REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
MINISTERE DE L'ENSEIGNEMENT SUPERIEUR DE LA RECHERCHE SCIENTIFIC

UNIVERSITÉ DE BOUIRA
FACULTE DES SCIENCES ET DES SCIENCES APPLIQUEES
LABORATOIRE DE RECHERCHE LIMPAF DE BOUIRA
DEPARTEMENT DE Informatique
MEMOIRE POUR L'OBTENTION DU DIPLOME DE MASTER Informatique
Option : Génie des Systémes Informatiques

THÈME

Proposition d'un mécaniseme de sécurité anti-spoofing attack dans les réseaux ad hoc

Réalisé par : MERZOUK Anzar

Encadré par : DEMMOUCHE Mouloud

Année universitaire : 2022/2023

الجمهورية الجزائرية الديمقراطية الشعبية
République Algérienne Démocratique et Populaire

وزارة التعليم العالي و البحث العلمي
جامعة أكلي محند أولحاج - البويرة

Ministère de l'Enseignement Supérieur
et de la Recherche Scientifique
Université Akli Mohand Oulhadj - Bouira
Tasdawit Akli Muhend Ulhağ - Tubirett

التصريح الشرفي الخاص بالالتزام بقواعد النزاهة العلمية

لإنجاز بحث

انا الممضي اسفله،

السيد(ة) مزوق أنزار الصفة: طالب (ماستر) / دكتوراه)

الحامل(ة) لبطاقة التعريف الوطنية: 110842159 والصادرة بتاريخ 2018.10.03

المسجل(ة) بكلية / معهد العلوم والعلوم التطبيقية قسم اعلام آلي

تخصص: هندسة الأنظمة المعلوماتية GSI

والمكلف(ة) بإنجاز اعمال بحث(مذكرة، التخرج، مذكرة ماستر، مذكرة ماجستير، اطروحة دكتوراه).

عنوانها: proposition d'un mécanisme de sécurité anti-spoofing attaque dans les Réseaux ad hoc.

أصرح بشرفي اني ألتزم بمراعاة المعايير العلمية والمنهجية الاخلاقيات المهنية والنزاهة الاكاديمية المطلوبة في انجاز البحث المذكور أعلاه.

التاريخ: 2023.09.24

توقيع المعني (ة)

هيئة مراقبة السرقة العلمية:

البويرة في: 2023/09/11

الامضاء

النسبة: % 20

Remerciements

Je remercie, tout d'abord, le bon Dieu qui m'a guidée sur le chemin de la sagesse et dusavoir, et qui m'a donné le courage, la volonté et la patience pour accomplir ce modeste travail.

Je tiens à exprimer ma profonde reconnaissance envers mon directeur de recherche, MonsieurDemouche Mouloud de m'avoir proposé ce sujet, de m'avoir guidé etorienté, de ses remarquescritiques, de sa patience, ainsi que pour l'inspiration et le temps qu'il a bien voulu me consacrer.

J'adresse mes vifs remerciements aux membres du jury pour avoir accepté d'évaluer ce travail, ainsi qu'envers les enseignants de notre département qui ont assuré notre formation universitaire.

Je tiens également à exprimer ma sincère gratitude envers mes chers amis Maa Bilal etBachouche Oussama pour leur précieux soutien et leur contribution à la finalisation demon travail. Sans leur implication physique et morale, ce travail n'aurait pas pu voir le jour. Leur appui a été inestimable, et je leur suis reconnaissant pour leur amitié et leur aide précieuse.

J'adresse également mes remerciements à toutes les personnes qui ont généreusement acceptéde partager leur témoignage. Leur précieuse contribution a constitué une base solide sur laquelle j'ai pu m'appuyer pour mener à bien ma démarche de recherche et d'analyse.

Cordialement

Merci a tous
M.Anzar

Dédicace

Ce mémoire est dédié en premier lieu aux êtres les plus chers à ma vie : à mes **parents**, les piliers solides qui m'ont constamment motivé, soutenu et guidé à travers les défis qui ont parsemé mon parcours académique. Leur indéfectible soutien a été la clé de ma persévérance et de ma détermination à poursuivre mon cursus. Leur amour inconditionnel et leurs encouragements ont été ma source d'inspiration inépuisable. Je vous remercie du fond du cœur pour tout ce que vous avez accompli pour moi.

à mes très chères sœurs : **Chahrazed, Nabila, Cylia** et **Kahina**

à mes chers frères : **Aguellid** et **Amazigh**

Je leur dédie ce travail pour tout ce qu'ils ont fait pour moi pendant mes années d'études.

À tous mes camarades de promotion et amis, avec qui j'ai fait ce parcours et partagé les moments joyeux et difficiles.

À tous mes enseignants, depuis l'école primaire jusqu'à l'université.

Résumé

Le spoofing est une attaque sévère où un nœud malveillant se fait passer pour un nœud légitime dans le réseau. L'objectif est d'obtenir un accès au réseau et d'ouvrir la porte à d'autres attaques plus dangereuses. La littérature propose des approches traditionnelles qui se basent essentiellement sur l'authentification basée sur la cryptographie, ainsi que d'autres approches utilisant des paramètres de signal et des numéros de séquence.

Ces solutions sont généralement coûteuses en termes de calcul, de capacité de stockage et de matériel nécessaire pour effectuer une contre-attaque. Notre solution repose sur l'historique des communications précédentes au sein du réseau, renforçant ainsi la confiance entre les nœuds communicants, et implique un ensemble de calculs pour effectuer la vérification de l'authentification. Notre solution est à la fois légère et évolutive, car elle ne nécessite aucun matériel supplémentaire ni aucune coopération entre les nœuds pour sa mise en œuvre.

Les résultats de simulation montrent que la solution proposée est efficace dans la détection de l'attaque de spoofing. Il reste à la comparer avec d'autres travaux de référence pour prouver davantage son efficacité et évaluer ses performances.

Mots clés : réseaux ad hoc, sécurité des réseaux ad hoc, attaques liées à l'identité, attaque de spoofing,...

Abstract

Spoofing is a serious attack where a malicious node impersonates a legitimate node on the network. The aim is to gain access to the network and open the door for more severe attacks. The literature proposes traditional approaches that rely primarily on cryptography-based authentication, as well as other approaches that utilize signal parameters and sequence numbers.

The cost of computation, storage capacity, and hardware required for a counterattack is typically high for these solutions. The history of previous communications within the network is the basis of our solution, which builds trust between communicating nodes and involves a set of calculations for authentication verification. Our solution is both lightweight and scalable, as it does not require any additional hardware or cooperation between nodes to be implemented.

The simulation results show that the proposed method works properly at identifying spoofing attempts. It still has to be compared with other reference works to confirm its efficacy and evaluate its performance.

Key words : ad hoc networks, ad hoc network security, identity-related attacks, spoofing attack,...

ملخص:

يعتبر الإنتحال هجوما خطيرا تنتحل فيه عقدة خبيثة صفة عقدة شرعية في الشبكة، والهدف هو الحصول على شرعية الدخول لهذه الشبكة وفتح الباب لمزيد من الهجمات الأكثر خطورة. تقترح أدبيات البحث مناهج تقليدية تعتمد بشكل اساسي على المصادقة المبنية على التشفير بالإضافة إلى مناهج أخرى تعتمد على إستعمال معلمات الإشارة والأرقام التسلسلية.

هذه الحلول تكون عموما مكلفة من حيث الحسابات وسعة التخزين والأجهزة المطلوبة لتنفيذ الهجوم المضاد. الحل المقترح من طرفنا يعتمد على تاريخ الإتصالات السابقة داخل الشبكة مما يعزز الثقة بين العقد الإتصالية، وتتضمن مجموعة من الحسابات لأداء التحقق من المصداقية. هذا الحل خفيف وقابل للتوسع حيث لايتطلب أي أجهزة إضافية أو تعاون بين العقد لتنفيذها.

أظهرت نتائج المحاكاة أن الحل المقترح فعال في اكتشاف هجمات الإنتحال إلا أن هذا يستدعي المقارنة مع أعمال مرجعية أخرى لإثبات فعاليتها بشكل أكبر.

كلمات مفتاحية: الشبكات المخصصة ، أمن الشبكات المخصصة ، هجمات ذات صلة بالهوية، هجوم الإنتحال

Table des matières

Table des figures

Liste des tableaux

Liste des abréviations

AES	Advanced Encryption Standard.
AODV	Ad hoc On Demand Distance Vector.
AP	Access Points.
ARP	Address Resolution Protocol.
CA	Certificate Authority.
DES	Data Encryption Standard.
DoS	Denial of Service.
DSDV	Destination Sequenced Distance Vector.
DSR	Dynamic Source Routing.
ECC	Elliptic Curve Cryptography.
FSR	Fisheye State Routing.
IARP	Protocole de routage intrazone .
IERP	Protocole de routage interzone .
IETF	Internet Engineering Task Force.
IP	Internet Protocol.
MAC	Media Access Control.
MAC	Message Authentication Code.
MANET	MobileAd hoc NETwork.
OLSR	Optimized Link State Routing protocol.
RREQ	Route REQuest.
RREP	Route REPlay.
RSA	Rivest-Shamir-Adleman.
RSS	Received Signal Strength.
ZRP	Zone Routing Protocol.

Introduction Générale

Les réseaux sans fil ad hoc, constitués d'un ensemble de nœuds interagissant sans nécessiter d'infrastructure fixe, ont évolué pour devenir un élément essentiel de la connectivité moderne grâce à leur multitude d'avantages.

Cependant, leur nature ouverte, le partage du médium de communication, l'absence d'infrastructure centralisée, et la mobilité inhérente des nœuds les rendent vulnérables à une variété d'attaques informatiques visant à compromettre la sécurité des communications. Ces attaques ciblent souvent différents services de sécurité, notamment l'authentification des nœuds, la préservation de l'intégrité et de la confidentialité des données, le maintien de la disponibilité du réseau, ainsi que la gestion du contrôle d'accès, entre autres.

Parmi ces menaces, les attaques liées à l'identité, et plus particulièrement l'attaque de spoofing, qui est notre sujet d'étude, occupent une place prépondérante en raison de leur capacité à usurper l'identité d'un nœud pour accéder au réseau, ouvrant ainsi la porte à des attaques plus sophistiquées et potentiellement dommageables.

Les méthodes traditionnelles pour contrer cette menace reposent souvent sur l'authentification basée sur la cryptographie ou sur l'utilisation de paramètres de signal et de numéros de séquence.

Cependant, ces solutions s'accompagnent généralement de coûts substantiels en termes de ressources informatiques, de capacité de stockage, et de matériel nécessaire pour leur mise en œuvre. C'est dans ce contexte que s'inscrit notre recherche, axée sur la quête d'une solution efficace pour détecter les attaques de spoofing au sein des réseaux ad hoc.

Cette démarche nous a conduit à entreprendre ce mémoire, qui se déploie en quatre chapitres pour offrir une compréhension en profondeur des réseaux ad hoc et de leurs enjeux en matière de sécurité. Le premier chapitre propose une vue d'ensemble des réseaux ad hoc, abordant leurs caractéristiques distinctives, leurs avantages, leurs inconvénients, leurs domaines d'application, ainsi que des informations essentielles sur le routage au sein de ces réseaux. Le deuxième chapitre explore la question de la sécurité au sein des réseaux ad hoc, se penchant sur les services de sécurité disponibles, les différentes catégories d'attaques qui les ciblent, ainsi que les mécanismes de sécurité existants destinés à les contrer.

Dans le troisième chapitre nous examinos l'état de l'art des attaques de spoofing, en présentant les solutions existantes documentées dans la littérature.

Ces analyses ont été cruciales pour le développement de notre propre solution, que nous exposons en détail. Enfin, le quatrième chapitre présente une simulation détaillée que nous

avons menée pour évaluer l'efficacité de notre proposition. En fin de compte, ce mémoire vise à approfondir notre compréhension de la sécurité des réseaux ad hoc, tout en offrant des outils pratiques pour renforcer leur protection contre les attaques de spoofing.

En sécurisant davantage ces réseaux, nous espérons encourager leur adoption continue et leur utilisation dans un éventail élargi d'applications critiques, tout en renforçant la fiabilité de nos communications sans fil.

Chapitre 1

Généralités sur les réseaux sans fil de type ad hoc

1.1 Introduction

Aujourd'hui , les réseaux sans fil, sont largement répandus et très populaires dans le domaine des télécommunications. du aux équipements mobiles a faible cout, et que la majorité des ordinateurs et d'autres appareils informatiques disposent de moyens de connexion a un ou plusieurs types de réseaux sans fils(Bluetooth , wifi...).

Alors un réseau sans fil est un réseau informatique qui connecte plusieurs appareils (ou biens systèmes informatiques) entre eux sans aucune connexion filaire(par ondes radio).

Les réseaux sans fil peuvent être classé en deux catégories, les réseaux avec infrastructure tel que un point d'accès qui fait la liaison entre les nœuds de réseau, la deuxième catégorie est celle des réseaux ad hoc.

Dans ce chapitre, nous allons commencer par présenter des généralités sur les réseaux sans fil de type ad hoc , leurs caractéristiques, leurs applications , leurs architectures , ainsi que les avantages et les inconvénients de ces réseaux , la différence entre eux et le mode avec infrastructure .

1.2 Réseaux sans fil

Les réseaux sans fil jouent un rôle crucial dans la vie des gens au travail, à la maison et les lieux publics. même si un réseau sans fil a un objectif simple, qui est de fournir des connexions entre les utilisateurs et les sources d'informations sans l'utilisation de fils, les concepts critiques des réseaux sans fil doivent être maîtrisés avant de comprendre-comment ils fonctionnent. Cette partie présente une définition approfondie des réseaux sans fil.

Définition 1.1.

Les réseaux sans fil, sont des réseaux de communication qui permettent la transmission de données sans utiliser de câbles physiques pour la connexion entre les dispositifs. Au lieu de cela,

les données sont transmises via des ondes radios, des micro-ondes ou des infrarouges, ce qui permet une communication sans fil entre les dispositifs connectés.

La popularité croissante des réseaux sans fil est due à leur souplesse, à la simplicité de leur installation et à leur capacité à favoriser la mobilité des appareils [27].

1.3 Classification des réseaux sans fil

D'après leurs architectures, Les réseaux sans fil ont la possibilité de fonctionner selon deux modes : le mode avec infrastructure et le mode sans infrastructure, également appelé mode ad hoc.

1.3.1 Mode avec infrastructure

Dans ce genre de réseaux, l'accès d'un nœud au réseau dépend de l'infrastructure de communication établie par le réseau lui-même. Cette infrastructure peut prendre différentes formes telles qu'un point d'accès (Access Point), d'un pont sans fil (Wireless Bridge), d'un routeur d'accès sans fil (Wireless Access Router), d'une station de base (Base Station Transceiver, BTS), et autres. Le choix de l'infrastructure est déterminé par divers facteurs tels que la nature des applications du réseau, l'étendue du réseau, la couverture souhaitée et la mobilité des nœuds. . .etc [41].

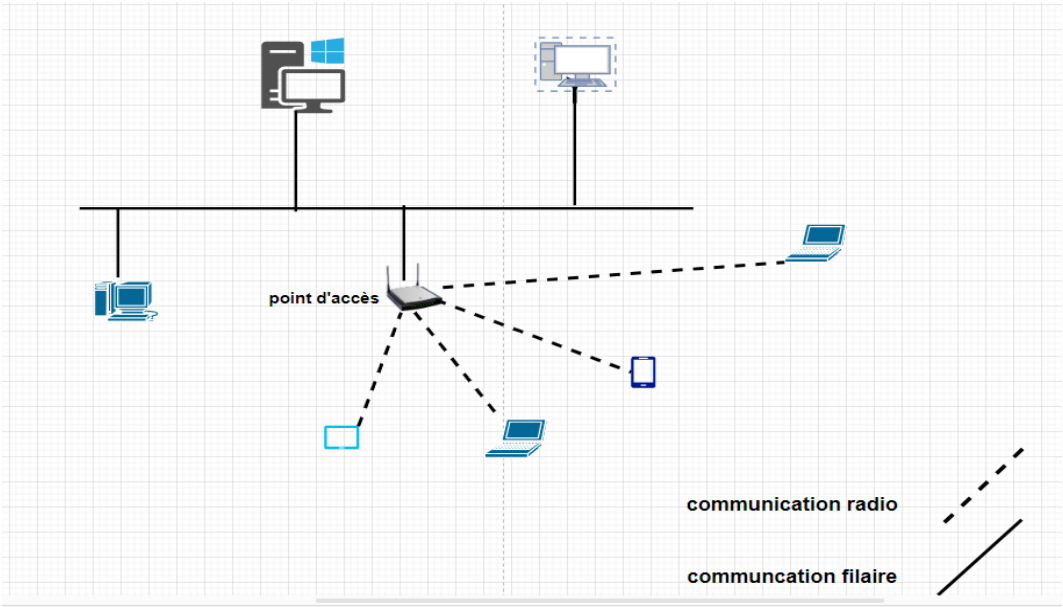

FIGURE 1.1 – Réseau en mode infrastructure

1.3.2 Mode sans infrastructure

Un réseau ad hoc ($MANET$), également connu sous le nom de réseau sans infrastructure, est constitué d'un groupe de nœuds mobiles qui forment un réseau temporaire, tout en ne nécessitant pas l'intervention d'une autorité centrale ni de dispositifs de support standard généralement présents dans les réseaux conventionnels.

Tous les nœuds sont mobiles et peuvent être connectés dynamiquement de manière arbitraire dans ces réseaux, les nœuds agissent en tant que routeurs, contribuant ainsi à la découverte et à la maintenance des chemins vers d'autres nœuds au sein du réseau.. (voir[33]).

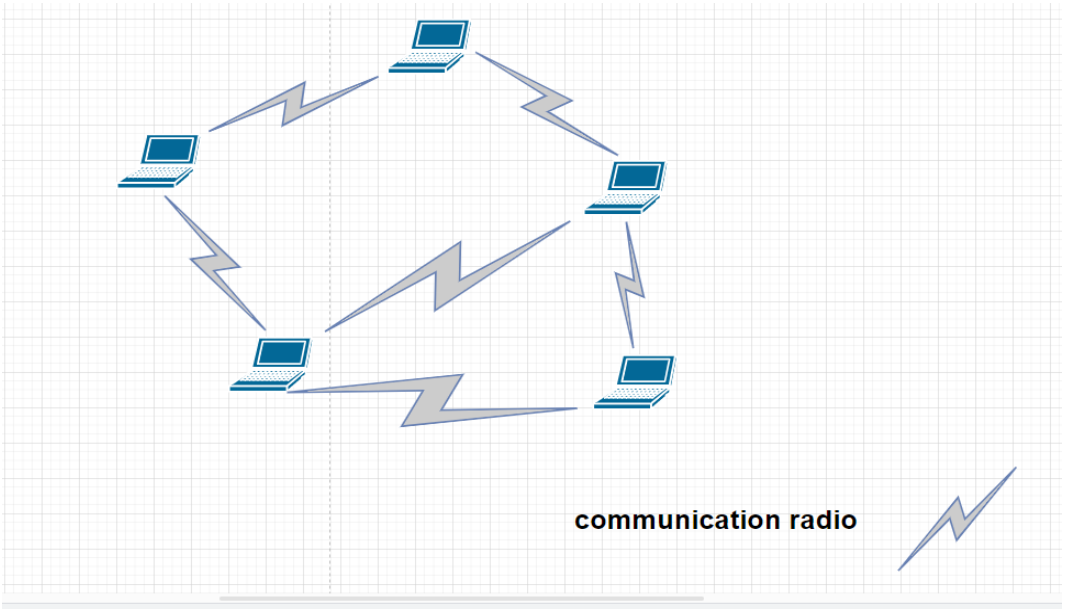

FIGURE 1.2 – Mode sans infrastructure

1.4 Les réseaux sans fil ad hoc

Définition 1.2.

Un réseau mobile sans fil ad hoc, couramment désigné sous le terme $MANET$ (Mobile Ad Hoc Network), est composé d'un ensemble de nœuds (captures, ordinateurs portables, terminaux ,..ect..) pouvant être mobile, interconnecté par une technologie sans fil, sans l'aide d'une infrastructure préexistante ou administration centralisée, où les nœuds sont libres de se déplacer aléatoirement et de s'organiser de manière arbitraire, entraînant ainsi une topologie réseau susceptible de changer rapidement et de façon imprévisible. On parle d'une topologie dynamique. Voir la figure

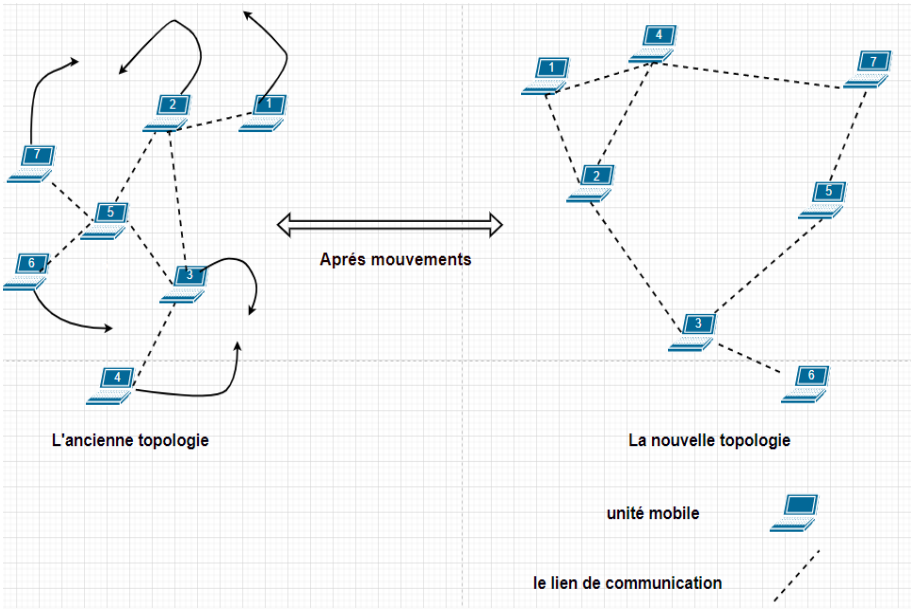

FIGURE 1.3 – Topologie dynamique des réseaux

Ce type de réseau est caractérisé dans la plupart du temps par une bande passante limitée, des contraintes d'énergie, l'hétérogénéité des nœuds, une sécurité physique limitée.

Dans un réseau ad hoc les nœuds peuvent être considérer comme des routeurs et terminaux à la fois, car la communication (l'envoie ou la réception des paquets de données) peut s'effectuer directement entre les nœuds ou à travers des nœuds intermédiaires qui agissent en tant que routeurs..

On peut représenter un réseau ad hoc sous forme d'un graphe $Ft = (Nt, Ct)$ où :

• Nt : désigne l'ensemble des nœuds du réseau.

• Ct : modélise l'ensemble des connexions entre les nœuds.

Si $e(x, y)$ appartient a Nt , cela veux dire que les nœuds x *et* y sont en mesure de communiquer directement à l'instant t [41].

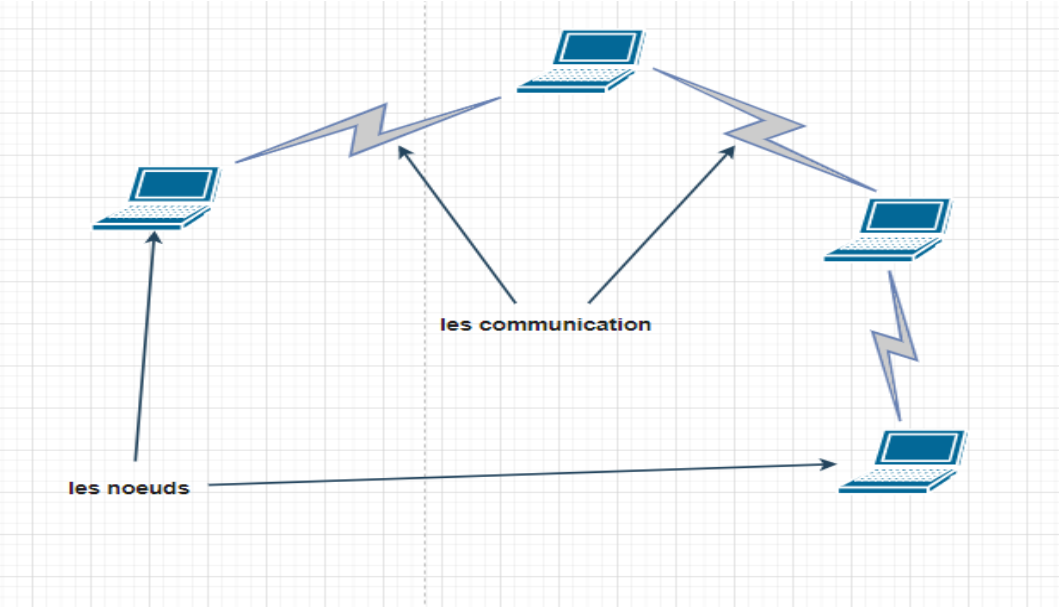

FIGURE 1.4 – Modélisation des réseaux ad hoc

1.4.1 Caractéristiques et avantages des réseaux ad hoc

D'après [20]

• **Autonome et sans infrastructure :** Les MANET fonctionnent sans avoir besoin d'une infrastructure établie ou d'une administration centralisée. Chaque nœud opère en mode peer to peer, agissant comme un routeur autonome et générant des données de manière indépendante.

