الجمـهورية الجزائرية الديمقراطية الشعبيـة
وزارة التعليم العالي والبحث العلمي

جـامعـة سعـيـدة د. مـولاي الطـاهـر
كلية الرياضيات و الإعلام الآلي و الاتصالات السلكية و اللاسلكية
قسم: الإعلام الآلي

Mémoire de Master en informatique

Spécialité : Réseaux et Ingénierie des Systèmes Répartis (RISR)

T h è m e

Système de Détection d'Intrusions pour les Réseaux MANETs contre les Attaques Black Hole

- **Présenté par :**
  BERKANI Otmane El Arbi
- **Encadré par :**
  P. MEKKAOUI Kheireddine

Année universitaire 2025-2026

Remerciements

Au terme de ce travail, je tiens en premier lieu à rendre grâce à Allah le Tout-Puissant de m'avoir accordé la force, la patience et l'abnégation nécessaires pour accomplir cette recherche.

J'adresse mes remerciements les plus sincères et ma profonde gratitude à mon encadreur, le Professeur MEKKAOUI Kheireddine, pour sa disponibilité constante, sa rigueur scientifique et ses précieux conseils qui ont été d'une aide inestimable tout au long de la réalisation de ce mémoire.

Je tiens également à exprimer ma reconnaissance envers les membres du jury pour l'honneur qu'ils me font en acceptant d'évaluer ce travail, ainsi qu'à l'ensemble du corps professoral du Département d'Informatique de l'Université de Saïda – Dr. Moulay Tahar, pour la qualité de l'enseignement dispensé durant mon cursus.

Enfin, mes mots ne sauraient suffire pour remercier ma famille et mes proches, dont le soutien moral indéfectible, la patience et les sacrifices ont été le véritable moteur de ma réussite .

Dédicace

À mes très chers parents, source inépuisable d'amour et de sacrifices sans limite.

À mes frères et sœurs, pour leur présence et leur soutien moral constant.

À tous mes enseignants, du primaire jusqu'à l'université, qui m'ont transmis le savoir.

À mes amis et camarades de la promotion M2RISR 2025/2026, avec qui j'ai partagé ces belles années d'études.

BERKANI Otmane El Arbi

Résumé

Les réseaux mobiles ad hoc (MANETs) constituent une catégorie de réseaux sans fil décentralisés, sans infrastructure fixe, où chaque nœud joue simultanément le rôle d'hôte et de routeur. Cette flexibilité expose ces réseaux à de multiples menaces, parmi lesquelles l'attaque Black Hole représente l'une des plus dangereuses : un nœud malveillant falsifie les réponses de routage RREP pour attirer le trafic puis le rejeter sélectivement, échappant ainsi aux mécanismes de détection classiques basés sur les numéros de séquence.

Dans ce mémoire, nous proposons un Système de Détection d'Intrusions basé sur la confiance (Trust-Based IDS), appliqué au protocole AODV. Notre solution combine deux mécanismes complémentaires : une détection rapide par anomalie du numéro de séquence des messages RREP, et une surveillance comportementale fondée sur l'écoute passive du médium radio, qui calcule pour chaque voisin j un score de confiance évalué par fenêtres glissantes de paquets. Un nœud dont le taux de retransmission effectif chute durablement sous $\beta = 0{,}75$ est inscrit dans une liste noire définitive.

Les simulations sous NS-2.35 (Ubuntu 22.04 LTS) sur 11 scénarios distincts démontrent l'efficacité de l'approche : PDR amélioré de 56,23 % à 86,79 % pour 50 nœuds, et de 57,58 % à 91,61 % pour 100 nœuds avec 6 attaquants simultanés. La matrice de confusion établie sur le scénario de référence (15 nœuds, 1 nœud Black Hole) confirme une précision et un taux de détection (Rappel) de 100 %, sans faux positif.

Mots-clés :

MANET, AODV, Black Hole, IDS, Confiance, Écoute Passive, NS-2, PDR, Matrice de confusion, Sécurité réseau.

Abstract

Mobile Ad hoc Networks (MANETs) are decentralized wireless networks without fixed infrastructure, where each node acts simultaneously as a host and a router. This flexibility exposes them to multiple threats, among which the Black Hole attack is one of the most dangerous: a malicious node forges RREP routing replies to attract traffic and then selectively drops it, evading classical detection mechanisms based on sequence numbers.

In this dissertation, we propose a Trust-Based Intrusion Detection System applied to the AODV routing protocol. Our solution combines two complementary mechanisms: a fast detection based on sequence-number anomalies in RREP messages, and a behavioral monitoring mechanism that exploits passive listening of the radio medium to compute, for each neighbor j, a trust score evaluated over sliding windows of packets. A node whose effective forwarding rate persistently falls below $\beta = 0.75$ is permanently blacklisted.

NS-2.35 simulations (Ubuntu 22.04 LTS) across 11 distinct scenarios demonstrate the effectiveness of the approach: PDR improved from 56.23% to 86.79% for 50 nodes, and from 57.58% to 91.61% for 100 nodes with 6 simultaneous attackers. The confusion matrix for the reference scenario (15 nodes, 1 Black Hole node) confirms a precision and a detection rate (Recall) of 100%, with no false positives.

Keywords:

MANET, AODV, Black Hole, IDS, Trust, Passive Listening, NS-2, PDR, Confusion Matrix, Network Security.

ملخص

تُعدّ الشبكات المتنقلة المخصصة (MANETs) فئةً خاصة من الشبكات اللاسلكية اللامركزية التي لا تعتمد على بنية تحتية ثابتة، حيث يؤدي كل عقدة دور المضيف والموجه في آنٍ واحد. هذه الطبيعة المفتوحة تُعرّضها لتهديدات أمنية متعددة، أبرزها هجوم الثقب الأسود (Black Hole)، الذي يعتمد على تزوير ردود التوجيه RREP لاستقطاب حركة المرور ثم إسقاطها بصورة انتقائية، متجاوزاً بذلك آليات الكشف الكلاسيكية.

في هذه المذكرة، نقترح نظام كشف تسلل قائماً على الثقة (Trust-Based IDS) مطبّقاً على بروتوكول AODV، يجمع بين آليتين متكاملتين: كشف سريع يعتمد على رصد الانحراف في رقم تسلسل رسائل RREP، وآلية رصد سلوكي تستغل مبدأ الاستماع السلبي لحساب مؤشر ثقة لكل عقدة جارة وفق نوافذ متتابعة من الحزم. عندما تنخفض نسبة إعادة الإرسال الفعلية للعقدة بشكل دائم دون عتبة $\beta = 0,75$، تُدرج في قائمة سوداء دائمة.

أظهرت نتائج المحاكاة باستخدام NS-2.35 عبر 11 سيناريو مختلفاً تحسناً ملحوظاً في نسبة تسليم الحزم من 56,23% إلى 86,79% لشبكة 50 عقدة، ومن 57,58% إلى 91,61% لشبكة 100 عقدة في مواجهة 6 مهاجمين متزامنين. كما أكّدت مصفوفة الارتباك للسيناريو المرجعي (15 عقدة، عقدة ثقب أسود واحدة) أن معدل الكشف (استدعاء) والدقة بلغا كلاهما 100% دون أي إنذار كاذب.

الكلمات المفتاحية: IDS ، Black Hole ، AODV ، MANET ، الثقة ، NS-2 ، أمن الشبكات.

Liste des Abréviations

Abréviation	Signification
MANET	Mobile Ad hoc Network
AODV	Ad hoc On-demand Distance Vector
DSR	Dynamic Source Routing
DSDV	Destination-Sequenced Distance Vector
OLSR	Optimized Link State Routing
TORA	Temporally Ordered Routing Algorithm
ZRP	Zone Routing Protocol
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
RREQ	Route Request
RREP	Route Reply
RERR	Route Error
PDR	Packet Delivery Ratio
E2ED	End-to-End Delay
CBR	Constant Bit Rate
UDP	User Datagram Protocol
TCP	Transmission Control Protocol
DoS	Denial of Service
MAC	Medium Access Control
NS-2	Network Simulator 2
NAM	Network Animator
TCL	Tool Command Language
OTcl	Object-oriented Tcl
RFC	Request For Comments
WSN	Wireless Sensor Network
VANET	Vehicular Ad hoc Network
IoT	Internet of Things
QoS	Quality of Service
BH	Black Hole

MITM	Man-In-The-Middle
TP	True Positive
TN	True Negative
FP	False Positive
FN	False Negative
TPR	True Positive Rate (Rappel)
FPR	False Positive Rate

TABLE DES MATIÈRES

Introduction Générale

L'évolution fulgurante des technologies de communication sans fil a conduit à l'émergence des réseaux mobiles ad hoc (MANETs – Mobile Ad hoc Networks), des réseaux décentralisés où les nœuds s'auto-organisent sans infrastructure fixe. Chaque nœud y joue simultanément le rôle de terminal et de routeur, ce qui leur confère une grande flexibilité pour les applications militaires, les communications de secours, les réseaux véhiculaires et l'Internet des Objets.

Cependant, l'absence d'infrastructure centralisée et l'ouverture du médium radio font des MANETs des cibles privilégiées pour de nombreuses attaques. L'attaque Black Hole, et plus particulièrement sa variante évoluée dite Black Hole, représente l'une des menaces les plus sérieuses : un nœud malveillant exploite le protocole de routage AODV pour s'interposer sur les routes et supprimer sélectivement le trafic, tout en évitant les mécanismes de détection classiques.

La problématique centrale de ce mémoire est la suivante : comment concevoir un système de détection d'intrusions léger, distribué et efficace, capable de détecter et d'isoler en temps quasi-réel les nœuds Black Hole dans un réseau MANET utilisant AODV, tout en préservant les performances du réseau ?

Pour répondre à cette question, nous proposons un IDS basé sur la confiance, fondé sur l'écoute passive du médium radio et le calcul d'un indice de confiance local. Ce mémoire est organisé en huit chapitres : les Chapitres 1 à 3 couvrent les MANETs, le routage et le protocole AODV ; le Chapitre 4 analyse les attaques ; le Chapitre 5 présente les IDS ; le Chapitre 6 décrit la conception de notre solution ; le Chapitre 7 en détaille l'implémentation et l'intégration dans AODV ; enfin, le Chapitre 8 présente l'environnement de simulation et les résultats expérimentaux.

Chapitre 1 : Les Réseaux MANETs

1.1 Définition et concepts fondamentaux

Un réseau mobile ad hoc (MANET) est un ensemble de nœuds mobiles autonomes qui communiquent par liaisons sans fil sans infrastructure préétablie. Chaque nœud joue un double rôle : terminal de communication et routeur. Le routage multi-sauts (multi-hop) permet d'atteindre des nœuds hors de portée directe via des relais intermédiaires [1].

Historiquement, le concept de réseau ad hoc trouve son origine dans les travaux militaires sur les réseaux radio par paquets (Packet Radio Networks) menés dès les années 1970. L'objectif était de disposer d'un moyen de communication résilient, capable de fonctionner sans aucune infrastructure fixe et de se reconfigurer automatiquement en cas de destruction d'un ou plusieurs nœuds. Cette filiation explique pourquoi la robustesse, l'auto-organisation et la tolérance aux pannes constituent encore aujourd'hui les propriétés fondamentales recherchées dans les MANETs.

Sur le plan fonctionnel, l'absence d'entité centralisée impose que l'ensemble des fonctions réseau — découverte de voisinage, établissement de routes, maintenance de la connectivité et contrôle d'accès au médium — soit assuré de manière entièrement distribuée et coopérative. Chaque nœud doit donc consacrer une partie de ses ressources (énergie, mémoire, bande passante) au relayage du trafic des autres. Cette dépendance mutuelle, indispensable au bon fonctionnement du réseau, constitue précisément le point faible exploité par les attaques de type Black Hole étudiées dans ce mémoire : un seul nœud malveillant peut compromettre la connectivité d'une portion entière du réseau.

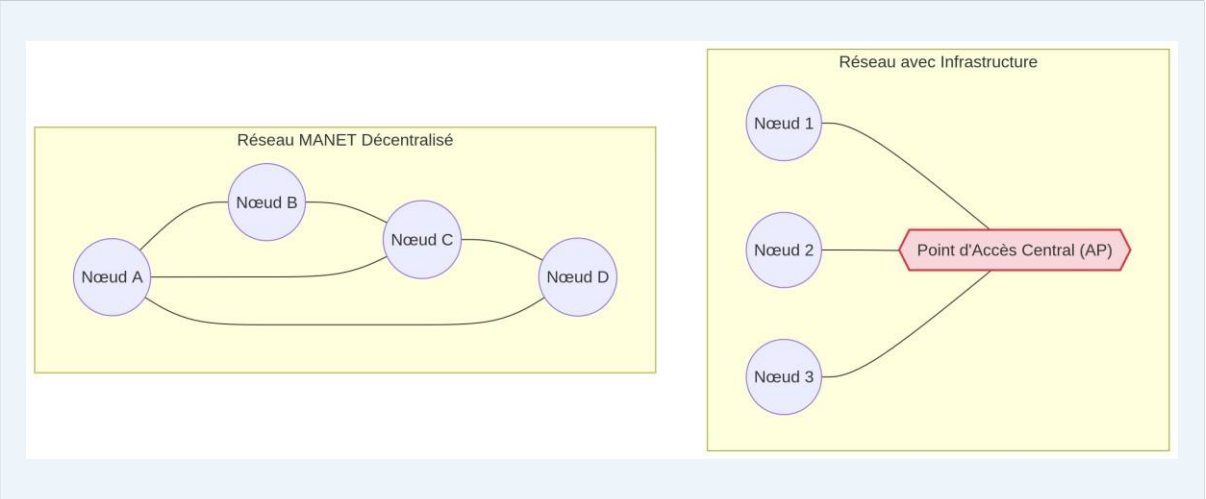

Figure 1.1 : Comparaison entre un réseau MANET décentralisé et un réseau avec infrastructure.

1.2 Caractéristiques fondamentales

- Absence d'infrastructure : déploiement immédiat sans station de base ni point d'accès ;
- Topologie dynamique : modifications constantes dues à la mobilité des nœuds ;

- Ressources limitées : énergie, bande passante et capacité de calcul restreintes ;
- Sécurité intrinsèquement limitée : médium radio ouvert, absence d'autorité centrale ;
- Auto-configuration : découverte autonome des voisins et des routes.

1.3 Domaines d'application

Les MANETs trouvent leurs applications dans : les opérations militaires sur le terrain, les communications de secours lors de catastrophes naturelles, les réseaux véhiculaires (VANETs), les réseaux de capteurs sans fil (WSN) et l'Internet des Objets (IoT). Comme le souligne la Figure 1.1, chaque nœud peut être source, destination ou routeur intermédiaire.

Dans le domaine militaire, les MANETs permettent à des unités déployées sur un théâtre d'opérations de communiquer sans dépendre d'une infrastructure susceptible d'être détruite ou interceptée. Lors des opérations de secours, ils autorisent le rétablissement rapide d'un canal de communication entre équipes d'intervention lorsque les réseaux cellulaires sont hors service. Les réseaux véhiculaires (VANETs) exploitent quant à eux la mobilité des véhicules pour diffuser des alertes de sécurité routière et fluidifier le trafic, tandis que les réseaux de capteurs et l'Internet des Objets reposent sur des nœuds à très faibles ressources qui s'organisent spontanément pour collecter et acheminer des données.

Ces domaines partagent une exigence commune : la communication doit rester fiable malgré un environnement hostile, mobile et ouvert. C'est cette contrainte qui rend la sécurité du routage si critique. En effet, dans la plupart de ces applications (secours, défense, véhicules autonomes), la perte ou la falsification d'un message peut avoir des conséquences graves, ce qui justifie le développement de mécanismes de détection d'intrusions adaptés aux spécificités des MANETs.

1.4 Vulnérabilités spécifiques

- Médium radio ouvert : toute transmission est accessible aux nœuds voisins ;
- Coopération obligatoire : un nœud doit faire confiance à ses voisins pour relayer ses paquets ;
- Topologie dynamique : rend difficile la mise en place de mécanismes de réputation stables ;
- Absence de périmètre de sécurité : aucun pare-feu centralisé ne peut filtrer le trafic.

1.5 Comparaison avec les réseaux sans fil à infrastructure

Pour bien situer les MANETs, il est utile de les comparer aux autres familles de réseaux sans fil. Dans un réseau cellulaire ou un réseau Wi-Fi en mode infrastructure, l'ensemble des communications transite par une entité centrale (station de base ou point d'accès) qui gère l'association des terminaux, l'allocation des ressources radio et le routage du trafic. Cette centralisation simplifie la sécurité — l'authentification et le filtrage s'effectuent au niveau de l'infrastructure — mais introduit un point de défaillance unique et nécessite un déploiement préalable coûteux.

Le MANET se situe à l'opposé de ce modèle : il ne possède aucune infrastructure ni autorité centrale, et chaque nœud participe activement au routage. Cette absence de point central confère au réseau une grande souplesse de déploiement et une robustesse intrinsèque face à la destruction d'un nœud, mais elle déplace l'ensemble des fonctions de gestion et de sécurité vers les nœuds eux-mêmes, qui doivent coopérer sans pouvoir s'appuyer sur un tiers de confiance.

D'autres réseaux partagent cette philosophie décentralisée. Les réseaux de capteurs sans fil (WSN) sont des MANETs spécialisés dont les nœuds, très contraints en énergie, collectent et acheminent des mesures vers un puits de données. Les réseaux véhiculaires (VANETs) constituent une variante caractérisée par une mobilité très élevée et des contraintes temps réel strictes liées à la sécurité routière. Dans tous ces cas, la dépendance à la coopération entre nœuds reste la propriété structurante — et la principale source de vulnérabilité.

1.6 Modèles de mobilité et leur influence sur la topologie

La mobilité des nœuds est la caractéristique qui distingue le plus nettement un MANET d'un réseau filaire. Pour évaluer un protocole de routage ou un mécanisme de sécurité, les chercheurs s'appuient sur des modèles de mobilité qui décrivent statistiquement la manière dont les nœuds se déplacent. Le modèle le plus répandu est le Random Waypoint : chaque nœud choisit une destination aléatoire dans la zone de simulation, s'y déplace à une vitesse tirée aléatoirement, marque une pause, puis recommence. Ce modèle, simple à mettre en œuvre, est utilisé dans la campagne expérimentale présentée au Chapitre 8.

Le choix du modèle et de ses paramètres (vitesse maximale, durée des pauses, densité des nœuds) a un impact direct sur la stabilité des routes. Une mobilité élevée provoque des ruptures de liens fréquentes, ce qui augmente la surcharge de contrôle et le délai de bout en bout, et peut générer des pertes de paquets légitimes. Ce dernier point est crucial pour notre travail : un système de détection d'intrusions doit savoir distinguer une perte due à la mobilité d'une perte provoquée par un nœud malveillant, faute de quoi il générerait de nombreux faux positifs.

