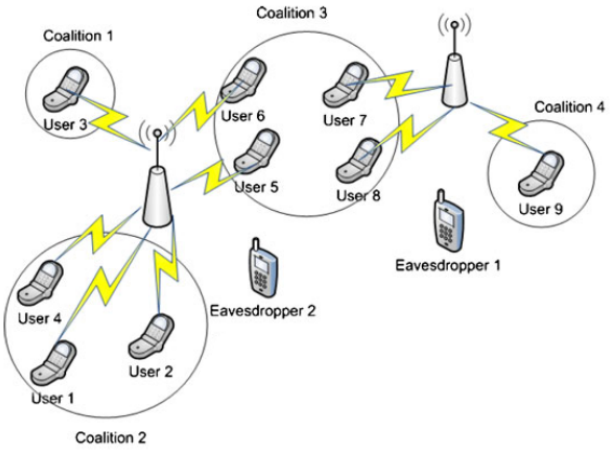

FIGURE 4.1 – Exemple du modèle.

A présent, nous allons définir $\tilde{P}$ la puissance de transmission d'information par tranche de temps. Dans l'approche non coopérative, l'émetteur $i \in \mathcal{N}$ utilise toute sa puissance $\tilde{P}$ pour transmettre des données à une destination $m_i \in \mathcal{M}$. Par contre dans l'approche coopérative, chaque émetteur $i \in S$ d'une coalition S partage sa puissance en deux parties. Une partie $\overline{P}_{i,\hat{i}}$ est utilisée lors de la première étape qui est la phase d'échange d'information, sa valeur est donnée par la relation :

$$\overline{P}_{i,\hat{i}} = \frac{\nu_0.\sigma^2}{|q_{i,\hat{i}}|^2}, \qquad (4.3)$$

où :
• $q_{i,\hat{i}}$: est le gain de canal entre l'utilisateur i et $\hat{i}$, calculé en utilisant la formule (4.1)
• σ^2 : est la variance de bruit.
• ν_0 : est un rapport signal bruit (SNR).

La relation (4,3) peut être interpréter comme suit : l'émetteur $i \in S$ annonce ses informations à tous les membres de sa coalition. Pour cela, il suffit qu'il envoie ses données à un émetteur $\hat{i} \in S\backslash\{i\}$ le plus loin de lui. De ce fait, tous les émetteurs appartenant à la coalition S reçoivent les informations. Tandis que la partie restante, notée P_i^s, est utilisée pour transmettre ses données à la destination m_i, qui est caractérisée par la relation :

$$P_i^s = (\widetilde{P} - \overline{P}_{i,\hat{i}})^+. \tag{4.4}$$

Une fois la coalition S est formée, ses membres peuvent annuler complètement le signal aux espions, par conséquent, augmenter le taux de secret. Pour cela, on définit :
$h_S = [h_{i_1,m_1}, ..., h_{i_{|s|},m_{|s|}}]^H$, $g_S^k = [g_{i_1,k}, ..., g_{i_{|s|},k}]^H$ et $w_S = [w_{i_1}, ..., w_{i_{|s|}}]^H$, qui représentent respectivement le canal de "utilisateur-destination", canal "utilisateur-espion k" et le poids de signal qui maximise le taux de secret,
où :
• H désigne la transposé du conjugué, c-à-d si les éléments de la matrice sont des réels on fait la transposé seulement, par contre si les éléments de la matrice sont des nombres complexes on effectue la transposé et on modifie ses éléments en multipliant la partie imaginaire par (-1).
En annulant le signal aux oreilles indiscrètes grâce au protocole DF, le taux de secret réalisé par l'émetteur $i \in S$ est :

$$C_{i,m_i}^{S,DF} = \frac{1}{2}\log_2(1 + \frac{(w_S)^H R_S w_S}{\sigma^2}), \tag{4.5}$$

où :
• $R_S = h_S.h_S^H$ est une matrice carrée $|S| \times |S|$.
• Le vecteur poids w_S se calcule par la formule [30] :

$$w_S = \beta_i^S G_S^H (G_S.G_S^H)^{-1} e, \tag{4.6}$$

où :
◦ $G_S = [h_s, g_S^1, ..., g_S^K]^H$ est une matrice $(K+1) \times |S|$.

◦ $\beta_i^S = \sqrt{\frac{P_i^S}{e^H (G_S.G_S^H)^{-1} e}}$.
◦ $e = [1, 0_{1\times K}]^H$ est un vecteur $(K+1) \times 1$.

