UNIVERSITÉ DE LORRAINE

IMSD

Rapport de projet long

Modélisation de la confiance dans les systèmes IoT par la théorie des jeux

MOUHDI Fadwa

EL ASKOURI Fatima ezzahra

Auteur

Encadrants : PASCAL Moyal,

SU Runbo

2022

Table des matières

1 Introduction

IoT (internet des objets) désigne le réseau d'appareils connectés équipés de capteurs ou d'autres technologies qui leur permettent de collecter et transmettre des données via Internet.De nos jours, il est très important de surveiller la sécurité de ces systèmes, or, c'est une tâche qui n'est pas toujours facile.

la théorie des jeux est l'une des méthodes les plus utilisées pour modéliser les problèmes de la sécurité dans les systèmes IOT. Un jeu est une situation interactive entre un ensemble de joueurs (qui peuvent d'être des noeuds dans ce cas) en tenant compte de leur actions et les gains associés à chaque stratégie.

Dans ce document, nous allons présenter deux exemples qui illustre l'application de la théorie des jeux pour résoudre les problèmes de sécurite.

Le premier exemple est un jeu non coppératif entre des noeuds attaquants qui visent à nuire au fonctionnement du réseau et l'IDS qui est un moyen important pour détecter le comportement des nœuds malveillants. En utilisant le cadre de la théorie des jeux, on a montré que le jeu atteint l'équilibre de Nash conduisant ainsi à la stratégie de défense pour l'IDS.

Le deuxième exemple est un jeu bayésien c'est à dire un jeu à information incomplète, nous avons itroduit ce type de jeu vu que généralment un jeu attaquant/défenseur est un jeu d'information incomplète où le défenseur est ne connait pas le type de son adversaire. Nous avons utilisé deux types des jeux bayésien : statique et dynamique, la différence entre les deux est que le premier ne prend pas en considération l'évolution du jeu c'est à dire que le défenseur a des croyances préalables fixées sur les types de son adversaire. En revanche, pour le second, le défenseur peut dynamiquement mettre à jour ses croyances sur la base de nouvelles observations des actions de l'adversaire et de l'historique du jeu.Finalement, nous avons déterminé les équilibres de Nash bayésiens pour chaque jeu.

2 État de l'art

2.1 Théorie des jeux

2.1.1 Principe

Un jeu est une situation dans laquelle deux joueurs ou plus prennent des décisions rationnelles selon des règles bien définies dans le but de recevoir un gain. La théorie des jeux est une branche des mathématiques qui traite et analyse ces jeux.

Un jeu est défini comme un triplet (P, S, U), où P est l'ensemble des joueurs, S est l'ensemble des stratégies de ces joueurs et U est l'ensemble des gains attendus . Le gain $U_i(s)$ exprime le bénéfice b du joueur i moins le coût c qu'il doit supporter en jouent une de ces stratégies : u = b - c. [6]

Dans un jeu à information complète avec n joueurs, on appelle un profil stratégique s= $\{s_i\}_{i=1}^{n}$ le n-tuple de stratégies des joueurs. Soit $mri_i(S_{-i})$ la fonction de meilleure réponse du joueur i aux stratégies des autres joueurs qui représentées par s_{-i}, cette fonction maximise $u_i(s_i, s_{-i})$ sur l'ensemble de toutes les stratégies possibles du joueur i (désignées par S_i), c'est-à-dire,

$$mri_i(s_{-i}) = argmax U_i(s_i, s_{-i})$$

Si un n-tuple de stratégies satisfait la relation $s_i = mri_i(s_{-i})$ pour chaque joueur i, puisque les joeueurs sont rationels, alors aucun d'eux ne choisira une stratégie différente de celle qui est dans le profil stratégique donné. Ce cas nous conduit au concept d'équilibre de Nash.

Un profil stratégique s^* vérifie l'équilibre de Nash (NE) si, pour chaque i, [6]

$$U_i(s_i^*, s_{-i}^*) \geq U_i(s_i, s_{-i}^*) \forall s_i \in S_i$$

les stratégies introduites ci-dessus sont des stratégie pures, or, parfois un joueur peut jouer une stratégie pure avec une certaine probabilité; de telles stratégies sont appelées stratégies mixtes.

Plus précisément, une stratégie mixte x_i du joueur i est une distribution de probabilité sur son ensemble S_i de stratégies pures. Un profil de stratégie mixte x*= $\{x_i^*\}_{i=1}^n$ vérifie l'équilibre de Nash à stratégie mixte si, pour chaque $x_i \in$X$_i$,

$$\tilde{U}_i(s_i^*, s_{-i}^*) \geq \tilde{U}_i(s_i, s_{-i}^*) \forall s_i \in S_i$$

où $\tilde{U}_i$ est la fonction de gain, X_i est l'ensemble des stratégies mixtes et x_{-i} représente les stratégies mixtes des joueurs autres que le joueur i.

