الجمهوريــة الجزائريــة الديمقراطيــة الشعبيــة

République Algérienne Démocratique et Populaire

و البحث العلمي وزارة التعليم العالي

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université MUSTAPHA Stambouli

Mascara

جامعة مصطفى اسطمبولي

معسكر

Faculté des Sciences Exactes

Département d'Informatique

THESE de DOCTORAT EN SCIENCE

Spécialité : Informatique

Intitulée

Développement d'un système de détection d'intrusion dans les réseaux mobiles

Présentée par **: KHALLADI Rachid**

Le 13/07/2022

Devant le jury :

Président	**Debakla Mohammed**	**MCA**	**Université de Mascara**
Examinateur	**Louazani Ahmed**	**MCA**	**Université de Relizane**
Examinateur	**Mekkaoui Kheireddine**	**MCA**	**Université de Saida**
Examinateur	**Benyahia Kada**	**MCA**	**Université de Saida**
Encadrant	**Rebbah Mohammed**	**MCA**	**Université de Mascara**
Co-Encadrant	**Smail Omar**	**MCA**	**Université de Mascara**

Année Universitaire : 2021-2022

REMERCIEMENTS

Je remercie Dieu le tout puissant de nous avoir donné la santé et la volonté d'entamer et de terminer cette thèse de doctorat.

Tout d'abord, ce travail ne serait pas aussi riche et n'aurait pas pu voir le jour sans l'aide et l'encadrement de Dr.REBBAH Mohammed et Dr.Smail Omar, je les remercie pour la qualité de leurs encadrement exceptionnel, pour leurs patience, rigueur et leurs disponibilité durant notre préparation de cette thèse.

Je suis trés conscient de l'honneur que m'on fait Dr.Debakla Mohammed en étant président du jury, Dr Louazani Ahmed, Dr.Mekkaoui Kheireiddine, Dr.Benyahia Kada d'avoir accepté d'examiner ce travail.

Mes remerciements s'adressent également à tous mes professeurs pour leurs générosités et la grande patience dont ils ont su faire preuve malgré leurs charges académiques et professionnelles.

DÉDICACE

Je dédie ce travail :

À mes chers parents qui n'ont jamais cessé de me supporter, me soutenir et m'encourager durant mes années d'études.

Qu'ils trouvent ici le témoignage de ma profonde gratitude et reconnaissance.

À ma chère femmes qui m'a toujours soutenu et encouragé durant les moments les plus difficiles.

À ma petite fille Fatima Zohra (Fatoum) et mon petit Mohammed AbdelDjalil (Djalilou).

À mes frères Fethi , Bachir et Ben Ameur.

À mes chers Amis : Mohammed, Djamel, Samir, Ibrahim, Youcef, Miloud et tous mes collegues du Département infirmatique

À tous ceux qui m'ont aidé - de près ou de loin - et ceux qui ont partagé avec moi les moments d'émotion lors de la réalisation de ce travail et qui m'ont chaleureusement supporté et encouragé tout au long de mon parcours.

À mes encadreurs Mohammed Rebbah et Omar Smail pour leurs conseils et soutien

Merci !

-KHALLADI Rachid

RÉSUMÉ

Les réseaux mobiles ad hoc (MANET) sont des réseaux sans infrastructure. La portée de communication entre les nœuds est limitée, où plusieurs sauts sont nécessaires pour transmettre un paquet de la source à la destination. Ces réseaux ont une topologie en constante évolution en raison de ses nœuds mobiles et de leurs connexions arbitraires, ce qui le rend vulnérable à différentes attaques. L'une des attaques les plus importantes de MANET est l'attaque par trou noir qui dégrade les performances du réseau en supprimant tous les paquets qui le traversent. Il existe plusieurs techniques pour détecter les attaques par trou noir dans le protocole vectoriel ad hoc à la demande.

Dans cette thèse, une nouvelle approche basée sur AACK Adaptative ACKnowledgement est proposée. Le système proposé consiste à détecter les attaques de trous noirs simples et multiples par un système de détection d'intrusion avec la technique SPlitted AACK. Le système est suffisamment robuste pour détecter toutes les attaques par trou noir en utilisant une division itérative du chemin principal jusqu'à la détection des nœuds malveillants. NS2 est utilisé pour la simulation. Nous avons testé notre système sur différents réseaux avec différentes tailles de réseau et différents nombres d'attaques, et nous avons comparé nos résultats avec certaines techniques de système de détection d'intrusion existantes. Une technique basée sur l'apprentissage automatique, plus précisément sur l'algorithme de forêt aléatoire avec sélection des meilleures caractéristiques, est également proposée. Cette dernière est testé sur le jeu de données NSL-KDD. Les résultats trouvés étaient très satisfaisants en termes d'exactitude 99,66%, Précision 99,85%, Rappel 99,83% et F1-Score 99,84%. Ainsi, les résultats se sont améliorés par rapport à ceux des autres techniques

Mots cles : MANET, AODV, Trou noir, Nœuds malveillants, Attaques multiples, SPlitted AACK, Apprentissage automatique, Détection d'intrusion, NSL-KDD, Forêt aléatoire, Sélection des meilleures caractéristiques.

ABSTRACT

Mobile Ad hoc NETworks (MANET) are networks without infrastructure. The communication range among nodes is limited, where several hops are needed to transmit a packet from the source to the destination. These networks have a constantly changing topology due to its mobile nodes and their arbitrary connections, which make it vulnerable for diferent attacks. One of the most important attacks in MANET is the black hole attack which degrades the performance of the network by removing all the packets passing through it.

There are several techniques for detecting black hole attacks in the ad hoc on demand vector protocol. In this thesis, a new approach based on AACK Adaptative ACKnowledgement is proposed. The proposed system is to detect the single and multiple black hole attacks by intrusion detection system with SPlitted AACK technique. The system is robust enough to detect all black hole attacks by using an iterative split of the main path until the detection of the malicious nodes. Network simulator 2 (NS2) is used for simulation. We tested our system on diferent networks with diferent network sizes and diferent numbers of attacks, and we compared our results with some existing intrusion detection system techniques.

On the other hand a technique based on machine learning, more precisely on the random forest algorithm with the selection of the best features,is also proposed. The latter is tested on the NSL-KDD dataset. The results found were very satisfying in terms of Accuracy 99,66%, Precision 99,85 %, Recall 99,83 % and F1-Score 99,84%. Thus, the results have improved when compared with those of other techniques.

Key words : MANET, AODV, Black hole, Malicious nodes, Multiple attacks, SPlitted AACK, Machine learning, Intrusion detection, NSL-KDD, Random Forest, Most Best Features Selection.

الملـــــــــخص

شبكات الجوال المتحركة (MANET) هي شبكات بدون بنية تحتية. نطاق الاتصال بين العقد محدود ، حيث يلزم وجود عدة قفزات لإرسال حزمة معلومات من المصدر إلى الوجهة. هذه الشبكات لها هيكل متغير باستمرار بسبب الأجهوة الكونة لها المتنقلة واتصالاتها العشوائية ، مما يجعلها عرضة لهجمات مختلفة. أحد أهم الهجمات في MANET هو هجوم الثقب الأسود الذي يضعف أداء الشبكة عن طريق إزالة جميع الحزم التي تمر عبرها. هناك العديد من التقنيات لاكتشاف هجمات الثقب الأسود في بروتوكول موجه حسب الطلب. في هذا العمل ، تم اقتراح نهج جديد يعتمد على AACK. النظام المقترح هو الكشف عن هجمات الثقب الأسود المفردة والمتعددة عن طريق نظام كشف التسلل بتقنية SPlitted AACK. النظام قوي بما يكفي لاكتشاف جميع هجمات الثقب الأسود باستخدام الانقسام التكراري للمسار الرئيسي حتى اكتشاف الجهاز المتسسل. يستخدم Network simulator 2 في المحاكاة. اختبرنا نظامنا على شبكات مختلفة ذات أحجام شبكات مختلفة وأعداد مختلفة من الهجمات ، وقارننا نتائجنا مع بعض تقنيات نظام كشف التسلل الحالية.

من ناحية أخرى ، تم اقتراح تقنية تعتمد على التعلم الآلي ، وبشكل أكثر دقة على خوارزمية الغابة العشوائية مع اختيار أفضل الميزات. يتم اختبار الأخير على مجموعة بيانات NSL-KDD. النتائج التي تم العثور عليها كانت مرضية للغاية من حيث الثقة 99،66٪ ، الدقة 99،85٪ ، Recall 99،83٪ و F1-Score 99،84٪. وبالتالي ، فقد تحسنت النتائج عند مقارنتها بنتائج التقنيات الأخرى.

الكلمات المفتاحية : MANET، AODV ، الثقب الأسود ، العقد الضارة ، الهجمات المتعددة ، SPlitted AACK ، التعلم الآلي ، كشف التسلل ، NSL-KDD، الغابة العشوائية ، اختيار أفضل الميزات..

Table des matières

Table des figures

Liste des tableaux

INTRODUCTION GÉNÉRALE

Introduction générale

Au cours des dernières années, nous avons assisté à une expansion rapide dans le domaine de l'informatique mobile en raison de la prolifération et la disponibilité d'appareils sans fil sur le marché.

Un réseau mobile ad hoc (MANET) est un réseau à configuration automatique de nœuds mobiles qui comprend des routeurs et des hôtes connectés par des liaisons sans fil. L'union de ces nœuds forme la configuration arbitraire de la topologie du réseau (Giordano Urpi, 2005). Il n'y a pas de colonne vertébrale pour une telle topologie. Les nœuds sans fil du réseau agissent comme des routeurs et transmettent des données et des messages de contrôle entre eux. Si le nœud A ne peut pas envoyer directement un message au nœud B, les nœuds à portée du nœud A agiront en tant que routeur (nœuds intermédiaires) pour ce nœud et transmettront le paquet à la destination. Les routeurs sont libres de se déplacer au hasard et de s'organiser arbitrairement ; la topologie du réseau change rapidement et de manière imprévisible. MANET peut fonctionner de manière autonome comme pour la petite organisation ou il peut être connecté à un réseau câblé plus large comme Internet. Cette topologie de réseau arbitraire donne un pouvoir immense au fonctionnement des MANET. Ces réseaux peuvent être déployés là où il n'y a pas de véritable dorsale pour le réseau. Les nœuds de MANET peuvent travailler ensemble et effectuer la tâche de manière autonome.

Les MANETS sont extrêmement utiles dans les scénarios où il n'est pas facile d'établir des points d'accès ou des récepteurs de base et où nous devons mettre à jour les informations rapidement et où une mobilité maximale est requise.

Au fur et à mesure que les MANET sont largement utilisés, la question de la sécurité est devenue l'une des principales préoccupations. Par exemple, la plupart des protocoles de routage proposés pour les MANET supposent que chaque nœud du réseau est coopératif et non malveillant. Par conséquent, un seul nœud compromis peut entraîner la défaillance de l'ensemble du réseau. Il existe des attaques passives et actives dans les MANET. Pour les attaques passives, les paquets contenant des informations secrètes peuvent être écoutés, ce qui viole la confidentialité.

Les attaques actives, y compris l'injection de paquets vers des destinations non valides dans le réseau, la suppression de paquets, la modification du contenu de paquets et l'usurpation d'identité d'autres nœuds violent la disponibilité, l'intégrité, l'authentification et la non-répudiation. Contrairement à leurs homologues câblés, les réseaux mobiles ad hoc ne disposent pas de pare-feu ou de serveurs centraux où toutes les intrusions peuvent être bloquées. Par conséquent, chaque nœud doit être équipé pour faire face à toutes sortes d'attaques. Afin d'assurer la sécurité, chaque nœud du réseau est authentifié à l'aide de techniques cryptographiques prises en charge par une autorité de certification (*Certaficate Autority*). Cependant, les MANETS ont une configuration dynamique et une autorité de certification centralisée ne peut pas être déployée sur le réseau. Les MANETS fonctionnent comme un modèle décentralisé et il est essentiel d'établir la confiance entre les nœuds du réseau. Un bon modèle de confiance doit être évolutif et robuste.

Même si la confiance est établie entre les nœuds du réseau, un nœud du réseau peut devenir malveillant. Ce nœud peut mal acheminer les paquets ou inonder le réseau de faux paquets. Ce nœud peut également modifier le contenu des informations des paquets sensibles au contenu.

Afin de détecter ce type de nœuds malveillants, il devrait y avoir un mécanisme de détection d'intrusion ainsi qu'un établissement de confiance et un routage sécurisé. La détection d'intrusion peut être définie comme un processus de surveillance des activités dans un système, qui peut être un ordinateur ou un système réseau. Le mécanisme par lequel cela est réalisé est appelé un système de détection d'intrusion (IDS). Un IDS collecte des informations sur les activités, puis les analyse pour déterminer s'il existe des activités qui violent les règles de sécurité.

Une fois qu'un IDS détermine qu'une activité inhabituelle ou une activité connue peut devenir une attaque, il génère alors une alarme pour alerter l'administrateur de sécurité. En outre, l'IDS peut également initier une réponse appropriée à l'activité malveillante. Bien qu'il existe aujourd'hui plusieurs techniques de détection d'intrusion développées pour les réseaux filaires, elles ne sont pas adaptées aux réseaux sans fil en raison des différences de leurs caractéristiques. Par conséquent, ces techniques doivent être modifiées ou de nouvelles techniques doivent être développées pour que la détection d'intrusion fonctionne efficacement dans les MANET.

Les mesures de détection d'intrusions telles que le chiffrement et l'authentification ne peuvent qu'empêcher les nœuds externes de perturber le trafic, mais ne peuvent pas être efficace lorsque

des nœuds compromis internes au réseau commencent à perturber le trafic. De nombreux événements historiques ont montré que les seules techniques de prévention des intrusions, qui constituent généralement une première ligne de défense, ne suffisent pas. À mesure que le système devient plus complexe, il y a aussi plus des faiblesses, ce qui entraîne plus de problèmes de sécurité.

Contrairement aux pare-feu qui constituent la première ligne de défense, la détection d'intrusion peut être utilisée comme un deuxième mur de défense, pour protéger le réseau contre de tels problèmes, et intervient après que l'intrusion s'est produite et qu'un nœud a été compromis. Si l'intrusion est détectée, une réponse peut être initiée pour prévenir ou minimiser les dommages au système.

De nombreux chercheurs (T.S. Sobh, 2006) (X.D. Hoang al, 2009) (C. Xenakis al, 2011) ont classé les IDS existants comme étant basés sur l'hôte ou sur le réseau, selon le mécanisme de collecte de données. Les IDS basés sur l'hôte fonctionnent sur les pistes d'audit du système d'exploitation, les journaux système et d'application, ou les données d'audit générées par les modules de noyau chargeables qui interceptent les appels système. Les IDS basés sur le réseau fonctionnent sur des paquets capturés à partir du trafic réseau. De plus, les IDS peuvent être classés en fonction de la technique de détection décrite ci-dessous :

Systèmes de détection basés sur les signatures : le système conserve les signatures des attaques connues et les utilise pour les comparer aux données capturées. Tout modèle correspondant est traité comme une intrusion. Cette technique peut atteindre de faibles taux de faux positifs, mais s'affaiblit pour détecter des attaques jusque-là inconnues. Comme un système de détection de virus, il ne peut pas détecter de nouveaux types de virus.

Systèmes de détection basés sur les anomalies : les profils normaux (comportements) des utilisateurs sont conservés dans le système. Le système compare les données capturées avec ces profils, puis traite toute activité qui s'écarte de la ligne de base comme une éventuelle intrusion en informant les administrateurs système ou en initialisant une réponse appropriée. Ce système estadapté aux attaques inconnues mais il donne des taux élevés de faux positifs.

Systèmes de détection basés sur des spécifications : Le système définit un ensemble de contraintes qui décrivent le bon fonctionnement d'un programme ou d'un protocole. Ensuite, il

surveille l'exécution du programme par rapport aux contraintes définies. Cette technique peut fournir la capacité de détecter des attaques jusque-là inconnues, tout en présentant un faible taux de faux positifs.

Le système de détection précoce des intrusions pour les MANET a été développé par (Marti S al, 2000), qui s'appelle *Watchdog*. Où chaque nœud surveillera le prochain saut pour s'assurer qu'il transmettra le paquet ou non. Comme décrit dans la même recherche, il présente plusieurs faiblesses, à savoir une collision ambiguë, des collisions de récepteurs, une puissance de transmission limitée, un faux comportement, une collusion et une chute partielle. De nombreuses recherches sont dédiées à la résolution de ces problèmes.

En fait, la préoccupation était de résoudre la collision du récepteur et la puissance d'émission limitée. Où, dans ces vulnérabilités, le nœud qui se comporte mal peut tromper l'expéditeur (moniteur) du paquet en lui faisant croire qu'il transmet correctement le paquet alors qu'il ne le fait pas. Une solution à ces problèmes a été proposée en 2005, qui est le schéma *TWOACK* (Balakrishnan, 2005). C'est un schéma basé sur l'accusé de réception qui assure la transmission du paquet sur trois nœuds consécutifs ; ainsi, l'audition ne sera plus utilisée. Ce mécanisme résout les deux problèmes mais avec une surcharge importante et plus de calculs qui affecteront la puissance et la mémoire du réseau, qui sont des ressources rares pour les MANET. De plus, cette technique détecte les liens qui se comportent mal plutôt que les nœuds malicieux, ce qui est considéré comme une faiblesse car de cette manière, le nœud qui se comporte mal aura plus de chances de supprimer des paquets de données.

AACK(Sheltami T al, 2009), était proposé afin d'améliorer les faiblesses de *TWOACK*, qui sont, la surcharge de routage et la détection des liens malicieux plutôt que des nœuds. De même, *AACK* présente toujours des faiblesses. Comme, il peut détecter la présence d'une intrusion mais il ne peut pas détecter vraiment le nœud intrus.

Notre mécanisme proposé *SP-AACK* (détaillé dans le chapitre 3), vise à améliorer les faiblesses d'*AACK*. Plus précisément la détection des nœuds malveillants quelques soit leurs nombres et leurs positions dans le réseau.

Le principe est de diviser le chemin en deux sous chemins à chaque fois que l'accusé de réception *AACK* n'est pas reçu. La division permet d'avoir plusieurs sous-chemins ce qui rend

la détection du nœud malveillant facile.

Pour s'assurer que les nouveaux nœuds sources / destinations ne sont pas malveillants, nous avons abordé un processus de vérification des nœuds source et destination. Initialement, les seuls nœuds confirmés à l'intérieur sont la source d'origine et la destination d'origine. Nous les avons exploités pour confirmer les autres. Commençant par le premier sous-chemin qui contient la source d'origine. Si nous recevons un accusé de réception de sa destination alors ce chemin est confirmé à l'intérieur.

Pour confirmer le deuxième sous-chemin, nous devons d'abord confirmer sa source en envoyant un *ACK* à la destination du premier sous-chemin, s'il est reçu alors cette source n'est pas un nœud malveillant. Ce processus est répété jusqu'à ce que tout le chemin soit confirmé. Les nœuds malveillants détectés seront envoyés dans une liste noire au fur et à mesure de la détection. Pour tester l'efficacité de mécanisme *SP-AACK* proposé, il a été testé pour la détection de l'une des plus cruelles attaques : l'attaque par trou noir (Black Hole attack). Cette dernière a une énorme influence sur le protocole *AODV* vue le grand nombre de paquets qui sera supprimé ou absorbé par cette attaque. Les expérimentations et les résultats sont discutés en détail dans le chapitre 3 (Khalladi et al, 2021).

D'autre techniques sont apparues dans le domaine de détection d'intrusion tel que les mécanismes de cryptographie qui offraient certains avantages en introduisant un retard considérable dans la communication. De plus, ils nécessitaient la connexion préalable pour maintenir le transfert de données entre les nœuds, ce qui n'est pas réalisable dans les réseaux ad hoc mobiles. Par conséquent, des méthodes hybrides sont nécessaires pour améliorer la sécurité dans MANET en tant que nœuds qui sont ouverts à diverses attaques dans différentes couches de MANET. Par exemple, certaines des attaques les plus courantes sont le déni de service, l'écoute clandestine, l'homme au milieu, l'inondation, Sybil, l'usurpation de trou de ver, l'usurpation d'identité, le trou noir, le brouillage et les attaques par trou gris, etc. qui ciblent des couches spécifiques.

Dans une certaine mesure, les systèmes de détection d'intrusion, les mécanismes de cryptage, l'analyse du spectre étalé et les pare-feu peuvent contribuer à détecter divers types d'attaques, mais la dernière décennie a vu un changement de paradigme réseau de la cryptographie vers de nouvelles technologies comme l'Intelligence Artificielle, l'apprentissage automatique et les

algorithmes génétiques.

Le mécanisme de détection d'intrusion correspond à la stratégie défensive déployée dans les MANET pour examiner et sonder les événements qui se produisent hors de l'ordinaire, qui comprend plusieurs méthodes pour détecter des anomalies dans le réseau. L'IDS peut généralement être de trois types : détection d'anomalies, détection d'abus ou détection orientée signature. Le mécanisme basé sur la détection d'anomalies peut filtrer les nœuds aberrants anormaux en les évaluant avec des modèles normaux réguliers. Un nœud est étiqueté comme intrus si une valeur aberrante est détectée.

La détection des abus et la détection basée sur les signatures reposent uniquement sur des signatures ou des modèles enregistrés. Elles ne peuvent donc pas être utilisées pour détecter des menaces ou des attaques innovantes. Ainsi, la détection basée sur les anomalies surpasse les deux autres en termes de capacité à gérer de nouveaux scénarios comme dans les MANET. Ce qui est connue pour sa nature d'environnement dynamique et ouvert où les nœuds peuvent se connecter et partir à tout moment de manière ad hoc. Ce qui les rend encore plus vulnérable à plusieurs attaques possibles. L'intention principale est de reconnaître toute activité malveillante avant le danger réel afin que les nœuds des MANET soient dotés de la capacité de filtrer les entrées illégales et non autorisées.

Étant donné que les nœuds sont limités en ressources telles que l'alimentation, le stockage, etc. Cela crée un immense défi dans la mise en œuvre de la détection d'anomalies dans les applications en temps réel. Les méthodes d'apprentissage automatique facilitent la découverte des menaces diverses et nouvelles ainsi que les vulnérabilités du système existant.

La configuration des techniques d'apprentissage automatique peut être basée sur des réseaux de neurones, la logique floue, des algorithmes génétiques, les réseaux bayésiens ou bien les algorithmes de classification. Ces technologies sont devenues une alternative remarquable pour les analystes de sécurité ainsi que pour les chercheurs afin d'arriver à une solution efficace et optimisée pour l'amélioration de la sécurité dans les environnements MANET.

Par conséquent, nous présenterons dans cette thèse une nouvelle approche qui peut effectuer la détection d'intrusion d'une manière efficace basée sur un modèle d'apprentissage automatique utilisant le puissant classifieur Random Forest sur l'ensemble de donnée NSL-KDD (Tavallaee

M et al, 2009). Les études ont montré qu'un apprentissage aveugle sur tous les attributs de l'ensemble de données, affaibli en quelque sorte le schéma de détection généré. Une solution s'avère très intéressante est la sélection des attributs importants. Nous avons proposé une méthode de sélection des attributs les plus importants, en calculant l'impact de chacun sur l'Accuracy total du modèle. Seul les attributs avec un impact élevé seront sélectionnés durant la phase d'apprentissage.

Les expérimentations et les résultats sont discuté en détail dans le chapitre 4(Khalladi et al, 2022).

Organisation de la thèse

Le reste de la thèse est organisé comme suit :

Le chapitre 1, s'attache à élucider dans sa première partie la notion des réseaux mobiles ad-hoc « MANET », à décrire leur historique, citer leurs caractéristiques, puis définir quelques domaines d'application, tout en passant sur le routage de ce réseau. Dans la deuxième partie de ce chapitre, l'un des sérieux problèmes dans ce type de réseau a été posé « La sécurité ». Cette partie définie ce qu'est une attaque informatique notamment les types d'attaques ainsi qu'une vue générale sur les techniques de sécurité existante.

Le chapitre 2 introduit les concepts essentiels à la détection d'intrusion. Différents types d'IDS sont détaillés, avec leurs forces et leurs faiblesses. Il présente aussi les travaux existants liés à la détection d'intrusion. Les différents modèles sont détaillés avec une courte présentation de leur fonctionnement. Les approches et les résultats sont successivement présentés. Enfin, les informations recueillies dans ce chapitre sont utilisées dans la conception des contributions discutés dans les chapitres suivants.

Le chapitre 3 présente l'une des célèbres attaques dans les réseaux ad-hoc. L'attaque par trou noir (Black Hole). Elle a été détaillée avec ses deux types simple ou multiple. Ainsi, son impact sur le protocole de routage AODV. Plusieurs travaux ont été discutés afin de proposer une solution générique regroupant quasiment toutes les techniques présentées à savoir : ACK, TWOACK, 3ACK et AACK.

Le chapitre 4 présente les apports de l'apprentissage automatique dans ce domaine et les différents ensembles de données spécifiques utilisés dans ce domaine. Une solution proposée sur la base des modèles de machine d'apprentissage notamment l'algorithme Random Forest pour classer les attaques sur l'ensemble de données les plus populaires dans la détection d'intrusion NSL-KDD. Une méthode de sélection des attributs importants a été proposée pour améliorer la précision du modèle.

La thèse est conclue en résumant les principaux points du mémoire. Les perspectives et les travaux futurs sont discutés.

CHAPITRE I

LES RÉSEAUX MOBILES AD-HOC

I.1 Introduction

L'évolution récente de la technologie dans le domaine de la communication sans fil et l'apparition des unités de calcul portables poussent aujourd'hui les chercheurs à faire des efforts afin de réaliser le but des réseaux : *« L'accès à l'information n'importe où et n'importe quand »* . Le concept des réseaux mobiles ad-hoc essaie d'étendre les notions de la mobilité à toutes les composantes de l'environnement. Ici, contrairement aux réseaux basés sur la communication avec infrastructure, aucune administration centralisée n'est disponible. Ce sont les hôtes mobiles eux-mêmes qui forment l'infrastructure du réseau. Aucune supposition ou limitation n'est faite sur la taille du réseau ad hoc ; le réseau peut contenir des centaines ou des milliers d'unités mobiles. (Misra S al, 2009) (Lima MN al, 2009).

La mobilité dans ces types de réseau n'est pas seulement un avantage mais aussi un inconvénient car elle engendre d'énormes problèmes de sécurité vue les vulnérabilités causées par l'absence d'une infrastructure. Dans ce chapitre, nous allons présenter les réseaux ad-hoc. Nous commençons par la définition de ces réseaux et leurs caractéristiques inhérentes. Ensuite, nous définissons quelques domaines d'application d'un réseau ad hoc, ses avantages et ses inconvénients sans oublier le routage d'un réseau ad-hoc. La dernière partie sera consacrée pour la sécurité dans ce type de réseau.