• **Sans fil :** Les nœuds échangent des données sans nécessiter de câbles physiques et partagent les mêmes canaux de communication (infrarouge, radio, etc...).

• **Topologies dynamiques :** Un réseau mobile ad hoc est un réseau temporaire formé dynamiquement de manière arbitraire par une collection de nœuds selon les besoins.

• **Routage à sauts multiples :** Aucun routeur spécialisé n'est requis ; chaque nœud joue le rôle d'un routeur, transférant les paquets pour faciliter l'échange d'informations entre les appareils mobiles.

• **Mobilité :** Les nœuds ont la liberté de se déplacer tout en maintenant des communications avec les autres nœuds. La topologie dynamique des réseaux ad hoc est due aux mouvements constants des nœuds participants, entraînant des changements permanents dans les schémas d'intercommunication entre les nœuds.

• **Scalabilité :** Les réseaux ad hoc peuvent être facilement crée ou étendus pour inclure de nouveaux nœuds, ce qui les rend utiles pour les situations où le nombre de nœuds peut varier considérablement.

1.4.2 Limites des réseaux ad hoc

Bien que les réseaux ad hoc soient généralement utilisés là où leurs avantages sont les plus mis en avant, il y a certaines limites :

• **Sécurité :** En raison de l'absence d'une infrastructure centralisée et de la nature dynamique des nœuds, une variété d'attaques peuvent cibler les réseaux ad hoc, y compris les attaques de routage malveillantes, les attaques par déni de service, les attaques d'écoute clandestine et les attaques de type "spoofing" [39].

• **Contrainte d'énergie :** l'une des principales limitations des communications sans fil est la durée de vie limitée des dispositifs mobiles, souvent alimentés par une batterie de capacité limitée. Cette contrainte est encore plus marquée dans les réseaux ad hoc, où les dispositifs consomment leur propre énergie pour acheminer les données vers d'autres appareils [45].

• **Bande passante limitée :** Une des caractéristiques fondamentales des réseaux basés sur la communication sans fil est l'utilisation d'un support de communication partagé. Cette utilisation commune implique que la bande passante allouée à chaque hôte soit limitée [11].

• **La capacité de transmission limitée :** : Les nœuds ont souvent une capacité de transmission limitée, ce qui nécessite une disponibilité suffisante de nœuds pour assurer la fiabilité de transmission[12].

• **Complexité de gestion :** En raison de l'absence d'une administration centralisée, la gestion du réseau doit être répartie entre différents nœudsce qui compliquent la gestion de ces réseaux (par exemple la détection des erreurs et leur gestion) [16].

1.4.3 Normes

Diverses technologies sans fil ont déjà été mises en œuvre dans la création de réseaux ad hoc. Quelques-unes de ces technologies comprennent :

• **Bluetooth :** La spécification Bluetooth a été établie par le Bluetooth Special Interest Group (SIG), une organisation composée de plusieurs grandes entreprises du secteur de l'électronique, telles que Microsoft, IBM, 3Com, Ericsson, Motorola, Intel, Lucent, Toshiba, Nokia, etc .

Bluetooth est une norme de communication sans fil à courte portée qui utilise des ondes radios dont la bande de fréquences est de 2,4 pour transmettre des données entre les dispositifs électroniques tels que des ordinateurs portables, des téléphones portables , des imprimantes et des écouteurs. . ..ect

(voir [2]).

• **IEEE 802.11 :** La norme $IEEE$ 802.11 est une spécification pour les réseaux sans fil locaux ($WLAN$), développée par le groupe de travail $IEEE$ 802.11, qui est un comité technique de l'Institute of Electrical and Electronics Engineers ($IEEE$) également connus sous le nom de Wi-Fi. La norme définit les protocoles de communication utilisés pour transférer des données entre les appareils sans fil. La bande passante utilisée par cette norme dépend de la révision de la norme. Les révisions les plus courantes actuellement utilisées sont 802.11ac et 802.11n, qui offrent une bande passante plus élevée que les versions antérieures.

La bande passante théorique maximale pour la norme $IEEE$ 802.11ac est de 6,9 $Gbps$, tandis que pour la norme $IEEE$ 802.11n, elle est de 600 $Mbps$. Cependant, ces vitesses théoriques ne

sont généralement pas atteintes dans des conditions réelles, car elles dépendent de nombreux facteurs tels que la distance, les obstacles, les interférences et le nombre d'appareils connectés [3].

• **Zigbee :** est une norme de réseau de capteurs sans fil à faible consommation d'énergie qui utilise la bande de fréquences de 2,4 GHz, Il est conçu pour les applications à faible débit de données et à longue durée de vie de la batterie, tels que les réseaux de capteurs sans fil pour la surveillance de l'environnement, la sécurité...ect, La norme Zigbee est basée sur la norme $IEEE$ 802.15.4 pour la communication physique sans fil et utilise un protocole de couche supérieure pour la communication de réseau. Il utilise également un maillage de nœuds pour assurer la connectivité du réseau, ce qui signifie que chaque nœud est connecté à plusieurs autres nœuds, créant ainsi une redondance de chemin pour la transmission de données.

La norme Zigbee est gérée par la Zigbee Alliance, Une organisation internationale engagée dans l'avancement et la propagation de la norme Zigbee [4].

1.4.4 Applications des Réseaux ad hoc

Dans un contexte historique, le premier domaine d'application des réseaux ad hoc fut à des fins militaires. Dans les années 1970, le $DARPA$ (Defence Advanced Research Projects Agency) proposent Packet Radio Network

. Ce protocole a été conçu pour établir un mécanisme de communication entre divers groupes d'unités en utilisant des liaisons radio entre les véhicules [30].

Ici, nous allons voir d'autre domaine d'application des $MANETS$ [33] :

• **Applications militaire :**

— Opérations militaire.

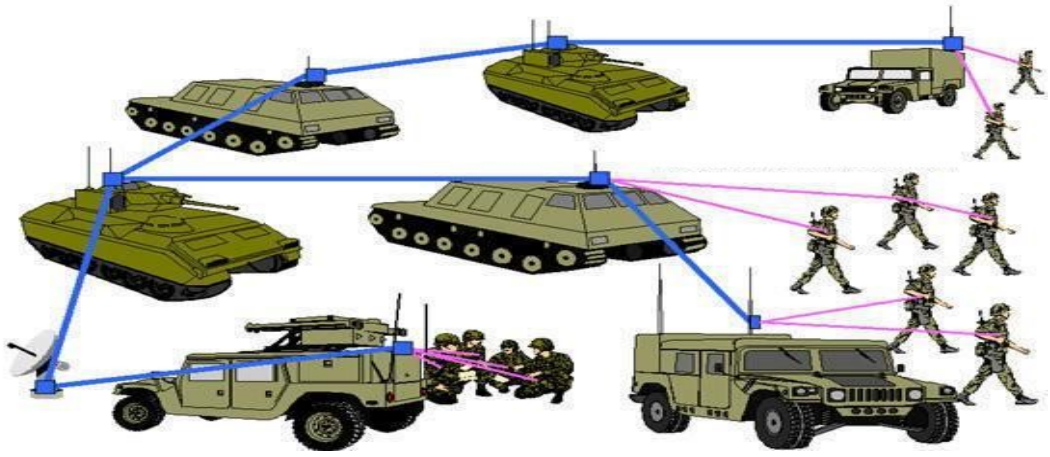

FIGURE 1.5 – Application militaires

• **Réseaux de capteurs (WSN) :**

— Applications domestiques : les nœuds de capteurs intelligents et les actionneurs peuvent être enfouis dans les appareils électroménagers pour permettre aux utilisateurs de gérer les appareils domestiques localement et à distance.

— Application environnementale incluant le suivi des mouvements d'animaux (par exemple, oiseaux et insectes), la détection chimique/biologique, l'agriculture de précision, etc.

— Suivi de données hautement corrélées dans le temps et l'espace, par exemple des capteurs distants pour la météo, les activités terrestres, etc.

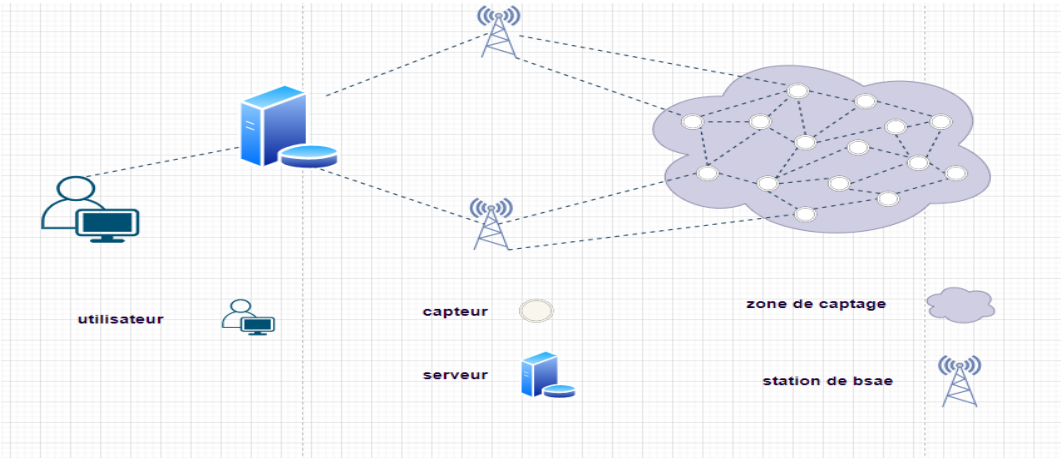

FIGURE 1.6 – Un réseaux de capteurs

• **Services d'urgence :**

— Opérations de recherche et de sauvetage, ainsi que de récupération après une catastrophe ; par exemple, récupération et transmission précoce de données de patients (dossiers, état, diagnostic) de/vers l'hôpital.

— Remplacement d'une infrastructure fixe en cas de tremblement de terre, d'ouragan, d'incendie, etc.

• **Environnements commerciaux :**

— Commerce électronique : par exemple, les paiements électroniques depuis n'importe où (c'est-à-dire les taxis)

— Entreprise :

i. Accès dynamique aux fichiers clients stockés dans un emplacement central sur la volée

— Services de véhicules :

i. Transmission de nouvelles, conditions routières, météo, musique

ii. Réseau ad hoc local avec les véhicules à proximité pour le guidage routier/accident

• **Applications éducatives :**

— Configuration de salles de classe virtuelles ou de salles de conférence

— Configuration de communications ad hoc lors de conférences, de réunions ou de cours Divertissement

1.5 Comparaison entre les deux types de réseaux sans fil :

Caractéristiques	Réseau avec infrastructure	Réseau sans infrastructure
Point central de contrôle	Présence d'un point d'accès ou d'un routeur central qui gère le trafic et les communications. Fournit une couverture	Pas de point central ; les appareils se connectent directement en mode pair-à-pair
Couverture	plus large grâce à des points d'accès bien positionnés.	Les connexions sont limitées
Configuration	Requiert une configuration préalable, notamment pour installer et positionner les points d'accès.	Moins de configuration nécessaire car les appareils se connectent directement
Flexibilité	Moins flexible en termes de déploiement en raison de la nécessité d'installer une infrastructure fixe.	Très flexible, adapté aux environnements où l'infrastructure est limitée ou inexistante
Coût de déploiement	Généralement plus élevé en raison de la mise en place d'infrastructures comme les points d'accès	Généralement moins élevé car il n'y a pas de coût lié à l'installation d'une infrastructure fixe.
Bande passante	Bande passante élevée	Bande passante limitée.
Topologie de réseau	Topologie de réseau statique	Topologie de réseau très dynamique avec multi-sauts.

Table 1.1 – Tableau comparatif entre les deux types de réseau

1.6 Le routage dans les réseaux ad hoc

Définition 1.3.

Le routage consiste à déterminer le chemin à suivre pour transmettre une information à son adresse spécifiée. Il peut être direct si les nœuds émetteur et récepteur se trouvent dans la même portée de transmission, ou nécessiter plusieurs étapes en passant par des points de commutation intermédiaires dans le cas d'une topologie plus complexe. En résumé, le routage implique un ensemble de mécanismes qui assurent le cheminement approprié de chaque paquet en transit afin qu'il atteigne sa destination [46] .

Le routage de réseau est le processus de sélection du chemin le plus approprié pour faire transiter le trafic réseau d'un point à un autre. Cela implique de déterminer le chemin optimal pour les paquets de données à travers un réseau en fonction de facteurs tels que la topologie du réseau, la bande passante disponible et la congestion du réseau. Le routage peut être effectué par des routeurs matériels ou par des logiciels s'exécutant sur des appareils de réseau (voir [ref]).

1.6.1 Modes de communication

Dans les réseaux ad hoc, il existe trois mode de communications comme illustre la figure suivant

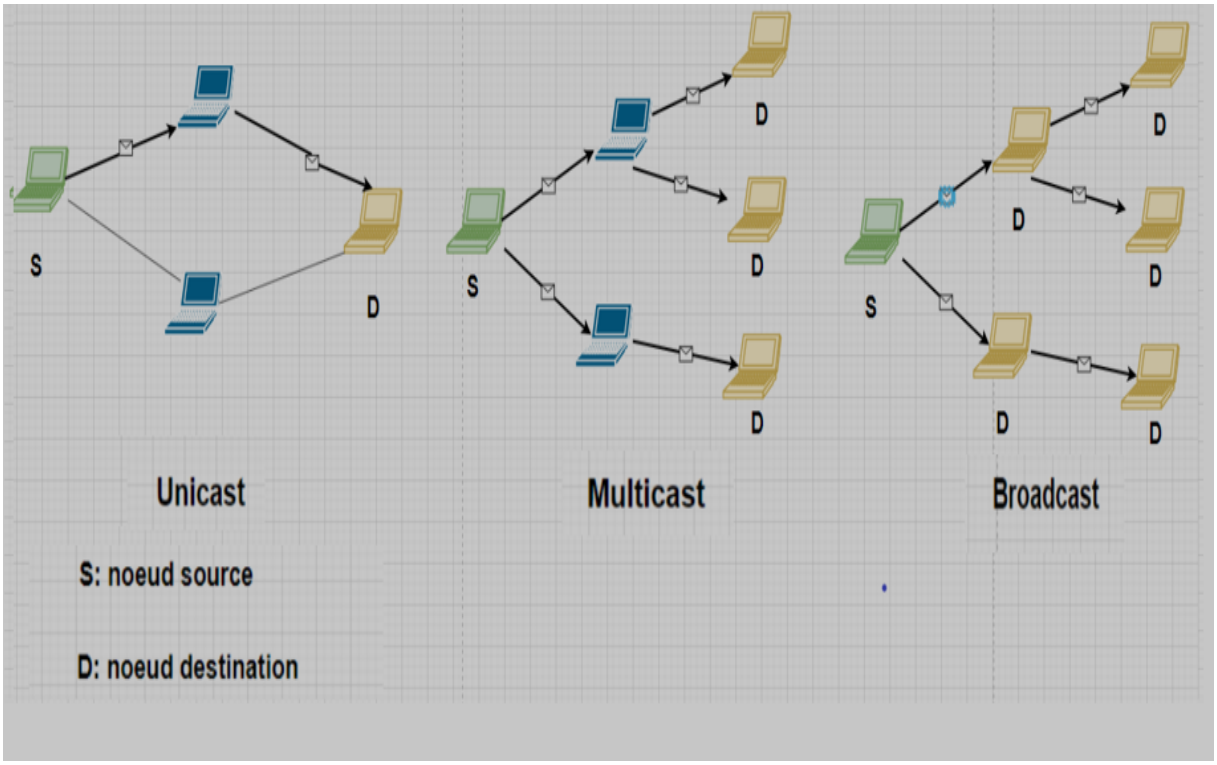

FIGURE 1.7 – Modes de communication

- **Mode unicast :** Il s'agit d'une communication point à point où les données sont dirigées vers une adresse unique, ce qui signifie qu'un seul nœud source communique avec une seule destination.
- **Mode multicast :** est un mode de communication où un émetteur envoie des données à un groupe spécifique de destinataires.
- **Mode broadcast :** c'est le mode de communication où un émetteur envoie des données à tous les nœuds du réseau.

1.6.2 Les protocoles de routage

Étant donné les limitations des réseaux ad hoc, la construction des routes doit être effectuée avec un minimum de contrôle et d'utilisation des ressources telles que la bande passante et l'énergie.

Dans $MANET$, différents types de des protocoles de routage ont été recommandés. Ces protocoles peuvent être classés en trois grandes catégories réactives (à la demande), protocoles de routage proactifs (pilotés par table) et hybrides , à savoir $AODV, OLSR$ *et* ZRP [35].

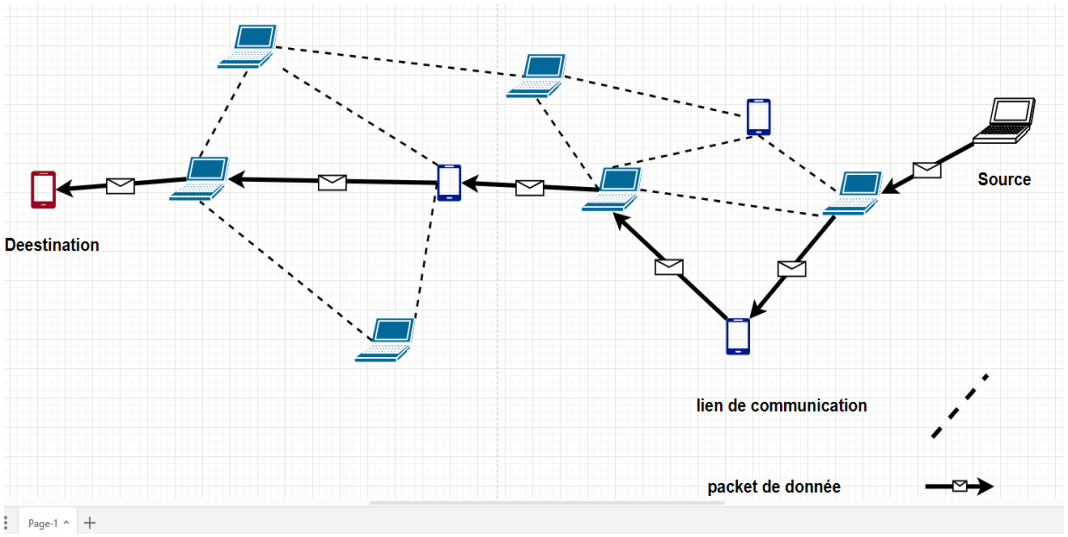

FIGURE 1.8 – Routage dans les réseaux ad hoc

En raison des contraintes des réseaux ad hoc, l'établissement de chemins de communication doit se faire avec une gestion minimale et une utilisation prudente des ressources telles que l'énergie et la bande passante.

Dans les réseaux ad hoc mobiles ($MANET$), différents types de protocoles de routage ont été développés. On peut regrouper ces protocoles en trois catégories principales : réactifs (à la demande), proactifs et hybrides. Parmi eux, on trouve des protocoles tels que $AODV, OLSR$ *et* ZRP [35].

• **Les protocoles de routage proactifs** D'apres le [7]

Les réseaux mobiles ad hoc mettent en œuvre des protocoles de routage proactifs qui reposent sur les mêmes principes que ceux adoptés dans les réseaux conventionnels câblés. Pour comprendre le fonctionnement de ces protocoles, il est essentiel d'examiner les deux principales méthodes de routage présentes dans les réseaux câblés : la méthode Link State (État de Liaison) et la méthode du Vecteur de Distance (Distance Vector). Ces deux méthodes nécessitent une mise à jour régulière des données de routage, diffusées par les différents nœuds de routage du réseau. Le protocole de Link State implique que chaque nœud de routage maintienne son propre vue de la topologie du réseau ainsi que l'état de ses liaisons sortantes. Périodiquement, il diffuse l'état des liaisons de ses voisins à tous les nœuds du réseau pour maintenir cette vue à jour. En revanche, le protocole du Distance Vector opère en diffusant à ses voisins sa perception des distances qui le séparent de tous les hôtes du réseau. Ceci permet à chaque nœud de calculer le chemin le plus court vers n'importe quelle destination en utilisant les informations reçues de tous les nœuds environnants.

Les protocoles de routage proactifs tentent de fusionner les avantages de ces deux approches en les adaptant aux environnements mobiles, tout en prenant en considération les particularités de ces contextes.

Parmi les protocoles proactifs : $DSDV, OLSR, GSR, FSR$, etc.

◇ **DSDV :** Destination Sequenced Distance Vector.

◇ **OLSR :** Optimized Link State Routing.

◇ **GSR :** Global State Routing.

◇ **FSR :** Fisheye State Routing.

Dans ce qui suit, nous allons présenter $DSDV$, un exemple typique des protocoles de routage proactif :

— **Destination sequenced distance vector (DSDV) :**

Le protocole de routage par vecteur de distance organisé par destination est dérivé de l'algorithme distribué de Bellman-Ford (DBF), un algorithme classique de vecteur de distance. Cependant, il comporte des améliorations pour éviter les boucles de routage présentes dans DBF. Cela est réalisé en étiquetant chaque entrée de la table de routage avec un numéro de séquence pour ordonner l'information de routage. Dans le cadre de $DSDV$, chaque nœud maintient une table de routage contenant une entrée pour chaque destination au sein du réseau. Les attributs associés à chaque destination comprennent le prochain saut, le nombre de sauts et un numéro de séquence, transmis par le nœud destinataire. Afin de propager les informations de routage le plus rapidement possible en cas de changement topologique, $DSDV$ utilise à la fois des mises à jour périodiques et des mises à jour déclenchées par des événements.

Les paquets de mise à jour contiennent les destinations accessibles depuis chaque nœud ainsi que le nombre de sauts requis pour les atteindre, tout en incluant le numéro de séquence associé à chaque route. $DSDV$ résout également les problèmes de fluctuation dans les mises à jour de la table de routage en utilisant des données de temps de stabilisation. De ce fait, $DSDV$ garantit des itinéraires sans boucles en permanence. Cependant, il présente plusieurs désavantages, tels que la complexité de la détermination des valeurs

optimales pour les paramètres et la nécessité d'attendre la réception de la prochaine mise à jour de routage émise par la destination avant d'actualiser son entrée dans la table de routage pour cette destination.

De plus, $DSDV$ ne prend pas en charge le routage à plusieurs chemins et peut entraîner une surcharge de messages de contrôle de communication en raison de l'utilisation conjointe de mises à jour périodiques et déclenchées par des événements.

•**Les protocoles de routage réactifs** D'apres [7] et dans la section précédente , nous avons examiné les protocoles de routage proactifs qui ont pour objectif de maintenir les chemins optimaux vers tous les nœuds du réseau au niveau de chaque nœud. Même si ces chemins ne sont pas utilisés activement, ils sont constamment préservés grâce à un échange continu de messages de mise à jour, ce qui peut entraîner une surcharge de contrôle dans les réseaux de grande taille. À l'inverse, les protocoles de routage réactifs, également désignés sous le nom de protocoles de routage à la demande, présentent une solution plus contemporaine pour le routage au sein des réseaux sans fil. La plupart des solutions actuellement étudiées par le groupe de travail $MANET$ de l'IETF appartiennent à cette catégorie de protocoles de routage. Ils répondent au besoin de mise en place de routes à la demande dans les réseaux ad hoc.

Les protocoles de routage relevant de cette catégorie ont pour but de créer et de maintenir les routes en fonction des besoins du réseau. Lorsqu'une route est nécessaire, une procédure de découverte globale est déclenchée pour obtenir des informations spécifiques qui étaient auparavant inconnues. Parmi les protocoles réactifs, on trouve : $DSR, AODV, RDMAR...$ect

◇ **DSR :** Dynamic Source Routing .

◇ **AODV :** Ad hoc On-demand Distance Vector.

◇ **RDMAR :** Relative Distance Micro-Discovery Ad hoc.

Exemple d'un protocole réactif :

— **Ad Hoc On-Demand Distance Vector (AODV) :**

Quand un nœud S souhaite atteindre une destination D, il envoie un message demandant une route à ses voisins, contenant le dernier numéro de séquence pour cette destination. La demande se propage à travers le réseau jusqu'à atteindre un nœud qui a une route pour cette destination. Chaque nœud participant à la diffusion de la demande établit une route inverse vers le nœud S.

