REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université A/ MIRA de Bejaia.
Faculté des sciences exactes
Département d informatique

Mémoire de fin cycle

En vue de l'obtention du Diplôme de Master 2 en informatique

Option : Recherche en réseaux et systèmes distribués

Thème

Présentation d'un modèle pour le comportement contradictoire dans les réseaux radio en présence d'un adversaire byzantine

Présenté par :
M^r^ CHABANE Saber
M^elle^ BOUICHE Andjima

Encadré par :
M^r^ HAMOUMA Moumen

Président du jury : **M^r^ BAADACHE Abderrahmane**
Examinateurs : **M^r^ OMAR Mawloud**

Promotion 2011

À la mémoire de ma mère

A mon père

À ma précieuse famille

A mes frères

A mes sœurs

A mon binôme Andjima

A mes collègues de travail

A tous mes amis.

CH. Saber

A mes très chers parents

À ma précieuse famille

À la mémoire de mes grandes mères

A mon frère

A mes sœurs

A mon binôme Saber

A mes collègues de travail

A tous mes amis en particulière Fatima

B. Andjima

En premier lieu, nous remercions le bon dieu de nous avoir la force et le savoir afin de réaliser ce modeste travail.

On tient à remercier chaleureusement notre promoteur M^r^ H. MOUMEN pour ces conseils, sa disponibilité, sa gentillesse, et surtout son précieux suivi durant la réalisation de ce travail.

Nous remercions aussi les membres du jury qui ont bien voulu nous faire l'honneur d'examiner et de juger notre travail.

CHABANE &BOUICHE

Sommaire

Chapitre II
Le problème des généraux Byzantins

Chapitre III
Présentation d'un modèle pour le comportement contradictoire

Liste des figures & des tableaux

Tableaux :

Figures:

Introduction générale

Avec l'arrivée des nouvelles technologies, l'informatique prend de plus en plus de la place dans tous les domaines, cela est dû aux avantages qu'offrent les systèmes informatiques dans le domaine des communications, en particulier les réseaux sans fil multifonctionnels qui ont connu une évolution spectaculaire ces dernières années. Ces réseaux sont devenus moins coûteux, ce qui permet de les utiliser dans tous les domaines.

Le média hertzien offre en effet des propriétés uniques, qui peuvent être résumées en trois points ; la facilité du déploiement, l'ubiquité de l'information et le coût réduit d'installation. Au cours de son évolution et malgré le succès des réseaux sans fil, il existe toute fois des pannes et erreurs qui sont soit acceptables ou inacceptables et parmi elles, les pannes Byzantine, ce type de pannes est considéré le plus difficile à gérer car ils sont des pannes de nature arbitraire.

Le concept de comportement Byzantin a été introduit pour la première fois par Lamport et Al, et dans lequel ils ont l'appelé par «Problèmes Byzantins Généraux », l'intérêt d'étudier ce problème est de déduire un algorithme qui résoud cette conséquence dans le domaine informatique qu'est devenu comme une exigence, pour pouvoir multiplier des processeurs (nœuds) afin de garantir une certaine sécurité dans les systèmes critiques. Trouver des algorithmes pour la détection du comportement Byzantin et l'identification facile du nœud corrompu. Faire combiner cette propriété avec l'auto-stabilisation pour améliorer la robustesse de ces algorithmes.

La diffusion sécurisée dans les réseaux radio et la réduction des temps de latence de diffusion dans les réseaux sans fil en présence d'un adversaire Byzantin, où chaque joueur (nœud) peut multicast un message à tous les joueurs au sein du rayon « r » est l'un des grand problèmes poser pour l'étude de modèle de comportement contradictoire. Les recherches effectuées dans ce domaine sont à un stade embryonnaire, très peu de travaux ont été consacrés à ce problème, parmi lesquelles on trouve une approche basée sur la présentation

d’un modèle pour le comportement contradictoire, qui se pose sur le problème des généraux Byzantins, que nous allons voir dans ce mémoire.

Afin de mener à bien notre travail, nous l’avons organisé en trois chapitres :

- Dans le premier chapitre, nous allons donner une idée générale sur les réseaux sans fil ainsi qu’une introduction sur le modèle de défaillances dans les systèmes distribués et les réseaux sans fil.
- Le second chapitre, nous l’avons consacré à la notion du problème des généraux Byzantins existant dans un système informatique.
- Le troisième chapitre est dédié à la présentation d’un modèle pour le comportement contradictoire.

Et enfin, notre travail s'achèvera par une conclusion générale.

Chapitre I.

Etat de l’art sur les réseaux sans fil

Chapitre I.

Etat de l’art sur les réseaux sans fil

I.1 Introduction

L’évolution de la communication sans fil et l’informatique mobile gagne de plus en plus de popularité, et les unités mobiles deviennent de plus en plus fréquentes, ceci a permis l’apparition de réseaux sans fil dans les entreprises et même chez les particuliers. Ces environnements mobiles offrent une grande flexibilité d'emploi, ils permettent la mise en réseau des sites dont le câblage serait trop difficile à réaliser et très coûteux.

Dans ce chapitre nous allons présenter quelques généralités liés aux réseaux sans fil. Il est organisé comme suit : La première partie est une brève présentation des réseaux sans fil, la seconde est dédiée a la taxonomie des réseaux sans fil, la troisième partie est consacrée aux différents types de réseaux sans fil existants, ensuite, nous aborderons en détails les modèle de défaillances dans les systèmes distribués et dans les réseaux sans fil, et enfin nous allons clôturer ce chapitre par une conclusion.

I.2 Définition d’un réseau sans fil

Un réseau sans fil (*wireless network*), comme son nom l’indique, est un réseau dans lequel au moins deux terminaux peuvent communiquer sans liaison filaire (via des ondes radiofréquences ou infrarouges). Grâce aux réseaux sans fil, les utilisateurs peuvent accéder à l’information indépendamment de leurs positions géographiques. Les terminaux du réseau (appelés généralement nœuds) se déplacent librement, tandis que le système doit assurer toutes les fonctionnalités et tous les services d’un réseau classique.

I.3 Taxonomie des réseaux sans fil

Il y a deux manières pour classer les réseaux sans fil. La première est basée sur la zone de couverture du réseau. Cette classification donne lieu à quatre catégories de réseaux sans fil: les réseaux personnels « ***WPAN*** », les réseaux locaux « ***WLAN***», les réseaux métropolitains «***WMAN***» et les réseaux étendus «***WWAN*** » comme nous montre la figure I.1.

La deuxième façon de voir les réseaux sans fil est selon le model et l'infrastructure de communication adoptée. Dans ce qui suit, nous donnerons des exemples pour chaque catégorie de réseau.

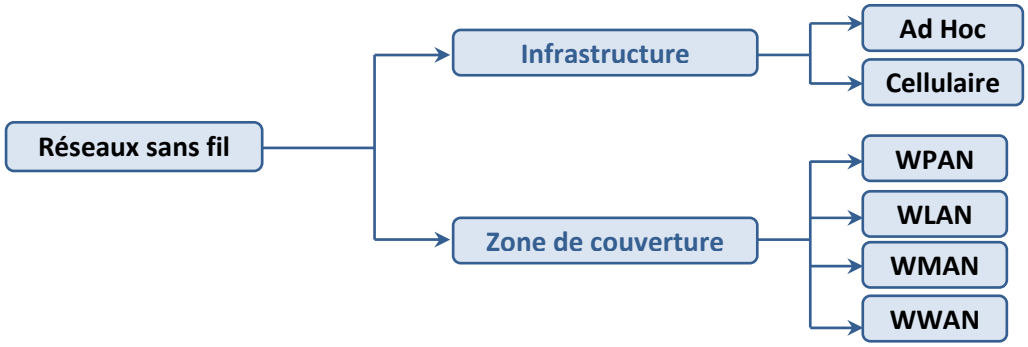


Figure I.1 Classification des réseaux sans fil.

I.3.1 Réseaux personnels sans fil (WPAN)

Le réseau personnel sans fil (WPAN -Wireless Personal Area Network) est constitué de connexions entre des appareils distants de seulement quelques mètres (PC, assistants, périphériques divers, etc.) comme dans un bureau ou une maison et concerne les réseaux sans fil d'une faible portée.

❖ **Bluetooth**

La principale technologie WPAN est la technologie Bluetooth [01], lancée par Ericsson en 1994, proposant un débit théorique de 1 Mbps pour une portée maximale d'une trentaine de mètres. Bluetooth, connue aussi sous le nom *IEEE 802.15.1*, possède l'avantage d'être très peu gourmand en énergie, ce qui le rend particulièrement adapté à une utilisation au sein de petits périphériques.

Bluetooth est un réseau à courte distance qui est destiné à remplacer le câble entre les composants électroniques et fournit une connexion RF (Radio Frequency) entre eux. La topologie du Bluetooth est en étoile. Il peut atteindre une distance de 10m. La puissance de

transmission typique est environ 1 mW. Bluetooth est normalisé par l'IEEE sous la référence IEEE 802.15.3 [4].

❖ **HomeRF (*Home Radio Frequency*)**

Lancée en 1998 par le HomeRF Working Group (formé notamment par les constructeurs Compaq, HP, Intel, Siemens, Motorola et Microsoft). Il propose un débit théorique de 10 Mbps avec une portée d'environ 50 à 100 mètres sans amplificateurs. La norme HomeRF soutenue notamment par Intel a été abandonnée en Janvier 2003, notamment quand les fondateurs de processeurs misent désormais sur les technologies Wi-Fi embarquée (via la technologie Centrino, embarquant au sein d'un même composant un microprocesseur et un adaptateur Wi-Fi).

❖ **HR-WPAN (High Rate-WPAN - IEEE 802.15.3)**

Comme pour Bluetooth, le standard HR-WPAN [03] adopte un modèle de réseau ad hoc avec une gestion centralisée par un maître appelé ici PNC (PicoNet Coordinator). Un PNC peut avoir jusqu'à 253 stations actives connectées à son piconet.

La couche physique du 802.15.3 utilise la bande ISM à 2,4 GHz. Une modulation de phase QPSK (Quadrature Phase Shift Keying) est utilisée pour le mode de base avec un débit de 11 Mbit/s. Quatre autres modulations sont également définies: DQPSK (Differential Quadrature Phase Shift Keying) 16 QAM (Quadrature Amplitude Modulation), 32 QAM et 64 QAM fournissant des débits respectifs de 22, 33, 44 et 55 Mbit/s.

Dans la sous couche MAC, le canal de transmission est divisé temporellement en supertrames. Chaque supertrame se décompose en trois parties: une trame balise (Beacon), la CAP (Contention Access Period) et la CFP (Contention Free Period).

La taille de la trame balise est en fonction des informations à transmettre. Cette trame est transmise par le PNC au début de chaque supertrame. Elle est destinée à l'ensemble des stations pour informer des paramètres du piconet. Parmi ces paramètres on trouve la durée de la supertrame, de la CFP mais aussi les informations d'allocations de ressources.

❖ **ZigBee (LR-WPAN - IEEE 802.15.4)**

Le comité IEEE a terminé de normaliser le standard 802.15.4 (Low Rate Wireless Personal Area Network) [03]. Les principaux objectifs de cette nouvelle norme, concurrents à la technologie Bluetooth dans certaines applications sont de mettre au point une technologie qui permet un transfert stable de données, une installation facile, un coût réduit et une très

basse consommation. Ce qui la rend particulièrement adaptée pour être directement intégrée dans de petits appareils électroniques (appareils électroménagers, hifi, jouets,...).

Au niveau de la couche physique, la norme 802.15.4 offre deux options qui sont combinées avec la sous couche MAC, permettront la mise en œuvre d'une large gamme d'applications.

Quelques applications peuvent exiger une bande passante dédiée pour atteindre des délais réduits. Pour accomplir ceci, l'IEEE 802.15.4 peut fonctionner en deux modes comme la montre la figure I-2. Dans le premier mode (avec supertrames), une station, appelée coordinateur du réseau, transmet des balises dans des intervalles prédéterminés (de 15 ms à 245 s). Le temps entre deux balises est divisé en 16 slots égaux. Un dispositif peut transmettre uniquement au début des slots. L'accès aux canaux est basé sur la méthode CSMA/CA.

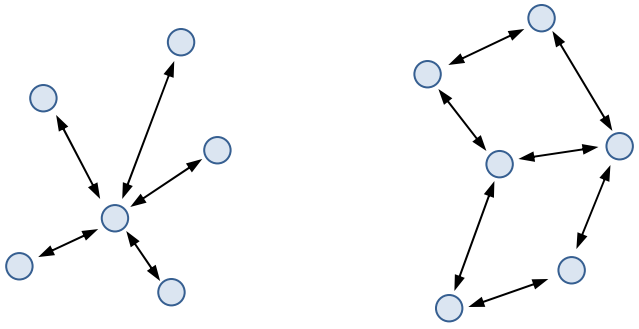


Figure I.2 Topologies étoile et peer-to-peer des réseaux IEEE 802.15.4

Dans le second mode, le coordinateur de réseau n'envoie aucune balise. Dans ce cas, l'accès au médium se fait par la méthode d'accès CSMA/CA classique. Comme dans la plupart des communications sans fil, des trames d'acquittement peuvent être utilisées dans les deux modes.

❖ **Liaisons infrarouges**

Elles permettent de créer des liaisons sans fil de quelques mètres avec des débits pouvant monter à quelques mégabits par seconde. Cette technologie est largement utilisée pour la domotique mais souffre toute fois des perturbations dues aux interférences lumineuses.

I.3.2 Réseaux locaux sans fils (WLAN)

Le réseau local sans fil (WLAN – Wireless Local Area Network) correspond au périmètre d'un réseau local installé dans une entreprise, dans un foyer ou encore dans un

espace public. Tous les terminaux situés dans la zone de couverture du WLAN peuvent s'y connecter. Il existe plusieurs technologies concurrentes:

❖ **Le WiFi (ou IEEE 802.11)**

Le standard ou la norme *IEEE 802.11* (*ISO/IEC 8802-11*) est un standard international décrivant les caractéristiques d'un réseau local sans fil (*WLAN*). Le nom **Wifi** (*Wireless Fidelity*), anciennement WECA (*Wireless Ethernet Compatibility Alliance*), l'organisme chargé de maintenir l'interopérabilité entre les matériels répondant à la norme 802.11. La technologie WiFi permet de créer un WLAN à haut débit. Ce dernier varie entre 11Mbps pour la norme 802.11b et 54Mbps pour la norme 802.11a/g.

Le WIFI est permet à des appareils de communiquer par les ondes radio a base de la norme IEEE 802.11

Les différentes versions sont nommées 802.11a, 802.11b,…, 802.11n. En règle générale, plus en plus une version est récente, plus en plus les débits proposés sont élevés. Voici un tableau présentant quelques révisions de la norme 802.11 et leur signification :

Nom de la norme	***Nom***	***Description***
802.11a	Wifi5	-Un haut débit (54 Mbps théoriques, 30 Mbps réels). -8 canaux radio dans la bande de fréquence des 5 GHz.
802.11b	Wifi	-la norme la plus répandue actuellement. -débit théorique de 11 Mbps (6 Mbps rééls) avec une portée pouvant aller jusqu'à 300 mètres dans un environnement dégagé. -La plage de fréquence utilisée est la bande des 2.4 GHz, avec 3 canaux radio disponibles.
802.11h		La norme *802.11h* vise à rapprocher la norme 802.11 du standard Européen (HiperLAN 2, doù le *h* de 802.11h) et être en conformité avec la réglementation européenne en matière de fréquence et d'économie d'énergie.
802.11g		La norme 802.11g offre un haut débit (54 Mbps

		théoriques, 30 Mbps réels) sur la bande de fréquence des 2.4 GHz. La norme 802.11g a une compatibilité ascendante avec la norme 802.11b, ce qui signifie que des matériels conformes à la norme 802.11g peuvent fonctionner en 802.11b
802.11Ir		La norme *802.11r* a été élaborée de telle manière à utiliser des signaux infra-rouges. Cette norme est désormais dépassée techniquement.
802.11j		La norme *802.11j* est à la réglementation japonaise ce que le 802.11h est à la réglementation européenne.

Tableau I.1 Les différentes révisions de la norme 802.11 [07].

La méthode d'accès au médium pour le WiFi est le CSMA/CA. L'accès au support est aussi contrôlé par l'utilisation d'espace interframe, ou IFS (InterFrame Spacing) qui correspond à l'intervalle de temps entre la transmission de deux trames.

❖ **hiperLAN2 (HIgh Performance Radio LAN 2.0)**

Norme européenne élaborée par l'ETSI (European Telecommunications Standards Institute), permet d'obtenir un débit théorique de 54 Mbps sur une zone d'une centaine de mètres dans la gamme de fréquence comprise entre 5 150 et 5 300 MHz [06].

❖ **DECT (Digital Enhanced Cordless Telecommunication)**

Norme des téléphones sans fils domestiques. Alcatel et Ascom développent pour les environnements industriels, telles les centrales nucléaires, une solution basée sur cette norme qui limite les interférences. Les points d'accès résistent à la poussière et à l'eau. Ils peuvent surveiller les systèmes de sécurité 24/24h et se connecter directement au réseau téléphonique pour avertir le responsable en cas de problème [06].