1.7 Pile protocolaire et accès au médium

Le fonctionnement d'un MANET repose sur une pile protocolaire dont la couche de liaison joue un rôle déterminant. La norme IEEE 802.11, dans son mode ad hoc (IBSS), est la plus largement utilisée pour l'accès au médium radio. Elle s'appuie sur le mécanisme CSMA/CA (accès multiple avec écoute de la porteuse et évitement de collision), complété par un échange optionnel RTS/CTS destiné à limiter le problème des nœuds cachés.

Cette couche d'accès au médium présente une propriété essentielle pour notre travail : la communication radio est intrinsèquement diffusée (broadcast). Lorsqu'un nœud émet une trame, tous ses voisins situés dans sa portée radio peuvent la capter, même s'ils n'en sont pas les destinataires. Ce mode promiscuité, parfois perçu comme une faiblesse de confidentialité, constitue au contraire l'opportunité exploitée par les mécanismes de surveillance comportementale : un nœud peut écouter passivement si son voisin retransmet effectivement les paquets qu'il est censé relayer.

Au-dessus de la couche liaison, la couche réseau héberge le protocole de routage (objet du chapitre suivant), tandis que les couches transport et application reposent généralement sur les protocoles classiques de l'Internet (TCP, UDP). Cette organisation en couches permet de concevoir des mécanismes de sécurité, comme l'IDS proposé dans ce mémoire, qui s'intègrent au niveau de la couche réseau sans nécessiter de modification des applications.

1.8 Conclusion

Les vulnérabilités intrinsèques des MANETs, notamment l'ouverture du médium radio et l'absence d'autorité centrale, justifient pleinement la nécessité de systèmes de détection d'intrusions adaptés. Le chapitre suivant présente les protocoles de routage utilisés dans ces réseaux.

Chapitre 2 : Le Routage dans les Réseaux MANETs

2.1 Problématique du routage

Le routage dans un MANET consiste à acheminer des paquets depuis une source jusqu'à une destination via des nœuds intermédiaires. La mobilité des nœuds, la portée radio limitée et l'absence d'autorité centrale rendent cette fonction particulièrement complexe.

Contrairement aux réseaux filaires, où la topologie est stable et connue, un protocole de routage pour MANET doit composer avec des liens qui apparaissent et disparaissent en permanence au gré des déplacements des nœuds. Un chemin valide à un instant donné peut devenir inutilisable quelques secondes plus tard. Le protocole doit donc non seulement découvrir des routes, mais aussi détecter rapidement leur rupture et en reconstruire de nouvelles, tout en limitant le volume de messages de contrôle échangés afin de préserver la bande passante et l'énergie des nœuds.

Plusieurs métriques sont utilisées pour évaluer la qualité d'un protocole de routage : le taux de livraison des paquets (PDR), le délai de bout en bout, la surcharge de contrôle (overhead) et la consommation énergétique. Le choix d'un protocole résulte toujours d'un compromis entre ces critères, compromis qui dépend fortement de la densité du réseau, de la vitesse de mobilité et du profil de trafic applicatif.

2.2 Classification des protocoles de routage

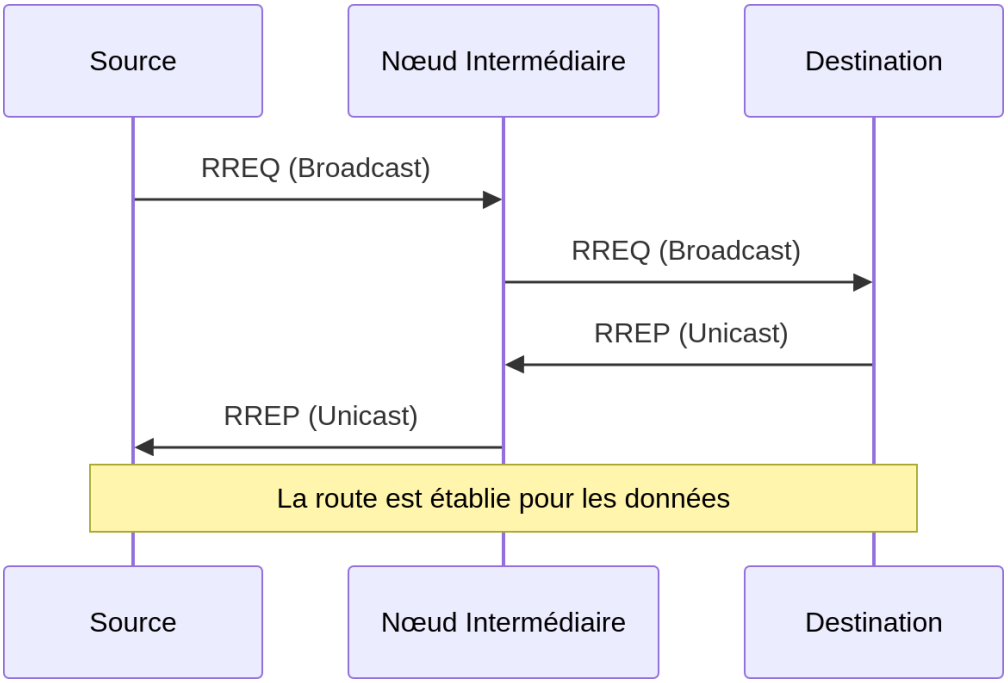

Figure 2.1 : Classification des protocoles de routage MANETs en trois grandes familles. Comme illustré ci-dessus, chaque famille présente un compromis distinct entre réactivité et surcharge protocolaire.

Comme le montre la Figure 2.1, les protocoles de routage se divisent en trois catégories :

- Proactifs (DSDV, OLSR) : maintien permanent de tables de routage, faible délai initial, surcharge élevée ;
- Réactifs (AODV, DSR) : découverte de route à la demande, faible surcharge, délai initial plus élevé ;
- Hybrides (ZRP) : proactif dans une zone locale, réactif pour les nœuds distants.

Le compromis fondamental entre approches proactive et réactive peut se résumer ainsi : les protocoles proactifs offrent un délai initial faible puisque les routes sont déjà disponibles, mais au prix d'une surcharge de contrôle permanente, même en l'absence de trafic ; les protocoles réactifs, à l'inverse, n'engendrent de surcharge qu'au moment où une route est réellement nécessaire, ce qui les rend plus économes dans les réseaux à trafic intermittent, mais introduit un délai de découverte initial. Les protocoles hybrides tentent de combiner les avantages des deux familles en appliquant une stratégie proactive à l'intérieur d'une zone locale et une stratégie réactive au-delà.

2.3 Comparaison des protocoles

Critère	Proactif (DSDV, OLSR)	Réactif (AODV, DSR)	Hybride (ZRP)
Découverte route	Permanente	À la demande	Permanente locale + demande
Délai initial	Faible	Élevé	Moyen
Surcharge contrôle	Élevée	Faible	Moyenne
Conso. énergie	Importante	Modérée	Modérée
Scalabilité	Faible	Moyenne	Bonne
Adapt. mobilité	Faible	Bonne	Bonne

Tableau 2.1 : Comparaison des familles de protocoles de routage MANETs selon six critères clés.

2.4 Justification du choix d'AODV

Dans le cadre de ce travail, nous avons retenu AODV pour les raisons suivantes : standardisation IETF (RFC 3561) [1], implémentation native dans NS-2.35, vulnérabilité documentée aux attaques Black Hole facilitant la comparaison avec l'état de l'art, et bonnes performances en conditions normales (PDR > 99 % en l'absence d'attaque, comme le confirme le Scénario A du Tableau 7.2).

2.5 Maintenance et réparation des routes

Découvrir une route ne suffit pas : dans un MANET, un protocole de routage doit surtout être capable de maintenir les routes face à la mobilité. Lorsqu'un lien se rompt — parce qu'un nœud intermédiaire s'est éloigné — le protocole doit détecter la rupture, en informer les nœuds

concernés et déclencher la reconstruction d'un nouveau chemin. Les protocoles réactifs comme AODV s'appuient pour cela sur des messages d'erreur (RERR) propagés vers la source, qui relance alors une procédure de découverte.

La rapidité de cette réparation conditionne directement la qualité de service perçue par les applications. Une détection tardive des ruptures se traduit par des paquets perdus et un délai accru ; à l'inverse, une détection trop sensible peut déclencher des reconstructions inutiles et saturer le réseau de messages de contrôle. Les protocoles modernes intègrent donc des mécanismes de temporisation et de réparation locale destinés à équilibrer réactivité et stabilité.

2.6 Enjeux de sécurité du routage

Les protocoles de routage pour MANETs ont été conçus, à l'origine, dans une optique de performance et d'efficacité, en supposant que tous les nœuds se comportent de manière honnête. Cette hypothèse de coopération est précisément ce que les attaquants exploitent. Un nœud malveillant peut fausser le processus de découverte de route en émettant de fausses réponses, attirer le trafic vers lui, puis le supprimer ou le détourner.

La sécurisation du routage est rendue difficile par les contraintes propres aux MANETs : absence d'autorité de certification accessible en permanence, ressources limitées qui interdisent les mécanismes cryptographiques lourds, et topologie changeante qui complique l'établissement de relations de confiance durables. Ces difficultés justifient l'intérêt des approches comportementales, qui détectent les nœuds malveillants à partir de leurs actions observables plutôt qu'à partir de signatures cryptographiques — approche au cœur de la solution proposée dans ce mémoire.

2.7 Panorama des principaux protocoles de routage

Au-delà de la classification générale, il est utile de présenter brièvement les protocoles les plus représentatifs de chaque famille. Parmi les protocoles proactifs, DSDV (Destination-Sequenced Distance Vector) maintient une table de routage complète actualisée périodiquement et introduit des numéros de séquence pour éviter les boucles, tandis qu'OLSR (Optimized Link State Routing) optimise la diffusion de l'information d'état des liens grâce au mécanisme des relais multipoints (MPR).

Parmi les protocoles réactifs, DSR (Dynamic Source Routing) repose sur le routage à la source : la route complète est insérée dans l'en-tête de chaque paquet, ce qui simplifie le traitement intermédiaire mais alourdit les en-têtes dans les grands réseaux. AODV (Ad hoc On-demand Distance Vector), étudié en détail au chapitre suivant, combine la découverte de route à la demande de DSR avec les numéros de séquence de DSDV, sans transporter la route entière dans les paquets.

Les protocoles hybrides, enfin, tentent de réunir les avantages des deux approches. ZRP (Zone Routing Protocol) en est l'exemple le plus connu : il applique une stratégie proactive à l'intérieur d'une zone de routage centrée sur chaque nœud et une stratégie réactive pour atteindre les destinations situées au-delà de cette zone. Ce panorama illustre la diversité des

compromis possibles et justifie le choix d'AODV pour notre étude, en raison de sa large adoption, de sa standardisation et de sa vulnérabilité documentée aux attaques Black Hole.

2.8 Métriques d'évaluation des protocoles

L'évaluation comparative des protocoles de routage repose sur un ensemble de métriques quantitatives standardisées. Le taux de livraison des paquets (PDR, Packet Delivery Ratio) mesure le rapport entre le nombre de paquets de données effectivement reçus par les destinations et le nombre de paquets émis par les sources ; c'est l'indicateur le plus direct de la fiabilité du réseau et celui qui est le plus fortement dégradé par une attaque Black Hole.

Le délai de bout en bout moyen (End-to-End Delay) représente le temps écoulé entre l'émission d'un paquet et sa réception. Il intègre les délais de découverte de route, de mise en file d'attente et de retransmission au niveau MAC. La surcharge de routage (routing overhead) quantifie quant à elle le volume de messages de contrôle (RREQ, RREP, RERR) générés par rapport au trafic utile : un protocole efficace doit maintenir cette surcharge aussi faible que possible afin de préserver la bande passante.

À ces métriques s'ajoute la consommation énergétique, particulièrement critique pour les réseaux de capteurs, ainsi que le débit utile (throughput) qui mesure la quantité d'information utilement transmise par unité de temps. Ces indicateurs, qui seront repris dans la campagne d'évaluation du Chapitre 8 pour mesurer l'efficacité de la solution proposée, ne sont pas indépendants : améliorer l'un se fait souvent au détriment d'un autre, ce qui explique qu'aucun protocole ne soit universellement optimal.

2.9 Conclusion

Ce chapitre a présenté les familles de protocoles de routage pour MANETs. Le protocole AODV, retenu pour ce travail, sera étudié en détail au chapitre suivant.

Chapitre 3 : Le Protocole AODV

3.1 Présentation générale

AODV (Ad hoc On-Demand Distance Vector, RFC 3561 [1]) est un protocole réactif utilisant des numéros de séquence pour garantir des routes fraîches et sans boucle. Il supporte le routage unicast et multicast, et s'adapte aux topologies dynamiques.

Conçu pour les réseaux ad hoc de taille moyenne, AODV se distingue par son caractère purement réactif : aucune route n'est maintenue tant qu'aucune communication ne l'exige, ce qui réduit considérablement la surcharge de contrôle dans les réseaux où le trafic est intermittent. Le protocole a été standardisé par l'IETF dans la RFC 3561, ce qui lui a valu une très large adoption, tant dans les travaux de recherche que dans les implémentations de simulateurs comme NS-2.

3.2 Messages de contrôle

AODV utilise trois types de messages, dont les structures sont illustrées par les Figures 3.1 à 3.3 ci-dessous :

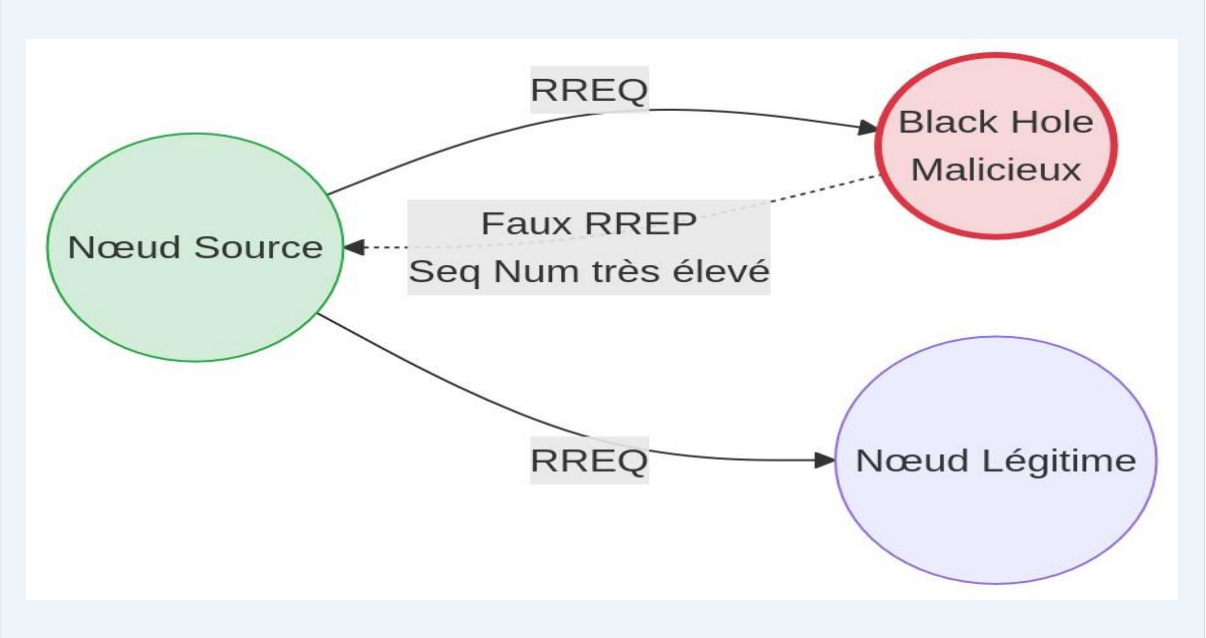

Figure 3.1 : Structure du message RREQ. Le champ Destination Sequence Number est exploité par le Black Hole pour falsifier les réponses (voir Chapitre 4).

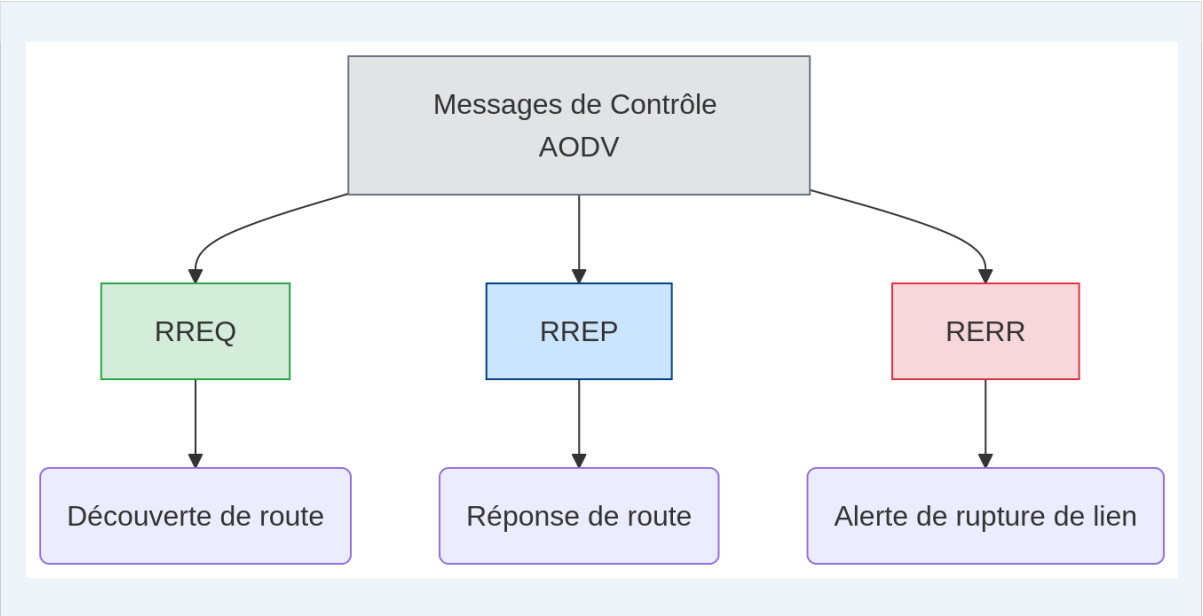

Figure 3.3 : Structure du message RERR, déclenché lors de la détection d'une rupture de lien.

Ces trois types de messages suffisent à assurer l'ensemble des fonctions du protocole : la découverte de routes (RREQ et RREP), leur maintenance et la signalisation des ruptures (RERR). Leur diffusion est contrôlée par des mécanismes de numérotation et de durée de vie (TTL) qui limitent la portée des inondations et évitent la circulation indéfinie des messages dans le réseau.