2.1.2 Jeu coopératif et non coopératif

Dans la théorie des jeux, on distingue deux approches différentes :

-L'approche stratégique ou jeu non coopératif

-L'approche coalitions ou TJ Coopératifs

Les jeux coopératifs sont des jeux dans lesquels les joueurs choisissent une stratégie particulière en négociant et en se mettant d'acoord entre eux. Cependant, les jeux non coopératifs sont des jeux dans lesquels les joueurs décident de leur propre stratégie afin maximiser leur profit c'est à dire que dans un jeu non coopératif, les joueurs ne communiquent pas dans le but de coordonner leurs actions

Dans la théorie des jeux, un jeu non coopératif est un jeu avec compétition entre des joueurs individuels, par opposition aux jeux coopératifs.

2.1.3 Jeu bayésien

Dans ce projet nous allons nous intéresser aux jeux bayésiens (statiques et dynamiques).

— ***Jeu bayésien statique***

Considérons n joueurs : i = 1, ..., n. La représentation de la forme normale d'un jeu bayésien statique est la suivante :

-Pour chaque joueur i = 1,..., n, nous avons un ensemble S_i de stratégies. On appelle s = (s_1, ..., s_n) un profil stratégique du jeu où $s_i \in$S$_i$

- On définit pour chaque joueur i un ensemble des types possibles du joueur T_i . Le vecteur t = (t_1, ..., t_n) contient le type de chaque joueur, où $t_i \in$T$_i$

- $p(t_i)$ est la probabilité qu'un joueur i soit du type t_i (probabiloté fixe au long du jeu). Le joueur i observe son propre type. Mais elle n'est pas certain des types des autres joueurs.

- Le gain du joueur i dépend des stratégies choisies et des types de joueurs :

$$U_i = U_i(s,t) = U_i(s_1, .., s_n, t_1, .., t_n)$$

Un profil stratégique pure s^*=(s_1^*, ..., s_n^*) dit un équilibre de Nash si pour chaque joueur i et pour chaque type t_i de i stratégie : s_i= $s_{t_i}^*$ vérifie :

$$max \sum_{t_{-i} \in T_{-i}} p(t_{-i}) U_i(s_1^*(t_1), ..., s_{i-1}(t_{i-1}), s_i, s_{i+1}^*(t_{t+1}), .., s_n^*(t_n))$$

— ***Jeu bayésien dynamique***

Le jeu bayésien statique est un jeu à une étape, pour lequel un joueur maximise son gain en fonction d'une croyance fixe sur le type de ses adversaires. En réalité, il est difficile d'attribuer des probabilités préalables précises pour les types de joueurs i, nous étendons donc le jeu bayésien statique à un jeu bayésien dynamique à plusieurs étapes, où le joueur met à jour ses croyances en fonction de l'évolution du jeu. Nous supposons que le jeu bayésien statique est joué de manière répétée dans chaque période de temps t_k, où k = 0, 1, ... les croyances peuvent être calculées en utilisant la règle de bayes [3]

2.2 Sécurité dans les systèmes IoT

IoT désigne le réseau d'appareils connectés équipés de logiciels, de capteurs, ou d'autres technologies qui leur permettent de collecter et de transmettre des données via Internet.

Un appareil IoT est toute « chose » connectée à Internet. Cela inclut les ordinateurs portable, les téléphones mobiles, les tablettes et les serveurs, ainsi que les appareils électroménagers, les imprimantes, les montres intelligentes , les appareils photo ...

La sécurité dans les systèmes IoT est une sous-section de « cyber sécurité » qui se concentre sur la surveillance, la protection et la remédiation des menaces liées à l'Internet des objets

L'IoT est susceptible de subir de nombreux types d'attaques : modification et/ou altération de messages, déni de service (DoS), écoute clandestine, attaques Sybil, etc. Concrètement, de nombreuses attaques réelles ont eu lieu au cours de la dernière période.[4]

2.3 L'application de la théorie des jeux dans les systèmes IOT pour résoudre les problèmes de sécurité

Dans cette section, nous allons présenter deux exemples qui traitent la problèmatique de la sécurite des systèmes IOT en utilisant la théorie des jeux.

le premier exemple utilise les jeux non coopératifs et compare ses résultats avec les résultats obtenus en utlisant d'autres alternatifs (MDP et la charge de traffic)

dans le deuxième exemple nous allons introduire la notion des jeux à information incomplètes

et donc traiter le sujet en utilisant les jeux bayésiens statiques et dynamiques.