I.3.3 Réseaux métropolitains sans fil (WMAN)

Le réseau métropolitain sans fil (WMAN pour Wireless Metropolitan Area Network) est connu sous le nom de Boucle Locale Radio (BLR). Les WMAN sont basés sur la norme IEEE 802.16. Permet des raccordements à des réseaux à large bande dans les secteurs qui ne sont pas servis par le câble ou le xDSL (Cross-Digital Subscriber Line). La boucle locale radio

offre un débit utile de 1 à 10 Mbit/s pour une portée de 4 à 10 kilomètres et utilise les bandes de fréquences entre 2,4 GHz et 3,5 GHz, ce qui destine principalement cette technologie aux opérateurs de télécommunication.

I.3.4 Réseaux étendus sans fil (WWAN)

Le réseau étendu sans fil (WWAN pour Wireless Wide Area Network) est également connu sous le nom de réseau cellulaire mobile. Il s'agit des réseaux sans fil les plus répandus puisque tous les téléphones mobiles sont connectés à un réseau étendu sans fil. Les principales technologies sont les suivantes:

- **UMTS** *(Universal Mobile Telecommunication System*) est une technologie de transmission de troisième génération. Elle offre un débit qui peut atteindre 2Mbps contre 9,6Kbps pour le GSM et 115 Kbps pour le GPRS.
- **GSM** (*Global System for Mobile Communication)* est un standard de téléphonie mobile utilisé principalement en Europe, en Afrique et en Asie.
- **GPRS** (*General Packet Radio Service*) est une évolution du GSM. Cette technologie permet l'accès à de nombreux services multimédia, accessible en WEB ou en WAP.

La deuxième catégorie est Le mode infrastructure dans lequel les clients sans fil sont connectés à un point d'accès.

I.3.5 Réseaux cellulaires

Un réseau sans fil cellulaire supprime certaines liaisons filaires entre les entités du réseau et substitue le mode de connexion filaire par une technologie nouvelle basée sur les ondes radioélectriques. Ce mode impose de fixer des bornes pour délimiter une région appelée zone de couverture. La figure suivante schématise les principales caractéristiques des réseaux cellulaires (avec infrastructure).

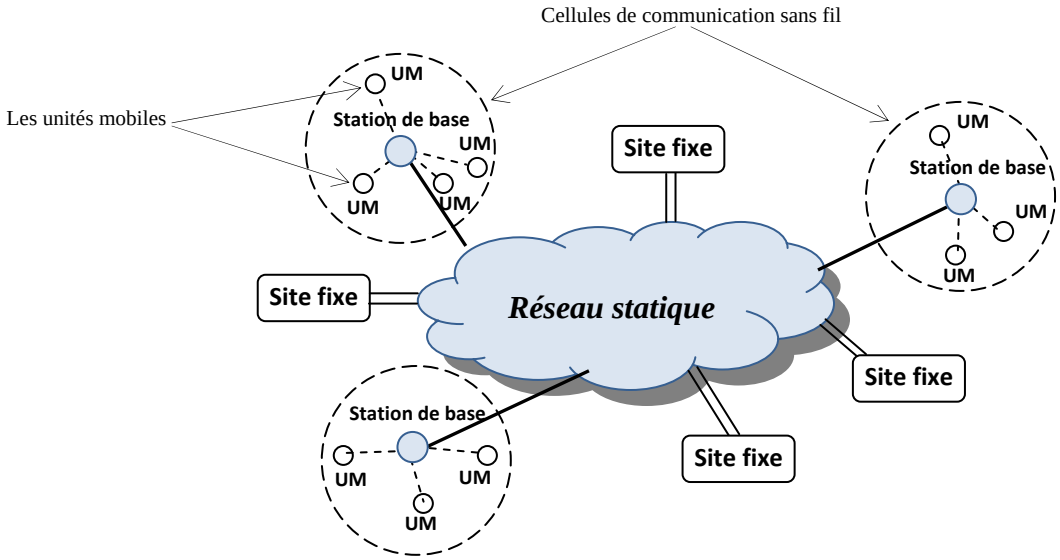


Figure I.3 Le modèle des réseaux sans fil avec infrastructure.

Parmi les sites fixes, on retrouve les stations de bases SB (les cercles noirs sur le schéma), appelées aussi points d'accès. Chaque station de base définit une région appelée *cellule*. Celle-ci correspond à la zone de couverture à partir de laquelle les unités mobiles (UM) peuvent émettre et recevoir des messages venants d'autres nœuds de l'intérieur ou de l'extérieur de la cellule. La communication entre deux nœuds (UM) connectés à deux points d'accès différents passe forcément par les SB correspondant aux cellules. Ces SB sont reliées entre elles par des liens filaires.

La configuration standard d'un système de communication cellulaire est un maillage de cellules hexagonales. C'est-à-dire que chaque cellule couvre une zone géographique selon la portée de la SB correspondante, mais lorsque la compétition devient importante pour l'allocation des canaux, la cellule est généralement divisée en sept cellules plus petites [08], comme illustré sur la figure I.4.

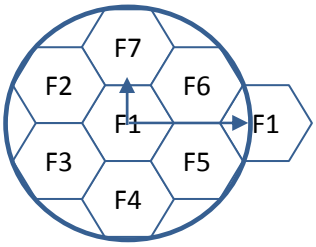


Figure I.4 Principe de réutilisation de fréquence.

I.3.6 Réseaux ad hoc (sans infrastructure)

La principale caractéristique qui fait la différence entre ce type de réseaux sans fil et un réseau sans fil classique est l'absence d'une infrastructure préexistante.

I.3.6.1 Définition d'un réseau ad hoc

Une définition formelle des réseaux ad hoc MANET (Mobile Ad hoc NETwork) est donnée par la RFC 2501. Il s'agit de réseaux sans fil et sans infrastructure fixe, utilisant généralement le médium radio, où chaque nœud peut jouer le rôle du client et de routeur. Les réseaux ad hoc sont auto-organisés, ce qui implique que la connectivité doit être préservée autant que possible automatiquement lorsque la topologie du réseau change (suite à l'apparition, la disparition ou au mouvement de certains nœuds) [06].

I.3.6.2 Principe de fonctionnement

On dit qu'un nœud B est voisin d'un autre nœud A, si B se trouve dans la zone d'émission de A. Donc, il faut définir des règles de gestion d'accès. En ce sens, lorsqu'un nœud émet, tous ses voisins ne peuvent être qu'en mode réception. A cause de la limite de la portée de transmission des nœuds, des relais (appelés aussi messagers) doivent être définis pour assurer la communication entre deux nœuds qui ne s'entendent pas (hors de la portée l'un de l'autre). Ce processus est appelé routage multi-sauts (ou Multi-hop outing). Ainsi, tous les nœuds d'un réseau Ad hoc coopèrent pour assurer les services fournis habituellement par les stations de base dans les réseaux avec infrastructure.

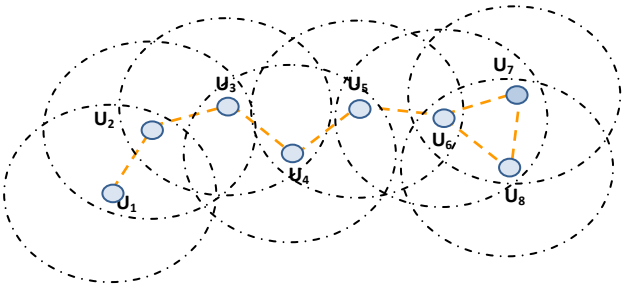


Figure I.5 Le routage multi-saut [06].

I.4 Les différents types de réseaux sans fil

Il existe principalement deux types de réseaux sans fil :

- Les réseaux utilisant les ondes infrarouges,
- Les réseaux utilisant les ondes radios (Bluetooth, Wifi, réseaux cellulaires, Wimax, etc.)

I.4.1 Les ondes infrarouges

Les ondes infrarouges sont couramment utilisées dans la vie courante (par exemple pour les télécommandes de télévisions). Grâce à elles, on peut créer des petits réseaux, notamment entre des téléphones portables et des ordinateurs.

Le principal inconvénient des réseaux créés avec les ondes infrarouges est qu'ils nécessitent que les appareils soient en face l'un de l'autre, séparés au maximum de quelques dizaines de mètres et qu'aucun obstacle ne sépare l'émetteur du récepteur puisque la liaison entre les appareils est directionnelle.

Contrairement aux technologies utilisant les ondes radio, les ondes infrarouges sont peu perturbées par l'environnement extérieur (microondes, émetteurs radio, etc.).

Les ondes infrarouges sont utilisées pour :

- La majorité des appareils avec une télécommande sans fil : télévision, chaîne HiFi, etc.
- Les télécommandes du verrouillage automatique des anciennes voitures
- Les télécommandes des jouets

I.4.2 Les ondes radios

Elles sont utilisées par un grand nombre de réseaux sans fil. A la différence des réseaux utilisant les ondes infrarouges, il faut prendre garde aux perturbations extérieures qui peuvent affecter la qualité des communications dans le réseau, à cause, par exemple, de l'utilisation de mêmes fréquences par d'autres réseaux ou la présence de certains matériaux qui altère la qualité des transferts. Cependant, les ondes radios ont l'avantage de ne pas être arrêtées par les obstacles et sont en général émises de manière omnidirectionnelle.

I.4.2.1 Propagation des ondes radios

Avec un minimum de connaissances sur la propagation des ondes radios, il est possible de mettre en place une architecture réseau sans fil, et notamment de disposer les bornes d'accès (point d'accès) de façon à obtenir une portée optimale. Les ondes radios (RF pour Radio Frequency) se propagent toujours en ligne droite et sont émises de manière directionnelle (exemple: les satellites) ou omnidirectionnelle (exemple: les antennes Wifi).

En pratique, le signal peut être perturbé si une onde radio rencontre un obstacle et la puissance du signal atténuée. L'atténuation augmente avec l'augmentation de la fréquence du signal et/ou de la distance. Et en plus, la valeur de l'atténuation dépend fortement du matériau composant l'obstacle. Par exemple, les obstacles métalliques provoquent généralement une forte réflexion, tandis que l'eau absorbe le signal.

Un signal source peut être amené à atteindre une station ou un point d'accès en empruntant des chemins multiples et parle dans ce cas de multi-path ou, cheminements multiples. Et le délai de propagation entre deux signaux ayant emprunté des chemins différents peut provoquer des interférences au niveau du récepteur car les données reçues se chevauchent. Ces interférences deviennent de plus en plus importantes lorsque la vitesse de transmission augmente car les intervalles de temps entre la réception des données sont de plus en plus courts.

Les chemins de propagation multiples limitent ainsi la vitesse de transmission dans les réseaux sans fil. Pour remédier à ce problème les cartes Wifi et points d'accès sont composés de deux antennes par émetteur. Ainsi, grâce à l'action de l'AGC (Acquisition Gain Controller) qui commute immédiatement d'une antenne à l'autre suivant la puissance des signaux, le point d'accès est capable de distinguer deux signaux provenant de la même station.

Les ondes infrarouges sont utilisées pour :

Les technologies de réseaux sans fil radio sont utilisées pour dans plusieurs modèles cité comme avant:

- Bluetooth
- Wifi
- Le mode « Infrastructure »
- Le mode « ad hoc »

I.5 Le modèle de défaillances dans les systèmes distribués et les réseaux sans fil

I.5.1 Définition d'un système distribué

Un système distribué est un ensemble de plusieurs calculateurs reliés en réseau qui collaborent pour des traitements. Tout système réparti doit assurer la prise en compte des contraintes de sûreté (algorithmique répartie des systèmes et des réseaux, calcul intensif, ...)

Le domaine d'utilisation du système est particulièrement dangereux et met en jeu des vies humaines avec des coûts liés aux pannes qui peuvent être immenses.

1. ***Domaine des transports***

- Conduite automatique de trains.
- Systèmes de contrôle en avionique.

2. ***Domaine de la production d'énergie***

- Conduite de centrales nucléaires.
- Conduite de barrages.

Plusieurs pannes menace les systèmes en généralement on peut le Ranger dans deux classes des pannes :

- Pannes catastrophiques : elles sont inacceptables.
- Pannes non catastrophiques : elles sont acceptables.

I.5.2 Définition: Faute, erreur et faille

Une faille (ou panne) du système se produit lorsque son comportement devient inconsistant et ne fournit pas le résultat voulu. La panne est une conséquence d'une ou plusieurs erreurs. Une erreur représente un état invalide du système du à une faute (défaut). La faute est donc la première cause de l'erreur, cette dernière provoque la faille du système.

I.5.3 Classification des pannes

Il est utile de classifier les pannes selon différents critères. Le schéma suivant vitrine une classification générale selon la durée, la cause ou le comportement d'une panne :

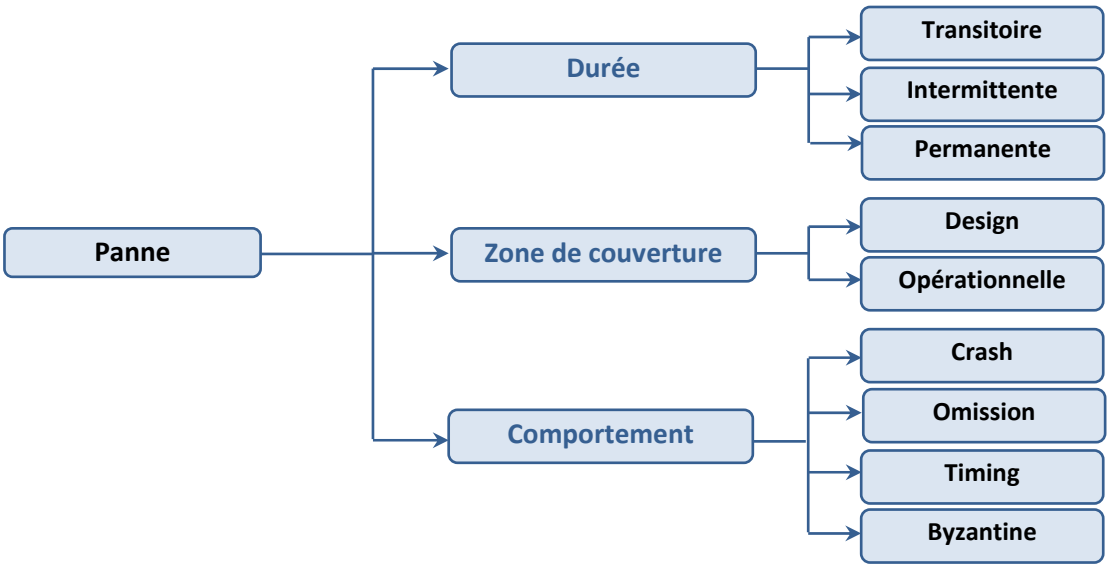


Figure I.6 Classification générale des pannes.

I.5.3.1 Pannes selon durée

Basée sur sa durée, la panne peut être classifiée en :

- ***Transitoire :***

  Conséquence d'un impact environnemental temporaire, elle peut éventuellement disparaître sans aucune intervention. La radiation cosmique est un exemple de panne transitoire.

- **Intermittente** :

  Intermittente est une variante de la panne transitoire, elle se produit occasionnellement et de façon imprévisible. Elle est généralement due à l'instabilité de certaines caractéristiques matérielles ou à l'exécution du programme dans un espace particulier de l'environnement.

- **Permanente** :

  Continue et stable dans le temps, la panne permanente persiste tant qu'il n'y a pas d'intervention externe pour l'éliminer. Un changement physique dans un composant provoque une panne matérielle permanente.

I.5.3.2 Pannes selon la cause

On distingue deux types de pannes selon leur cause :

- **Panne de design:**

  Due à une mauvaise structuration du réseau ou du composant en particulier. En pratique, ce genre de panne ne devrait pas exister grâce aux tests et simulations avant la réalisation finale du réseau ;

- **Panne opérationnelle :**

  Ce sont des pannes qui se produisent durant le fonctionnement du système. Elle est généralement due aux causes physiques. En outre, on peut distinguer, spécialement pour les réseaux de capteurs, trois principales causes:

  - ***Energie :*** l'épuisement de la batterie cause l'arrêt d'un site (capteur par exemple). La consommation d'énergie est très importante pour déterminer la durée de vie d'un capteur, et donc de tout le réseau.
  - ***Sécurité :*** la destruction physique accidentelle ou intentionnelle pas un ennemi peut être une cause de panne. L'absence de sécurité dans les réseaux de capteurs augmente le risque des pannes de ce type.
  - ***Transmission :*** la nature vulnérable de transmission radio, la présence d'obstacles dans les environnements hostiles ainsi que les interférences électriques peuvent être la source d'une faute lors du transfert de données.

I.5.3.3 Pannes selon le comportement résultant

Après l'occurrence d'une panne, on distingue quatre différents comportements possibles du composant concerné :

- **Panne accidentelle (Crash) :**

  Une fois le composant en panne accidentelle ou franche il cesse immédiatement et de façon indéfinie de répondre à toute sollicitation ou de générer de nouvelles requêtes (jusqu'à une réparation).

  Exemple: Panne franche de processeur.

  - Coupure de voie physique.
  - Certains types de programmes.
  - erronés (exemple boucle).
  - Système d'exploitation inter bloqué.
  - Le composant soit, s'arrête complètement de fonctionner ou bien continue mais sans retourner à un état stable (valide).

- **Panne d'omission :**

  En réponse à un événement en entrée un composant ne délivre jamais la réponse attendue (le composant ne peut fournir son service habituel pendant une certaine période se que provoque une perte de quelques données). On d'autres thermes la définition des panne d'omission réside de faite qu'un composant n'est plus capable d'améliorer son service (échec total).