Lorsqu'un nœud qui a une route vers D reçoit la demande, il répond avec un message de route contenant le nombre de sauts nécessaires pour atteindre D ainsi que le numéro de séquence le plus récent. Tous les nœuds qui aident à relayer cette réponse établissent également une route vers la destination. Pour maintenir les routes à jour, les nœuds envoient périodiquement des messages HELLO, et si trois messages consécutifs ne sont pas reçus, le lien est considéré comme invalide. Quand un lien devient invalide, tout nœud qui a récemment utilisé ce lien reçoit une réponse de route non sollicitée avec une métrique infinie pour la destination. Cela pousse le nœud à créer une nouvelle route vers cette destination en utilisant la méthode de découverte de route mentionnée précédemment.

Il est important de noter que l'$AODV$ ne fonctionne qu'avec des liens bidirectionnels, ce qui peut présenter un inconvénient.

•**Les protocoles de routage hybride** Protocoles de routage hybrides, combinaison de protocoles de routage réactifs et proactifs. Ils ont été proposés pour réduire la surcharge de contrôle des protocoles de routage proactifs et également pour diminuer la latence causée par la découverte de route dans les protocoles de routage réactifs. Les protocoles de routage hybrides incluent ZRP (Zone Routing Protocol) et $TORA$ (Temporarily Ordered Routing Algorithm) [35]

— **Le protocole ZRP (Zone Routing Protocol) :**
Il est raisonnable de supposer que la majorité des communications ont lieu entre des nœuds situés à proximité les uns des autres. Le protocole ZRP offre un cadre pour les autres protocoles et son comportement est adaptatif. Il se base sur des zones qui sont des groupes de nœuds voisins avec des zones en chevauchement et chaque zone pouvant avoir une taille différente. Le protocole ZRP est constitué de plusieurs composants qui, ensemble, offrent les avantages de ZRP. Chaque composant fonctionne indépendamment pour assurer une efficacité optimale. Les composants de ZRP sont :

◇ **IARP :** Protocole de routage intrazone .

◇ **IERP :** Protocole de routage interzone .

◇ **BRP :** Protocole de résolution de diffusion.

LARP est le premier composant de ZRP. $IARP$ est utilisé pour communiquer avec les nœuds intérieurs de la zone. Si la topologie du réseau change, les nœuds peuvent changer rapidement. Il permet de ne prendre en compte que la route locale.

IERP est le composant global réactif de ZRP. Il utilise une approche réactive pour communiquer avec les nœuds situés en dehors de la zone. Il change la manière dont la découverte de route est gérée. Des requêtes de route sont émises par IERP lorsque la demande de route est faite.

BRP est utilisé pour diriger la demande de route initiée par IERP global réactif. Il est utilisé pour maximiser l'efficacité et augmenter les requêtes discutées [35].

1.7 Comparaison entre les protocoles proactifs et réactifs

Caractéristiques	**Protocoles proactifs**	**Protocoles réactifs**
Découverte de route	Établissent des tables de routage dès le départ, avant même que des requêtes de transmission ne soient reçues	Découvrent les routes en réponse aux demandes de transmission. Aucune table de routage préétablie.
Utilisation de bande passante	Utilisent une certaine quantité de bande passante pour les mises à jour régulières des tables de routage.	Utilisent moins de bande passante car les mises à jour ne se produisent que lorsque des demandes de transmission sont générées
Efficacité de la bande passante	Moins efficaces en termes d'utilisation de la bande passante car les mises à jour se produisent même si aucune transmission n'est en cours.	Plus efficaces en termes d'utilisation de la bande passante car les mises à jour ne surviennent que lorsque des transmissions sont nécessaires
Adaptabilité aux changements	Moins adaptatifs aux changements de topologie car les tables de routage ne sont pas mises à jour en temps réel.	Très adaptatifs aux changements de topologie car les routes sont calculées en temps réel en réponse aux demandes de transmission.
Energie	Consommation énergétique plus importante	Consommation énergétique réduite
Échelle de réseau	Adaptés aux réseaux de taille moyenne	Adaptés aux grands réseaux.
réactivité	Pas de temps de réaction	Temps de réaction long

TABLE 1.2 – Tableau comparatif entre les protocoles de routage proactif et réactifs

1.8 Conclusion

Dans ce chapitre, une vue d'ensemble des réseaux ad hoc a été présentée, mettant en évidence leur domaine d'application ainsi que les mécanismes de routage qui y sont associés. Comme observé, ces réseaux se démarquent par leur simplicité, leur déploiement rapide et leur faible coût, attribuables à l'absence de câblage et d'infrastructure fixe. Toutefois, ces caractéristiques inhérentes exposent ces réseaux à de multiples vulnérabilités informatiques. Malgré la diversité des solutions de sécurité présentées dans la littérature, la protection de ces réseaux reste un défi majeur et un problème qui reste ouvert à la recherche. Le chapitre suivant mettra en évidence cette problématique en examinant les différentes attaques informatiques ciblant les réseaux ad hoc, ainsi que les approches qui ont été proposées pour relever ces défis.

Chapitre 2

Sécurité dans les réseaux ad hoc

2.1 Introduction

Les réseaux ad hoc sont des réseaux de communication sans fil où les nœuds sont mobiles et peuvent se connecter dynamiquement les uns aux autres sans avoir besoin d'une infrastructure fixe. Bien que ces réseaux offrent une grande flexibilité et une grande portabilité, ils présentent également des défis importants en matière de sécurité.

Les réseaux ad hoc sont particulièrement vulnérables aux attaques de sécurité, car les nœuds du réseau ne sont pas toujours fiables et peuvent être compromis ou malveillants. Les attaques les plus courantes dans les réseaux ad hoc sont le détournement de paquets , l'usurpation d'identité, le brouillage, l'injection de fausses données et le déni de service.

La sécurité dans les réseaux ad hoc est donc essentielle pour garantir la disponibilité, l'intégrité, et la confidentialité des données échangées entre les nœuds du réseau. Afin d'assurer la sécurité des réseaux ad hoc, différentes méthodes de protection ont été suggérées, notamment l'authentification, la cryptographie, la détection d'intrusion et la gestion de clés.

Dans le présent chapitre, nous allons examiner les diverses catégories d'attaques de sécurité au sein des réseaux ad hoc, les techniques de sécurité les plus courantes utilisées pour protéger ces réseaux, ainsi que les défis et les limites de la sécurité dans les réseaux ad hoc.

2.2 Vulnérabilité des réseaux ad hoc

• **Absence de gestion centralisée :** les $MANET$ ne disposent pas d'un serveur de surveillance centralisé. ce qui complique la détection des attaques en raison de la difficulté de surveiller le trafic au sein d'un réseau ad hoc à la fois hautement dynamique et étendu. Cette absence de gestion centralisée engendre aussi des défis en ce qui concerne la gestion de la confiance entre les nœuds (voir [47]).

• **Scalabilité :** La mobilité des nœuds au sein des réseaux ad hoc provoque un changement constant de leur échelle, ce qui pose un défi majeur en matière de sécurité. Les mécanismes de sécurité doivent donc être capables de s'adapter à des réseaux de grande taille, tout en restant efficaces pour des réseaux de plus petite taille.

Par conséquent, les protocoles et services appliqués au réseau ad hoc, tels que le protocole de routage et le service de gestion de clés, doivent être compatibles avec l'échelle en évolution continue du réseau ad hoc [31].

• **Contrainte d'énergie :** Certains ou tous les nœuds d'un MANET peuvent dépendre de batteries ou d'autres sources limitées pour leur énergie. Cela peut causer des problèmes de sécurité, notamment les attaques de déni de service où les attaquants peuvent cibler ces nœuds en envoyant continuellement des paquets supplémentaires ou en les piégeant dans des calculs longs ou infinis, ce qui consomme leur énergie. Par conséquent, le nœud cible sera hors service pour toute utilisation légitime, car il a consommé toute son énergie [31].

• **Bande passante limitée :** Les réseaux ad hoc ont des liens sans fil à capacité variable et faible qui sont plus susceptibles aux interférences, au bruit externe et à l'atténuation du signal [28].

2.3 Les défis de sécurité dans les réseaux manet

En général, il y a deux aspects importants en matière de sécurité : les services de sécurité et les attaques. Les services de sécurité font référence à des politiques de protection visant à assurer la sécurité du réseau, tandis que les attaques exploitent les vulnérabilités du réseau pour contourner un service de sécurité. Dans les deux parties suivantes, nous présentons une brève discussion sur ces aspects de sécurité.

2.3.1 les Services de sécurité

Le défi de sécuriser les réseaux $MANET$ est complexe en raison des caractéristiques particulières de ces réseaux. Pour fournir un niveau de sécurité adéquat, il est essentiel de trouver un compromis entre les différents services de sécurité. cinq services de sécurité importants sont présentés avec leurs défis respectifs :

• **Authentification :** L'objectif de ce service vise à garantir des communications fiables entre deux nœuds distincts. Lorsqu'un nœud reçoit des paquets en provenance d'une source, il doit être certain de l'identité du nœud émetteur. Une manière de fournir ce service est d'utiliser des certificats.

• **Confidentialité :** Le service de confidentialité implique que chaque nœud ou application doit avoir accès uniquement aux services spécifiés auxquels il est autorisé à accéder. La plupart des services assurant la confidentialité des données recourent à des méthodes de chiffrement. Cependant, en l'absence d'une autorité de contrôle centralisée, la distribution et la gestion des de clés deviennent plus compliquées [1].

• **Intégrité :** C'est le service qui garantit qu'un message n'est pas modifié intentionnellement ou non pendant la transmission, ce qui signifie que le message reçu est le même que celui qui a été envoyé [50] . Pour garantir ce service, on peut utiliser les fonctions de hachage.

• **La non-répudiation :**Est un service qui garantit qu'une entité ne peut pas nier avoir émis ou reçu un message. Dans les réseaux ad hoc, ce service est très important , car les nœuds peuvent agir de manière malveillante en niant leur participation à des actions malveillantes ou en accusant à tort d'autres nœuds. [13] Parmi les techniques qui peuvent assurer ce service,

on trouve la signature numérique, qui attribue une signature unique à chaque message envoyé, empêchant ainsi les nœuds de nier l'envoi de ces messages.

• **Disponibilité :** Ce service de sécurité garantit à chaque nœud autorisé un accès constant aux données et aux services au sein du réseau. Cependant, les réseaux ad hoc mobiles, avec leur topologie dynamique et leur environnement ouvert, présentent des défis pour maintenir cette disponibilité. Le temps d'accès, mesuré comme la durée nécessaire à un nœud pour atteindre les services ou les données du réseau, joue un rôle important en matière de sécurité. Ainsi, gérer efficacement cette dimension de la disponibilité est crucial pour assurer des communications fluides et fiables au sein du réseau [42] .Pour garantir ce service, plusieurs techniques telles que la tolérance aux pannes, la détection et la prévention des intrusions, etc., sont utilisées.

2.4 Les attaques dans les réseaux ad hoc

Les attaques au sein des réseaux ad hoc peuvent être classées selon différents critères, comme le montre la figure. Elles peuvent être catégorisées en fonction de l'action malveillante (passive, active) ou de leurs sources (interne, externe).

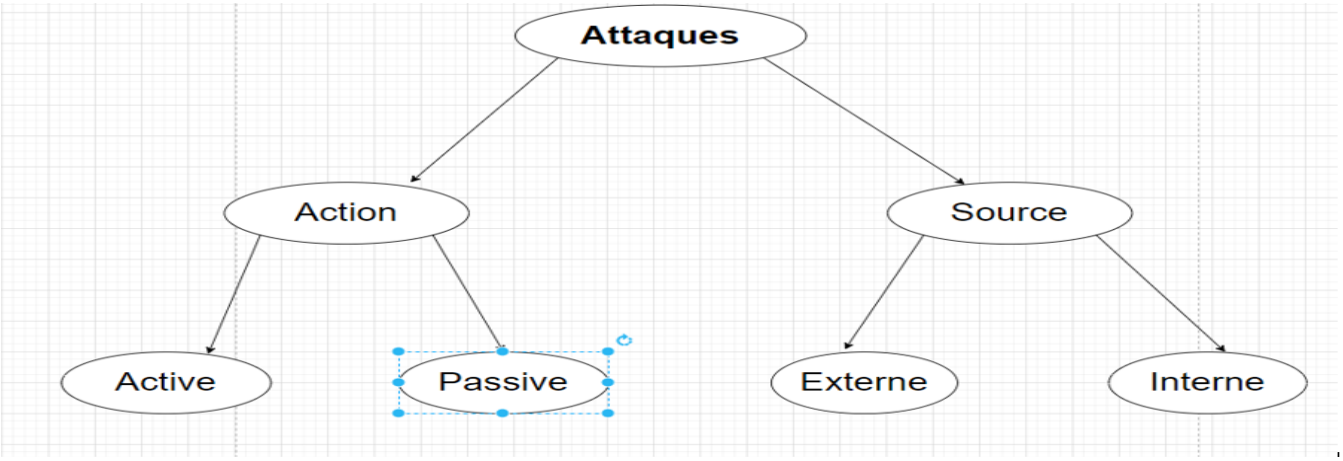

FIGURE 2.1 – Classification des attaques

2.4.1 Attaques internes vs attaques externes :

Une attaque externe se produit lorsqu'un nœud malveillant, n'appartenant pas au réseau, déclenche une attaque ayant pour but de causer de la congestion, de propager de fausses informations de routage ou de perturber le fonctionnement des nœuds légitimes dans le réseau [32].

Par contre, une attaque interne se produit à l'intérieur du réseau, où l'attaquant peut prendre part à la communication entre les nœuds. un nouveau nœud introduit dans le réseau peut se comporter en tant qu'attaquant après avoir obtenu un accès au réseau. cet accès peut être

obtenu soit par la conclusion d'un accord avec un nœud déjà existant, soit en se faisant passer pour un autre nœud.

Il est très difficile de prédire les attaques internes par rapport aux attaques externes [15].

Les attaques de sécurité dans les $MANET$ peuvent être classées en deux gatégories principales : les attaques passives et les attaques actives.

2.4.2 Les attaques actives et passives :

• **Les attaques passives :** Les attaques passives sont des attaques où un attaquant non autorisé observe et surveille les communications sans perturber les échanges ou causer des dommages directs au système ciblé. l'objectif principal des attaques passives est de recueillir des informations confidentielles ou des données sensibles en vue d'attaques futures plus nuisibles sans être détecté. Les exemples courants d'attaques passives incluent l'écoute clandestine, l'analyse de trafic et la collecte d'informations [43].

Voila un exemple d'une attaque de type passive :

— `Attaque d'écoute indiscrète (Eavesdropping Attack)` : L'écoute indiscrète désigne une tentative illégale de surveiller secrètement les communications privées entre deux parties légitimes ou plus. Cette pratique consiste à intervenir et à lire des messages ainsi que des conversations à l'aide des récepteurs non autorisés. Dans la figure 6, l'attaquant C surveille attentivement l'acquisition d'informations confidentielles qui doivent rester secrètes entre les deux parties A et B autorisées en communication. Ces informations confidentielles peuvent inclure des clés privées, des clés publiques, des emplacements ou des mots de passe des nœuds.

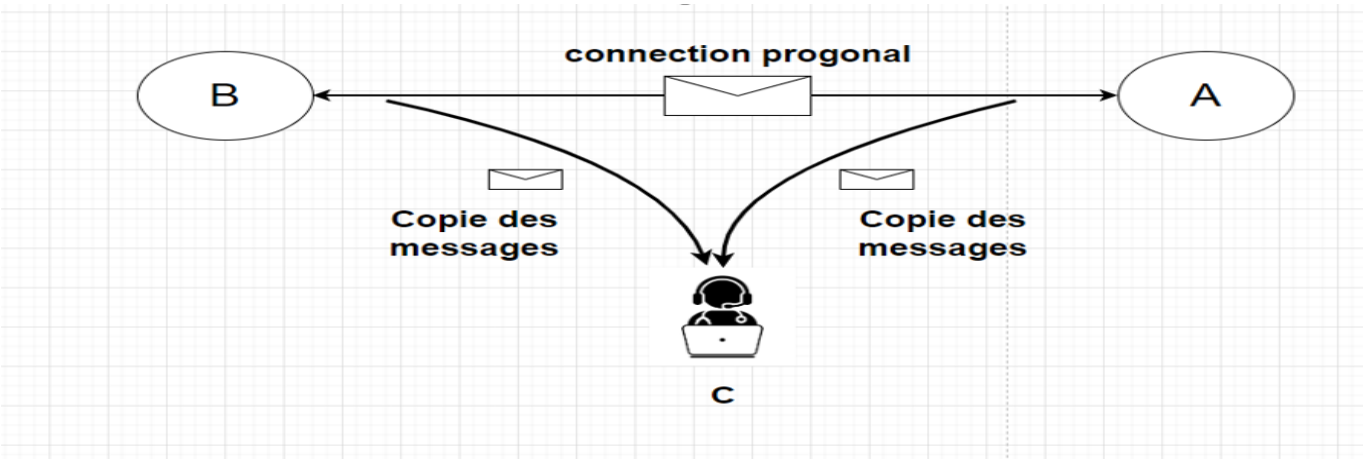

FIGURE 2.2 – Eavesdropping attack

Pour contrer les attaques passives, différentes techniques de sécurité peuvent être mises en œuvre, telles que l'authentification des utilisateurs, le cryptage des données et la surveillance de l'activité du réseau. Le cryptage des données vise à protéger les informations contre l'écoute clandestine, tandis que l'authentification des utilisateurs garantit que seules

les personnes autorisées peuvent accéder aux informations ou aux services. La surveillance de l'activité du réseau peut aider à détecter les comportements suspects et à prévenir les attaques passives avant qu'elles ne deviennent un problème majeur [8].

• **Les attaques actives :** D'apres [43] Les attaques actives sont des attaques malveillantes qui provoquent des changements non autorisés dans l'état du réseau, telles que la modification, la suppression de paquets, , l'usurpation d'identité ,le déni de service, etc. Contrairement aux attaques passives, les attaques actives impliquent une interaction avec le réseau. Ces des attaques qui cherchent à causer des dommages directs au réseau en altérant les données ou en perturbant le trafic.

Les attaques actives sont généralement lancées par des utilisateurs ou des nœuds autorisés à opérer dans le réseau, ce qui les rend plus difficiles à détecter et à prévenir que les attaques passives. Les attaques actives se divisent en plusieurs catégories, parmi lesquelles on peut citer :

— textbfAttaques de suppression, modification et fabrication : Ces types d'attaques ciblent les réseaux ad hoc avec des conséquences potentiellement dangereuses. Dans les attaques de suppression, les paquets légitimes sont intentionnellement éliminés, entraînant des retards, des pertes de données et des pannes de communication. Les attaques de modification altèrent le contenu ou la destination des paquets, ce qui présente des risques pour les nœuds et les utilisateurs en compromettant l'intégrité des données. Les attaques de fabrication introduisent des paquets malveillants dans le réseau, perturbant le flux de trafic et ouvrant la voie à des attaques de déni de service. Parmi ces attaques, on trouve :

◇ `BlackHole attack :` Lors d'une attaque de type "trou noir", un nœud malveillant exploite le protocole de routage pour se faire passer comme ayant le chemin le plus court vers le nœud ciblé afin d'intercepter ses paquets. Dans les protocoles de type inondation, si la réponse malveillante atteint le nœud demandeur avant la réponse provenant du nœud légitime, une fausse route est créée. Ce nœud malveillant peut alors décider de supprimer les paquets [6].

Deux types d'attaques de trou noir peuvent être distingués :

i. *Attaque de trou noir interne :* Le nœud malveillant est un nœud interne qui ne cherche pas à s'insérer dans une route active entre une source donnée et une destination. Si par hasard ce nœud malveillant fait partie d'une route de données active, il peut immédiatement lancer son attaque dès le début de la transmission des données. Cette attaque est interne car le nœud malveillant fait déjà partie de la route de données. Dans ce cas, il n'y a aucune violation de la spécification du protocole de routage, et le nœud malveillant n'a rien à faire pour mener son attaque.

ii. *Attaque de trou noir externe :* Le nœud malveillant est un nœud externe qui cherche à s'insérer dans une route active. Pour cela, il viole les spécifications du protocole de routage et exécute le processus d'attaque [6].

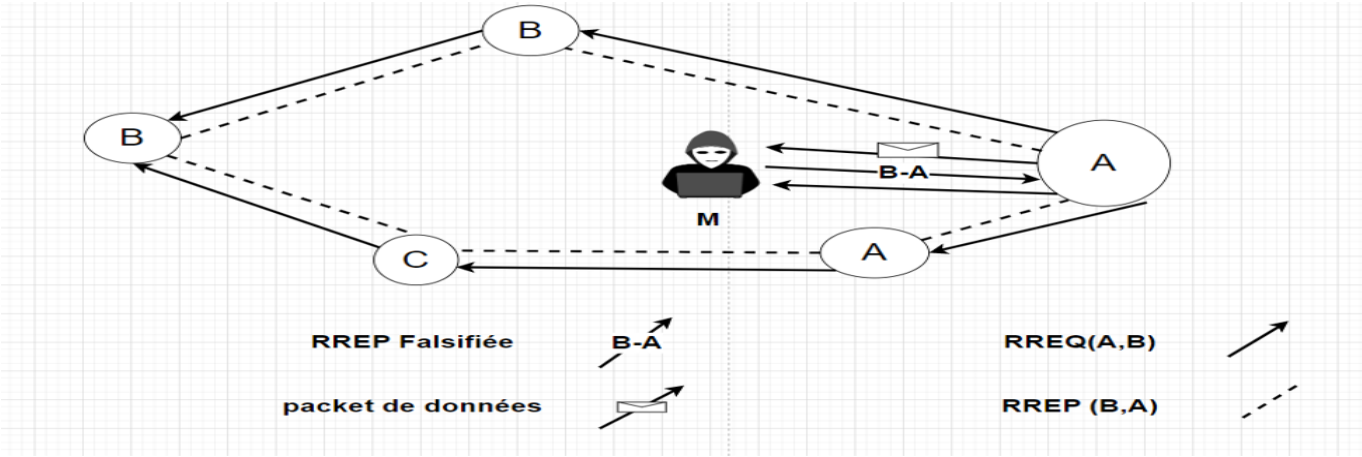

FIGURE 2.3 – Attaque blackhole

◇ **Gray Hole Attack :** L'attaque de "trou gris" représente une variante de l'attaque du "trou noir", où un nœud malveillant se comporte initialement comme un nœud honnête pendant le processus de découverte de la route. Ensuite, de manière silencieuse, il rejette certains ou la totalité des paquets de données qui lui sont destinés pour être transmis, même en l'absence de congestion. Les attaques GrayHole sont plus difficiles à détecter car elles ne provoquent pas toujours une perte totale de connectivité, mais elles peuvent entraîner une communication incorrecte ou incohérente.

— **Les attaques d'identité :** Ce type d'attaque consiste à ce qu'un nœud malveillant utilise l'identité d'un autre nœud légitime dans le réseau, voire même exploite un ensemble d'identités dans le réseau pour tromper les autres nœuds et exécuter des actions malicieuses. Cette catégorie d'attaques inclut :

◇ **Spoofing attaque :** une attaque dans laquelle un nœud malveillant usurpe l'identité d'un autre nœud légitime (son adresse IP ou son adresse MAC), envoyant ainsi des messages aux autres nœuds sous le nom de la victime. Cette usurpation permet à l'attaquant d'éviter à l'attaquant d'éviter d'être rejeté du réseau et peut également servir de base pour d'autres attaques.

◇ **Sybil attaque :** : Ce type d'attaque décrit la situation dans laquelle un nœud malveillant tente de créer de nombreuses fausses identités fictives au sein du réseau. dans cette attaque les nœuds malveillants peuvent tromper les

autres nœuds du réseau et manipuler les mécanismes de contrôle et de prise de décision [38].

Une des conséquences de l'attaque Sybil est la possibilité de fausser l'agrégation d'informations ou de votes. Par exemple, si un mécanisme d'agrégation des données est utilisé pour prendre des décisions collectives, un nœud malveillant avec plusieurs identités fictives peut influencer les résultats en soumettant plusieurs fausses informations.