2.3.1 Jeu non coopératif

2.3.1.1 Jeu non coopératif

Dans cet exemple, trois schémas différents pour détecter les intrusions sont présentés. Dans les trois schémas, on se référé à IDS qui un système de détection d'intrusion et dont tâche est de protéger les nœuds de capteurs. En raison des limitations du système, IDS ne peut pas protéger tous les nœuds de capteur, et donc il doit chosir un nœud de capteur pour le protéger et cela sur la base de l'un des trois schémas présentés, dans ce qui suit, on appelera ces noeuds par des clusters [5].

Dans le premier schéma, un jeu non coopératif entre l'attaquant et les nœuds capteurs est défini, En utilisant le cadre de la théorie des jeux, on a montré que le jeu atteint l'équilibre de Nash pour l'attaquant et l'IDS, conduisant ainsi à la stratégie de défense pour l'IDS.

Dans le second schéma, un système de détection d'intrusion basé sur MDP est introduit. Au début, IDS observe le système et apprend le comportement de l'attaquant et essaie ensuite de décider quel nœud a besoin de protection. S'il protège le même nœud que l'attaquant voulait attaquer, l'attaque échoue, or, si l'attaquant attaque un nœud différent du nœud que L'IDS protège donc l'attaque réussit.

Dans le troisième schéma, une métrique intuitive est utilisée, IDS choisit de protéger le nœud qui a la charge de trafic la plus élevée.

A la fin de l'exemple, une comparaison des performances de chacune de ces trois shémas est faite. [5]

Par rapport à un cluster fixe k, l'attaquant a trois stratégies : (AS_1) attaquer le cluster k , AS_2 n'attaquer aucun cluster, AS_3 attaquer un cluster différent de k. L'IDS a également deux stratégies : SS_1 défendre le cluster k ou SS_2 défendre un autre cluster.

Les gains de de l'IDS et de l'attaquant sont exprimés sous forme matriciel (voir matrice A et B) on définit les notions suivantes : [5]

- U(t) : l'utilité des sessions en cours du réseau de capteurs.
- AL_k : la perte moyenne en perdant le cluster k .
- C_k : le coût moyen de la défense du cluster k .
- N_k : le nombre de nœuds dans un cluster k .

la matrice des gains de l'IDS est la suivante :

$$A_{ij} = \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \end{bmatrix}$$

a_{11}=U(t)-C_k est le gain lorsque l'attaquant et l'IDS choisissent le même cluster K pour attaquer et défendre respectivement, donc pour l'IDS, sa valeur d'utilité d'origine U(t) seront déduits des frais de défense.

a_{12}=U(t)-C_k est le gain lorsque lorsque l'attaquant n'attaque pas du tout, mais IDS défend un cluster k, nous devons donc déduire le coût de la défense

a_{13}=U(t)-C_k-$\sum_{i=1}^{N_{K'}} AL_{k'}$ est le gain lorsque l'attaquant attaque le cluster k, mais IDS défend le clusterk'. Dans ce cas, nous soustrayons le coût moyen de la défense d'un cluster, de l'utilité d'origine, ainsi que la déduction de la perte moyenne de perdre d'un autre cluster.

a_{21}=U(t)-$C_{k'}$-$\sum_{i=1}^{N_K} AL_k$ est le gain lorsque l'attaquant et l'IDS choisissent deux clusters différents pour attaquer et défendre respectivement.

a_{22}=U(t)-$C_{k'}$ est le gain lorsque l'attaquant n'attaque pas du tout, mais IDS défend un cluster k' , nous devons donc déduire le coût de la défense.

a_{23}=U(t)-$C_{k'}$-$\sum_{i=1}^{N_{K"}} AL_{k"}$ est le gain lorsque IDS défend le cluster k' mais que l'attaquant attaque un autre cluster. Dans ce cas nous soustrayons le coût moyen de la défense d'un cluster, de l'utilité d'origine, ainsi que la perte moyenne de la perte d'un autre cluster. [5]

on définit la matrice des gains de l'attaquant comme suivant :

$$B_{ij} = \begin{bmatrix} b_{11} & b_{12} & b_{13} \\ b_{21} & b_{22} & b_{23} \end{bmatrix}$$

CW est le coût d'attendre et d'attaquer dans l'avenir.