I.2 Réseaux Mobile ad-hoc

Les systèmes de communication cellulaires sont basés essentiellement sur l'utilisation des réseaux filaires et la présence des stations de base qui couvrent les différentes unités mobiles du système. La contre partie de ces réseaux sont des réseaux ad-hoc qui se forment spontanément et qui s'organisent automatiquement sans avoir besoin d'une infrastructure existante (Giordano Urpi, 2005).

Definition 1 : Un réseau mobile ad hoc, appelé généralement MANET *(Mobile Ad hoc NETwork)*, consiste en une grande population relativement dense d'unités mobiles qui se déplacent dans un territoire quelconque et dont le seul moyen de communication est l'utilisation des interfaces sans fil, sans l'aide d'une infrastructure préexistante ou d'administration centralisée. (Koujalagi, 2018)

Definition 2 : Un réseau mobile ad hoc est un ensemble d'hôtes mobiles sans fil formant

un réseau temporaire sans l'aide d'une administration centralisée ou de services de support standard. Sa topologie est dynamique : les nœuds entrent et sortent du réseau en permanence. Dans ce type de réseau, il n'y a pas de contrôle centralisé ou d'infrastructure fixe pour prendre en charge la configuration / reconfiguration du réseau. (Omari Sumari, 2010)

I.2.1 Présentation des Réseaux Mobiles ad-hoc

Un réseau ad hoc peut être modélisé par un graphe $G_t = (V_t, E_t)$ ou V_t représente l'ensemble des nœuds (i.e. les unités ou les hôtes mobiles) du réseau et E_t modélise l'ensemble des connections qui existent entre ces nœuds (voir la figure I.1). Si $e = (u,v)$ appartient à E_t, cela veut dire que les nœuds u et v sont en mesure de se communiquer directement a l'instant t.

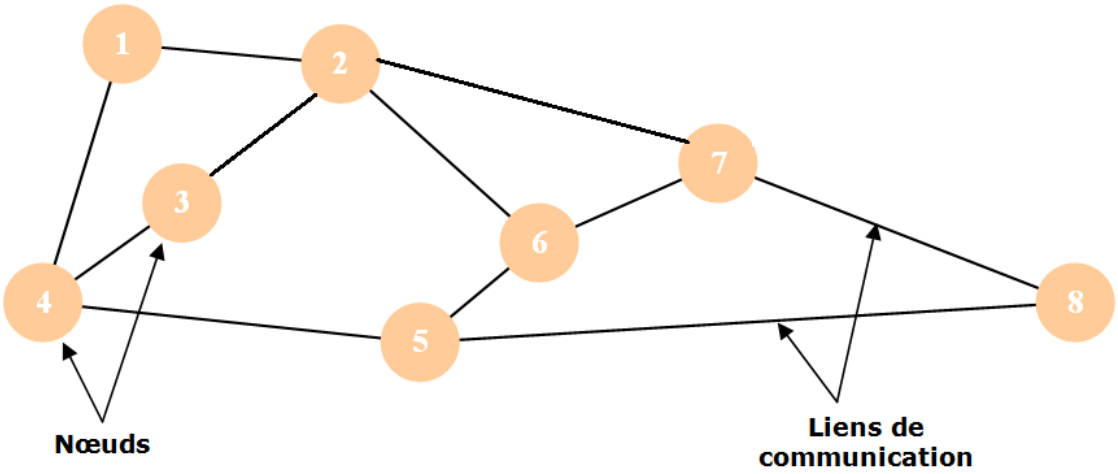

Figure I.1 – Modélisation d'un réseau ad-hoc.

La topologie du réseau peut changer à tout moment (voir la figure I.2), elle est donc dynamique et imprévisible, ce qui fait que la déconnexion des unités est très fréquente.

I.2.2 Caractéristiques des réseaux ad-hoc

Les réseaux mobiles ad hoc sont caractérisés par ce qui suit (Giordano Urpi, 2005) (Omari Sumari, 2010) (Lawrence.E Ramavel. Latha, 2016) :

- **Une topologie dynamique :** Les nœuds mobiles sont des unités autonomes du réseau et sont libres de se déplacer arbitrairement. La topologie du réseau peut changer de manière aléatoire et rapide à des moments imprévisibles et peut consister en des liaisons

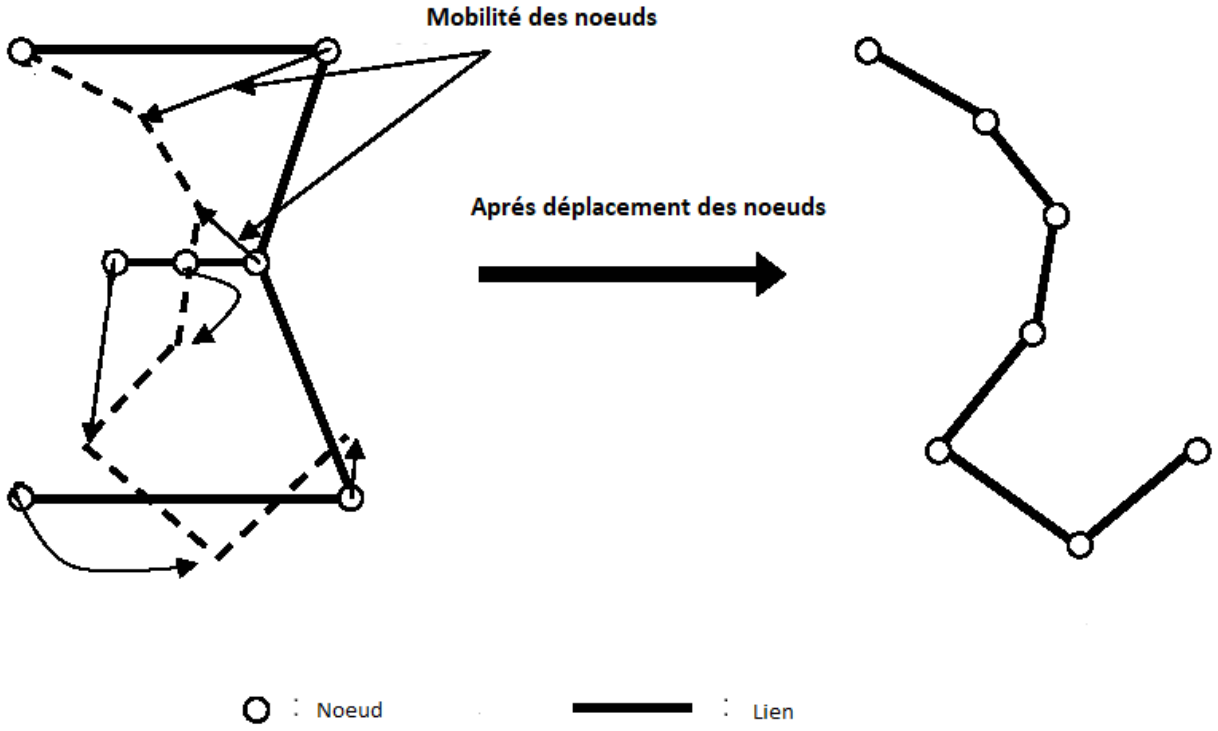

Figure I.2 – Changement de la topologie des réseaux ad-hoc .

bidirectionnelles et unidirectionnelles. Les nœuds peuvent facilement sortir ou entrer dans la portée radio de divers autres nœuds et ainsi la localisation d'un nœud particulier devient difficile. Les informations de routage des nœuds changent continuellement à mesure que leur mouvement devient aléatoire.

- ▷ **Autonome et sans infrastructure :** MANET est un système sans infrastructure qui n'a pas de serveur central ou de matériel spécialisé et de routeurs fixes. Toutes les communications entre les nœuds sont assurées uniquement par une connectivité sans fil. La gestion du réseau doit être répartie sur différents nœuds, ce qui rend difficile la détection et la gestion des pannes.
- ▷ **Auto-configuration :** MANET est un réseau auto-configurable dans lequel les activités du réseau, y compris la découverte de la topologie et la livraison des messages, sont exécutées par les nœuds eux-mêmes. Chaque nœud mobile est un nœud indépendant, qui peut fonctionner à la fois comme hôte et comme routeur et générer des données indépendantes.
- ▷ **Routage multi-sauts :** lorsqu'un nœud tente d'envoyer des informations à d'autres nœuds qui sont hors de sa portée de communication, le paquet doit être transmis via un

ou plusieurs nœuds intermédiaires. c'est à dire. Chaque nœud agit comme un routeur et transmet les paquets de l'autre pour permettre le partage d'informations entre les hôtes mobiles.

- ▷ **Évolutivité du réseau (Scalabilité) :** la plupart des applications MANET impliquent de grands réseaux avec des milliers de nœuds (exemple : réseaux de capteurs) et l'évolutivité est essentielle au déploiement réussi de ces réseaux. En ce qui concerne l'évolutivité, des défis se posent dans des domaines tels que l'adressage, le routage, la gestion de la localisation, la gestion de la configuration, l'interopérabilité, la sécurité, les technologies sans fil à haute capacité, etc.
- ▷ **Des contraintes d'énergie :** les hôtes mobiles sont petits et légers avec moins de capacité de processeur, un stockage à faible consommation d'énergie et une petite taille de mémoire. Ils sont alimentés par des ressources énergétiques limitées telles que de petites batteries. Pour ces nœuds, les critères de conception de système les plus importants pour l'optimisation peuvent être la conservation de l'énergie. Cette limitation entraîne une vulnérabilité et certaines attaques peuvent essayer d'engager inutilement les nœuds mobiles, de sorte qu'ils continuent à utiliser leur batterie.
- ▷ **Liaisons sans fil :** les liaisons sans fil rendent le réseau mobile ad hoc peu fiable et sensible à divers types d'attaques et ont une capacité nettement inférieure à celle de leurs homologues câblés. En raison de l'alimentation électrique limitée des nœuds sans fil et de la mobilité des nœuds, les liaisons sans fil entre ces nœuds dans MANET ne sont pas cohérentes pour les participants à la communication. De plus, les effets des conditions d'accès multiples, d'évanouissement, de bruit et d'interférence peuvent dégrader la capacité d'une liaison sans fil au fil du temps et le débit effectif peut être inférieur à la capacité de transmission maximale de la radio.
- ▷ **Variation des capacités des liaisons et des nœuds :** Chaque nœud mobile peut être équipé d'une ou plusieurs interfaces radio qui ont des capacités de transmission ou de réception variables et fonctionnent à travers différentes bandes de fréquences. Cette hétérogénéité des capacités radio des nœuds peut entraîner la formation de liaisons asymétriques. De plus, chaque nœud mobile peut avoir une configuration logicielle/matérielle différente, ce qui entraîne une variabilité des capacités de traitement. La conception de protocoles et d'algorithmes de réseau pour ce réseau hétérogène peut être complexe et peut nécessiter une adaptation dynamique aux conditions changeantes telles que les conditions

de puissance et de canal, les variations de charge/distribution du trafic, la congestion, etc.

I.2.3 Domaines d'utilisation des réseaux ad-hoc

Le réseau Ad hoc n'a besoin d'aucune installation fixe, ceci lui permettant d'être rapide et facile à déployer. En effet, la robustesse, le coût réduit qui rend ce réseau très utilisé dans plusieurs domaines (Giordano Urpi, 2005) (Omari Sumari, 2010) (N. Bhaskar al, 2021) :

- **Services Militaires :** Les réseaux sans fil ad hoc peuvent être utiles pour établir une communication entre un groupe de soldats pour des opérations tactiques. La capacité de mettre en place rapidement un réseau parmi les unités militaires dans une région hostile sans aucune infrastructure de soutien peut fournir un avantage tactique considérable sur le champ de bataille pour les forces amies. Par exemple, chaque soldat peut transporter un appareil mobile qui représente l'un des nœuds mobiles dans un réseau ad hoc reliant tous les soldats, chars et autres véhicules. La prise en charge des applications militaires nécessite des mécanismes d'auto-organisation qui fournissent une communication robuste et fiable dans des situations de combat dynamiques.

  Une autre application dans ce domaine est la coordination de véhicules militaires se déplaçant à grande vitesse tels que des flottes d'avions ou de navires de guerre. De telles applications nécessitent une communication rapide et fiable. Par exemple, le chef d'un groupe de soldats peut vouloir donner un ordre à tous les soldats ou à un groupe de soldats impliqués dans l'opération. À cet égard, le protocole de routage de ces applications doit être capable de fournir une communication multidiffusion rapide, sécurisée et fiable avec prise en charge du trafic en temps réel. Comme les applications militaires nécessitent une communication très sécurisée, les nœuds montés sur véhicule doivent être très sophistiqués et puissants. L'utilisation de plusieurs émetteurs-récepteurs haute puissance, chacun ayant la capacité de sauter entre différentes fréquences, améliore la communication.

- **Services d'urgence :** Les réseaux ad hoc sont très utiles dans les opérations d'urgence telles que la recherche et le sauvetage, le contrôle des foules et les opérations de reprise après sinistre. Dans les environnements où les installations de communication basées sur l'infrastructure conventionnelle sont détruites en raison de catastrophes naturelles telles que les tremblements de terre. Le déploiement immédiat de réseaux sans fil ad hoc serait une bonne solution pour coordonner les activités de sauvetage. Comme les réseaux ad hoc nécessitent une configuration réseau initiale minimale pour leur fonctionnement, très peu

ou pas de retard est nécessaire pour rendre le réseau pleinement opérationnel.
Les équipes d'intervention d'urgence peuvent mettre en place rapidement des réseaux Ad hoc pour remplacer les infrastructures détruites, permettant aux équipes de mieux coordonner leurs efforts. En situation d'urgence, les réseaux câblés pourraient être détruits et il y aura un besoin de réseau sans fil, qui pourrait être déployé rapidement pour la coordination des secours.

- ▷ **Applications de collaborations :** Un autre domaine dans lequel les réseaux sans fil ad hoc trouvent des applications est l'informatique collaborative. Pour certains environnements d'entreprise, le besoin d'informatique collaborative peut être plus important à l'extérieur qu'à l'intérieur des environnements de bureau, comme lors d'une réunion d'affaires à l'extérieur du bureau pour informer les clients d'une mission donnée. Dans de tels cas, un réseau ad hoc peut être utilisé pour coopérer et échanger des informations sur un projet donné. L'exigence d'une infrastructure de communication temporaire pour une communication rapide avec une configuration minimale entre un groupe de personnes lors d'une conférence ou d'un rassemblement nécessite la formation d'un réseau sans fil ad hoc.

  Par exemple, imaginez un groupe de chercheurs qui souhaitent partager leurs résultats de recherche ou leur matériel lors d'une conférence, ou un enseignant distribuant des notes à la classe à la volée. Dans de tels cas, la formation d'un réseau sans fil ad hoc avec le support nécessaire pour un routage multidiffusion fiable peut servir l'objectif. Les applications de partage de fichiers distribuées utilisées dans de telles situations ne nécessitent pas un haut niveau de sécurité comme dans un environnement militaire, mais la fiabilité du transfert de données est d'une grande importance.

- ▷ **Réseaux domestique et éducation :** L'application la plus simple et la plus directe des réseaux Ad hoc à la maison et au bureau est la mise en réseau d'ordinateurs portables, de PDA et d'autres appareils compatibles WLAN en l'absence d'une station de base sans fil. Une autre application domestique qui relève de la classe des réseaux personnels (PAN) est le remplacement des câbles via des liaisons sans fil, comme dans Bluetooth. Tous les périphériques peuvent se connecter à un ordinateur via des liaisons Bluetooth sans fil, ce qui élimine le besoin de filaire Connexions. Ils peuvent également permettre le streaming vidéo et audio entre les nœuds sans fil en l'absence de toute station de base.

Les activités éducatives peuvent également bénéficier des réseaux ad hoc. Par exemple, les étudiants qui fréquentent une salle de classe peuvent utiliser leur ordinateur portable pour obtenir le dernier matériel de cours à partir de l'ordinateur portable d'un professeur au fur et à mesure que la classe progresse. Les universités et les campus, les salles de classe virtuelles, les communications ad hoc lors de réunions ou de conférences sont quelques-unes des applications éducatives des réseaux ad hoc. Du côté récréatif, la théorie des jeux traite de la prise de décision multi-personnes, dans laquelle chaque décideur essaie de maximiser son utilité. La coopération des utilisateurs est nécessaire au fonctionnement des réseaux Ad hoc ; par conséquent, la théorie des jeux fournit une bonne base pour analyser les réseaux. Généralement, les personnes qui jouent à des jeux multijoueurs utilisent Internet, avec un hôte distant et ce modèle est appelé le modèle client-serveur. En cas d'utilisateurs multiples, chaque utilisateur se connecte à un serveur commun et le serveur transmet les paquets aux utilisateurs connectés.

I.2.4 Avantages et inconvénients des réseaux mobile ad hoc

La nature dynamique et l'abscence d'une infractucture fixe pour les réseaux ad-hoc donnent une vision sur les principaux avantages et inconvénients dans ce type de réseau (Giordano Urpi, 2005).

I.2.4.1 Avantages de MANET

- ▷ **Sans routeur :** le principal avantage de l'utilisation d'un réseau ad hoc est la connexion à Internet sans avoir besoin d'un routeur sans fil. Cela rend le réseau ad hoc plus abordable que le réseau traditionnel car nous n'avons pas le coût supplémentaire d'un routeur.
- ▷ **Vitesse :** La création d'un réseau ad hoc à partir de la phase initiale nécessite quelques changements de paramètres et aucun matériel ou logiciel supplémentaire. Pour connecter plusieurs ordinateurs rapidement et facilement, le réseau ad hoc est une solution idéale.
- ▷ **Tolérance aux pannes :** MANET prend en charge les échecs de connexion car les protocoles de routage et de transmission sont conçus pour gérer ces situations.
- ▷ **Installation rapide :** Le niveau de flexibilité pour la configuration de MANET est élevé. L'installation d'un MANET est simple et rapide et élimine le besoin de tirer les câbles à travers les murs et les plafonds. De plus, ils ne nécessitent aucune installation ou infrastructure préalable et, par conséquent, ils peuvent être installés en très peu de temps.

- ▷ **Connectivité :**L'utilisation de points centralisés ou de passerelles n'est pas nécessaire pour la communication au sein du MANET, en raison de la collaboration entre les nœuds dans la tâche de livraison des paquets.
- ▷ **Coût :** MANET pourrait être plus économique dans certains cas car il n'y a pas de coût d'infrastructure fixe et il réduit la consommation d'énergie aux nœuds mobiles.

I.2.4.2 Inconvénients de MANETS

- ▷ **Liaisons asymétriques :** La plupart des réseaux câblés reposent sur des liaisons symétriques, qui sont toujours fixes. Mais ce n'est pas le cas avec les réseaux Ad-hoc car les nœuds sont mobiles et peuvent constamment changer de position au sein du réseau. Considérons par exemple un MANET où le nœud B envoie un signal au nœud A mais cela ne dit rien sur la qualité de la connexion dans le sens inverse.
- ▷ **Surdébit de routage :** dans les MANET, les nœuds changent souvent d'emplacement au sein du réseau. Ainsi, certaines routes obsolètes sont générées dans la table de routage, ce qui entraîne une surcharge de routage inutile.
- ▷ **Interférence :** C'est l'un des problèmes majeurs des réseaux MANET. Une transmission peut interférer avec une autre et un nœud peut entendre les transmissions d'autres nœuds et peut corrompre la transmission totale.
- ▷ **Connexion redondante :** la connexion dans les réseaux MANET doit être redondante pour récupérer les échecs de connexion. Une connexion avec une redondance élevée devrait être robuste malgré de nombreuses défaillances de nœuds. L'algorithme de routage peut gérer une redondance élevée, mais la mise à jour de la table de routage prend beaucoup de temps.
- ▷ **Topologie dynamique :** les nœuds peuvent rejoindre ou quitter le réseau à tout moment ou les caractéristiques du support peuvent changer. Dans les réseaux MANET, les tables de routage doivent en quelque sorte refléter ces changements de topologie et les algorithmes de routage doivent être adaptés. Par exemple, dans un réseau fixe, la mise à jour de la table de routage a lieu toutes les 30 secondes. Cette fréquence de mise à jour peut être très faible pour les MANET.

I.3 Routage dans les réseaux MANET

Les communications dans les réseaux ad hoc constituent une tâche difficile à réaliser. En effet, en l'absence d'infrastructure, l'acheminement d'un paquet d'une source vers son nœud destination n'est pas aisé. Il s'agit de découvrir une route entre les deux nœuds qui sera amené à changer dans le temps et être découverte lors d'une prochaine communication. Généralement, le routage est une méthode d'acheminement d'information vers la bonne destination à travers un réseau de connexion donné. Il consiste à assurer une stratégie qui garantit à n'importe quel moment, un établissement de routes qui soient correctes et efficaces entre n'importe quelle paire de nœuds appartenant au réseau, ce qui assure l'échange des messages d'une manière continue (Giordano Urpi, 2005) .

I.3.1 Notions sur le routage

Vu de la difficulté de routage dans les réseaux Ad Hoc, une variété des techniques sont utilisées par les stratégies existantes pour résoudre ce problème. Suivant ces techniques plusieurs classifications sont apparues parmi lesquelles nous allons citer : Routage hiérarchique ou plat. (Omari Sumari, 2010) (Ramasamy Rajeswari, 2020)

- **Les protocoles de routage à plat :** supposent que tous les nœuds sont égaux. La condition essentielle pour qu'un nœud décide de router des paquets pour un autre dépendra de sa position. Le protocole AODV *(Ad Hoc On Demand Distance Vector)* (Ramasamy Rajeswari, 2020) est l'un des protocoles utilisant cette technique.
- **Les protocoles de routage hiérarchique :** chaque noeud mobile peut assurer un(des) rôle(s) qui varient de l'un à l'autre. Certains d'entre eux sont élus pour assumer des fonctions particulières qui conduisent à une vision en plusieurs niveaux de la topologie du réseau .

I.3.1.1 Routage à vecteurs de distance

Dans ce type de routage, chaque nœud partage périodiquement sa table de routage à ses voisins contenant les adresses des nœuds destination du réseau et la distance (nombre de sauts) pour atteindre chacun d'eux. Cette table se met à jour si une nouvelle route plus courte est découverte, ou si l'un des nœuds constituant le chemin pour atteindre une destination donnée

change de distance vers cette destination, ou encore si un nœud inconnu est trouvé (c'est-à-dire, qui n'existe pas dans sa table).(Yi Lu al, 2003)

I.3.1.2 Routage à état de liens

Les protocoles de routage, dans ce type, le réseau est met à jour seulement quand un changement de réseau se produit. Il est créé pour surmonter les inconvénients du protocole à vecteur de distance. Chaque routeur tente de créer sa propre carte interne de la topologie du réseau. Au démarrage, lorsqu'un routeur devient actif, il envoie des messages pour collecter les informations auprès de ces voisins (auxquels il est directement connecté). Il fournit également l'état du lien pour atteindre le routeur (actif ou non). Ces informations sont utilisées par d'autres routeurs pour créer une carte de la topologie du réseau, qu'elle est, ensuite, utilisé pour choisir le meilleur chemin. Ces protocoles répondent rapidement aux modifications du réseau d'où ils envoient des mises à jour à chaque changement de réseau et des mises à jour périodiques à des intervalles de temps longs tels que 30 minutes. Si le lien change d'état, un message est généré et propagé contenant la mise à jour concernant ce lien vers tous les routeurs pour actualiser leurs tables de routage (Shewaye Sirika al, 2016) .

I.3.2 Techniques de routage

I.3.2.1 Routage à source et routage saut par saut

Deux techniques sont distinguées (Pinaki Mitrea, 2020), que l'on décrit comme suit :

- ▷ Routage à la source « source routing » le paquet routé doit indiquer l'intégralité du chemin que devra suivre pour atteindre sa destination. L'entête du paquet va donc contenir la liste des différents nœuds menant vers la destination.
- ▷ Routage saut par saut « hop by hop » le paquet doit connaitre uniquement l'adresse du prochain nœud vers la destination. Ce type de routage est le routage le plus repandu dans l'Internet, c'est le système de routage par défaut. AODV fait partie des protocoles qui utilisent cette technique .

I.3.2.2 Routage uniforme ou non uniforme

Une autre méthode de classification est basée sur le rôle que jouent les nœuds dans un schéma de routage. Selon ce critère de classification, on distingue les protocoles de routage

uniformes et non uniformes. Dans un protocole de routage uniforme, tous les nœuds mobiles ont le même rôle, importance et fonctionnalité. Dans un protocole de routage non uniforme, certains nœuds ont des fonctions de gestion et de routage particulières. Les protocoles non uniformes à leur tour peuvent être subdivisés selon l'organisation des nœuds mobiles et selon les stratégies de gestion et de routage en : des protocoles basés sur les zones, basés sur les clusters ou basés sur des nœuds noyaux (Pinaki Mitrea, 2020).

I.3.3 Protocoles de routage dans les réseaux ad Hoc

Pour rendre la communication dans les réseaux ad hoc plus efficace, de nombreux protocoles et algorithmes ont été proposés. Leurs fonctions principales est de fournir le chemin le plus court en termes de nombre de sauts entre une source et une destination de manière a ce que le nombre de messages générés soit minimum. (Mehran A al , 2004) Le routage dans les réseaux Ad hoc est assez délicat étant donnée la nature dynamique de la topologie de ce type de réseaux. Pour cela, de nombreux protocoles ont été proposés pour résoudre le problème multi saut, chacun fondé sur différents concepts et reposant sur différentes hypothèses et intuitions. (Mehran A al, 2004) (Pinaki Mitrea, 2020)

I.3.3.1 Classification des protocoles de routage

La classification des protocoles de routage se fait selon la méthode de création et de maintenance de routes lors de l'acheminement des données. En fonction des informations de routages échangés et les méthodes de calcul des routes utilisées. On distingue trois familles de protocoles de routage ad hoc :

- ▷ Les protocoles de routage dits « proactifs ».
- ▷ Les protocoles de routage *« réactifs »*.
- ▷ Les protocoles de routage dits « Hybrides ».

Entre ces deux familles, une autre approche qui fait un mélange entre les deux approches précédentes, il s'agit des protocoles dits « hybrides » qui utilisent à la fois les protocoles proactifs et les protocoles réactifs. La figure 1.3 illustre la classification des protocoles de routage pour réseaux Ad-hoc (Khalid.K al, 2020).