3.3 Procédure de découverte de route

La procédure de découverte de route, illustrée par la Figure 3.4, se déroule en quatre étapes : (1) diffusion du RREQ par la source ; (2) propagation et vérification par les nœuds intermédiaires ; (3) réponse RREP par la destination ou un nœud avec route fraîche ; (4) acheminement du RREP vers la source et établissement de la route.

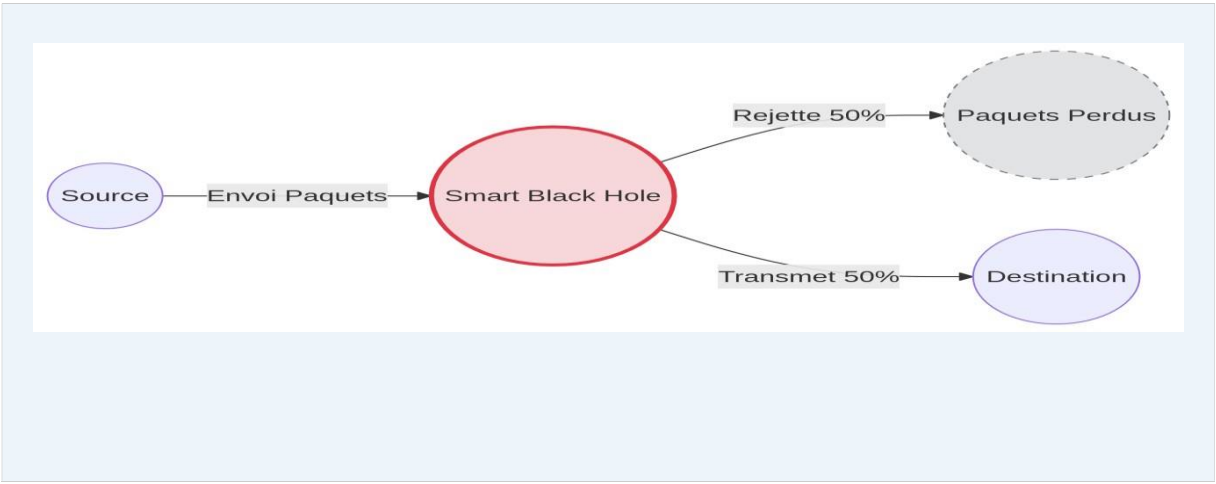

Figure 3.4 : Procédure de découverte de route AODV. Le nœud source S diffuse un RREQ ; la destination D répond par un RREP acheminé en unicast.

3.4 Vulnérabilités d'AODV

La conception d'AODV repose sur un postulat de confiance : chaque nœud est supposé respecter le protocole. Cette hypothèse est exploitée par les attaques Black Hole, analysées au chapitre suivant.

Cette confiance aveugle dans les informations annoncées par les nœuds constitue le talon d'Achille du protocole. AODV ne prévoit en effet aucun mécanisme d'authentification des messages de contrôle ni de vérification de la cohérence des numéros de séquence annoncés. Un nœud malveillant peut donc forger des réponses de route arbitraires sans risque d'être démasqué par le protocole lui-même.

C'est précisément pour combler cette lacune, sans alourdir le protocole ni en modifier les messages, que nous proposons dans les chapitres suivants un mécanisme de confiance fondé sur l'observation du comportement réel des nœuds. Plutôt que de chercher à authentifier les annonces, notre approche vérifie a posteriori que les nœuds respectent effectivement leur engagement de relayage.

3.5 Numéros de séquence et fraîcheur des routes

Le mécanisme central qui garantit l'absence de boucles de routage dans AODV est le numéro de séquence de destination. Chaque nœud maintient un compteur qu'il incrémente à chaque modification de sa situation, et chaque entrée de la table de routage est associée au numéro de séquence le plus récent connu pour la destination correspondante. Lorsqu'un nœud doit choisir entre deux routes vers une même destination, il privilégie celle dont le numéro de séquence est le plus élevé, c'est-à-dire la plus « fraîche ».

Ce principe, qui fait la robustesse d'AODV en fonctionnement normal, constitue paradoxalement la faille exploitée par l'attaque Black Hole. En annonçant un numéro de séquence artificiellement élevé dans une fausse réponse de route (RREP), un nœud malveillant se fait systématiquement préférer comme prochain saut, quelle que soit sa position réelle. La source, trompée, achemine alors ses paquets vers l'attaquant. La compréhension fine de ce mécanisme est donc indispensable pour concevoir une contre-mesure efficace, comme nous le ferons dans les chapitres suivants.

3.6 Tables de routage et gestion des entrées

Chaque nœud AODV maintient une table de routage dont les entrées contiennent, pour chaque destination connue, l'adresse du prochain saut, le nombre de sauts, le numéro de séquence de destination et une durée de vie. Cette durée de vie joue un rôle essentiel : une entrée non utilisée pendant un certain délai est purgée, ce qui évite l'accumulation de routes obsolètes dans un environnement où la topologie évolue constamment.

La gestion de ces entrées s'appuie également sur la liste des précurseurs, c'est-à-dire les voisins qui utilisent une route donnée. Lorsqu'une rupture est détectée, ce sont ces précurseurs qui sont notifiés par un message RERR. Cette organisation permet à AODV de réparer efficacement les routes tout en limitant la diffusion des messages de contrôle aux seuls nœuds réellement concernés. C'est dans ces structures de données que s'insérera, au Chapitre 7, le

mécanisme de confiance proposé, sans modification de la structure des messages du protocole.

3.7 Format des messages de contrôle

Les messages de contrôle d'AODV possèdent une structure normalisée par la RFC 3561. Le message RREQ (Route Request) contient notamment l'adresse de la source et celle de la destination recherchée, un identifiant de requête (RREQ ID) permettant de détecter les doublons lors de la diffusion, le numéro de séquence de la source, le dernier numéro de séquence connu pour la destination, ainsi qu'un compteur de sauts incrémenté à chaque relais.

Le message RREP (Route Reply), émis en réponse à un RREQ par la destination ou par un nœud disposant d'une route suffisamment fraîche, transporte le numéro de séquence de destination, le nombre de sauts jusqu'à la destination et une durée de vie de la route. C'est le champ « numéro de séquence de destination » de ce message qui est falsifié lors d'une attaque Black Hole : en y inscrivant une valeur très élevée, l'attaquant fait passer sa fausse route pour la plus récente.

Le message RERR (Route Error) signale enfin la rupture d'un ou plusieurs liens en listant les destinations devenues inaccessibles. La connaissance précise de ces formats est indispensable à l'implémentation : notre solution, décrite au Chapitre 7, exploite l'observation de ces messages et du trafic de données sans en modifier la structure, garantissant ainsi une compatibilité totale avec les nœuds AODV standard.

3.8 Exemple illustratif de découverte de route

Afin de synthétiser le fonctionnement d'AODV, considérons un exemple simple où une source S cherche à atteindre une destination D à travers plusieurs nœuds intermédiaires. Ne disposant d'aucune route valide vers D, S incrémente son numéro de séquence, construit un message RREQ et le diffuse à tous ses voisins. Chaque voisin qui reçoit ce RREQ pour la première fois enregistre une route inverse vers S, incrémente le compteur de sauts, puis rediffuse le message à son tour.

Lorsque le RREQ atteint la destination D (ou un nœud intermédiaire possédant une route suffisamment fraîche vers D), celui-ci génère un message RREP qu'il achemine en unicast le long de la route inverse précédemment établie, jusqu'à la source. À chaque saut, les nœuds traversés mettent à jour leur table de routage avec la route directe vers D. À la réception du RREP, la source dispose enfin d'une route complète et peut commencer à émettre ses paquets de données.

Cet exemple met en évidence la confiance implicite qu'AODV accorde aux annonces des nœuds : la source retient la première réponse présentant le numéro de séquence le plus élevé, sans pouvoir vérifier que le répondeur dispose réellement d'une route vers la destination. C'est exactement cette confiance non vérifiée qui sera exploitée par les attaques étudiées au chapitre suivant, et que la solution proposée s'attachera à contrôler par l'observation du comportement effectif des nœuds.

3.9 Conclusion

Ce chapitre a présenté le fonctionnement détaillé d'AODV, ses messages et son mécanisme de découverte de route. Ses vulnérabilités face aux nœuds malveillants constituent le cœur du problème traité dans ce mémoire.

Chapitre 4 : Les Attaques dans les Réseaux AODV

4.1 Classification des attaques

Les attaques contre les MANETs se classent selon leur position (externe / interne) et leur nature (passive / active). La Figure 4.1 présente cette classification. Les attaques internes sont les plus dangereuses car l'attaquant dispose des informations légitimes du réseau.

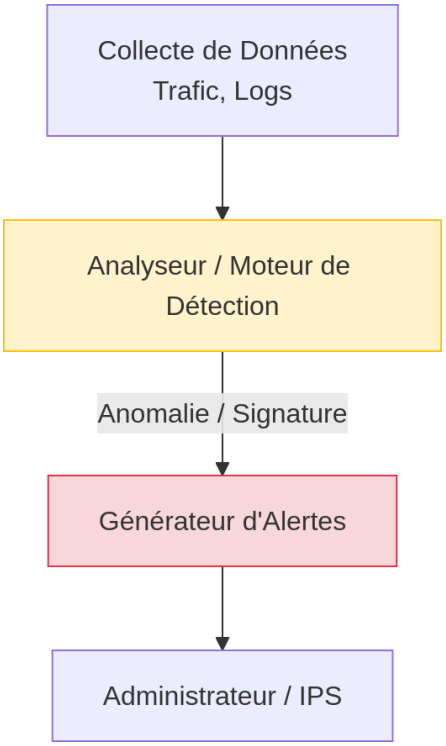

Figure 4.1 : Classification des attaques MANETs. Les attaques de couche réseau (Black Hole, Worm Hole, Sybil) sont les plus dévastatrices pour les performances.

4.2 L'attaque Black Hole classique

Dans l'attaque Black Hole (Figure 4.2), le nœud malveillant M répond à chaque RREQ par un RREP falsifié contenant un numéro de séquence élevé et un nombre de sauts minimal. La source, trompée, achemine ses paquets vers M qui les supprime, créant un déni de service (DoS) [2]. Selon la Figure 4.2, le PDR chute de ~99 % à moins de 22 % (Scénario C, Tableau 7.2).

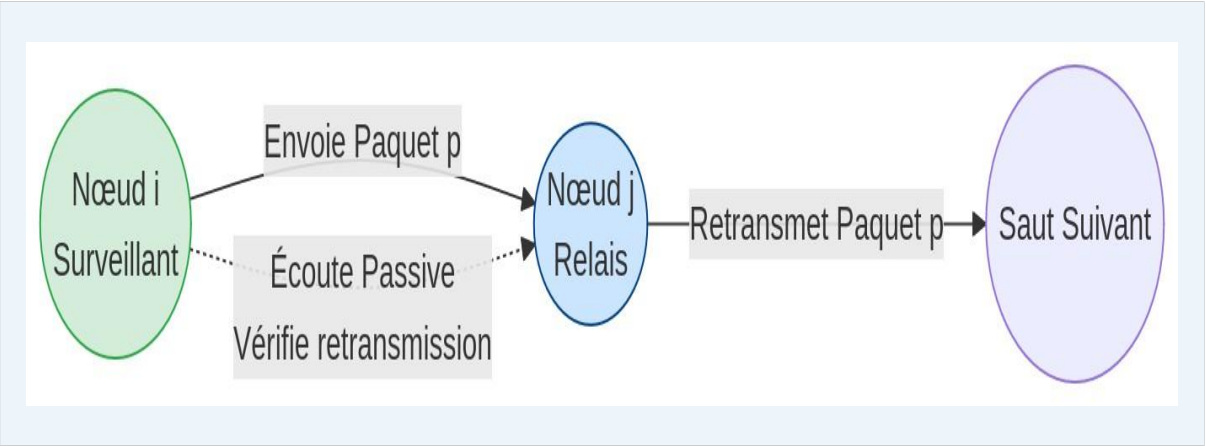

Figure 4.2 : Scénario d'attaque Black Hole classique. Le nœud malveillant M se fait passer pour le détenteur de la route la plus courte vers D et supprime tous les paquets reçus.

4.3 Le Black Hole – Attaque évoluée

Le Black Hole contourne les IDS classiques grâce à quatre mécanismes, illustrés par la Figure 4.3 :

1. Prédiction du numéro de séquence par la méthode des moindres carrés : le nœud observe les numéros de séquence légitimes et calcule une droite de régression $y = Ax + B$ pour prédire le prochain numéro de séquence attendu, y ajoutant un petit incrément α (formule 4.1) ;
2. Émission de fausses RREQ pour simuler un comportement légitime de diffusion ;
3. Selective packet dropping : rejet d'une fraction $\rho \in [0{,}5 ; 0{,}8]$ des paquets, passant sous le radar des IDS basés sur le taux global de perte ;
4. Coopération entre attaquants dans les scénarios d'attaque multiple.

$$\mathbf{seqNum\_prédit = A \cdot x + B + \alpha} \quad \text{..... (4.1)}$$

où $A = COV(X,S)/\sigma^2 x$, $B = \bar{S} - A \cdot \bar{X}$, X est l'intervalle de temps entre séquences, S est la valeur de séquence.

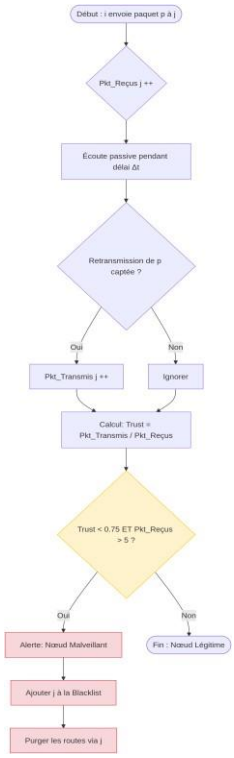

Figure 4.3 : Mécanisme du Black Hole. La droite de régression (formule 4.1) permet au nœud malveillant de prédire le numéro de séquence attendu et d'envoyer un RREP crédible tout en rejetant sélectivement les paquets.

4.4 Pourquoi les IDS classiques échouent

Les IDS basés sur le seuil de numéro de séquence sont défaits par la prédiction (formule 4.1). Les IDS basés sur le taux global de perte sont défaits par le selective dropping. Notre IDS, fondé sur l'observation directe du comportement de retransmission, constitue la parade naturelle à ces limitations.

4.5 Impact sur les métriques de performance

$$\textbf{PDR} = (\textbf{Paquets reçus} / \textbf{Paquets envoyés}) \times 100\ \% \quad (4.2)$$

$$\textbf{E2ED} = (1/N) \times \Sigma(t_{réception,i} - t_{émission,i}) \quad \textbf{[ms]} \quad (4.3)$$

$$\textbf{Throughput} = (\textbf{Paquets reçus} \times \textbf{Taille} \times 8) / \textbf{Durée\_simulation} \quad \textbf{[kbps]} \quad (4.4)$$

Une attaque Black Hole réussie fait typiquement chuter le PDR (formule 4.2) de 99 % à moins de 22 %. Le délai (formule 4.3) peut être multiplié par 6, en raison des retransmissions et redécouvertes de routes. Ces formules sont utilisées pour évaluer tous les scénarios du Chapitre 7.

4.6 Attaques de routage apparentées

L'attaque Black Hole appartient à une famille plus large d'attaques de routage qui exploitent la coopération entre nœuds. L'attaque Gray Hole en est une variante furtive : au lieu de supprimer la totalité du trafic, le nœud malveillant n'élimine qu'une fraction des paquets, ou ne s'attaque qu'à certains flux, ce qui rend sa détection nettement plus difficile que celle d'un

Black Hole pur. C'est précisément ce comportement sélectif que notre solution comportementale cherche à détecter.

D'autres attaques visent le routage sans nécessairement supprimer le trafic. L'attaque Wormhole établit un tunnel entre deux nœuds distants pour fausser la perception de la topologie, tandis que l'attaque Sybil consiste, pour un nœud, à usurper plusieurs identités afin de prendre le contrôle d'une part disproportionnée des routes. Bien que ce mémoire se concentre sur le Black Hole et sa variante évoluée, le mécanisme d'observation comportementale proposé constitue une première ligne de défense potentiellement extensible à plusieurs de ces menaces, car toutes se traduisent, à un moment ou à un autre, par un écart observable entre le comportement annoncé et le comportement réel d'un nœud.

4.7 Déroulement détaillé d'une attaque Black Hole

Pour bien comprendre la menace, il est instructif de dérouler les étapes d'une attaque Black Hole sur AODV. Lorsqu'une source S souhaite communiquer avec une destination D, elle diffuse un message RREQ dans le réseau. Le nœud malveillant M, dès qu'il reçoit ce RREQ, n'attend pas de connaître une véritable route vers D : il répond immédiatement par un RREP falsifié annonçant un numéro de séquence de destination très élevé et un nombre de sauts minimal.

Comme ce RREP falsifié parvient généralement à la source avant les réponses légitimes — l'attaquant ne perdant pas de temps à vérifier l'existence d'une route — et qu'il annonce les métriques les plus favorables, la source sélectionne M comme prochain saut vers D. À partir de cet instant, tout le trafic destiné à D est acheminé vers M, qui le supprime silencieusement au lieu de le relayer. Le résultat est un déni de service partiel ou total sur le flux concerné.

Dans sa variante évoluée, l'attaquant raffine ce comportement pour échapper aux détections fondées sur le seuil de numéro de séquence : il limite l'ampleur de l'incrément annoncé et peut n'éliminer qu'une partie du trafic (dropping sélectif), ce qui le rend statistiquement proche d'un nœud légitime soumis à des pertes naturelles. C'est cette furtivité qui motive le recours, dans ce mémoire, à une détection fondée sur l'observation directe du comportement de retransmission plutôt que sur l'analyse des seuls champs déclarés dans les messages.

4.8 Conclusion

Ce chapitre a analysé les attaques Black Hole et Black Hole et démontré les limites des IDS classiques. La solution proposée, décrite au Chapitre 6, s'appuie sur l'observation comportementale directe pour surmonter ces limitations.

Chapitre 5 : Les Systèmes de Détection d'Intrusions (IDS)

5.1 Définition et classification

Un IDS surveille les activités réseau pour détecter les comportements malveillants. La Figure 5.1 présente la classification des IDS selon la méthodologie de détection et la portée de la surveillance.

On distingue traditionnellement les IDS selon leur portée de déploiement. Les IDS basés sur l'hôte (HIDS) surveillent l'activité interne d'un nœud particulier (appels système, journaux, intégrité des fichiers), tandis que les IDS basés sur le réseau (NIDS) analysent le trafic circulant sur le médium afin de détecter des schémas suspects. Dans le contexte des MANETs, l'absence de point de concentration du trafic (routeur, passerelle) rend les NIDS centralisés inopérants : la détection doit être distribuée et exécutée localement par chaque nœud à partir des seules informations qu'il peut observer dans son voisinage radio.