CI est le coût de l'intrusion pour l'attaquant

PI(t) est le gain moyen de chaque attaque.

b_{11} = b_{21} = PI(t)- CI c'est les gains lorsque l'attaquant attaque le cluster k,

b_{12}=b_{22} = CW c'est les gains du mode non-attaque, et en tant qu'attaquant dans ces deux modes décide d'attaquer dans le futur CW est le coûs à payer pour attendre.

b_{13}=b_{23} =PI(t)- CI c'est les gains lorsque l'attaquant attaque des clusters différents de cluster k. Nous soustrayons le coût moyen de l'attaque du profit moyen de la concordance d'un cluster.

1-pour IDS, la meilleure stratégie consiste à trouver le meilleur cluster à défendre, qui est celui avec la valeur maximale de U(t) -C_k

2-pour l'attaquant, la meilleure stratégie consiste à trouver le bon cluster à attaquer et puisque ; PI –CI est supérieur à CW , donc l'attaquant est toujours encouragé à attaquer

De 1 et 2, on conlut que le jeu a un équilibre de Nash en stratégie pure (AS_1, SS_1)

2.3.1.2 MDP :

un processus de décision de Markov (MDP) est un modèle pour les problèmes de décision stochastiques séquentiels, c'est un quadruplet (S,A,R,tr), où S l'ensemble d'états est, A est l'ensemble d'actions,R est la fonction de récompense et tr est la fonction de transition d'états. [5]

Les actions modifient les états et l'effet des actions sur les états est capturé par la fonction de transition. La fonction de transition attribue une distribution de probabilité à chaque paire (état, action).

La fonction de récompense attribue une valeur réelle à chaque paire (état, action), qui décrit la récompense immédiate (ou le coût) de l'exécution de cette action dans cet état.

Le critère utilisé pour sélectionner l'action dans chaque état est la maximisation de sa récompense future. Plus précisément, l'objectif est de choisir une action qui permet de maximiser le rendement attendu.

Le but de ce shéma est de faire la prédition du comportement futur de l'attaquant en prenant en considération le comportement passé de l'attaquant et donc les états passés du système.

2.3.1.3 Mesure intuitive : trafic

Pour le troisième schéma, une métrique intuitive est utilisé, qui est la charge d'activité et qui indique le trafic de chaque cluster, l'IDS doit choisir le cluster à défendre contre les attaques en fonction de ce paramètre,ainsi, à chaque créneau horaire, il défend le cluster qui a la valeur de traffic la plus élevée.[5]