- **Panne de synchronisation (Timing) :**

  Le composant effectue son traitement mais fournit le résultat en retard.

  Exemple:

  - Surcharge d'un processeur.
  - Horloge trop rapide.
  - Délai de transmission trop long.

- **Panne Byzantine :**

  Cette panne est de nature arbitraire. Tout comportement s'écartant des spécifications (principalement en ce que les résultats sont non conformes) est qualifié de comportement byzantin (Lamport). Cette panne est définie par le comportement du composant est donc imprévisible. Du à des attaques très malicieuses, ce type de pannes est considéré le plus difficile à gérer. On distingue quelquefois :

  a) Fautes byzantines "naturelles"

  Les pannes byzantines naturelles proviennent généralement d'erreurs physiques non détectées (mémoire, transmissions réseaux, etc.)

  Exemple:

  - Erreur physique non détectée (sur une transmission de message, en mémoire, sur une instruction).
  - Erreur logicielle amenant une non vérification des spécifications.

  b) Fautes byzantines "malicieuses"

  Les pannes byzantines volontaires proviennent principalement d'attaques visant à faire échouer le système.

  Exemple:

  - Comportement visant à faire échouer le système (sabotage, virus ....).

Notre domaine d'étude est basé sur l'étude de ce type des pannes, il existe d'autres classifications de ce type des pannes.

I.5.4 Classification complémentaire des pannes byzantines

La signature des messages et la vérification de signature dans les systèmes distribués ou dans les réseaux sans fil (authentification et intégrité) entraînent une résistance aux pannes byzantines bien meilleure (surtout pour ce qui concerne les modifications quelconques qui pourraient être effectuées sur les messages du fait de la transmission via des sites malicieux).

De manière plus générale l'usage des fonctions cryptographiques simplifie les protocoles de communication tolérant les pannes byzantines.

On distingue donc parfois:

1) ***La classe des fautes byzantines :*** pour lesquelles les communications sont non authentifiées.
2) ***La classe des fautes byzantines :*** qui apparaissent malgré les signatures ("pannes Byzantines authentifiées").

I.6. Conclusion

Les récents progrès des communications, des technologies informatiques et des technologies électroniques ont permis l'apparition des réseaux sans fil et depuis leur création, les réseaux de communication sans fil ont connu un succès sans cesse croissant au sein des communautés scientifiques et industrielles. Grâce à ses divers avantages, cette technologie a pu s'instaurer comme acteur incontournable dans les architectures réseaux actuelles. Au cours de son évolution, le paradigme sans fil a vu naître diverses architectures dérivées, telles que : les réseaux cellulaires, les réseaux locaux sans fils et autres.

Malgré le succès des réseaux sans fil, il existe toute fois des panne et erreur, nous avons donné quelques exemples, parmi eux les pannes Byzantine, dans le chapitre suivant nous allons expliquer le problème et principe de ce genre de pannes.

Chapitre II.

Le problème des généraux Byzantins

Chapitre II.

Le problème des généraux Byzantins

II.1 Introduction

Le problème de composants défectueux dans un système informatique (ou ailleurs) peut être exprimé de façon abstraite en terme de généraux de l'armée Byzantine qui campent autour d'une cité ennemie (Ce problème est connu dans la littérature comme « les généraux byzantins Problème BGP » [7]). Ne communicant qu'à l'aide de messagers, ceux-ci doivent se mettre d'accord sur un plan de bataille commun, sinon la défaite est assurée. Mais il se peut que l'un ou plusieurs de ces généraux soient des traîtres, qui essayent de semer la confusion parmi les autres. Le problème est donc de trouver un algorithme pour s'assurer que les généraux loyaux arrivent tout de même à se mettre d'accord sur un plan de bataille.

Nous allons donc montrer qu'en utilisant uniquement des messages oraux, ce problème peut être résolu, si, et seulement si, plus des deux tiers des généraux sont loyaux ; ainsi un seul traître peut confondre deux généraux loyaux. Avec des messages écrits non modifiables, le problème peut être résolu pour un nombre quelconque de traître. Tout au long de cette étude nous tenterons de voir les analogies avec les systèmes informatiques.

Avant d'explique ce problème et sa liaison vers les systèmes informatiques nous allons éclaircir un autre sujet qui est la tolérance aux pannes et les techniques de tolérances aux fautes dans les réseaux sans fil.

II.2 La tolérance aux pannes

La conception d'une procédure pour la tolérance aux pannes dépend de l'architecture et des fonctionnalités du système. Cependant, certaines étapes générales sont exécutées dans la plupart des systèmes, tel que c'est illustré dans la figure suivante :

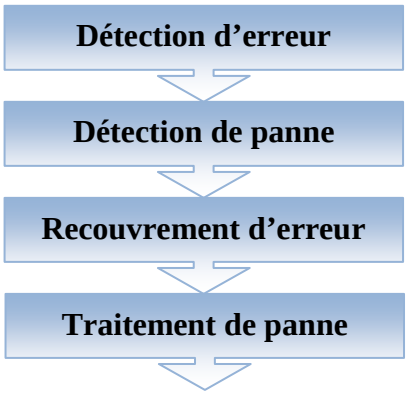


Figure II.1 Procédures de tolérance aux pannes.

II.2.1 Les phases de tolérance aux pannes [09]

II.2.1.1 Détection d'erreur

C'est la première phase de procédures de tolérance aux pannes, dans laquelle on reconnaît qu'un événement inattendu s'est produit. Les techniques de détection de pannes sont généralement classifiées en deux catégories : en ligne et autonome (offline). La détection offline est souvent réalisée à l'aide de programmes de diagnostic qui s'exécutent quand le système est inactif. La détection en ligne vise l'identification de pannes en temps réel et est effectuée simultanément avec l'activité du système.

II.2.1.2 Détention de la panne

Cette phase établit des limites des effets de la panne sur une zone particulière afin d'empêcher la contamination des autres régions. En cas de détection d'intrusion, par exemple, l'isolation des composants compromis minimise le risque d'attaque des composants encore fonctionnels.

II.2.1.3 Recouvrement d'erreur

C'est la phase dans laquelle on effectue des opérations d'élimination des effets de pannes. Les deux techniques les plus utilisées sont « masquage de panne » et «répétition »

- ***Masquage de panne :*** utilise l'information redondante correcte pour éliminer l'impact de l'information erronée ;
- ***Répétition :*** après que la panne soit détectée, on effectue un nouvel essai pour exécuter une partie du programme, dans l'espoir que la panne soit transitoire.

II.2.1.4 Traitement de panne

Dans cette phase, la réparation du composant en panne isolé est effectuée. La procédure de réparation dépend du type de la panne. Les pannes permanentes exigent une substitution du composant avec un autre composant fonctionnel. Le système doit contenir un ensemble d'éléments redondants.

II.3 Les techniques de tolérances aux fautes dans les réseaux sans fil

Les techniques de tolérances ou protocoles tolérants aux pannes peuvent être vus de plusieurs angles différents. On réalise des composants pour tolérer l'une des classes de pannes précédentes. De ce fait, un ensemble de critères est défini pour les classifier.

II.3.1 A quoi sert les techniques de tolérance ?

La tolérance aux pannes a connu une importance considérable parmi les différents domaines de recherche dans les réseaux sans fil; du à leurs contraintes d'énergie, d'environnement et de déploiement. Ce dernier étant d'un coût prohibitif, présente un handicape pour la réorganisation du réseau en cas de panne d'un ou plusieurs de ses sites de réseau sans fil. D'où, il était impératif d'introduire une technique ou un mécanisme de tolérance aux pannes dans tous les protocoles implémentés au niveau des différentes couches de l'architecture réseau sans fil afin de garantir le bon fonctionnement du réseau même après la faille de certains de ses composants.

II.3.2 Classification des techniques de tolérance

Il existe plusieurs techniques de tolérance, ces dernières on peut le classer sous trois catégories différentes distinctes.

II.3.2.1 Classification selon la phase de traitement

Dans cette classification, nous divisons l'ensemble des algorithmes en deux principales catégories préventif et curatif :

- ***Algorithme préventif :***

  Implémente des techniques tolérantes aux pannes qui tentent de retarder ou éviter tout type d'erreur afin de garder le réseau fonctionnel le plus longtemps possible. Cet algorithme applicable si le traitement est effectue avant la panne.

- ***Algorithme curatif :***

  Si le traitement est effectué avant la panne ; on parle donc d'algorithmes curatifs. Elle utilise une approche optimiste, où le mécanisme de tolérance aux pannes implémenté n'est exécuté qu'après la détection de pannes. Pour cela, plusieurs algorithmes de recouvrement après pannes sont proposés dans la littérature.

Exemple :

- Le recouvrement du chemin de routage.
- L'élection d'un nouvel agrégateur...etc.

II.3.2.2 Classification architecturale

Cette classification traite les différents types de gestion des composants, soit au niveau des sites individuellement ou bien sur tout le réseau. Nous distinguons trois catégories principales :

- ***Conservation d'énergie:***

  La première chose à faire lors de la mise en place d'un réseau sans fil consiste à positionner intelligemment les points d'accès selon la zone que l'on souhaite couvrir et de pensé sur l'énergie. Cette catégorie est considérée comme une approche préventive, où les protocoles définissent une distribution uniforme pour la dissipation d'énergie entre les différents sites, afin de mieux gérer la consommation d'énergie et augmenter ainsi la durée de vie de tout le réseau.

- **Gestion de flux :**

  Cette catégorie regroupe les techniques qui définissent des protocoles de gestion de transfert des données. Nous pouvons trouver des approches préventives ou curatives sur les différentes couches (réseau, liaison de données...etc.) telles que :

  - Routage multi-chemin.
  - Recouvrement de route.
  - Allocation de canal.
  - Mobilité.

- **Gestion des données :**

  Les protocoles classés dans cette catégorie offrent une meilleure gestion de données et de leur traitement. Deux principales sous-catégories sont déterminées :

  - Agrégation
  - Clustering

II.3.2.3 Classification selon le niveau d'implémentation

Cette classification permet de répartir les protocoles sur les différentes couches de l'architecture des réseaux sans fil. Ainsi, les algorithmes de routage sont au niveau réseau, les techniques de sélection de canal sur la couche MAC...etc.

II.4 Le problème des Généraux Byzantins

Imaginons que plusieurs divisions de l'armée Byzantine campent autour de la cité ennemie, chacune d'entre elle étant dirigée par son propre général. La seule façon de communiquer dont ils disposent est l'utilisation de messagers. Après avoir observé l'ennemi, ils doivent se mettre d'accord sur un plan d'action commun. Le problème est que certains de ces généraux peuvent être des traîtres, qui tentent d'empêcher les généraux loyaux de se mettre d'accord.

II.4.1 Définition de problème

Le BGP peut être illustré de la façon suivante. Supposons une petite ville est assiégée par l'armé Byzantine, l'armée est organisée dans plusieurs bataillons, chacune commandée par un général. Bien que la ville soit assez petite, elle a un système de défense moderne, de sorte

que la ville ne peut être capturée par l'armée byzantine. Si suffisamment de bataillons attaquent simultanément. Un commandant général envoie des commandes à tous les lieutenants-généraux afin d'organiser une attaque. Malheureusement, certains des lieutenants généraux peuvent être soudoyés par le maire de la ville assiégée, de sorte que ces généraux n'attaquent pas la ville. Spécifiquement, ils envoient des commandes qui peu être en conflit ou des informations à d'autres généraux, afin de contourner toute tentative pour parvenir à un accord sur le plan de bataille. Pire encore, il n'existe aucune garantie que le général commandant est fidèle ou non ?.

Formellement, le problème peut être décrit de la façon suivante :

Supposons que nous avons **n** généraux, où un général est le commandeur (ce général est aussi appelé émetteur). Un protocole pour résoudre le BGP doit satisfaire aux deux exigences suivantes :

- ***Accord:*** Tous les généraux loyaux obéissent à la même ordre, c'est à dire, pour n'importe deux généraux fidèles **p** et **q**, nous avons ***vp = vq.***
- ***Validité:*** Si le général commandant est fidèle, tous les généraux loyaux obéit à l'ordre qu'il envoie, alors, pour chaque générale loyal **p**, nous avons **vp = c**.

Notez que si le commandant est fidèle, alors la première condition découle de la seconde. Évidemment, nous ne pouvons pas poser des exigences sur les généraux qui ne sont pas loyaux, car ils ne sont pas nécessaires pour se conformer n'importe quel protocole des spécifications.

Les généraux doivent donc disposer d'un algorithme pour garantir les deux conditions et que :

A. **Tous les généraux loyaux se mettent d'accord sur le même plan d'action.**

Les généraux loyaux feront tous ce que l'algorithme leur a dits de faire, mais les traîtres peuvent faire ce qu'ils veulent. L'algorithme doit donc garantir la condition A, et ce sans se préoccuper de ce que les traîtres choisissent de faire. Les généraux loyaux ne doivent pas seulement trouver un accord, mais aussi trouver un plan raisonnable.

B. **Un petit nombre de traître ne peut pas faire que les généraux loyaux choisissent un mauvais plan.**

La condition B est difficile à formaliser étant donné qu'elle nécessite de définir ce qu'est un mauvais plan. Nous nous contenterons donc d'étudier la façon dont ils arrivent à se mettre d'accord. Chaque général observe l'ennemi et communique avec ces observations aux autres. Soit *v(i)* l'information communiqué par le $i^{ème}$ général. Chaque

général doit donc utiliser une méthode pour combiner les valeurs *v*(1),..., *v*(*n*) en un plan d'action unique, avec *n* le nombre de généraux. La condition A peut être obtenue si tous les généraux utilisent la même méthode pour combiner les informations, et la condition B peut être obtenue en utilisant une méthode "robuste ". Par exemple, si la décision qui doit être prise est soit *Attaque* ou *Retraite*, alors *v(i)* peut être la décision du général *i* et la décision finale peut être basée sur la majorité de ces décisions.

Des traîtres peuvent modifier cette décision seulement si les généraux loyaux étaient divisés de manière égale quant à la décision à prendre, auquel cas aucune des décisions ne peut être considérée comme mauvaise. Bien que cette approche puissent ne pas être la seule façon de satisfaire les conditions A et B, c'est la seule connue. Elle suppose qu'il existe une méthode qui permette aux généraux de communiquer leurs valeurs *v(i)* aux autres. Une méthode évidente est, pour le $i^{ème}$ général, d'envoyer *v(i)* par messager aux autres généraux. Malheureusement, cela ne fonctionne pas car pour que la condition A soit satisfaite, il faut que tous les généraux obtiennent le même ensemble de messages *v(1),..., v(n)*, et un traître peut très bien envoyer des messages différents à chacun des autres généraux. Pour que la condition A soit satisfaite, il faut que la condition suivante soit vraie :

1. ***Tous les généraux loyaux doivent obtenir les mêmes informations v(1),..., v(n).***

   Cette condition implique qu'un général loyal, ne va pas forcément utiliser la valeur *v*(*i*) reçue de i, puisque si le $i^{ème}$ général est un traître, il a très bien pu envoyer des valeurs différentes à chacun. Cela signifie donc que, si l'on souhaite vérifier la condition 1 et qu'on ne fait pas attention, il est possible que les généraux utilisent une valeur de *v(i)* différente de celle envoyée par i et ce même si le général i est loyal. Il ne faut pas permettre cela si nous souhaitons vérifier la condition B. Nous avons alors de plus la nécessité suivante :

2. ***Si le $i^{ème}$ général est loyal, alors la valeur qu'il a envoyé doit être utilisée par tous les généraux loyaux comme étant v(i).***

Nous pouvons alors réécrire la condition 1 comme ceci (que le $i^{ème}$ général soit loyal ou pas) :

- ***Deux généraux loyaux quelconques utilisent la même valeur pour v(i)…….*** **1'**

Résultat important :

Les conditions **1'** et **2** portent les deux sur une même valeur envoyée par le $i^{ème}$ général. On peut alors restreindre notre étude du problème à : *comment un seul des généraux envoie-t-il sa*

valeur aux autres ? On formulera cela en termes de commandant qui envoie un ordre à ces lieutenants, ce qui nous amène au problème des Généraux Byzantins.

Un Général commandant doit envoyer un ordre à ses n-1 lieutenants, de manière à ce que :

- Tous les lieutenants loyaux obéissent au même ordre…….. IC1
- Si le général est loyal, alors chaque lieutenant doit obéir à l'ordre qu'il a envoyé…..…… IC2

IC1 et IC2 sont connues comme les conditions de consistance interactive (**I**nteractive **C**onsistency conditions). Il faut remarquer que si le commandant est loyal, alors IC2 $\Longrightarrow$IC1.

Ce problème, du point de vue informatique, peut être représenté de la façon suivante :

Soit un réseau de **n** processeurs qui peuvent communiquer les uns avec les autres seulement par le biais de messages, à travers des canaux de communications bidirectionnel, il faut s'assurer qu'un processeur envoie des données aux **n-1** autres processus, de telle façon que :

- Les processeurs fiables reçoivent les mêmes données……. IC1
- Si le processeur émetteur est fiable, alors la valeur reçue est celle qui a été envoyée……. IC2

On voit bien que le problème de non-fiabilité que l'on cherche à résoudre peut alors provenir soit du processeur lui-même, soit de la liaison de donnée. Les deux cas n'ont donc pas à être différenciés. Si une liaison n'est pas fiable, alors le processeur sera considéré comme non fiable. Il faut de plus remarquer que dans le cadre de systèmes informatiques, il est plus probable que des données ne soient pas envoyées, plutôt que fausses.