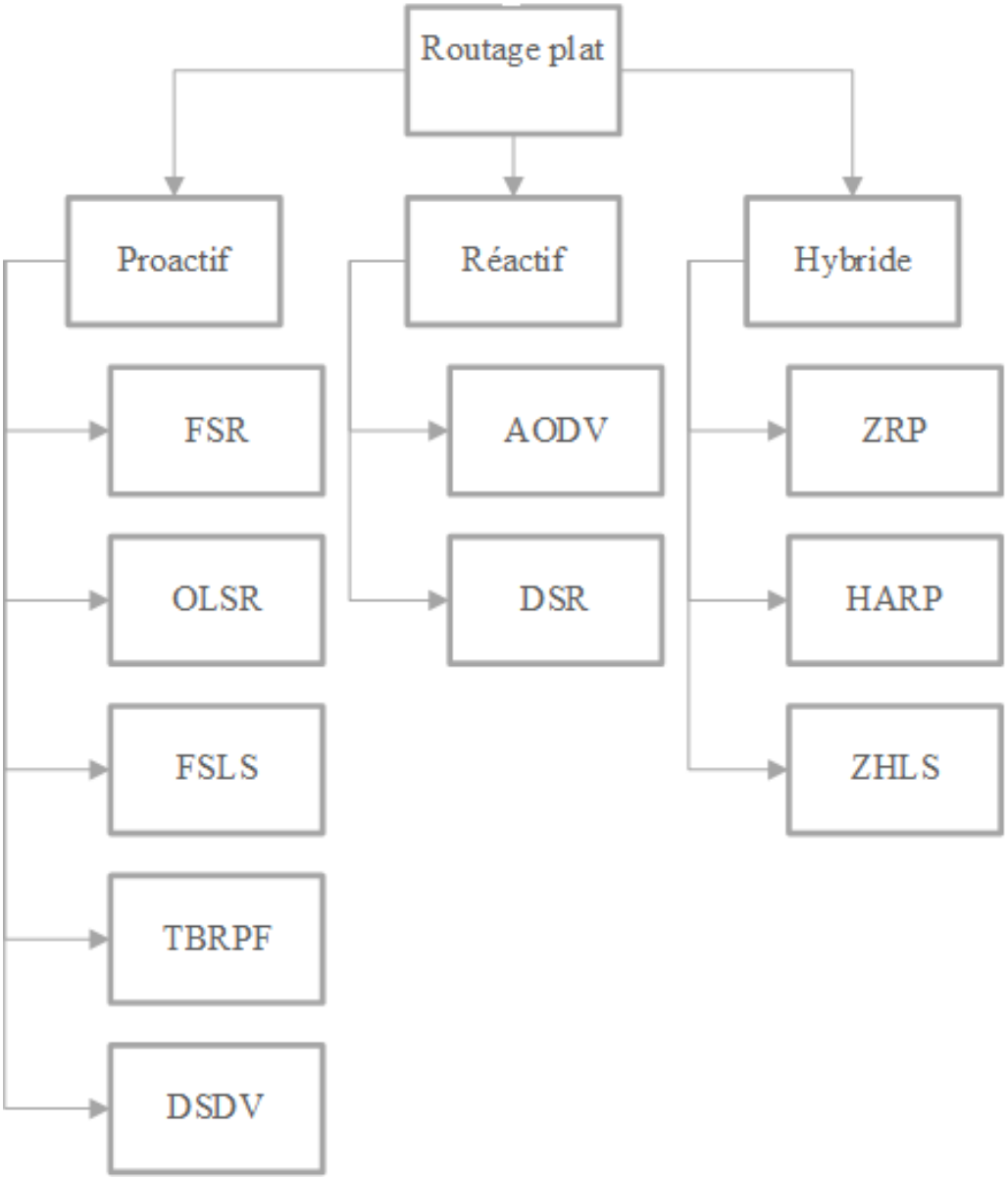

Figure I.3 – Classification des protocoles de routage(Khalid.K al, 2020)

I.3.3.2 Protocoles de routage proactifs

Les procédures de création et de maintenance des routes durant la transmission des paquets de données sont contrôlées périodiquement. Ces protocoles essaient de maintenir les meilleurs chemins existants vers toutes les destinations possibles au niveau de chaque nœud du réseau. Les routes sont sauvegardées et actives dans quelques tables même si elles ne sont pas utilisées. La mise à jour permanente de ces dernières est assurée par un échange continu de messages. Lorsqu'un nœud reçoit un paquet de contrôle, il met à jour ses tables de routages. Ainsi, de nouvelles routes seront construites sur la base des informations topologiques transportées par

les trames de contrôle. Ce processus est déclenché aussi à chaque changement de topologie pour reconstruire à nouveau les routes. (Mbarushimana.C al, 2007)
Le trafic induit par les messages de contrôle et de mise à jour des tables de routage peut être important et partiellement inutile. Ce qui gaspille la capacité du réseau sans fil. De plus, la taille des tables de routage croit linéairement en fonction du nombre de nœuds. Parmi les protocoles de routages proactifs les plus connus on citera : DSDV (Fahad Taha al, 2018), OLSR (Thomas.C al, 2003), FSR, WRP, GSR, HSR, LSR, DREAM. (Saika, A, 2010)(Yadav, 2017)..etc.

I.3.3.3 Protocoles de routage réactifs

Les protocoles réactifs également appelés protocoles à la demande, se basent sur la découverte et le maintien des routes. Suite à un besoin, une procédure de découverte globale de routes est lancée. Ce processus s'arrête une fois la route trouvée ou toutes les possibilités sont examinées. Dès que la communication est établie, cette route est maintenue jusqu'à ce que la destination devienne inaccessible ou jusqu'à ce que la route ne soit plus désirée.
Ces protocoles peuvent être classifiés en deux catégories : routage source et routage saut-par-saut. Dans les protocoles à routage source, les paquets de données portent dans leurs entêtes les adresses de tous les nœuds constituant le chemin à partir de la source jusqu'à la destination. De ce fait, les nœuds intermédiaires acheminent les paquets selon les informations qui se trouvent dans l'entête de chaque paquet de données. Les nœuds intermédiaires n'ont pas besoin de maintenir des informations sur les chemins actifs. De plus, ils n'ont pas besoin de maintenir la connectivité avec leurs voisins. (Kaur al, 2013)
Dans le routage saut-par-saut, chaque paquet de données porte uniquement l'adresse de la destination et celle du saut prochain. De ce fait, chaque nœud intermédiaire utilise sa table de routage pour acheminer chaque paquet de données. Le trafic de contrôle des protocoles réactifs est réduit. Les nœuds du réseau ne génèrent aucun trafic de contrôle sans qu'il soit nécessaire. Ceci permet de réduire la charge du trafic dans le réseau.
Parmi les protocoles basés sur ce principe on cite : DSR, AODV (Fahad Taha al, 2018), TORA (Yadav, 2017)... etc.

I.3.3.4 Protocoles de routage Hybrides

Les protocoles de routage hybrides combinent les deux approches de routage réactif et proactif. Le routage à l'intérieur des zones est assuré par un protocole de routage proactif alors

que le routage entre les zones est assuré par un protocole de routage réactif.
Ils utilisent un protocole proactif, pour apprendre le proche voisin. Ils disposent des routes immédiatement dans le voisinage. Au-delà de cette zone prédéfinie, le protocole hybride fait appel aux techniques des protocoles réactifs pour chercher des routes. Avec ce découpage, le réseau est partagé en plusieurs zones, et la recherche de route en mode réactif peut être améliorée. (Kaur al, 2013) A la réception d'une requête de recherche réactive, un nœud peut indiquer immédiatement si la destination est dans le voisinage ou non, et par conséquent savoir s'il faut diriger la requête vers les autres zones sans déranger le reste de sa zone. Il existe plusieurs protocoles hybrides on citera : ZRP et ZHLS (Yadav, 2017)... etc

I.4 Sécurité des réseaux Ad-hoc

La sécurité informatique est un ensemble de techniques assurant que les ressources (matérielles ou logicielles), d'un système d'information d'une organisation donnée, sont utilisées uniquement dans le cadre où il est prévu qu'elles le soient (Giordano Urpi, 2005).

I.4.1 Sécurité des réseaux ad-hoc

L'un des problèmes importants dans les réseaux filaires ainsi que pour les réseaux ad hoc est la sécurité. Les réseaux ad hoc sont beaucoup plus vulnérables aux attaques que les réseaux câblés en raison de leurs contraintes, notamment la faible puissance, le changement dynamique et l'ouverture de la topologie de réseau, la décentralisation et la faible puissance de la batterie. Les caractéristiques uniques des réseaux ad hoc présentent elles-mêmes un nouvel ensemble de défis non triviaux pour la conception de la sécurité, qui comprend une architecture de réseau ouverte, un support sans fil partagé, des contraintes de ressources strictes, une topologie de réseau hautement dynamique et bien d'autres (Giordano Urpi, 2005) (Sarika et al., 2016). La sécurité du réseau ad hoc est basée essentiellement sur les exigences de sécurité et les types d'attaques. La taxonomie de la sécurité du réseau ad hoc est donnée dans la Figure 1.4

I.4.2 Besoins de sécurité

Les besoins de base en sécurité pour les MANET sont plus ou moins les mêmes que pour les réseaux filaires ou sans fil avec infrastructure. Dans ce qui suit les concepts fondamentaux des services de sécurité (Sarika et al., 2016) :

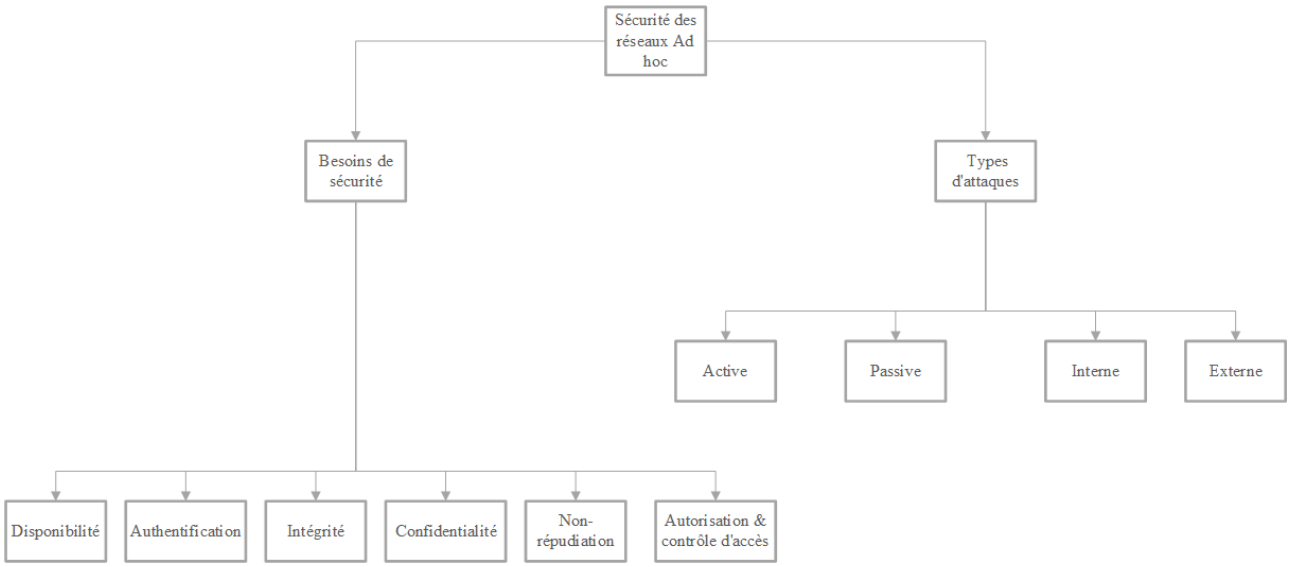

Figure I.4 – Besoins sécurité et types d'attaques dans les réseaux MANET (Khalid.K al, 2020)

Authentification : Consiste à vérifier l'identité d'un nœud ou d'une entité dans le réseau. L'absence d'authentification permet facilement à un nœud malicieux d'usurper l'identité d'un autre nœud dans le but de bénéficier des privilèges attribués à ce nœud ou d'effectuer des attaques sous l'identité de ce nœud.

Confidentialité : C'est un service essentiel pour assurer une communication privée entre les nœuds. C'est une protection contre les menaces qui peuvent causer la divulgation non autorisée d'informations alors qu'il faut veiller au caractère privé de l'information. Elle est principalement basée sur la cryptographie, en particulier les algorithmes de chiffrement.

Intégrité : Il garantit que personne ne pourrait empiéter et altérer les données transférées via le réseau. Le récepteur des données doit d'abord confirmer que l'expéditeur des données est celui qui est authentifié et non pas malveillant ou compromis. Cela est dû au fait qu'un nœud compromis enverra éventuellement des données falsifiées. En d'autres termes, les données envoyées par un nœud malveillant ou les données corrompues par des problèmes de propagation doivent être évitées immédiatement.

Non-répudiation : Le terme « non-répudiation » signifie que deux entités communicantes ne peuvent pas se nier l'une l'autre ou leurs messages. Il est bénéfique pour l'identification et la suppression des nœuds malveillants. Par exemple, lorsque le nœud A reçoit un message involontaire du nœud B, puis en utilisant le même message, le nœud A peut identifier le nœud B comme malveillant via la non-répudiation et notifier également les autres nœuds..

Disponibilité : C'est assurer la continuité du service fourni par un nœud même en présence

d'une attaque. Pour assurer à tous les nœuds l'accès aux ressources réseau tel que le routage, l'accès aux données, la protection contre les menaces qui peuvent causer la perturbation des fonctions du réseau est fortement nécessaire,

I.4.3 Défis de sécurité

Les caractéristiques distinctes des réseaux ad hoc ont posé quelques défis liés à la sécurité qui pourraient être pris en compte lors de la conception d'un protocole de sécurité pour ces réseaux.

- ▷ **Menaces :** un certain nombre d'attaques allant des attaques passives (écoute clandestine) aux attaques actives (interférence) sont attendues sur les liaisons en raison de la nature ouverte des médias sans fil. Aussi, sur ces réseaux, des attaques de toutes parts sont susceptibles de se produire, contrairement aux réseaux fixes filaires protégés par des pare-feux. Les dommages possibles peuvent inclure des fuites d'informations, l'usurpation d'identité de nœud et des altérations de message. Les solutions de sécurité devraient envisager des remèdes à toutes ces menaces.
- ▷ **Sécurité physique :** les nœuds des réseaux ad hoc sont indépendants et disposent d'une sécurité physique de faible niveau. Par conséquent, ils peuvent être compromis ou piratés plus facilement. Les solutions de sécurité peuvent prendre en compte les attaques malveillantes attendues internes et externes. Ces attaques provenant de nœuds malveillants sont difficiles à identifier car il est difficile de suivre ces nœuds dans la masse des nœuds des réseaux ad hoc.
- ▷ **Nature dynamique :** les solutions de sécurité avec des configurations statiques sont inadéquates pour la topologie dynamique du réseau. Les systèmes de sécurité distribués sont nécessaires car les solutions de sécurité centralisées ne sont plus acceptables.

I.4.4 Classification des attaques

Dans les MANET, selon le niveau d'intrusion et les actions menées par un attaquant, on distingue généralement deux catégories d'attaques : les attaques passives et les attaques actives (Sbai Elboukhari, 2018) (Bhattacharyya et al., 2011).

I.4.4.1 Attaque passive

Dans les attaques passives, le protocole de routage n'est pas perturbé. Des informations précieuses telles que la hiérarchie des nœuds et la topologie du réseau sont obtenues. Le but de l'attaquant est d'obtenir des informations en cours de transmission. Les attaques passives sont très difficiles à identifier car elles n'impliquent aucune modification des données.

Ecoute clandanstine (Eaves Dropping) : Le but de l'écoute clandestine est d'obtenir des informations confidentielles lors de la communication. Les informations confidentielles peuvent inclure l'emplacement, la clé publique, la clé privée ou même les mots de passe des nœuds. Il est essentiel que ces données soient cachées aux personnes non autorisées.

Analyse du trafic (Traffic Analysis) : Dans cette attaque, l'attaquant scrute le trafic, détermine l'emplacement, découvre les hôtes communicants, détecte la fréquence et la longueur du message en cours d'échange. Ces informations sont utilisées pour prédire la nature de la communication. Tout le trafic entrant et sortant du réseau n'est pas modifié.

Surveillance (Monitoring) : Les nœuds sont surveillés. Les transactions par paquets et les autres activités du nœud sont vérifiées et auditées

I.4.4.2 Attaque Active

Les attaques actives sont les attaques effectuées par les nœuds malveillants. De plus, ces nœuds consomment de l'énergie pour effectuer les attaques. Les attaques actives impliquent certains changements de données ou la création de fausses informations. Les attaques suivantes entrent dans la catégorie des attaques actives :

Trous d'évier (Sink holes) : Un nœud compromis tente d'attirer les données vers lui, à partir de tous les nœuds voisins. Le nœud écoute toutes les données communiquées entre ses nœuds voisins. Ces attaques peuvent également se produire sur des réseaux ad hoc tels que AODV en utilisant des techniques telles que la maximisation du numéro de séquence ou la minimisation du nombre de sauts.

Déni de service (DOS) : Les attaques DoS (Denial of Service) sont effectuées en inondant une sorte de trafic réseau vers la cible. Cela épuise la puissance de traitement de la cible et rend les services fournis par la cible indisponible. La nature distribuée des services le rend impraticable. De plus, les réseaux mobiles ad hoc sont plus vulnérables que les réseaux filaires. Le canal radio sujet aux interférences et la puissance limitée de la batterie sont à l'origine de cette vulnérabilité.

Attaque de trou de ver (Wormhole Attack) : Les attaques de trous de ver sont des

menaces graves pour les protocoles de routage. Lorsque l'attaquant enregistre un paquet à un endroit et le redirige vers un autre emplacement, le routage est interrompu. Cela se produit en raison de la redirection. Ces mésaventures sont appelées attaques wormhole. (Bhattacharyya et al., 2011)

Usurpation d'identité (Spoofing) : L'usurpation d'identité se produit lorsqu'un nœud malveillant se fait passer pour un autre nœud. Il le fait pour modifier la vision de la topologie du réseau qu'un nœud innocent peut rassembler(Bhattacharyya et al., 2011). L'usurpation d'identité est également appelée l'homme du milieu. L'attaquant y parvient en affichant son IP comme l'adresse IP du nœud qu'il veut agir.

Fabrication : Les attaques effectuées en générant de fausses informations de routage sont de la fabrication. Celles-ci sont difficiles à identifier car elles se présentent comme des constructions de routage valides, en particulier en cas d'erreur. Ils affirment qu'un voisin ne peut plus être contacté.

Attaque Sybil : Lorsqu'un nœud se fait passer pour un groupe de nœuds, on parle d'attaque Sybil. Il s'agit d'une attaque complexe car un nœud dépend de nombreux nœuds intermédiaires pour la communication, et il existe donc des algorithmes redondants pour assurer la livraison des données. Cependant, si un seul nœud malveillant est capable de représenter plusieurs nœuds, cela devient plus simple pour l'attaquant. Désormais, les nœuds de destination ne peuvent pas interpréter la modification des paquets. De fausses recommandations sur l'intégrité d'une certaine partie peuvent également être délivrées, attirant ainsi plus de trafic vers elle. (Bhattacharyya et al., 2011)

Attaque de trou noire (Black-Hole attack) : Le trou noir est un type d'attaque qui peut être facilement utilisée dans le processus de routage. Elle apparait quand un nœud refuse de coopérer dans le processus de routage. En effet, les nœuds égoïstes refusent de relayer les messages de contrôle des autres nœuds et qui sont destinés à être diffusés dans le réseau entier.(Alnadhery Baneamoon, 2020 ; khamayseh et al., 2011 ; Sen, 2011)

Dans cette attaque :

- ▷ Le nœud malveillant détecte l'existence d'une route active et prend note de l'adresse de la destination.
- ▷ Le nœud malveillant prépare un paquet route réponse (RREP) dans lequel : le champ d'adresse de destination est défini sur l'adresse de destination falsifiée, le numéro de séquence est fixé à une plus grande valeur et le nombre de sauts est mis à une petite

valeur.

- ▷ Le nœud malveillant envoie cette réponse RREP vers le nœud intermédiaire le plus proche appartenant à la voie active réelle (pas nécessairement vers le nœud source lui-même).
- ▷ La réponse de route RREP reçue par le nœud intermédiaire sera retransmise au moyen de chemin inverse pré-établi vers le nœud source de données.
- ▷ Le nœud source met à jour sa table de routage par les nouvelles informations reçues dans la réponse de route.
- ▷ La source utilise la nouvelle route à l'envoi de données.
- ▷ Le nœud malveillant commence à ignorer les données de la route à laquelle il appartient.

Attaque du trou gris (Grey Hole Attack) : Un cas spécial dans l'attaque de trou noir est l'attaque de trou gris. Elle peut être vue comme la variation de l'attaque de base du trou noir dans laquelle les paquets sont déposés sélectivement. Généralement, ces attaques sélectives vers l'avant sont principalement de deux types.(Bhattacharyya et al., 2011)
1- Transfert de tous les paquets TCP mais suppression de tous les paquets UDP.
2- Lorsque 50% des paquets sont abandonnés ou abandonnés avec une distribution probabiliste, cela semble perturber le réseau et les mesures de sécurité sont incapables de le détecter.
Dans l'attaque trou gris, une attaque peut ignorer les paquets provenant d'une seule source ou d'une adresse IP ou d'une plage d'adresses IP et transmettre les paquets de données restants. Les nœuds du trou gris sont très efficaces. Dans le trou gris, chaque nœud du réseau enregistre les activités dans la table de routage et gère une table sur tous les nœuds voisins pour acheminer un paquet de données vers le nœud final ou le nœud souhaité, et lorsque le nœud source souhaite acheminer un paquet vers le nœud de destination, il vérifie la table de routage si une route spécifique y est présente ou non. Sinon, il utilise la découverte d'itinéraire

I.4.4.3 Autre types de classification d'attaques

Attaque externes ou internes : Selon le domaine d'appartenance d'un nœud, les attaques actives peuvent elles mêmes être classées en deux catégories, à savoir les attaques externes et internes (Yasin Abu Zant, 2018). Un attaquant interne est celui qui arrive à contrôler le réseau, c'est à dire, un nœud interne ayant le statut d'un membre du réseau et qui dispose d'un ensemble de connaissances associe à ce statut (clé secret, table de routage . . .). Les attaques internes sont menées par des nœuds compromis qui sont autorisés à participer au fonctionnement du réseau.

Les attaques internes sont généralement plus dangereuses et difficiles à détecter que les attaques externes. Tandis que les attaques externes sont réalisées par des nœuds qui n'appartiennent pas au domaine de réseau. Un attaquant externe ne dispose pas à priori des connaissances mais il est capable d'effectuer des opérations cryptographiques pour empêcher le réseau de communication de produire une charge supplémentaire.

Attaque individuelle ou attaque distribuée : En effet, les attaques peuvent être de type individuelles ou par collusion avec d'autres participants qui sont appelées également distribuées. Les attaques individuelles sont menées par un seul nœud attaquant. Puisque les capacités de communication et de calcul de l'attaquant sont en général similaires à celles des autres nœuds du réseau, ces attaques demeurent relativement simples, et sont d'autant plus limitées par rapport aux mécanismes de sécurité qui sont mis en œuvre. En revanche, rien n'empêche à des nœuds attaquants de mutualiser leurs informations et leurs ressources, en exploitant les connexions qu'ils ont entre eux. Ces attaques distribuées, nécessitant plusieurs nœuds répartis à différents endroits dans le réseau, sont généralement plus évoluées et plus dangereuses. Par ailleurs, en raison de l'intervention de plusieurs nœuds intermédiaires, leur détection et l'identification précise de leurs origines sont plus complexes (Yasin Abu Zant, 2018).

I.4.5 Mécanisme de sécurité dans les réseaux MANET

En général, il existe deux types de techniques de sécurité dans MANET, notant la détection d'intrusion et les techniques de routage sécurisé. (Giordano Urpi, 2005) (Sarika et al., 2016)

I.4.5.1 Détection d'intrusion

Un système de détection d'intrusion *(Intrusion Detection System)* est un élément indispensable d'un système de sécurité qui est principalement introduit pour détecter d'éventuelles violations de la politique de sécurité en surveillant les activités du système et en répondant à celles qui sont apparemment intrusives. Si une attaque est détectée dans le réseau, une réponse est lancée pour éviter ou réduire les dommages au système.

Détection d'intrusion basée sur une mauvaise utilisation Signatures d'attaque de détection des IDS basées sur une mauvaise utilisation avec les activités actuelles du système. Ils sont généralement préférés par les IDS commerciaux car ils sont efficaces et ont un faible taux de faux positifs. Le principal inconvénient est qu'il ne peut pas détecter de nouvelles attaques. Il

est nécessaire de mettre à jour fréquemment la base de données, car le système n'est aussi solide que sa base de données de signatures.

Détection d'intrusion basée sur les anomalies Il détecte les intrusions comme des anomalies, c'est-à-dire des écarts par rapport aux comportements normaux. Les activités normales qui sont détectées comme des anomalies par un IDS peuvent être élevées dans ce type de détection et il est également capable de détecter des attaques inconnues.

Détection d'intrusion basée sur les spécifications Dans ce cas, les intrusions sont identifiées comme une violation d'exécution des termes des protocoles de routage. Ils sont généralement utilisés pour détecter les modifications et forger des attaques. Cependant, cette technique ne peut pas détecter les attaques qui ne violent pas directement les spécifications du protocole.

I.4.5.2 Routage sécurisé

Il existe de nombreux types d'attaques contre la couche de routage dans les MANET, dont certaines sont plus sophistiquées et plus difficiles à détecter que d'autres, telles que les attaques Wormhole et les attaques Rush.

Watchdog et Pathrater Watchdog et Pathrater augmentent les performances de MANET en présence de nœuds qui se comportent mal. Watchdog identifie un mauvais comportement en stockant les paquets à transmettre dans une mémoire tampon et il se faufile de manière promiscueusement pour décider si le nœud voisin transmet les paquets sans altération ou non. Si les paquets qui sont furtivement correspondent au tampon du nœud d'observation, puis ils sont rejetés. Alors que les paquets qui résident dans la mémoire tampon au-delà d'un délai d'expiration sans aucune correspondance réussie sont marqués comme ayant été abandonnés ou modifiés. Le nœud responsable de la transmission du paquet est alors noté comme suspect. Si le nombre d'infractions devient supérieur à un certain seuil prédéterminé, le nœud est marqué comme malveillant. Les informations sur les nœuds malveillants sont transmises au composant Pathrater pour être incluses dans l'évaluation du chemin (Augustine James, 2015).