2.3.1.4 Evaluations

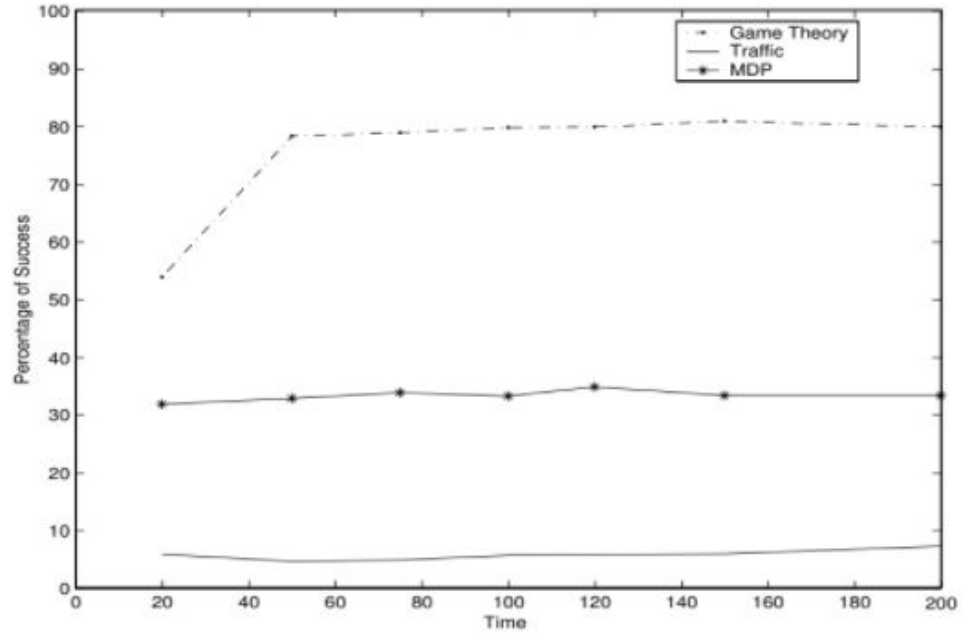

Fig. 2. N=50

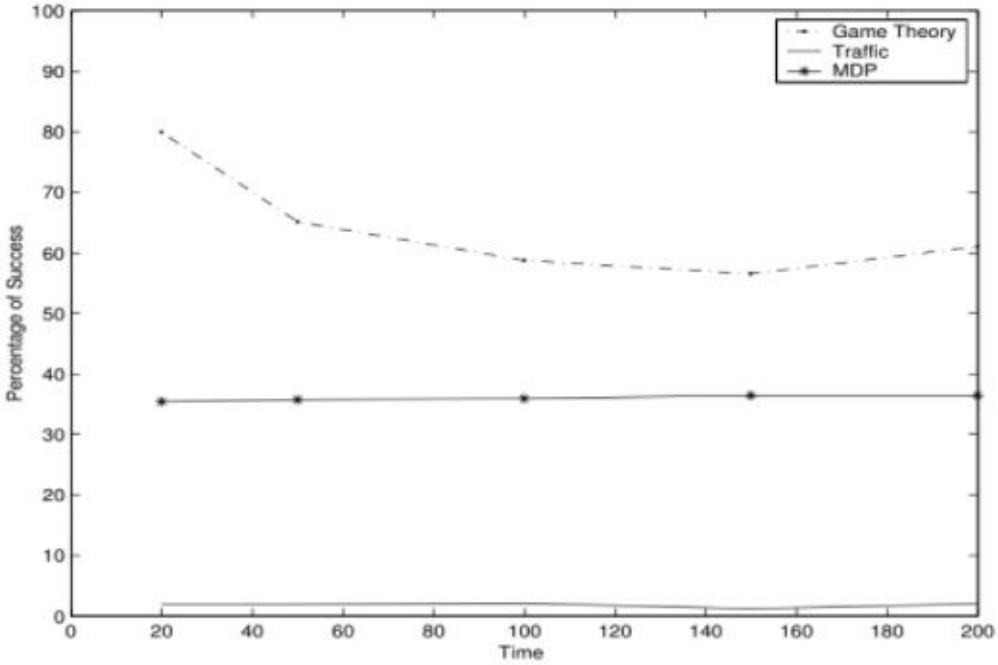

Fig. 3. N=200

Les figures ci-dessus [5] illustrent le taux de réussite (défendre le même noeud qui est attaqué) pour 50 et 200 nœuds dans les trois schémas, le cadre théorique des jeux, le MDP et la métrique intuitive.

N	20	50	100	200
temps en ms	243	590	1434	3245

Le tableau suivant décrit le temps que l'IDS doit passer pour apprendre et être capable de prédire le prochain nœud le plus vulnérable. [5]

Comme les résultats l'indiquent, en utilisant la théorie du jeu, les performances de l'IDS sont meilleures que les performances de l'approche MDP et de la métrique intuitive, de plus, dans le cadre de la théorie des jeux, nous avons pas besoin de temps supplémentaire pour apprendre et être capable à prédire.

2.3.2 Jeu bayésien

Le mauvais comportement des réseaux ad hoc peut être infligé par des nœuds malveillants qui visent à nuire au fonctionnement du réseau en montant des attaques contre des couches diffrentes du réseau.

Les IDS sont des moyens pour surveiller et détecter le comportement des nœuds malveillants et donc de jouer le rôle du défenseur.

Dans cette perspective, une approche de la théorie des jeux est proposée pour modéliser les interactions entre le nœud attaquant et le nœud défenseur.

Le but de la formulation de jeu bayésien est parce que dans la plupart des cas, un jeu attaquant/défenseur est un jeu d'information incomplète où le défenseur est incertain du type de son adversaire (qui'il soit régulier ou malveillant).

Dans les jeux bayésiens on distingue entre deux types : jeu bayésien statique et jeu bayésien dynamque, la différence entre les deux est que le premier ne prend pas en compte l'évolution du jeu, c'est à dire que le défenseur a des croyances fixées sur les types de son adversaire. En revanche, pour le second, le défenseur met à jours ses croyances sur la base de nouvelles observations des actions de l'adversaire et de l'historique du jeu, et peut ensuite ajuster sa stratégie de surveillance. [3]

2.3.2.1 Jeu bayésien statique

2.3.2.1.1 Présentation du jeu

Considérons deux joueurs i et j qui sont respectivement le noeud attaquant et le défenseur, le premier st soit régulier, désigné par θ_i= 0, soit malveillant, désigné par θ_i= 1, le deuxième est de type régulier noté par θ_j = 0 et son type est connu des deux joueurs.

Le type malveillant du joueur i a deux stratégies pures : Attaquer et Ne pas attaquer. Le type régulier du joueur i a une stratégie pure : Ne pas attaquer. Le défenseur j a deux stratégies pures : Surveiller et ne pas surveiller. .