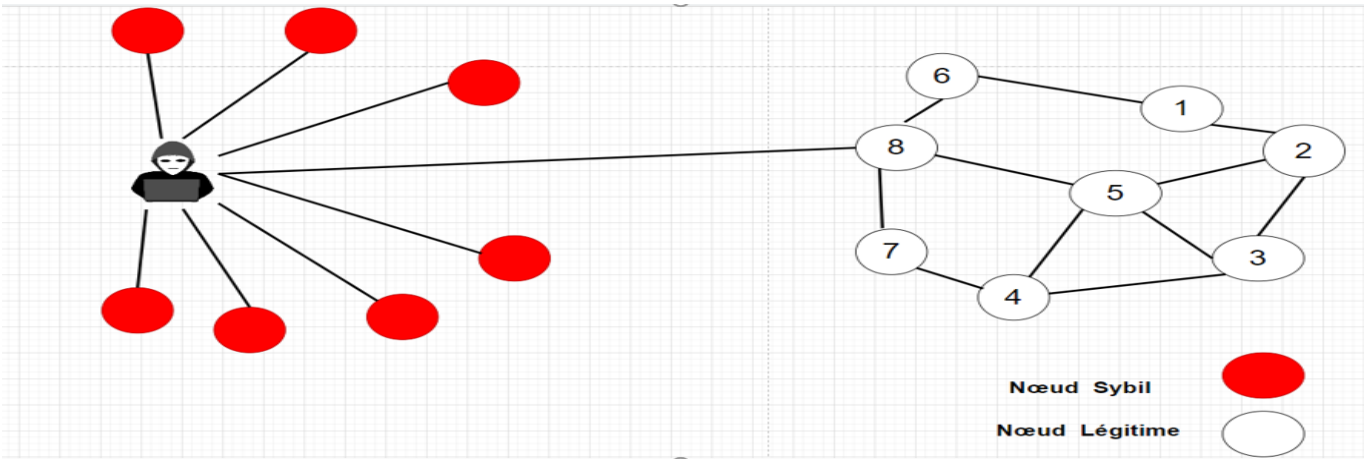

FIGURE 2.4 – Un exemple d'une attaque sybil

◇ **Man in the Middle attack :** L'attaque de l'homme du milieu (Man-in-the-middle) dans les réseaux ad hoc est une menace majeure pour la sécurité des communications entre les nœuds légitimes. Cette attaque se produit lorsque un attaquant parvient à insérer son propre nœud malveillant entre deux nœuds légitimes qui tentent d'établir une connexion. L'attaquant se positionne ainsi comme un intermédiaire invisible dans la communication, et trompe les nœuds légitimes en les faisant croire qu'ils communiquent directement entre eux.

Une fois que l'attaquant a réussi à infiltrer le réseau ad hoc, il peut surveiller et intercepter toutes les données échangées entre les nœuds légitimes, et il peut également manipuler les informations en supprimant des messages ou en les modifiant...etc. Dans certains cas, l'attaquant peut même usurper l'identité de l'expéditeur ou du destinataire afin de tromper les nœuds légitimes.

Cette attaque peut avoir des conséquences graves sur la disponibilité, l'intégrité, et la confidentialité des données dans le réseau ad hoc. Les informations sensibles peuvent être exposées, les communications légitimes peuvent être perturbées ou altérées, et la confiance entre les nœuds légitimes peut être compromise [5].

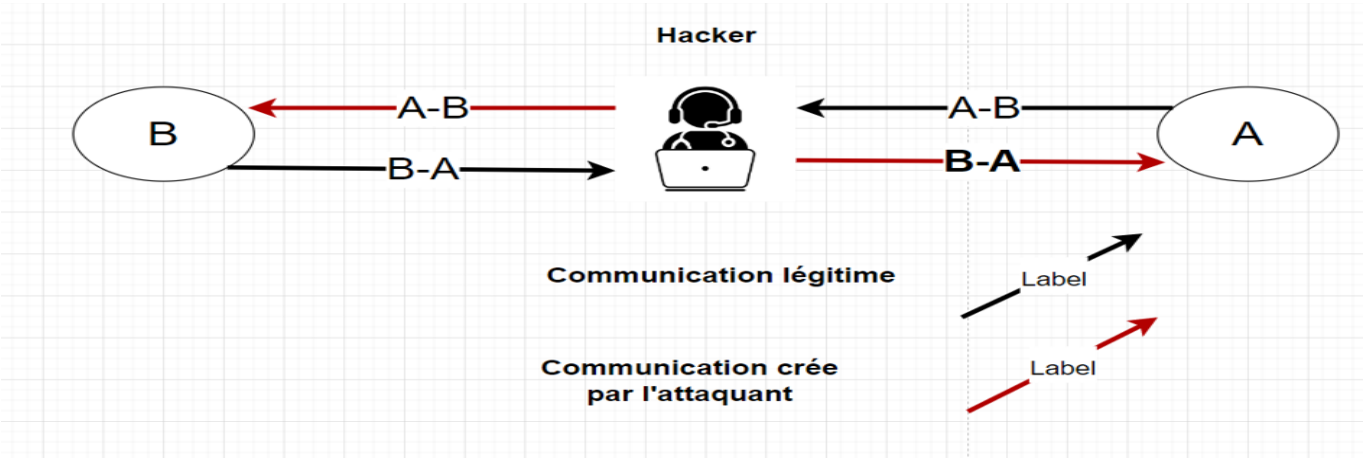

FIGURE 2.5 – Attaque de l'homme du dilieu

— **Les attaques de perturbation de fonctionnement de réseau :** Ces attaques visent à perturber ou compromettre le fonctionnement normal du réseau en épuisant les ressources des nœuds victimes, en saturant la bande passante , et rendant ainsi les communications impossibles ou très difficiles.

Parmi ces attaques :

◇ `Attaque de déni de service` (*dos*): Il s'agit d'une forme d'attaque dans laquelle un attaquant tente de rendre un service ou une ressource inaccessible en saturant la bande passante, en épuisant les ressources système, ou en exploitant une vulnérabilité dans le système cible. Les attaques par déni de service visent à empêcher les utilisateurs légitimes d'accéder au réseau ou à la ressource cible.

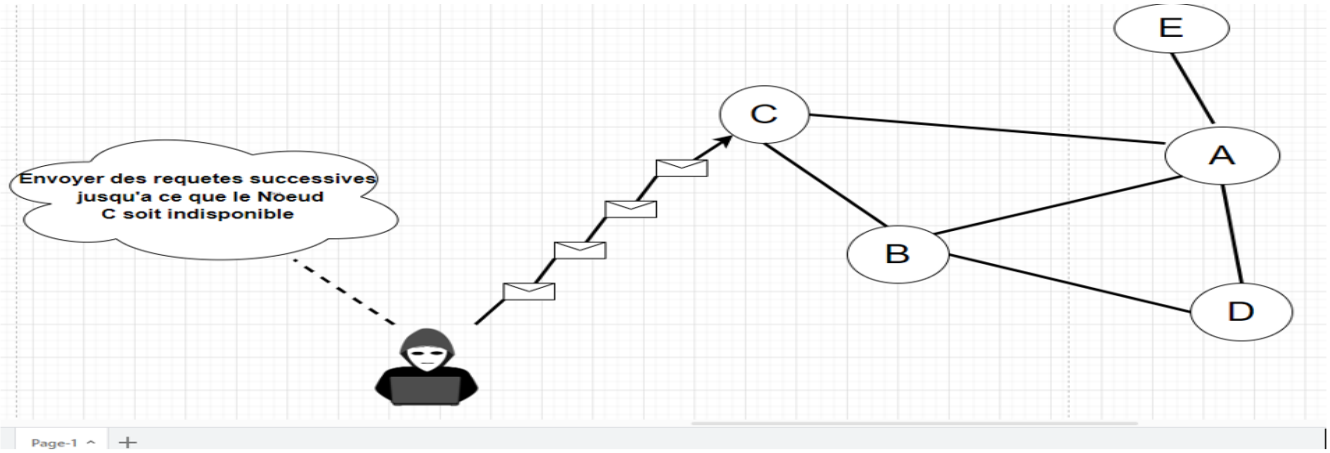

FIGURE 2.6 – Un exemple d'attaque par déni de service

◇ `Attaques de brouillage (Jamming Attack):` ces attaques consistent à émettre des signaux radio pour perturber la communication normale des nœuds du réseau. Cela peut entraîner une interruption de service ou à une perte de données .

◇ SYN `Flooding attack :` Lors d'une attaque SYN flooding dans un $MANET$, un nœud malveillant envoie intentionnellement un grand nombre de paquets SYN frauduleux à d'autres nœuds du réseau. Normalement, lors de l'établissement d'une connexion TCP, un nœud envoie un paquet SYN à un autre nœud, qui répond avec un paquet $SYN + ACK$, puis le premier nœud envoie un paquet ACK pour finaliser la connexion.

Cependant, dans une attaque SYN flooding, l'attaquant n'envoie pas les paquets ACK nécessaires pour finaliser les connexions. Cela entraîne l'accumulation de connexions TCP à moitié ouvertes sur les nœuds victimes, épuisant ainsi leurs ressources, telles que la mémoire et la capacité de traitement. En conséquence, les nœuds victimes deviennent incapables de traiter de nouvelles connexions légitimes, entraînant une perturbation du réseau et un déni de service (voir figure suivante :SYN flooding attack [9].

— **Attaque par rejoue :** Dans cette forme d'attaque, l'attaquant intercepte et mémorise des données légitimes échangées entre les nœuds de réseau. Par la suite, ces données sont réinsérées et reproduites, créant ainsi un "rejoue" des informations dans le réseau. L'objectif est de déclencher des actions indésirables ou malveillantes en dupliquant les données légitimes déjà échangées. Cette classe d'attaques inclut :

◇ `Wormhole attaque :` une attaque de wormhole (ou attaque de ver) est une attaque de sécurité dans laquelle un nœud malveillant capture des paquets à un endroit du réseau et les "tunnelise" vers un autre nœud malveillant situé à distance, qui les rejoue localement. Cette création d'un tunnel virtuel permet aux paquets tunnelisés d'arriver plus tôt ou avec moins de sauts par rapport aux paquets transmis via des routes multihop normales, créant ainsi l'illusion que les deux extrémités du tunnel sont très proches l'une de l'autre. Les nœuds malveillants utilisent ce tunnel pour compromettre le fonctionnement des protocoles de routage et l'intégrité des données circulant dans le réseau, en lançant par exemple des attaques de suppression sélective de paquets ou en attirant le trafic de routage à travers le tunnel [37].

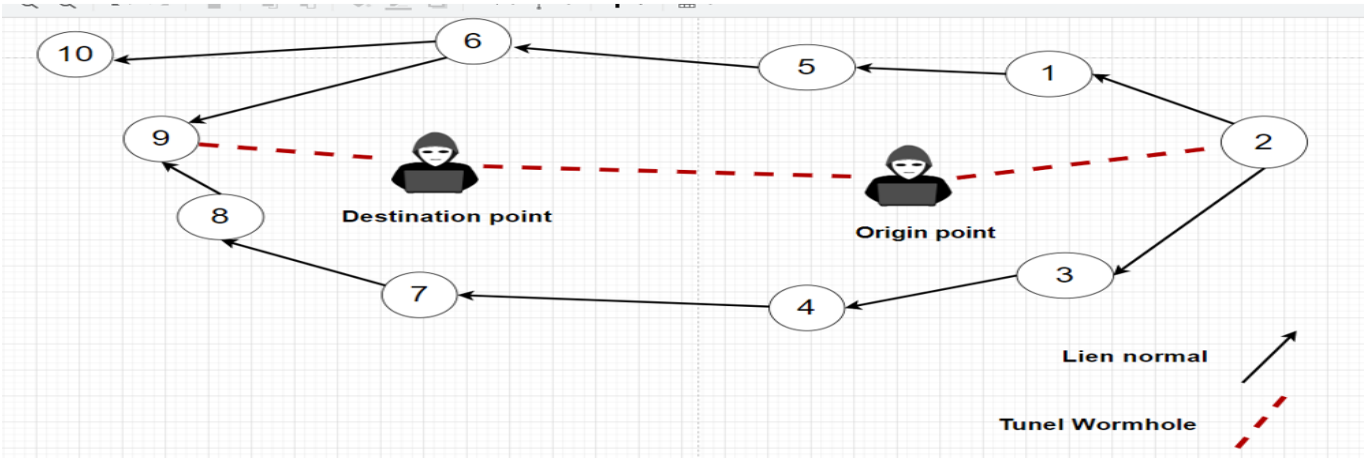

FIGURE 2.7 – Wormhole attaque

2.5 Les techniques et mécanismes de sécurité dans les réseaux ad hoc

Comme on as vu , les réseaux $MANETS$ sont vulnérables a plusieurs types d'attaques, Pour atténuer ces risques, plusieurs mécanismes de sécurité peuvent être utilisés, voici quelques-uns des mécanisme couramment utilisés :

2.5.1 Cryptographie

La cryptographie est l'application des techniques mathématiques et informatiques visant à sécuriser les informations de manière à les rendre incompréhensibles pour les personnes non autorisées. Elle implique l'utilisation de méthodes de chiffrement pour transformer un message clair en un message chiffré à l'aide d'une clé. Le processus inverse, appelé déchiffrement, permet de reconvertir un message chiffré en un message clair. Il y a deux formes de cryptographie :

•**Cryptographie symétrique** Dans ce genre de cryptographie, une seule clé est nécessaire pour à la fois le chiffrement et le déchiffrement. Cela signifie qu'une fois que l'entité émettrice a crypté les données avec cette clé, l'entité réceptrice peut les déchiffrer en utilisant la même clé. Parmi les systèmes de chiffrement symétrique les plus couramment utilisés, on trouve DES *et* AES.

◇ DES **:** Data Encryption Standard.

◇ AES **:** Advanced Encryption Standard.

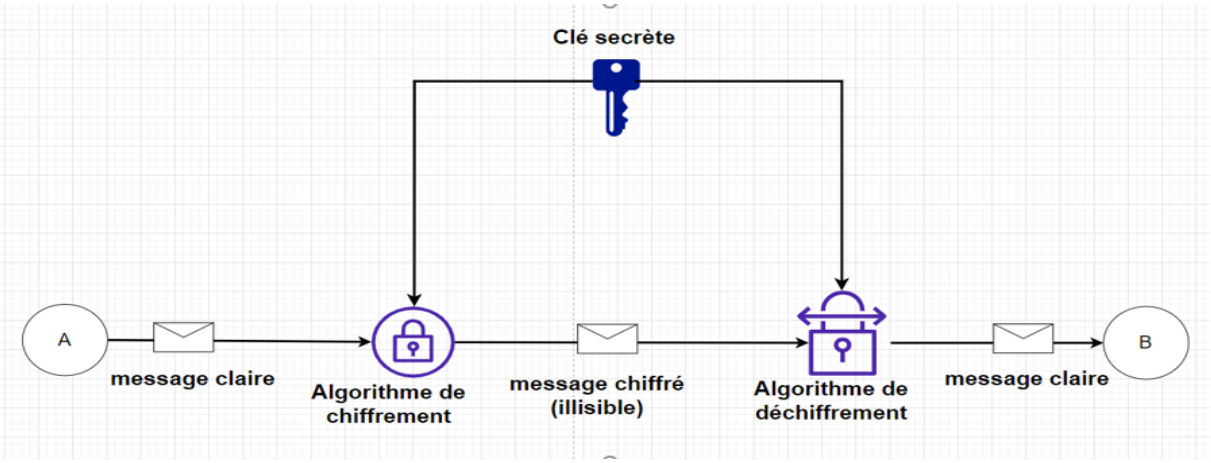

FIGURE 2.8 – Cryptographie symétrique

•Cryptographie asymétrique

est un type de cryptographie qui utilise une paire de clés distinctes pour le chiffrement et le déchiffrement des données, Cette paire de clés est composée d'une :

— `Clé publique :` la clé publique est distribuée et accessible à toutes les entités, elle est utilisée pour chiffrer les données par l'émetteur avant de les envoyer au destinataire.

— `Clé privée :` La clé privée est une clé secrète unique pour chaque entité, elle est utilisée pour déchiffrer les données cryptées reçus a l'aide de la clé publique correspondante. La clé privée ne doit pas être partagée avec d'autres entités.Parmi les systèmes de chiffrement symétrique les plus couramment utilisés, on trouve *RSA*, Diffie-Helleman et *ECC*.

◇ **ECC :** Elliptic Curve Cryptography.

◇ **RSA :** Rivest-Shamir-Adleman.

La figure suivant,montre le fonctionnement de ce type de cryptage :

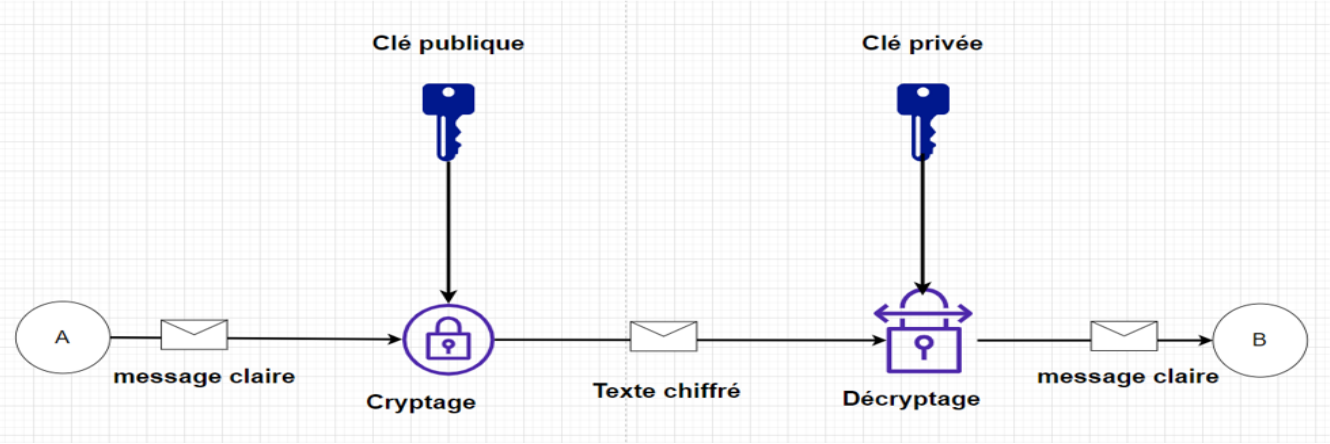

FIGURE 2.9 – Cryptographie asymétrique

2.5.2 Les fonctions de hachage

Une fonction de hachage est une fonction qui prend en entrée des données de longueur variable (telles qu'un message pouvant contenir des milliers ou des millions de bits) et produit en sortie un élément de longueur fixe appelé 'haché' "ou " empreinte " , est une fonction a sens unique, ca veux dire il est impossible de retrouver le message original a partir de l'empreinte calculer. [14] , Elles sont utilisées pour vérifier l'intégrité des données, stocker les mots de passe de manière sécurisée, générer des signatures numériques, créer des identifiants uniques pour les fichiers..ect

En cas de modification des données d'entrée, même d'un seul bit, la fonction de hachage garantit la génération d'une valeur de sortie totalement différente.

Les fonctions de hachage sont largement utilisées en cryptographie et dans d'autres domaines, Des exemples de fonctions de hachage couramment utilisées incluent $MD5$, $SHA-1$, $SHA-256$ *et* $SHA-3$.

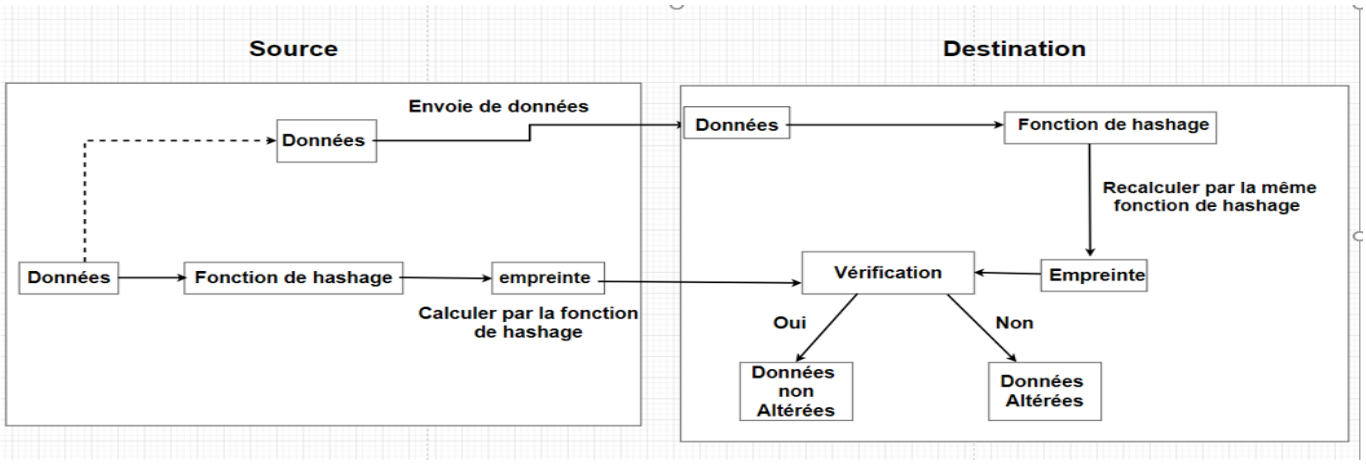

FIGURE 2.10 – Fonction de hachage

2.5.3 La signature numérique

Est un mécanisme cryptographique permettant à un destinataire de vérifier l'intégrité ,l'authenticité et la non répudiation d'un message. Cette méthode s'appuie sur l'usage de la cryptographie asymétrique et les fonctions de hachage .

Voici comment fonctionne le processus de signature numérique :

- `Hachage :` Tout d'abord, le message ou les données d'origine sont soumis à une fonction de hachage, qui génère une empreinte numérique(un haché).
- `Chiffrement :` Ensuite, l'émetteur utilise sa clé privée pour chiffrer l'empreinte générée précédemment. Le chiffrement avec la clé privée crée la signature numérique.
- **Création d'un message signée :** La signature numérique est attachée au message d'origine, formant un message signé.
- `Vérification :` Le récepteur utilise la clé publique de l'émetteur pour décrypter la signature numérique et obtenir l'empreinte correspondante. Ensuite, il applique la fonction de hachage au message ou aux données d'origine reçus pour générer une nouvelle empreinte.
- `Comparaison des empreintes :` Le destinataire compare l'empreinte obtenue à partir de la vérification avec l'empreinte déchiffrée de la signature. Si les deux empreintes correspondent, cela indique que le message n'a subi aucune modification depuis qu'il a été signé et que l'émetteur est authentique.

2.5.4 Certificats numériques

Un certificat numérique est un fichier électronique qui lie de manière cryptographique la clé publique d'une entité, à des informations d'identification spécifiques à cette entité , ces certificats sont délivrés par des autorités de certification (CA), des entités de confiance qui vérifient l'identité des propriétaires avant de leur délivrer un certificat [17].

2.5.5 Mécanismes de vérification de voisinage

Dans les réseaux ad hoc, il est essentiel de s'assurer que les nœuds voisins sont authentiques et fiables. Des mécanismes de vérification de voisinage peuvent être utilisés pour évaluer l'intégrité des nœuds adjacents et détecter les comportements suspects. Voici quelques exemples :

- `Échange de certificats numériques :` Les nœuds adjacents peuvent s'échanger des certificats numériques pour vérifier l'identité et l'authenticité de chaque nœud.
- `Mécanismes de vérification d'intégrité :` Les nœuds peuvent utiliser des mécanismes de vérification d'intégrité pour détecter les modifications non autorisées ou les altérations des informations échangées avec les nœuds voisins.
- `Mécanismes de surveillance du voisinage :` Les nœuds peuvent surveiller le comportement de leurs voisins et détecter les comportements suspects ou malveillants, tels que les nœuds qui envoient un trafic excessif ou qui tentent d'interférer avec les communications.

2.5.6 Mécanismes de confiance

Les réseaux ad hoc peuvent mettre en place des mécanismes de confiance pour évaluer la fiabilité et la crédibilité des nœuds participants. Ceci peut contribuer à prendre des décisions de routage plus fiables et à prévenir les nœuds malveillants ou compromis [10]

Voici un exemple :

- `Validation basée sur l'historique :` Les nœuds peuvent se baser sur l'historique des interactions passées avec d'autres nœuds pour évaluer leur confiance. Par exemple, si un nœud a eu des interactions fiables et réussies avec un nœud donné dans le passé, il peut accorder une plus grande confiance à ce nœud dans le futur.

2.5.7 Détection et prévention des attaques

Des mécanismes de détection et de prévention des attaques, tels que la surveillance du trafic, les techniques de détection d'intrusion et les mécanismes de filtrage, peuvent être utilisés pour minimiser ces risques [21] Voici quelques exemple :

- `Mécanismes de détection d'intrusion :` Les nœuds peuvent utiliser des techniques de détection d'intrusion pour surveiller les activités du réseau et identifier les comportements malveillants ou les attaques en cours.
- `Filtrage des paquets :` Les nœuds peuvent mettre en place des mécanismes de filtrage des paquets pour bloquer les paquets malveillants ou non autorisés provenant des nœuds non fiables.

2.6 Conclusion

Dans ce chapitre, on a présenté un aperçu de la sécurité dans les réseaux ad hoc, en abordant les différents types d'attaques et les vulnérabilités inhérentes à ces réseaux. de plus, on a exposé les solutions de sécurité qui ont été adoptées dans la littérature pour faire face aux attaques.

Dans le chapitre suivant, on va examine en détail l'état de l'art de l'attaque spoofing, qui constitue le cœur de notre étude. Cela nous permettra ensuite de présenter en détail la solution que nous avons proposée.