• Le facteur $\frac{1}{2}$ explique le fait que la moitié de la puissance est réservée pour l'échange d'information.

4.2.1 Modélisation de la sécurité de la couche physique sous forme d'un jeu coalitionnel

Le problème de sécurité de la couche physique peut être modélisé par un jeu coalitionnel $(\mathcal{N}, V)$ à utilité non transférable, dont les composantes sont :

- **Les joueurs**

  Le jeu se déroule entre les nœuds émetteurs du réseau.

  Soit $\mathcal{N} = \{1, 2, \cdots, N\}$ l'ensemble des nœuds émetteurs.

- **La fonction caractéristique**

  V est la fonction caractéristique qui associe à chaque sous-ensemble S, $S \subseteq \mathcal{N}$, un vecteur de $\mathbb{R}^{|S|}$, dont chaque élément noté $V_{i_j}(S)$ représente le gain du joueur $i_j \in S$ pendant sa tranche de temps.

Ainsi, pour une coalition $S = \{i_1, \cdots, i_{|S|}\}$, on définit le vecteur profit $V(S)$ par :

$$V(S) = (V_{i_1}(S), \cdots, V_{i_{|S|}}(S)), \tag{4.7}$$

où :

$$V_{i_j}(S) = \begin{cases} (C^S_{i_j,m_{i_j}} - C_{i_j}(S))^+, & \text{si} \quad P^S_{i_j} > 0\,; \qquad \forall j = 1, ..., |S| \\ -\infty \qquad\qquad\quad , & \text{sinon.} \end{cases}$$

- $C^S_{i_j,m_{i_j}}$ représente le gain en terme de taux de secret de l'utilisateur $i_j \in S$ calculé avec la formule (4.5).
- $C_{i_j}(S)$: est une fonction qui calcule la perte pour l'utilisateur $i_j \in S$ en terme de taux de secret.

Pendant l'échange d'information, les espions peuvent surprendre la transmission et causer une perte de taux de secret. Cette dernière est mesurée par la relation :

$$\hat{C}^e_{i_j,k} = \frac{1}{2}\log(1 + \frac{\overline{p}_{i_j,\hat{i_j}}.|g_{i_j,k}|^2}{\sigma^2}). \tag{4.8}$$

• La fonction $C_{i_j}(S)$ est définie par la relation :

$$C_{i_j}(S) = \max_{k \in \mathcal{K}} \hat{C}^e_{i_j,k}, \qquad j = 1, ..., |S|. \tag{4.9}$$

Remarque : Pour le jeu coalitionel $(\mathcal{N}, V)$ proposé, la taille de n'importe quelle coalition $S \subseteq N$ qui se formera doit satisfaire la contrainte $|S| > K$, cela veut dire, pour annuler le signal aux espions c-à-d $C^e_{i_j,k} = 0$, chaque coalition qui doit se former doit au moins avoir $(K+1)$ joueurs, sinon aucun vecteur w ne peut convenir pour maximiser le taux de secret.

4.3 Algorithme de formation de coalitions

Dans cette section, nous allons présenter un algorithme de formation de coalitions, dans le cadre des réseaux Ad-hoc afin d'améliorer le taux de secret.

Algorithme

Phase 0 : Initialisation

A l'état initiale, le réseau est partitionné comme suit : $T = \{\{1\}, \{2\}, ..., \{N\}\}$, où N désigne le nombre de nœuds émetteurs.

Phase 1 : Découverte de voisins

Chaque nœud examine son environnement afin de trouver d'autres partenaires pour coopérer, et former des ensembles S tels que T=$\{S_1$,..., $S_L\}$.

Phase 2 : Formation de coalitions

Cette phase est constituée de 4 étapes :

- Etape 1 :
  On partitionne l'ensemble S_l de cardinalité $|S_l| = m$ en une structure de coalitions $\Pi_0 = \{\{i_1\}, ..., \{i_m\}\}$.
- Etape 2 :
  Etant donnée la structure de coalitions courante Π_c, chaque nœud $i_j \in \Pi_c$ cherche une coalition $S_k \in \Pi_c \cup \emptyset$ telle que

$$V_{i_j}(S_k \cup \{i_j\}) > V_{i_j}(S_{\Pi_c}(i_j)). \qquad (4.10)$$

- Etape 3 :
  Si la relation (4.10) est vérifiée, alors le nœud i_j quitte la coalition courante Π_c et rejoint la nouvelle coalition S_k et on met à jour Π_c :

$$\Pi_{c+1} = (\Pi_c \backslash \{S_{\Pi_c}(i_j), S_k\}) \cup \{S_{\Pi_c}(i_j) \backslash \{i_j\}, S_k \cup \{i_j\}\},$$

  sinon le nœud i_j reste dans sa coalition
  et

$$\Pi_{c+1} = \Pi_c.$$

- Etape 4 :
  Répéter les étapes 2 et 3 jusqu'à ce que Π_c converge vers une structure finale Π_f.