Note : le mot processeur est employé dans sa définition globale, c'est à dire qu'il s'agit d'une entité effectuant un traitement sur des données, il peut très bien désigner un processeur, un processus, site dans un réseau, ou encore un ordinateur.

II.4.2 La solution impossible

Considérons les deux cas suivants, avec 3 généraux :

Il est impossible pour le Lieutenant 1 de savoir qui est le traître, car dans les deux cas il reçoit les mêmes informations.

Dans le premier cas, pour satisfaire **IC1,** le Lieutenant 1 doit attaquer.

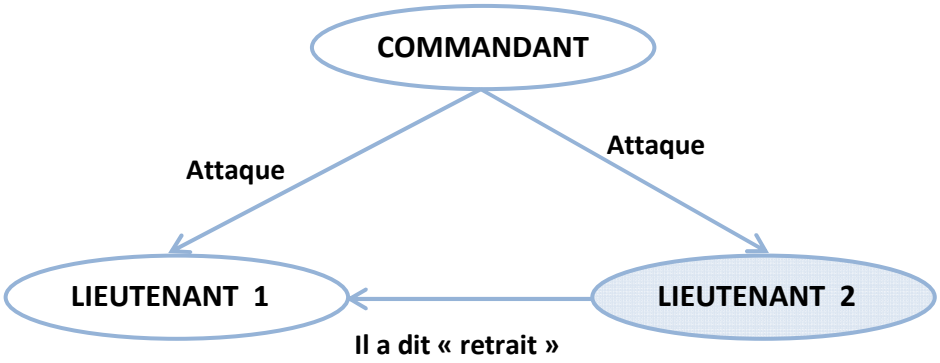


Figure II.2 Le premier cas le lieutenant 2 est un traître.

Dans le deuxième cas, si le Lieutenant 1 attaque, il viole **IC2**.

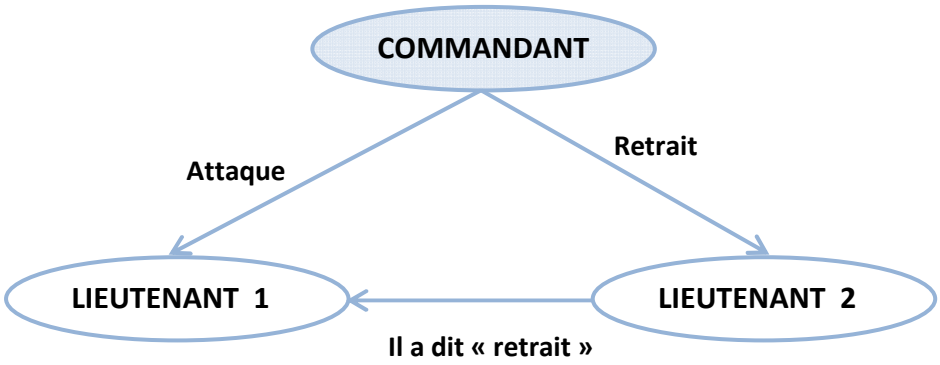


Figure II.3 Le deuxième cas le commandant est un traître.

Donc, il n'existe pas de solutions pour trois généraux en la présence d'un traître. La preuve est en dehors du cadre de ce travail, mais les lecteurs intéressés pas celle ci peuvent se reporter à **[29]**.

Dans la suite de ce chapitre, Examinons maintenant des algorithmes permettant de résoudre ce problème. On note par **n** le nombre total de généraux impliqués dans la communication, et par **m** le nombre de traîtres parmi eux.

II.4.3 La solution avec des messages oraux (n>3m)

Il nous faut tout d'abord définir les suppositions suivantes sur les messages (les remarques entre parenthèses correspondent aux conséquences sur un système informatique) :

S1 : Chaque message envoyé est délivré correctement (pas de pertes de messages).

S2 : Le destinataire d'un message sait qui lui a envoyé (réseau complètement connecté avec liaisons fiables).

S3 : L'absence d'un message peut être détectée (les systèmes doivent être synchrones).

Les suppositions S1 et S2 permettent d'empêcher un traître d'interférer dans une communication entre deux autres généraux et S3 permet d'éviter qu'un traître ne sème la confusion en n'émettant pas de messages.

II.4.3.1 L'Algorithme OM() :

Cet algorithme est appelé OM(m) (**O**ral **M**essage), mais on le trouve aussi sous la forme UM(n, m) (**U**nsigned **M**essage). On suppose qu' :

- ✓ Une valeur par défaut **vdef** est définie pour le cas ou aucun message n'est envoyé par un traître.
- ✓ une fonction **majorité** à été définie telle que : **majorité(v_1, v_2,..., v_{n-1}) = v** si la majorité des valeurs v_i = **v**.

Cas où il n'y a pas de traître (OM(0)):

- o Le commandant envoie **v** à chacun des **n-1** lieutenants.
- o Chaque lieutenant utilise la valeur reçue du commandant ou **vdef** si il n'a rien reçu.

Cas où il y a m traîtres (OM(m)):

- o Le commandant envoie **v** à chacun des **n-1** lieutenants.
- o Pour Chaque Lieutenant$_i$,

  Soit v_i = valeur reçue du commandant ou **vdef** si aucune valeur n'a été reçue

  Envoyer v_i aux **n-2** lieutenants en utilisant **OM(m-1)**
- o Pour chaque **i** & chaque **j** != **i**,

  Soit v_j = valeur que Lieutenant$_i$ a reçue du Lieutenant$_j$ à l'étape (2) ou **vdef** si il n'a rien reçu. Et le lieutenant$_i$ utilise la valeur majorité**(v_1,...,v_{n-1})**.

Exemple:

Nous prenons le cas où **n**=4 et **m**=1 (**OM(1)**) comme nous montre la figure suivante.

Premier cas : le Lieutenant 3 est un traître.

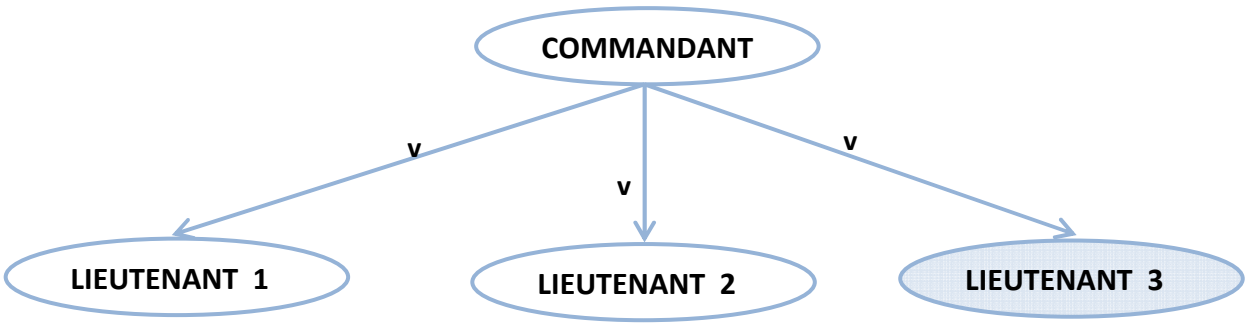


Figure II.4 Exemple de l'algorithme (OM(1)) a l'étape (1) « le Lieutenant 3 est un traître »

A la fin de l'étape (1), on aura les résultats suivants :

Lieutenant 1 : $v_1 = v$

Lieutenant 2 : $v_2 = v$

Lieutenant 3 : $v_3 = v$

Et a la fin de l'étape (3) on aura:

Lieutenant 1 : $v_1 = v$, $v_2 = v$, $v_3 = y$

Lieutenant 2 : $v_1 = v$, $v_2 = v$, $v_3 = x$

Lieutenant 3 : $v_1 = v$, $v_2 = v$, $v_3 = v$

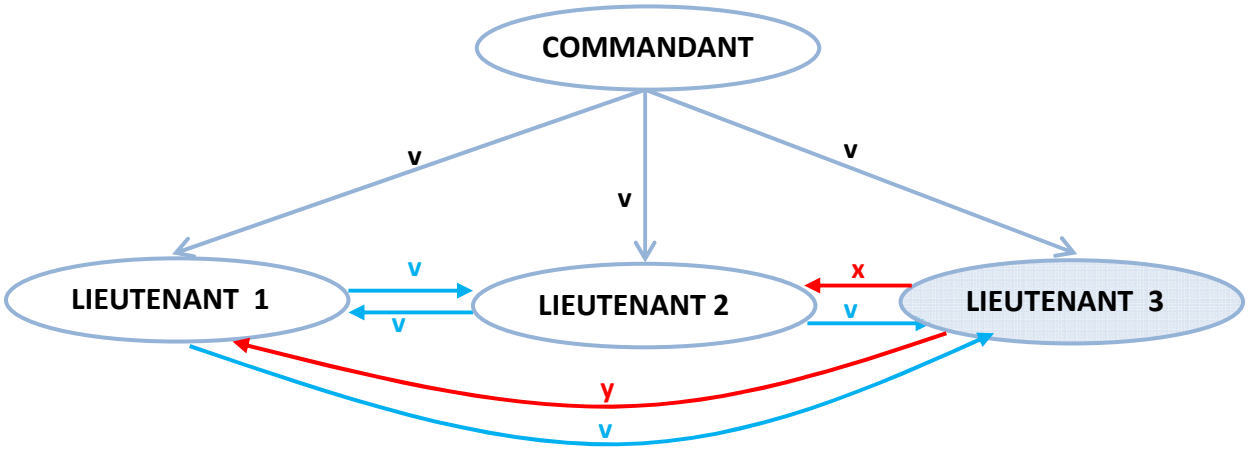


Figure II.5 Exemple de l'algorithme (OM(1)) a l'étape (3) « le Lieutenant 3 est un traître »

Il est possible que x = y, de même qu'il peut s'agir d'une absence de message. A la fin de l'étape (3) chacun des lieutenants a reçu un ensemble de valeurs et arrive à la même décision (**IC1**) ; La valeur envoyée par le commandant est bien la valeur majoritaire (**IC2**).

Le schéma suivant illustre bien les étapes (1) et (2) :

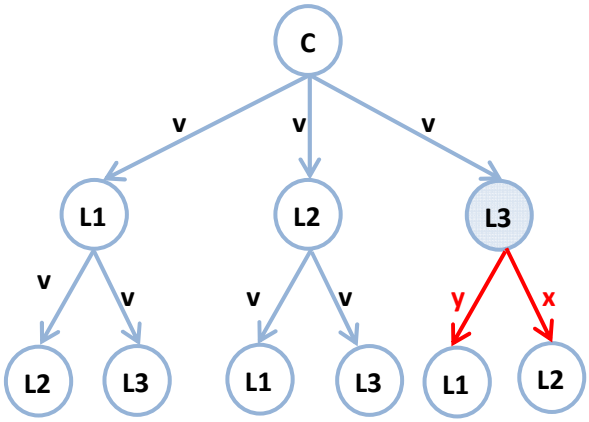


Figure II.6 Exemple de l'algorithme (OM(1)) pour les deux étapes « le Lieutenant 3 est un traître »

Second cas : le commandant est un traître

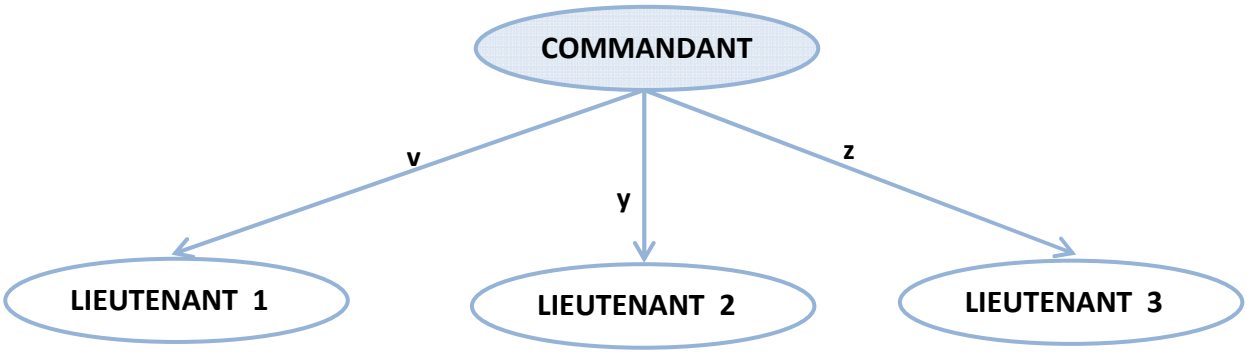


Figure II.7 Exemple de l'algorithme (OM(1)) a l'étape (1) « le commandant est un traître »

A la fin de l'étape (1) :

Lieutenant 1 : $v_1 = x$

Lieutenant 2 : $v_2 = y$

Lieutenant 3 : $v_3 = z$

Et a la fin de l'étape (3) on aura:

Lieutenant 1 : $v_1 = x$, $v_2 = y$, $v_3 = z$

Lieutenant 2 : $v_1 = x$, $v_2 = y$, $v_3 = z$

Lieutenant 3 : $v_1 = x$, $v_2 = y$, $v_3 = z$

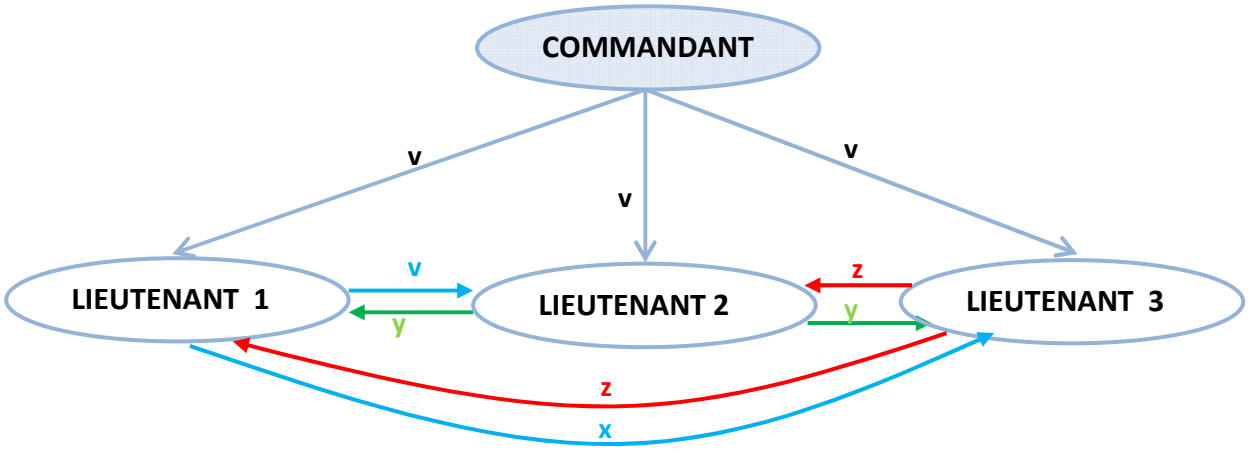


Figure II.8 Exemple de l'algorithme (OM(1)) a l'étape (3) « le commandant est un traître »

A la fin de l'étape (3), les trois lieutenants loyaux ont reçu la même valeur **majorité(x, y, z)** et les contraintes **IC1** et **IC2** sont donc respectées.

Le schéma suivant illustre les étapes (1) et (2) :

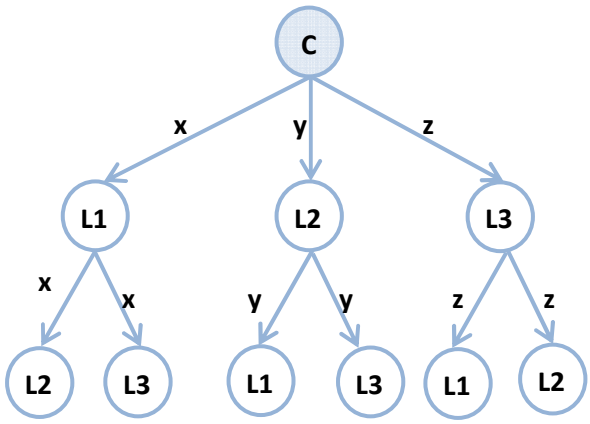


Figure II.9 Exemple de l'algorithme (OM(1)) pour les deux étapes « le commandant est un traître »

II.4.4 La solution de l'algorithme avec m arbitraire

Pour prouver la validité de l'algorithme pour un **m** arbitraire, énonçons tout d'abord le lemme suivant :

Lemme 1 : ***Pour tout m et k, l'algorithme OM(m) satisfait IC2 si il y a plus de 2k+m généraux et au plus k traîtres.***

Démonstration : La preuve se fait par récurrence sur **m**. **IC2** spécifie seulement ce qui doit se passer dans le cas où *le commandant est loyal*. Montrons que le lemme est vérifié pour **m**=0 :
De **S1** il ressort que **OM(0)** fonctionne si le commandant est loyal, c'est à dire que **OM(0)** satisfait bien **IC2**. Supposons maintenant que **OM(m-1)** satisfait **IC1** pour **m>0** et prouvons que c'est vrai pour **m**. A l'étape (1), le commandant loyal envoie une valeur **v** aux **n-1** lieutenants. A l'étape (2) chaque lieutenant loyal applique **OM(m-1)**et par hypothèse nous avons : **n>2k+1** ou **n-1>2k+(m-1)**.
Par récurrence, chaque lieutenant loyal obtient $\mathbf{v_j}$ = **v** de chaque lieutenant loyal **j**. Comme il y a au plus **k** traîtres et que **n-1>2k+(m-1)>=2k** c'est à dire que **k<(n-1)/2**, la majorité des **n-1** lieutenants sont loyaux. Ainsi chaque lieutenant loyal a $\mathbf{v_i}$ = **v** comme majorité des **n-1** valeurs pour i, il obtient **majorité($\mathbf{v_1,...,v_{n-1}}$) = v** à l'étape (3), ce qui vérifie **IC2**. Ce qui nous amène au théorème suivant :

Théorème

Pour tout **m**, l'algorithme **OM(m)** satisfait les conditions **IC1** et **IC2** si il y a plus de **3m** généraux et au plus **m** traîtres.