Chapitre 3

Etude de l'attaque spoofing et la solution proposée

3.1 Introduction

L'évolution des réseaux ad hoc a ouvert de nouvelles perspectives dans le domaine des communications sans fil.Comme on as déjà vu,ces réseaux dynamiques et autonomes permettent aux dispositifs de se connecter directement les uns aux autres, sans dépendre d'une infrastructure centrale. Cependant, avec cette liberté et cette flexibilité viennent également des défis en termes de sécurité.

Les attaques informatiques représentent une menace sérieuse pour les réseaux ad hoc, compromettant leur fonctionnement, leur intégrité et leur confidentialité. Parmi ces attaques, les attaques de spoofing constituent une préoccupation majeure. Le spoofing fait référence à une technique où un attaquant usurpe l'identité d'un autre appareil ou d'un nœud du réseau afin de tromper les autres appareils et d'intercepter ou de manipuler les communications.

L'objectif de ce chapitre est d'offrir une vision approfondie des attaques de spoofing dans les réseaux ad hoc, ainsi que des mesures de sécurité déjà existantes. Cette connaissance servira de base solide pour la proposition d'un mécanisme de sécurité anti-spoofing plus avancé, qui sera présenté dans la suite de ce chapitre.

3.2 L'attaque spoofing dans les réseaux ad hoc

Dans cette section, nous allons définir et donner un exemple sur l'attaque spoofing dans les réseaux ad hoc.

Définition 3.1.

Lors d'une attaque de spoofing, l'attaquant se fait passer pour un autre nœud du réseau, ce qui lui permet de recevoir les messages qui étaient destinés à ce nœud spécifique. Généralement, ce type d'attaque est lancé dans le but de gagner un accès au réseau afin de mener d'autres attaques, ce qui peut causer de graves dysfonctionnements. Cette attaque peut être réalisée par n'importe quel nœud malveillant ayant suffisamment d'informations sur le réseau pour falsifier

l'identité d'un de ses membres. En utilisant cette fausse identité et en offrant une incitation attractive, le nœud malveillant peut tromper les autres nœuds pour qu'ils établissent des routes vers lui-même plutôt que vers le nœud d'origine. Un nœud malveillant poursuivant cet objectif essaiera probablement de se faire passer pour un nœud se trouvant sur le chemin du flux de données qu'il souhaite intercepter. Cette tromperie peut être réalisée en modifiant les données de routage ou en se faisant passer pour un partenaire de communication digne de confiance pour les nœuds voisins [29].

Les attaques de spoofing peuvent être :

- **IP Spoofing :** L'usurpation d'adresse IP, également connue sous le nom de spoofing IP, est une pratique utilisée en Réseau informatique, dans laquelle des paquets du protocole Internet (IP) sont créés avec une adresse IP source falsifiée. L'objectif de cette pratique, appelée spoofing, est de dissimuler l'identité réelle de l'émetteur ou de se faire passer pour un autre système informatique.

  L'usurpation d'adresse IP peut être utilisée par des intrus réseau pour compromettre les mesures de sécurité du réseau, notamment l'authentification basée sur les adresses IP. Cette forme d'attaque, qui implique la modification de milliers de paquets simultanément, peut être extrêmement complexe. Elle est particulièrement efficace lorsque des relations de confiance existent entre les machines [34].

- **MAC spoofing :** le MAC spoofing dans les réseaux ad hoc est une technique d'usurpation d'adresse MAC qui peut compromettre la sécurité du réseau en permettant à un attaquant de se faire passer pour un nœud légitime , cette attaque peut être utilisée à des fins malveillantes. Par exemple, un attaquant peut usurper l'adresse MAC d'un nœud légitime afin de tromper les autres nœuds et de détourner le trafic réseau à son avantage. Cela peut lui permettre de surveiller ou d'intercepter les communications, de perturber le fonctionnement du réseau ou même de mener des attaques plus avancées, telles que des attaques de déni de service.

- **ARP spoofing (ou usurpation ARP) :** L'ARP (Address Resolution Protocol) est un protocole qui sert à associer les adresses IP aux adresses MAC dans le but de faciliter la transmission de données. Lors d'une attaque par usurpation ARP, un acteur malveillant envoie de faux messages ARP à travers un réseau local pour lier son adresse MAC à l'adresse IP d'un membre légitime du réseau. Le résultat de cette attaque est que les données destinées à l'adresse IP légitime sont dirigées vers l'attaquant. Les attaquants utilisent fréquemment l'usurpation ARP pour voler des informations, altérer des données en transit ou perturber le flux sur un réseau local Les attaques ARP spoofing peuvent également servir de base à d'autres types d'attaques, incluant le déni de service, le détournement de session et les attaques de type homme du milieu.

Exemple 3.1.

L'utilisation de l'attaque spoofing pour lancer une attaque de type black hole,chacun des nœuds **L**,**M**,**N** et **D** possède une route vers la destination **Z**, Un nœud malveillant **X** modifie son adresse MAC de manière à ce qu'elle corresponde à celle de L et annonce faussement qu'il dispose d'un chemin plus court ou plus efficace vers la destination Z ,Les autres nœuds du réseau, faisant confiance à cette information, redirigent leur trafic vers le nœud malveillant **X**,

qui peut alors soit intercepter, manipuler ou supprimer le trafic ou bien crée une boucle de routage infini, soit simplement l'ignorer.

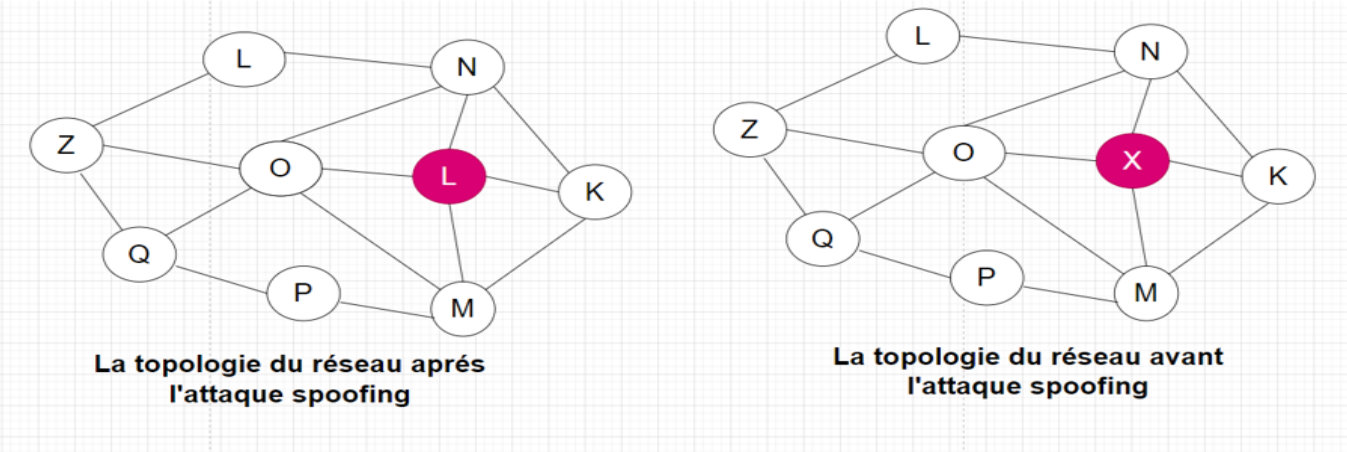

FIGURE 3.1 – Exemple d'une attaque spoofing

3.3 Approches de sécurité contre les attaques spoofing

Autre que l'approche traditionnelle pour prévenir les attaques d'usurpation d'identité qui repose sur l'authentification basée sur la cryptographie, dans ce qui suit, nous allons présenter d'autres approches.

• En 2004, les auteurs J. Hall et al [33] ont proposé une méthode spécifique pour améliorer la capacité de détection des intrusions dans les réseaux sans fil. Pour ce faire, ils ont combiné la technique de Radio Frequency Fingerprinting (RFF) avec un Système de Détection d'Intrusion (IDS) conçu pour les réseaux sans fil.

La méthode de Radio Frequency Fingerprinting (RFF) fonctionne en identifiant de manière unique les émetteurs-récepteurs en se basant sur des caractéristiques spécifiques du signal radio généré lors de la transmission. Cette "empreinte digitale" unique est extraite à partir de la partie transitoire du signal radio. En d'autres termes, chaque appareil émetteur-récepteur laisse une signature distincte dans le signal radio, ce qui permet de les identifier de manière précise.

L'approche proposée améliore également la performance d'un Système de Détection d'Intrusion (IDS) sans fil en corrélant plusieurs observations dans le temps à l'aide de filtres bayésiens. Cela signifie que l'IDS analyse et compare plusieurs enregistrements de signal radio collectés à différents moments pour détecter des anomalies ou des comportements inattendus qui pourraient indiquer une tentative d'intrusion.

Les résultats de simulations effectuées dans l'étude ont démontré l'efficacité de la technique RFF pour résoudre le problème de détection d'intrusion dans les réseaux sans fil. En incorporant la Radio Frequency Fingerprinting et en utilisant des méthodes de corrélation temporelle, cette approche a permis d'identifier avec succès les intrusions potentielles dans les réseaux sans fil.

• En 2006, les auteurs D. Faria et D. Cheriton [25] ont introduit une technique basée sur la création de vecteurs de niveaux de puissance du signal (Received Signal Strength - RSS) reçus à partir de plusieurs points d'accès pour chaque paquet reçu. Ces vecteurs, appelés "signalprints". Cette technique permet de distinguer les appareils légitimes de ceux situés hors de la zone ciblée en analysant les variations de puissance du signal. Les règles d'appariement sont ensuite utilisées pour déterminer si les empreintes de signal proviennent d'un même émetteur ou non , contribuant ainsi à la détection des attaques de spoofing Les valeurs à l'intérieur des signalprints sont organisées dans le même ordre, où la position i dans le vecteur indique l'intensité du signal reçu (mesurée en dBm) a partir du point d'accès numéro i.

Pour contrer les attaques avancés qui pourraient manipuler leur puissance d'émission pour échapper à la détection, Cheriton et Faria ont suggéré l'utilisation de la puissance de signal différentielle plutôt que la puissance absolue du signal. L'intensité du signal différentiel est obtenue en calculant la différence entre les valeurs d'intensité du signal dans le signalprint et la valeur maximale présente dans ce signalprint. Deux règles d'appariement sont définies pour évaluer si deux signalprints proviennent du même émetteur : le maximum d'appariement (max-match) et le minimum d'appariement (min-match). Un max-match de "dB" est enregistré lorsque les différences entre les valeurs de signal dans les deux signalprints sont inférieures à un seuil "dB" ($/S1[i] - S2[i]/ < dB$), permettant d'identifier si les deux signalprints sont générés par le même émetteur. Par contre , les min-matchs servent à distinguer les signalprints provenant de dispositifs distincts. Un min-match de "dB" est observé lorsque les différences entre les valeurs de signal dans les deux signalprints dépassent un seuil "dB"($/S1[i] - S2[i]/ > dB$).

• En 2006, les auteurs F. Guo et T. Chiueh [29]

ont introduit un algorithme de détection pour contrer les attaques d'usurpation d'adresse MAC légitime afin d'accéder au réseau sans fil.

L'algorithme repose sur l'écart entre les numéros de séquence présents dans l'en-tête MAC de la norme $IEEE802.11$. Lorsqu'un nombre significatif de lacunes dépassant un seuil prédéfini est observé au niveau d'un nœud dans un certain laps de temps, cela peut indiquer une tentative d'usurpation d'identité (spoofing). Cependant, cette méthode peut engendrer un taux élevé d'alertes erronées en raison des pertes de paquets dans le réseau. L'objectif de sécurité est de détecter si un attaquant (nœud E) tente de se faire passer pour l'émetteur légitime A (spoofing). Pour identifier les attaques de spoofing, l'entité B utilise la différence entre les numéros de séquence consécutifs $modulo4096$ des paquets qu'elle reçoit de l'émetteur A. Soit "di" la différence entre le numéro de séquence du paquet actuel $S(k-i)$ et celui du paquet précédent $S(k-i-1)$, exprimée comme $di = [S(k-i-1) - S(k-i)]mod4096$. Si un nombre considérable de lacunes dépassant un seuil défini est constaté dans les numéros de séquence (c'est-à-dire lorsque les di sont élevés), cela indique que des paquets sont manquants ou reçus hors séquence, ce qui est inhabituel dans une communication légitime.

• En 2007, Li et Trappe [40] proposent une méthode différente qui repose sur le même principe de numéro de séquence. Cependant, au lieu de se limiter à deux paquets consécutifs pour détecter l'attaque de spoofing, cette méthode se base sur l'utilisation d'une fenêtre de paquets provenant d'une identité spécifique. En considérant la fenêtre $W(k) = [S(k); S(k-1); \ldots; S(k-N-1)]$ composée de N numéros de séquence de paquets consécutifs, le détecteur d'attaque calcule les $N-1$ numéros de séquence de différences, à savoir $d1, d2, \ldots, dN-1$, où $di = [S(k-i-1) - S(k-i)]mod4096$. En employant cette fenêtre de données, une tentative

de spoofing peut être détectée si la valeur maximale de di dépasse un seuil, ou si la somme cumulée des différences dans la fenêtre excède un certain seuil. Bien que cette méthode présente l'avantage de réduire les fausses alertes négatives grâce à l'utilisation de la fenêtre, elle implique également un coût de calcul plus élevé par rapport à l'approche précédente.

• En 2009, J. Yang et al. [22] ont développé une technique appelée $DEMOTE$(Detection of Mobile Identity Spoofing in Wireless Environments) La méthode proposée exploite les mesures de la force du signal reçu (RSS - Received Signal Strength) collectées sur une période de temps. Ces mesures de RSS sont utilisées pour analyser les variations du signal provenant des différents émetteurs-récepteurs sans fil, et elles sont utilisées pour établir un seuil optimal qui divise ces mesures en différentes classes. Cette partition des mesures RSS en classes permet d'identifier plus facilement les variations anormales dans les lectures du signal.

L'algorithme ALignment Prediction (ALP) est ensuite utilisé pour exploiter la contrainte temporelle présente dans les lectures RSS. ALP prédit l'alignement optimal des lectures RSS dans les différentes classes partitionnées, ce qui permet de reconstruire de manière précise les trajectoires et les mouvements des émetteurs-récepteurs. Cette reconstruction des traces RSS contribue à identifier les schémas de mouvement suspects ou non conformes, ce qui aide à détecter les attaques d'usurpation d'identité.

Les résultats obtenus ont montré que la méthode $DEMOTE$,permet une détection précise des attaques d'usurpation d'identité. Elle fonctionne à la fois dans l'espace du signal (mesures de RSS) et dans l'espace physique (localisation des émetteurs-récepteurs). En combinant l'analyse des variations de signal dans le temps avec la reconstruction des trajectoires des appareils, cette méthode s'avère efficace pour détecter et prévenir les attaques d'usurpation d'identité dans les environnements sans fil mobiles.

• En 2011, F.A. Barbhuiya et al [24]. ont développé un système actif de détection d'intrusion basé sur des systèmes à événements discrets (DES) pour détecter l'usurpation d'identité ARP (Address Resolution Protocol).

Le système proposé, appelé système de détection d'intrusion (IDS) basé sur DES, repose sur une modélisation formelle basée sur les états de transition. Cette modélisation est utilisée pour analyser différents scénarios d'attaques d'usurpation d'identité ARP, en identifiant ceux qui peuvent être détectés et ceux qui ne le peuvent pas. En utilisant cette modélisation, le système peut anticiper les actions des attaquants et détecter des comportements anormaux qui pourraient indiquer une usurpation d'identité.

Un aspect intéressant de ce système est son utilisation d'un mécanisme de sondage actif. Plutôt que de simplement observer le trafic réseau passifement, le système envoie activement des requêtes ARP pour valider les associations entre adresses IP et adresses MAC. Cela permet de détecter plus rapidement les tentatives d'usurpation d'identité en vérifiant les correspondances entre les adresses.

Ce système de détection d'intrusion fonctionne au niveau logiciel et s'exécute sur un seul hôte, ce qui signifie qu'il ne nécessite pas de matériel ou de logiciel supplémentaire sur les autres hôtes du réseau. Les résultats ont montré que malgré l'utilisation d'un mécanisme de sondage actif, les frais généraux supplémentaires en termes de trafic étaient négligeables dans les IDS basés sur DES. En somme, cette approche offre une méthode proactive pour détecter et prévenir les attaques d'usurpation d'identité ARP dans un réseau.

3.4 Solution proposée

Notre solution consiste à créer un mécanisme de routage qui permet de détecter la présence d'une attaque de type spoofing dans un réseau ad hoc. Supposons qu'on a un réseau ad hoc qui contient un ensemble des nœuds avec des liens bidirectionnels, Pour expliquer clairement son fonctionnement, On va diviser le mécanisme en les étapes suivantes. :

- ◇ Création des Tables de transmissions pour chaque nœud de réseau.
- ◇ Construction de paquet de données par le nœud émetteur.
- ◇ Vérification de packet par le nœuds destinataire.
- ◇ Mise à jour des tables de transmissions et des tables des numéros de références.
- ◇ Développement de la solution proposée .
- ◇ Objectif générale de la solution propsée .

3.4.1 Création des tables de transmissions pour chaque nœud de réseau

La première étape de cette solution implique la création d'une table dédiée pour chaque nœud du réseau. Cette table contiendra l'historique complet des transmissions effectuées au sein du réseau, représenté par :

- **Ns :** représente le nœud source qui va faire la transmission de pakcet de données.
- **Nd :** représente le nœud destinataire qui va recevoir le packet , et fait des vérifications par la suite.
- **Tx(Timestamp) :** Un élément important au sein de cette table, représentant le temps de la dernière transmission émise par le nœud source.
- **Hash Tx :** représente le hashage des données de la table de transmission à l'instant **Tx** de la dernière transmission dans la table.

  Soit un réseau ad hoc qui contient un ensemble de 3 nœuds, Pour illustrer cette étape, la Figure suivant propose un exemple concret de cette table, permettant ainsi de visualiser son organisation et son contenu.

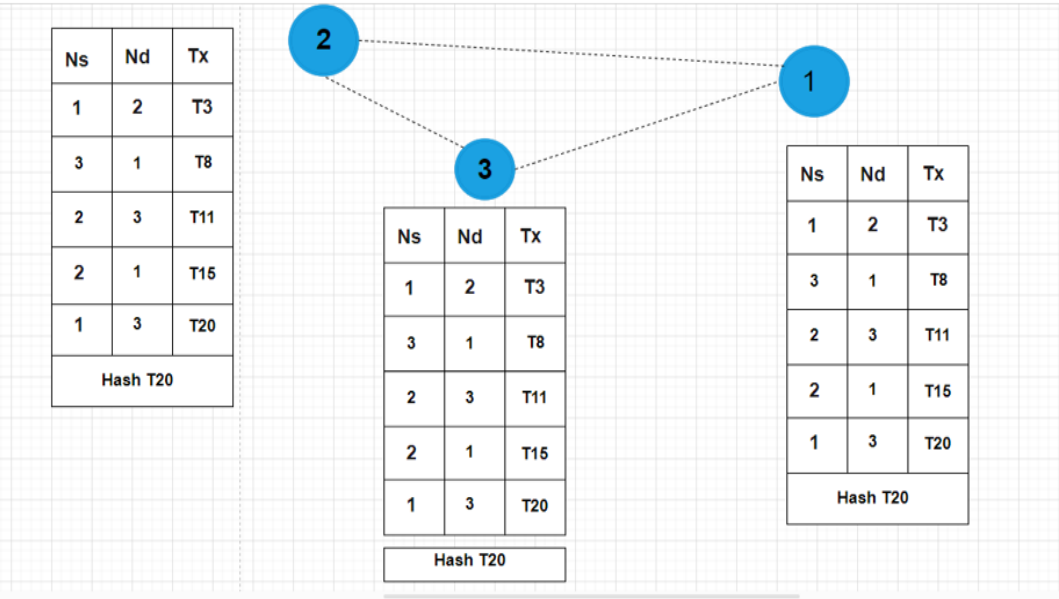

FIGURE 3.2 – Les tables de transmission

3.4.2 Construction de paquet de données par le nœud èmetteur

Dans cette phase, on va examiner en détail les paquets de données émis par les nœuds sources. Chacun de ces paquets transporte des informations importantes, permettant ainsi aux nœuds destinataires de faire la différence entre les paquets émanant de nœuds légitimes et ceux issus de nœuds malveillants, Ces paquets sont conçus pour contenir les éléments suivants :

- **IP source :** Cette adresse IP identifie le nœud source responsable de l'émission du paquet de données.
- **IP destination :** Cette adresse IP cible le nœud destinataire où le paquet doit arriver.
- **XXXXXX :** Les données encapsulées ,représentant un ensemble de données spécifiques, ces données constituent le message envoyé par le nœud source.
- **Timestamp (Tx) :** Indiquant le moment précis de la dernière transmission effectuée par le nœud source dans le réseau.
- **Hash du Timestamp (Hash Tx) :** : Corresponde au hachage de toutes les données contenues dans la table de transmission au moment Tx.

IP source	**IP** destination	**XXXXXX**	**TX**	**Hash TX**

TABLE 3.1 – Un paquet de données

3.4.3 Vérification des paquets par le nœud destinataire

Dans cette étape, le nœud destinataire joue un rôle principal pour déterminer l'authenticité du paquet reçu et ainsi distinguer entre une transmission et une transmission malveillante. Les vérifications suivantes sont entreprises :

- ◇ **Vérification initiale des adresses IP :** Le nœud destinataire commence par vérifier les deux champs fondamentaux de l'en-tête du paquet, à savoir l'adresse IP source et l'adresse IP destination. Cette première étape permet de déterminer si le paquet est destiné au nœud où le paquet est arrivé ou à un autre nœud du réseau.
- ◇ **Validation du Timestamp (Tx) :** Ensuite, le nœud destinataire compare le Timestamp (Tx) reçu avec le Timestamp enregistré dans sa propre table de transmission. Cette comparaison permet de vérifier si le moment de la dernière transmission enregistrée par le nœud source concorde avec le Timestamp indiqué dans le paquet reçu.
- ◇ **Vérification du Hash du Timestamp (Hash Tx) :** Pour renforcer daavantage la confiance dans l'intégrité de la transaction, attestant que le paquet émane d'une source légitime, le nœud destinataire calcule le Hash du contenu de sa propre table de transmission au moment spécifié par le Timestamp (Tx) reçu. Ce calcul est ensuite comparé avec le $HashTx$ inclus dans le paquet reçu.

• **Analyse Des Résultats De La Vérification :**

— **Dans le cas normal (c'est-à-dire en l'absence d'une attaque de spoofing) :**

- ◇ **Tx :** s'avère positive. la vérification du Timestamp (Tx) : s'avère positive. Cela signifie que lorsqu'un nœud destinataire compare le Timestamp (Tx) reçu avec celui contenu dans sa propre table de transmission, une concordance est établie.
- ◇ **La vérification du Hash Tx :** Puisque les données contenues dans la table du nœud destinataire sont les mêmes que celles présentes dans les nœuds sources ainsi que dans tous les autres nœuds du réseau, le $HashTx$ reçu et le $HashTx$ calculé par le nœud destinataire sont automatiquement égaux.

— **Dans le cas contraire ou une attaque spoofing est présente :**

Cependant, si le scénario inverse se produit et qu'une attaque de spoofing est en cours, plusieurs anomalies apparaîtront. Si le Timestamp (Tx) reçu ne correspond pas à celui contenu dans la table du nœud destinataire, et si le $HashTx$ calculé par ce même nœud diffère du $HashTx$ reçu, cela constitue un signe possible de présence d'une attaque de spoofing. En conséquence, le nœud destinataire rejettera la transmission en cours et déclenchera une alerte signalant la probabilité d'une attaque de spoofing en cours.

Exemple 3.2.

supposons qu'on a un réseau réseaux ad hoc contient 4 nœuds légitimes, et un nœud Malveillant (le nœud numéro 5) :

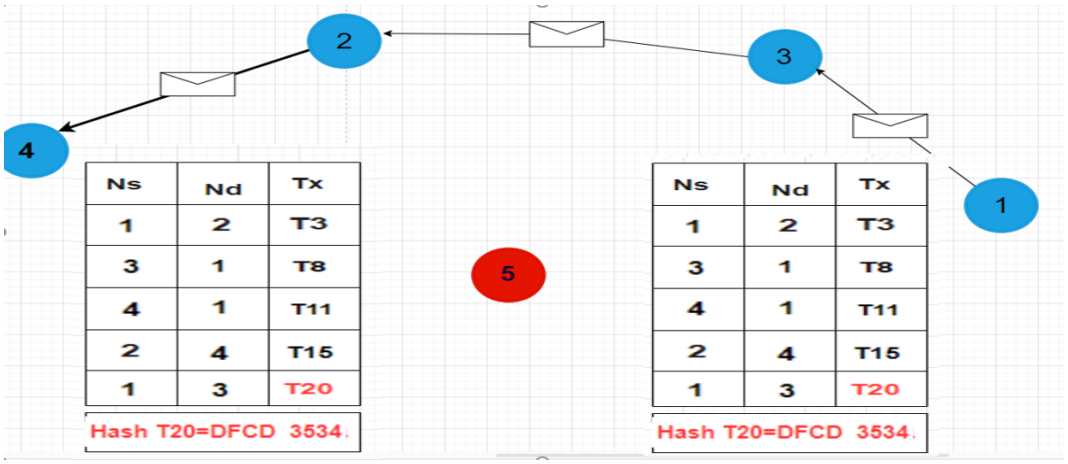

FIGURE 3.3 – Exemple d'un réseau ad hoc avec la présence d'un nœud malveillant

i. **1 er cas :** Dans une situation normale, le nœud légitime 1 envoie un message au nœud 4.