Phase 3 : Transmission des données

4.3.1 Organigramme de l'application

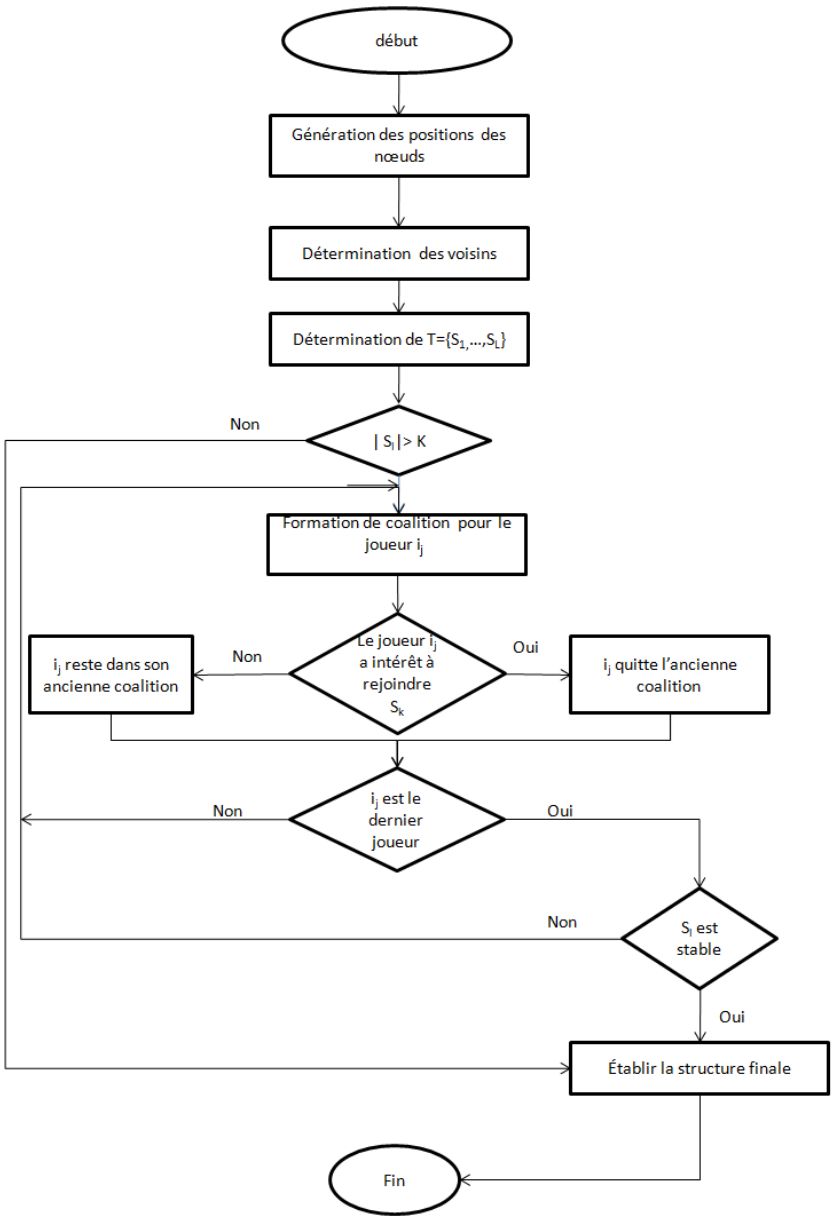

FIGURE 4.2 – Organigramme de l'algorithme de formation de coalitions

4.3.2 Description de l'algorithme

L'algorithme se compose principalement de 3 phases essentielles : découverte de voisins, formation de coalitions et transmission des données.