Démonstration : Encore une fois la preuve se fait en raisonnant par récurrence sur **m**. Si il n'y a pas de traîtres, il est alors facile de démontrer que **OM(0)** satisfait **IC1** et **IC2**. Nous supposons alors que le théorème est vrai pour **OM(m-1)** et prouvons qu'il est vérifié pour **OM(m)**, **m**>0. Considérons tout d'abord le cas où le commandant est loyal. En prenant **k** = **m** dans le Lemme précédent, nous pouvons voir que **OM(m)** satisfait **IC2**. **IC1** est impliqué par **IC2** puisque le lieutenant est loyal, donc nous n'avons en fait qu'à considérer le cas où le commandant est un traître.

Il y a au plus **m** traîtres et le commandant est l'un d'entre eux, donc au plus **m-1** lieutenant sont des traîtres. Puisqu'il y a plus de **3m** généraux, il y a plus de **3m-1** lieutenants, et **3m-1>3(m-1)**. Nous pouvons alors appliquer l'hypothèse de récurrence pour déduire que **OM(m-1)** satisfait **IC1** et **IC2**. Ainsi pour chaque **j**, chaque groupe de deux lieutenants obtient la même valeur pour $\mathbf{v_j}$ à l'étape (3) (cela se déduit par **IC2** si l'un des deux lieutenants est le lieutenant **j**, et par **IC1** dans les autres cas). Ainsi, chaque groupe de deux lieutenants obtient le même vecteur de valeurs $\mathbf{v_1,..., v_{n-1}}$ et obtient donc la même valeur **majorité($\mathbf{v_1,..., v_{n-1}}$)** à l'étape (3), ce qui prouve **IC1**.

Remarque :

- Nombre total de messages : **$O(n^{m+1})$**. (voir **[30]**)
- Les **m+1** étapes d'échange de messages sont une caractéristique fondamentale des algorithmes qui arrivent à un consensus en la présence de **m** éventuels processus déficients.

Le résultat le plus important à retenir, en dehors de l'algorithme, est que le Problème des Généraux Byzantins est solvable si n>3m (dans le cas de l'utilisation de messages oraux).

II.4.5 La solution avec des messages écrits et signes (m quelconque)

La difficulté à résoudre le problème des 3 généraux se trouve dans la capacité d'un lieutenant traître de mentir à propos de l'ordre reçu du commandant, ainsi, si nous pouvons restreindre cette capacité en ajoutant les suppositions suivantes aux trois précédentes (**S1**, **S2** et **S3**), le problème des trois généraux est alors solvable pour un nombre quelconque de traîtres.

S4 : (a) La signature d'un général loyal ne peut pas être imitée, et toute modification du contenu d'un message peut être détectée (un message peut être supprimé, mais pas modifié).
(b) N'importe qui peut vérifier l'authenticité d'un message (personne ne peut tromper un général).

Cela s'applique facilement à des systèmes informatiques par l'utilisation de signatures numériques (souvent associées aux algorithmes de cryptographie moderne).

II.5 Applications aux systèmes informatiques

Nous avons déjà énoncé les conditions **IC1** et **IC2** modifiées afin de s'appliquer à des systèmes informatiques, ainsi que les correspondances avec les suppositions **S1, S2, S3** et **S4**.

Nous avons aussi tenté de montrer à chaque fois le parallèle qui pouvait être fait avec de tels systèmes. Etudions maintenant les domaines d'applications.

L'intérêt d'un tel algorithme dans le domaine informatique est de pouvoir multiplier des processeurs afin de garantir une certaine sécurité dans les systèmes critiques. Par exemple, un système de surveillance d'une centrale nucléaire va nécessiter que les mêmes données soient traitées par plusieurs processeurs différents. Cela dans le but de garantir que si l'un des processeurs venait à souffrir d'un dysfonctionnement, les valeurs qu'il envoie ne soient pas traitées par le système de surveillance.

On voit donc que ce genre d'algorithme a une importance capitale dans le cadre de la mise en œuvre de systèmes informatiques fiables, ou critiques.

On peut remarquer qu'en informatique, un processeur peut très bien générer de manière aléatoire des données, et donc la signature numérique d'un autre processeur. Bien évidemment, cela est fort peu probable et peut être négligé, surtout si on choisit une taille de signature suffisamment conséquente. Une autre remarque est que si les problèmes de dysfonctionnement sont dus à des actions externes comme un humain essayant de corrompre le système, les signatures numériques peuvent alors être remplacées par des systèmes de cryptographie. Il existe une version simplifiée du problème (**Weak Byzantine General Problem**) qui peut être utilisée dans le cadre des bases de données distribuées. Les lecteurs intéressés peuvent se reporter à **[31]**.

- **Problèmes, critiques**

Ces algorithmes proposent bien une solution au Problème des Généraux Byzantins, néanmoins, quelques problèmes restent posés, principalement dans le cadre de leur mise en œuvre dans les systèmes informatiques existants.

La première remarque à faire est le nombre important de messages générés par de tels algorithmes. Mais cela est dû à la complexité du problème et ne peut malheureusement pas être réduit.

Il est bien sûr possible de faire quelques suppositions supplémentaires tel que, en informatique, il est plus probable qu'un composant tombe en panne, plutôt que se mette à envoyer des données corrompues. Mais si l'on cherche à mettre en œuvre des systèmes réellement fiable, alors de telles suppositions n'ont pas lieu d'être.

En conclusion, ces solutions ne sont applicables que dans des systèmes spécifiquement prévus à cet effet (du fait de la topologie), mais aussi où la performance a moins d'importance que la fiabilité. En effet ces algorithmes sont excessivement consommateurs de ressources (processeur et réseau).

II.6 Topologies de réseau

Dans les sections précédentes, nous avons seulement discuté du Problème des généraux Byzantine sous l'hypothèse que chaque générale peut envoyer un message à tous les autres généraux. Autrement dit, la topologie du message sous-jacent dans la transmission système de Sion était supposée être un graphe complet. Dans les grandes conçoit qu'il n'est

pas réaliste que chaque périphérique (général) est connecté à un autre appareil, si le nombre de composants **n** augmente linéairement, alors le nombre de nécessaire des liens de communication est $\binom{n}{2} = n(n-1)/2$ augmente quadratiquement.

En pratique, il est donc important de réduire le nombre des l'indépendantes voies de communication à charge. Maintenant, la question se pose s'il est possible de résoudre les problèmes généraux byzantins dans les topologies de réseau autres que graphiques complètes.

De toute évidence, une condition nécessaire pour la solvabilité de problème byzantine généraux est que le graphe sous-jacent est connecté (sinon, le graphe contient au moins deux composants qui ne peuvent communiquer les uns avec les autres, dans le cas contraire ont na pas les moyens de coordonner leurs plans d'attaque). Cependant, la connectivité n'est pas suffisante, comme nous montre la figure II-6 (a). Où le graphe contient deux composantes, reliées par « un pont » entre les deux généraux P1 et P2, il n'ya pas d'autres chemins de communication entre les composants graphique. Cette configuration ne peut même pas tolérer un échec, comme le général p1 ou P2 peut gêner à chaque tentative de parvenir à un consensus, si elles agissent d'une manière déloyal.

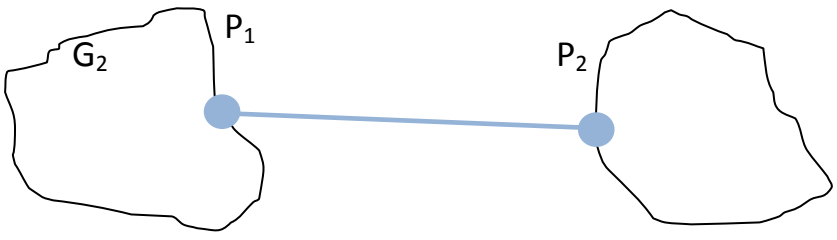
Il s'avère que le paramètre critique de la communication est le graphe de connectivité nœud. On note **Con(G)** le nœud connective du graphe G.et ce denier a un nœud-connectivité k, si il ya au moins k chemins disjoints de la communication entre chaque paire de nœuds dans le graphe. Dolev [2] a montré le résultat fondamental suivant:

Proposition :

Le compte tenu d'un réseau de communication avec graphe G, le problème byzantines généraux peuvent être résolus si et seulement si con(G) ≥ 2m +1.

En d'autres termes, le nombre de généraux déloyal doit être inférieure de la moitié du nœud connective d'un réseau. Pour mettre en œuvre de ce résultat, considérons le scénario du pire cas représenté dans la figure II-6 (b). Supposons que le graphe est constitué de deux sous-graphes G1 et G2, reliés par un pont, formé par un ensemble de généraux. Dans le pire des cas, tous les généraux déloyaux sont présents seulement dans le pont. Chaque message d'un général en G1

(a)



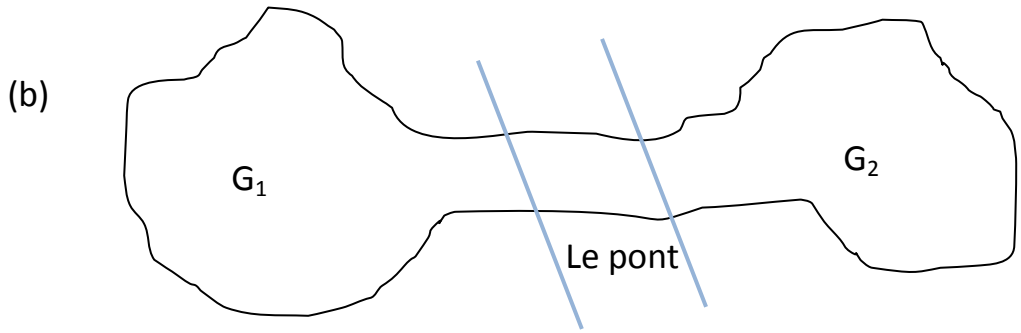


Figure II.10 Les différentes topologies réseau.

Pour s'adressé à un général dans G2 doit passer le pont. Si les généraux sur la collusion déloyale pont, ils peuvent changer tous les messages de G1 à G2 pour avoir une valeur spécifique et chaque message de G2 à G1 pour mener une valeur différent. Ce portement peut causer les généraux dans G1 pour s'entendre sur une différente valeur que ceux dans G2. Pour contrecarrer cette attaque, le pont doit être suffisamment « large » pour que les données qui passe à travers seront assez non modifiable. Cette observation donne naturellement à proposition précédente.

II.7 Conclusion

Généralement, les échecs peuvent avoir plusieurs formes. Pour l'exemple, l'un des périphériques du système peut refuser de délivrer les informations nécessaires à d'autres parties du système. Pire encore, l'appareil peut envoyer des informations conicine et incohérentes à d'autres parties du système. Ces échecs sont appelés « byzantine échecs » et dans ce chapitre on a examiné le problème byzantines généraux (BGE), telle que posée par Lamport, Pease et Shostak en 1982. Dans ce problème, n généraux assiéger une petite ville de besoin pour atteindre un accord sur un plan de bataille, même si les généraux sont m déloyal et essayer de subvertir le régime. Le BGP est communément accepté comme un moyen naturel de défaillances du modèle dans un système distribué et les réseaux sans fil.

Chapitre III.

Présentation d’un modèle pour le comportement contradictoire

Chapitre III.

Présentation d'un modèle pour le comportement contradictoire

III.1 Introduction

Ce chapitre traite une question importante dans les réseaux sans fil : la sécurité. Une revue littéraire des travaux de recherches mène bien pour répondre à ce problème. En résumé, ce chapitre aborde les sujets suivants:

- Introduction au problème de comportement Byzantin comme initialement introduite par Lamport et Al [11].
- La tolérance aux fautes Byzantin dans les réseaux sans fil : dans ce cas on va s'appuyer dans notre travail sur le problème des généraux Byzantins (ou de diffusion sécurisé) dans le modèle standard dans lequel la communication est disponible par paire entre toutes les parties du réseau.

III.2 Comportement Byzantin

III.2.1 Définition d'un comportement Byzantin

Dans les réseaux sans fil [11, 12, 13], le terme se réfère à « Byzantin » certains nœuds dans le réseau qui présentent un comportement anormal, plus précisément, il traite deux types d'un tel comportement:

- ***Disfonctionnement :*** Dans ce cas, les nœuds pourraient fonctionner incorrectement à cause d'une panne de courant ou d'une mauvaise configuration.
- ***La malice*** : malicieux, les nœuds pourraient fournir des informations incorrectes, mentir sur les informations de routage, la discrimination entre les différents types de trafic en envoyant quelques-uns et ignorer les autres. Il est supposé que les nœuds malveillants peuvent perturber le réseau de différentes manières tout en restant inaperçus.

Le concept de comportement Byzantin a été introduit pour la première fois par Lamport et Al [11], et dans laquelle ils ont appelé le «Problèmes Byzantins Généraux", ci-dessous est un résumé du problème, une description de la façon dont elle a été initialement adressée, et le suivi des citations.

Lamport et Al [11] sont les premiers à travailler pour résoudre le problème du consensus dans les systèmes distribués, en la présentant en termes d'une histoire connue sous le nom « Byzantin Problème Généraux ». Brièvement, dans ce problème, il y a un certains nombres de processeurs « n », connu sous le nom « des généraux ». Ils forment un réseau maillé de telle sorte que toute paire de généraux peuvent communiquer en privé par le biais des canaux appelés «messages oraux». L'un des généraux est supposé avoir un rôle particulier (commandant), en ce qu'il envoie une valeur binaire (Commande) pour les n-1 généraux, appelés lieutenants. La valeur binaire correspond à «Attaque» ou «retraite».

L'idée est que certains des généraux, y compris le commandant, pourraient être traîtreux. Un général félon peut présenter d'une manière sournoise, comme en omettant d'envoyer des messages, d'envoyer des messages malformés, l'envoi de messages falsifiés, ou en envoyant messages contradictoires aux différents nœuds. Cependant, le comportement souhaité est que les généraux honnêtes (non défectueux processeurs) sont censés parvenir à un accord avec les trois conditions suivantes:

- Terminaison: Finalement chaque général honnête fixe sa décision.
- Accord: la valeur de décision est la même pour tous les généraux honnêtes.
- Intégrité: si le commandant est honnête, puis tous les généraux honnêtes décider de la valeur que le commandant initié.

Le concept a été apprécié par la communauté informatique et inspiré ses membres pour générer des centaines d'articles et des thèses. Certains des résultats sont résumés comme suit:

- Aucune solution n'existe si le nombre des généraux honnêtes est inférieur ou égal à 2/3 du nombre total des généraux [14].
- Si des défauts « t » sont tolérées, moins de « t » rondes sont nécessaires pour toute détermination de l'algorithme [15].
- Dans un système asynchrone, le problème est insolvable [16].

En conséquence de ces résultats, apportant la notion de consensus aux réseaux semblent plus difficile parce que les réseaux ne sont pas entièrement connecté et la communication dans la réalité est asynchrone, pour ne pas mentionner que l'information soit livrée n'est pas aussi simple que l'attaque ou la retraite. La section suivante montre comment un tel réseau peut être conçu et mis en œuvre avec l'existence de nœuds byzantins.

III.2.2 La sécurité et le comportement Byzantin

Le comportement Byzantins est habituellement utilisé dans le contexte de la sécurité. Cependant, la distinction entre les deux doit être claire. Les modèles de défaillance Byzantins ne sont pas développait à l'origine pour faire face aux attaques malveillantes.

Le comportement Byzantins n'aborde pas la question de la confidentialité des données, c'est à dire, la confidentialité des données, l'intégrité et l'authentification. En effet, les algorithmes Byzantins nécessitent la réplication du message, ce qui signifie que les données confidentielles peuvent être exposées à un risque. La clé est la seule solution pour le secret des données est d'impliquer les modèles de cryptographie.

Les modèles Byzantins et les modèles de sécurité doivent être utilisés comme un seul composant d'un système solide qui assure la survie du réseau et la confidentialité des données.

III.2.3 Les niveaux de robustesse

Tous les réseaux sont exposés à des défaillances suite à des nœuds corrompus ou à des liens de communication déconnectés. Avec les nœuds Byzantins, les échecs se produisent en raison des fonctionnements anormaux, qu'ils soient délibérés ou non. L'algorithme de robustesse peut être classé dans les quatre niveaux suivants:

III.2.3.1 Les échecs simples

Certains réseaux ignorent la possibilité de défaillance d'un nœud. En conséquence ces réseaux continuent à fonctionner a l'existence de nœuds, mais avec un fonctionnement

incorrecte. Cette situation rend les tâches d'entretien compliqué d'où le manuel d'intervention est nécessaire pour amener le réseau à nouveau.