Supposons que la valeur de la sécurité du défenseur j vaut w, où w > 0. En pratique, w pourrait être la valeur (monétaire) des actifs protégés. En d'autres termes, w représente une perte de sécurité dont la valeur est équivalente à un degré de dommage tel que la perte de réputation, la perte d'intégrité des données, le coût du contrôle des dommages, etc.

.	suveiller	ne pas surveiller
attaquer	(1-2α) W-C_a,(2α -1) W -C_m	W-C_a , -W
ne pas attaquer	0, - β W -C_m	0,0

.	suveiller	ne pas surveiller
ne pas attaquer	0, - β W -C_m	0,0

α : le taux des vrais posotifs

β : le taux des faux posotifs

W : la valeur de sécurité du défenseur j.

C_m : le coût du serveillance

C_a : le coût d'attaque.

les tableaux ci-dessus représente les gains des joueurs (le premier reprèsente les gains lorsque le joueur i est malveillant et le deuxième les reprèsente lorsque le joueur i est régulier. [8]

Si le type malveillant du joueur i décide d'attaquer et le défenseur décide de ne pas surveiller, alors, le gain du défenseur j est w et le gain du type malveillant du joueur i est son gain de réussite moins le coût d'attaque, c'est-à-dire w C_a.

Si le type malveillant du joueur i décide d'attaquer et le défenseur décide de ne surveiller, alors, le gain du défenseur j est le gain attendu de la détection de l'attaque qui est αw -(1- α)w = (2α -1)w moins le coût de surveillance C_m. En revanche, le gain du type malveillant du joueur i est la perte du défenseur j(qui est (1- 2α)w) moins le coût d'attaque

Si le joueur i decide de ne pas attaquer, alors son gain est toujours de 0, le gain du défenseur j est de 0 s'il décide de ne pas surveiller, et il a un coût de surveillance C_m et une perte attendue -βw due aux fausses alarmes s'il surveille

2.3.2.1.2 Détermination de l'équilibre de Nash bayésien

Supposons que le défenseur j attribue une probabilité préalable μ_0 au fait que le joueur i soit malveillant.

-Si le joueur i joue sa paire de stratégies pures (Attaquer si malveillant, Ne pas attaquer si régulier), alors le gain attendu du défenseur j en surveillant est :

$$E(surveiller) = \mu_0((2\alpha - 1)w - C_m) - (1 - \mu_0)(\beta w + C_m)$$

le gain attendu en jouant sa stratégie pure ne pas surveiller est :

$$E(nePasSurveiller) = -\mu_0 W$$

si E (surveiller) > E (nePasSurveiller) c'est à dire si $\mu_0 > \frac{(1+\beta_0)W+C_m}{(2\alpha+\beta-1)W}$ alors la meilleure réponse du joueur j est de surveiller

Par contre, si le défenseur j surveille alors attaquer ne sera pas la meilleure réponse pour le type malveillant du joueur i, par conséquent la stratégie ((Attaquer si malveillant, ne pas attaquer si régulier), surveiller, μ_0) n'est pas un équilibre de Nash bayésien.

si $\mu_0 < \frac{(1+\beta_0)W+C_m}{(2\alpha+\beta-1)W}$, la meilleure réponse pour le défenseur j est de ne pas surveiller, d'autre part,si le défenseur j ne surveille pas, alors (attaquer si malveillantne etpas attaquer si régilier) est la meilleur réponse du joueur i. On conclut que ((attaquer si malveillant, ne pas attaquer si régulier), ne pas surveiller, μ_0) est un équilibre de Nash bayésien à stratégie pure.

- Si le type malveillant du joueur i joue sa stratégie pure (ne pas attaquer), la stratégie dominante du défenseur j est (nes pas surveiller). Cependant, si le défenseur j ne surveille pas, la meilleure réponse pour le type malveillant du joueur i est d'attaquer. on conclut que la stratégie ((Ne pas attaquer si malveillant, Ne pas attaquer si régulier), Ne pas surveiller) n'est pas un équilibre de Nash bayésien.

On peut conclure quil n'existe pas d'équilibre de Nash bayésien à stratégie pure pour le jeu lorsque$\mu_0 > \frac{(1+\beta_0)W+C_m}{(2\alpha+\beta-1)W}$, on doit donc chercher un équilibre de Nash en stratégie mixte. Soit p la probabilité avec laquelle le joueur i attaque et q la probabilité avec laquelle le défenseur j surveille.