Le nœud 4 effectue ensuite les vérifications de Tx et de $HashTx$:

Le Tx reçu de la part du nœud 1 correspond au Tx contenu dans la table de transmission du nœud 4, c'est-à-dire $T20$.

Le $HashTx$ reçu de la part du nœud 1 correspond au $HashTx$ calculé par le nœud 4, qui est $DFCD3534$.

Ces vérifications Amènent à l'acceptation du message par le nœud 4 .

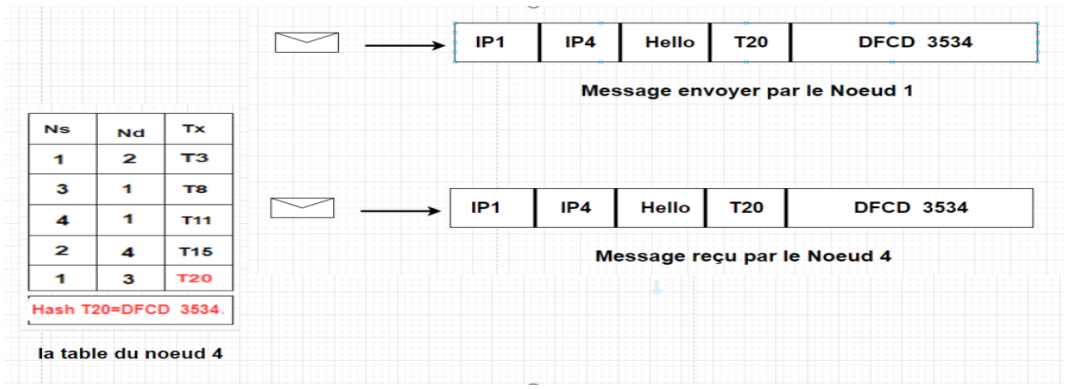

FIGURE 3.4 – Vérification d'un paquet de données légitimes reçu par le nœud destinataire 4

ii. **2eme cas :** Présence d'une attaque spoofing :

le nœud malveillant 5 envoie un message au nœud 4 en utilisant l'adresse du nœud légitime 1.

Le nœud 4 réalise ensuite les vérifications de Tx et de $HashTx$:

Le Tx reçu de la part du nœud malveillant 5, qui est $T62$, est incompatible avec le Tx contenu dans la table de transmission du nœud 4, qui égal à $T20$.

Le $HashTx$ reçu de la part du nœud malveillant 5, qui est $AF4FD3332$, ne correspond pas au $HashTx$ calculé par le nœud 4, égal à $DFCD3534$. Cependant, il constate une incohérence entre les données calculées localement et les données reçues. Dans ce contexte,le nœud 4 rejette le message et déclenche une alerte signalant une tentative d'attaque par spoofing..

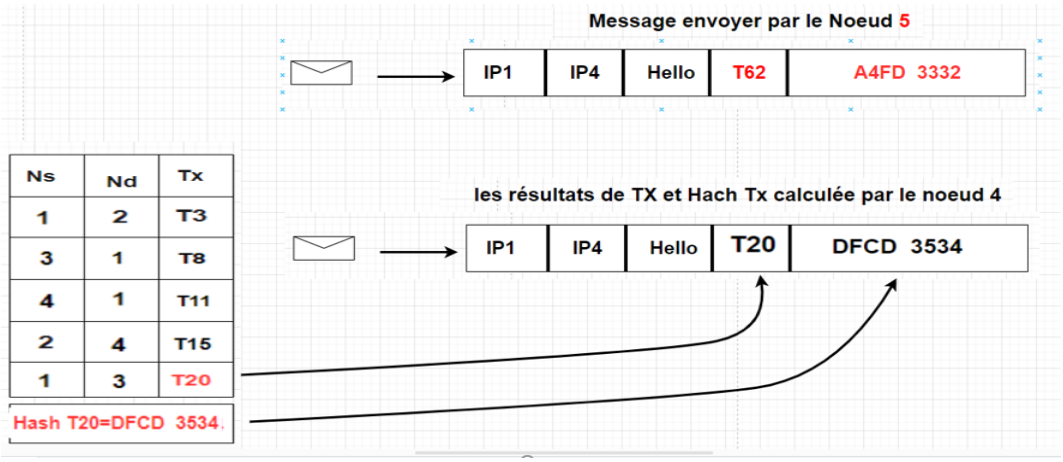

FIGURE 3.5 – Vérification d'un paquet de données malveillantes par le nœud destinataire 4

• **Problématique 1 :** Qu'advient-il si un message envoyé par un nœud légitime est altéré en cours de route avant d'atteindre sa destination ? Cela signifie qu'un individu pourrait altérer le contenu du message sans changer l'identité du nœud légitime.

— **Solution :**

Dans ce scénario, une autre forme d'attaque, connue sous le nom d'attaque de l'homme du milieu (man in the middle), peut survenir. Bien que l'on puisse considérer cette attaque comme une variante de l'attaque de spoofing, il est important de rappeler le concept vu dans le chapitre 2. L'attaque de l'homme du milieu implique l'interception et potentiellement la modification des communications entre deux parties légitimes, tout en préservant leur ignorance de l'intermédiaire malveillant.

L'essentiel de cette attaque est de faire croire aux parties légitimes qu'elles communiquent directement l'une avec l'autre, alors qu'en réalité, l'ensemble de leurs échanges passe par l'attaquant. Cela implique généralement la création de fausses identités pour les parties légitimes et la manipulation des données échangées.

Du fait que cette attaque altère l'identité et les échanges des parties légitimes, le mécanisme précédemment énoncé n'offre pas de protection contre cette variante d'attaque. Afin de préserver l'intégrité des données transmises par les nœuds légitimes et d'éviter toute altération, une solution s'impose :

Je propose l'ajout d'une nouvelle composante, le **Hash2 Tx**, au message émis. Cette composante renferme le hachage de l'ensemble de données **XXXXXX** que la source souhaite transmettre, ainsi que les données contenues dans sa table de transmission.

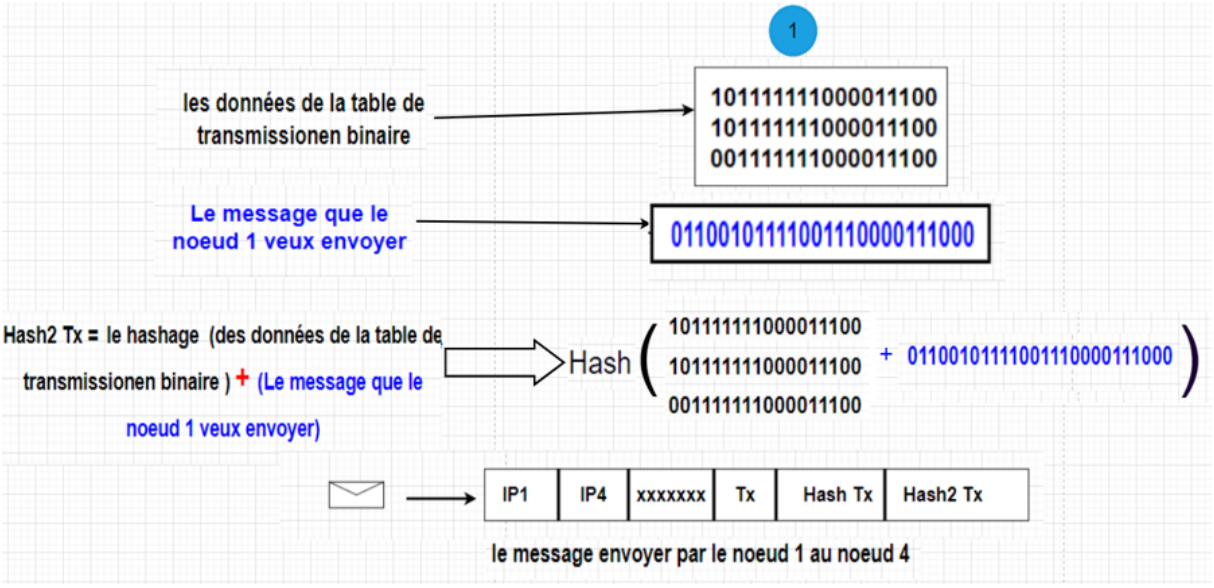

FIGURE 3.6 – Explication du fonctionnement de $Hash2Tx$

Une fois que le paquet de données parvient à sa destination, une comparaison est effectuée entre les champs suivants : $TX, HashTxetHash2Tx$.

- ◇ **Première scénario :** Si les valeurs reçues de TX et $HashTx$ diffèrent de celles calculées par le nœud destinataire, cela indique, comme précédemment évoqué, que le paquet de données a été envoyé par un nœud malveillant. Dans ce cas, un acte d'usurpation d'identité d'un nœud légitime par un nœud malveillant est en jeu.
- ◇ **Deuxième scéénario :** : Si les valeurs reçues de TX et $HashTx$ correspondent p celles calculées par le nœud destinataire, mais que le $Hash2Tx$ reçu ne concorde pas avec la valeur calculée du $Hash2Tx$, cela signifie que le message a été transmis par un nœud légitime équipé d'une table de transmission correcte. Cependant, il est à noter que les données **XXXXXX** envoyées ont été modifiées en cours de transmission, ce qui laisse entendre une altération du contenu pendant le cheminement.

Exemple 3.3.

Pour illustrer, considérons un scénario dans un réseau ad hoc où le nœud malveillant numéro 5 souhaite transmettre un message au nœud 4 en se faisant passer pour le nœud 1. Supposons les données suivantes :

◇ Données de la table des nœuds légitimes 1 et 4 : 100000111100111001

◇ Message envoyé : 1111000101

• Dans le contexte normal, si le paquet est émis par le nœud légitime 1 :

◇ $TX = T20$.

◇ $HashT20 = 23322A323FFF$.

◇ $T20 = Hash(100000111100111001 + 1111000101) = AFD42A323DEF$.

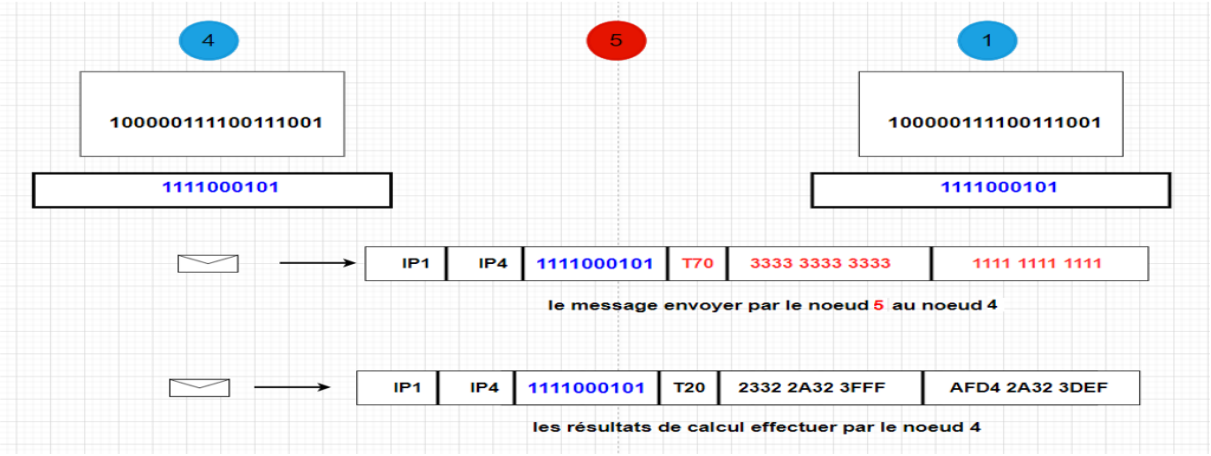

FIGURE 3.7 – Dans le contexte normal, si le paquet est èmis par le nœud légitime 1

i. **Scénario 1 :**

Lorsqu'un message est envoyé par le nœud malveillant 5, usurpant l'identité du nœud 1, les résultats reçus pour TX, $HashTx$ et $Hash2Tx$ diffèrent des calculs effectués par le nœud 4. En conséquence, le nœud 4 rejette le message, suspectant une tentative de manipulation par un nœud malveillant. Le système déclenche alors une alerte signalant une tentative d'usurpation d'identité du nœud 1 par un nœud malveillant.

Les résultats de $TX, HashTX$ *et* $Hash2TX$ reçus ne correspondent pas aux résultats calculés par le nœud 4. Par conséquent, le nœud 4 refuse le message et suppose que le paquet a été envoyé par un nœud malveillant. Il déclenche ensuite une alerte signalant une tentative d'usurpation d'identité du nœud 1 par un nœud malveillant.

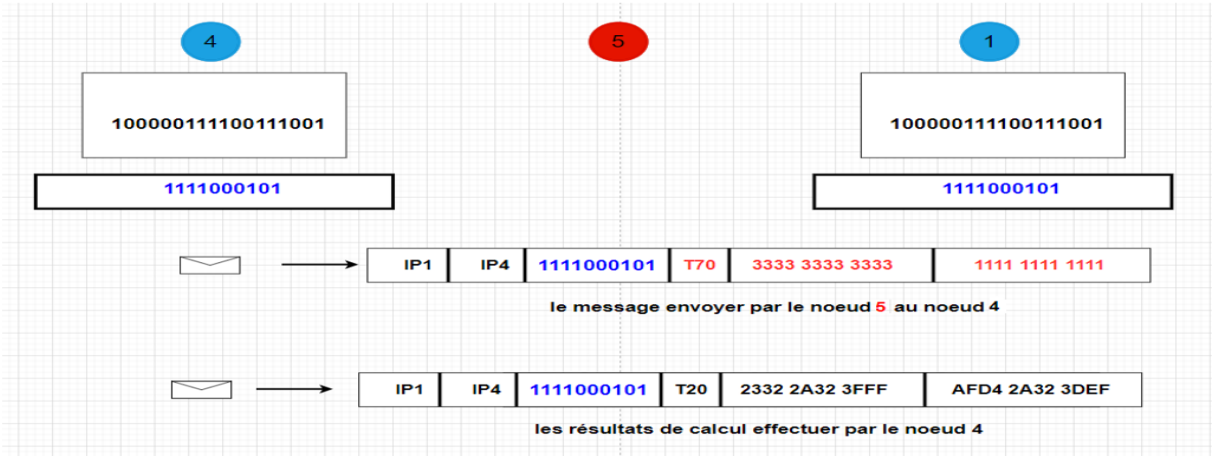

FIGURE 3.8 – Exemple du scénario 1

ii. **Scénario 2 :**

Lorsqu'un message est transmis par le nœud légitime 1, avant qu'il n'atteigne le nœud de destination 4, le nœud malveillant 5 altère le paquet en modifiant uniquement le contenu du message envoyé, c'est-à-dire "1111000101".

Lorsque le paquet modifié atteint le nœud 4, celui-ci effectue des vérifications sur TX *et* $HashTX$, constatant une correspondance dans les calculs. Il extrait ensuite le message reçu, noté **"XXXXXXX"**, qui correspond à "00000001" dans notre exemple. Le nœud 4 ajoute les données de sa table, égales à "100000111100111001" dans notre exemple, au message reçu. Il applique ensuite une fonction de hachage à ce nombre agrégé pour calculer $Hash2TX$.

Le $Hash2TX$ calculé est "AAAA AAAA AAAA", ce qui diffère du $Hash2TX$ reçu. Étant donné que les calculs sur TX *et* $HashTX$ sont corrects, le nœud 4 considère que le paquet a été envoyé par le nœud légitime 1. Cependant, étant donné que le $Hash2TX$ calculé est incorrect, cela indique que le message a été altéré par un nœud malveillant en cours de route avant d'atteindre sa destination. Par conséquent, le nœud 4 rejette le message et génère une alerte dans le réseau.

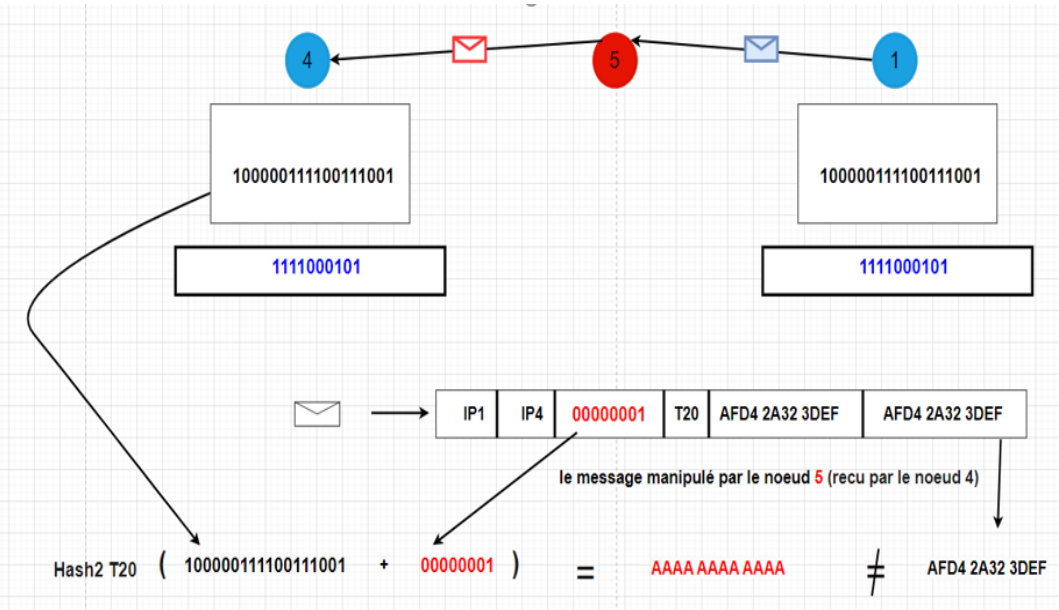

FIGURE 3.9 – Exemple du scénario 2

• **Problématique 2 :**

Que se produit-il en cas d'une attaque émanant d'un nœud inséré au sein des réseaux, soit une attaque interne ? Dans ce scénario, le nœud malveillant détient la table de transmission ainsi que toutes les données présentes chez les nœuds légitimes. Par conséquent, tout nœud a la capacité d'emprunter l'identité d'un autre nœud et de crée un paquet de données, dissimulant ainsi son propre rôle malveillant.. Face à cette situation complexe, quelle serait la solution adéquate ?

— **Solution :**

La solution que je propose consiste à établir un moyen de confiance entre chaque paire de nœuds. Pour cela, chaque nœud aurait une autre table spéciale supplémentaire pour chaque nœud au sein du réseau , distincte de la table partagée entre tous les nœuds , Cette table unique renfermerait les numéros de séquence des paquets de données échangés précédemment entre les deux nœuds en question.

Quand un nœud envoie un message à un autre nœud, il joindrait le numéro de séquence qui montre le dernier message qu'ils ont partagé. C'est comme un code de confiance entre ces deux nœuds. Le nœud qui reçoit le message aurait aussi une liste avec tous les numéros des messages passés qu'il a échangés avec l'autre nœud. Il vérifierait alors si le numéro du message reçu est le même que celui dans sa propre liste.

Si tout est correspondant , le message serait accepté. Dans le cas contraire, le message serait refusé et un avertissement serait envoyé pour signaler qu'il y a peut-être une tentative d'entrée non autorisée dans le réseau.

Exemple 3.4.

Supposons qu'on un réseau composé de 4 nœuds :

Ns : numéro de séquence.

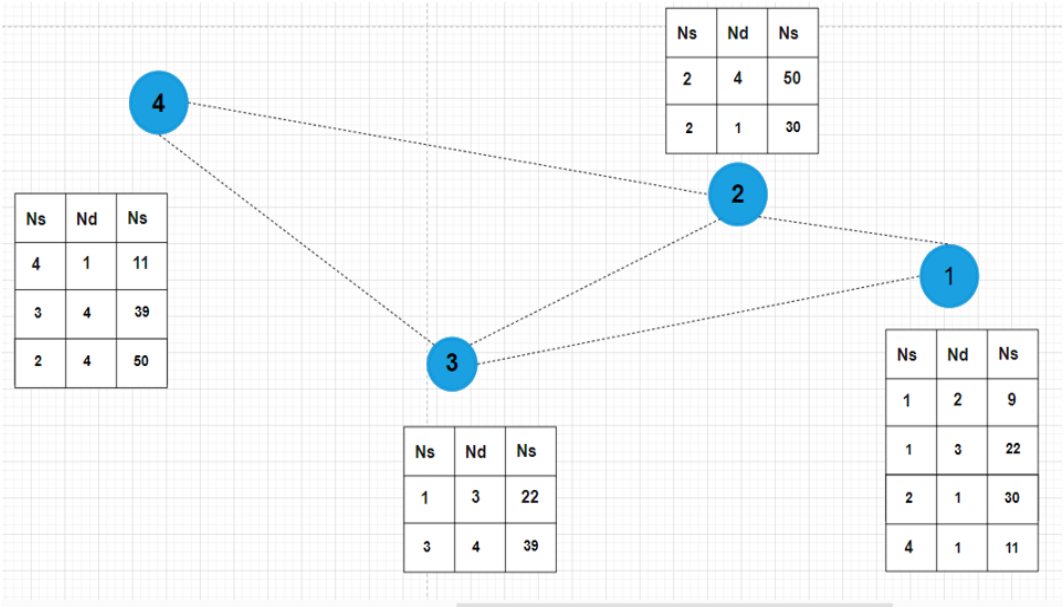

FIGURE 3.10 – Les tables des numéros de séquence

Supposons que le nœud 2 souhaite envoyer un message au nœud 4. Comme on peut le voir dans la table des numéros de séquence du nœud 2, le dernier paquet échangé entre le nœud 2 et le nœud 4 contient le numéro de séquence "50". Ce numéro de séquence se trouve uniquement dans les tables des nœuds 2 et 4. Ainsi, lorsque le nœud 4 reçoit le paquet, il vérifie le numéro de séquence de la manière suivante :

- ◇ Si Ns=50 : alors le message provient bien du nœud 2.
- ◇ Si Ns est différent de 50 : cela signifie qu'un autre nœud tente d'utiliser l'identité du nœud 2. Par conséquent, le nœud 4 déclenche une alerte.

Comme le montre cet exemple, les numéros de séquence sont partagés uniquement entre les deux nœuds qui échangent des messages. Par conséquent, il est impossible qu'un nœud du réseau utilise l'identité d'un autre nœud, car il ne possède pas les numéros de séquences spécifiques de ce nœud.

Voila le paquet de données envoyer par le nœud 2 :

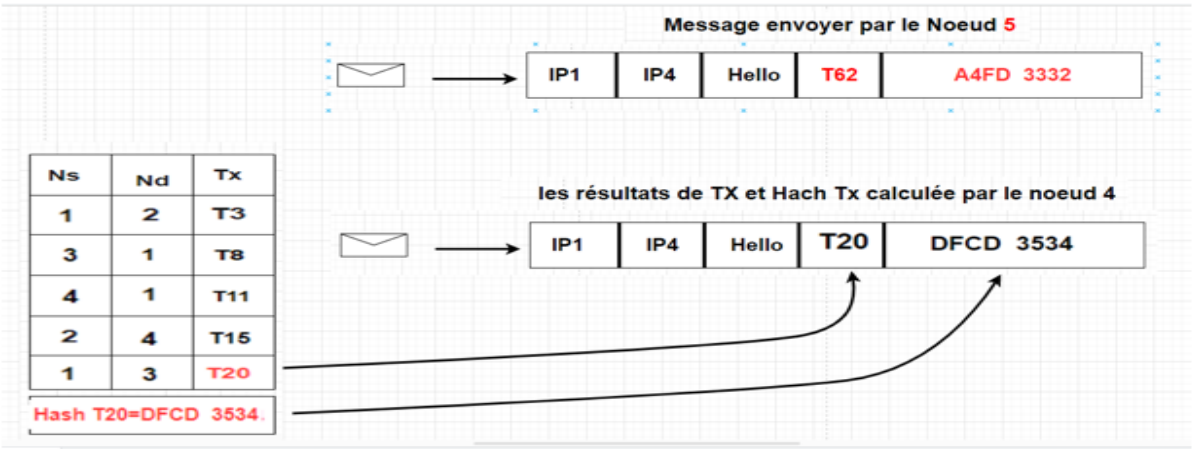

FIGURE 3.11 – Vérification d'un paquet de données malveillantes par le nœud destinataire 4

3.4.4 Mise à jour des tables de transmissoins et des tables des numéros de squérences

Une fois que la transmission est réussie, c'est-à-dire que le nœud destinataire a accepté le paquet reçu du nœud source, une étape importante intervient. Lorsque le nœud destinataire approuve le message qu'il a reçu, il déclenche l'envoi d'une réponse non seulement au nœud source, mais également à l'ensemble des autres nœuds au sein du réseau. Cette réponse informe tous les nœuds qu'une transmission s'est déroulée avec succès. Par la suite, tous les nœuds au sein du réseau mettent à jour leur table de transmission en y ajoutant les détails de cette nouvelle transmission (Ns, Nd, Tx).