Pathrater sur un nœud séparé fonctionne pour évaluer tous les nœuds bien connus dans un réseau particulier. Les évaluations sont établies et mises à jour du point de vue d'un nœud particulier. Les nœuds commencent avec une évaluation non biaisée qui est modifiée au fil du temps en fonction du comportement observé lors de la transmission de paquets. Les nœuds qui sont observés par le watchdog comme ayant mal agi reçoivent une note immédiate de -100. Il convient de différencier le fait qu'une mauvaise conduite est détectée comme une mauvaise

gestion / modification de paquet, tandis qu'un comportement non fiable est détecté comme une rupture de liaison (Augustine James, 2015).

Une approche de routage ad hoc sécurisée utilisant des communautés d'auto-guérison localisées : Le concept de *« communauté auto-réparatrice »* est basé sur l'examen selon lequel la transmission des paquets dépend généralement de plus d'un voisin immédiat. La sécurité basée sur la communauté s'intègre dans la redondance des nœuds à chaque étape de transfert, de sorte que la transmission conventionnelle basée sur les nœuds système est parfaitement convertie en un nouveau système de transfert par communauté. Puisqu'une communauté d'auto-guérison n'a de sens que lorsqu'il y a au moins un « bon » nœud coopératif dans la communauté.

Plusieurs techniques de routage aident à sécuriser le routage ad hoc. Certaines d'entre elles traitent des attaques spécifiques qui visent à perturber les services de routage ad hoc, et fournissent des solutions pour aider à se défendre contre ces attaques tandis que d'autres techniques tentent de fournir des outils ou des schémas efficaces pour protéger les services de routage ad hoc de toutes sortes d'attaques. Étant donné que le service de routage est l'un des services réseau les plus importants dans les MANET, il peut y avoir de nouveaux types d'attaques émergents contre ce type de routage.

I.5 Conclusion

Dans ce chapitre, nous avons donné une vue générale sur les MANET, leurs caractéristiques, leurs utilisations. Nous avons présenté les différentes techniques de rouratge dans ces réseaux. Nous avons, aussi, mis l'accent sur le problème de sécurité dans les MANET. Les différentes vulnérabilités des MANET, ainsi que les attaques possibles qui peuvent survenir ont été aussi étudiées.

L'étude faite dans ce chapitre, nous aidera à comprendre les méthodes sous-jacentes, les lacunes des systèmes existants pour permettre d'avoir une idée claire de la direction dans laquelle notre travail de recherche devrait se poursuivre pour développer un système efficace avec des fonctionnalités performantes.

CHAPITRE II

SYSTÈMES DE DÉTECTION D'INTRUSION

II.1 Introduction

Aujourd'hui, la sécurité du réseau est devenue importante en raison de l'utilisation croissante des ordinateurs. Chaque jour, les utilisateurs sont soumis à de nouveaux types d'attaques, il est donc essentiel de les alerter de toute activité malveillante se déroulant sur le réseau. Comme la menace devient un problème sérieux de jour en jour, il est nécessaire de mettre en œuvre un système qui réalise une détection et une réponse plus rapides des attaques pour protéger les données qui sont échangées sur le réseau. Pour le partage de biens confidentiels, privés, publics ou commerciaux utilisant la connexion Internet, la protection de ces biens contre les attaques intrusives est primordiale.

Le système de détection d'intrusion (IDS) joue un rôle important dans la sécurité du réseau, et c'est un domaine de recherche primordial de nos jours. L'apparition d'événements illégaux dans un système informatique ou dans un réseau est appelé intrusion, et diagnostiquer de tels événements comme illégaux est appelé détection (Gupta al, 2008). La détection d'intrusion fait référence à l'analyse des événements qui se produisent dans un système informatique ou dans un réseau et à la vérification si l'événement est normal ou nuisible.(Bhati al,2019)

II.2 Procédures de détection d'intrusion

La première phase du processus de détection d'intrusion est l'accumulateur de données dans lequel les événements sont générés sur la base des données du journal. Ces données de journal sont formées à l'aide des données collectées par le système cible. Les données peuvent être le trafic réseau, les journaux du système d'exploitation ou les journaux des applications. Les données stockées dans le référentiel de configuration sont ensuite utilisées dans la phase de détection d'intrusion. Dans la détection d'intrusion, plusieurs analyseurs travaillent simultanément sur les mêmes données. Ils appliquent plusieurs scripts de correspondance pour faire correspondre les chaînes de texte, qui sont uniques à diverses intrusions. Cette phase est similaire à divers antivirus dans lesquels le code malveillant est comparé à diverses signatures présentes dans la base de données. Il existe d'autres moyens d'effectuer une détection, comme la détection d'un comportement anormal dans le trafic réseau, mais ce type de techniques peut entraîner de nombreuses fausses alarmes. Le référentiel de protocoles de détection contient les règles et les algorithmes permettant de détecter et de prévenir les intrusions. Les principales informations

sur la détection d'intrusion qui doivent être envoyées à l'unité de réponse sont stockées dans le protocole de détection. L'unité de réponse où la réponse contient ces types de données qui sont de nature intrusive, et elles doivent être manipulées avec soin. La réponse est générée pour ces données à l'aide d'instructions de réponse (*Reply Statements*) qui sont présentes dans le référentiel de protocole de réponse. La décision sur la manière de répondre à plusieurs événements est prise par l'unité de réponse principale et la base de données du protocole de réponse. L'unité de réponse peut recevoir plusieurs entrées de différents analyseurs dans un environnement distributif, et ainsi, elle peut collaborer sur toutes les alarmes provenant de la soumission principale. Afin d'aider l'administrateur, l'unité de réponse peut effectuer certaines tâches après avoir détecté une intrusion, comme créer une alarme pour avertir le contrôleur, configurer pour arrêter le système ou couper la connexion d'où provient le trafic malveillant. (Bhati al,2019)

II.3 Taxonomie des systèmes de détection d'intrusion

Plusieurs taxonomies existent dans le domaine de détection d'intrusion (H.J. Liao al, 2013). Il ressort clairement de la figure II.1 que l'IDS peut être classé en différents groupes selon différentes perspectives notant : les mécanismes de détection, la réponse de détection, la source de données, mode de détection, architecture réseau, fréquence d'utilisation, type de données et collecte de données. La Figure II.1 montre la taxonomie la plus formelle et générale. Dans cette section, nous allons décris les différents systèmes de détection d'intrusion.

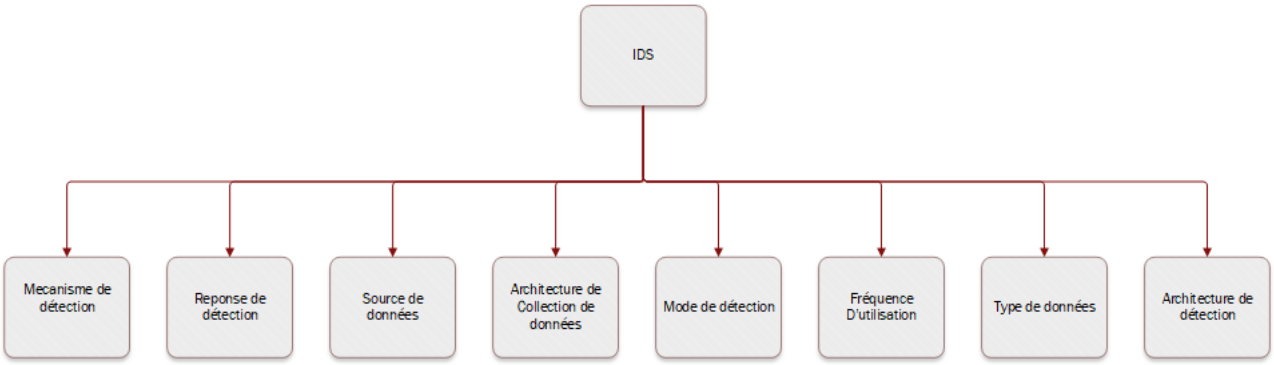

Figure II.1 – Taxonomie des systèmes de détection d'intrusion

II.3.1 IDS basé sur un mécanisme de détection

Les IDS peuvent être regroupés en trois grandes catégories (Figure II.2) en fonction du mécanisme utilisé pour la détection, qui est basé sur la signature ou l'utilisation abusive, l'analyse basée sur les anomalies et l'analyse de protocole avec état ou la spécification (C. Xenakis al, 2011). Plus tard, un nouveau mécanisme est apparu, hybride en combinant les trois mécanismes. Les avantages et les inconvénients de chacun d'eux sont également donnés dans le tableau II.1.

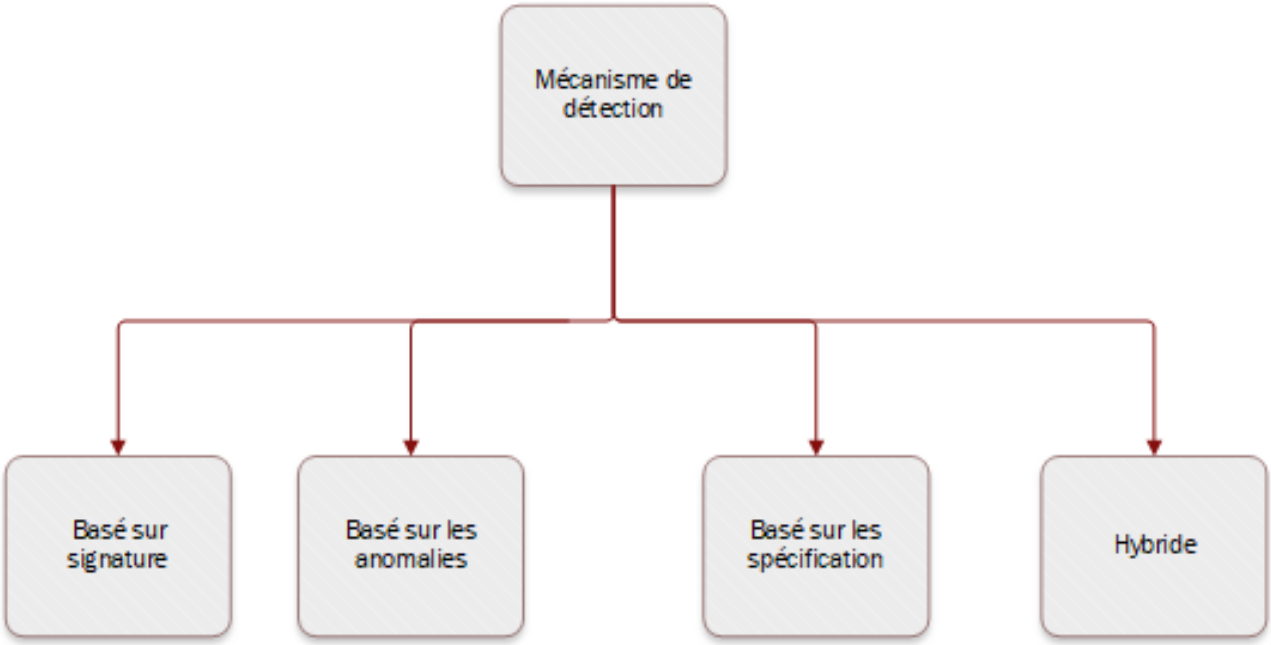

Figure II.2 – IDS basé sur un mécanisme de détection

II.3.1.1 IDS basé sur la signature

Une signature est essentiellement un modèle (chaîne) ou une combinaison de modèles qui se rapporte à une menace déjà connue. La détection de signature correspond en fait aux modèles stockés avec la menace détectée. Si la correspondance s'est produite ; une intrusion est détectée (X.D. Hoang al, 2009). Il est également appelé basé sur les connaissances, car le mécanisme utilise les connaissances stockées dans sa base de données pour reconnaître les intrusions. En d'autres termes, lorsque l'IDS utilise des informations stockées pour reconnaître les attaques, on parle alors de détection d'intrusion basée sur la connaissance. Selon (T.S. Sobh, 2006), l'IDS basé sur les signatures est plus probablement un antivirus qui pourrait détecter efficacement les modèles connus mais ne parvient pas à détecter de nouvelles attaques ou de nouveaux virus.

Le collecteur de trafic collecte des données provenant de diverses sources telles que le trafic réseau et/ou les fichiers journaux (journal de l'hôte, journal des applications). Le collecteur de trafic envoie les données suspectes à l'IDS basé sur la signature concernée. L'IDS analyse les données à la recherche de menaces et de vulnérabilités. Cette analyse implique la comparaison des données avec les signatures de menaces déjà connues. Ces signatures sont fournies par la base de signatures (signatures DB). Si la signature des menaces connues correspond à la menace trouvée dans les données d'audit, l'IDS bloque instantanément la menace et une alarme est générée. L'administrateur système est également informé de l'occurrence d'une attaque. D'autre part, si la signature des menaces connues ne correspond pas aux données infectées suspectées, le système est autorisé à poursuivre son fonctionnement habituel et l'administrateur système est informé que l'attaque suspectée n'est pas une attaque réelle.

II.3.1.2 IDS basé sur les anomalies

Ce mécanisme est également appelé IDS basé sur le comportement dans de nombreux articles. L'écart par rapport au comportement notoire est appelé anomalie, tandis que le profil est le comportement normal attendu qui est dérivé sur une période de temps de la surveillance de la connexion réseau, des hôtes ou des activités régulières. Ainsi, les approches basées sur les anomalies comparent les activités en cours avec le profil de comportement normal existant. Lorsque l'écart dépasse un seuil spécifié, une alarme est générée. Les modèles basés sur les anomalies détectent les intrusions avec précision avec moins de taux de fausses alarmes négatives et positives (O. Kachirski al, 2003). Le profil peut être statique ou dynamique. Il est développé pour des attributs tels que le nombre d'e-mails envoyés, l'utilisation du processeur et les tentatives de connexion qui ont échoué. Ce mécanisme comprend deux phases : l'apprentissage et la détection. Dans la phase d'apprentissage, l'IDS doit d'abord apprendre les comportements normaux, puis il est autorisé à démarrer la phase de détection (V. Chandola al, 2009). Les IDS basés sur les anomalies sont en outre divisés en trois groupes principaux tels que ceux basés sur les statistiques, basés sur l'exploration de données et basés sur l'apprentissage automatique (P.G. Teodoro al, 2009). Les données entrantes sont analysées par l'IDS. Si un comportement suspect est détecté, alors IDS consulte le référentiel de profils normaux (base de données de profils normaux). Après analyse, si le comportement est marqué comme normal par l'IDS, alors la situation est qualifiée de fausse alarme. D'autre part, si le comportement suspecté ne correspond pas aux profils normaux stockés, l'IDS marque ce comportement comme profil

anormal. L'IDS envoie alors ce profil anormal à l'analyseur de menaces. L'analyseur de menaces consulte la base de données des menaces connues pour identifier la menace comme menace connue ou menace inconnue. Si la menace est marquée comme connue, l'alarme est générée instantanément. L'alarme est également déclenchée si la menace est marquée comme inconnue. Le rapport est envoyé à l'administrateur système concernant la menace (connue ou inconnue). En cas de menace inconnue, l'administrateur l'envoie à l'apprenant. L'apprenant apprend le comportement de cette nouvelle menace et l'envoie à la base de données de menaces connues à des fins de stockage.

II.3.1.3 IDS basé sur les spécifications

Ce mécanisme est également appelé analyse de protocole avec état car l'IDS utilisant ce mécanisme connaît en fait l'état du protocole. La spécification signifie un ensemble de règles et de seuils définis pour le comportement prévisible des modules de réseau tels que les protocoles, les nœuds et les tables de routage. Les approches détecteront l'intrusion lorsqu'une déviation du comportement du réseau est détectée par rapport au comportement spécifié pour celui-ci. Les approches basées sur les spécifications et sur les anomalies ont le même objectif de détection des anomalies. Mais la différence de signification entre ces deux est que, dans l'approche basée sur les spécifications, les règles sont définies manuellement pour chaque spécification par un expert humain (J. Amaral al, 2014). Une autre différence principale entre ces deux types d'IDS est que l'IDS basé sur les anomalies détecte l'effet des comportements anormaux tandis que l'IDS basé sur les spécifications détecte les comportements anormaux connus. La définition manuelle des règles de spécification crée des taux de faux positifs inférieurs par rapport aux approches basées sur les anomalies (I. Butun al, 2014). Cependant cette méthode est chronophage et pleine de retards (M. Zeeshan al, 2017).

II.3.1.4 IDS hybride

Les schémas qui relèvent du groupe hybride utilisent la combinaison du mécanisme basé sur la spécification, l'anomalie et la signature afin d'améliorer l'IDS avec un minimum de défauts. Les approches hybrides utilisent nécessairement deux ou trois mécanismes d'IDS (O. Awodele al, 2009). Une approche hybride (M.A. Aydin al, 2009) combinait un IDS mal utilisé/basé sur la signature et sur les anomalies. La fréquence de détection passe de 27 à 146 attaques sur 201 attaques. D'autres travaux comme (G.V. Nadiammai al, 2013) combinent l'IDS statistique et

basé sur la signature et le taux de détection est augmenté de 77 à 149 attaques sur 180 attaques.

Approche	Avantages	Inconvénients
Basé sur les signatures	• Méthode simple, précise et efficace pour capturer les intrusions connues. • Donne une analyse contextuelle détaillée. • La protection est instantanée après l'application. • Détection rapide et solution fréquente.	• Impossible de détecter des attaques inconnues et des variantes d'attaques inconnues • Mises à jour fréquentes difficiles • Nécessite plus de temps pour maintenir les connaissances. • Compréhension limitée des protocoles et des états.
Basé sur les anomalies	• Utile pour les attaques inconnues. • Faible dépendance aux systèmes d'exploitation et autres logiciels système. • Fourni une installation pour la détection des abus privilégiés.	• Précision du profil est médiocre en raison des changements fréquents dans les événements observés. • Suspendre la disponibilité du service pendant la reconstruction du profil de comportement. • Fourniture en temps opportun de l'alarme est médiocre.
Basé sur les spécifications	• Forte emprise sur les états du protocole. • Distinguez facilement les séquences de commandes inattendues. • Taux de faux positifs plus faibles que les autres.	• Traçage fréquent et l'examen des états du protocole consomment des ressources. • Menaces avec violation indirecte du comportement du protocole sont difficiles à détecter. • Incompatible avec les systèmes d'exploitation et les points d'accès dédiés.
Hybride	• Développement flexible aux exigences. • Capable d'adopter n'importe quel mécanisme ou mécanisme de combinaison.	• Lourd pour les appareils à contraintes de mémoire. • Consommation d'énergie est importante en raison des frais généraux de calcul.

Table II.1 – Avantages et inconvénients des différents mécanismes de détection d'intrusion

II.3.2 IDS basé sur la réponse de détection

Les IDS peuvent également être classés en deux classes, à savoir les IDS actifs et les IDS passifs (Voir Figure II.3), en fonction de leur réponse lorsqu'une intrusion est détectée (R.

Janakiraman al, 2003). Un aperçu de ces IDS est présenté ci-dessous.

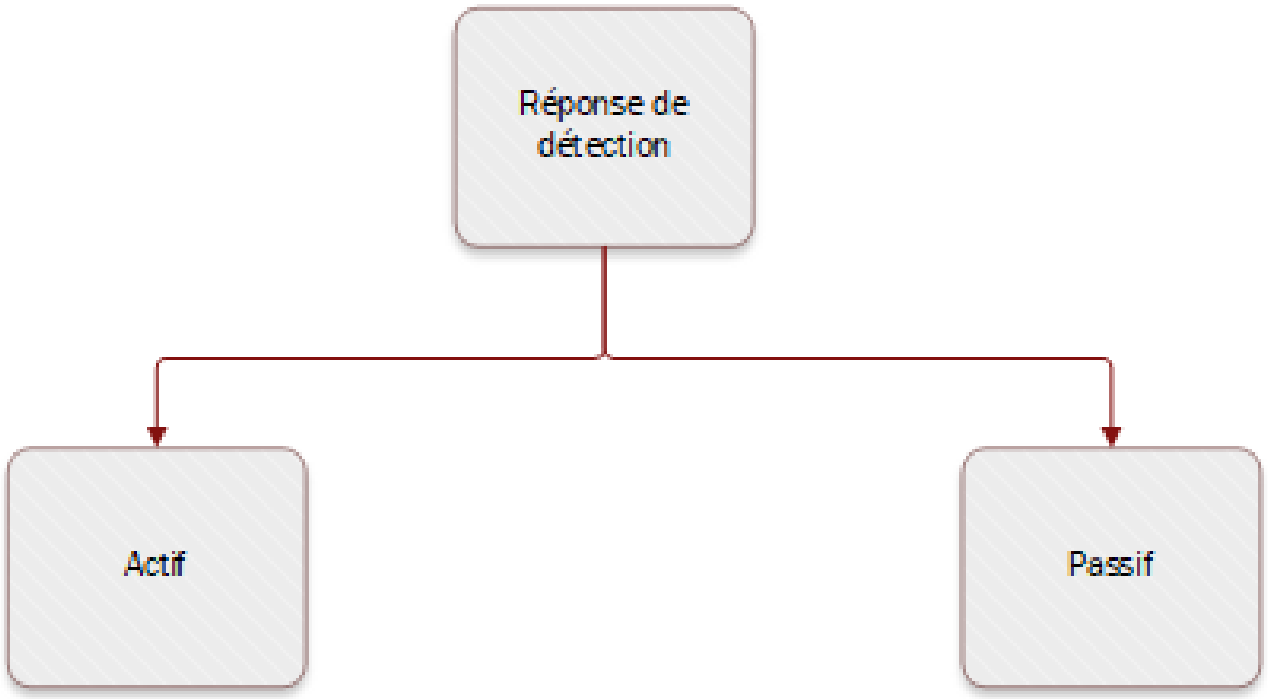

Figure II.3 – IDS basé sur la réponse de détection

II.3.2.1 IDS actif

Un IDS actif détecte les menaces dans un système ou un réseau et répond activement en bloquant ou en prévenant les menaces détectées. Étant donné que l'IDS actif lui-même empêche la menace après sa détection sans aide extérieure, il est donc également appelé système de détection et de prévention des intrusions (IDPS). Les systèmes IDSP sont réputés pour leur protection automatisée et sont largement utilisés pour protéger les systèmes en temps réel. Ils ont certaines limitations en raison des exigences d'énormes ressources de mémoire et de calcul.

II.3.2.2 IDS passif

Passive IDS, comme son nom l'indique, est un IDS qui surveille uniquement le réseau ou un système en silence et ne joue aucun rôle direct dans la prévention de la menace. Au lieu de cela, informez un administrateur ou toute autre entité responsable de bloquer la menace.

II.3.3 IDS basé sur la source de données

Les systèmes de détection d'intrusion sont classés en quatre types en fonction de la source des données(Voir Figure II.4). Ces types sont décrits un par un.

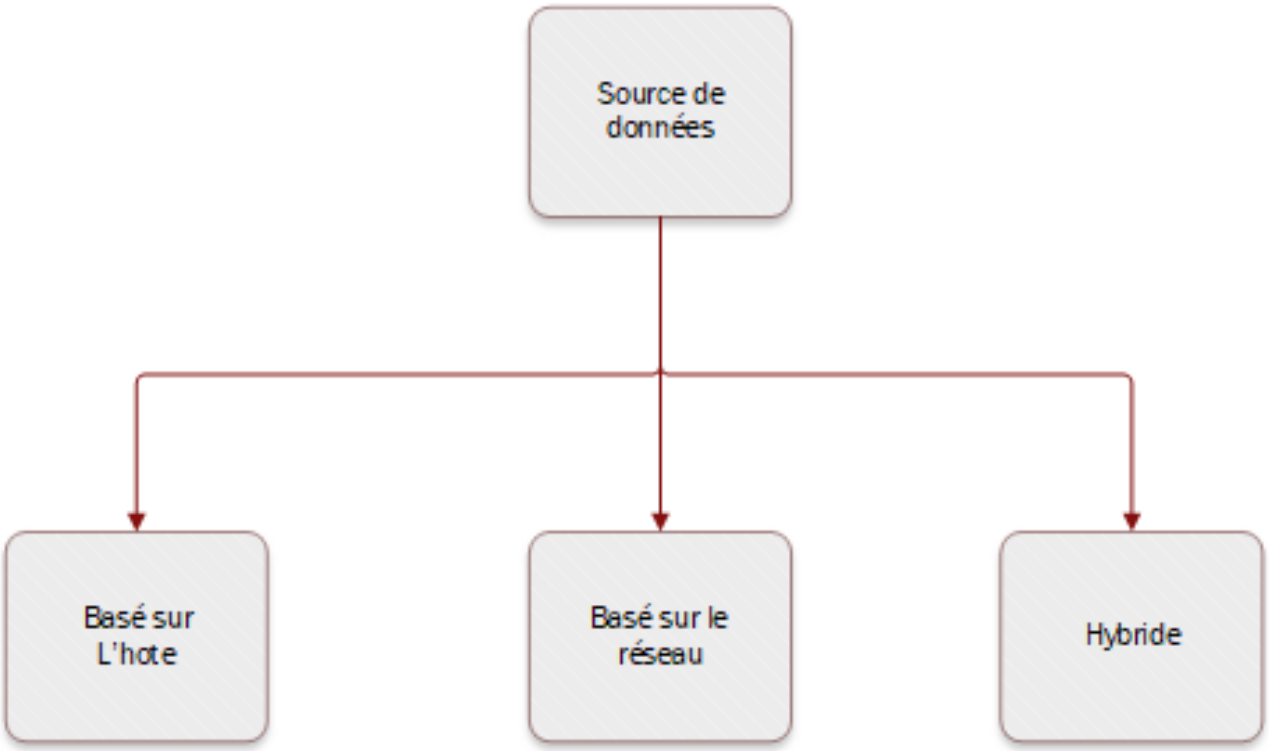

Figure II.4 – IDS basé sur la source de données

II.3.3.1 Système de détection d'intrusion basé sur l'hôte (HIDS)

Comme son nom l'indique, HIDS est installé sur un hôte ou un système et est chargé de surveiller et de prévenir les menaces sur cet hôte uniquement. De telles menaces peuvent affecter un système de plusieurs manières, notamment l'accès au système, la modification des fichiers système, l'occupation inutile de la mémoire du système et l'occupation permanente du processeur (L. Vokorokos al, 2010). Toutes ces activités sont destinées à rendre le système indisponible pour les tâches assignées. HIDS observe en permanence les fichiers journaux sur l'hôte pour prévenir de telles menaces. Une autre méthode pour protéger l'hôte consiste à surveiller l'utilisation du système en temps réel. Un tel système de détection d'intrusion bénéficie d'une stratégie de protection élevée. Il est très difficile pour un attaquant d'envahir directement le système. L'inconvénient du HIDS est le coût d'installation élevé, en particulier dans le cas de réseaux plus importants. C'est un fait que HIDS utilise les ressources de chaque hôte. Par conséquent, il

n'est pas attrayant pour les réseaux ad hoc à ressources limitées

II.3.3.2 Système de détection d'intrusion basé sur le réseau (NIDS)

Le système de détection d'intrusion réseau est destiné à détecter l'intrusion dans les données transmises par le réseau ou le sous-réseau aux utilisateurs rattachés. NIDS écoute passivement le traffic réseau et essaie de détecter les intrusions en comparant les données d'audit avec les menaces déjà connues stockées dans sa base de données. Si à n'importe quel moment une correspondance se produit, il génère une alarme et avertit l'administrateur concerné. La session d'analyse comprend l'analyse des paquets, de leurs charges utiles et de l'adresse IP et des ports. Un tel système de détection d'intrusion est moins cher en termes de coût d'installation par rapport au HIDS. Cependant, la surveillance du trafic sortant et entrant de l'ensemble du réseau entraîne un goulot d'étranglement des performances. De plus, ils provoquent également des retards de communication. Le NIDS souffre du problème du point de défaillance unique (V. Giovanni al, 1999).