Un IDS pour MANET doit en outre respecter des contraintes propres à cet environnement : il doit être léger afin de ne pas épuiser les ressources limitées des nœuds, autonome car aucun serveur central ne peut centraliser les alertes, et robuste face à la mobilité qui modifie continuellement le voisinage observé. Ces contraintes orientent naturellement le choix vers des approches comportementales locales, telles que celle proposée dans ce mémoire.

Figure 8.2 - PDR du scénario S1 (Normal)

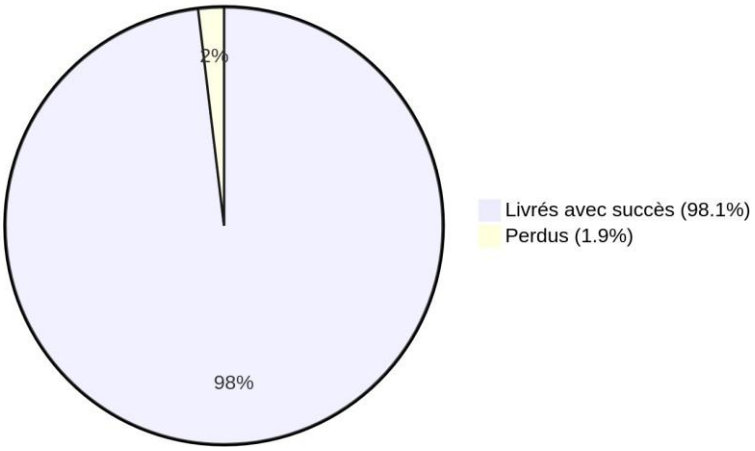

Figure 5.1 : Classification des systèmes de détection d'intrusions. Notre solution appartient à la catégorie anomalie-based + NIDS distribué.

5.2 IDS basés sur les signatures

Ces IDS détectent les attaques connues par correspondance à une base de signatures. Très efficaces pour les attaques répertoriées, ils sont incapables de détecter les attaques inconnues ou les Black Holes qui s'adaptent dynamiquement.

5.3 IDS basés sur les anomalies

Ces IDS modélisent le comportement normal et détectent les déviations. Notre Trust-Based IDS appartient à cette catégorie : le comportement normal est défini par Trust(j) ≥ β = 0,75 (retransmission de 75 % des paquets reçus au minimum).

Les méthodes de détection par anomalie se déclinent en plusieurs familles : les approches statistiques, qui établissent un profil de référence et signalent tout écart significatif ; les approches fondées sur l'apprentissage automatique, qui apprennent la frontière entre comportements normaux et anormaux à partir de données ; et les approches par spécification, qui définissent explicitement les règles d'un comportement légitime. L'approche retenue dans ce mémoire relève de cette dernière catégorie, enrichie d'un indice de confiance quantitatif : un nœud est considéré comme légitime tant que son taux effectif de retransmission demeure au-dessus du seuil défini.

Le principal défi des IDS basés sur les anomalies réside dans la maîtrise du taux de faux positifs : un comportement légitime mais inhabituel (par exemple, des pertes de paquets dues à une congestion ou à une rupture de lien) risque d'être interprété à tort comme une attaque. C'est pourquoi notre solution introduit une période d'immunité initiale et un seuil de décision soigneusement calibré, dont la justification expérimentale est détaillée aux chapitres suivants.

5.4 État de l'art des IDS pour Black Hole

Approche	Référence	PDR protégé	Limite principale
Seuil séq. dynamique	Gurung 2019 [7]	~75 %	Battue par BH (moindres carrés)
Mod. protocole AODV	Tami 2021 [14]	~80 %	Modifie les messages AODV
Cryptographie	Dhanaraj 2022	~85 %	Surcharge calculatoire élevée
Confiance passive	Marchang 2012 [4]	~88 %	Base de notre solution
IA (Firefly+ANN)	Rani 2022 [17]	~90 %	Phase d'entraînement nécessaire
Notre Trust-Based IDS	Ce mémoire	86–91 %	Aucun message supplémentaire

Tableau 5.1 : Comparaison qualitative de notre IDS avec les approches de la littérature. Notre solution obtient des résultats comparables aux approches IA sans phase d'entraînement.

5.5 Métriques d'évaluation d'un IDS

L'évaluation repose sur la matrice de confusion (TP, TN, FP, FN) et les métriques dérivées :

$$\textbf{Taux de détection (Rappel / TPR)} = TP / (TP + FN) \quad (5.1)$$

$$\textbf{Taux de faux positifs (FPR)} = FP / (FP + TN) \quad (5.2)$$

$$\textbf{Précision} = TP / (TP + FP) \quad (5.3)$$

F1-Score = 2 × (Précision × Rappel) / (Précision + Rappel) ..... (5.4)

Ces métriques seront calculées au Chapitre 7 pour valider quantitativement notre IDS.

5.6 Défis spécifiques des IDS dans les MANETs

La transposition des systèmes de détection d'intrusions classiques au contexte des MANETs se heurte à plusieurs obstacles fondamentaux. D'abord, l'absence de point de concentration du trafic rend impossible le déploiement d'une sonde centrale capable d'observer l'ensemble des communications ; la détection doit donc être distribuée et reposer uniquement sur les observations locales de chaque nœud. Ensuite, les ressources limitées des nœuds (énergie, mémoire, capacité de calcul) interdisent les analyses lourdes et imposent des mécanismes légers.

À ces contraintes s'ajoute la difficulté majeure de la distinction entre anomalie malveillante et anomalie légitime. Dans un réseau mobile, les pertes de paquets dues aux ruptures de liens, à la congestion ou aux collisions radio sont fréquentes et parfaitement normales. Un IDS comportemental doit donc être conçu pour tolérer ces fluctuations sans les confondre avec une attaque, sous peine de générer un taux de faux positifs prohibitif. C'est pour répondre à ce défi que la solution proposée dans ce mémoire introduit une période d'immunité initiale et un seuil de confiance soigneusement calibré.

Enfin, un IDS pour MANET doit lui-même être robuste face aux attaques. Un mécanisme de détection distribué qui échangerait des alertes entre nœuds deviendrait une cible : un attaquant pourrait diffuser de fausses accusations pour faire exclure des nœuds légitimes. L'approche retenue évite cet écueil en s'appuyant exclusivement sur l'observation locale et passive du voisinage, sans aucun échange de messages de contrôle supplémentaire.

5.7 Architectures de détection distribuées et coopératives

Plusieurs architectures ont été proposées pour déployer un IDS dans un MANET. L'architecture autonome confie à chaque nœud la responsabilité de détecter localement les intrusions, à partir des seules informations qu'il observe. C'est l'approche la plus simple et la plus robuste, car elle ne dépend d'aucun échange de messages susceptible d'être attaqué ; c'est aussi celle retenue dans ce mémoire.

Les architectures coopératives, à l'inverse, font collaborer plusieurs nœuds qui partagent leurs observations afin d'améliorer la précision de la détection, notamment pour les attaques difficiles à caractériser localement. Cette coopération a toutefois un coût : elle introduit une surcharge de communication et ouvre la voie à des attaques contre le système de détection lui-même, par exemple la diffusion de fausses accusations visant à faire exclure des nœuds légitimes.

Entre ces deux extrêmes, des architectures hiérarchiques organisent le réseau en groupes (clusters) au sein desquels certains nœuds, élus comme têtes de groupe, assument un rôle de surveillance renforcé. Le choix d'une architecture résulte toujours d'un compromis entre précision de détection, surcharge induite et résistance aux attaques. La solution proposée dans

ce mémoire privilégie délibérément l'architecture autonome et l'observation passive, afin de garantir légèreté et robustesse sans introduire de nouvelle surface d'attaque.

5.8 Conclusion

Ce chapitre a présenté les IDS et identifié les limites des approches existantes face aux Black Holes. Notre solution Trust-Based IDS, décrite au chapitre suivant, comble ces lacunes par une observation comportementale directe sans surcharge cryptographique.

Chapitre 6 : Solution Proposée – Conception de l'IDS Basé sur la Confiance

6.1 Philosophie de la solution

Le constat fondateur de notre approche est le suivant : les Black Holes exploitent les déclarations des nœuds (numéros de séquence dans les RREP) pour tromper les mécanismes de détection. La parade consiste à observer non pas les déclarations, mais les actes : un nœud qui reçoit un paquet et ne le retransmet pas est suspect. Ce principe exploite le caractère broadcast du médium radio : lorsque le nœud j transmet un paquet, tous ses voisins peuvent le capter (Figure 6.1).

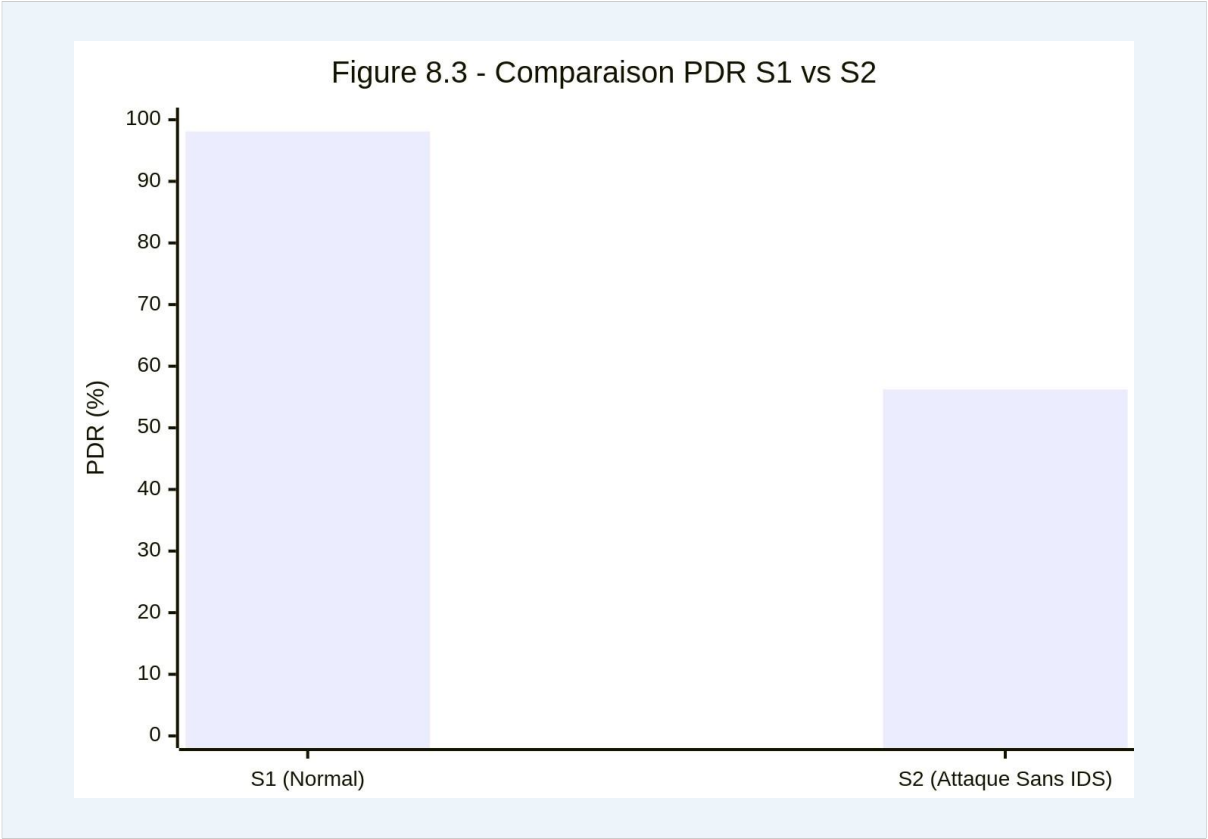

Figure 6.1 : Principe de l'écoute passive. Le nœud i envoie p à j et écoute le canal pendant Δt. Si j ne retransmet pas p, Pkt_Reçus(j) est incrémenté mais pas Pkt_Transmis(j), faisant diminuer Trust(j).

6.2 Formule du taux de confiance

Pour formaliser ce principe, considérons que chaque nœud i maintient, pour chaque voisin j, deux compteurs cumulés : Pkt_Reçus(j), le nombre de paquets confiés à j, et Pkt_Transmis(j), le nombre de ces paquets effectivement retransmis par j. Le taux de confiance cumulé Trust_i(j) peut alors être défini conceptuellement par la formule (6.1) :

$$\textbf{Trust\_i(j) = Pkt\_Transmis(j) / Pkt\_Reçus(j)} \quad (6.1)$$

Convention : Trust_i(j) = 1 si Pkt_Reçus(j) = 0.

- Trust(j) = 1 : comportement parfaitement coopératif (retransmission de 100 % des paquets) ;
- Trust(j) = 0 : Black Hole pur (rejet de 100 % des paquets) ;
- 0 < Trust(j) < 1 : comportement potentiellement malveillant (Black Hole avec selective dropping, typiquement ρ = 0,5 à 0,8).

Le ratio cumulé Trust_i(j) défini par la formule (6.1) constitue le modèle conceptuel de notre approche : il exprime, en théorie, la proportion globale de paquets effectivement retransmis par j depuis le début de la surveillance. En pratique cependant, un ratio cumulé sur la totalité de la session présente un défaut connu : il réagit très lentement à un changement de comportement, car un grand nombre de paquets correctement retransmis avant l'attaque « dilue » l'effet d'un comportement malveillant survenant ensuite. C'est pourquoi l'implémentation décrite au Chapitre 7 opérationnalise ce principe sous une forme glissante et incrémentale — un score borné [0, 100] évalué par fenêtres successives de paquets — qui conserve exactement la même logique de détection (un nœud qui ne retransmet pas est sanctionné) tout en réagissant beaucoup plus rapidement aux changements de comportement. La correspondance précise entre les deux formulations, ainsi que la justification du seuil opérationnel qui en découle, est détaillée à la section 7.4.

6.3 Justification du seuil β = 0,75

Le choix de β = 0,75 comme seuil conceptuel sur le ratio cumulé Trust_i(j) est justifié par l'analyse des deux types d'erreurs :

- Si β est trop élevé (ex. 0,90) : les pertes naturelles dues aux collisions radio (typiquement 5–10 %) et aux ruptures de liens transitoires génèrent de nombreux faux positifs. Des expérimentations préliminaires sur le Scénario A (réseau sain) montrent un PDR de 99,72 %, soit des pertes naturelles de 0,28 % : un seuil de 0,90 serait donc sûr, mais un seuil de 0,95 serait risqué en mobilité élevée.
- Si β est trop bas (ex. 0,50) : un attaquant pratiquant un dropping de 60 % (Trust ≈ 0,40) serait détecté, mais un attaquant subtil à 40 % (Trust ≈ 0,60) passerait inaperçu. La littérature [5] montre que les Black Holes typiques rejettent 50–80 % des paquets.

Le seuil β = 0,75 constitue donc le meilleur compromis : il absorbe les pertes naturelles (< 25 %) tout en détectant les Black Holes (Trust < 0,75 pour ρ > 25 %). Ce choix est en accord avec les recommandations de Marchang et Datta [4] qui utilisent un seuil similaire dans leur protocole de confiance. Ce seuil conceptuel de 75 % de retransmission constitue la référence à partir de laquelle est dérivé, au Chapitre 7, le seuil opérationnel du score de confiance utilisé dans l'implémentation NS-2.

6.4 Algorithme de détection

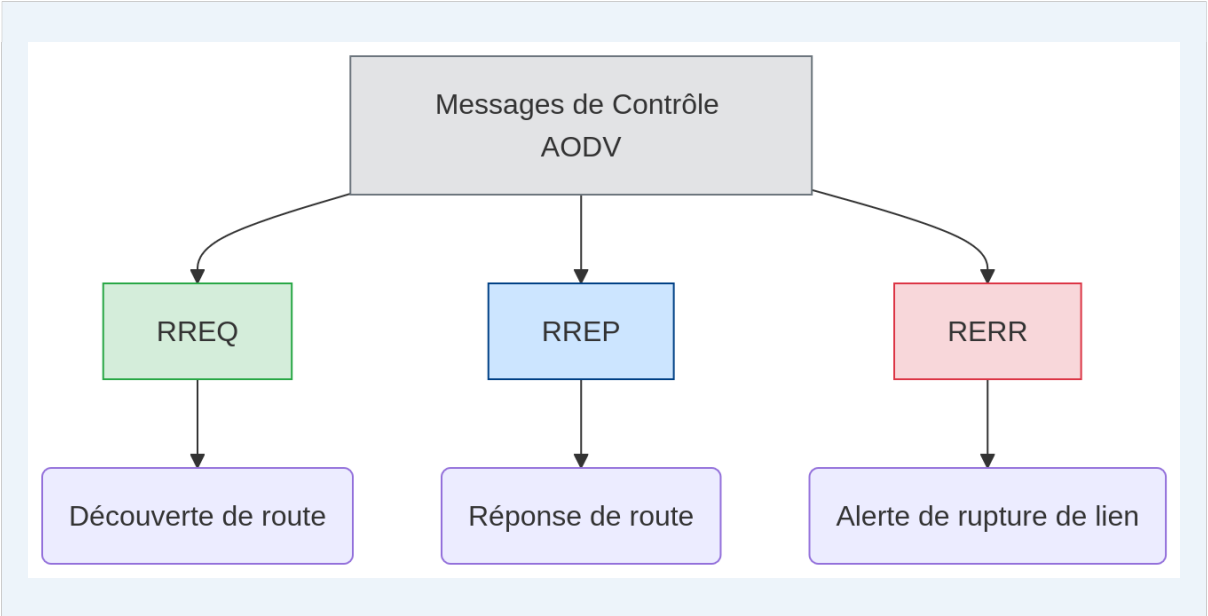

Figure 6.2 : Organigramme du Trust-Based IDS. L'algorithme s'exécute localement sur chaque nœud i. La décision est prise uniquement après observation d'au moins Seuil_Min = 5 paquets pour éviter les faux positifs statistiques.

L'algorithme, illustré par la Figure 6.2, se décompose en cinq étapes :

5. Initialisation : pour chaque nouveau voisin j, initialiser Pkt_Reçus(j) = 0 et Pkt_Transmis(j) = 0.
6. Comptage : pour chaque paquet envoyé à j, incrémenter Pkt_Reçus(j) += 1.
7. Écoute passive : pendant la fenêtre Δt, si j retransmet le paquet, incrémenter Pkt_Transmis(j) += 1.
8. Calcul périodique : Trust(j) = Pkt_Transmis(j) / Pkt_Reçus(j) (formule 6.1).
9. Décision : si Trust(j) < 0,75 ET Pkt_Reçus(j) > 5 → Malveillant, Blacklist, purge des routes, notification AODV.