Cependant, une distinction se fait entre le nœud source et le nœud destinataire. Les deux nœuds mettent à jour leurs propres tables. Ils y intègrent les informations relatives à la nouvelle transmission, à savoir "Ns, Nd, Tx". De plus, ils ajoutent le numéro de séquence du paquet à leur table des numéros de séquence. Cette mise à jour coordonnée des tables permet d'assurer la confiance des échanges au sein du réseau, garantissant ainsi que les informations soient correctement enregistrées et partagées entre eux.

Exemple 3.5.

• Dans un réseau de 4 nœuds, le nœud 1 envoie un message au noued 4, voila le paquet de donner envoyer par le noeud1 :

IP1	IP4	XXXXXX	T20	Hash T20	Hash 2 T20	Ns=36

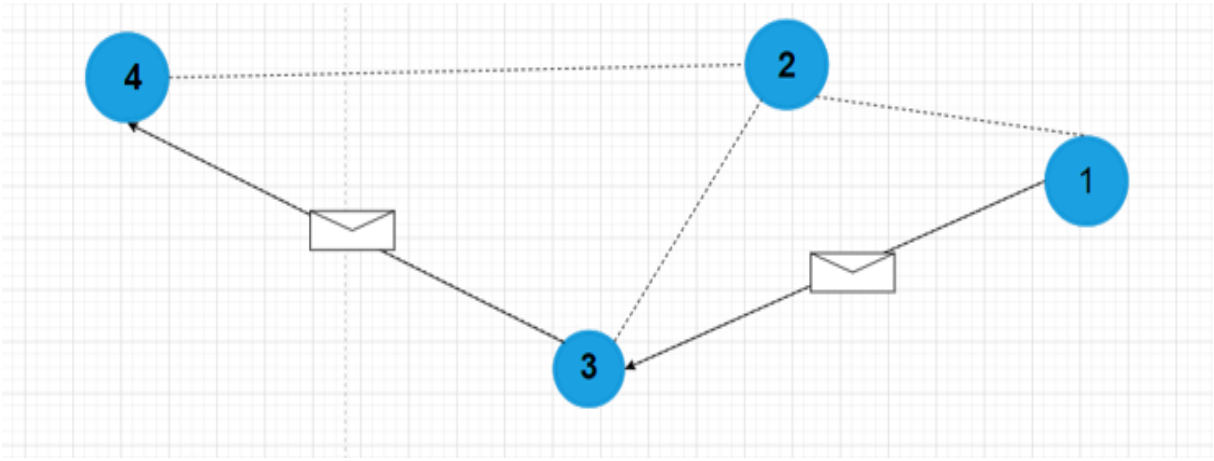

FIGURE 3.12 – Transmission d'un paquet légitime

• Lorsque le paquet arrive à sa destination (nœud 4), ce nœud effectue ses vérifications et accepte le paquet envoyé par le nœud 1.

• Le nœud 4 met à jour ses deux tables, celle de transmission et celle des transactions. Ensuite, il envoie un message de notification à tous les autres nœuds du réseau (en diffusion générale, ou "broadcast").Et voila les 3 paquets envoyer par le nœud 4 lorsque il accepte le message :

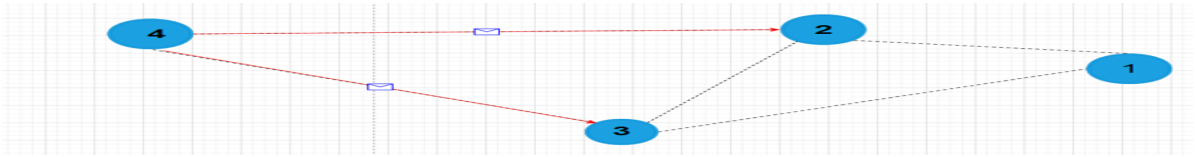

FIGURE 3.13 – Transmission des messages de notification

• " Voila les 3 paquets de notification envoyés par le noeud 4 :

IP4	IP3	Le nœud 1 a effectué une transmission réussie vers le nœud 4 en un temps noté Tx.. **Ns=1,Nd=4,Tx**.
IP4	IP2	Le nœud 1 a effectué une transmission réussie vers le nœud 4 en un temps noté **Tx..Ns=1,Nd=4,Tx**.
IP4	IP1	Le nœud 1 a effectué une transmission réussie vers le nœud 4 en un temps noté **Tx..Ns=1,Nd=4,Tx**.

• Voila la nouvelle mise à jour des tables : On voit les modifications avec la couleur rouge sur la figure.

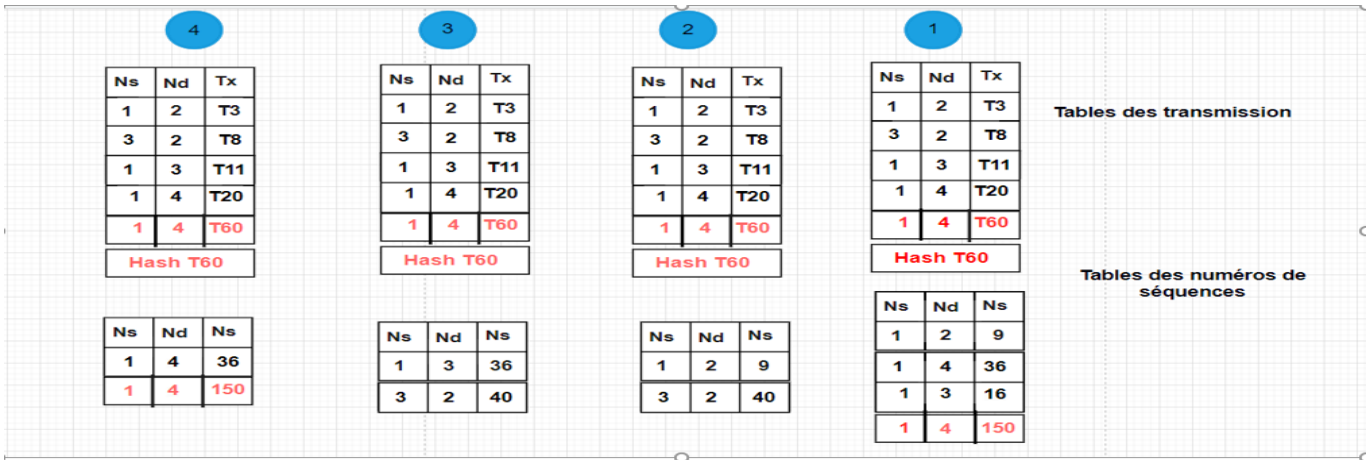

FIGURE 3.14 – Mise à jour des tables de transmission et des tables de numéros de séquence

3.5 développement de la solution proposée

Pour l'instant, notre solution n'est pas terminée car elle n'est pas fiable dans certains cas. Donc, au cours du développement de notre idée, nous avons identifié deux problématiques pour mieux développer notre solution.

Problématique 1 : Qu'advient-il si un message envoyé par un nœud légitime est altéré en cours de route avant d'atteindre sa destination ? Cela signifie qu'un individu pourrait altérer le contenu du message sans changer l'identité du nœud légitime.

Solution :

Dans ce scénario, une autre forme d'attaque, connue sous le nom d'attaque de l'homme du milieu (man in the middle), peut survenir. Bien que l'on puisse considérer cette attaque comme une variante de l'attaque de spoofing, il est important de rappeler le concept vu dans le chapitre 2. L'attaque de l'homme du milieu implique l'interception et potentiellement la modification des communications entre deux parties légitimes, tout en préservant leur ignorance de l'intermédiaire malveillant.

L'essentiel de cette attaque est de faire croire aux parties légitimes qu'elles communiquent directement l'une avec l'autre, alors qu'en réalité, l'ensemble de leurs échanges passe par l'attaquant. Cela implique généralement la création de fausses identités pour les parties légitimes et la manipulation des données échangées.

Du fait que cette attaque altère l'identité et les échanges des parties légitimes, le mécanisme précédemment énoncé n'offre pas de protection contre cette variante d'attaque. Afin de préserver l'intégrité des données transmises par les nœuds légitimes et d'éviter toute altération, une solution s'impose :

On propose d'ajouter une nouvelle composante, le Hash2 Tx, au message émis. Cette composante renferme le hachage de l'ensemble de données **XXXXXX** que la source souhaite transmettre, ainsi que les données contenues dans sa table de transmission.

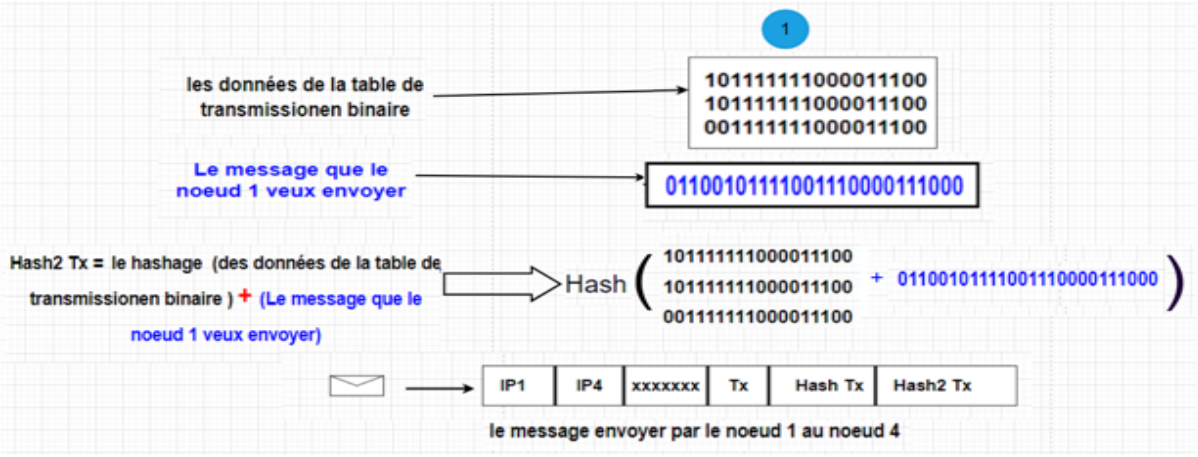

FIGURE 3.15 – Explication du fonctionnement de Hash2 Tx

Une fois que le paquet de données parvient à sa destination, une comparaison est effectuée entre les champs suivants : $TX, HashTx$ *et* $Hash2Tx$.

- **Premier scénario :** Si les valeurs reçues de TX et Hash Tx diffèrent de celles calculées par le nœud destinataire, cela indique, comme précédemment évoqué, que le paquet de données a été envoyé par un nœud malveillant. Dans ce cas, un acte d'usurpation d'identité d'un nœud légitime par un nœud malveillant est en jeu.
- **Deuxième scénario :** : Si les valeurs reçues de TX et Hash TX correspondent à celles calculées par le nœud destinataire, mais que le Hash2 TX reçu ne concorde pas avec la valeur calculée du Hash2 TX, cela signifie que le message a été transmis par un nœud légitime équipé d'une table de transmission correcte, mais que les données **XXXXXX** envoyées ont été modifiées en cours de transmission, ce qui laisse entendre une altération du contenu pendant le cheminement.

Exemple 3.6.

Pour illustrer, considérons un scénario dans un réseau ad hoc où le nœud malveillant numéro 5 souhaite transmettre un message au nœud 4 en se faisant passer pour le nœud 1. Supposons les données suivantes :

— Données de la table des nœuds légitimes 1 et 4 : 100000111100111001

— Message envoyé par le nœud 1 : 1111000101

  - Dans le cas normal, si le paquet est émis par le nœud légitime 1 :

— $TX = T20$.

— $HashT20 = 23322A323FFF$.

— $Hash2T20 = Hash(100000111100111001 + 1111000101) = AFD42A32$

— $3DEF$.

- **Scénario 1 :** Lorsqu'un message est envoyé par le nœud malveillant 5, usurpant l'identité du nœud 1. Les résultats de TX, Hash TX et Hash2 TX reçus ne correspondent pas aux résultats calculés par le nœud 4. Par conséquent, le nœud 4 refuse le message et suppose que le paquet a été envoyé par un nœud malveillant. Il déclenche ensuite une alerte signalant une tentative d'usurpation d'identité du nœud 1 par un nœud malveillant.

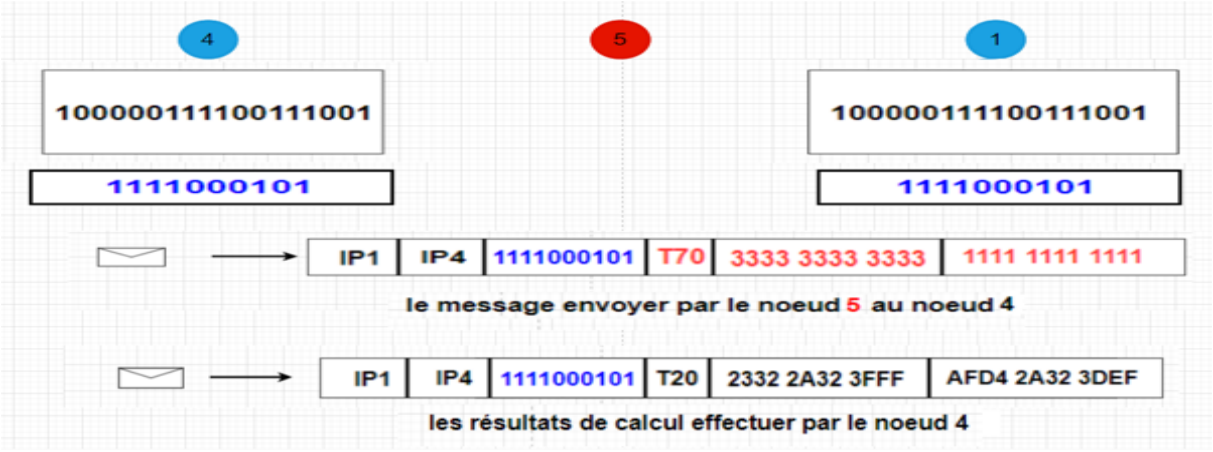

FIGURE 3.16 – Exemple du scénario 1

- **Scénario 2 :** Lorsqu'un message est transmis par le nœud légitime 1, avant qu'il n'atteigne le nœud de destination 4, le nœud malveillant 5 altère le paquet en modifiant uniquement le contenu du message envoyé, c'est-à-dire "1111000101".

  Lorsque le paquet modifié atteint le nœud 4, celui-ci effectue des vérifications sur TX et $HashTX$, constatant une correspondance dans les calculs. Il extrait ensuite le message reçu, noté "$XXXXXXX$", qui correspond à "00000001" dans notre exemple. Le nœud 4 ajoute les données de sa table, égales à "100000111100111001" dans notre exemple, au message reçu. Il applique ensuite une fonction de hachage à ce nombre agrégé pour calculer $Hash2TX$.

  Le $Hash2TX$ calculé est "AAAA AAAA AAAA", ce qui diffère du $Hash2TX$ reçu. Étant donné que les calculs sur TX *et* $HashTX$ sont corrects, le nœud 4 considère que le paquet a été envoyé par le nœud légitime 1. Cependant, étant donné que le $Hash2TX$ calculé est incorrect, cela indique que le message a été altéré par un nœud malveillant en cours de route avant d'atteindre sa destination. Par conséquent, le nœud 4 rejette le message et génère une alerte dans le réseau.

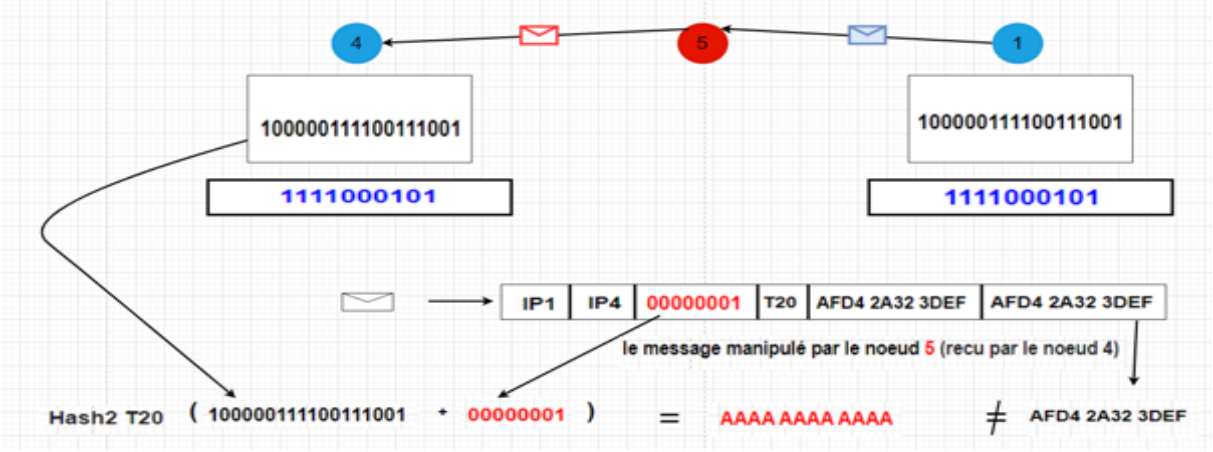

FIGURE 3.17 – Exemple du scénario 2

Problématique 2 : : Que se produit-il en cas d'une attaque émanant d'un nœud inséré au sein des réseaux, soit une attaque interne ? Dans ce scénario, le nœud malveillant détient la table de transmission ainsi que toutes les données présentes chez les nœuds légitimes. Par conséquent, tout nœud a la capacité d'emprunter l'identité d'un autre nœud et de crée un paquet de données, dissimulant ainsi son propre rôle malveillant.. Face à cette situation complexe, quelle serait la solution adéquate ?

Solution : La solution que nous proposons consiste à établir un moyen de confiance entre chaque paire de nœuds. Pour cela, chaque nœud aurait une autre table spéciale supplémentaire pour chaque nœud au sein du réseau , distincte de la table partagée entre tous les nœuds , Cette table unique renfermerait les numéros de séquence des paquets de données échangés précédemment entre les deux nœuds en question.

Quand un nœud envoie un message à un autre nœud, il joindrait le numéro de séquence qui montre le dernier message qu'ils ont partagé. C'est comme un code de confiance entre ces deux nœuds. Le nœud qui reçoit le message aurait aussi une liste avec tous les numéros des messages passés qu'il a échangés avec l'autre nœud. Il vérifierait alors si le numéro du message reçu est le même que celui dans sa propre liste.

Si tout est correspondant , le message serait accepté. Dans le cas contraire, le message serait refusé et un avertissement est envoyé pour signaler qu'il y a peut-être une tentative d'entrée non autorisée dans le réseau.

Exemple 3.7.

Supposons qu'on a un réseau composé de 4 nœuds :

Ns : numéro de séquence.

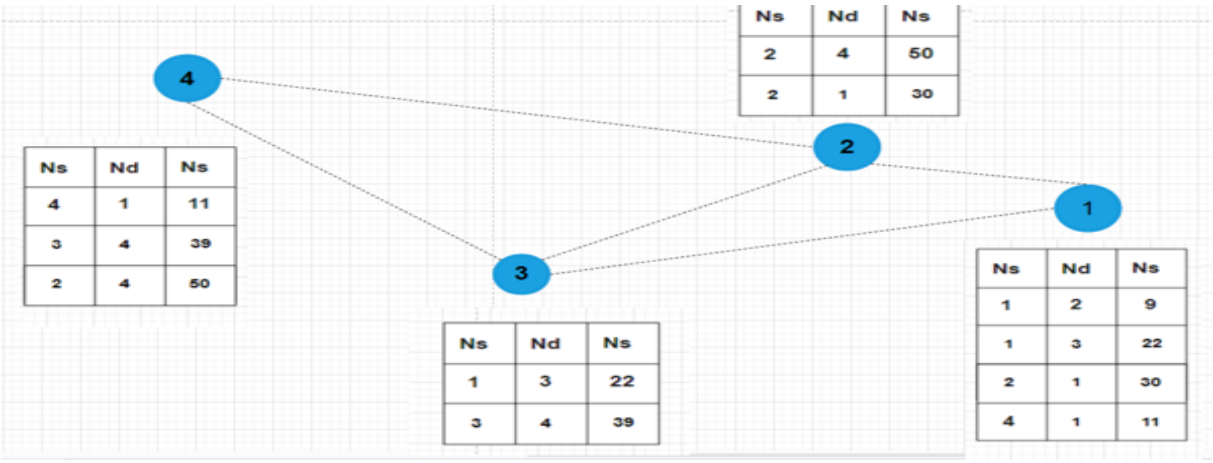

FIGURE 3.18 – Les tables des numéros de séquence.

Supposons que le nœud 2 souhaite envoyer un message au nœud 4. Comme on peut le voir dans la table des numéros de séquence du nœud 2, le dernier paquet échangé entre le nœud 2 et le nœud 4 contient le numéro de séquence "50", ce numéro de séquence se trouve uniquement dans les tables des nœuds 2 et 4, ainsi, lorsque le nœud 4 reçoit le paquet, il vérifie le numéro de séquence de la manière suivante :

- ◇ Si Ns=50 : alors le message provient bien du nœud 2.
- ◇ Si Ns est différent de 50 : cela signifie qu'un autre nœud tente d'utiliser l'identité du nœud 2. Par conséquent, le nœud 4 déclenche une alerte.

  Comme le montre cet exemple, les numéros de séquence sont partagés uniquement entre les deux nœuds qui échangent des messages. Par conséquent, il est impossible qu'un nœud du réseau utilise l'identité d'un autre nœud, car il ne possède pas les numéros de séquences spécifiques de ce nœud.

  Voila le paquet de données envoyer par le nœud 2 :

IP2	IP4	XXXXXX	Tx	Hash Tx	Hash2 Tx	Ns.Tx

Remarque 3.1.

Pour renforcer la sécurité de la mise à jour du message, une étape supplémentaire peut être mise en place : l'ajout d'un **hash Tx**. Les autres nœuds dans le réseau calculent également ce hash et le comparent avec celui reçu. Cette démarche leur permet de vérifier avec certitude que le message de mise à jour provient effectivement d'un nœud légitime. En ajoutant le hashage Tx au processus, on assure une couche de protection supplémentaire qui garantit que les informations de mise à jour sont authentiques et non altérées, renforçant ainsi la confiance dans les échanges au sein du réseau.

Remarque 3.2.

Dans la présentation de ma solution, pour une meilleure compréhension, à été principalement mis l'accent sur les détails de développement de l'idée proposée. Cependant, comme la plupart des mécanismes de routage sécurisé, il est recommandé d'utiliser la cryptographie pour renforcer la sécurité des données échangées entre les nœuds. le partage initial des clés est une étape importante pour établir un environnement de confiance entre les nœuds avant toute communication. Ceci permet aux nœuds de chiffrer et de déchiffrer les données envoyées.

3.6 Objectif générale de la solution proposée

L'objectif principal de la solution proposée est de garantir que seuls les nœuds disposant à la fois de la table de transmission et de la table des numéros de séquences peuvent effectuer des transmissions avec leur propre adresse.

En cas d'usurpation de l'identité d'un autre nœud par un attaquant, ce dernier ne peut pas envoyer de messages en utilisant l'adresse usurpée, car il ne peut pas créer le paquet de données sans disposer de l'historique des communications précédentes.

De plus, il est évident que les messages malveillants peuvent être facilement détectés.

3.7 Conclusion

Au cours de ce chapitre, on à examiné les différents types d'attaques de type "spoofing" dans les réseaux ad hoc, ainsi que les solutions existantes pour contrer ces attaques. on à également élaboré un mécanisme de routage proposé, basé sur l'historique des communications au sein du réseau et l'utilisation de fonctions de hachage. Cette approche me permet de détecter la présence d'attaques "spoofing" dans différents scénarios potentiels.

Dans le prochain chapitre, nous allons présenter la simulation pour mettre en évidence l'efficacité de la solution avancée.

Chapitre 4

Simulation et analyse de performances

4.1 Introduction

La simulation est un élément essentiel de la recherche en sécurité des réseaux, car elle nous permet d'observer le comportement des réseaux dans divers scénarios. Pour ce faire, nous commencerons par définir l'environnement de travail, y compris les spécificités de notre configuration matérielle et logicielle. Ensuite, nous décrirons les scénarios de simulation, en mettant l'accent sur la précision et l'efficacité de notre solution dans la détection des attaques de type spoofing.