Dans la première phase, qui est la découverte de voisins, chaque nœud examine son environnement afin de trouver des candidats pour coopérer. Chaque nœud se retrouve avec un ensemble de voisins. On classe ces ensembles par ordre croissant par rapport à leur cardinalité et on prend l'ensemble ayant la cardinalité maximale qu'on notera S_l. Par la suite on élimine tous les nœuds appartenant à cet ensemble S_l. On répète la procédure jusqu'à ce qu'on obtienne une structure $T = \{S_1, ..., S_L\}$, puis on teste si $|S_l| < K$ où K désigne le nombre d'espions, on partitionne l'ensemble S_l en des sous-ensembles de cardinalité égale à 1, sinon on envoie l'ensemble S_l à la phase 2.

Dans la seconde phase, qui est la formation de coalitions, chaque nœud essaye de coopérer avec ses voisins afin d'améliorer son utilité (taux de secret).
Chaque nœud $i_j \in S_l$ forme une coalition avec ses voisins avec une contrainte qu'elle contienne un nombre de nœuds supérieur aux nombres d'espions. Une fois qu'une coalition est formée, le nœud $i_j \in S_l$ compare son utilité dans l'ancienne coalition par rapport à la nouvelle, s'il a intérêt à être dans la nouvelle, il la rejoint et il quitte l'ancienne coalition. Il reste à vérifier, si la taille de l'ancienne coalition est supérieure aux nombres d'espions, donc elle est gardée, sinon elle est divisée en sous-ensembles de coalitions individuelles (cardinalité égale 1).
On répète la procédure pour tous les joueurs jusqu'à l'obtention d'une structure S_l stable. Et pour finir, cette phase est répétée pour toutes les coalitions $S_l \in T$, afin d'obtenir une structure T stable.

La troisième phase est relative à la transmission des données.
Si un nœud i_j se retrouve dans une coalition de taille une, la transmission des données se fait en une seule étape où ce dernier utilise toute sa puissance $\widetilde{P}$ pour l'envoie de ses données à la destination m_{i_j}. Sinon, la transmission des données se fait en deux étapes :
Etape 1 : échange d'informations avec les membres de sa coalition en utilisant le protocole DF.
Etape 2 : tous les nœuds appartenant à la coalition dirigent leurs antennes vers la destination m_{i_j} et transmettent les données de i_j.

4.4 Simulation et interprétation des résultats

Après avoir décri le modèle, nous passons maintenant à son évaluation. En utilisant la simulation, notre choix de langage de programmation s'est porté sur MATLAB.

Les paramètres d'entrée

Un réseau Ad-hoc est défini par sa couverture [3], comprenant N émetteurs, K espions et M destinations, où les positions des nœuds constituant le réseau sont générée selon une loi uniforme.

La puissance de transmission, notée $\tilde{P}$, est fixée pour tous les émetteurs du réseau.

le rayon de transmission de chaque émetteur, noté r.

Un rapport signal bruit (SNR), noté ν_0.

La variance du bruit, notée σ^2.

Exemple d'application

On prend $\mu = 3$, et on simule pour les valeurs suivantes :

Variable	Valeur	Unité
(A, B)	(3×3)	$Km \times Km$
N	15	-
K	2	-
M	2	-
$\tilde{P}$	10	mW
r	0.5	Km
ν_0	10	dB
σ^2	-90	dBm
μ	3	-

Remarque :

•dB ou décibel est une mesure du niveau de puissance.

• $Puissance(dBm) = Puissance(dB) + 30$.

Une fois que les positions des différents nœuds constituant le réseau sont simulées, on excute l'algorithme de formation de coalitions.

3. taille en coordonnées A et B.

4.4.1 Résultat de la simulation et interprétation

Une fois que la simulation a été faite conformément aux paramètres mentionnés dans le tableau précédent, on obtient la figure suivante :

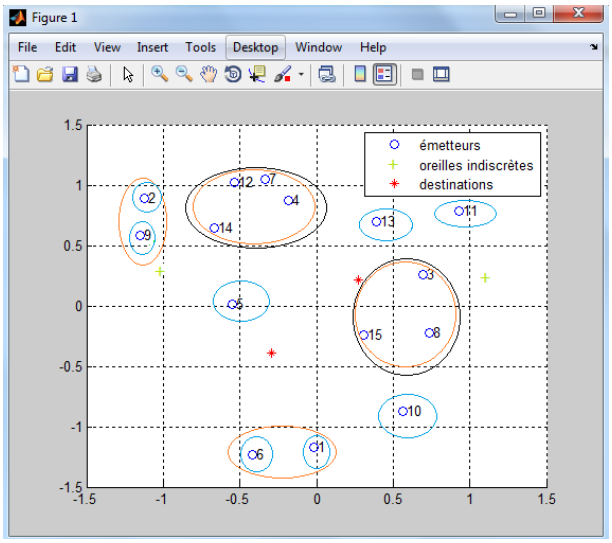

FIGURE 4.3 – Résultat de simulation.