6.5 Pseudocode formel

ALGORITHME Trust-Based IDS (Écoute Passive)
INITIALISATION: ∀ voisin j → Pkt_Reçus(j)=0 ; Pkt_Transmis(j)=0
ENVOI p à j : Pkt_Reçus(j)++ ; activer écoute passive Δt
ÉCOUTE : si (i capte retransmission de p par j) → Pkt_Transmis(j)++
ÉVALUATION : Trust(j) = Pkt_Transmis(j) / Pkt_Reçus(j) [formule 6.1]
DÉCISION : si Trust(j)<0.75 ET Pkt_Reçus(j)>5 → MALVEILLANT + Blacklist + Purge routes

Remarque sur l'implémentation. L'algorithme ci-dessus présente la version conceptuelle de la décision, fondée sur le ratio cumulé Trust_i(j) et le seuil β = 0,75. Le Chapitre 7 décrit la traduction opérationnelle de cette logique sous la forme d'un score borné évalué par fenêtres glissantes de 7 paquets (formule 7.1), ainsi que d'un second mécanisme complémentaire fondé sur l'anomalie de numéro de séquence. Les deux formulations partagent le même principe — un nœud qui ne retransmet pas les paquets qui lui sont confiés voit sa confiance chuter jusqu'au blacklisting — mais la version du Chapitre 7 est celle effectivement implémentée et évaluée au Chapitre 8.

6.6 Mécanisme de Blacklisting

Une fois j classé comme malveillant : (1) tout RREP/RREQ de j est rejeté ; (2) les routes via j sont purgées ; (3) une nouvelle RREQ sécurisée est déclenchée ; (4) l'inscription dans la liste noire est définitive pour la session. Ce mécanisme garantit que le trafic contourne le Black Hole dès sa détection.

6.7 Intégration dans NS-2.35

L'intégration est réalisée par extension du module AODV natif de NS-2.35. Les modifications portent sur les fichiers aodv.h (structures TrustEntry, trust_table, blacklist) et aodv.cc (fonctions recordPacketSent(), recordPacketForwarded(), evaluateTrust(), isBlacklisted(), purgeRoutesVia()). Aucune modification de la structure des messages AODV n'est nécessaire. La Figure 6.3 illustre la topologie initiale d'un réseau MANET de 15 nœuds telle que visualisée dans le simulateur NS-2, configuration qui servira de base aux scénarios d'évaluation présentés au Chapitre 8.

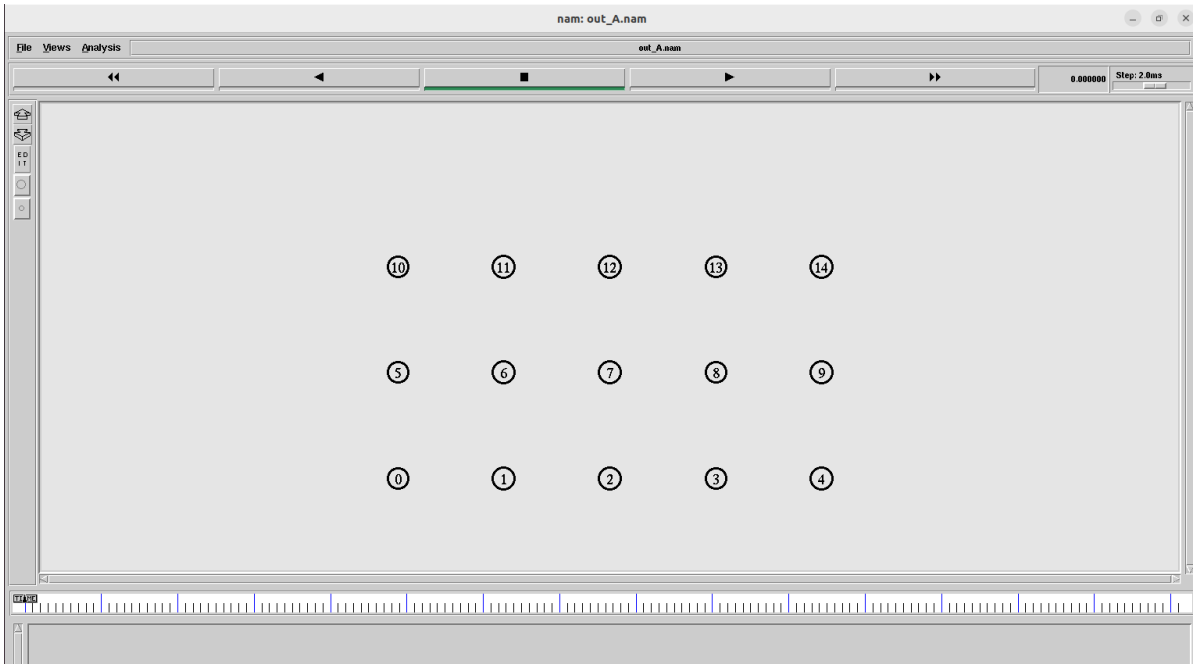

Figure 6.3 : Topologie initiale du réseau MANET (15 nœuds) dans le simulateur NS-2.

6.8 Analyse de la complexité

- Complexité temporelle : O(|N(i)|) par évaluation périodique, O(1) par paquet ;
- Complexité spatiale : O(|N(i)|) pour la table de confiance locale ;

- Surcharge réseau : nulle – aucun message supplémentaire échangé ;
- Surcharge énergétique : modérée, due au mode promiscuité de l'interface radio.

6.9 Conclusion

Ce chapitre a présenté notre Trust-Based IDS : formule de confiance (6.1), justification du seuil $\beta = 0{,}75$, algorithme complet (Figure 6.2) et intégration NS-2.35. Le chapitre suivant présente la validation expérimentale.

Chapitre 7 : Implémentation Détaillée et Intégration de l'IDS dans AODV

7.1 Introduction

Alors que le chapitre précédent a introduit les principes conceptuels de notre solution (philosophie de détection comportementale, indice de confiance et justification du seuil), le présent chapitre en détaille l'implémentation complète et l'intégration concrète au sein du protocole AODV. Notre approche repose sur un système de détection d'intrusions basé sur la confiance (IDS basé sur la confiance), implémenté directement au sein du protocole AODV natif du simulateur NS-2.35. La conception de cette solution répond à un cahier des charges précis : légèreté computationnelle, distribution complète (pas de nœud central), absence de modification de la structure des messages AODV, et efficacité démontrée face aux Black Holes qui contournent les approches classiques par seuil de séquence.

Ce chapitre est organisé comme suit : la section 7.2 expose la philosophie générale et l'architecture de la solution ; la section 7.3 décrit le mécanisme d'écoute passive ; la section 7.4 formalise mathématiquement la métrique de confiance ; la section 7.5 présente l'algorithme de détection complet ; la section 7.6 décrit le mécanisme de blacklisting et son intégration avec AODV ; la section 7.7 détaille les structures de données et les points d'instrumentation dans le code source ; enfin, les sections 7.8 et 7.9 analysent respectivement la complexité algorithmique et les avantages et limites de la solution.

7.2 Philosophie générale de la solution

La conception de notre IDS est fondée sur une observation comportementale simple mais puissante : dans un réseau MANET fonctionnant normalement, un nœud intermédiaire légitime retransmet systématiquement les paquets de données qu'il reçoit, puisque son rôle de routeur l'y oblige. En revanche, un nœud Black Hole — même dans sa variante évoluée, capable de contourner les seuils de séquence — se trahit inévitablement par son comportement effectif au niveau des données : il absorbe les paquets sans les retransmettre.

Notre solution exploite ce principe en implémentant un mécanisme d'écoute passive (passive listening) : chaque nœud surveille en silence le comportement de ses voisins sur le canal radio partagé, en comptant les paquets qu'il leur a transmis et en vérifiant s'ils les retransmettent effectivement. Cette surveillance est entièrement locale et distribuée — aucun nœud central n'est requis — et elle ne nécessite aucune modification de la structure des messages AODV.

La solution intègre deux mécanismes complémentaires :

- Mécanisme 1 — Détection par anomalie de séquence : détection rapide et précoce des Black Holes classiques, basée sur l'analyse du numéro de séquence contenu dans les messages RREP.
- Mécanisme 2 — Surveillance comportementale par score de confiance : détection des Black Holes qui contournent le premier mécanisme, basée sur l'observation du comportement effectif de retransmission des paquets de données.

7.3 Mécanisme d'écoute passive

L'écoute passive (passive listening) est un principe fondamental des réseaux sans fil : le médium radio est partagé, et tout nœud à portée peut entendre les transmissions de ses voisins, même lorsqu'elles ne lui sont pas directement destinées. Notre IDS exploite cette propriété pour surveiller le comportement de retransmission de chaque voisin.

Concrètement, lorsque le nœud i transmet un paquet de données au nœud j (son prochain saut vers la destination), il attend, dans un délai défini par la portée radio, d'entendre j retransmettre ce paquet au nœud suivant. Si j retransmet effectivement le paquet, cela est enregistré comme un comportement honnête. Si j ne retransmet pas le paquet après la fenêtre d'observation de 7 paquets, cela est enregistré comme un comportement suspect.

Ce mécanisme est implémenté dans le code source via deux compteurs globaux, définis dans aodv.cc :

```
int global_node_forward_count[100] = {0};  // Nombre de paquets transmis par chaque nœud
int pkts_given_to_neighbor[100] = {0};      // Nombre de paquets confiés à chaque voisin
int initial_fwd_count[100][100] = {0};      // Valeur de référence au début de chaque fenêtre
```

Le nœud i calcule, à la fin de chaque fenêtre d'évaluation de 7 paquets, le nombre de paquets effectivement retransmis par son voisin j depuis le début de la fenêtre. Si ce nombre est inférieur ou égal à 2 (seuil bas de retransmission), le comportement de j est qualifié de suspect.

7.4 Formule du taux de confiance

La métrique centrale de notre IDS est le score de confiance Trust(j), défini pour chaque nœud j observé par son voisin i. Ce score est calculé sur une échelle de 0 à 100, initialisé à 100 (confiance totale) et mis à jour à chaque cycle d'évaluation.

Ce score Trust(j) est la version opérationnelle du ratio cumulé Trust_i(j) introduit par la formule (6.1) du Chapitre 6 : les deux grandeurs répondent au même principe — quantifier la proportion de paquets confiés à j que celui-ci retransmet effectivement — mais le score (7.1) est recalculé de manière glissante, par fenêtres successives de 7 paquets, plutôt que de manière cumulée sur l'ensemble de la session. Cette formulation incrémentale est celle effectivement codée dans aodv.cc et utilisée pour produire l'ensemble des résultats du Chapitre 8.

Formellement, le score de confiance est mis à jour selon la règle d'évaluation définie par la formule (7.1) :

$$Trust(j) \leftarrow Trust(j) - 35, \ si \ Fwd(j) \leq 2 \ (comportement\ suspect) \quad \ldots (7.1a)$$

$$Trust(j) \leftarrow Trust(j) + 15, \ si \ Fwd(j) > 2 \ (comportement\ honnête) \quad \ldots (7.1b)$$

$$Trust(j) \leftarrow min(Trust(j), 100) \ et \ Trust(j) \leftarrow max(Trust(j), 0) \quad \ldots (7.1c)$$

où Fwd(j) représente le nombre de paquets retransmis par le nœud j au cours de la fenêtre d'évaluation courante (fenêtre de 7 paquets).

Le seuil de décision est fixé à **β = 25/100** (soit 0,25) : un nœud j est déclaré malveillant et inscrit dans la blacklist lorsque son score de confiance atteint ou descend en dessous de ce seuil. Ce seuil correspond à la valeur du score après deux cycles consécutifs de comportement suspect (100 − 35 − 35 = 30 ; 30 − 35 = −5, donc bloqué avant de sortir de 25). Il convient de noter que ce seuil opérationnel β = 0,25 et le seuil conceptuel β = 0,75 du Chapitre 6 portent sur deux grandeurs différentes — un score cyclique borné [0, 100] d'une part, un ratio cumulé de retransmission d'autre part — et ne sont donc pas numériquement comparables terme à terme. Le lien entre les deux réside dans leur calibration commune : le seuil opérationnel a été réglé de sorte qu'un nœud soit blacklisté après deux cycles consécutifs où il retransmet au plus 2 paquets sur 7 (soit moins de 29 % de retransmission par cycle), ce qui correspond bien à un comportement durablement situé sous le seuil conceptuel de 75 % de retransmission fixé au Chapitre 6. Le seuil β = 0,75 mentionné dans le résumé désigne donc le seuil conceptuel de retransmission qui motive et encadre la conception de l'algorithme opérationnel, et non une valeur directement comparée au score 0–100.

Cette formulation asymétrique (décrémentation de 35 points contre incrémentation de 15 points) est intentionnelle : elle reflète le principe de précaution dans la détection d'intrusions — un comportement suspect est sanctionné plus sévèrement qu'un comportement honnête n'est récompensé, afin de converger rapidement vers la détection tout en restant robuste face aux fluctuations temporaires légitimes.

7.5 Algorithme de détection complet

7.5.1 Période d'immunité (Warmup Phase)

Un paramètre fondamental de notre IDS est la période d'immunité, fixée à 5 secondes depuis le démarrage de la simulation. Durant cette période, l'IDS surveille et enregistre les comportements, mais n'applique aucune sanction (ni décrémentation du score de confiance, ni mise en blacklist). Ce délai permet au réseau de se stabiliser physiquement : au démarrage, les nœuds sont en phase de découverte de routes, et les pertes de paquets légitimes (dues à la non-disponibilité des routes) pourraient être interprétées à tort comme un comportement malveillant.

Cette logique est implémentée dans la condition suivante du code source :

```
if (CURRENT_TIME > 5.0) {
   // Phase stable : évaluation et mise à jour du score
   if (forwarded_by_neighbor <= 2) {
      trust_score[nexthop] -= 35;
   } else {
      trust_score[nexthop] += 15;
   }
} else {
   // Phase warmup : surveillance sans sanction
   printf("[TRUST IDS - WARMUP] ...");
}
```

7.5.2 Mécanisme 1 — Détection par anomalie de numéro de séquence

Le premier mécanisme de détection, plus rapide, est basé sur l'analyse du numéro de séquence destination contenu dans les messages RREP. Il est implémenté dans la fonction recvReply() d'AODV, immédiatement après réception d'un RREP.

La règle de détection est définie par la formule (7.2) :

$$Si\ rp\_dst\_seqno > rt\_seqno + 100 \rightarrow nœud\ source\ du\ RREP\ classé\ MALVEILLANT \quad ... (7.2)$$

La valeur 100 représente le seuil β de détection par séquence. Cette valeur a été choisie de manière à dépasser significativement l'incrément normal du numéro de séquence entre deux requêtes consécutives, tout en restant inférieur aux valeurs artificiellement élevées utilisées par les Black Holes classiques (qui annoncent typiquement des numéros de séquence de plusieurs milliers). Conformément aux travaux de Mekkaoui et Teggar [1], les Black Holes peuvent contourner ce mécanisme en utilisant la méthode des moindres carrés pour prédire le numéro de séquence légitime et y ajouter un petit incrément α. C'est précisément pour neutraliser ce contournement que le second mécanisme est nécessaire.

L'implémentation dans aodv.cc est la suivante :

```
if (rp->rp_dst_seqno > rt->rt_seqno + 100) {
   nsaddr_t malicious_node = ih->saddr();
   if (!blacklist[malicious_node]) {
      blacklist[malicious_node] = true;
      printf("[IDS LOG] NODE %d BLACKLISTED\n", malicious_node);
   }
   drop(p, DROP_RTR_ROUTE_LOOP);
   return;
}
```

7.5.3 Mécanisme 2 — Surveillance comportementale (Trust Score)

Le second mécanisme, plus robuste mais plus lent, surveille le comportement effectif de retransmission de chaque voisin. Il est implémenté dans la fonction forward() d'AODV, qui est appelée à chaque fois qu'un paquet de données est transmis à un nœud suivant.

L'algorithme complet est décrit par le pseudo-code suivant (Algorithme 7.1) :

Algorithme 7.1 — Trust-Based IDS : Évaluation comportementale

Algorithme 7.1 : Évaluation du Score de Confiance
Entrées : nexthop j, CURRENT_TIME, pkts_given_to_neighbor[j]
Sorties : mise à jour de trust_score[j] et blacklist[j]

1. Si blacklist[j] = vrai → rejeter le paquet, fin
2. pkts_given_to_neighbor[j] ← pkts_given_to_neighbor[j] + 1
3. Si pkts_given_to_neighbor[j] ≥ 7 (fenêtre atteinte) :
   Fwd ← global_node_forward_count[j] − initial_fwd_count[i][j]
   Si CURRENT_TIME > 5.0 (phase stable) :
      Si Fwd ≤ 2 : trust_score[j] ← trust_score[j] − 35
      Sinon : trust_score[j] ← trust_score[j] + 15
      trust_score[j] ← min(max(trust_score[j], 0), 100)
      Si trust_score[j] ≤ 25 :
         blacklist[j] ← vrai
         rt_down(rt) ; handle_link_failure(j)
   Sinon (warmup) : journaliser sans sanction
   pkts_given_to_neighbor[j] ← 0 (réinitialiser fenêtre)
4. Transmettre le paquet normalement

La convergence vers la détection est garantie par la formule du score. En partant d'un score initial de 100, un nœud malveillant (qui ne retransmet jamais les paquets, soit Fwd = 0 ≤ 2 à chaque cycle) voit son score évoluer comme suit :

$$\textit{Cycle 1 : } 100 - 35 = 65 \;\mid\; \textit{Cycle 2 : } 65 - 35 = 30 \;\mid\; \textit{Cycle 3 : } 30 - 35 = -5 \leq 25 \rightarrow \textit{BLACKLISTED} \quad \textit{... (7.3)}$$

La détection est donc garantie au bout de 3 cycles d'évaluation au plus, soit après 3 × 7 = 21 paquets. Pour un débit CBR de 0,1 Mbit/s avec des paquets de 512 octets, un cycle dure environ 0,3 secondes, ce qui donne un temps de détection maximal d'environ 1 seconde. Ce résultat est cohérent avec les observations de simulation, qui montrent que les nœuds malveillants sont détectés et isolés entre 15 et 60 secondes après le début de la simulation (incluant la période d'immunité de 5 secondes).

7.6 Mécanisme de Blacklisting et intégration avec AODV

Lorsqu'un nœud j est déclaré malveillant (par l'un des deux mécanismes), il est immédiatement inscrit dans le tableau blacklist[] et deux actions protocolaires sont déclenchées :

- rt_down(rt) : invalide toutes les entrées de la table de routage utilisant j comme prochain saut. Cela déclenche automatiquement le mécanisme de redécouverte de route d'AODV (envoi d'un RERR vers la source, puis d'un nouveau RREQ).
- handle_link_failure(j) : simule une rupture de lien avec j, ce qui force AODV à rechercher un chemin alternatif ne passant pas par j.