II.3.3.3 Système de détection d'intrusion hybride

Pour surmonter les inconvénients mentionnés ci-dessus du HIDS et du NIDS, un autre système d'intrusion, à savoir le système de détection d'intrusion hybride, est développé, qui combine les fonctionnalités des deux IDS. Les IDS hybrides contiennent des agents qui jouent le rôle de communication entre HIDS et NIDS. Les agents mobiles visitent chaque hôte et effectuent le processus de détection en vérifiant les fichiers journaux du système. A côté des agents mobiles, il existe d'autres agents, à savoir des agents centraux qui parcourent l'ensemble du réseau pour détecter les anomalies de trafic.

II.3.4 IDS basé sur le mode de détection

En fonction du mode de détection, les IDS peuvent être divisés en deux sous-groupes tels que les IDS en ligne et les IDS hors ligne (Voir Figure II.5). La différence entre eux est indiquée ci-dessous.

II.3.4.1 IDS en ligne

Online IDS est une classe de taxonomie IDS dans laquelle le trafic réseau (entrant et sortant) est surveillé en permanence pour détecter les intrusions. Si une intrusion est détectée dans le

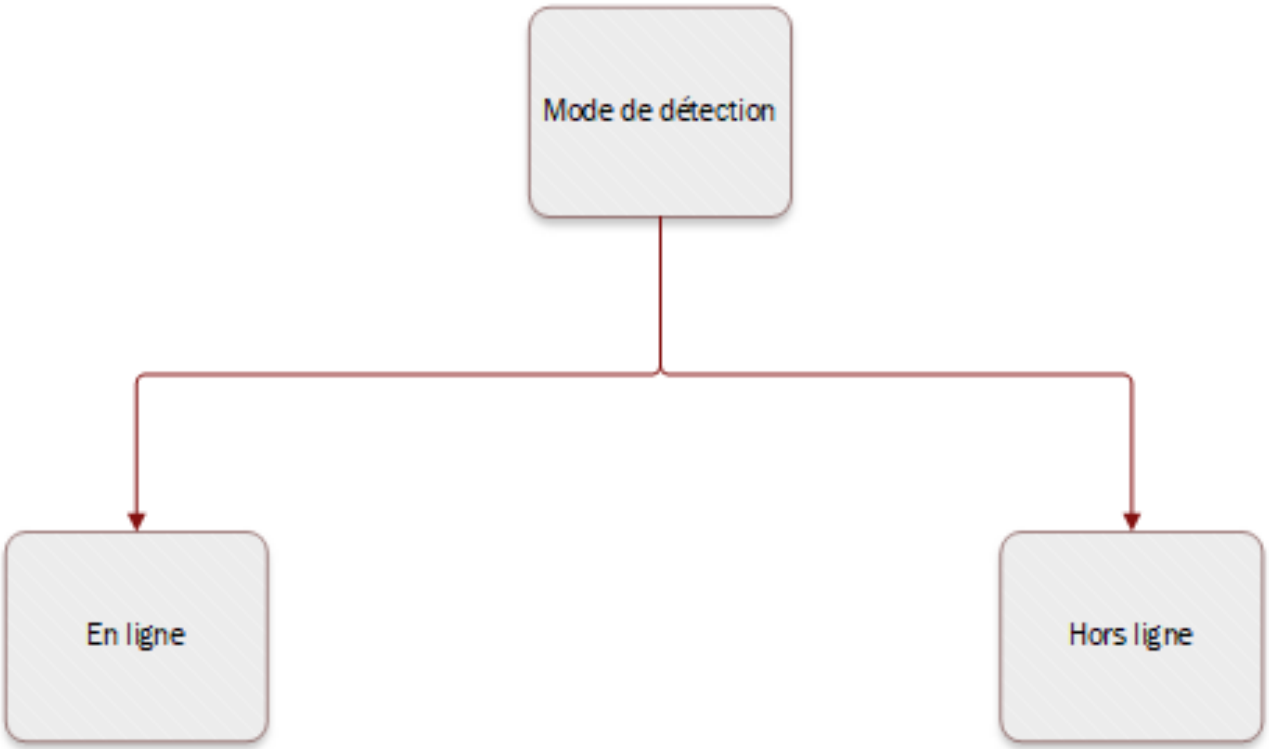

Figure II.5 – IDS basé sur le mode de détection

trafic entrant ou sortant, elle est bloquée dès que possible par le module d'atténuation de l'IDS (S. Lee al, 2011). Il s'agit de la classe IDS la plus largement utilisée et est également appelée IDS en temps réel. L'importance d'un tel IDS est davantage due au réseau accessible à tous, à tout moment et de partout.

II.3.4.2 IDS hors ligne

D'autre part, l'IDS hors ligne détecte de temps à autre les intrusions dans les référentiels de données autonomes des grands systèmes centraux. Les IDS hors ligne sont relativement utilisés à plus petite échelle en raison de l'utilisation d'activités basées sur le réseau partout et dans toutes sortes d'applications sur ce globe.

II.3.5 IDS basé sur l'architecture de détection

L'architecture fait référence à la structure opérationnelle du système de détection d'intrusion. L'IDS peut être classé en quatre groupes différents en fonction de l'architecture de détection telle que l'architecture d'agent autonome, distribuée et coopérative, hiérarchique et mobile (Voir Figure II.6).

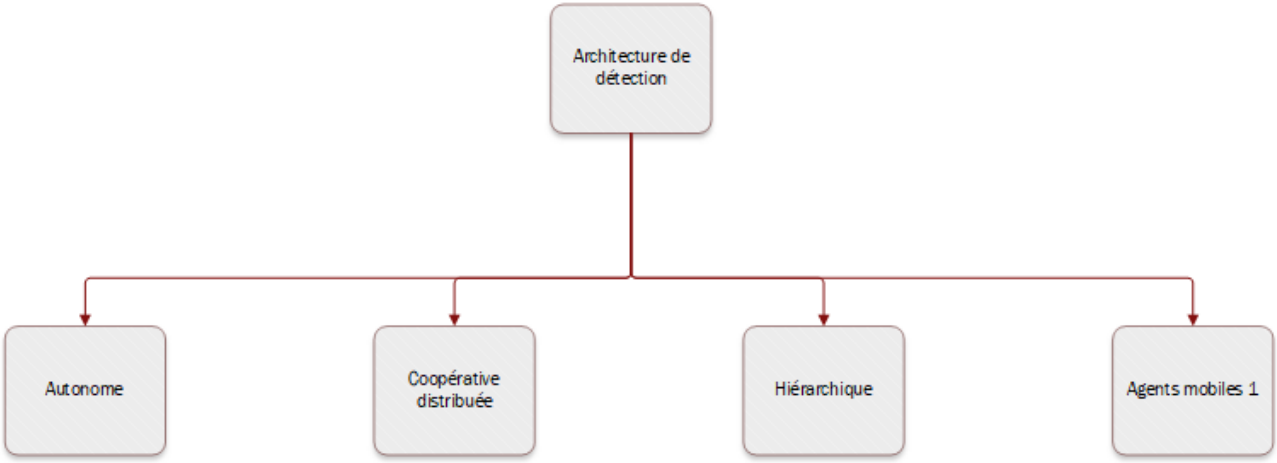

Figure II.6 – IDS basé sur une architecture de collecte de données

II.3.5.1 Architecture autonome

Il ressort clairement du nom que chaque nœud d'une telle architecture possède son propre moteur de détection d'intrusion qui détecte les intrusions pour ce nœud spécifique uniquement. Les données collectées par ce nœud spécifique sont utilisées pour comparer avec l'activité malveillante pour la prise de décision. Cette architecture est robuste grâce au fonctionnement indépendant de chaque IDS. Un tel IDS nécessite moins de ressources et peut être déployé facilement. Two Stage IDS (A.P. Lauf al, 2010) est un schéma basé sur une architecture autonome. Les limites courantes de cette architecture sont :

- ▷ Les attaques coordonnées ne sont pas détectées dans ces IDS.
- ▷ Peut provoquer une collision en raison d'un IDS indépendant à chaque nœud.
- ▷ La précision de détection est faible par rapport aux IDS distribués.

II.3.5.2 Architecture coopérative distribuée

Identique à l'architecture autonome, IDS est également installé sur chaque nœud de l'architecture distribuée. Leur fonction est de détecter les intrusions en surveillant les données d'audit locales. Un point qui différencie cette architecture de la précédente est que les données ou résultats d'audit sont partagés avec les nœuds voisins. Cela aide à fournir un mécanisme de détection distribué et coopératif pour la résolution des attaques qui étaient difficiles dans une architecture autonome (C.V. Zhou al, 2010). Cette architecture a amélioré la précision de détection et est capable de détecter les attaques coordonnées. Cette architecture est robuste aux modifications des réseaux. Architecture IDS coopérative basée sur l'analyse des réseaux sociaux

(W. Wei al, 2009) et l'IDS assisté par amis (S.A. Razak al, 2008) présentent des schémas basés sur l'architecture coopérative distribuée. Certaines limitations de cette architecture sont :

- ▷ Le maintien d'un mécanisme de détection local et global génère une architecture complexe.
- ▷ Augmentation des frais généraux de communication en raison de la coopération.
- ▷ Sujet aux attaques telles que les attaques de chantage.

II.3.5.3 Architecture hiérarchique

Cette architecture IDS divise le réseau en clusters multicouches où chaque cluster a peu de membres avec un chef de cluster. Chaque chef de cluster joue un rôle de premier plan et a plus de responsabilités que les nœuds ordinaires. Un IDS plus sophistiqué est installé sur le cluster head. Des IDS ordinaires et légers sont installés sur les nœuds restants du cluster. Cette architecture a réduit le risque d'attaques passives telles que les écoutes clandestines. Contrairement à l'architecture distribuée, cette architecture ne nécessite pas de coopération et le surcoût de communication est réduit. Il est également robuste aux modifications du réseau. L'IDS hiérarchique utilisant le modèle de la théorie des jeux (H. Otrok al, 2008), l'IDS hiérarchique optimal (K. Manousakis al, 2008) et la détection d'anomalies de cluster (H. Deng al, 2006) sont quelques-unes des approches basées sur l'architecture hiérarchique. Certaines limitations bien connues sont :

- ▷ Signaler des retards.
- ▷ Les dommages à la tête du cluster peuvent affecter l'ensemble du cluster.
- ▷ Communication supplémentaire en raison du changement répété du chef de cluster.

II.3.5.4 Architecture basée sur les agents mobiles

Cette architecture dispose d'agents avec des logiciels spécialisés et peuvent se déplacer librement ici et là pour visiter chaque nœud du réseau. Tous les nœuds sont censés installer un logiciel agent. Ils ont la capacité de corréler les activités suspectes trouvées dans les nœuds surveillés. Cette architecture prend en charge l'ajout de nouvelles capacités sans redémarrer le système de détection (S.A. Onashoga al, 2009). Des charges et des latences réseau plus faibles sont les avantages de cette architecture, ainsi que l'opulence de la tolérance aux pannes. Cette architecture montre également une évolutivité dans un environnement hétérogène. **Limites :**

- ▷ Encourus par des retards de détection d'intrusion et de rapport plus élevés.

- ▷ Problème de portabilité dû aux environnements hétérogènes qui peuvent dégrader les performances.
- ▷ Les agents sont fréquemment compromis.

II.3.6 IDS basé sur la fréquence d'utilisation

Sur la base de la manière dont un outil de détection d'intrusion accomplit son analyse, les IDS peuvent être classés en deux types tels que l'IDS continu et l'IDS périodique (Voir Figure II.7) (M. Peter al, 2001).

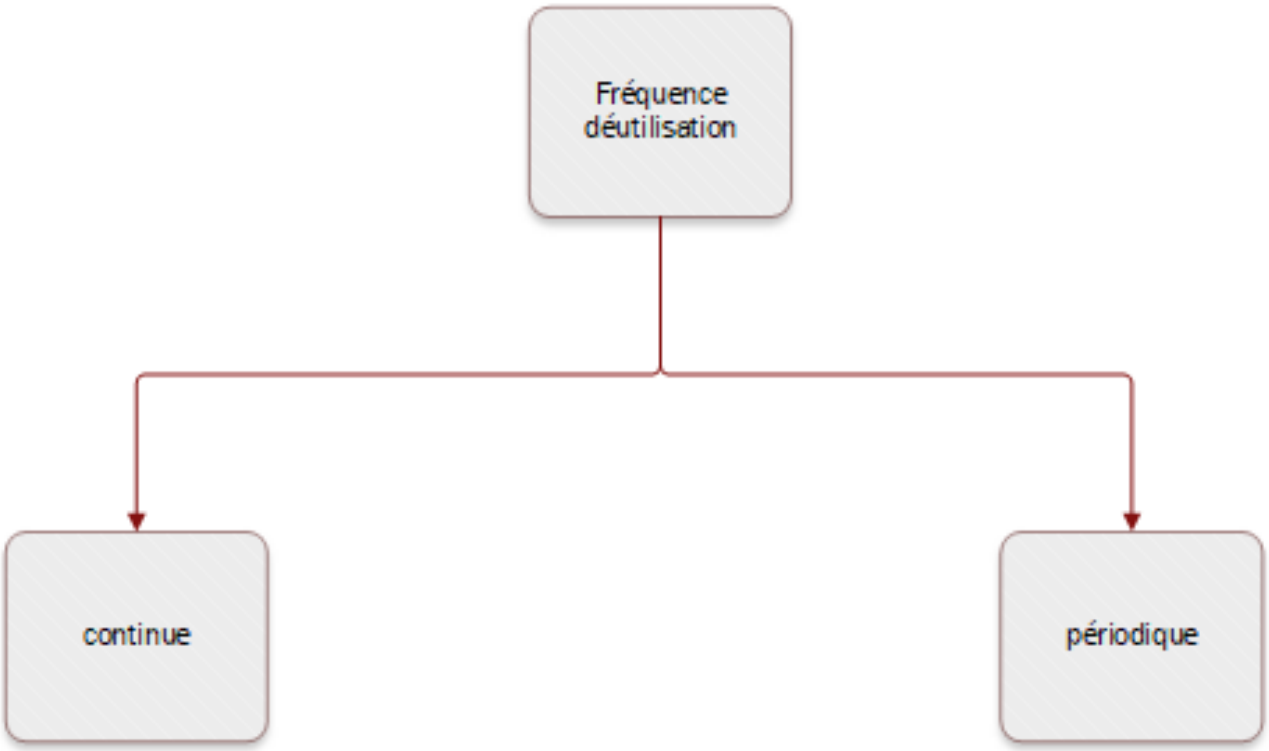

Figure II.7 – IDS basé sur la fréquence d'utilisation

II.3.6.1 IDS continu

En IDS continu, les outils de détection des intrusions, surveillent en permanence le réseau ou le système. Chaque fois qu'un acte de violation de la sécurité ou une attaque est détecté, il est piégé et bloqué avec une action immédiate. Il est principalement utilisé dans une configuration où les données entrent et sortent en continu du système ou du réseau. De tels systèmes ou réseaux sont également appelés systèmes temps réel (T. Li al, 2019). L'IDS continu est très efficace et ne laisse jamais les intrus effectuer les tâches nuisibles prévues à tout moment. Cependant, en

raison de la surveillance continue, il consomme continuellement des ressources du réseau, ce qui entraîne des problèmes informatiques et énergétiques.

II.3.6.2 IDS périodiques

Dans l'IDS périodique, l'outil de détection prend une vue d'ensemble du système ou du réseau connecté et l'analyse pour la détection d'intrusion. Si une intrusion est détectée, elle est empêchée de nuire au réseau. D'autre part, si l'intrusion n'est pas détectée, il attend la prochaine période à venir. En raison de la stratégie de détection par période, on parle d'IDS périodique. Ce type d'IDS est efficace en termes d'énergie et de calcul que son homologue (IDS continu). Cependant, si une intrusion envahit pendant la période d'attente de l'IDS, elle peut endommager le réseau dans une certaine mesure, jusqu'à ce qu'elle soit atténuée.

II.3.7 Types de données utilisés par IDS

IDS peut utiliser tout type (nature) de données pour les analyser à des fins de détection d'intrusions. Ces types de données incluent le journal de l'hôte, le journal des applications, le trafic réseau et le trafic sans fil (Voir Figure II.8)(K. Scarfone, 2007).

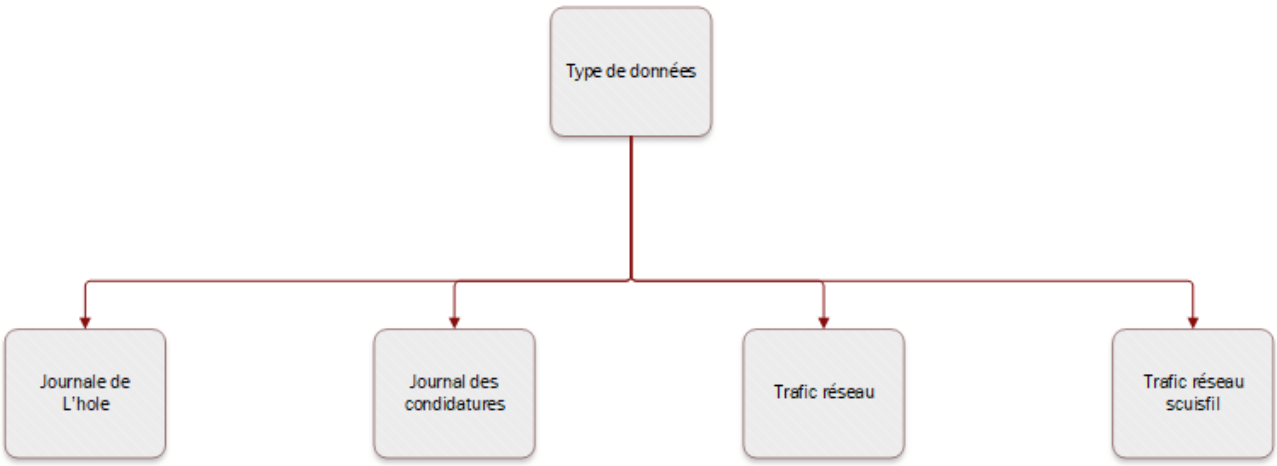

Figure II.8 – IDS basé sur type de données

II.3.7.1 Journal de l'hôte

Diverses activités sont exécutées par un utilisateur sur la machine hôte. Ils communiquent entre eux. Le journal de l'hôte est un fichier ou un ensemble de fichiers créé par le logiciel système (OS) qui enregistre toutes les communications et tous les événements ayant eu lieu

entre l'utilisateur et la machine hôte. L'attaquant peut envahir le système pour l'infecter à travers les données communiquées. Ce journal d'hôte est la seule source permettant à un IDS de collecter et d'analyser les intrusions, de sorte que les vulnérabilités attendues puissent être évitées avant qu'elles ne se propagent dans l'ensemble du système et ne l'effondrent. Une alarme est également générée par l'IDS pour avertir le système. Le journal de l'hôte contient les sources de données telles que les sources système, la comptabilité et syslog. (K. Scarfone, 2007)

II.3.7.2 Journal des candidatures

Le journal des applications est également un fichier ou un ensemble de fichiers créés par une application exécutée sur une machine et qui enregistrent des événements. Ce journal peut contenir des événements, des erreurs et des avertissements. Il est également appelé fichier journal d'application. L'IDS associé, utilisez ce fichier journal pour analyser les intrusions. Certains des événements pouvant être enregistrés par le fichier journal des applications sont les suivants.

- ▷ Alerte d'espace disque faible
- ▷ Survenance d'une opération
- ▷ Apparition d'une erreur empêchant le démarrage de l'application
- ▷ Connexion réussie, indiquant un audit de sécurité réussi
- ▷ Échec de la connexion, indiquant l'échec de l'audit

II.3.7.3 Trafic réseau

Trafic réseau généralement appelé flux d'informations ou de données, vers et depuis le réseau. La fonction de l'IDS résidant à mi-chemin de ce trafic est de filtrer ce trafic contre les intrusions et les menaces nuisibles.

II.3.7.4 Trafic réseau sans fil

Trafic de réseau sans fil composé de données et d'informations associées aux réseaux sans fil uniquement. Ces réseaux comprennent les réseaux de capteurs sans fil, les réseaux mobiles ad hoc, les réseaux de véhicules et bien d'autres. Le nom, réseau sans fil spécifie que le flux de trafic entre la source et la destination se fait via des liaisons sans fil.

II.3.8 IDS basé sur une architecture de collecte de données

Les IDS basés sur l'architecture de collecte de données sont divisés en deux classes telles que les IDS centralisés et les IDS distribués (Voir Figure II.9).

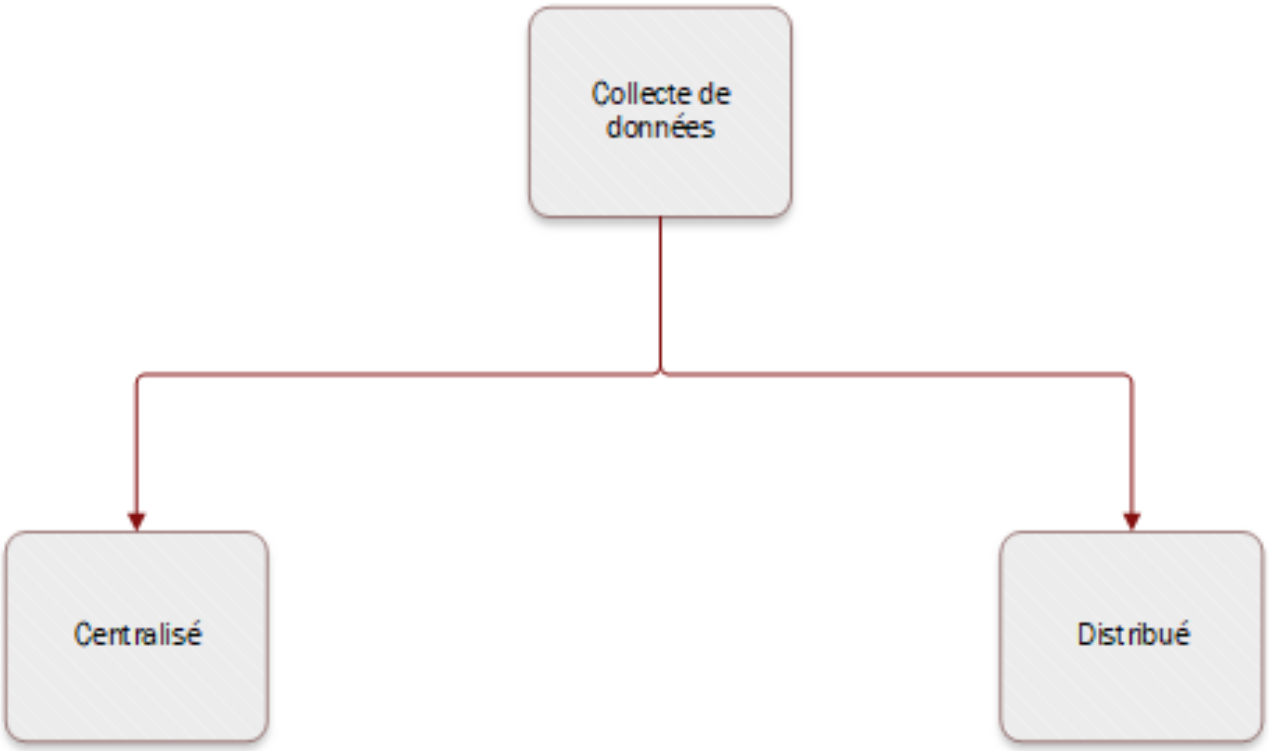

Figure II.9 – IDS basé sur une architecture de collecte de données

II.3.8.1 IDS centralisé

Dans l'IDS centralisé, les données sont collectées à partir d'une source unique telle qu'un serveur central, un système autonome et un nœud individuel (F. Sabahi A. Movaghar, 2008). Ces données sont ensuite analysées, et si une intrusion est découverte, elle est bloquée par l'action de l'IDS associé. Les autres IDS ne sont pas impliqués dans cette décision.

II.3.8.2 IDS distribué

L'IDS distribué collecte des données à partir de plusieurs sources ou de plusieurs IDS subordonnés tels que l'IDS mobile. De ce fait, l'identification d'une intrusion repose sur la décision collaborative de tous les IDS associés. Ils sont généralement utilisés dans une situation où un seul IDS n'est pas entièrement sûr de l'occurrence d'une activité intrusive. Certains des

derniers schémas d'IDS distribués sont (S.R. Snapp al, 2017) et (S. Deng al, 2017) et une enquête sur les IDS distribués est (S. Sharma al, 2018).

II.4 Techniques de détection d'intrusion

Jusqu'à présent, diverses méthodologies ont été utilisées pour détecter les intrusions dans les réseaux ad hoc. Dans ce qui suit, nous allons discuter les techniques les plus importantes et les plus connues utilisées pour la détection d'intrusions. Deux grandes familles sont envisageables :

II.4.1 Méthodes basé sur les heuristiques

Ces méthodes sont généralement basées sur les réseaux de neurones, les techniques bio-inspiré.

(Govindarajan al, 2011) ont proposé une technique de détection d'intrusion développée par une méthode de classification hybride basée sur les réseaux de neurones pour améliorer la précision de la prédiction. Il utilise des modèles d'erreurs, accélérant les méthodes pour leurs données pertinentes. Les auteurs ont conclu que la méthode proposée donne une meilleure précision de détection par rapport au modèle non hybride.

(Kumar al, 2007) ont utilisés le réseau de neurones artificiels (ANN) appliqué avec succès pour le développement de l'IDS. Il fournit une représentation simple de la relation non linéaire entre l'entrée et la sortie et sa vitesse de calcul inhérente. Un SOM est un type d'ANN qui est formé par apprentissage non supervisé pour une production d'une représentation discrétisée de faible dimension de l'espace d'entrée sous forme de carte.