La figure 4.3 illustre la structure du réseau résultant de l'algorithme de formation de coalitions pour un réseau avec $N = 15$ utilisateurs, $K = 2$ espions et $M = 2$ destinations, où les utilisateurs s'organisent en une structure de coalitions, avec la taille de chacune strictement plus grande que K ou égale à 1.
Les coalitions de tailles plus grandes que K sont représentées par les cercles noires, et celles de taille une sont représentées par des cercles bleus. Par contre, les cercles rouges représentent des ensembles de nœuds voisins.
Par exemple, les utilisateurs 5, 13, n'ayant aucun associé approprié pour former une coalition de taille plus grande que $K = 2$, ne coopèrent pas et se retrouvent dans des coalitions singletons. Par contre, les utilisateurs $\{4, 7, 12, 14\}$ coopèrent et forment une coalition car tous les utilisateurs tirent profit, vu que $V(\{4, 7, 12, 14\}) = (22.44 \quad 33.96 \quad 33.35 \quad 32.85)$ qui est une amélioration par rapport à leurs utilités dans le cas non coopératif qui vaut $V_4(\{4\}) = 17.32$, $V_7(\{7\}) = 24.89$, $V_{12}(\{12\}) = 19.65$, $V_{14}(\{14\}) = 26.27$.
La coalition {1,6} n'est pas retenue car sa taille est exactement égale au nombre $K = 2$ espions. Ainsi, les utilisateurs agiront comme des singletons.

A présent, nous allons faire une comparaison d'utilité moyenne (taux de secret) entre l'approche coopérative et non coopérative, en fonction du nombre d'utilisateurs N. Les résultats de simulation sont présentés dans la figure suivante :

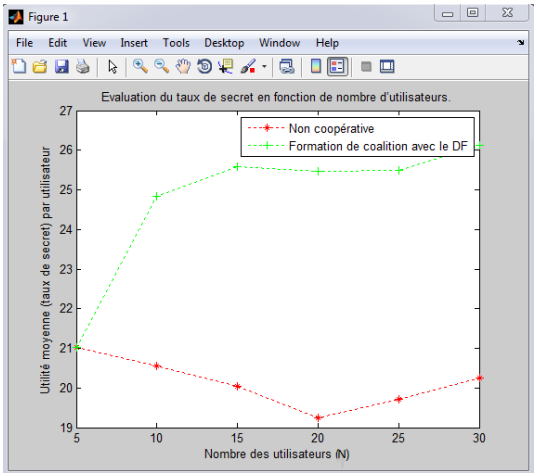

FIGURE 4.4 – Evaluation du taux de secret moyen en fonction du nombre d'utilisateurs.

On remarque que la courbe de la forme coopérative est au dessus de la courbe de la forme non coopérative montrant clairement que les utilisateurs ont intérêt à coopérer afin d'augmenter la quantité d'information fiable transmise.
On remarque que l'utilité est la même pour les deux approches quand $N = 5$, cela signifie qu'il n'y a pas de coalition de taille plus grande que K qui est formée, par contre, quand $N = 10$, on remarque que l'utilité des joueurs dans l'approche coopérative est supérieure à celle de l'approche non coopérative à cause des coalitions qui sont formées dans l'approche coopérative.
La courbe de l'approche coopérative est croissante cela peut être interprétée comme suit : l'augmentation du nombre d'utilisateurs favorise la formation de coalitions du fait qu' à mesure que le nombre d'utilisateurs N croit, la probabilité de trouver des associés croit aussi.

La comparaison d'utilité moyenne entre l'approche coopérative et non coopérative pour 240 nœuds est illustrée dans la figure ci-dessous :

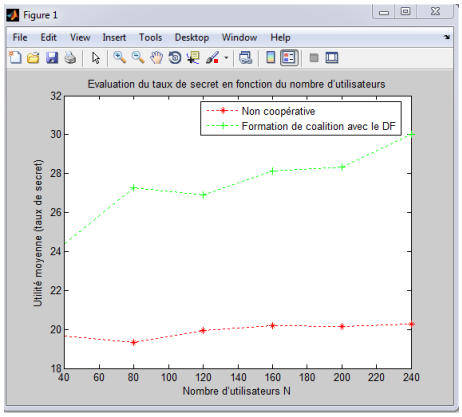

FIGURE 4.5 – Evaluation du taux de secret moyen en fonction du nombre d'utilisateurs.