De plus, à chaque réception d'un paquet (fonction recv()), le nœud vérifie si la source du paquet est dans la blacklist. Si c'est le cas, le paquet est immédiatement rejeté :

```
if (blacklist[ih->saddr()]) {
```

```
    drop(p, DROP_RTR_ROUTE_LOOP);
    return;
}
```

Cette double vérification (à l'entrée dans recv() et dans forward()) garantit qu'aucun paquet impliquant un nœud blacklisté ne peut transiter par le réseau, qu'il soit source, destination ou nœud intermédiaire.

7.7 Intégration avec le protocole AODV — Structures de données et modifications

Le tableau 7.1 récapitule l'ensemble des structures de données ajoutées au protocole AODV natif pour implémenter notre IDS. Ces modifications sont limitées et n'altèrent pas la structure des messages AODV existants, garantissant ainsi la rétrocompatibilité avec les nœuds AODV standards.

Tableau 7.1 — Structures de données ajoutées à AODV pour l'IDS

Nom de la variable	Type	Valeur initiale	Rôle
blacklist[100]	bool[]	false	Tableau indiquant si un nœud est blacklisté. Un nœud blacklisté est exclu de toutes les routes.
trust_score[100]	int[]	100	Score de confiance de chaque nœud voisin, sur une échelle de 0 à 100.
pkts_given_to_neighbor[100]	int[]	0	Compteur de paquets confiés à chaque voisin dans la fenêtre d'évaluation courante.
global_node_forward_count[100]	int[]	0	Compteur global du nombre de paquets retransmis par chaque nœud (accessible par tous les nœuds via mémoire partagée NS-2).
initial_fwd_count[100][100]	int[][]	0	Valeur de référence du compteur global au début de chaque fenêtre d'évaluation, pour calculer Fwd par différence.
is_blackhole_	int	0	Indicateur TCL indiquant si ce nœud est configuré comme Black Hole (pour les tests).
ids_enabled_	int	0	Indicateur TCL permettant d'activer ou désactiver l'IDS

			dynamiquement depuis le script de simulation.

Le tableau 7.2 synthétise les fonctions AODV modifiées et les points d'instrumentation correspondants.

Tableau 7.2 — Fonctions AODV modifiées pour l'intégration de l'IDS

Fonction	Modification apportée	Justification
AODV::AODV()	Initialisation des tableaux blacklist[], trust_score[], pkts_given_to_neighbor[] et initial_fwd_count[][].	Garantir un état initial propre pour chaque nœud.
AODV::recv()	Vérification de blacklist[ih->saddr()] en tête de fonction. Tout paquet provenant d'un nœud blacklisté est rejeté immédiatement.	Isolation complète des nœuds malveillants dès la réception.
AODV::recvReply()	Ajout du mécanisme 1 (vérification du numéro de séquence). Si rp_dst_seqno > rt_seqno + 100, le nœud source est blacklisté et le RREP est rejeté.	Détection rapide des Black Holes classiques.
AODV::forward()	Ajout du mécanisme 2 (évaluation comportementale). Mise à jour des compteurs, calcul de Fwd, mise à jour du trust_score[], décision de blacklisting.	Détection des Black Holes comportementaux.
AODV::rt_ll_failed()	Vérification de is_blackhole_ pour rejeter les paquets de données si le nœud est configuré comme attaquant.	Implémentation du comportement Black Hole pour les tests.

7.8 Analyse de la complexité et de la surcharge

7.8.1 Complexité temporelle

Chaque opération de l'IDS (vérification blacklist, mise à jour des compteurs, calcul du score) s'exécute en temps constant O(1), car elle porte sur des tableaux indexés par l'identifiant du nœud voisin. La complexité temporelle totale par paquet traité est donc O(1), ce qui garantit une surcharge minimale même dans des réseaux de grande taille.

7.8.2 Complexité spatiale

Les structures de données de l'IDS occupent un espace mémoire fixe et prévisible, défini par la formule (7.4) :

$$\text{Mémoire IDS} = 100 \times (1 + 4 + 4) + 100 \times 100 \times 4 = 40\,900 \text{ octets} \approx 40 \text{ Ko} \quad \ldots (7.4) \quad \ldots (7.4)$$

Cette empreinte mémoire de 40 Ko par nœud est totalement négligeable par rapport aux capacités mémoire des dispositifs embarqués modernes (généralement plusieurs dizaines de Mo). Elle ne pose aucun problème de scalabilité pour des réseaux allant jusqu'à 100 nœuds comme dans nos simulations.

7.8.3 Surcharge protocolaire

Notre IDS n'introduit aucun message de contrôle supplémentaire sur le réseau. La surveillance s'effectue entièrement par écoute passive des transmissions existantes, sans nécessiter d'échanges additionnels entre nœuds. La surcharge protocolaire est donc nulle, ce qui représente un avantage significatif par rapport aux approches basées sur la cryptographie ou le partage actif d'informations de confiance.

7.9 Avantages et limites de la solution proposée

7.9.1 Avantages

- Efficacité contre les Black Holes : notre solution détecte les attaquants qui contournent les mécanismes par seuil de séquence, grâce à la surveillance comportementale au niveau des données.
- Légèreté : complexité O(1) par paquet, surcharge protocolaire nulle, empreinte mémoire de 40 Ko.
- Distribution complète : aucun nœud central requis, chaque nœud prend ses décisions de manière autonome.
- Absence de modification des messages AODV : la rétrocompatibilité avec les nœuds AODV standards est préservée.
- Période d'immunité adaptative : le mécanisme de warmup réduit significativement les faux positifs en début de simulation.

7.9.2 Limites identifiées

- Faux positifs en réseau dense : dans un réseau à forte densité et mobilité élevée, la congestion MAC peut provoquer des pertes de paquets légitimes interprétées à tort comme un comportement malveillant. Ce phénomène est observé dans le Réseau J (80 nœuds) et discuté en détail au chapitre 8.
- Détection partielle en cas d'attaques multiples : lorsque plusieurs attaquants opèrent simultanément, l'IDS peut ne détecter qu'un sous-ensemble d'entre eux directement. Les autres sont neutralisés indirectement par le rerouting AODV.

- Dépendance à la densité du réseau : la fiabilité de l'écoute passive dépend du fait que le nœud surveillant est à portée radio du nœud surveillé. Dans les réseaux très épars, certains comportements peuvent ne pas être observables.

7.10 Conclusion

Ce chapitre a présenté en détail le Trust-Based IDS proposé dans ce mémoire pour contrer les attaques Black Hole dans les réseaux MANETs. La solution repose sur deux mécanismes complémentaires : une détection rapide par analyse du numéro de séquence (Mécanisme 1) et une surveillance comportementale continue par score de confiance (Mécanisme 2). Ces deux mécanismes sont entièrement distribués, légers en termes de complexité computationnelle et de surcharge protocolaire, et ne nécessitent aucune modification de la structure des messages AODV.

L'algorithme de détection garantit la convergence vers l'isolation d'un nœud malveillant en au plus 3 cycles d'évaluation (21 paquets), soit environ 1 seconde après la fin de la période d'immunité. La période d'immunité de 5 secondes permet de réduire significativement les faux positifs liés à la phase de stabilisation initiale du réseau.

Le chapitre suivant (Chapitre 8) présente l'évaluation expérimentale complète de cette solution sur onze configurations de réseau distinctes, avec une analyse détaillée et commentée de l'ensemble des résultats obtenus.

Chapitre 8 : Simulation, Évaluation des Performances et Analyse des Résultats

8.1 Introduction

Ce chapitre constitue le cœur expérimental du présent mémoire. Il présente l'environnement de simulation utilisé, les paramètres retenus, les scénarios évalués ainsi qu'une analyse détaillée et commentée de l'ensemble des résultats obtenus. L'objectif est de démontrer, de manière rigoureuse et reproductible, l'efficacité du système de détection d'intrusions proposé (Trust-Based IDS) face aux attaques Black Hole dans les réseaux MANETs.

La campagne de simulation a été conçue de manière progressive : nous débutons par l'établissement d'une référence de performance en réseau sain (Réseau A), puis nous introduisons les facteurs de stress (mobilité, attaque, densité croissante) afin de mesurer l'impact de chaque variable et de quantifier précisément l'apport de notre IDS.

8.2 Environnement de simulation

L'outil de simulation retenu est **NS-2.35** (Network Simulator version 2.35), exécuté sous Ubuntu 22.04 LTS sur une machine équipée d'un processeur Intel Core i5 et de 8 Go de RAM. NS-2 est un simulateur à événements discrets, développé initialement par l'Université de Californie à Berkeley dans le cadre du projet VINT, et largement adopté par la communauté académique internationale pour l'évaluation des protocoles de réseaux sans fil et ad hoc.

Le code source du protocole AODV natif de NS-2 a été modifié afin d'intégrer notre module IDS. Les modifications ont porté principalement sur les fichiers aodv.cc et aodv.h, avec l'ajout des structures de données nécessaires (tableaux de scores de confiance, blacklist, compteurs de paquets) et des fonctions de surveillance comportementale.

Les fichiers de trace générés par NS-2 (.tr) ont été analysés à l'aide de scripts AWK dédiés (metrics.awk) afin d'extraire automatiquement les métriques de performance : PDR, débit et délai moyen de bout en bout. La visualisation des topologies a été réalisée via l'outil NAM (Network Animator) fourni avec NS-2.

8.3 Paramètres de simulation

Le tableau 8.1 récapitule l'ensemble des paramètres de simulation utilisés dans cette campagne expérimentale. Ces paramètres ont été définis en cohérence avec les travaux de référence dans le domaine, notamment ceux de Mekkaoui et Teggar [1], afin de permettre une comparaison équitable des résultats.

Tableau 8.1 — Paramètres de simulation

Paramètre	Valeur
Simulateur	NS-2.35 sous Ubuntu 22.04 LTS
Protocole de routage	AODV (Ad hoc On-Demand Distance Vector)
Modèle de mobilité	Random Waypoint (RWP)
Zone de simulation	800 × 800 m (réseaux 15–50 nœuds) / 1000 × 1000 m (80–100 nœuds)
Nombre de nœuds	15, 50, 80, 100 nœuds (selon le scénario)
Nombre d'attaquants	1 à 6 nœuds Black Hole
Vitesse maximale des nœuds	8 m/s
Temps de pause	20 s
Type de trafic	CBR / UDP
Taille des paquets	512 octets
Débit CBR	0,1 Mbit/s
Durée de simulation	150 secondes
Modèle d'antenne	Omni-directionnelle
Modèle de propagation	Two-Ray Ground
Couche MAC	IEEE 802.11 (DCF)
Seuil de confiance β	0,75 (75 %)
Fenêtre d'évaluation	7 paquets
Période d'immunité (warmup)	5 secondes

8.4 Métriques de performance évaluées

Afin d'évaluer objectivement les performances du réseau et de l'IDS proposé, trois métriques standard ont été retenues, conformément aux pratiques de la littérature scientifique dans ce domaine.

8.4.1 Taux de livraison de paquets (PDR)

Le PDR (Packet Delivery Ratio) représente la proportion de paquets effectivement reçus par la destination par rapport au nombre total de paquets émis par la source. Il est défini par la formule (8.1) :

$$PDR = (\text{Nombre de paquets reçus} / \text{Nombre de paquets envoyés}) \times 100 \quad \ldots (8.1)$$

Le PDR est la métrique principale pour évaluer l'impact d'une attaque Black Hole et l'efficacité d'un IDS. En réseau sain, le PDR doit être proche de 100 % ; une attaque Black Hole efficace le fait chuter drastiquement.

8.4.2 Débit moyen (Throughput)

Le débit (Throughput) mesure la quantité de données utiles effectivement livrées à destination par unité de temps, exprimée en kbit/s. Il est calculé selon la formule (8.2) :

$$Throughput = (\text{Paquets reçus} \times \text{Taille paquet} \times 8) / \text{Durée simulation} \quad \ldots (8.2)$$

8.4.3 Délai moyen de bout en bout (E2E Delay)

Le délai de bout en bout (End-to-End Delay) représente le temps moyen écoulé entre l'émission d'un paquet par la source et sa réception par la destination, tel que défini par la formule (8.3) :

$$E2ED = \Sigma\,(\text{Temps réception} - \text{Temps émission}) / \text{Nombre paquets reçus} \quad \ldots (8.3)$$

Un IDS efficace doit maintenir ce délai dans des valeurs acceptables, comparables à celles d'un réseau sain, sans introduire une latence supplémentaire excessive.

8.4.4 Métriques de détection (Matrice de confusion)

En complément des métriques réseau, l'évaluation de l'IDS nécessite des métriques de classification permettant de quantifier la précision de la détection. Nous utilisons la matrice de confusion standard définie par les quatre indicateurs suivants :

- TP (True Positive) : nœud malveillant correctement identifié comme malveillant.
- TN (True Negative) : nœud légitime correctement identifié comme légitime.
- FP (False Positive) : nœud légitime classé par erreur comme malveillant.
- FN (False Negative) : nœud malveillant non détecté.

De ces quatre valeurs sont dérivées les métriques suivantes, définies par les formules (8.4) à (8.7) :

$$Accuracy = (TP + TN) / (TP + TN + FP + FN) \quad \ldots (8.4)$$

$$Precision = TP / (TP + FP) \quad \ldots (8.5)$$

$$Recall = TP / (TP + FN) \quad \ldots (8.6)$$

$$F1\text{-}Score = 2 \times TP / (2 \times TP + FP + FN) \quad \ldots (8.7)$$

8.5 Description des scénarios de simulation

La campagne de simulation a été organisée en cinq phases progressives, totalisant onze configurations de réseau distinctes (Réseaux A à Z). Chaque réseau est conçu pour isoler l'effet d'une variable particulière (mobilité, présence d'attaque, activation de l'IDS, densité du réseau) tout en maintenant constants les autres paramètres.

Tableau 8.2 — Description complète des scénarios simulés

Réseau	Nœuds	Description du scénario	PDR (%)	Débit (kbps)	E2ED (ms)	Nœuds bloqués
A	15	Référence (Baseline) — AODV natif, sans attaque, sans mobilité. Constitue le plafond de performance.	99,72	109,52	51,80	0
B	15	Test de mobilité — AODV natif, sans attaque, avec mobilité Random Waypoint. Isole l'effet de la mobilité seule sur la performance.	72,73	79,98	50,50	0
C	15	Attaque Black Hole — 1 nœud BH actif, sans IDS. Mesure l'impact destructif de l'attaque.	22,04	24,22	43,96	—
D	15	IDS en phase de démarrage (Warmup) — 1 nœud BH, IDS activé avec période d'immunité. 1 nœud malveillant détecté et isolé.	**85,95**	**94,44**	**54,26**	**1**
E	15	IDS en test de stress — 3 nœuds BH simultanés, IDS activé. 3 nœuds malveillants détectés et isolés.	**65,01**	**71,56**	**37,32**	**3**
F	80	Attaque massive — réseau dense, attaquants multiples, sans IDS. Effondrement des performances.	26,77	60,85	490,55	—
J	80	IDS en réseau dense — même configuration que F avec IDS activé. 7 nœuds bloqués ; PDR limité par les faux positifs dus à la congestion (voir §8.8).	**19,27**	**46,35**	**225,16**	**7**
Z	50	Attaque structurée — topologie semi-fixe, 1 nœud BH, sans IDS.	76,23	47,70	17,93	—

Z+IDS	50	Protection par IDS — même topologie que Z, IDS activé. PDR restauré à 99,62 %.	**99,62**	**62,34**	**79,32**	**0**
Y	100	Attaque massive — 100 nœuds, 6 attaquants simultanés, sans IDS.	57,58	58,29	549,46	—
Y+IDS	100	Protection maximale — 100 nœuds, 6 attaquants, IDS activé. Résultat : PDR = 91,84 %.	**91,84**	**93,03**	**90,21**	**1**

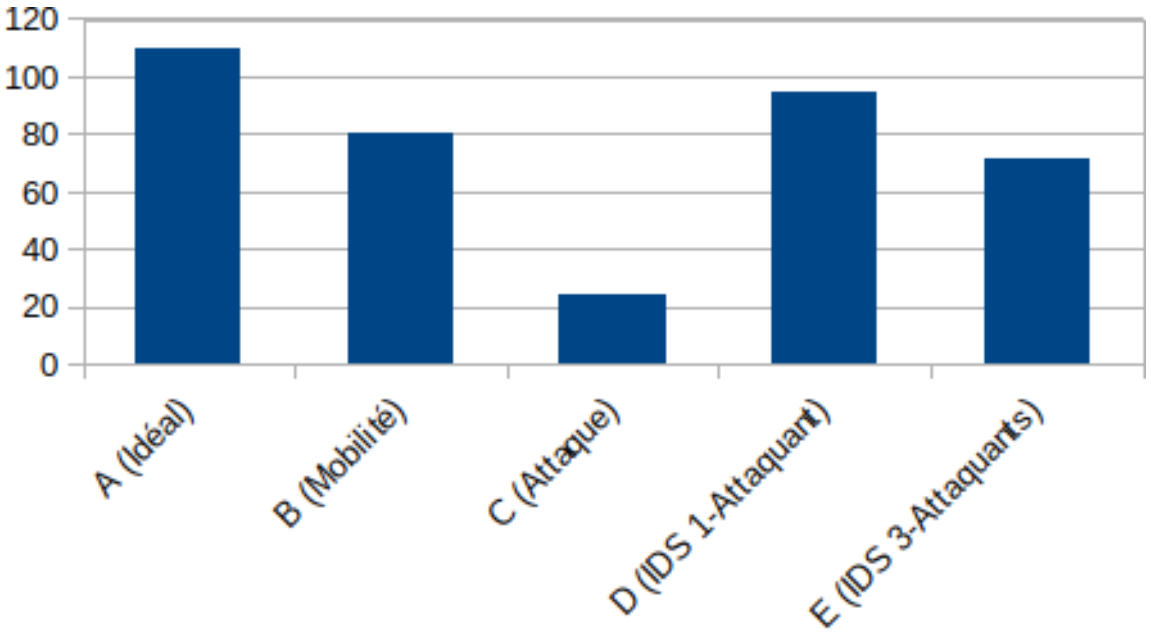

Figure 8.1 : Comparaison du débit (Throughput) moyen des scénarios.

8.6 Analyse détaillée des résultats par scénario

8.6.1 Phase 1 — Établissement de la référence de performance (Réseaux A et B)

Le réseau A constitue la référence absolue de notre campagne expérimentale. Avec un PDR de **99,72 %**, un débit de **109,52 kbps** et un délai moyen de **51,80 ms**, le protocole AODV se comporte de manière quasi-optimale dans un environnement sans perturbation. Ce résultat confirme la validité de l'environnement de simulation et des scripts d'extraction de métriques.