4.2 Environnement de travail

4.2.1 Environnement matériel

Dans le cadre de notre étude, nous avons réalisé notre simulation sur un ordinateur DELL de 4è*me* génération équipé d'un processeur Intel $Corei3$ cadencé à 2.00 GHz et doté de 4 Go de mémoire RAM, fonctionnant sous un système d'exploitation Windows 10 64 *bits*.

4.2.2 Environnement logiciel

- **Présentation du simulateur $OMNeT^{++}$:** $OMNeT^{++}$ (Object-oriented Modular Network Environment Toolkit) est un environnement de simulation open source largement utilisé pour la modélisation et la simulation des réseaux de communication. Il propose un vaste éventail de bibliothèques, de composants et d'outils permettant de simuler des scénarios de réseaux ad hoc. $OMNeT^{++}$ est implémenté en C^{++} et en NED (Network Description Language).
- **Le langage C^{++} :** La programmation en C^{++} simplifie la création des modèles de simulation grâce à son approche orientée objet. Ce langage est couramment utilisé pour le développement des protocoles de communication dans les réseaux ad hoc.
- **Le langage NED :** est un langage de description des réseaux utilisé dans $OMNeT^{++}$. Il est spécialement conçu pour décrire l'architecture des réseaux et les interactions entre les

modules de simulation. Il facilite la définition de la topologie du réseau, des liaisons entre les nœuds ainsi que des paramètres propres à chaque module.

Scénarios et simulations :

Sur une surface de 700 × 450 m^2, 10 nœuds sont répartis aléatoirement. Dans un premier temps, nous allons examiner le fonctionnement normal de notre mécanisme de routage en l'absence d'attaque, et observer comment les nœuds s'échangent des paquets entre eux. Ensuite, nous étudierons le fonctionnement de ce mécanisme lorsque l'attaque spoofing est présente.

◇ **Scénario 1 :** Ce scénario présente le fonctionnement du réseau lorsque aucune attaque de type spoofing n'est apparue. Le tableau (TAB suivant) répertorie les paramètres du réseau sur lesquels les simulations de notre mécanisme sont effectuées.

Paramètres	Valeurs
Simulateur	$Omnet^{++}$ 6.0.1
Temps de simulation (ms)	100
Nombre de nœuds légitimes	10
Nombre de nœuds malveillants	0
Temps de simulation (ms)	100
Terrain de simulation	700*450

TABLE 4.1 – Paramètres de simulation en l'absence d'attaque de spoofing

La figure suivante montre la topologie et la simulation de notre réseau sous $OMNET^{++}$:

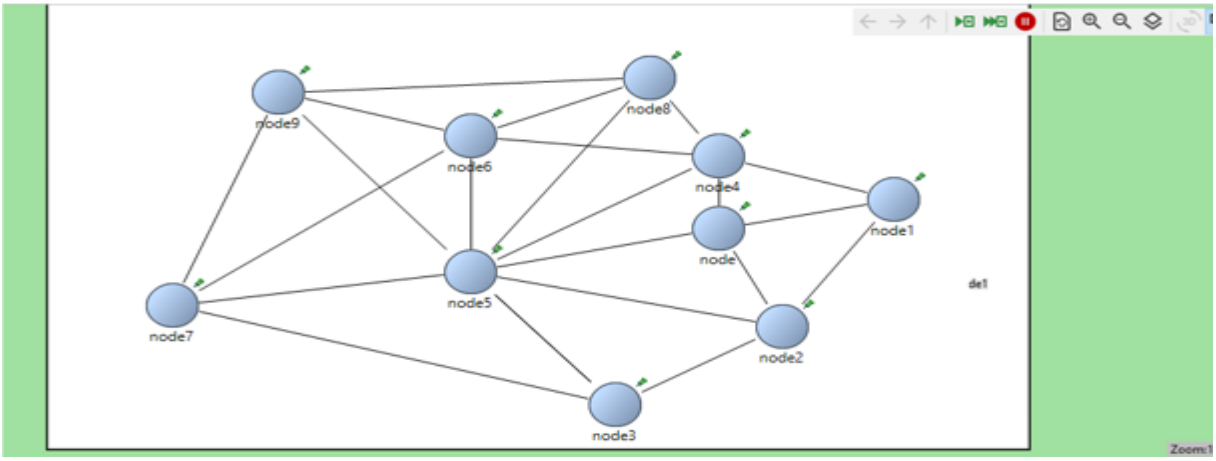

FIGURE 4.1 – Topologie de réseau en l'absence d'attaque de spoofing

On peut observer que tous les nœuds communiquent entre eux sans que des messages ne soient refusés. Le tableau suivant présente les résultats obtenus :

Nombre de nœuds légitimes	10
Nombre de nœuds malveillants	0
Nombre de messages envoyés	50
Nombre de messages reçus	50
Nombre de messages perdus	0

TABLE 4.2 – Tableau présentant les résultats du premier scénario.

On a obtenu les résultats suivants : un nombre de paquets envoyés de 50 et aucun paquet perdu. Cela confirme que le mécanisme sur lequel nous travaillons, représentant la solution proposée dans le chapitre 3, fonctionne correctement. La figure suivante montre la console sous $OMNET^{++}$:

```
** Event #1  t=0  Network.node[0] (Node, id=2)  on selfmsg Message-0 to-6 (Message, id=0)
Message bien recu
** Event #2  t=0  Network.node[7] (Node, id=9)  on Message-0 to-6 (Message, id=0)
Message bien recu
** Event #3  t=0  Network.node[9] (Node, id=11)  on Message-0 to-6 (Message, id=0)
Message bien recu
** Event #4  t=0  Network.node[8] (Node, id=10)  on Message-0 to-6 (Message, id=0)
Message bien recu
** Event #5  t=0  Network.node[1] (Node, id=3)  on Message-0 to-6 (Message, id=0)
Message bien recu
** Event #6  t=0  Network.node[7] (Node, id=9)  on Message-0 to-6 (Message, id=0)
Message bien recu
** Event #7  t=0  Network.node[8] (Node, id=10)  on Message-0 to-6 (Message, id=0)
Message bien recu
** Event #8  t=0  Network.node[7] (Node, id=9)  on Message-0 to-6 (Message, id=0)
Message bien recu
** Event #9  t=0  Network.node[9] (Node, id=11)  on Message-0 to-6 (Message, id=0)
```

FIGURE 4.2 – Console $OMNET^{++}$ en l'absence d'attaque

◇ **Scénario 2 :** Dans ce cas, le nœud 9 est un nœud malveillant qui utilise l'identité d'un autre nœud légitime dans le réseau. Le tableau (TAB suivant) répertorie les paramètres du réseau sur lesquels les simulations de notre mécanisme sont effectuées.

Paramètres	Valeurs
Simulateur	Omnet ++ 6.0.1
Temps de simulation (ms)	100
Nombre de nœuds légitimes	9
Nombre de nœuds malveillants	1
Temps de simulation (ms)	100
Terrain de simulation	700*450

TABLE 4.3 – Paramètres de simulation en présence de l'attaque spoofing

La figure suivante présente la topologie et la simulation de notre réseau sous $OMNeT^{++}$:

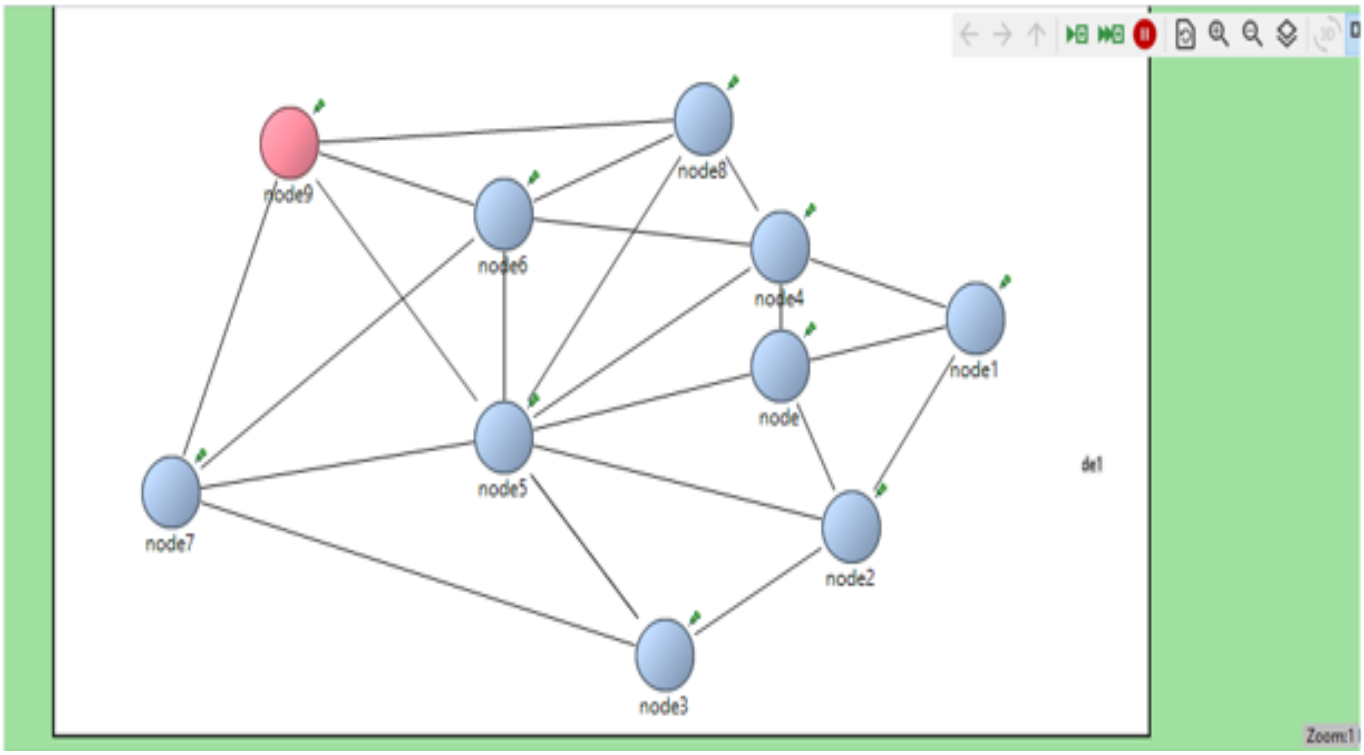

FIGURE 4.3 – Topologie de réseau en présence d'attaque de spoofing

les résultats obtenue lors de ce scénarios sont :

Nombre de nœuds légitimes	9
Nombre de nœuds malveillants	1
Nombre de messages légitimes envoyés	45
Nombre de messages légitimes reçus	45
Nombre de messages malveillants envoyés	5
Nombre de messages malveillants reçus	0

On peut voir qu'à chaque fois que le nœud 9 envoie un paquet, le nœud destinataire détecte l'attaque et refuse le message de ce nœud. De plus, on peut observer que cette attaque n'influence pas le fonctionnement de notre mécanisme, cela signifie que les nœuds refusent le message falsifié tout en continuant de suivre les communications entre eux. Les figures suivantes montrent les consoles sous $OMNeT^{++}$:

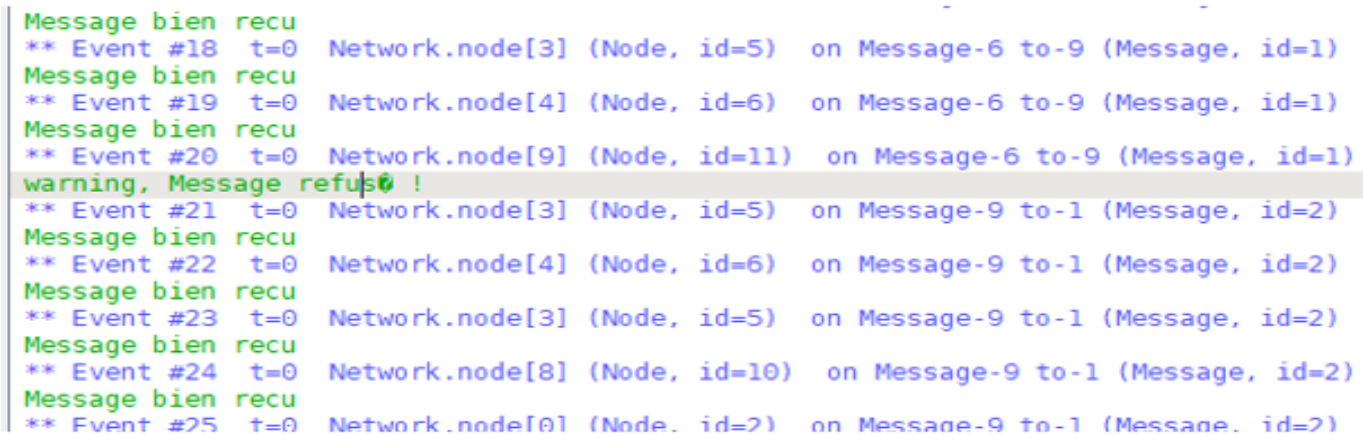

FIGURE 4.4 – Console $OMNeT^{++}$ en présence d'attaque

4.3 Conclusion

Dans ce chapitre, nous avons entamé notre exploration en débutant par la description de l'environnement de travail que nous avons mis en place. Ensuite, nous avons examiné en détail les scénarios que nous avons élaborés dans le cadre du simulateur $OMNeT^{++}$, avant d'étudier en profondeur les résultats obtenus. Cette analyse s'est focalisée sur l'évaluation de la performance et de la précision de notre solution proposée.

Conclusion général

Ce mémoire a exploré en profondeur le monde complexe des réseaux sans fil ad hoc, mettant en évidence leur nature dynamique, leur flexibilité et, malheureusement, leurs vulnérabilités en matière de sécurité, en particulier face aux attaques de spoofing. Notre objectif était de proposer une solution pour contrer ces attaques et renforcer la sécurité de ces réseaux dynamiques.

Au fil de notre recherche, nous avons commencé par une vue d'ensemble des réseaux ad hoc, discutant de leurs caractéristiques, avantages, limitations et applications. Nous avons également examiné les protocoles de routage, les mécanismes de sécurité existants et les attaques potentielles qui peuvent compromettre la fiabilité de ces réseaux.

Nous avons ensuite présenté en détail notre solution proposée pour lutter contre l'attaque de spoofing. Cette solution a été développée à partir du principe de l'historique des communications, afin de renforcer la confiance entre les nœuds communicants. Nous avons décrit en profondeur les étapes de mise en œuvre et fourni des résultats de vérification qui démontrent l'efficacité de notre solution dans divers situations.

L'ensemble de ce travail de recherche vise à répondre à une problématique de sécurité critique dans les réseaux ad hoc, tout en contribuant à une meilleure compréhension des défis spécifiques auxquels ces réseaux sont confrontés. Notre solution propose une réponse concrète à une menace croissante et démontre la faisabilité d'une sécurité renforcée dans ces environnements dynamiques.

Il est important de noter que cette recherche n'est qu'une étape dans la quête continue de sécuriser les réseaux ad hoc. Les défis de sécurité évoluent constamment, et de nouvelles menaces peuvent émerger. Par conséquent, il est essentiel de maintenir la vigilance et de poursuivre la recherche dans ce domaine.

En conclusion, ce mémoire apporte une contribution significative à la sécurité des réseaux ad hoc en proposant une solution anti-spoofing efficace. Il espère également susciter l'intérêt pour la recherche future visant à renforcer encore davantage la sécurité dans ces réseaux dynamiques. La sécurité est un élément clé de la connectivité moderne, et nous aspirons à un avenir où les réseaux ad hoc puissent continuer à prospérer en toute confiance

Bibliographie

[1] Dos attack in mobile ad hoc networks : A survey.h. *IEEE*, 12 :535–541, 2012.

[2] consulté :. *https ://www.bluetooth.com/*, le 12 Mars 2023 à 21 :30.

[3] consulté :. *https ://standards.ieee.org/standard/80211.xhtml*, le 12 Mars 2023 à 22 :35.

[4] consulté :. *https ://www.zigbee.org/*, le 12 Mars 2023 à 23 :15.

[5] Mahmood A Al-Shareeda and Selvakumar Manickam. Man-in-the-middle attacks in mobile ad hoc networks (manets) : Analysis and evaluation. *Symmetry*, 14(8) :1543, 2022.

[6] Abderrahmane Baadache and Ali Belmehdi. Avoiding black hole and cooperative black hole attacks in wireless ad hoc networks. *arXiv preprint arXiv :1002.1681*, 2010.

[7] Nadjib Badache, Djamel Djenouri, Abdelouahid Derhab, and Tayeb Lemlouma. Les protocoles de routage dans les réseaux mobiles ad hoc. *Revue RIST*, 12(2) :77–112, 2002.

[8] Stefano Basagni, Marco Conti, Silvia Giordano, and Ivan Stojmenovic. *Mobile ad hoc networking : cutting edge directions*. John Wiley et Sons, 2013.

[9] Shruti Bhalodiya and Krunal Vaghela. Study of detection and prevention techniques for flooding attack on aodv in manet. *International Journal of Science and Research (IJSR)*, 4(1) :433–436, 2015.

[10] Azzdine Boukerche. *algorithms and protocols for wireless and mobile ad hoc networks*. John Wiley et Sons, Inc., Hoboken, New Jersey simultaneously in Canada, 2009.

[11] Chouaib Boulkamh. *Prise en compte de la Qos par les protocoles de routage dans les réseaux mobiles Ad Hoc*. PhD thesis, Université de Batna 2, 2008.

[12] Gary Breed. Wireless ad hoc networks : Basic concepts. *High frequency electronics*, 1 :44–47, 2007.

[13] Levente Buttyan and Jean-Pierre Hubaux. *Security and cooperation in wireless networks : thwarting malicious and selfish behavior in the age of ubiquitous computing*. Cambridge University Press, 2007.

[14] Network Associates International BV. *Introduction à lacryptographie*, volume 5. Network Associates, 1990- 1998.

[15] Pooja Chahal, Gaurav Kumar Tak, and Anurag Singh Tomar. Comparative analysis of various attacks on manet. *International Journal of Computer Applications*, 111(12), 2015.

[16] Imrich Chlamtac, Marco Conti, and Jennifer J-N Liu. Mobile ad hoc networking : imperatives and challenges. *Ad hoc networks*, 1(1) :13–64, 2003.

[17] Jean-Noël Colin. Du secret à la confiance... quelques éléments de cryptographie. In *L'identification électronique et les services de confiance depuis le règlement eIDAS*, pages 7–28. Larcier, 2016.

[18] denial malware. Spoofing attacks. *Rapid7's Vulnerability Intelligence Report*, 2022.

[19] James F. Kurose et Keith W. Ross. Couche réseau : Plan de données. *Computer Networking*, 2003.

[20] S.Basagni M.Conti et S.Giordano et I.Stojmenovic. *Mobile Ad Hoc Networking*. A John Wiley et Sons,INC,canada, 2004.

[21] Li et Song. *Security and privacy in mobile social networks*. 2013.

[22] J Yang et Y Chen et W Trappe. Detecting spoofing attacks in mobile wireless environments et proc ann ieee comm soc conf. *Sensor*, 2009.

[23] S. Lu et L. Zhang F. Ye, H. Luo. *"Security in Ad Hoc Wireless Networks : A Survey."*. Springer, 2004.

[24] S Biswas F.A. Barbhuiya and S Nandi. An active des based ids for arp spoofing. *IEEE International*, pages 2743 – 2748, 9 Oct 2011.

[25] Cheriton D Faria D. Detecting identity-based attacks in wireless networks using signalprints, in : Wise '06 proceedings of the 5th acm workshop on wireless security. In *Recent Advances in Intrusion Detection : 8th International Symposium, RAID 2005, Seattle, WA, USA, September 7-9, 2005. Revised Papers 8*, pages pp 43–52. Springer, Septembre, 2006.

[26] Eduardo B Fernández, Saeed Rajput, Michael VanHilst, and María M Larrondo-Petrie. Some security issues of wireless systems. In *Advanced Distributed Systems : 5th International School and Symposium, ISSADS 2005, Guadalajara, Mexico, January 24-28, 2005, Revised Selected Papers 5*, pages 388–396. Springer, 2005.

[27] James T Geier. *Wireless Networks first-step*. Cisco Press, 2005.

[28] Priyanka Goyal, Vinti Parmar, Rahul Rishi, et al. Manet : vulnerabilities, challenges, attacks, application. *IJCEM International Journal of Computational Engineering et Management*, 11(2011) :32–37, 2011.

[29] Fanglu Guo and Tzi-cker Chiueh. Sequence number-based mac address spoof detection. In *Recent Advances in Intrusion Detection : 8th International Symposium, RAID 2005, Seattle, WA, USA, September 7-9, 2005. Revised Papers 8*, pages 309–329. Springer, 2006.

[30] Michaël Hauspie. *Contributions à l'étude des gestionnaires de services distribués dans les réseaux ad hoc*. Theses, Université des Sciences et Technologie de Lille - Lille I, January 2005.

[31] Zaiba Ishrat. Security issues, challenges et solution in manet. *IJCST*, 2(4) :108–112, 2011.

[32] Pradip M Jawandhiya, Dr Mangesh Ghonge, MS Ali, and JS Deshpande. A survey of mobile ad hoc network attacks. *Pradip M. Jawandhiya et. al./International Journal of Engineering Science and Technology*, 2(9) :4063–4071, 2010.

[33] Geetha Jayakumar and Gopinath Ganapathy. Performance comparison of mobile ad-hoc network routing protocol. *International Journal of Computer Science and Network Security (IJCSNS)*, 7(11) :77–84, 2007.

[34] Keshav Jindal, Surjeet Dalal, and Kamal Kumar Sharma. Analyzing spoofing attacks in wireless networks. In *2014 Fourth International Conference on Advanced Computing et Communication Technologies*, pages 398–402. IEEE, 2014.

[35] Harjeet Kaur, Varsha Sahni, and Manju Bala. A survey of reactive, proactive and hybrid routing protocols in manet : a review. *network*, 4(3) :498–500, 2013.

[36] Tim Keary. Expert en administration rÉseau. *comparitech*, March 14, 2023.

[37] Issa Khalil, Saurabh Bagchi, and Ness B Shroff. Liteworp : a lightweight countermeasure for the wormhole attack in multihop wireless networks. In *2005 International Conference on Dependable Systems and Networks (DSN'05)*, pages 612–621. IEEE, 2005.

[38] Shefali Khatri, Punit Sharma, Prashant Chaudhary, and Anchit Bijalwan. A taxonomy of physical layer attacks in manet. *International Journal of Computer Applications*, 117(22), 2015.

[39] Jiejun Kong, Z Petros, Haiyun Luo, Songwu Lu, and Lixia Zhang. Providing robust and ubiquitous security support for mobile ad-hoc networks. In *Proceedings Ninth International Conference on Network Protocols. ICNP 2001*, pages 251–260. IEEE, 2001.

[40] Xiao L and Trappe W. Fingerprints in the ether : Using the physical layer for wireless authentication. *Proceedings of IEEE*, pages 4646–4651, 2007.

[41] M.Frikha. *Réseau ad hoc*. Lavoisier, 2010.

[42] C PRIYA, S. Banu et THEEBENDRA. Une étude sur les défis de sécurité dans les réseaux mobiles ad hoc. revue internationale de recherche en applications informatiques et robotique. *ISSN*, 11(2030) :2320–7345, 2016.

[43] Sevil Sen, John A Clark, and Juan E Tapiador. Security threats in mobile ad hoc networks. *Security of self-organizing networks : MANET, WSN, WMN, VANET*, pages 127–147, 2010.

[44] Guy SENOUCI, Sidi-Mohammed et PUJOLLE. Minimisation de la consommation d'énergie dans les réseaux ad hoc. in : Annales des télécommunications. *Paris, Societe de la Revue optique*, 4(1) :500–518, 2005.

[45] Sidi-Mohammed Senouci and Guy Pujolle. Minimisation de la consommation d'énergie dans les réseaux ad hoc. In *Annales des télécommunications*, volume 60, pages 500–518. Paris, Societe de la Revue optique., 2005.

[46] John F Shflch. Inter network naming, addressing, and routing. 1978.

[47] Umesh Kumar Singh, Shivlal Mewada, Lokesh Iaddhani, and Kamal Bunkar. An overview and study of security issues & challenges in mobile ad-hoc networks(manet). *International Journal of Computer Science and Information Security*, 9(4) :106–111, 2011.

[48] Natalie Tischler. Application security knowledge base. *veracode Dynamic Analysis*, 2018.

[49] WordPress. Sc-16(2) : Anti-spoofing mechanisms. *CSF Tools*, 2018.

[50] Lidong Zhou and Zygmunt J Haas. Securing ad hoc networks. *IEEE network*, 13(6) :24–30, 1999.