Le tableau suivant résume les résultats illustrés par la figure 1.5

Nombre d'utilisateurs	Approche coopérative	Approche non coopérative
40	24.42	19.67
80	27.27	19.34
120	26.92	19.94
160	28.15	20.17
200	28.33	20.13
240	30.03	20.28

La figure suivante illustre l'utilité moyenne en terme du taux de secret en fonction du nombre d'espions (d'oreilles indiscrètes) dans les deux cas : coopératif et non coopératif.

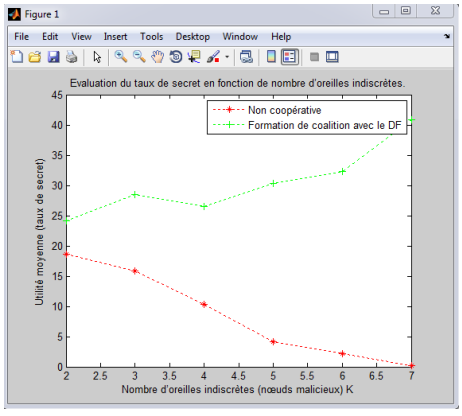

FIGURE 4.6 – Evaluation du taux de secret en fonction du nombre d'oreilles indiscrètes.

On remarque que la courbe de la forme coopérative est toujours au dessus de la courbe de celle non coopérative ce qui favorise la coopération.

Nous allons présenter maintenant un tableau qui illustre les différentes structures de coalitions résultant de l'algorithme de formation de coalitions où les nœuds du réseau change de position.

	Structure finale
1	{{5,10,11 ;12},{9,13,14},{2,4,15},{1},{3},{8},{6},{7}}
2	{{5,6,8},{13},{2},{3},{7},{4,12,15},{1},{10},{9},{14},{11}}
3	{ {11},{1,10,13},{2,5,6,8},{3,7,15},{4},{12},{9},{14}}
4	{{4,7,9},{1},{2},{3},{6},{5},{8},{15},{10},{11},{12},{13},{14}}
5	{{1,8,10,12,15},{4,5,1},{6,11,14},{2},{3},{7},{9}}

On remarque que la position des nœuds influe sur la structure résultante, cela est dû à la première phase de l'algorithme car pour coopérer il faut qu'ils soient proches les uns des autres, le nœud 5 forme une coalition avec (10,11,12) dans la première simulation par contre dans seconde, il se retrouve avec (6,8), cela peut être expliqué comme suit :
lors de la première simulation, le nœud 5 se retrouve proche de (10,11,12), par contre dans la seconde, il change de position dû à l'une des caractéristique du réseau Ad-hoc qui est la mobilité, de ce fait le nœud 5 forme une coalition avec (6,8) car ils sont proches.

Remarque Dans ce travail, nous avons constaté que la grande coalition se forme rarement à cause de la puissance nécessaire pour l'échange d'information et la perte de secret durant la phase d'échange d'information.

4.5 Conclusion

Dans ce chapitre, nous avons traité le problème de sécurité dans les réseaux Ad-hoc, en modélisant le problème de la sécurité de la couche physique sous forme d'un jeu coalitionnel à utilité non transférable. Nous avons également proposé un algorithme de formation de coalitions inspiré de [14] qui constitue l'essentiel de notre contribution, et nous l'avons implémenté sous le logiciel MATLAB.

D'après les résultats de l'algorithme, nous avons constaté que l'approche coopérative permet de réaliser des gains meilleurs par rapport à l'absence de coopération et de ce fait les nœuds émetteurs constituant le réseau ont intérêt à coopérer afin d'améliorer leur utilité en terme du taux de secret. Les résultats de l'algorithme montrent aussi que la structure finale résultante est stable.

Conclusion Générale

La sécurité était et demeure une question importante dans le cadre des réseaux Ad-hoc, car l'espionnage d'information lors de la transmission des données par les oreilles indiscrètes peut endommager la qualité de l'information. De ce fait, de nombreux travaux ont été réalisés dans le but d'améliorer le taux de secret. La théorie des jeux constitue un outil efficace avec lequel on peut cerner l'interaction entre les différents nœuds constituant le réseau afin de sécuriser la transmission des données.