Le gain attendu du défenseur j en surveillant est :

E(surveiller)=p μ_0 ((2α -1)W -C_m) - (1- p) μ_0 (β W +C_m)-(1- μ_0)(β W+ Cm)

Le gain du déffenseur j s'il ne surveille pas est : E(nePasSurveiller)= -p μ_0 W

Pour déterminer l'équilibre en stratégie mixe, on s'appuie sur la condition d'indifférence des statégies différentes des joueurs, ainsi on détermine la probabilité que le joueur i attaque de fa-

çon que le joueur j soit inddifférent entre surveiller et ne pas surveiller, c'est à dire en imposant E(surveiller) = E(nePasSurveiller). On obtient

$$p* = \frac{\beta W + C_m}{(2\alpha + \beta) W \mu_0}$$

De la même façon, on impose E(attaquer)=E(ne pas attaquer) et on obtient :

$$q* = \frac{W - C_a}{2\alpha W}$$

Finalement, (p* si malveillant, ne pas attaquer si régulier, q*,'μ_0 est un équilibre de Nash bayésien en stratégie mixte.[8]

2.3.2.2 Jeu baysésien dynamique

2.3.2.2.1 Présentation du jeu

On suppose dans le cadre d'un jeu bayésien statique que le défenseur a une croyance fixe sur le type de son adversaire, toutefois, cela est défficile en réalité, donc il faut éteindre le jeu bayésien statique à un jeu bayésien dynamique à plusieurs étapes, où le défenseur met à jour ses croyances selon l'évolution du jeu.

On suppose que le jeu bayésien statique se joue de manière répétée dans chaque période de temps t_k, où k=0, 1..n

On suppose qu'au début de chaque étape du jeu t_k le type malveillant du joueur i choisit une action $a_i\, t_k$ qui est soit attaquer ou ne pas attaquer, le type régulier a une seule action qui est ne pas attaquer, de même, le défenseur j choisit une action $a_j\, t_k$ qui est soit surveiller ou ne pas surveiller.

Dans un jeu bayésien dynamique, les stratégies mixtes dépendent de l'histoire du jeu et sont appelées stratégies de comportement.

Une stratégie de comportement pour le joueur i, désignée par σ_i, est définie comme : $\sigma_i\ (a_i(t_k)/\theta_i$, $h_i^j(t_k))$, où $h_i^j(t_k)$ représente le profil de l'historique des actions du joueur i par rapport à son adversaire j au début de l'étape de jeu t_k

Nous définissons une stratégie de comportement pour le défenseur j comme $\sigma_j\ (a_j(t_k)/\theta_j$, $h_j^i(t_k))$ où h_j^i représente le profil d'historique d'action du défenseur j par rapport à son adversaire i au début de l'étape du jeu t_k

On définit le profil de l'historique des actions du joueur i par rapport au défenseur j à l'étape du jeu t_k, h_i^j comme un vecteur binaire qui contient les actions du joueur i à chaque étape t_0, ..., t_{k-1}, qui est

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

où $a_i^j(t_k)$ est l'action du joeur i par rapport au joueur j à l'étape t_k

Pour simplier, une utilise les notations suivantes[3] :

$$\sigma_i(a_i(t_k) = attaquer \backslash \theta_i, h_i^j(t_k)) = p$$

$$\sigma_i(a_i(t_k) = nepasattaquer \backslash \theta_i, h_i^j(t_k)) = 1 - p$$

$$\sigma_i(a_j(t_k) = surveiller \backslash \theta_j, h_j^i(t_k)) = q$$

$$\sigma_i(a_j(t_k) = nepassurveiller \backslash \theta_j, h_j^i(t_k)) = 1 - q$$

Dans la première étape du jeu, t_0, la croyance du défenseur j sur le type malveillant de son adversaire est notée μ_0. Dans les étapes suivantes du jeu dynamique, le défenseur j met à jour ses croyances à la fin de chaque étape du jeu en utilisant la règle de Bayes :

$$\mu_j(\theta_i \backslash a_i(t_k), h_i^j(t_k)) = \frac{\mu_j(\theta_i \backslash h_i^j(t_k)) P(a_i(t_k) \backslash \theta_i, h_i^j(t_k))}{\sum_{\tilde{\theta_i}} \mu_j(\tilde{\theta_i} \backslash h_i^j(t_k)) P(a_i(t_k) \backslash \tilde{\theta_i}, h_i^j(t_k))}$$

avec, $P(a_i(t_k) \backslash \theta_i, h_i^j(t_k))$ est la probabilité que l'action a_i soit observée à cette étape du jeu, compte tenu du type d'adversaire et de l'historique de l'étape du jeu.