(Li F, 2010) a décrit le système de détection d'intrusion de réseau neuronal hybride utilisant un algorithme génétique. C'est une méthode qui résout les contraintes ainsi que les problèmes d'optimisation sans contrainte basés sur la sélection naturelle. Il personnalise rapidement une population de solutions individuelles. Pour analyser à la fois les abus et les modèles anormaux, le réseau de neurones a été largement utilisé. La conception de la structure du réseau neuronal évolutif hybride (HENN) et la sélection des caractéristiques intégrant l'IDS sont proposées. L'auteurs a analysé le schéma proposé en termes de précision détection.

(Tong al, 2009) ont proposé un IDS hybride RBF et basée sur Elman pour le modèle de réseau neuronal où le taux de détection et le taux de faux positifs sont déterminés. La sensibilité du système se configure facilement et autorise les utilisateurs finaux à régler le système pour des tolérances acceptables sans enregistrer pour recycler le réseau de neurones.

(Aljawarneha al, 2018) ont proposé un système de détection d'intrusion qui vise à explorer les anomalies méta-heuristiques présentes dans le réseau. Ils ont réalisé cette expérience sur la partie binaire et multiclasse du jeu de données NSL-KDD. Les résultats de l'expérience ont montré une réduction des calculs et du temps. Le résultat de la méthode proposée a également présenté la précision du modèle à 98,56 % pour les ensembles de données NSL-KDD. Mais ils ont également publié des numéros avec des taux de faux négatifs élevés et faibles.

(Kushwah al, 2022) ont proposé un schéma DSGS (*Delay Sensitive Gateway Selection*) inspiré d'un algorithme génétique tenant compte du problème de retard du réseau en minimisant la distance totale parcourue par les nœuds source jusqu'à la passerelle. Les performances du schéma DSGS basé sur AG proposé sont étudiées à l'aide d'une approche comparative. Les résultats de la simulation démontrent que le schéma proposé surpasse de manière significative les schémas conventionnels et est capable d'atteindre un débit de réseau plus élevé tout en minimisant le délai de bout en bout.

(Karthick al, 2012) ont proposé une approche hybride pour la détection adaptative d'intrusion dans le réseau. Dans l'intrusion réseau adaptative, il existe des architectures en deux étapes. Dans la première étape ou l'étape initiale utilisant un classificateur probabiliste, les anomalies potentielles sont détectées à partir du trafic. Dans la deuxième étape, un modèle basé sur le modèle de Markov caché (*HMM*) est utilisé pour réduire l'attaque à l'adresse IP donnée. HMM est un modèle génératif qui modélise les données séquentielles. En HMM, les états et les transitions en relation ne sont pas visibles.

II.4.2 Méthodes basé sur les régles

(Liang, 2014) propose une combinaison de la logique floue et des réseaux de neurones. L'auteur a donné l'algorithme des bases FNN de Takagi-Sugeno (T-S) qui utilise la combinaison de la théorie floue avec des réseaux de neurones pour la classification des objets et reconnaît le comportement normal et anormal. Il aide à surmonter les faiblesses antérieures telles que

la faisabilité, le manque de normes, la flexibilité et l'adaptabilité des réseaux de neurones conventionnels. En raison de la suppression de la redondance et des données incertaines dans l'ensemble de données KDD d'origine, cette méthode proposée a atteint une précision de détection supérieure à 90 %.

Une approche efficace de détection d'intrusion qui combine Bayes naïf (NB) avec arbre de décision (DT) a été proposée par (Panda al, 2011). À l'aide de la sélection directe, les attributs sélectionnés ont été modélisés par DT au départ et par Bayes naïf à chaque étape.

Combiner les avantages de la forêt aléatoire qui se compose de nombreux arbres de décision et de l'optimisation des essaims de particules qui est essentiellement une technique d'optimisation stochastique basée sur la population, appelée PSO-RF. (Malik et al, 2012) ont proposé une sélection de fonctionnalités et une classification en tant que première et deuxième étapes, respectivement. La première étape nécessitait un PSO binaire tandis que la deuxième étape nécessitait un algorithme de forêt aléatoire. La technique proposée offre de meilleures performances que les autres techniques de classification en termes de taux moyen de faux positifs et taux moyen de détection d'intrusion pendant les attaques. Tandis que pendant les enregistrements normaux, l'algorithme RF a atteint moins de taux de faux positifs.

(Jamili al, 2009) ont utilisé la détection d'intrusion basée sur la propagation hybride dans les réseaux bayésiens. Le réseau bayésien est un réseau de modélisation qui est utilisé pour le problème qui englobe l'incertitude. L'algorithme d'inférence d'arbre de jonction est utilisé pour calculer l'inférence exacte discrète. Il y a beaucoup de scepticisme dans l'ensemble de données en raison duquel la sécurité devient difficile. Ces scepticismes ou incertitudes ont principalement deux origines. L'une est due au caractère incertain de l'information, c'est-à-dire résultant de phénomènes stochastiques. Deuxièmement, le caractère imprécis et incomplet des informations en raison d'une connaissance insuffisante est appelé incertitude épistémique. Le Dataset DARPA a été utilisés pour concevoir et tester l'IDS.

(Aydin al, 2009) ont proposé un système de détection d'intrusion hybride qui fonctionne pour la sécurité du réseau des ordinateurs à l'aide d'une méthode de rétropropagation et d'une carte auto-organisée. Le système proposé a également donné de meilleures performances pour les attaques connues et les attaques inconnues. Seules les attaques connues sont rencontrées par

les systèmes basés sur les signatures, tandis que les systèmes basés sur les anomalies rencontrent des attaques inconnues.

(Abebe Lalitha,2015) ont proposé une technique pour détecter les attaques connues et inconnues. Ils ont utilisé un classificateur de forêt aléatoire pour détecter les attaques connues et un ensemble SVM à classe unique pour les attaques inconnues. Il améliore le taux de détection élevé avec un faible taux de faux positifs. (Ahmedim al, 2019) ont proposé un système de détection d'intrusion hiérarchique qui fonctionne sur une combinaison d'arbre de décision et d'arbre REP, et d'autres algorithmes basés sur des règles comme l'algorithme JRip et Forest PA afin d'améliorer la précision et le taux de détection. Ils ont vérifié leur expérience sur l'ensemble de données CICIDS2017. Les résultats de leur expérience étaient de 94,457 % de précision pour DR, et une précision globale de 96,66 %, et le FAR le plus bas avec 1,145 %.

(Cepheli al, 2016) ont proposé un système de détection d'intrusion afin de détecter les attaques DDoS. Leur modèle proposé fonctionne sur une combinaison de méthodes basées sur les anomalies (créées à l'aide de modèles de mélange gaussiens multidimensionnels, GMM) et de méthodes basées sur la signature (créées à l'aide de Snort). Ils ont réalisé leur expérience sur deux différents ensembles de données DARPA et l'ensemble de données des banques commerciales. Le résultat de leur expérience a vérifié les meilleures performances proposées par eux, car le taux de précision pour la DARPA était de 92,1%.

(Kamarudin al, 2019) ont proposé une méthode de sélection de caractéristiques dans des dimensions plus élevées, qui nécessite une combinaison de procédure de sélection de filtre et d'enveloppe. Le classificateur Random Forest (RF) a été utilisé pour évaluer les caractéristiques sélectionnées par la méthode de filtrage. L'expérience a été testée sur les jeux de données KDD99 et DARPA 1999. Le résultat de l'expérience était un taux de faux positifs de 0,03 %.

(H.Ghayvat al, 2016) ont proposé une approche pour la détection d'une attaque par trou de ver. Grâce à l'utilisation de cette technologie sécurisée de vecteur de distance ad hoc à la demande (AODV), l'attaque par trou de ver dans les MANET peut être rapidement découverte. L'utilisation d'une signature numérique est utilisée pour éviter cette attaque. La signature numérique ainsi que la méthode de la chaîne de hachage sont utilisées pour atténuer le nœud de trou de ver. La durée de vie et le débit de la technologie suggérée sont maximisés contrairement

à l'approche précédente, et la latence du réseau est réduite. La technique proposée améliore la qualité de service, mais la suppression des erreurs inutiles reste un souci.

II.5 Conclusion

Dans ce chapitre, nous avons décrit en détail les systèmes de détection d'intrusion. Commençons par les définir et expliquer leurs processus généraux de fonctionnement. Nous avons aussi présenté les différentes taxonomies de classification des IDS.

Pour conclure, une classification des différentes techniques de détection était présentée. Tous les points décrit dans ce chapitre ont été renforcé par des travaux de recherche existants. Cela, nous a permis d'avoir une vision claire dans ce domaine et nous a aidé de contribuer des solutions qui seront présenté dans les chapitres suivants.

CHAPITRE III

DÉTECTION DES ATTAQUES BLACKHOLE DANS LE PROTOCOLE AODV

III.1 Introduction

Les MANET sont des réseaux constitués d'un ensemble d'unités mobiles qui ne nécessitent pas d'infrastructure fixe ni d'administration centralisée. Un réseau MANET se distingue par plusieurs caractéristiques telles que la topologie dynamique, la contrainte énergétique, la capacité de liaison limitée et variable et la sécurité physique limitée. La mobilité dans ce type de réseau est non seulement un avantage, mais aussi un inconvénient qui les rend vulnérables à toutes les attaques (Koajalagi A, 2018)(Kumari A al, 2020). L'un des problèmes sérieux des réseaux MANET est la sécurité puisque les attaques peuvent être internes ou externes (Yasin A al, 2018). Ainsi, ces attaques peuvent influencer le trafic de données ou contrôler le trafic (Bhattacharyya A al, 2011). Plusieurs techniques ont vu le jour pour résoudre ce problème, notamment les systèmes de détection d'intrusion (IDS), les systèmes de prévention d'intrusion (IPS) et diverses méthodes de sécurité. Les IDS sont des systèmes conçus spécifiquement pour détecter la source de l'attaque.

Watchdogs (Marti S al, 2000) est un mécanisme de détection d'intrusion basé sur l'écoute du nœud voisin. D'autres systèmes de base ont également vu le jour grâce auxquels on peut citer un ACK basé sur un acquittement avec un seul saut. Two-ACK (*(Two-ACKnowledgement)*(Balakrishnan, 2005)(Lee J-S, 2008), A3ACK *(Adaptative 3-ACKnowledgement)*(Sheltami T al, 2014), AACK *(Adaptative ACKnowledgement)*(Sheltami T al, 2009), EAACK *(Enhanced Adaptative ACKnowledgement)* (Shakshuki E al, 2013) sont également des systèmes de détection d'intrusion basés sur des accusés de réception. Dans notre travail, nous essayons de trouver des schémas basés sur AACK pour détecter les attaques de trous noirs (Kumari A al, 2020) sur le protocole AODV (Koujalagi A, 2018)(Yasin A al, 2018).

La contribution de cette étude est triple : (1) Détecter l'intrusion d'une ou de plusieurs attaques de trous noirs avec un modèle générique, rapide et efficace ; (2) Garantir une trajectoire seine ; (3) Augmenter le taux de paquets reçus, ce qui augmente le taux de livraison de paquets (PDR) et le débit avec un délai de bout en bout minimum. Notre travail est basé sur AACK (Lee J-S, 2008)(Sheltami T al, 2009), mais il inclut l'utilisation de ACK, 2-ACK (Two-ACK) et 3-ACK. L'idée est de diviser le chemin en deux si l'accusé de réception AACK n'est pas reçu. Cette méthode nous a permis d'avoir plusieurs sous-chemins qui facilitent la détection du nœud malveillant. Chacun de ces sous-chemins a sa source et sa destination. Cependant, la question

qui se pose ; comment s'assurer que les sources et les destinations des sous-chemins ne sont pas malveillantes ?

Nous avons abordé avec notre solution une étape de vérification des nœuds source et destination. Au début, les seuls nœuds confirmés à l'intérieur sont la source d'origine et la destination d'origine, nous les avons exploités pour confirmer les autres. En commençant par le premier sous-chemin qui contient la source d'origine, si nous recevons un accusé de réception de sa destination alors ce chemin est confirmé à l'intérieur.

Pour confirmer le deuxième sous-chemin, nous devons d'abord confirmer sa source en envoyant un ACK à la destination du premier sous-chemin, s'il est reçu alors cette source n'est pas un nœud malveillant. Ces deux étapes sont répétées jusqu'à ce que tout le chemin soit confirmé. Chaque fois qu'un nœud malveillant est détecté, il sera envoyé à une liste noire.

III.2 Prés-requis

III.2.1 Attaque par trou noir (BlackHole)

L'attaque par trou noir (Kamari A al, 2020) (Chavan A al, 2020) est l'une des attaques les plus connues. Dans ce type d'attaques, le nœud malveillant tente d'attirer le plus de chemins possible afin de pouvoir contrôler le plus grand nombre de données circulant dans le réseau. Le principe d'insérer un nouveau nœud pour forcer un maximum de voisins à modifier leurs tables de routage. Les données envoyées transitent par ce nœud malveillant pour les forcer à lui transmettre les informations. Les informations reçues par ce dernier seront détruites et ne seront jamais remises sur le réseau. L'attaquant se place généralement à un endroit stratégique et supprime tous les messages. Cela crée une sorte de puits ou de trou noir dans le réseau. Le trafic absorbé peut ainsi être redirigé vers un autre nœud ou disparaître complètement. L'attaque par trou noir simple est un nœud malveillant qui ignore ou abandonne tous les paquets de données qui le traversent. Si ce nœud connecte deux composants, le réseau sera séparé en deux composants déconnectés (Khalladi et al,2019)(voir Figure III.1).

Attaque de trou noir multiple et coopérative

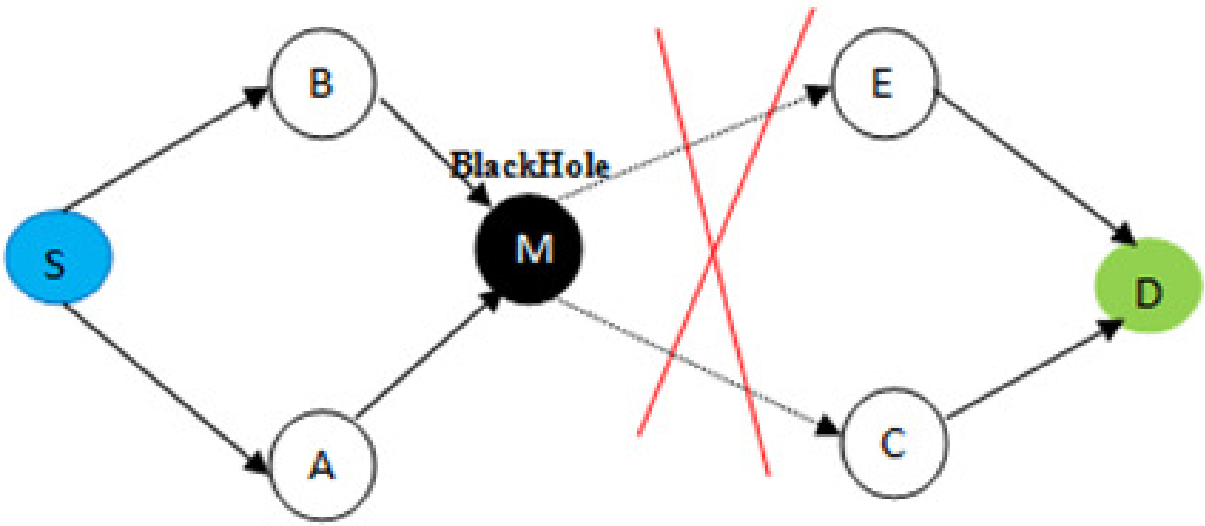

Figure III.1 – Attaque par trou noir(BlackHole)

Elle est presque identique à la précédente, mais il y a plus d'un nœud malveillant qui perturbe le réseau simultanément. Il s'agit de l'une des attaques les plus sévères pouvant totalement entraver le fonctionnement d'un réseau ad hoc. Il s'agit d'une attaque par trous noirs multiples, mais les nœuds malveillants y coopèrent.

III.2.2 Spécification de l'attaque par trou noir dans AODV

Le vecteur ad hoc à la demande (AODV) (Koujalagi A,2018)(Yasin A al, 2018) est basé sur un algorithme de vecteur de distance et ne demande l'itinéraire qu'en cas de besoin. Chaque nœud intermédiaire qui se trouve dans la route entre un nœud source et un nœud destination doit conserver une table de routage qui contient : L'adresse de la destination, le prochain nœud à utiliser pour atteindre la destination, la distance en numéro de nœud, le numéro de séquence de la destination et l'heure d'expiration de l'entrée de la table. AODV utilise trois types de messages pour créer et maintenir des itinéraires : le RREQ (*Route Request*) pour demander un itinéraire, le RREP (*Route Replay*) pour répondre à une demande d'itinéraire et le RERR pour signaler une panne d'itinéraire (voir Figure III.2). Cette attaque vise à modifier le protocole de routage ou le trafic transitant par un nœud spécifique contrôlé par l'attaquant. Le nœud malveillant peut violer la spécification du protocole de routage pour se trouver dans le chemin qui relie la source et la destination des données. Cela peut être fait lorsqu'un nœud source envoie un paquet RREQ au nœuds intermédiaires pour trouver un nouveau chemin vers la destination. Lorsque le nœud corrompu reçoit le paquet RREQ, il répond avec un paquet RREP

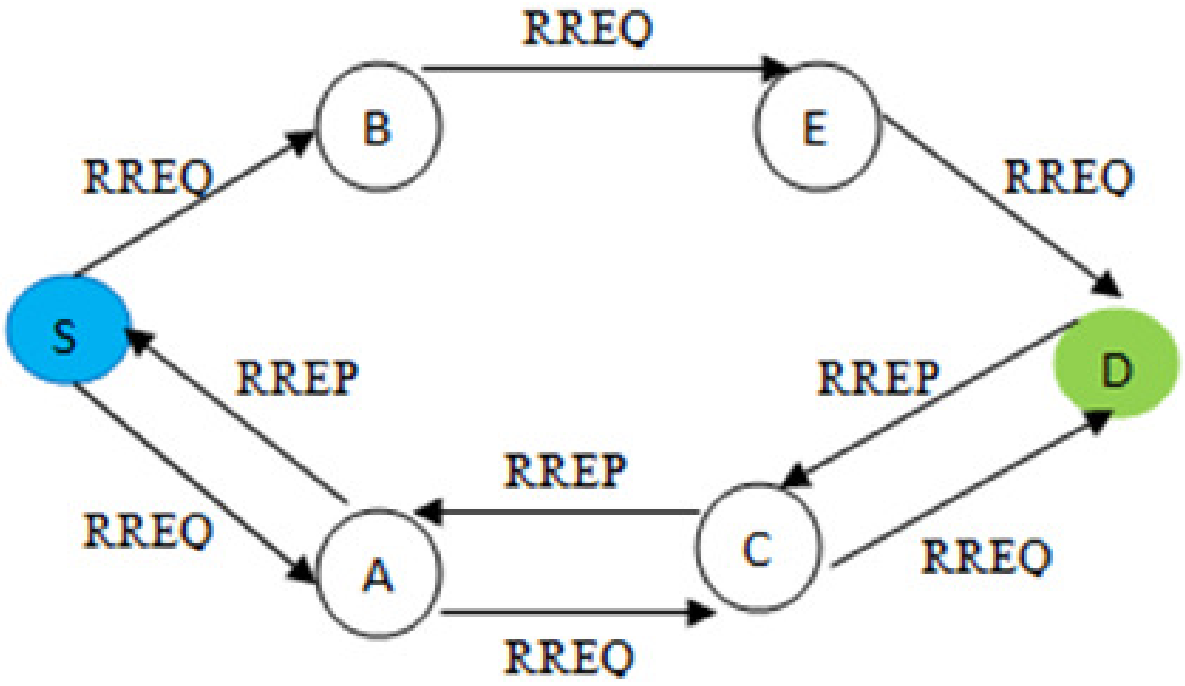

Figure III.2 – Protocole AODV

avec un numéro de séquence non seulement erroné mais aussi élevé pour augmenter ses chances de faire partie de la route. Si le paquet RREP atteint la source en premier par rapport aux réponses du nœuds légitimes, il peut ignorer d'autres messages RREP provenant d'autres nœuds et sélectionner la route à travers le nœud corrompu pour envoyer des paquets et s'adapter à la route. Le trafic absorbé peut être soit redirigé vers un autre nœud, soit disparaître complètement (Singh V al, 2019).

III.3 Techniques de detection des attaques par trou noir

Dans (Yasin A al, 2018)), la technique proposée utilise une minuterie et un message d'appât pour détecter les attaques de trous noirs intelligents. Il fonctionne en deux phases. Dans la première phase appelée *Baiting*, chaque nœud a un appât-minuterie avec une valeur aléatoire de B secondes. Le minuteur crée et diffuse une demande d'appât chaque fois qu'il atteint B avec un faux identifiant généré aléatoirement. Le trou noir envoie une réponse au nœud source en affirmant qu'il a une route lorsqu'il reçoit la demande appâtée, puis le nœud source considère immédiatement le nœud qui a répondu comme un trou noir et l'ajoute à la liste des trous noirs. Pour éviter d'encombrer le réseau avec de fausses demandes, la valeur de TTL (*Time-To-live*) est définie pour chaque demande d'appât. Dans la deuxième phase appelée *Réponse non voisine*,

chaque nœud connaît ses nœuds adjacents en utilisant le processus de diffusion de message Hello. Lorsqu'une relecture est reçue par le nœud source, il vérifie l'ID du NWSP (*Node With the Shortest Path*). S'il est dans la liste des trous noirs ; la rediffusion est rejetée ; sinon, il vérifie si l'ID existe dans la liste des voisins en comparant l'ID avec ceux de la liste des voisins. Si NWSP n'est pas un nœud voisin et pour éviter toute communication avec des nœuds inconnus, cette relecture est rejetée par le nœud source. Les auteurs cherchent à améliorer leur modèle proposé pour augmenter le débit et le débit de livraison des paquets, ainsi que pour réduire les délais de bout en bout.

Enhanced RIDAODV (Hamamreh A, 2018) est un protocole amélioré et modifié basé sur le mécanisme RID-AODV. La solution proposée met l'accent sur la création d'une liste noire dynamique pour chaque nœud du réseau. Chaque nœud dépend du nombre de non-concordances des valeurs de hachage des paquets reçus par rapport à certaines valeurs de seuil. Le seuil est fonction de la mobilité (seuil variable) pour annuler l'effet de la défaillance normale de la liaison. Le changement soudain du temps d'aller-retour (*Round-Trip Time*) peut décider d'ajouter / supprimer d'autres nœuds à / de sa liste noire. Ce modèle est très coûteux car il modifie le protocole AODV lui-même, en particulier dans le délai de bout en bout.

Dans (Koujalagi A,2018), après que le nœud source a effectué un paquet de demande de route de diffusion (RREQ), il reçoit une réponse de route multiple de la demande de route correspondante. La première réponse d'itinéraire fournie est considérée comme la réponse d'un nœud malveillant et sera supprimée de la table à l'aide du mécanisme d'enregistrement RREP. Ensuite, la deuxième réponse d'itinéraire est choisie par le mécanisme de sauvegarde RREP et la positionne comme une réponse du nœud de destination correspondant. Les données sont transmises au chemin par lequel le deuxième RREP est arrivé. Cette solution augmente le PDR de 5% par rapport à la situation d'attaque du Blackhole.

IBFWA (Kumar V,2017) (Integrated Bloom Filter with Watchdog Algorithm) est proposé pour éviter la perte de paquets dans le chien de garde. Le nœud est validé par le processus de génération de clé d'une autorité de certification (Certificate Authority). Après cela, il vérifie si le nœud est normal ou attaquant. Le nœud sera bloqué et la communication à travers lui sera évitée, s'il s'agit d'un nœud Blackhole. Sinon, il sera ajouté au réseau et la communication via celui-ci sera activée si un nœud est compromis et révoqué en tant que nœud normal.

Dans (Augustine A al,2015) un mécanisme de surveillance est utilisé pour détecter une attaque Blackhole à la base de divers IDS a été planifiée avec un schéma d'acquittement. Cette méthode envoie un message d'alarme au nœud source lors de la détection d'une attaque Blackhole.

ESAACK (Enhanced and Secured Adaptive Acknowledgement) est proposé par (Kumar S al,2019) pour arranger certaines faiblesses de Watchdog. Tout d'abord, il s'agit de créer des points centraux. Ensuite, ils sont associés et leur accessibilité est vérifiée. Une tradition croisée est présentée, appelée tradition de coordination rassemblée. Il isole un cadre agrégé dans différents rassemblements. La coordination intra-assemblage se fait par une tradition proactive qui diminue le retard dans la correspondance des points centraux à l'intérieur du groupe. La tradition de croisement proposée est un mélange d'approche RSA et BE. Pour cela, l'approche a réduit le point central malin par lequel le niveau de sécurité est révisé. Cet algorithme utilise les notions de cryptographie en implémentant l'algorithme RSA qui alourdit son exécution.

III.4 Modele proposé

Comme mentionné ci-dessus, le modèle *AACK* est basé sur un accusé de réception envoyé du nœud de destination au nœud source. S'il reçoit l'accusé de réception alors le chemin est sûr, sinon, on passe au modèle *2ACK* pour détecter les nœuds malveillants. Notre travail vise à améliorer le fonctionnement de ce modèle, nous avons gardé le principe général, mais nous avons modifié la méthode de détection. Tout d'abord, le nœud source envoie un paquet de données au nœud de destination et attend un accusé de réception (*AACK*) du nœud de destination. S'il ne reçoit pas l'accusé de réception, alors le chemin contient un ou plusieurs nœuds malveillants. Pour les détecter, nous divisons le chemin en deux sous-chemins(Khalladi et al,2021).

Nous appliquons l'étape précédente pour les deux sous-chemins. Chaque fois que nous ne recevons pas d'accusé de réception, nous effectuons une scission, jusqu'à ce que les nœuds malveillants soient trouvés. Une étape de confirmation est nécessaire après chaque opération de découpage. Elle consiste à confirmer les sources de chaque sous-chemin en envoyant un ACK de confirmation de la source du sous-chemin courant vers la destination du sous-chemin précédent à condition que ce dernier soit un chemin sûr, comme le montre la figure III.3. Nous avons appelé notre solution SP-AACK (SPlitted AACK).
Si la longueur du chemin est égale à trois nœuds, le 3-ACK est utilisé.

Si la longueur du chemin est égale à deux nœuds, le 2-ACK est utilisé.

Si la longueur du chemin est égale à un seul nœud, l'ACK est utilisé.