Dans ce mémoire, nous avons modelisé le problème de la sécurité de la couche physique sous forme d'un jeu coalitionnel, où les nœuds émetteurs coopèrent et forment des coalitions pour augmenter la quantité d'informations fiables transmises. Ceci nous a conduit à développer un algorithme de formation de coalition qui permet de construire une structure stable.

Ce mémoire s'est focalisé sur l'insertion de la théorie des jeux coopératifs au problème de sécurité des réseaux Ad-hoc.

Le premier chapitre a été consacré aux réseaux Ad-hoc où nous avons défini quelques notions de base telles que les caractéristiques, les avantages et les vulnérabilités. Dans le second chapitre nous avons introduit la théorie des jeux où nous avons défini les concepts de base ainsi quelques jeux de formation de coalitions. Le troisième chapitre est une synthèse des principaux modèles de jeux traitant les problèmes de sécurité dans les réseaux Ad-hoc rencontré dans la littérature. Dans le chapitre quatre nous avons présenté un modèle qui traite l'un des nouveaux aspects liées à la sécurité des réseaux Ad-hoc, où nous avons commencé par la présentation du modèle puis la modélisation de ce dernier sous forme d'un jeu coalitionnel. En suite nous avons établie un algorithme de formation de coalitions et terminer par une implémentation numérique sous MATLAB.

L'algorithme élaboré permet aux utilisateurs de s'organiser en coalitions dans le but d'accroitre leurs utilités en terme de confidentialité. A cause de la simulation des positions des nœuds on n'a pas pu établir une comparaison entre notre algorithme et l'algorithme établi dans [31].

L'exécution de notre algorithme pour plusieurs instance en variant les différents paramètres nous a permet d'obtenir presque les mêmes résultats :
•La courbe de la forme coopérative est toujours au dessus de la courbe de la forme non coopérative ce qui favorise la coopération.
•L'évaluation du taux de secret moyen en fonction du nombre d'utilisateurs N montre que la courbe de l'approche coopérative est croissante cela peu être interprétée comme suit : l'augmentation du nombre d'utilisateurs favorise la formation de coalitions du fait qu'à mesure que le nombre d'utilisateurs N croit, la probabilité de trouver des associés croit aussi.
La seule différence réside dans le nombre d'utilisateurs N, où nous avons exécuté notre algorithme pour $N = 240$, par contre, leur algorithme est exécuté pour $N = 45$.

En guise de perspective, le modèle pourrait être étendu en prenant en compte le fait qu'un nœud peut être à la fois émetteur et récepteur ce qui reflète de près la réalité. En se qui concerne l'algorithme de formation de coalition, ce dernier peut être améliore en réduisant la complexité qui influe sur le temps d'exécution.

Bibliographie

[1] M. T. Abbes. Proposition d'un protocole à économie d'énergie dans un réseau hybride GSM et Ad-hoc. Thèse de doctorat, Université d'Oran, 2011-2012.

[2] B. Ait-Salem. Sécurisation des réseaux Ad-hoc : systèmes de confiance et de détection de répliques. Thèse de doctorat, Université de Limoges, 2011.

[3] R. J. Aumann. The core of a cooperative game without side payments. Transactions of the American Mathematical Society, Vol. 98, No. 3, pp :539-552, March 1961.

[4] A. BAADACHE. Sécurité du routage dans les réseaux mobiles Ad-hoc. Mémoire de magistère, Université A.MIRA de Béjaia, Octobre 2005.

[5] A. Babakhouya. Sécurité de Routage, Mémoire de magistère, Université A.MIRA de Béjaia, 2004-2005.

[6] J. S. Baras. T. Jiang, P. Purayastha. Constrained coalition games and networks of autonomous agents. ISCCSP, Malta, 2008.

[7] F. Bloch. Sequential formation of coalitions with fixed payoff division and externalities. Games and Economic Behavior, Vol. 14, No. 0043, pp :90-123, 1996.

[8] J. Chen. R. Zhang. L. song, Z. Han. B. Jiao. Joint relay and jammer selection for secure two-way relay networks. arXiv :1111.7108v1 [cs.IT], Nov 2011.

[9] C. D'aspermont. A.Jacquemin. J. J. Gabszewicz. J. Weymark. On the stability of collusive price leadership. Canadian Journal of Economics, Vol. 16, pp :17-25, 1983.

[10] H. I. Doaa. E. Hassan, S. El-Dolil. Relay and jammer selection schemes for improving physical layer security in two-way cooperative networks. Computers and Security, vol. 50, pp :47-59. 2015.