III.2.3.2 Stabilisation Auto

Les algorithmes de cette catégorie montrent une légère amélioration par rapport à la catégorie précédente. Ils garantissent l'exactitude tant que le réseau est libre de disfonctionnement des nœuds, qui peut être réalisé qu'après ces nœuds sont supprimés.

III.2.3.3 Détection de comportement Byzantin

Les algorithmes conçus avec cette propriété ne sont pas capable de travailler correctement avec l'existence de nœuds Byzantins, mais ils identifient facilement un nœud corrompu. En combinant cette propriété avec l'auto-stabilisation pour améliorer la robustesse de ces algorithmes.

III.2.3.4 Robustesse Byzantines

Cette propriété exige le plus haut niveau du réseau. Robustesse: un réseau continu à fonctionner correctement même avec l'existence de mauvais nœuds. Cependant, la détection Byzantine n'est pas nécessairement atteinte.

Récemment, un certain nombre de documents, tels que [12,13,17,18], ont montrés la nécessité de l'intégration d'un algorithme, tels que le routage, avec la robustesse Byzantines pour atténuer les attaques internes et donc d'assurer l'interopérabilité du réseau à tout moment. Yu et Al dans [17], ont sécurisés leur algorithme de routage interne et externe contre l'attaques (Byzantine). Plus précisément, les fonctions cryptographiques asymétriques sont utilisées pour défendre contre les attaques externes. Ces fonctions supposent que chaque nœud possède des clés (public / privé) paire. Les nœuds trouvent leurs voisins grâce à la découverte de route signée par messages. Ensuite, chaque nœud crée un ensemble de clés partagées, qu'il peut utiliser avec différents nœuds à différents niveaux - 1-hop, 2-hop, ou plus. Ils se défendent contre une attaque Byzantine en utilisant le message et la redondance de route. Une fois la phase de découverte de l'itinéraire, un itinéraire peut être sélectionné parmi les itinéraires disjoints. Au pire, un nœud compromis peut déposer des paquets, mais en raison de la redondance des paquets, la destination s'attend à recevoir le même message de nœuds différents et de ne pas recevoir à partir d'un certains nœuds qui suggèrent un comportement Byzantin.

Un message est diffusé en amont et en aval pour laisser à la fois, la source et la destination se renseigner sur tous les nœuds malveillants et chaque nœud construit un référentiel de confiance local pour les nœuds qu'il connaît, sur la base des observations de comportement.

En conséquence, un chemin contenant un nœud avec une valeur de confiance faible est exclu.

Maintenant, on passe à la deuxième partie de ce chapitre qui est réservée à l'étude de la diffusion sécurisée dans les réseaux sans fil, en présence d'un adversaire Byzantin. Mais avant d'entrer dans le sujet, il est nécessaire de définir quelques points importants et fournit la première analyse de la diffusion dans les réseaux sans fil, sécuriser le cas des adversaires Byzantins.

Nous notons que la diffusion sécurisée est impossible dans la présence d'un adversaire puissant. Pour contourner cet obstacle, nous faisons l'hypothèse suivante: il existe un calendrier pour le préfixe aux joueurs de communiquer et que tout le monde (y compris les corrompus) adhère à ce calendrier. Sous cette hypothèse, nous donnons un protocole de diffusion simple qui est t sûr, chaque fois que l'adversaire à corrompu le maximum de voisins (environ ¼ fraction p) d'un joueur honnête. D'autre part, nous montrons qu'il est impossible d'atteindre la diffusion sécurisée lorsque l'adversaire corrompe (environ une fraction $\frac{1}{P}$) les voisins d'un joueur honnête.

III.3 Les problèmes de Broadcast

Broadcast est l'un des problèmes les plus fondamentaux en matière de communication réseau. Dans ce problème, il est un acteur dans le réseau, le concessionnaire, qui a besoin d'envoyer un message à tous les autres joueurs. Le défi consiste à mettre en place un canal de diffusion à partir des primitives les plus faibles, sous réserve de certaines contraintes ou des paramètres de performance. Le problème des généraux Byzantins est de minimiser la latence de diffusion dans les réseaux sans fil.

III.4 La diffusion sécurisée

Diffusion sécurisée (également connue sous le nom de problème des généraux Byzantins (*Byzantine Generals Problem*)). Introduite par Pease, Shostak et Lamport, le problème est défini comme suit: il y a « n » joueurs et l'un d'eux, le concessionnaire est titulaire d'une entrée « m ». Aussi, il y a un adversaire avec la puissance de calcule illimitée (un adversaire Byzantin « a Byzantine Adversary ») qui peut corrompre les joueurs à « t » joueurs. Un joueur corrompu peut se comporter d'une façon arbitraire. En fin de compte, tous les joueurs honnêtes doivent s'entendre sur une valeur commune. Si le concessionnaire n'est pas corrompu, alors la valeur commune doit être égale à « m ».

Dans le modèle standard de communication où seuls les paires sont disponibles, Pease, Shostak et lamprt [14] montrent que la diffusion est possible si et seulement si t $<\frac{n}{3}$. Des efforts ont été faits pour étendre le modèle standard pour tolérer un plus grand nombre de joueurs corrompus. Fitzi et Maurer [19] montrent qu'avec deux canaux en fonte (où diffuser un message à tout sous-ensemble de deux joueurs), une diffusion est possible si et seulement si t $<\frac{n}{2}$. Considine, Levin et Metcalf [20] d'étende en général le résultat à la k-cast canaux. En particulier, ils montrent que la diffusion est possible si et seulement si t $<\frac{k}{k+1}n$. Amitanand, sanketh, Srinathan, Vinod et Rangan [33] Étudie le cas où les réseaux locaux sont présents (joueurs partageant le même réseau LAN peuvent envoyer des messages multicast les uns aux autres) dans l'addition des canaux par paire.

III.5 Minimiser la latence dans les réseaux de diffusion de radio

Dans les réseaux sans fil, chaque joueur peut multicast un message à tous les joueurs au sein de rayon « r ». Dans la littérature [21.22.23.24.25], la plupart se concentre sur la réduction des temps de latence de diffusion dans les réseaux sans fil. Les délais de transmission arrivent par le fait que si deux joueurs multicast des messages simultanément, puis un joueur dans le rayon des deux joueurs ne peut rien recevoir a cause de bruit. Comme noté dans [26], il n'y a pas beaucoup de résultats qui sont connus sur les réseaux sans fil avec la présence de failles. Pagani et Rossi [27] étudie les cas où une panne passagère peut apparaître. Kranakis, Krizanc et Pelc dans [26] considèrent l'effet d'un adversaire passif (un joueur ne sera pas corrompu d'envoyer ou de recevoir aucun message) sur la latence de diffusion est moins.

III.6 Présentation du modèle

Comme noté avant, les travaux [21.20.19] ont été faits pour étendre le modèle standard pour les problèmes des généraux Byzantins, en supposant le multicast-canaux. Dans les réseaux sans fil, un joueur ne peut communiquer qu'aux joueurs au sein d'une distance fixe. A notre connaissance, la diffusion dans les réseaux sans fil en présence d'un adversaire Byzantin n'a pas été étudiée avant, et dans cette partie on présentera les grands axes pour la mise en œuvre à un tel problème.

Nous allons définir formellement le problème et décrire les résultats déjà obtenu ci-dessous, mais avant d'entamer ce point, nous allons donner une brève explication du modèle contradictoire.

Dans le modèle standard, un joueur corrompu par un adversaire byzantin peut se comporter d'une manière arbitraire. Toutefois, ce modèle accusatoire est trop fort dans le cas des réseaux radio. S'il n'y a pas de restriction sur la façon dont un joueur peut avoir un comportement corrompu, il peut continuer à envoyer du bruit de sorte qu'aucun joueur honnête dans le rayon peut envoyer / recevoir un message. Pour éviter ce genre d'attaque, nous plaçons la restriction suivante:

Il existe un calendrier préfix pour permettre aux joueurs d'envoyer des messages à tour de rôle afin qu'il n'y ait pas de collision messages, un joueur corrompu ne pouvait envoyer un message lorsque son tour viendra. Comme bondissant les retards de transmission n'est pas notre préoccupation dans ce cas, il suffit d'utiliser un calendrier naïf. Autre que cette restriction, un joueur corrompu peut s'écarter forme de protocole prescrit d'une façon qu'il veut.

Au lieu de la délimitation du nombre total des joueurs corrompus, on s'intéresse à la délimitation du nombre de joueurs corrompus dans le rayon des joueurs honnêtes. Cela pourrait être considéré comme la modélisation de la situation où les joueurs corrompus sont distribués de manière uniforme à travers le réseau. Par ailleurs, délimitant le nombre total de joueurs corrompus ne seront pas très intéressant, car un adversaire peut simplement corrompre tous dans le rayon d'un joueur en particulier honnête (le nombre total sera une constante indépendante du nombre de joueurs).

III.6.1 Définition du problème

Dans ce qui suit nous considérons une grille carrée dont chaque point intégrale (x, y) représentent un joueur par p(x, y). Pour éviter l'anomalie du cas limité, la grille carrée est de

taille infinie. Chaque joueur a accès à un canal de diffusion de radio de rayon r. Un joueur de p (x, y) peut multicast un message à tous les joueurs dans un formulaire distance de r à (x, y). Nous appelons ces joueurs les voisins de p (x, y). Nous notons que chaque joueur a πr^2+E(r)-1 voisins où |E(r) |≤ $2\sqrt{2\pi r}$ (Gauss [28] montre que le nombre de points entiers à l'intérieur des limites d'un cercle de rayon r centré à l'origine). Nous supposons que le réseau est synchrone et qu'il existe un calendrier (schediling) préfixe qui permet aux joueurs d'envoyer des messages à tour de rôle afin qu'aucune paire de voisins de n'importe quel joueur va envoyer des messages dans le même tour. Un exemple de calendrier, pourrait être le suivant: A joueur p(x, y) envoie un message seulement à leur tour *(x mod (2r +1)) * (2r +1) + (y mod (2r +1)) mod (2r + 1)* ^{2} et le schedule (calendrier ou le programme) répète chaque $(2r+1)^2$ tours.

Un joueur peut être corrompu par un active et par l'ensemble puissant d'adversaire. Un joueur qui n'est pas corrompu est un joueur honnête. Pour chaque joueur honnête, l'adversaire peut corrompre jusqu'à « t » de ses voisins. Un joueur corrompu peut déroger au protocole prescrit d'une manière arbitraire, sauf qu'il peut envoyer un seul message lorsque son tour viendra. Il ya un joueur spécial, connu sous le nom revendeur, qui multicast un message « m » à ses voisins au début.

L'objectif est de parvenir à diffuser dans la présence d'un tel adversaire et nous disons que la diffusion est atteinte si tous les joueurs honnêtes finiront de recevoir et accepter « m ».

III.6.2 Résultats

Nous enquêtons quand il est possible d'obtenir la diffusion et nous montrent la partie supérieure suivante et les bornes sur t:

- Pour t < $\frac{1}{4}r\left(r+\sqrt{\frac{r}{2}}+1\right)-2$, nous donnons un protocole simple qui peut atteindre la diffusion (en supposant que $\sqrt{\frac{r}{2}}$ est un entier).
- Pour t ≥ [$\frac{r}{2}$ (2r +1)], nous montrons qu'il est impossible d'atteindre la diffusion (ceci est valable pour tout r entier).
- Combinassions de ces derniers, avec le fait que chaque joueur honnête à πr^2 + E (r) -1 voisins (Q (E (r)) = r), on note que pour r grand (plus large), la diffusion peut être atteinte que si une corrompt adversaire a moins d'une fraction de voisins d'un joueur

honnête, d'autre part, la diffusion ne peut être atteinte que si ya une corrompions adversaire d'un $\frac{1}{\pi}$ fraction de voisins d'un joueur honnête.

Les résultats ci-dessus sont pour la métrique L_2. Sont aussi les mêmes résultats obtenus pour les métriques L_1 et L_∞ dans cette phase. Nous montrons que pour la métrique L_1, ou la diffusion peut être atteinte si $t < \frac{1}{4} r\left(r + \sqrt{\frac{r}{2}} + 1\right) - 2$ et elle ne peut être atteinte que si $t \geq [\frac{r}{2}(r+1)]$; et pour les L_∞ métrique, la diffusion peut être atteint que si $t < \frac{1}{2} r\left(r + \frac{r}{2} + 1\right)$ et ne peut être atteint que si $t \geq [\frac{r}{2}(2r+1)]$.

Remarque

La distance entre deux points (x_1, y_1) et (x_2, y_2) est définie comme suit :

- $\sqrt{(x_1 - x_2)^2 + (y_1 - y_2)^2}$ pour la métrique L_2
- $|x_1 - x_2| + |y_1 + y_2|$ pour la métrique L_1
- $\{|x_1 - x_2|, |Y_1 - Y_2|\}$ pour L_∞

Maintenant, nous allons discuter notre protocole de la diffusion et de donner nos résultats de la borne inférieure et on terminera dans les deux cas par en prouver la valeur de la transformation du problème de la métrique L_2 aux métriques L_1 / L_∞.

III.7 Le protocole de diffusion

Comme indiqué précédemment dans la section II.5.1 (la définition du problème), nous supposons que nous avons un calendrier préfixe pour permettre aux joueurs d'envoyer des messages à tour de rôle afin qu'il n'y ait pas de collision message. Dans la suite, lorsque nous disons qu'un joueur multicast un message « m », nous voulons dire la « m » joueur de multidiffusion à son tour disponible suivant.

III.7.1 La description du protocole

1. Le croupier multicasts le message « m » à ses voisins.
2. Si un joueur est un voisin du croupier, après avoir reçu le message « m » à partir du croupier, accepte « m » et les multidiffusions « m » à ses voisins et se termine le protocole.
3. Si un joueur n'est pas un voisin du croupier, après avoir reçu une copie « t+1 » d'un message « m » à partir de « t +1 » voisins distincts, « m » accepte et les multidiffusions « m » à ses voisins et se termine le protocole.

III.7.2 Analyse

Dans le troisième théorème qu'on va voir après dans ce chapitre, on va montrer que le protocole ci-dessus peut atteindre la diffusion dans la métrique L_∞ si l'adversaire peut corrompre au plus $t < \frac{1}{4}r\left(r + \sqrt{\frac{r}{2}} + 1\right)$ voisins d'un joueur honnête. Ensuite, nous allons montrer comment réduire le problème dans la métrique L_1 à la métrique L_∞ en théorème 6, et de la métrique L_2 à L_1 dans le théorème 7. Tout au long de cette analyse, nous supposons que $\sqrt{\frac{r}{2}}$ est un entier.

Sans perte des généralités, supposons que le concessionnaire est à (0,0). Nous noterons « m » le message envoyé par le concessionnaire dans la première étape de notre protocole, l'ensemble des joueurs { p(x, y): $x_1 \leq x \leq x_2 \wedge y_1 \leq y \leq y_2$} comme p[$x_1 \ldots x_2, y_1 \ldots y_2$]. Lorsque $x_1 = x_2$, nous allons simplement écrire p[$x_1, y_1 \ldots y_2$]. De même, quand $y_1 = y_2$, nous allons écrire p[$x_1 \ldots x_2, y_1$]. Il faut signaler que la relation de voisinage est symétrique, c'est-à-dire si p' est voisin de p, alors p est voisin de p'. A noter également que suivant notre protocole, un marchand corrompu ne pouvait nuire à ses voisins honnêtes ne considérera que le premier message diffusé par le concessionnaire. Dans notre analyse on considère que le concessionnaire est honnête. Avant de traiter le théorème n°3, on définira certaines propriétés de base du protocole.

Lemme 1 : ***Si un joueur honnête accepte un message m', alors m' = m.***

Démonstration : on suppose le contraire, qu'il y a certains joueurs honnêtes qui acceptent des messages différents de m. soit p le premier joueur honnête qui accepte un message différent m'. p ne peut pas être un voisin du croupier depuis d'un voisin du croupier qui acceptera seulement m.

Par conséquent, p a reçu t +1 copies de m' par t+1 voisins différents. Depuis au plus t voisins peut être corrompu, au moins un et un seul joueur honnête accepte et diffuse « m' » avant p. cela viole la définition de p.

Lemme 2 : ***Pour un joueur honnête p, s'il existe un ensemble de pays voisins S tels que |S| ≥ 2t+1 et tous les joueurs honnêtes en S ont accepté m, alors p sera éventuellement accepter m.***

Démonstration : Il ya au moins t +1 joueurs honnêtes dans le S. par la nature du protocole, p sera éventuellement accepter m

III.7.2.1 Théorème 03

Si t $< \frac{1}{4} r \left(r + \sqrt{\frac{r}{2}} + 1 \right)$ alors le protocole de diffusion peut atteindre dans la métrique L_∞.

Démonstration : on a dans la métrique L_∞, l'ensemble des voisins d'un joueur p (x, y) est égale à p[x-r…x+r, y-r…y+r]. Pour prouver le théorème 3, il suffit de prouver que pour tout entier positif « n », tous les joueurs honnêtes dans p[-n…n, -n…n]. Finiront par accepter m.