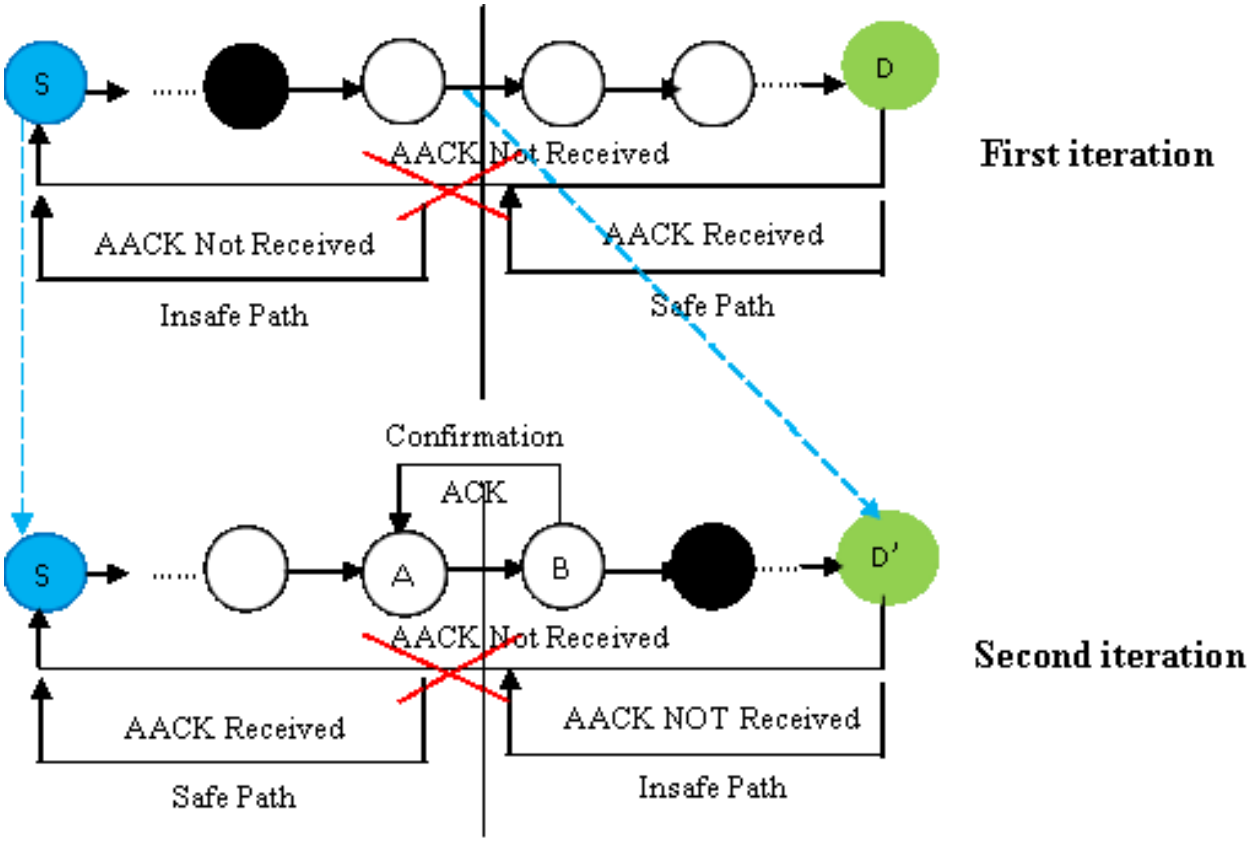

Figure III.3 – Processus du modèle proposé

III.4.1 Organigramme

La figure III.4 montre les étapes de notre modèle pour la détection des nœuds de trous noirs. Initialement, nous envoyons un accusé de réception $AACK$ de la destination à la source, s'il est reçu, le chemin est sûr, sinon le chemin contient un ou plusieurs nœuds malveillants.

La détection de ces nœuds applique ceci comme suit. Tout d'abord, nous lisons le nombre de nœuds dans le chemin (N) puis nous divisons le chemin en deux sous-chemins. L'étape précédente est répétée à chaque fois que l'accusé $AACK$ n'est pas reçu. Au cours de ce processus, chaque fois que nous détectons un nœud de trou noir, il sera envoyé à une liste noire. Pour garantir l'efficacité de notre modèle, pour chaque opération de fractionnement, nous devons confirmer que les sources d'information ne sont pas des nœuds malveillants. Par conséquent,

chaque nouvelle source doit envoyer un *ACK* à la destination du sous-chemin le plus proche.

La confirmation des nœuds est une opération que nous avons ajoutée pour garantir que les nœuds désignés comme sources et destinations de chaque sous-chemin ne sont pas malveillants. Pour cela, dans tous les nœuds, nous nous assurons que la source initiale et la destination initiale ne sont pas malveillantes, donc le plus petit sous-chemin contenant la source initiale est automatiquement sûr (la source d'origine confirme ce chemin). Ce sous-chemin sera utilisé pour la confirmation des autres sous-chemins suivants, donc le prochain sous-chemin doit être confirmé (un ACK est envoyé de la source de ce sous-chemin vers la destination du sous-chemin déjà confirmé , si l'accusé de réception est reçu alors la nouvelle source est à l'intérieur. Sinon, c'est un nœud malveillant, et il sera envoyé à la liste noire) (voir Algorithme 1)

Algorithm 1 Confirmation steps

Require:
S : Original Source
D : Original Destination N : Number of sub-paths
S, D : Are safe nodes
$Subpath_1$: confirmed sub-path
for all sub-paths **do**
  Send an ACK From First node of $sub - path_{i+1}$ to the last Node of $sub - path_i$
  if ACK received **then**
    First node of $sub - path_{i+1}$ is safe
  else
    First node of $sub - path_{i+1}$ is malicious
    Send First node of $sub - path_{i+1}$ to the blacklist
  end if
end for
All safe and successive sub-paths are combined into one safe path.

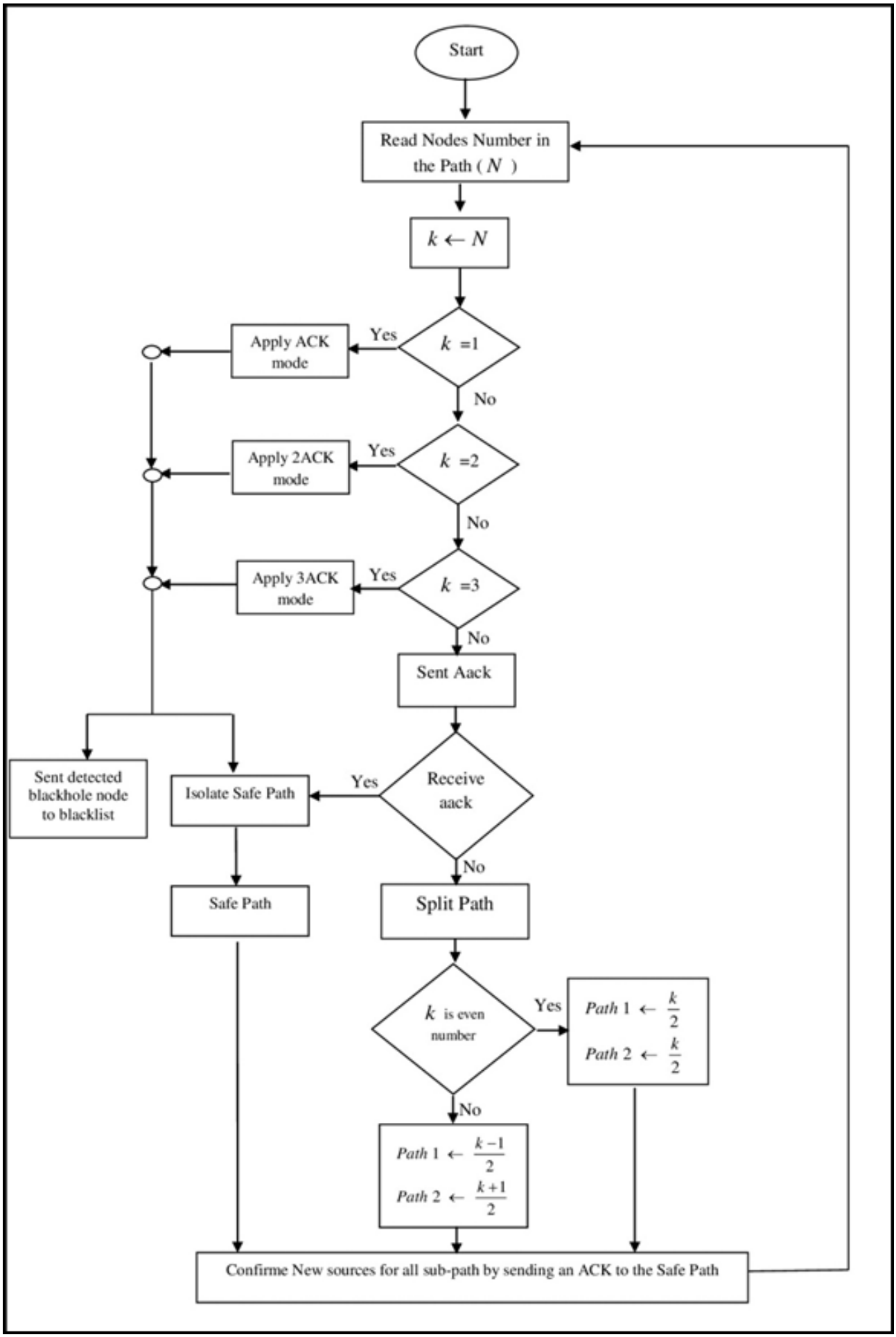

Figure III.4 – Ogranigramme du modèle proposé

III.5 Application

III.5.1 Attaque single

En supposant qu'un réseau se compose de 10 nœuds, le nœud 1 est la source et le nœud 10 est la destination. Les autres nœuds sont des nœuds ordinaires, sauf que le nœud 9 est un nœud de trou noir. Pour la détection du nœud malveillant, nous procédons à la détection avec le modèle SP-AACK. Le nœud 1 ne reçoit pas d'$AACK$ du nœud 10, ce qui implique que le chemin contient au moins un nœud de trou noir. Alors on divise le chemin dans deux sous-chemins, un sous-chemin contenant les nœuds de 1 à 5, et le second contient les nœuds de 6 à 10. Le nœud 1 reçoit un $AACK$ des nœuds 5, ce sous-chemin est donc confirmé et ne contient aucun nœuds malveillants.

Nous devons confirmer le nœud 6 (désigné comme la source du sous-chemin) en envoyant un ACK au nœud 5. Le nœud 6 est confirmé comme non malveillant. Ce dernier ne reçoit pas d'$AACK$ du nœud 10, il y a donc un nœud malveillant dans ce chemin. Nous répétons l'opération de division et nous obtenons 2 autres sous-chemins, un sous-chemin contenant les nœuds 6 et 7, et l'autre contenant les nœuds 8, 9 et 10. Le nœud 6 reçoit un ACK du nœud 7, donc ce sous-chemin ne ne pas contenir de nœud malveillant.

Le nœud 8 doit être confirmé comme non malveillant en envoyant un ACK au nœud 7. Le sous-chemin 8,9,10 est le sous-chemin contenant le nœud trou noir. Comme il s'agit d'un sous-chemin à 3 nœuds (2 sauts), nous appliquons le schéma *Two-ACK* pour détecter que le nœud 9 est malveillant. Ce nœud est envoyé à la liste noire et on obtient un sous chemin sans nœud malveillant. La figure III.5 montre l'envoi de messages $AACK$ et de confirmation ACK.

III.5.2 Attaque multiple

Nous appliquons maintenant SP-AACK sur le même réseau précédent mais avec 2 nœuds trous noirs (les nœuds 3 et 9 sont malveillants). Les 2 sous-chemins contiennent un nœud de trou noir. Pour le premier sous-chemin avec les nœuds de 1 à 5 qui contient un nœud malveillant, on se sépare et on obtient deux sous-chemins, un sous-chemin contenant les nœuds 1 et 2, et le

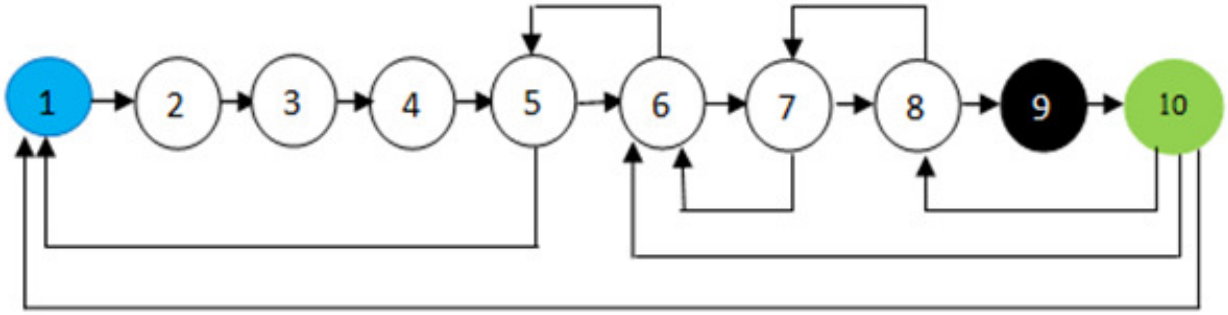

Figure III.5 – Détection d'une attaque par trou noir simple (Single BlackHole)

second contient les nœuds 3, 4 et 5. Le nœud 1 reçoit un *ACK* du nœud 2, ce sous-chemin est donc confirmé et ne contient pas de nœuds de trous noirs.

Pour le deuxième sous-chemin, nous devons d'abord confirmer le nœud 3 en envoyant un ACK au nœud 2. Ce nœud est détecté comme malveillant et envoyé vers la liste noire. Le sous-chemin contient maintenant les nœuds 4 et 5. Le nœud 2 reçoit un *ACK* du nœud 4 ce qui signifie que 4 n'est pas malveillant, donc ce nœud reçoit un *ACK* des nœuds 5, donc le sous-chemin 1, 2, 4 et 5 ne contient aucun nœud malveillant (après détection et isolement du nœud 3). La détection des nœuds malveillants dans les chemins 6, 7, 8, 9 et 10 est effectuée de la même manière que celle décrite pour les sous-chemins 1, 2, 3, 4 et 5. Les étapes de détection décrites ci-dessus sont illustrées à la Figure III.6.

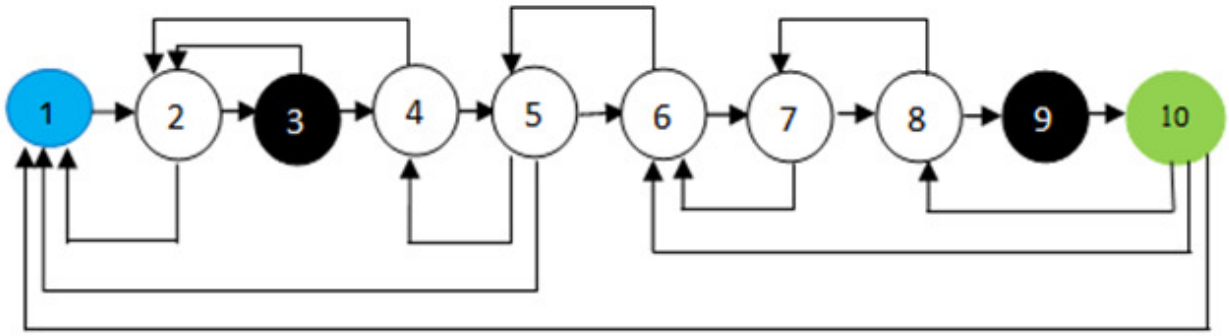

Figure III.6 – Détection d'une attaque par trou noir multiple (Multiple BlackHole)

L'avantage du modèle *SP-AACK* est que même si nous avons plusieurs attaques, nous les traitons comme une seule attaque après avoir divisé le chemin (voir Figure III.6).

III.6 Experimentation

Nous avons utilisé NS-2,35 pour la simulation. Le modèle proposé est simulé pour des réseaux de différentes tailles, 10, 15, 20, 25 et 30 nœuds, avec un nombre de nœuds malveillants de 2, 3 et 4 pour chaque réseau. La simulation se fait en deux étapes. La première étape consiste à simuler tous les fichiers TCL sans le modèle proposé ; la seconde consiste à re-simuler les fichiers avec le modèle SP-AACK. Pour montrer l'efficacité du modèle SP-AACK, nous avons choisi des métriques de performance, telles que le PDR, le délai de bout en bout et le débit pour tous les scénarios (sans solution et avec solution).

Ratio de livraison de paquets PDR (Packet Delevery Ratio) :C'est le taux de paquets reçus par rapport au nombre total de paquets envoyés.

$$\text{PDR}=\frac{Number\ of\ packets\ received\ *\ 100}{Total\ number\ of\ packets\ sent}$$

THROUGHPUT : Le débit peut être défini comme la quantité de données transférées de l'expéditeur au destinataire dans une quantité donnée de temps. Il est mesuré en bits par seconde ou en paquets par seconde **?**.

$$\text{Throughput}=\frac{N\ of\ delivered\ packets\ *\ Packet\ size\ *\ 8}{Simulation\ time}$$

EndToEnd Delay : Le temps mis par un paquet pour voyager la source à la destination est appelée le délai de bout en bout **?**.

$$End-to-EndDely=Receivedtime-Senttime$$

Paramètres de simulation Les valeurs des paramètres de simulation sont résumées dans le tableau 1.

Paramètre	Valeur
Système d'exploitation	Linux Mint 18.10/Windows(Cygwin)
Version du Simulateur	2.35
Protocole de routage	AODV
Nombre Total des nœuds	10,15,20,,25,30
Nombre des nœuds Blackhole	1,2,3,4
Type de trafic	CBR/ UDP
la taille du paquet	512 kbits
Couche MAC	Mac/802_11
Temps de simulation	300s

Table III.1 – Paramètres de simulation

III.7 Resultats

Comme mentionné précédemment, nous avons testé le modèle SP-AACK dans différents réseaux comprenant un nombre de nœuds variant de 10 à 30 nœuds, avec un nombre de nœuds malveillants de 1, 2, 3 et 4 nœuds trous noirs. Dans nos simulations, la position initiale du nœud source et du nœud destination est déinie sur les bords opposés du réseau. Le reste des nœuds est placé au hasard (y compris les nœuds de trou noir). Le protocole utilisé est le protocole AODV.

Chaque simulation a été réalisée sous le protocole natif AODV, AODV avec trou noir et avec le modèle SP-AACK. Nous fixons la taille des paquets à 512 octets, le temps de simulation à 300 secondes, le protocole de transport est UDP et enfin le type de trafic utilisé est le débit binaire constant (CBR). Le tableau 1 montre les paramètres de simulation. Les résultats obtenus sont présentés dans les Fig. 7, 8, 9 et 10. Nous avons appelé « Black hole » un réseau avec des nœuds malveillants et « D-Black hole » un réseau avec le modèle SP-AACK.

III.7.1 Résultats SP-AACK

III.7.1.1 Attaque unique(simple)

La figure 7 montre les résultats pour un seul nœud de trou noir. On constate que le PDR est remarquablement augmenté (+70% en moyenne) après application de SP-AACK, il varie entre 21.18% et 36.46% en présence de nœuds malveillants ceci du fait du nombre réduit de paquets reçus, alors quand on applique le modèle SP-AACK le PDR varie entre 47.06% et 100%.

On remarque également une légère augmentation du délai de bout en bout qui dû à deux facteurs, le premier est la diminution du nombre de paquets reçus en présence de nœuds malveillants puis l'ensemble de ces paquets sont récupérés grâce au modèle SP-AACK et le second est dû au traitement effectué pour la détection des nœuds malveillants (partage du réseau).

Le débit est également augmenté (+ 47 % en moyenne) dans SP-AACK, car les nœuds malveillants sont éliminés.

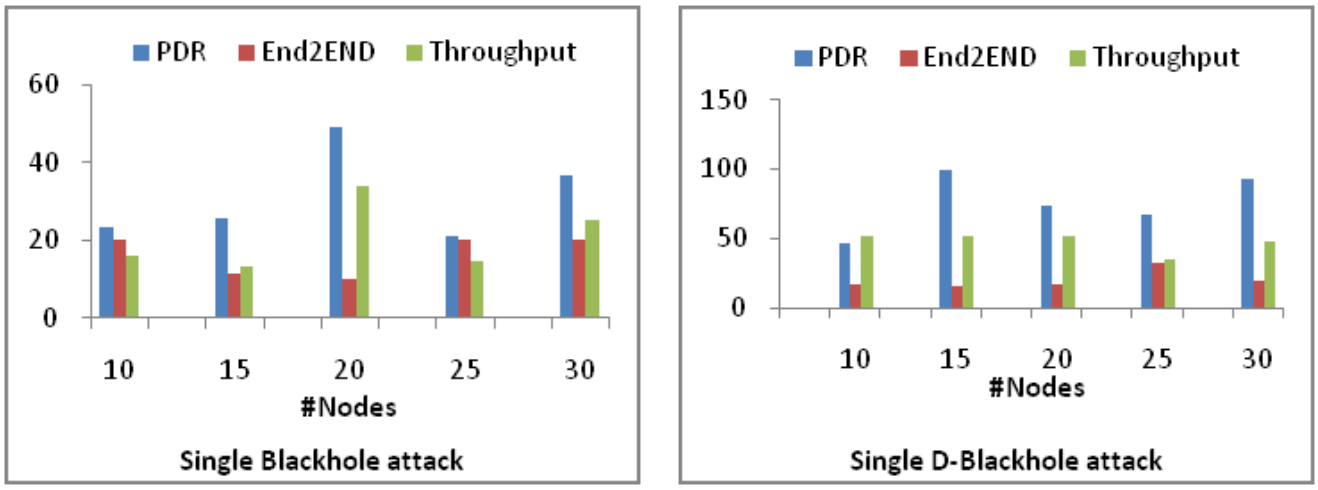

Figure III.7 – Résultat du SP-AACK avec trou noir simple (Single BlackHole)

III.7.1.2 Attaque multiple

Les résultats obtenus pour 2 nœuds de trous noirs sont présentés à la Figure III.8. Après l'application de la solution proposée, le PDR varie entre 73,64% et 100%. Alors qu'en présence de nœuds malveillants, il varie entre 0,21 et 24,3 puisque le nombre de paquets reçus a diminué. L'approche proposée a augmenté le PDR (+ 72% en moyenne).

Après l'élimination des nœuds malveillants, le Débit a également augmenté (+ 48 % en moyenne). La récupération des paquets perdus et les traitements effectués pour la détection des nœuds malveillants (l'opération split) ont contribué à la légère augmentation du délai End To End.

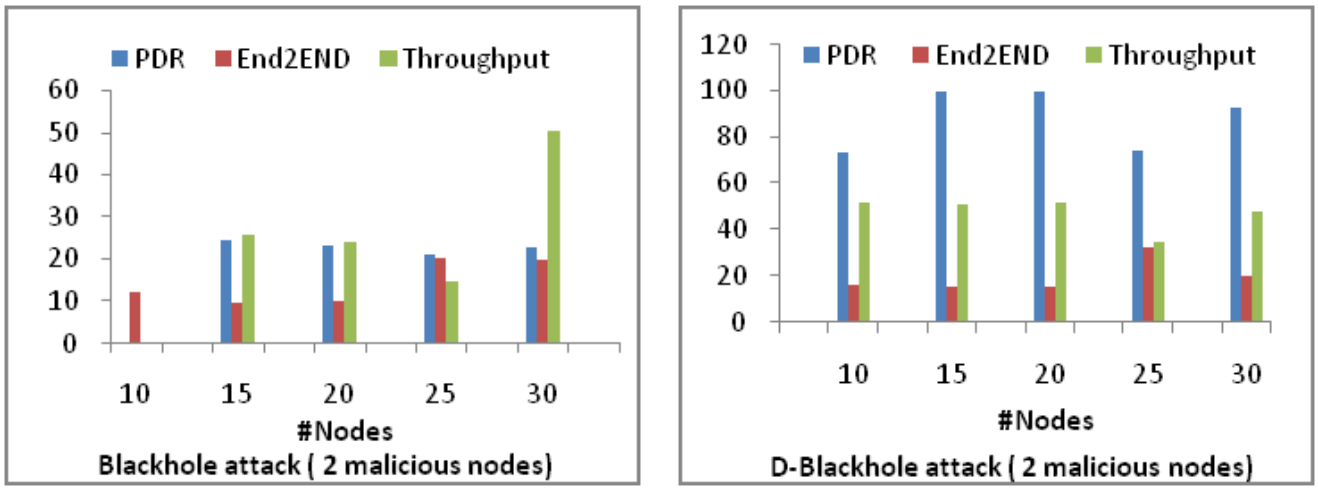

Figure III.8 – Résultat du SP-AACK avec deux trous noir (multiple BlackHole)

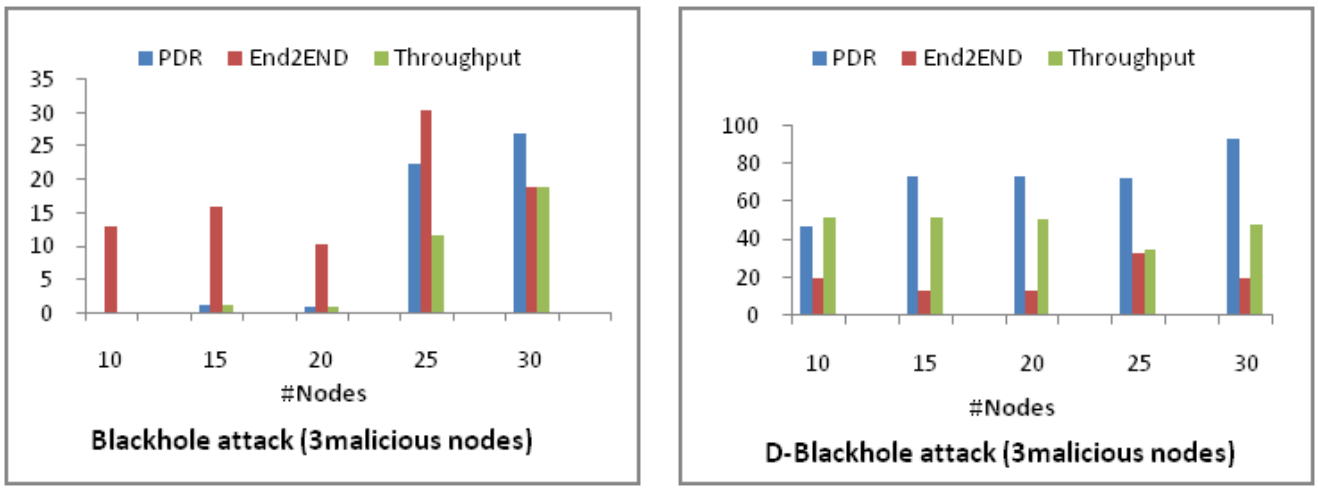

Figure III.9 – Résultat du SP-AACK avec trois trous noir (multiple BlackHole)

Les figures 9 et 10 montrent les résultats obtenus avec 3 et 4 nœuds malveillants, respectivement. On remarque que le PDR est presque nul lorsqu'il existe des nœuds malveillants, ceci en raison de la perte totale de paquets causée par les nœuds trou noir. Après application du modèle SP-AACK, nous remarquons que le PDR est augmenté (+ 85% en moyenne), nous avons donc pu récupérer un grand nombre de paquets perdus.