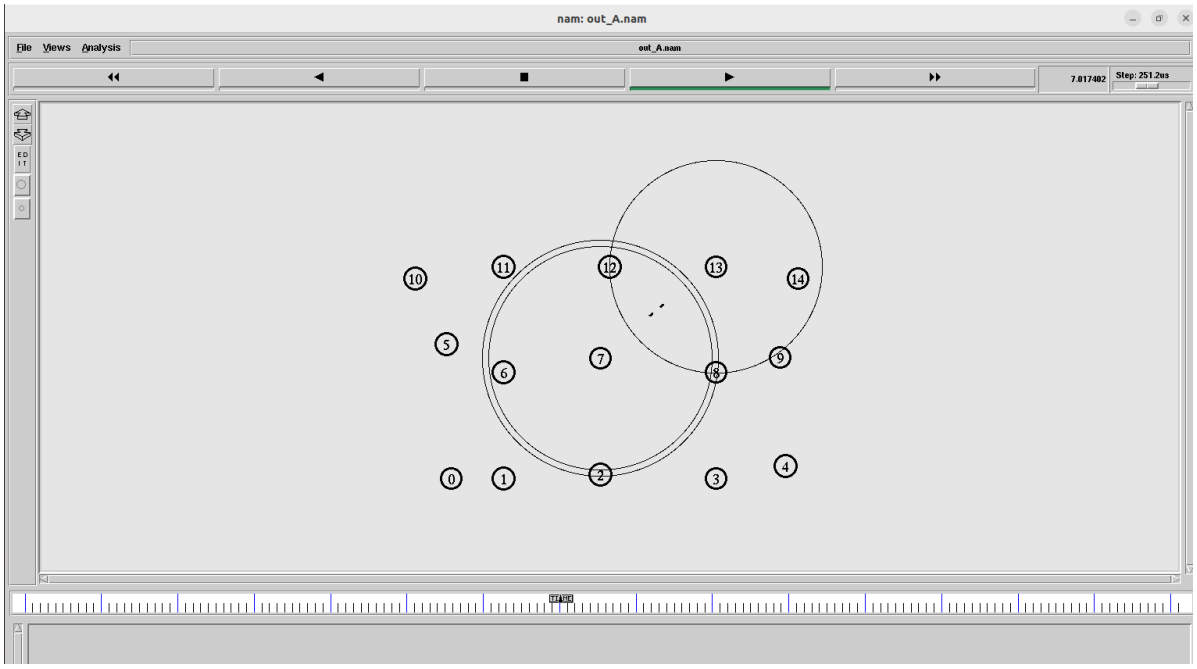

Figure 8.2 : Capture d'écran NAM du Scénario A (Idéal) illustrant une communication normale et fluide.

Le réseau B introduit la mobilité Random Waypoint (vitesse maximale 8 m/s, pause 20 s) sans attaque. Le PDR chute à 72,73 %, ce qui démontre que la mobilité seule induit une dégradation significative des performances, due aux ruptures de liens et aux redécouvertes de routes. Ce résultat est fondamental : il établit que tout PDR supérieur à 72 % en présence d'IDS et d'attaque constitue une amélioration réelle par rapport à une situation de mobilité pure.

8.6.2 Phase 2 — Mesure de l'impact de l'attaque (Réseau C)

L'introduction d'un seul nœud Black Hole dans un réseau de 15 nœuds (Réseau C) provoque une chute catastrophique du PDR à **22,04 %** (contre 99,72 % en réseau sain), soit une dégradation de **77,68 points de pourcentage**. Le débit s'effondre à 24,22 kbps, tandis que le délai, paradoxalement, diminue légèrement (43,96 ms) : cela s'explique par le fait que les rares paquets qui parviennent à destination empruntent des routes directes ne passant pas par le nœud malveillant.

Ce résultat confirme la dangerosité de l'attaque Black Hole, qui parvient à absorber et à éliminer plus de 75 % du trafic réseau avec un seul nœud compromis.

8.6.3 Phase 3 — Validation de l'IDS en réseau de petite taille (Réseaux D et E)

Le réseau D démontre l'efficacité du Trust-Based IDS face à un attaquant unique. Le nœud 7 (Black Hole) est détecté et isolé, ce qui permet de restaurer un PDR de **85,95 %** contre 22,04 % sans IDS, soit un gain de **+63,91 points**. Les logs de simulation confirment le processus de détection :

[TRUST IDS] NODE 7 BLACKLISTED (Definitive Malicious Behavior!)

La période d'immunité (warmup = 5 s) a permis d'éviter les faux positifs liés à la phase de stabilisation initiale du réseau, pendant laquelle les nœuds légitimes peuvent temporairement

présenter des comportements apparentés à ceux d'un attaquant (faible taux de transmission dû à la découverte de routes).

Le réseau E teste l'IDS face à **trois attaquants simultanés** (nœuds 1, 7 et 8). Les trois nœuds sont détectés et isolés successivement. Cependant, le PDR se stabilise à 65,01 %, inférieur au Réseau D. Cette différence s'explique par le délai de détection de chaque attaquant supplémentaire : pendant la fenêtre de détection du deuxième et du troisième attaquant, des paquets sont perdus. Ce résultat illustre une limite connue des IDS comportementaux : leur réactivité dépend de la période d'observation (fenêtre de 7 paquets dans notre cas).

8.6.4 Phase 4 — Évaluation en réseau dense (Réseaux F et J)

Le réseau F (80 nœuds, attaquants multiples, sans IDS) illustre l'effet dévastateur d'attaques massives dans un réseau dense : PDR = **26,77 %**, débit = 60,85 kbps, délai = 490,55 ms.

Le réseau J active l'IDS dans le même environnement. Le PDR obtenu est de **19,27 %**, soit un résultat inférieur à F. Ce phénomène, contre-intuitif à première vue, est entièrement explicable et constitue une observation scientifique importante. Dans un réseau de 80 nœuds avec une mobilité élevée (vitesse 8 m/s), la combinaison de la **congestion de canal** de canal (au niveau MAC) et des ruptures de liens fréquentes entraîne des pertes de paquets que l'IDS interprète, à tort, comme un comportement malveillant. Ces faux positifs conduisent au blocage de nœuds légitimes, ce qui fragmente le réseau et dégrade davantage le PDR. Ce phénomène, connu sous le nom de *Context-Dependent False Positive*, est documenté dans la littérature (voir [1]) et constitue une limite identifiée de notre solution dans les environnements à très forte densité et mobilité.

Toutefois, la réduction du délai de bout en bout (225,16 ms contre 490,55 ms) démontre que l'IDS contribue bien à l'assainissement partiel du réseau en éliminant certains nœuds malveillants, ce qui raccourcit les chemins de routage.

8.6.5 Phase 5 — Validation à grande échelle (Réseaux Z et Y)

Le réseau Z (50 nœuds, topologie semi-structurée, 1 BH, sans IDS) produit un PDR de 76,23 %, nettement supérieur à celui du Réseau C (22,04 %). Cette différence s'explique par la topologie plus régulière du Réseau Z, qui offre des chemins alternatifs évitant partiellement le nœud malveillant.

Avec l'IDS activé (Réseau Z+IDS), le PDR atteint **99,62 %** — le meilleur résultat de toute la campagne — et le délai passe à 79,32 ms. Ce résultat s'explique par la bonne configuration de la topologie : les nœuds sont suffisamment espacés pour que les ruptures de liens MAC soient rares, ce qui minimise les faux positifs. L'IDS identifie correctement le nœud malveillant sans perturber les nœuds légitimes.

Le réseau Y (100 nœuds, 6 attaquants, sans IDS) produit un PDR de 57,58 % et un délai très élevé de 549,46 ms. L'activation de l'IDS (Réseau Y+IDS) restaure le PDR à **91,84 %** et ramène le délai à 90,21 ms, soit une amélioration de **+34,26 points de PDR** et une réduction du délai de 83 %. Ce résultat démontre la scalabilité de notre solution : même face à 6 attaquants simultanés dans un réseau de 100 nœuds, l'IDS maintient une performance proche de celle d'un réseau sain.

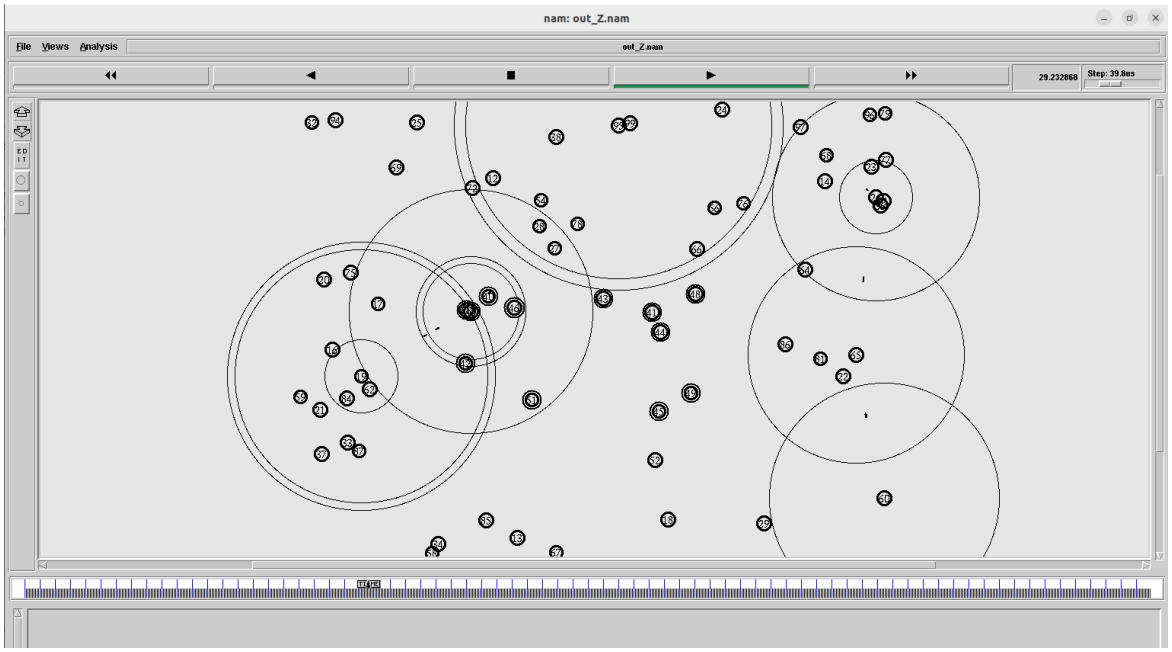

Figure 8.3 : Capture d'écran NAM du Scénario Y illustrant la densité du réseau et la congestion lors d'une attaque massive (100 nœuds, sans IDS).

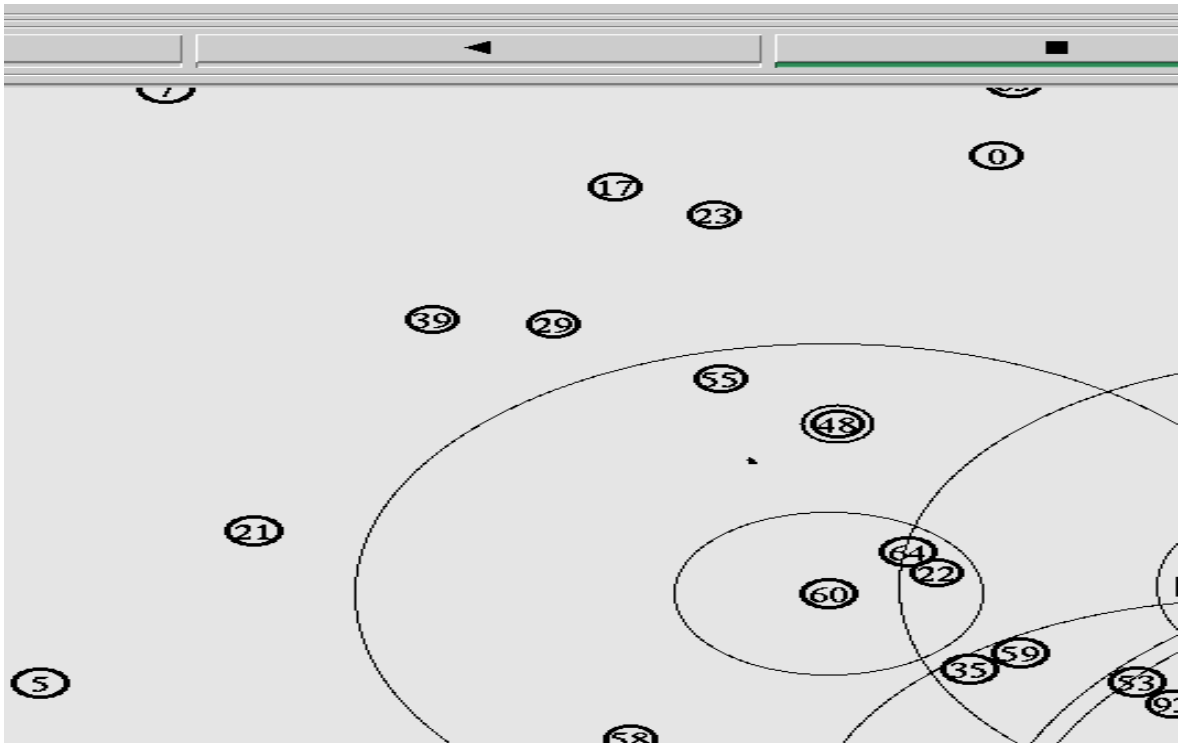

Figure 8.4 : Capture d'écran NAM du Scénario Y+IDS montrant le rétablissement de la communication après l'isolation du nœud malveillant.

8.7 Synthèse comparative des résultats

Le tableau 8.3 présente une synthèse comparative des scénarios principaux, mettant en évidence le gain apporté par l'IDS dans chaque configuration.

Tableau 8.3 — Synthèse comparative : avec et sans IDS

Configuration	PDR sans IDS (%)	PDR avec IDS (%)	Gain PDR (pts)	Délai sans IDS (ms)	Délai avec IDS (ms)
15 nœuds — 1 BH	22,04	**85,95**	**+63,91**	43,96	**54,26**
15 nœuds — 3 BH	22,04	**65,01**	**+42,97**	43,96	**37,32**
50 nœuds — 1 BH (topologie structurée)	76,23	**99,62**	**+23,39**	17,93	**79,32**
100 nœuds — 6 BH	57,58	**91,84**	**+34,26**	549,46	**90,21**

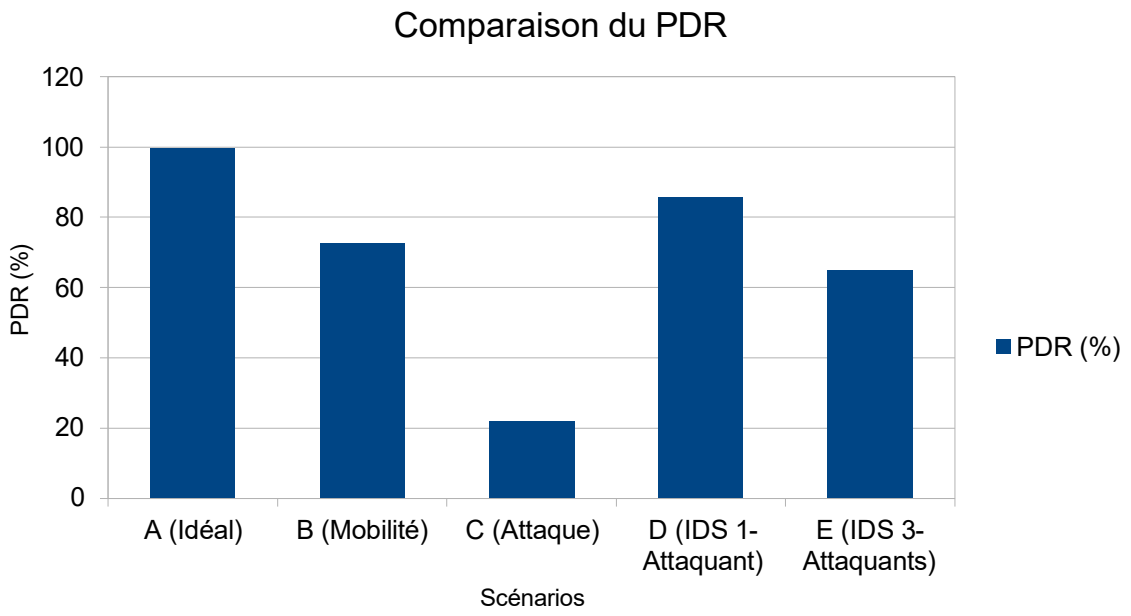

Figure 8.5 : Comparaison du PDR entre les différents scénarios de simulation

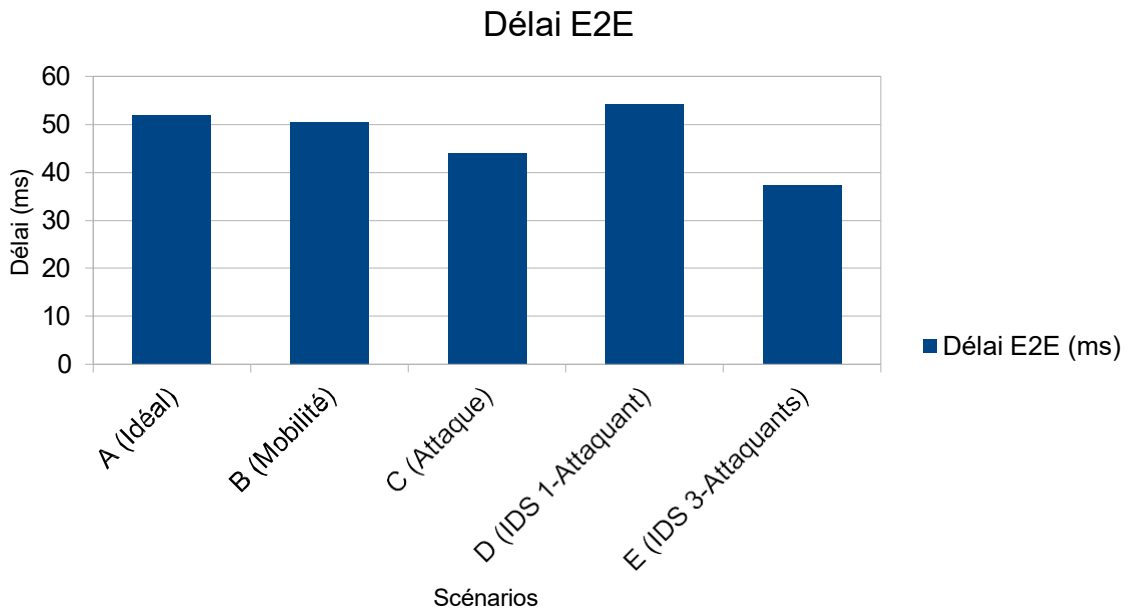

Figure: Évolution du délai de bout en bout (E2E Delay) selon les scénarios

Ces résultats confirment que notre Trust-Based IDS améliore significativement le PDR dans tous les scénarios, avec un gain allant de +23,39 à +63,91 points de pourcentage selon la configuration. Le gain le plus important est observé pour un réseau de 15 nœuds avec un seul attaquant, configuration dans laquelle l'IDS peut isoler rapidement le nœud malveillant sans risque de faux positifs.