- Cas de base:

  Lorsque n ≤ r, l'énoncé est ordinairement vrai.
- L'hypothèse d'induction:

  Tous les joueurs honnêtes dans p[-n…n, -n…n] finiront par accepter m.
- La marche de l'introduction:

  Nous allons partitionner l'ensemble p[n+1,0…n+1] en deux sous-ensembles et affirment que tous les joueurs honnêtes dans chaque sous-ensemble finiront par accepter m dans les lemmes suivants :

  - p[n+1,0…n-$\sqrt{\frac{r}{2}}$] (Suit lemma4)
  - p[n+1, n-$\sqrt{\frac{r}{2}} + 1$…n+1](Lemme 5)

La raison pour laquelle nous divisons la preuve en deux lemmes séparés parce que la preuve du dernier lemme dépend du résultat de la première.

Par symétrie et l'hypothèse d'induction, on pourrait conclure que tous les joueurs honnêtes dans p[-(n+1)…(n+1), -(n+1)…(n+1)] et finiront par accepter m.

Définir les ensembles S_0, S_1 ……$S_{\sqrt{\frac{r}{2}}}$ comme nous l'a schématise la figure suivante :

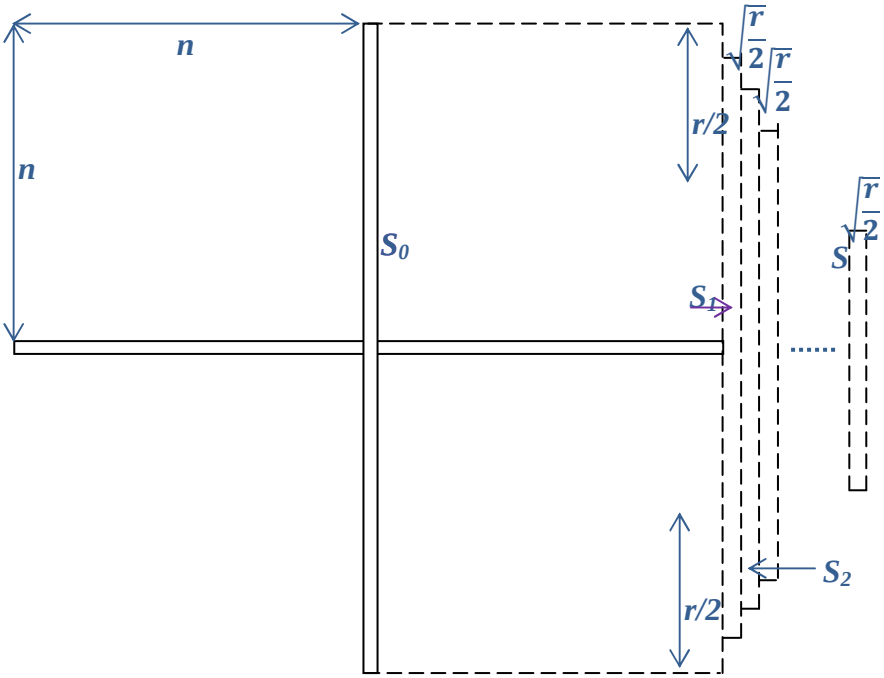


Figure III.1 L'ensemble S_0, S_1 ……$S_{\sqrt{\frac{r}{2}}}$

On a:

$$S_0 = \text{p[0…n, -n…n]}$$

$$S_1 = \text{p[n+1, -(n-}\sqrt{\frac{r}{2}}\text{)… (n-}\sqrt{\frac{r}{2}}\text{)]}$$

$$\vdots$$

$$S_i = \text{p[n+i, -(n-}\ i\sqrt{\frac{r}{2}}\text{)… (n-}\ i\sqrt{\frac{r}{2}}\text{)]}$$

$$\vdots$$

$$S_{\sqrt{\frac{r}{2}}} = \text{p[n+}\sqrt{\frac{r}{2}}\text{, -(n-}\sqrt{\frac{r}{2}}\sqrt{\frac{r}{2}}\text{)… (n-}\sqrt{\frac{r}{2}}\sqrt{\frac{r}{2}}\text{)]}$$

Lemme 4 : ***Si tous les joueurs honnêtes dans p[-n…n, -n…n] ont accepté m, alors tous les honnêtes joueurs dans S_i finiront par accepter m pour $0 \leq i \leq \sqrt{\frac{r}{2}}$***

Démonstration : tous les honnêtes joueurs dans S_0 finiront par accepter m depuis S_0 est un sous-ensemble de p[-n…n, -n…n]

Supposons que tous les joueurs honnêtes dans $S_0 \sqcup S_1 \ldots \sqcup S_{i-1}$ avoir accepté m ($1 \leq i \leq \sqrt{\frac{r}{2}}$). On note chaque p(n+i, n- $i\sqrt{\frac{r}{2}} - j$) dans S_i comme p_j avec ($0 \leq j \leq 2(n- i\sqrt{\frac{r}{2}})$. Pour montrer que tous les joueurs honnêtes dans S_i , finiront par accepter m, par symétrie, il suffit de montrer que pour n'importe honnête dans p_j finira par accepter m pour $0 \leq j \leq 2(n- i\sqrt{\frac{r}{2}})$. Observons que l'ensemble S' = p [0..n+i-1, - (n-$(i-1)\sqrt{\frac{r}{2}}$)… (n- $(i-1)\sqrt{\frac{r}{2}}$)] est un sous-ensemble de $S_0 \sqcup S_1 \ldots \sqcup S_{i-1}$. On note comme l'intersection de S'et l'ensemble des voisins du p_j comme il est modeler sur la figure III-2.

Si nous savions la borne inférieure de |Ŝ| par $r\left(r+1+\sqrt{\frac{r}{2}}\right)$, Depuis t < $\frac{r}{2}\left(r+1+\sqrt{\frac{r}{2}}\right)$

Dans le lemme 2, il s'ensuit qu'une honnête p_j va achèvera par l'acceptation de m. Notez que :

$$\hat{S} = p\left[n + -r \ldots n + i - 1, \max\{ n - i\sqrt{\frac{r}{2}} - j - r, -(n - (i-1)\sqrt{\frac{r}{2}})\}\right.$$

$$\left. \ldots \min\{ n - i\sqrt{\frac{r}{2}} - j + r, (n - (i-1)\sqrt{\frac{r}{2}})\}\right]$$

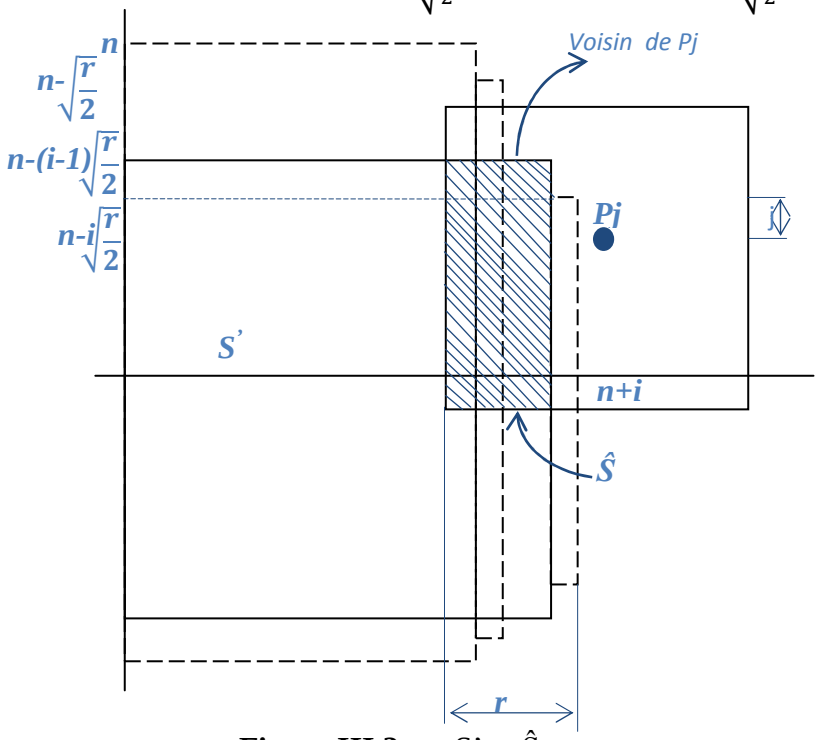


Figure III.2 S' et Ŝ

Maintenant,

$$\min \{ n- i\sqrt{\frac{r}{2}} - j + r, (n - (i-1)\sqrt{\frac{r}{2}})\} - \max \{ n- i\sqrt{\frac{r}{2}} - j - r, -(n - (i-1)\sqrt{\frac{r}{2}})\}$$

$$= \min \{ 2r, 2\left(n - i\sqrt{\frac{r}{2}}\right) + \sqrt{\frac{r}{2}} - j + r, \sqrt{\frac{r}{2}} + j + r, 2(n - i\sqrt{\frac{r}{2}} + \sqrt{\frac{r}{2}})\}$$

$$\geq \min \{ 2r, n - i\sqrt{\frac{r}{2}} + \sqrt{\frac{r}{2}} + r, \sqrt{\frac{r}{2}} + r, 2(n - i\sqrt{\frac{r}{2}} + \sqrt{\frac{r}{2}})\} \; car \; (0 \leq j \leq n - i\sqrt{\frac{r}{2}})$$

$$\geq \min \{ 2r, n + \frac{r}{2} + \sqrt{\frac{r}{2}} + r, \sqrt{\frac{r}{2}} + r, 2n - r + 2\sqrt{\frac{r}{2}}\} \; car \; (i \leq \sqrt{\frac{r}{2}})$$

$$\geq \sqrt{\frac{r}{2}} + r \; car \; (r \leq n)$$

Par conséquent,

$$|\hat{S}| \geq ((n + i - 1) - (n + i - r) + 1)\left(r + 1 + \sqrt{\frac{r}{2}}\right) = r\left(r + 1 + \sqrt{\frac{r}{2}}\right)$$

Lemme 5 : ***tous les joueurs honnêtes dans p [n+ 1, $n+1-\sqrt{\frac{r}{2}}$… n+1] accepteront éventuellement m***

Démonstration : puisque R = p [n + 1… $n+\sqrt{\frac{r}{2}}$, $n+1-r$… $n-\frac{r}{2}$] est un sous-ensemble de $S_1 \sqcup \ldots\ldots\ldots \sqcup S_{\sqrt{\frac{r}{2}}}$, dans la résulte du lemme 4 que tous les joueurs honnêtes dans R accepteront éventuellement m. et par la symétrie, tous les joueurs honnêtes dans U= p [$n+1-r$… $n-\frac{r}{2}$, n + 1… $n+\sqrt{\frac{r}{2}}$] acceptera aussi m éventuellement. Pour un joueur de p dans M_r tel que M_r = p [$n+1, n-\frac{r}{2}+1$… n], Tous les joueurs dans (R ⊔ U) est un voisin. Par ailleurs, p à au moins r (r +1) voisins et par conséquent, le nombre de voisins de p dans $S_0 \sqcup R \sqcup U$ est au moins égal a $r(r+1) + 2\sqrt{\frac{r}{2}}\left(\frac{r}{2}\right)\left(r + 1 + \sqrt{\frac{r}{2}}\right) = r\left(r + 1 + \sqrt{\frac{r}{2}}\right)$.

Dans le lemme 2, tous les joueurs honnêtes dans M_u (qu'est un super-ensemble de p [$n+1, n-\sqrt{\frac{r}{2}}+1$… n]) finiront par l'acceptation éventuellement de m, Et par symétrique, tous les joueurs honnêtes dans M_u = p [$n-\frac{r}{2}+1$… n, n+1] accepteront éventuellement m.

Maintenant, pour chaque joueur dans $R \sqcup U \sqcup M_r \sqcup M_u$ est un voisin de $p(n+1, n+1)$. En outre, avec l'addition, $p(n+1, n+1)$ a au moins r^2 voisins dans S_0, donc le nombre des voisins de $p(n+1, n+1)$ dans $S_0 \sqcup R \sqcup U \sqcup M_r \sqcup M_u$ .est au moins égal a : $r^2 +$

$2\sqrt{\frac{r}{2}}\left(\frac{r}{2}\right) + 2\left(\frac{r}{2}\right) = r\left(r + 1 + \sqrt{\frac{r}{2}}\right)$. Par le lemme 2 aussi, les honnêtes dans p$(n+1, n+1)$ finiront par accepter m.

On a achevé la démonstration pour la métrique L_∞ et on va passer aux métriques L_1 et L_2. Nous allons montrer comment réduire le formulaire problème de la métrique L_1 à la métrique L_∞ sous la forme du théorème 6, et de L_2 à L_1 dans le théorème 7.

III.7.2.2 Théorème 6

Si t $< \frac{1}{4}\left(r\left(r + \sqrt{\frac{r}{2}} + 1\right)\right) - 2$, alors le protocole peut atteindre la diffusion dans la métrique L_1.

Démonstration : Notez que dans la métrique L_1, l'ensemble des voisins d'un joueur de p (x, y) est égale à {p$(\bar{x}, \bar{y})$:$|\bar{x} - x| + |\bar{y} - y| \leq$ r}et pour démontrer ce théorème, nous avons besoin de montrer que tous les joueurs honnêtes dans l'ensemble {p(x, y)} accepteront probablement m. le fait de tourner le plan de 45 °(Figure III-3), nous avons pu voir que le problème est le même que tous les joueurs honnêtes présentant dans l'ensemble{p(x, y): $x + y$ est pair} et m sera accepté finalement, où le groupe des voisins d'un joueur p(x, y) est égale à {p(x, y): max $(|x - x| + |y - y|) \leq$ r $\wedge$ $x + y$ est pair (even)}. En grosso modo, c'est le même problème dans la métrique L_∞, sauf que la grille carrée est remplie. C'est pourquoi la borne est de ½ à celle de la métrique L_∞, et connu le -2 comme un décalage provient de l'erreur d'arrondie. La démonstration détaillée est semblable à celle du théorème 3.

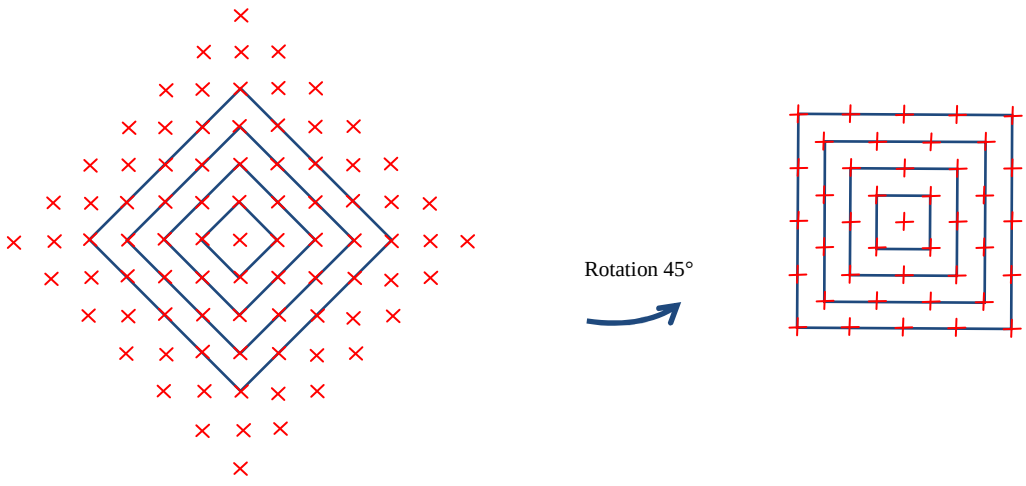


Figure III.3 Transformant le problème de la métrique L_1 à L_∞

III.7.2.3 Théorème 7

Si $t < \frac{1}{4}(r\left(r + \sqrt{\frac{r}{2}} + 1\right)) - 2$, alors le protocole peut atteindre la diffusion dans la métrique L_2.

Démonstration : quelque soit p (x, y), {p (x, y): max (| $x - x$ |+| $y - y$ |) ≤ r} ⊑ { p (x,y): | $x - x|^2 + | y - y|^2 \leq r^2$}, tout voisin de p (x, y) dans la métrique L_2 est un voisin dans la métrique L_1, on peut dire que le théorème 6 est une implication du théorème 7.

III.8 Les bornes inférieures

Dans ce qui reste dans ce chapitre, nous présentons les résultats sur la borne inférieure des valeurs de t où il est impossible de parvenir à la diffusion. L'idée est de définir un ensemble des joueurs corrompus qui divisent la grille carrée en deux moitiés, de telle sorte qu'un joueur honnête sur une moitié ne peut pas prendre des messages diffusés par les joueurs sur l'autre moitié. Sans perte de généralité, nous supposons que le concessionnaire (dealer) est à (0,0). Nous allons d'abord examiner la métrique L_∞, puis réduire le problème à partir L_2 à la métrique L_∞.