[11] L. Dong. Z. Han, A. P. Petropulu. H. V. Poor. Improving wireless physical layer security via cooperating relays. IEEE Transactions on Signal Processing, March 2010.

[12] R. P. Gilles. The cooperative game theory of networks and hierarchies. Springer Edition, 2010.

[13] A. Gliz. Theorie des jeux et economie de l'information. Ecole Superieure de Commerce, pp :1-198, 2010.

[14] M. Guazzone. C. Anglano, M. Sereno. A game-theoretic approach to distributed coalition formation in energy-aware cloud federations (extended version). arXiv : 1309.2444v5 [cs.DC], Jan 2014.

[15] G. Jiang. S. Shen. K. Hu, L. Huang. H. Li. R. Han. Evolutionary game-based secrecy rate adaptation in wireless sensor networks. International Journal of Distributed Sensor Networks, March 2015.

[16] S. Krasa. Coalition structure values in differential information economies :is unity a strength ?. Journal of Mathematical Economies, pp :51-62, 2003.

[17] M. Kurz S. Hart. Endogenous formation of coalitions. Econometrica,Vol. 53, pp :1047-1064, 1983.

[18] M. Kurz S. Hart. Stable coalition structures. Econometrica,Vol. 53, pp :1047-1064, 1984.

[19] X. Li, M. R. Lyu. A novel coalitional game model for security issues in wireless networks. Globecom, 2008.

[20] K. Maafa. Sur les jeux stratégiques multicritères avec formation de coalitions et gain non transférables. Mémoire de magistère, Université A.MIRA de Béjaia, 2010.

[21] R. B. Mayerson. Game theory. Harvard University Press paperback Edition, 1997.

[22] L. Melit. Le problème d'élection dans les réseaux mobiles ad hoc. Mémoire de magistère, Université A.MIRA de Béjaia, 2004-2005.

[23] J. V. Neumann and O. Morgenstern. Theory of game and economic behavior. Princeton Univercity Press, USA, 1944.

[24] C. Nikolenyi. Coordination problem and grand coalition : the puzzle of the government formation game in the Czech Republic, 1998. Communist and Post-Communist Studies, pp :325-344, 2003.

[25] H. Otrok, M Debbabi. C. Assi, P. Bhattacharya. A cooperative approach for analyzing intrusions in mobile Ad-hoc networks. 27th International Conference on Distributed Computing Systems Worksshops (ICDCSW'07), 2007.

[26] C. Perkins. Ad hoc networking. Addison wesley, 2001 .

[27] M. S. Radjef. La théorie des jeux coopératifs. Cours de master2. Département de Recherche Opérationnelle, Université A.MIRA de Béjaia, 2015.

[28] M. S. Radjef. La théorie des jeux différenielles. Cours de master2. Département de Recherche Opérationnelle, Université A.MIRA de Béjaia, 2015.

[29] D. Ray. A game-theoretic perspective on coalition formation, Oxford University Press, New York, 2007.

[30] W. Saad. Z. Han. T. Baser. M. Debbah and A. Hjorungnes. Physical layer security : coalitional games for distributed cooperation. In : Proc. 7th int. symp. On modeling and optimisation in mobile, Ad-hoc, and Wireless networks, Saoul, South Korea, 2009.

[31] W. Saad. Z. Han. T. Baser. M. Debbah and A. Hjorungnes. Physical layer security : distributed coalitional formation games for secure wireless transmission. Mobile Netw Appl, 2010.

[32] Y. Sang-Seung. Endogenous formation of customs unions under imperfect competition : open regionalism is good. Journal of International Economics, Vol. 41, pp :153-177, 1996.

[33] Y. Sang-Seung. Endogenous formation of economic coalitions : A survey on the partition function approach. Sogang University, Seoul 121-742, Korea. 1999.

[34] J. M. Smith. Evolution and the theory of games. Cambridge University Press, 1982

[35] B. R. Smith and J. J. Garcia-Luna-Aceves. Securing the border gateway routing protocol. In Proc. of Global Internet, London, UK, November 1996.

[36] S. Thoron. Négociations multilatérales entre entreprises hétérogènes : la loi du plus fort ou l'union fait la force. Technical Report 18-2005. GREQAM, Avril 2003.

[37] R. Vohra. D. Ray. Coalitionnal power and public goods. Journal of Political Economy. Vol. 109, pp :1355-1384, 2001.

[38] M. Yildizoglu. Introduction à la théorie des jeux. DUNOD, Paris, 2003.