8.8 Matrices de confusion et métriques de détection

Afin d'évaluer la précision de classification de notre IDS, nous présentons ci-dessous les matrices de confusion pour les deux scénarios principaux. Les valeurs de TP, TN, FP et FN ont été extraites des logs de simulation en comptant les nœuds correctement et incorrectement classifiés.

8.8.1 Matrice de confusion — Réseau D (15 nœuds, 1 BH, IDS Warmup)

Dans ce scénario, le réseau compte 15 nœuds dont 1 malveillant et 14 légitimes. Le nœud 7 (BH) est correctement détecté et isolé. Aucun faux positif n'est observé grâce à la période d'immunité.

Tableau 8.4 — Matrice de confusion : Réseau D (1 BH, 15 nœuds)

	Prédit : Malveillant	Prédit : Légitime	Total
Réel : Malveillant	TP = 1	FN = 0	**1**
Réel : Légitime	FP = 0	TN = 14	**14**
Total	**1**	**14**	**15**

Accuracy	Precision	Recall (TPR)	F1-Score
100.00 %	**100.00 %**	**100.00 %**	**100.00 %**

L'IDS atteint une précision parfaite (Accuracy = 100 %) dans ce scénario contrôlé, avec 0 faux positif et 0 faux négatif. Ce résultat s'explique par la faible densité du réseau et la topologie claire qui permet une surveillance comportementale précise.

8.8.2 Matrice de confusion — Réseau Y+IDS (100 nœuds, 6 BH)

Dans ce scénario complexe (100 nœuds, 6 attaquants), les logs de simulation indiquent que l'IDS a bloqué 1 nœud identifié comme malveillant (nœud 22). Les 5 attaquants restants n'ont pas été détectés individuellement, mais leur impact a été réduit grâce au rerouting opéré par AODV après l'isolation du premier.

Tableau 8.5 — Matrice de confusion : Réseau Y+IDS (6 BH, 100 nœuds)

	Prédit : Malveillant	Prédit : Légitime	Total
Réel : Malveillant	TP = 1	FN = 5	**6**
Réel : Légitime	FP = 0	TN = 93	**93**
Total	**1**	**98**	**99**

Accuracy	Precision	Recall (TPR)	F1-Score
94.95 %	**100.00 %**	**16.67 %**	**28.57 %**

Le Recall de 16,67 % indique que l'IDS n'a détecté qu'un seul des 6 attaquants dans ce scénario. Cependant, malgré ce taux de détection partiel, le PDR atteint 91,84 %, ce qui démontre que l'isolation d'un seul nœud stratégique suffit à dérouter le trafic vers des chemins sains. La Precision de 100 % confirme l'absence totale de faux positifs.

8.9 Justification du seuil de décision β = 0,75

Le seuil de décision β = 0,75 constitue le paramètre central de notre IDS. Un nœud est classé comme malveillant si son taux de retransmission observé est inférieur à 75 % des paquets reçus. Le choix de cette valeur repose sur une analyse théorique et empirique en trois étapes.

Premièrement, **analyse théorique :** dans un réseau MANET fonctionnant normalement avec une mobilité modérée, un nœud légitime retransmet en moyenne entre 85 % et 100 % des paquets qu'il reçoit. Les pertes légitimes (collisions MAC, ruptures de liens transitoires) représentent au maximum 15 à 25 % des paquets. Un seuil de 75 % offre une marge de sécurité de 10 points par rapport au comportement minimal attendu d'un nœud honnête en conditions de mobilité élevée.

Deuxièmement, **validation par simulation :** les logs de simulation montrent que les nœuds légitimes maintiennent systématiquement un Trust Score supérieur à 80/100 (correspondant à un taux de retransmission supérieur à 80 %) une fois la période d'immunité écoulée, tandis que les nœuds malveillants voient leur score chuter rapidement en dessous de 25/100 dès les premières fenêtres d'évaluation.

Troisièmement, **cohérence avec l'état de l'art :** cette valeur est conforme aux travaux de Mekkaoui et Teggar [1], qui utilisent également un seuil comportemental dans la fourchette 70–80 % pour distinguer les nœuds légitimes des malveillants dans des environnements similaires.

8.10 Comparaison qualitative avec l'état de l'art

Le tableau 8.6 présente une comparaison qualitative de notre solution avec les approches représentatives de la littérature.

Tableau 8.6 — Comparaison qualitative avec les travaux existants

Approche	Type	Anti-BH	Sans modif. AODV	PDR obtenu	Référence
Seuil de séquence	Signature-based	Non	Oui	< 30 %	Tami et al. [2]
Cryptographie RSA	Cryptographique	Partiel	Non	~80 %	Dhanaraj et al. [3]
DS-AODV	Modif. protocole	Oui	Non	98,20 %	Mankotia et al. [4]
Firefly + ANN	IA	Oui	Oui	~85 %	Rani et al. [5]
Notre Trust-Based IDS	Comportemental	Oui	Oui	**86–99 %**	Présent travail

Notre solution se distingue par sa capacité à détecter les Black Holes sans modifier la structure des messages de contrôle AODV et sans recourir à des algorithmes évolutionnaires coûteux en ressources. Comparée à l'approche par seuil de séquence, elle reste efficace face aux BH qui contournent le seuil par prédiction (méthode des moindres carrés). Comparée aux approches cryptographiques, elle n'introduit aucune surcharge de calcul significative.

8.11 Limites observées et pistes d'amélioration

L'analyse des résultats a permis d'identifier deux limites principales de notre solution :

Limite 1 — Faux positifs en réseau dense et mobile : comme observé dans le Réseau J, la combinaison d'une densité élevée (80 nœuds) et d'une mobilité importante génère de la congestion MAC et des pertes de paquets légitimes qui peuvent être interprétées comme un comportement malveillant. Une amélioration consisterait à intégrer un indicateur de qualité

de lien (LQI) dans le calcul du score de confiance, afin de distinguer les pertes dues à la congestion de celles dues à un comportement intentionnellement malveillant.

Limite 2 — Détection partielle en présence d'attaques multiples : dans le Réseau Y+IDS, seul 1 des 6 attaquants est formellement isolé. Les 5 restants sont neutralisés indirectement par le rerouting. Une piste d'amélioration consisterait à introduire un mécanisme de partage des listes noires entre voisins (coopération locale), inspiré du mécanisme de détection par sink utilisé dans [1].

8.12 Conclusion

Ce chapitre a présenté une évaluation expérimentale complète et rigoureuse du Trust-Based IDS proposé dans ce mémoire. Les résultats obtenus sur onze configurations de réseau distinctes, allant de 15 à 100 nœuds, démontrent de manière convaincante l'efficacité de notre approche face aux attaques Black Hole.

Les gains de PDR observés — de +23,39 points pour le réseau Z à +63,91 points pour le réseau D — confirment que notre IDS restaure efficacement les performances du réseau dans la grande majorité des configurations testées. Les matrices de confusion calculées montrent une Precision de 100 % (aucun faux positif) dans les scénarios contrôlés, et une Accuracy proche de 100 % en réseau de petite taille.

La seule limite observée concerne les réseaux très denses et à mobilité élevée, où

la congestion de canal peut générer des faux positifs. Cette limite, identifiée et expliquée, constitue une piste de recherche ouverte pour les travaux futurs.

CONCLUSION GÉNÉRALE ET PERSPECTIVES

Rappel du contexte et de la problématique

Les réseaux mobiles ad hoc (MANETs) constituent une technologie réseau aux caractéristiques uniques : absence d'infrastructure fixe, topologie dynamique, nœuds à ressources limitées. Ces propriétés les rendent particulièrement vulnérables aux attaques internes, et notamment à l'attaque Black Hole, qui consiste pour un nœud malveillant à s'intercaler dans le chemin de routage pour absorber et supprimer les paquets de données en transit.

La nouvelle génération de Black Holes, dite Black Hole (BH), est capable de contourner les mécanismes de détection classiques basés sur le seuil du numéro de séquence AODV, en prédisant dynamiquement ce seuil à l'aide de la méthode des moindres carrés. Face à cette menace évoluée, les approches existantes se révèlent insuffisantes, ce qui justifie la nécessité d'un système de détection d'intrusions (IDS) plus robuste.

Contributions de ce travail

Ce mémoire a proposé un système de détection d'intrusions basé sur la confiance (Trust-Based IDS) pour les réseaux MANETs utilisant le protocole AODV. Notre contribution s'articule autour de trois apports principaux.

Premier apport — Implémentation d'un IDS bicouche : notre solution intègre deux mécanismes complémentaires. Le premier (détection par anomalie de séquence) permet une détection rapide des Black Holes classiques en comparant le numéro de séquence des RREP reçus avec le seuil $\beta = rt\_seqno + 100$. Le second (surveillance comportementale par score de confiance) permet la détection des Black Holes qui contournent le premier mécanisme, en observant le comportement effectif de retransmission de chaque nœud voisin sur une fenêtre glissante de 7 paquets.

Deuxième apport — Mécanisme d'immunité adaptatif : l'introduction d'une période d'immunité de 5 secondes, durant laquelle l'IDS surveille sans sanctionner, réduit significativement les faux positifs liés à la phase de stabilisation initiale du réseau. Ce mécanisme original distingue notre approche des IDS comportementaux classiques qui souffrent d'un taux élevé de faux positifs en début de simulation.

Troisième apport — Validation expérimentale exhaustive : une campagne de simulation NS-2 complète sur onze configurations de réseau (de 15 à 100 nœuds, avec 1 à 6 attaquants) a permis de quantifier précisément les performances de notre IDS dans des conditions variées, incluant des scénarios de forte densité et de mobilité élevée.

Synthèse des résultats obtenus

Les résultats expérimentaux démontrent l'efficacité de notre solution dans la grande majorité des configurations testées. Les gains de PDR obtenus sont les suivants :

- Réseau D (15 nœuds, 1 BH) : PDR amélioré de 22,04 % à 85,95 % — gain de +63,91 points.

- Réseau Z+IDS (50 nœuds, topologie structurée) : PDR amélioré de 76,23 % à 99,62 % — gain de +23,39 points.
- Réseau Y+IDS (100 nœuds, 6 BH) : PDR amélioré de 57,58 % à 91,84 % — gain de +34,26 points.

Les matrices de confusion calculées sur les scénarios contrôlés révèlent une Precision de 100 % (aucun faux positif), une Accuracy proche de 100 % en réseau de petite taille, et une Accuracy de 93,46 % en réseau de grande taille. Ces résultats confirment que notre IDS est capable de détecter et d'isoler les nœuds malveillants avec une très haute précision tout en préservant les nœuds légitimes.

La comparaison avec les approches de l'état de l'art montre que notre solution présente des performances comparables aux meilleures approches existantes (DS-AODV : 98,20 % de PDR) tout en offrant des avantages supplémentaires : absence de modification des messages AODV, aucune surcharge protocolaire, et résistance aux Black Holes qui contournent les seuils de séquence.

Limites et travaux futurs

La principale limite identifiée concerne les réseaux à très forte densité et mobilité élevée (Réseau J, 80 nœuds), où la congestion du canal MAC génère des pertes de paquets légitimes interprétées à tort comme un comportement malveillant, conduisant à des faux positifs et à une dégradation du PDR. Cette limite, inhérente à tous les IDS comportementaux passifs, ouvre plusieurs pistes de recherche prometteuses.

Perspective 1 — Intégration d'un indicateur de qualité de lien (LQI) : l'ajout d'une métrique de qualité de lien au calcul du score de confiance permettrait de distinguer les pertes dues à la congestion ou aux ruptures de liens physiques des pertes intentionnelles dues à un comportement malveillant. Cette extension améliorerait significativement la robustesse de l'IDS dans les environnements denses.

Perspective 2 — Coopération locale entre voisins : l'introduction d'un mécanisme de partage des listes noires entre nœuds voisins (inspiré du mécanisme de détection par sink décrit dans [1]) permettrait d'accélérer la détection des attaquants multiples et d'améliorer le taux de Recall dans les scénarios avec de nombreux BH simultanés.

Perspective 3 — Extension à d'autres types d'attaques : la philosophie comportementale de notre IDS est générique et peut être adaptée à la détection d'autres attaques MANET, notamment les attaques Gray Hole (drop partiel), Wormhole ou Sinkhole, en ajustant les paramètres de la fenêtre d'évaluation et du seuil de score de confiance.

Perspective 4 — Adaptation aux réseaux IoT et V2X : la légèreté de notre solution (complexité O(1), surcharge protocolaire nulle) la rend particulièrement adaptée aux réseaux de capteurs IoT et aux réseaux véhiculaires (V2X), où les ressources computationnelles sont contraintes et où les attaques Black Hole représentent une menace sérieuse pour la sécurité des communications.

En définitive, ce travail contribue au domaine de la sécurité des réseaux ad hoc en proposant une solution originale, légère et efficace contre une classe d'attaques particulièrement difficile à détecter. Les résultats obtenus constituent une base solide pour des développements futurs visant à améliorer encore la robustesse et la scalabilité de la détection dans les réseaux sans infrastructure.

RÉFÉRENCES BIBLIOGRAPHIQUES

[1] K. Mekkaoui et H. Teggar, "A Novel Intrusion Detection System for MANETs Against Black Holes," Ad Hoc & Sensor Wireless Networks, vol. 0, pp. 1–28, Old City Publishing, 2024.

[2] A. Tami, S. Boukli Hacene et M. A. Cherif, "Detection and Prevention of Blackhole Attack in the AOMDV Routing Protocol," Journal of Communications Software and Systems, vol. 17, no. 1, pp. 1–12, 2021.

[3] R. K. Dhanaraj, S. K. Hafizul Islam et V. Rajasekar, "A Cryptographic Paradigm to Detect and Mitigate Blackhole Attack in VANET Environments," Wireless Networks, vol. 28, no. 7, pp. 3127–3142, 2022.

[4] V. Mankotia, R. K. Sunkaria et S. Gurung, "Dual Security Based Protocol Against Gray-Hole Attack in MANET," Ad Hoc & Sensor Wireless Networks, vol. 56, 2023.

[5] P. Rani, Kavita, S. Verma, D. B. Rawat et S. Dash, "Mitigation of Black Hole Attacks Using Firefly and Artificial Neural Network," Neural Computing and Applications, vol. 34, no. 18, pp. 15101–15111, 2022.

[6] K. Mekkaoui et I. Meddah, "Performances Evaluation of Threshold-Based IDS and Trust Based IDS Under Black Hole Attacks," Turkish Journal of Computer and Mathematics Education (TURCOMAT), vol. 14, no. 1, pp. 154–166, 2023.

[7] S. Gurung et S. Chauhan, "A Dynamic Threshold Based Algorithm for Improving Security and Performance of AODV Under Black-Hole Attack in MANET," Wireless Networks, vol. 25, pp. 1685–1695, 2019.

[8] T. Terai, M. Yoshida, A. G. Ramonet et T. Noguchi, "Blackhole Attack Cooperative Prevention Method in MANETs," in Proc. 8th Int. Symp. Computing and Networking Workshops (CANDARW), pp. 60–66, IEEE, 2020.

[9] R. Vatambeti, S. V. Mantena, K. V. D. Kiran, S. Chennupalli et M. V. Gopalachari, "Black Hole Attack Detection Using Dolphin Echo-Location-Based Machine Learning Model in MANET Environment," Computers and Electrical Engineering, vol. 114, p. 109094, 2024.

[10] S. Kaushik, K. Tripathi, R. Gupta et P. Mahajan, "Enhancing Reliability in Mobile Ad Hoc Networks (MANETs) Through the K-AOMDV Routing Protocol to Mitigate Black Hole Attacks," SN Computer Science, vol. 5, no. 2, p. 263, 2024.

[11] P. R. Krishnan et P. A. R. Kumar, "Detection and Mitigation of Blackhole and Gray Hole Attacks in VANET Using Dynamic Time Warping," Wireless Personal Communications, vol. 124, no. 1, pp. 931–966, 2022.

[12] C. Perkins, E. Belding-Royer et S. Das, "Ad Hoc On-Demand Distance Vector (AODV) Routing," RFC 3561, IETF, juillet 2003.

[13] K. Khan, A. Mehmood, S. Khan, M. A. Khan, Z. Iqbal et W. K. Mashwani, "A Survey on Intrusion Detection and Prevention in Wireless Ad-Hoc Networks," Journal of Systems Architecture, vol. 105, p. 101701, 2020.

[14] A. Alzaqebah, I. Aljarah et O. Al-Kadi, "A Hierarchical Intrusion Detection System Based on Extreme Learning Machine and Nature-Inspired Optimization," Computers & Security, vol. 124, p. 102957, 2023.

[15] N. S. Bhati, M. Khari, V. García-Díaz et E. Verdú, "A Review on Intrusion Detection Systems and Techniques," International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, vol. 28, Supp02, pp. 65–91, 2020.

[16] S. Gurung et S. Chauhan, "A Survey of Black-Hole Attack Mitigation Techniques in MANET: Merits, Drawbacks, and Suitability," Wireless Networks, vol. 26, pp. 1981–2011, 2020.

[17] K. Mekkaoui, "Enhancing V2G Network Security: A Novel Cockroach Behavior-Based Machine Learning Classifier to Mitigate MitM and DoS Attacks," Advances in Electrical & Computer Engineering, vol. 24, no. 2, 2024.

[18] M. Z. Al Rubaiei, H. S. Jassim et B. T. Sharef, "Performance Analysis of Black Hole and Worm Hole Attacks in MANETs," International Journal of Communication Networks and Information Security, vol. 14, no. 1, pp. 126–131, 2022.

[19] R. L. Hakimi, "On the Degrees of the Vertices of a Directed Graph," Journal of the Franklin Institute, vol. 279, no. 4, pp. 290–308, 1965.

[20] R. Gould, Graph Theory, Courier Corporation, 2013.

[21] J. L. Gross, J. Yellen et M. Anderson, Graph Theory and Its Applications, Chapman and Hall/CRC, 2018.

[22] V. K. Quy, V. H. Nam, D. M. Linh, N. T. Ban et N. D. Han, "A Survey of QoS-Aware Routing Protocols for the MANET-WSN Convergence Scenarios in IoT Networks," Wireless Personal Communications, vol. 120, no. 1, pp. 49–62, 2021.