Lemme 8 : ***Si*** $t \geq [\frac{1}{4}r(2r + 1)]$***, il est impossible d'atteindre une diffusion dans la métrique*** L_∞**.**

Démonstration : nous définissons deux joueurs de remorquage fixe P_1 et P_2 comme suit:

- ***Pour r est pair***

$P_1 = \{(x, y) : 1 \leq x \leq r \wedge x$ est impaire$\}$

$P_2 = \{(x, y) : 1 \leq x \leq r \wedge x$ est pair$\}$

- ***Pour r est impaire***

$P_1 = \{(x, y) : (1 \leq x < r \wedge x$ est impaire$) \vee (x = r \wedge y$ est impaire$)\}$

$P_2 = \{(x, y) : (1 \leq x < r \wedge x$ est pair$) \vee (x = r \wedge y$ est pair$)\}$

Une représentation picturale de P_1 et P_2 est transcrite dans la figure suivante :

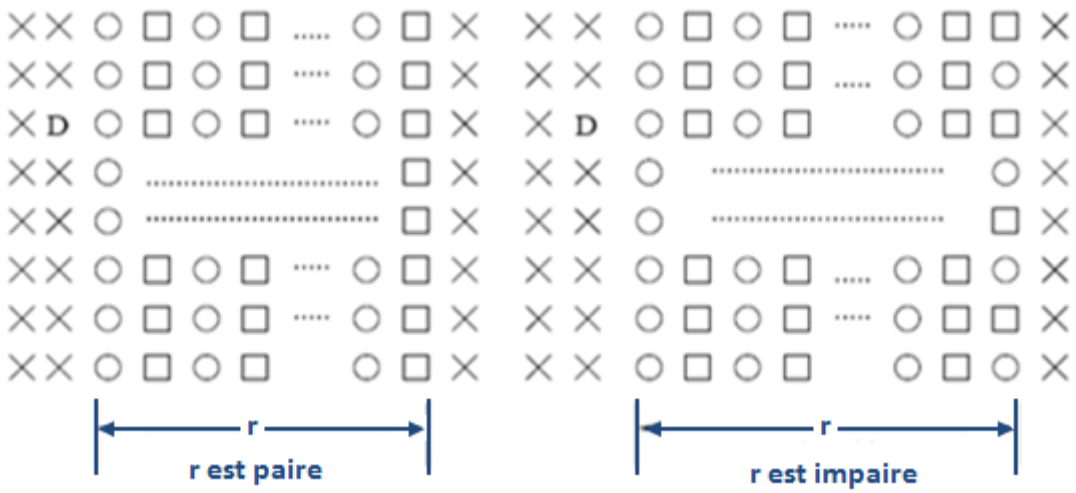


Figure III.4 La borne inférieure dans la métrique L∞

On note qu'aucun joueur honnête P (x, y) avec (x > r) peut distinguer les deux scénarios suivants:

- ***Le premier scénario:***
  - Le distributeur broadcaste le message m.
  - L'adversaire corrompt tous les joueurs dans P_1 et tous les joueurs corrompus agissent comme si le distributeur diffusé le message $\widetilde{m}$.
  - Tous les joueurs sont honnêtes dans P_2.
- ***Le second scénario:***
  - Le distributeur broadcaste le message $\widetilde{m}$.
  - L'adversaire, corrompt tous les joueurs dans P_2 et tous les joueurs corrompus agissent comme si le distributeur diffusé le message m.
  - Tous les joueurs dans P_1 sont honnêtes.

Ce que restant dans cette phase est de faire valoir l'adversaire a corrompu au plus $[\frac{1}{2}r(2r+1)]$ voisins d'un joueur honnête dans les deux scénarios. Mais cela est vrai, depuis n'importe quel joueur qui n'est pas dans $P_1(P_2)$ qui contient au plus $[\frac{1}{2}r(2r+1)]$ voisins dans $P_1(P_2)$.

III.8.1 Théorème 9

Si $t \geq [\frac{1}{2}r(2r+1)]$ alors il est impossible d'atteindre une diffusion dans la métrique L_2.

Démonstration : cela découle du théorème 8 car tout voisin d'un joueur en p dans la métrique L_2 est un voisin de p dans la métrique L_∞.

Par souci d'exhaustivité, nous incluons le résultat d'impossibilité dans la métrique L_1.

III.8.2 Théorème 10

Si $t \geq \frac{1}{2}r(r+1)$ alors il est impossible d'atteindre une diffusion dans la métrique L_1.

Démonstration : nous définissons deux joueurs P_1 et P_2 comme suit :

- ***Pour r est pair***
  - $P_1 = \{(x,y) : 1 \leq x+y \leq r \wedge x+y \text{ est impaire}\}$
  - $P_2 = \{(x,y) : 1 \leq x+y \leq r \wedge x+y \text{ est pair}\}$
- ***Pour r est impaire***
  - $P_1 = \{(x,y) : (1 \leq x+y < r \wedge x \text{ est impaire}) \vee (x+y = r \wedge y \text{ est impaire})\}$
  - $P_2 = \{(x,y) : (1 \leq x+y < r \wedge x \text{ est pair}) \vee (x+y = r \wedge y \text{ est pair})\}$

Une représentation picturale de P_1 et P_2 est transcrite dans la figure suivante :

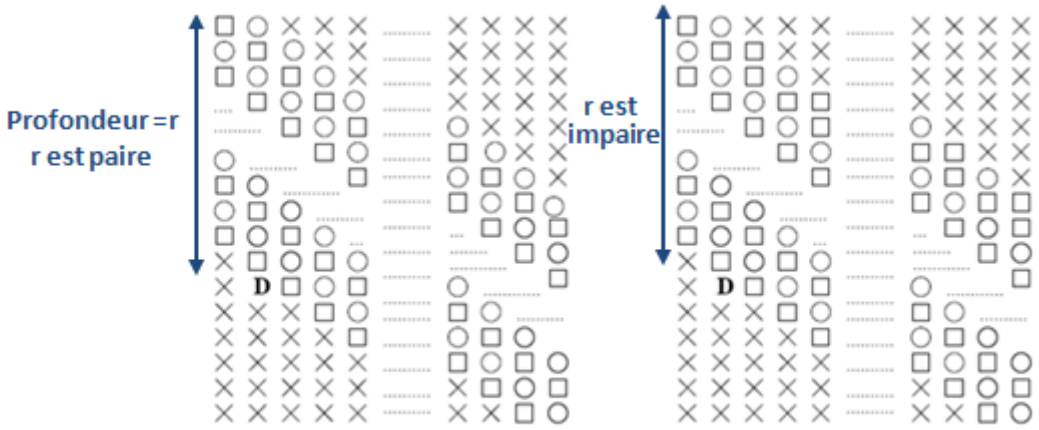


Figure III.5 La borne inférieure dans la métrique L_1

En utilisant le même argument instruit dans le théorème 8, nous pouvons montrer que le théorème est vrai et aussi long pour n'importe quel joueur qui n'est pas dans $P_1(P_2)$ et a tous au plus $\frac{1}{2}r(r+1)$ voisins dans $P_1(P_2)$. Nous utilisons la même observation que nous faisons dans le théorème 6, c'est-à-dire tourner par 45 ° pour faire le comptage (figure III-3). Avec cette observation, il est facile de voir que le nombre de voisins est majoré par $\frac{1}{2}r(r+1)$.

III.9 Conclusion

Dans ce chapitre nous avons défini le comportement Byzantin où certains nœuds dans le réseau présentent un comportement anormal, et nous avons aussi présenté un de modèle qui été faits pour étendre le modèle standard pour les problèmes des généraux Byzantins, en supposant le multicast-canaux. Dans les réseaux sans fil, un joueur ne peut communiquer qu'aux joueurs au sein d'une distance fixe. Et bien, on montré, qu'il est possible d'obtenir la diffusion si $t < \frac{1}{4}\left(r\left(r+\sqrt{\frac{r}{2}}+1\right)\right)-2$ d'une part, et d'autre part, il est impossible d'atteindre la diffusion lorsque $t \geq \frac{1}{2}r(r+1)$ ces limites ne sont pas étanches et il sera intéressant de savoir si l'étroit des limites peuvent être obtenues.

Conclusion générale

Le travail réalisé présente une étude et une présentation d'un modèle pour le comportement contradictoire dans les réseaux radio et on a montré, qu'il est possible d'obtenir la diffusion si t $< \frac{1}{4}(r\left(r + \sqrt{\frac{r}{2}} + 1\right)) - 2$ d'une part, et d'une autre part, il est impossible d'atteindre la diffusion lorsque $t \geq \frac{1}{2} r(r+1)$ ces limites ne sont pas étanches et il sera intéressant de savoir si l étroit des limites peuvent être obtenues. Dans notre modèle, nous supposons l'existence d'un calendrier de préfixe et un joueur corrompu qui doit suivre le calendrier. Nous savons qu'il est impossible de parvenir à diffuser si les joueurs corrompus s'écarte de l'horaire indéfiniment, mais que faire si un joueur corrompu pourrait provoquer des collisions messages d'un nombre borné de k fois? . Noter que cela ne pouvait pas être simplement résolu en demandant un joueur honnête de diffuser k+1 fois. Le problème est le suivant, 'A' un joueur corrompu qui croupier « concessionnaire » et diffuse des messages incohérents, un joueur corrompu sur sa gauche cause de laissé pour la première fois un message incorrecte, et un autre joueur corrompu trouve sur la droite cause de laissé pour la deuxième fois un message correcte, maintenant les joueurs sur la gauche recevront un message différent de ces joueurs sur la droite et pourtant ils ne connaîtront pas que le concessionnaire est corrompu.

Dans ce mémoire nous avons adapté notre travail sur trois phases principales :
Dans la première phase, nous avons abordé les grands principes régissant les réseaux sans fil. Nous avons présenté, également, le modèle de défaillances dans les systèmes distribués et les réseaux radio.

Dans la deuxième partie nous avons défini et expliquer la notion du problème des généraux Byzantins pour trois nœuds et pour « n » nœuds et la relation de ce problème vers les systèmes informatiques.
Dans la phase d'exposition de modèle (la troisième partie) de ce travail, nous avons dédié à la présentation d'un modèle pour le comportement contradictoire dans les réseaux radio, et on à supposé que le réseau est synchrone et qu'il existe un calendrier (schediling) préfixe pour les joueurs.

En perspectives, ce travail peut être complété par l'inclusion dans le cas où le réseau est asynchrone et sur d'autres phases de parcours des nœuds de réseau.

Bibliographie

[01] N. Bulusu, J. Heidemann, and D. Estrin. *GPS-less low cost outdoor localization for very small devices*. Technical report 00-729, Computer science department, University of Southern California, Apr. 2000.

[02] IEEE Standard for Information Technology -Telecommunications and information exchange between systems- Local and metropolitan area networks- Speci_c requirements.
Part 15.1 : Wireless Medium Access Control (MAC) and Physical Layer (PHY) Speci_cations for Wireless Personal Area Networks (WPANs). June 2002.

[03] Draft 802.15.4. "Wireless Medium Access Control (MAC) and Physical Layer (PHY) specifications for Low Rate Wireless Personal Area Networks (LR-WPAN)". 2003

[04] IEEE Standard for Information Technology- Telecommunications and information exchange between systems- Local and metropolitan area networks- Speci_c requirements.
Part 15.3 : Wireless Medium Access Control (MAC) and Physical Layer (PHY). September 2003.

[05] *IEEE, Groupe de travail 802.11*: "http://grouper.ieee.org/groups/802/11/ ". 1999.

[06] Dominique Dhoutaut. *Etude du standard IEEE 802.11 dans le cadre des réseaux Ad hoc*: de la simulation à l'expérimentation. Thèse pour obtenir le grade de Doctorat en Informatique. 2003.

[07] J. ANZEVUI, « WIFI », Université de Genève 2006-2007

[08] Tayeb Lemlouma. *Le Routage dans les Réseaux Mobiles Ad Hoc*. Mini projet proposé par Dr. Nadjib Badache septembre 2000.

[09] Y.CHALLAL, Réseaux de capteurs sans fil, Sep 2008, page 45

[10] pour tolérance dans les Sd 1 R. Strong "Problems in fault-tolerant distributed systems", Publication IEEE ISBN 135-/85/0000/0300s01.00.

[11] L. Lamport, R. Shostak, and M. Pease, "The Byzantine Generals Problem", ACM Transactions on Programming Languages and Systems, Vol. 4, No. 3, July 1982, pp 382-410.

[12] Radia Perlmen, Routing with Byzantine Robustness, Sun Microsystems, Sep2005.

[13] B. Awerbuch, R. Curtmola, D. Holmer, C. Nita-Rotaru, and H Rubens, "Mitigating Byzantine Attacks in Ad Hoc Wireless Networks," Department of Computer Science, Johns Hopkins University, Tech. Rep. Version 1, March 2004.

[14] M. Pease, R. Shostak, L. Lamport, "Reaching Agreement in the Presence of Faults", JACM 27, 2, 228-234, 1980.

[15] M. Fischer and N. Lynch, "A Lower Bound for the Time to Assure Interactive Consistency". Information Processing Letters 14, 4, 183-186, 1982.

[16] M. Fischer, N. Lynch, and M. Paterson, "Impossibility of Distributed Consensus with One Faulty Process", JACM, 32, 2, 374-382, 1985.

[17] M. Yu, S. Kulkarni, and P. Lau, "A New Secure Routing Protocol To Defend Byzantine Attacks For Ad Hoc Networks", IEEE Int. Conf. on Networks (ICON'05), vol. 2, pp. 1126-1131, Nov. 16-18, Kuala Lumpur, Malaysia.

[18] B. Awerbuch, D. Holmer, C. Nita-Rotaru, and H. Rubens, "An on-demand secure routing protocol resilient to byzantine failures," in ACM Workshop on Wireless Security (WiSe) 2002, 2002.

[19] M. Fitzi et U. Maurer. From partial consistency to global broadcast. In Proceedings of thirty-second annual ACM symposium on theory of computing page 494-503. ACM Press,2000.

[20] J.considine,L.A.Levin,and D Metcalf. Byzantine agreement with faulty majority using bounded broadcast. arXiv.org e-print archive,2003.

[21] N. Alon, A.bar-Noy, N. linial, et D.Peleg. A lower bound for radio broadcast. J comput.Syst.Sci., 43(2):290-298,1991.

[22] I.Gaber and Y.Mansour. Broadcast in radio networks. In preceedings of the sixth annual ACM-SIAM symposium on Discrete algorithms,pages 577-585. Society for Industrial and Applied Mathematics,1995.

[23] E.Kushilevitz and Y. Mansour. An Ó (d log(n/d)) lower bound for broadcast in radio networks, In proceedings of twelfth annual ACM symposium on principales of distributed computing, pages 65-74 ACM Press, 1993

[24] D.R Kowalski et A.Pelc Broadcasting in undirected ad hoc radio networks. In Proceedings of twenty-second annual symposium on principales of distributed computing, page 73-82 ACM Press,2003

[25] E.Pagani et G.P Rossi. Broadcasting algorithms in radio networks with unknown topolgy. In Proceedings of the 44 th annual IEEE Symposium on Foundations of computer Science, pages 492-501,2003

[26] E.Kranakis, D. krizanc, et A pelc, Fault-tolerant broadcasting in radio networks (extended abstract). In proceedings of the 6th annual European symposium on algorithms, pages 283-294. Springer-verlag,1998.

[27] E.Pagani et G.P Rossi. Reliable broadcast in mobile multihop packet networks. In proceedings of the 3rd annual ACM/IEEE international conference on mobile computing and networking, pages 34-42, ACM Press, 1997.

[28] E. W.Weisstein. « Gauss's Circle problem » From MathWorld-A Wolfram Web Resource.

[29] L. Lamport, R. Shostak, and M. Pease, "The Byzantine Generals Problem", ACM Transactions on Programming Languages and Systems, Vol. 4, No. 3, July 1982, pp 102

[30] Kramer, Magee," The Byzantine Generals Problem (consensus in the presence of uncertainties) ", ACM Press,1998.

[31] Johan Karlsson." Fault Tolerance in distibuted system ", JACM 27, 2001.

Résumer

Ce travail porte sur l'étude et la conception d'un modèle pour le comportement contradictoire dans les réseaux radio tolérant byzantin. Cette étude a été motivé par l'importance de la diffusion sécurisée dans les réseaux radio et la réduction des temps de latence de diffusion dans les réseaux sans fil, en présence d'un adversaire Byzantin.

On suppose qu'il existe un calendrier de préfixe et un joueur corrompu qui doit suivre ce dernier. Et nous savons aussi qu'il est impossible de parvenir à diffuser si les joueurs corrompus s'écarte de l'horaire indéfiniment, mais que faire si un joueur corrompu pourrait provoquer des collisions messages d'un nombre borné de k fois? La réponse a cette question est qu'il est possible d'obtenir la diffusion si t $<\frac{1}{4}(r\left(r+\sqrt{\frac{r}{2}}+1\right))-2$ d'une part, et d'autre part, il est impossible d'atteindre la diffusion lorsque $t \geq \frac{1}{2}r(r+1)$ ces limites ne sont pas étanches

Mots clés : *réseaux sans fil, problème des généraux Byzantins, la diffusion sécurisée, le comportement contradictoire*

Abstract

This work involves the study and design of a model for the contradictory behavior in radio networks tolerating byzantine. This work was motivate by the importance of secure broadcast in radio networks and reducing latency broadcast in wireless networks, in the presence of a Byzantine adversary.

Assume that there exists a schedule for prefix and corrupt a player must follow it. And we also know that it is impossible to achieve if the players spread corrupt deviates from the schedule indefinitely, but what if a player could cause collisions corrupted messages in a bounded number of times k? The answer of this question it is possible to obtain the distribution if t $<\frac{1}{4}(r\left(r+\sqrt{\frac{r}{2}}+1\right))-2$ the one hand, and on the other hand, it is impossible to reach the $t \geq \frac{1}{2}r(r+1)$ distribution when these limits are not closed

Keywords: *wireless networks, Byzantine generals problem, secure distribution, the contradictory behavior*