2.3.2.2.2 Détermination de l'équilibre de Nash bayésien

Pour déterminer l'équilibre de stratégie mixte,on fait la même chose que pour le jeu bayésien statique, c'est à dire qu'on s'appuie sur la condition d'indifférence des différentes stratégies des joueurs.

A l'étape t_k, si le défenseur j observe que l'action de son adversaire i était une attaque, alors son gain attendu en surveillant est :

$$E(a_j(t_k) = surveiller / a_i(t_k) = attaquer) =$$

$$(((2\alpha - 1)W - C_m)p + (-\beta W - C_m)(1-p))\mu_j(\theta_i = 1 \backslash a_i(t_k), h_i^j(t_k)) + (\beta W - C_m)\mu_j(\theta_i = 0 \backslash a_i(t_k), h_i^j(t_k))$$

le gain du joueur j si'il ne surveille pas est

$$E(a_j(t_k) = nepassurveiller / a_i(t_k) = attaquer) = Wp\mu_j(\theta_i = 1 \backslash a_i(t_k), h_i^j(t_k))$$

Le joueur i choisit p de sorte que le défenseur j reste indifférent entre Surveiller et Ne pas surveiller. C'est-à-dire que p est calculer mettant les deux gains égaux

$$p* = \frac{\beta W + C_m}{(2\alpha + \beta) W \mu_j(\theta_i = 1 \backslash a_i(t_k), h_i^j(t_k))}$$

On fait la même façon on chosit la probabilité avec laquelle le défenseur surveille de sorte que le type malveillant du joueur i soit indifférent entre attaquer et ne pas attaquer

$$q* = \frac{W_{Ca}}{2\alpha W}$$

Finalement, on peut conclure que (p*, q*, $\mu_j(\theta_i \backslash a_i(t_k), h_i^j(t_k))$) est un équilibre de Nash bayésien.[3]

3 Conclusion

L'objectif de ce travail était de présenter des exemples d'application de la théorie des jeux dans le domaine de la sécurité des réseaux.

Nous avons commencé par présenter en général la notion de la théorie des jeux et des systèmes IOT, nous avons présenté également certains types des jeux (jeu non coopératif, jeu bayésien statique et dynamique).

Le premier exemple présenté traite le sujet en utilisant un jeu non coopératif qui est un jeu dans lesquel les joueurs décident de leur propre stratégie afin maximiser leur profit, à la fin nous avons montré que ce jeu atteint l'équilibre de Nash.

Le deuxième exemple est une application des jeux bayésiens statiques et dynamiques où on pose l'hypothèse que le joueur j (défenseur) n'a pas une information complète sur le type de l'autres joueur i (attaquant), à la fin de cette exemple nous avons démontré que les jeux atteignent l'équilibre de Nash bayésien en stratégie mixte.

Bibliographie

[1] Auteur EVENTUEL, Auteur AUTRE, and Auteur DERNIER. Exemple de titre. *Journal quelconque*, 2019. URL : `http://www.siteQuelconque.com`.

[2] Rocscience Inc. URL : `https://www.rocscience.com/software/rocfall`.

[3] Yu Liu, Cristina Comaniciu, and Hong Man. A bayesian game approach for intrusion detection in wireless ad hoc networks. In *Proceeding from the 2006 workshop on Game theory for communications and networks*, pages 4–es, 2006.

[4] Arbia Riahi Sfar, Enrico Natalizio, Yacine Challal, and Zied Chtourou. A roadmap for security challenges in the internet of things. *Digital Communications and Networks*, 4(2) :118–137, 2018.

[5] Afrand Agah, Sajal K Das, Kalyan Basu, and Mehran Asadi. Intrusion detection in sensor networks : A non-cooperative game approach. In *Third IEEE International Symposium on Network Computing and Applications, 2004.(NCA 2004). Proceedings.*, pages 343–346. IEEE, 2004.

[6] Mohammad Hossein Manshaei, Quanyan Zhu, Tansu Alpcan, Tamer Bacşar, and Jean-Pierre Hubaux. Game theory meets network security and privacy. *ACM Computing Surveys (CSUR)*, 45(3) :1–39, 2013.

[7] Jeffrey Pawlick, Edward Colbert, and Quanyan Zhu. A game-theoretic taxonomy and survey of defensive deception for cybersecurity and privacy. *ACM Computing Surveys (CSUR)*, 52(4) :1–28, 2019.

[8] Xiao Wang, Renjian Feng, Yinfeng Wu, Shenyun Che, and Yongji Ren. A game theoretic malicious nodes detection model in manets. In *2012 IEEE 9th International Conference on Mobile Ad-Hoc and Sensor Systems (MASS 2012)*, pages 1–6. IEEE, 2012.