Le débit est toujours faible voire nul en présence de nœuds malveillants du fait du nombre réduit de paquets délivrés. L'application du modèle SP-AACK a augmenté le débit d'environ (+ 88 % en moyenne).

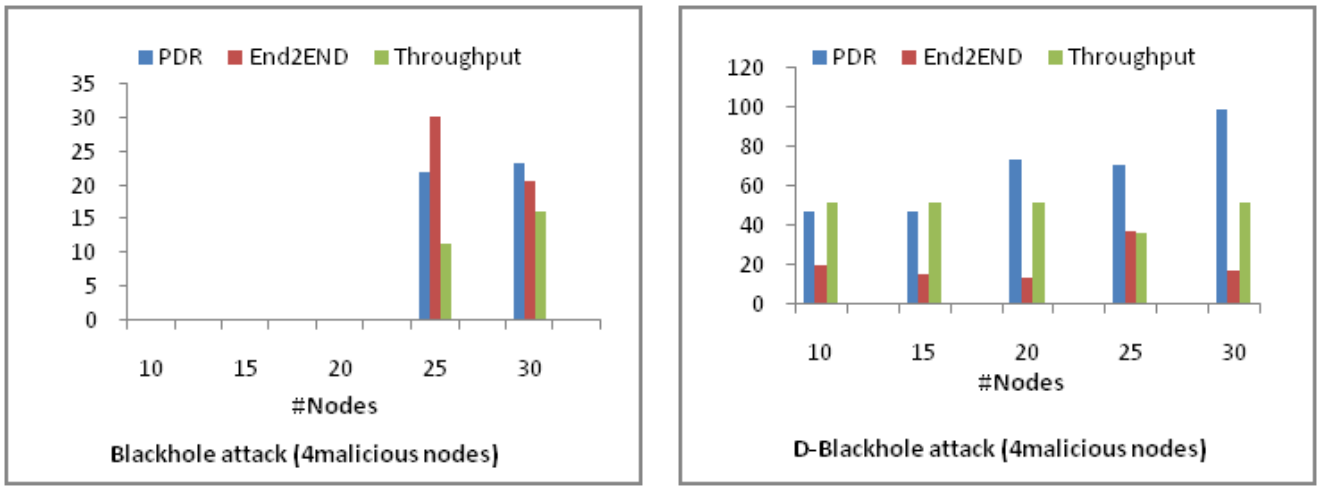

Figure III.10 – Résultat du SP-AACK avec quatre trous noir (multiple BlackHole)

Dans certains cas, on remarque que le délai de bout en bout est nul, cela signifie qu'aucun paquet n'est livré. Sinon, il augmente légerement à cause du grand nombre de paquets récupérés.

III.7.2 PDR par rapport au nombre de nœuds de trous noirs

Comme le montre le tableau III.2, les nœuds malveillants ont une influence directe sur le PDR. Un nombre élevé de nœuds malveillants peut impliquer une réduction du PDR. Par exemple, le PDR dans un réseau de 20 nœuds avec 2 nœuds malveillants est de 23,22%, avec 3 nœuds malveillants est de 1,02% et avec 4 nœuds malveillants est de 0%.
En contrepartie, le PDR dans un réseau de 30 nœuds avec 2 nœuds malveillants est de 23,67%, avec 3 nœuds malveillants est de 27% et avec 4 nœuds malveillants est de 23,42%. En général, la présence d'un ou plusieurs nœuds malveillants diminue le PDR.

Dans la plupart des cas, la taille du réseau a également son impact sur le PDR. Par exemple, pour le cas de deux nœuds malveillants, le PDR dans un réseau de 10 nœuds est de 0,21% par contre le PDR dans un réseau de 30 nœuds atteint 22,61%. Ces deux facteurs (la taille du réseau et le nombre de nœuds malveillants) ont une influence sur le PDR.

Si nous remarquons bien dans le tableau III.2, notre approche donne de meilleurs résultats même si le réseau contient un nombre considérable de nœuds (sans tenir compte du nombre de nœuds malveillants), le PDR atteint de 93% à 99%.

# Nodes	# Black hole nodes	PDR	
		Black hole	D-Black hole
10	1	23.42	47.06
	2	0.21	73.64
	3	0.2	47.3
	4	0	47.28
15	1	25.46	100
	2	24.3	99.58
	3	1.22	73.64
	4	0	47.28
20	1	48.88	74.08
	2	23.22	100
	3	1.02	73.22
	4	0	73.6
25	1	21.18	67.21
	2	21.18	74.58
	3	22.4	73
	4	22	71.28
30	1	36.46	93.28
	2	22.67	93.28
	3	27	93
	4	23.42	99

Table III.2 – PDR VS Nombre des noeuds trou noire

III.7.3 SP-AACK par rapport à AODV natif

Pour montrer l'efficacité de SP-AACK, nous le comparons aux valeurs d'un AODV natif. Pour cela, nous avons pris un exemple de 30 nœuds avec 4 nœuds malveillants.

Les métriques de comparaison sont toujours le PDR, le débit et le délai de bout en bout. Comme le montre la Figure III.11, SP-AACK fournit des résultats progressifs par rapport au nombre de nœuds du réseau. En prenant, par exemple, un réseau de 10 nœuds, le PDR en AODV natif est de presque 100 %, en présence de nœuds de trous noirs est pratiquement de 0 % et en SP-AACK est de 47 %, il n'est pas parfait comme celui de l'AODV natif mais nous avons quand même pu récupérer 47% des paquets perdus (ceci dû à la présence de 4 nœuds malveillants sur 10 nœuds au total). Si nous prenons maintenant un réseau de 30 nœuds, le PDR avec trou noir est de 23,42 %, le PDR obtenu avec SP-AACK est de 99 %, ce qui est presque le même obtenu dans l'AODV natif.

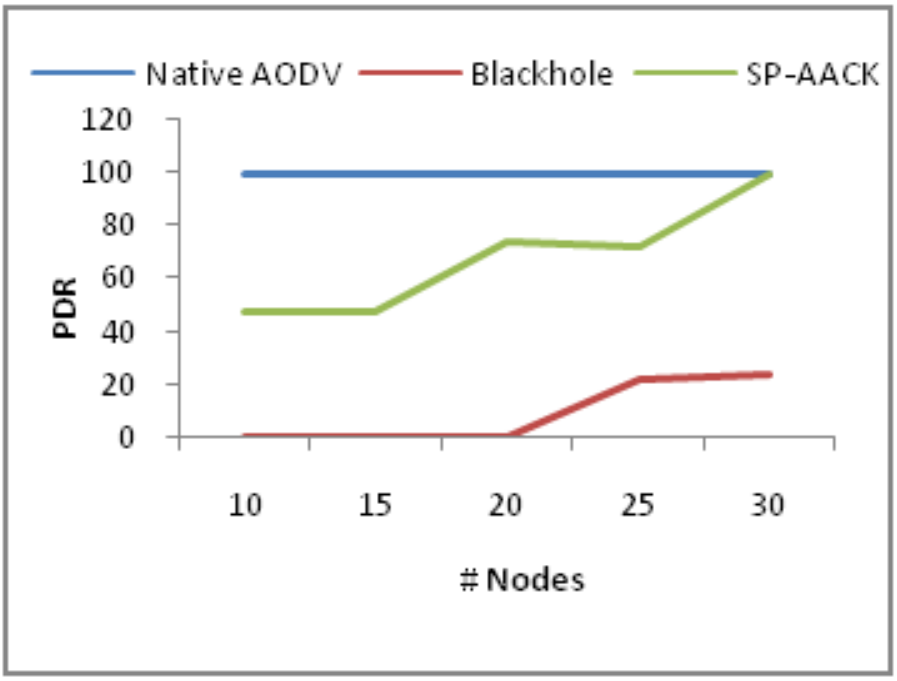

Figure III.11 – Comparaison du PDR

La figure III.12 montre une comparaison en termes de délai de bout en bout. Il est clair dans la figure que SP-AACK donne un délai de bout en bout meilleur que celui de l'AODV natif.

Concernant le débit, la figureIII.13 montre les résultats obtenus pour les 3 scénarios. le Débit obtenu par SP-AACK est quasiment identique à celui obtenu dans l'AODV natif à l'exception du réseau de 25 nœuds qui est un peu réduit et ceci dû à la perte de certains paquets que nous

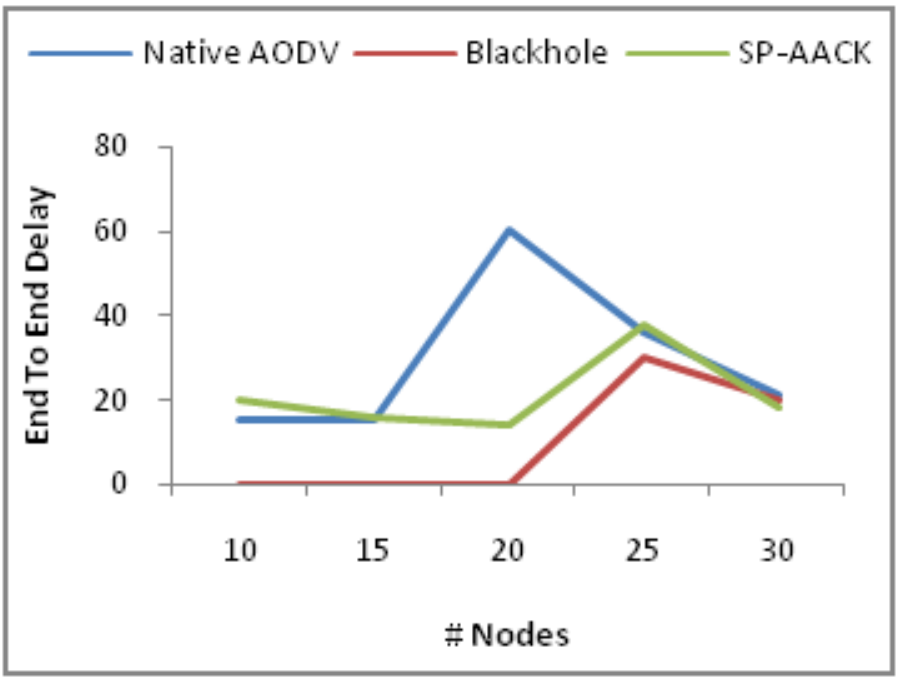

Figure III.12 – Comparaison du délai de bout en bout(EndToEnd Delay)

n'avons pas pu récupérer (si on revoit un coup d'œil dans Tableau III.2, on voit que le PDR pour un réseau de 25 nœuds avec 4 trous noirs peut diminuer par rapport à l'autre, ce qui justifie la diminution du débit).

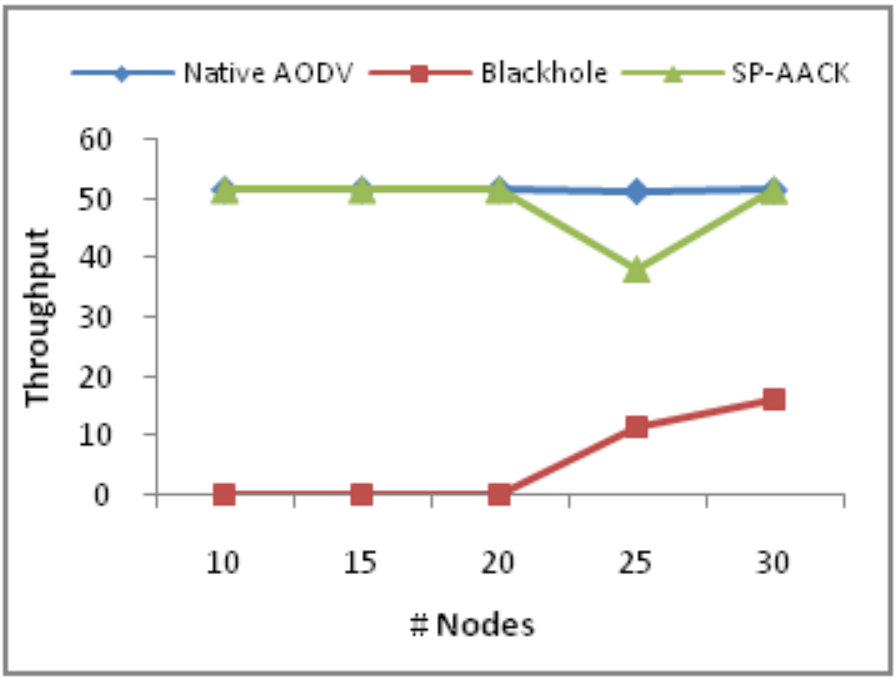

Figure III.13 – Comparaison du délai du débit(Throughput)

III.7.4 SP-AACK par rapport à d'autres approches

Pour garantir l'efficacité de notre solution, nous l'avons comparée avec d'autres approches discutées dans (Hamamreh A,2018) ; notant R-AODV, RID-AODV et Enhanced RID-AODV. Pour ces approches, nous avons calculé les 3 métriques de performance (PDR, End To End delay et Throughput), avec un nombre de nœuds trou noir qui varie entre 1, 2, 3 et 4 nœuds. La figure III.14 montre que le PDR obtenu avec SP-AACK est bien meilleur que les autres approches, cela est dû à l'efficacité de notre solution en termes de récupération des paquets perdus. La figure 15 montre l'impact du nombre de nœuds de trous noirs sur le débit, donc le

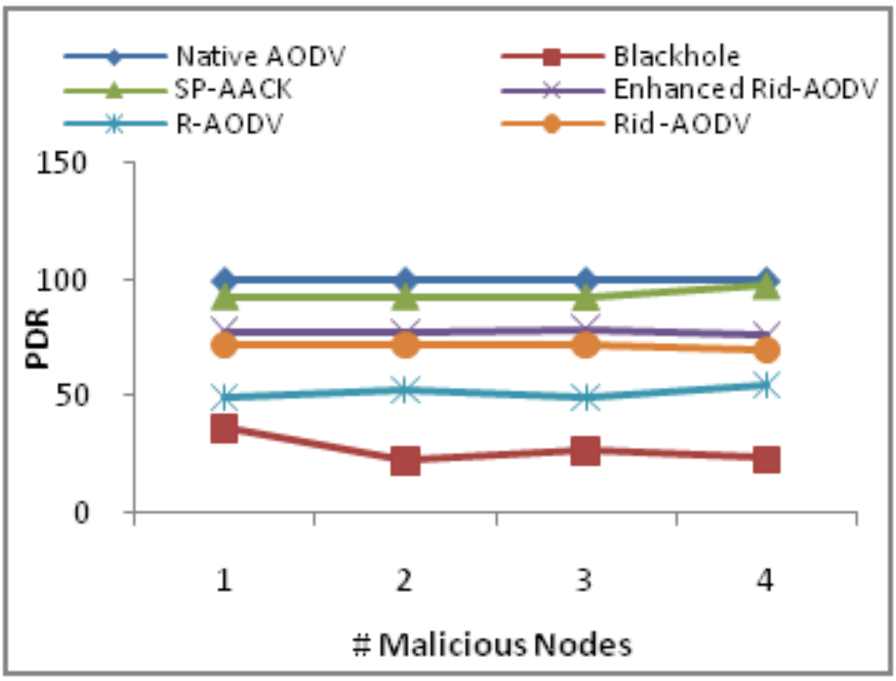

Figure III.14 – PDR dans les différents protocoles

résultat obtenu pour les solutions. Il est clair que SP-AACK est le meilleur pour le débit suivi de Enhanced RID-AODV puis les autres. L'un des points forts de SP-AACK, est d'avoir un délai End To End réduit par rapport à l'autre, sauf celui pour R-AODV qui est quasiment égal à celui obtenu par SP-AACK. Les résultats obtenus sont présentés dans la figure III.16.

III.7.5 SP-AACK par rapport aux approches d'apprentissage automatique

L'apprentissage automatique est l'un des outils de détection d'intrusion les plus utilisés, en particulier pour la détection d'attaques par trou noir. Nous avons fait une petite comparaison

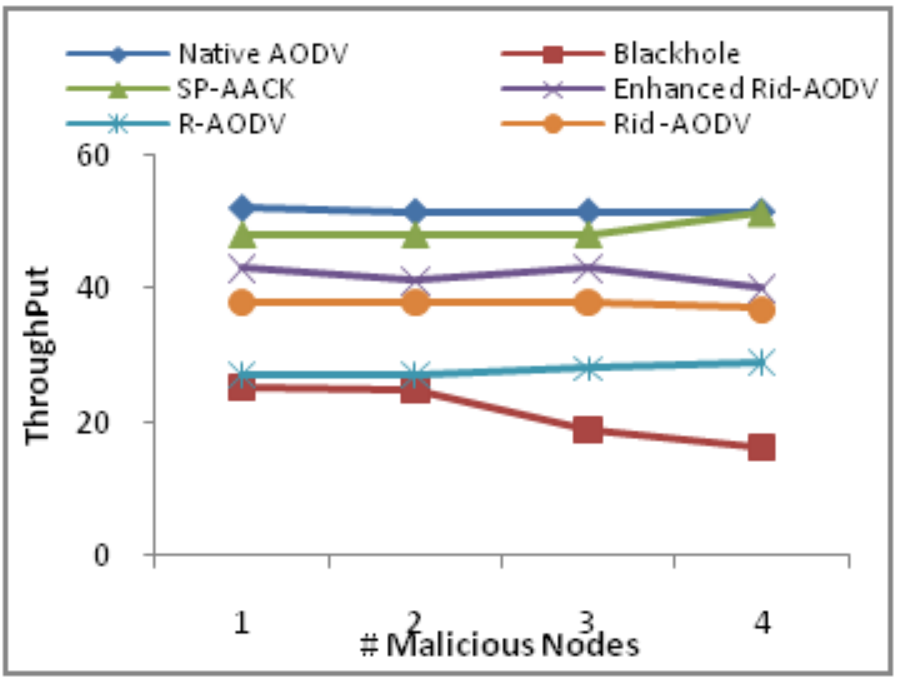

Figure III.15 – Délai de bout en bout dans les différents protocoles

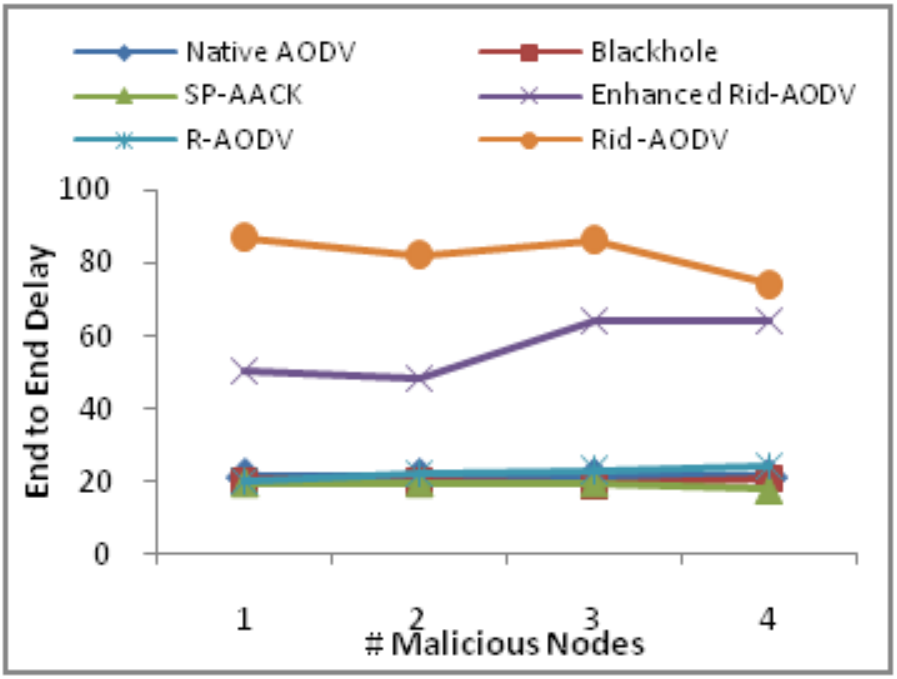

Figure III.16 – Délai de bout en bout dans les différents protocoles

entre SP-AACK et certaines solutions basées sur l'apprentissage automatique. Cette comparaison nous permettra de positionner la solution existante et d'envisager les perspectives et les améliorations nécessaires à une détection très efficace. Nous avons choisi des réseaux contenant 20, 30 et 40 nœuds avec des nœuds simples et 2 trous noirs. La comparaison se fait entre SP-AACK et des solutions basées sur le machine learning notamment BDD-AODV, Mi-AODV

et hybride en termes de PDR. Les résultats obtenus sont présentés dans les figures III.17 et III.18.

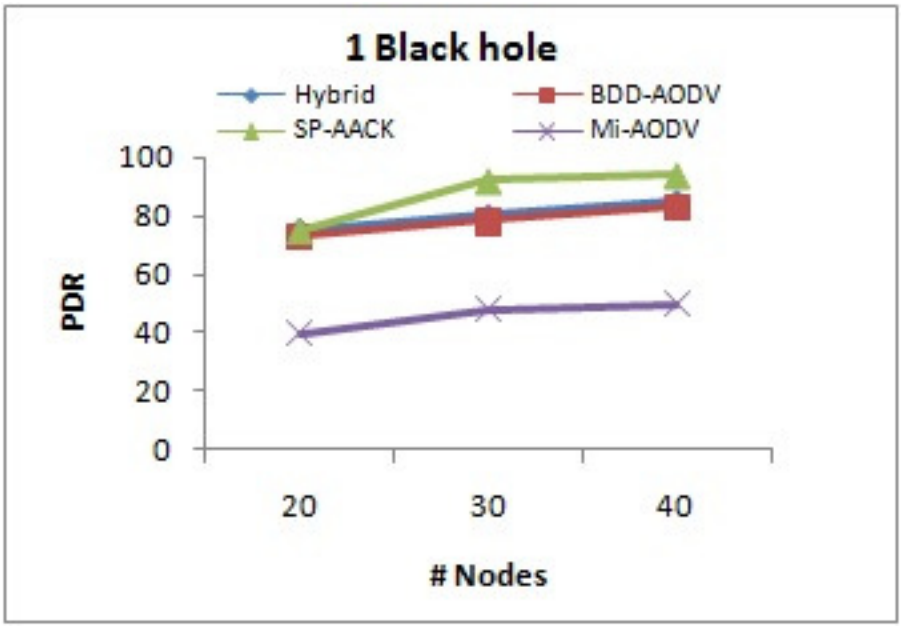

Figure III.17 – Comparaison PDR pour un noeud trou noir

Il est clair que SP-AACK donne un nombre significatif de paquets par rapport aux autres techniques. Sur la base de cette analyse, l'utilisation de l'apprentissage automatique combiné à SP-AACK est très intéressante.

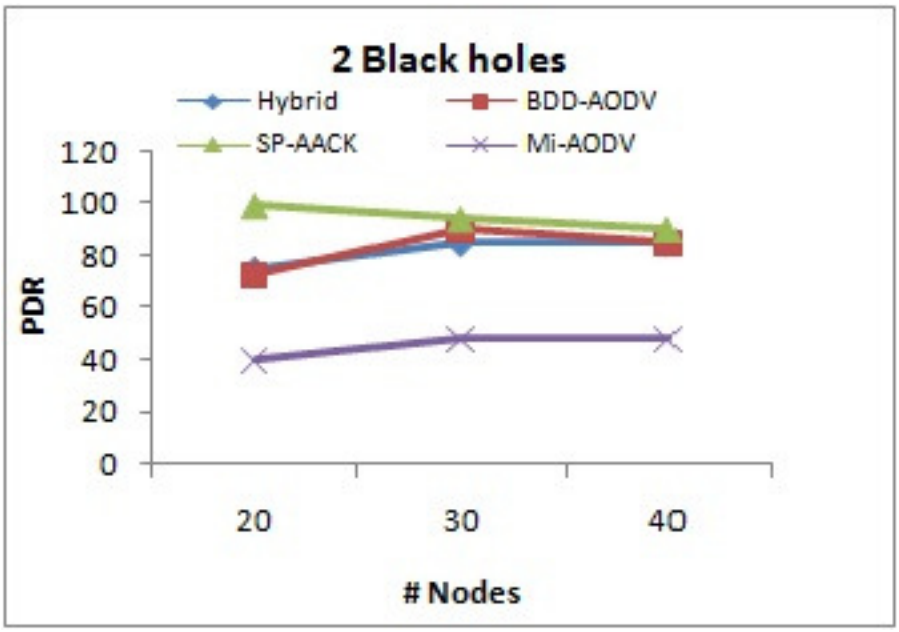

Figure III.18 – Comparaison PDR pour deux noeud trou noir

III.8 Conclusion

L'attaque par trou noir est l'une des attaques les plus sérieuses que l'on puisse infuser sur un réseau MANET, car elle permet la perte d'un grand nombre de paquets. Cette perte diminue le PDR et le débit et perturbe le délai de bout en bout. Notre approche est basée sur AACK appelé SP-AACK (SPlitted AACK), il suffit de scinder chaque fois que l'AACK n'est pas reçu. Cette solution nous permet de détecter les attaques de trous noirs simples et multiples. SP-AACK nous a permis d'augmenter le PDR a +72 en moyenne.

Plusieurs approches ont été proposées, chacune avec ses forces et ses faiblesses. Les résultats obtenus ont montré que SP-AACK est meilleur notamment en PDR et en Débit. En ce qui concerne le délai de bout en bout, il donne de bons résultats en équivalence avec les autres modèles proposés. L'envoi d'accusés de réception peut créer une surcharge, ce qui est une limitation. Par conséquent, des techniques d'améliorations supplémentaires sont nécessaires pour le réduire. Une comparaison avec certains apprentissages automatiques basés sur des solutions est faite pour donner une vision des travaux futurs.

CHAPITRE IV

DÉTECTION A BASE D'APPRENTISSAGE AUTOMATIQUE

IV.1 Introduction

L'évolution croissante de l'informatique, notamment dans le domaine des réseaux et de la communication a donné naissance à plusieurs types de réseaux. Les réseaux mobiles ad hoc (MANET) sont les réseaux d'aujourd'hui, compte tenu de leur simplicité, surtout avec l'absence d'infrastructure fixe. La sécurité est un problème sérieux dans ce type de réseaux car les attaques peuvent provenir de l'intérieur ou de l'extérieur et influencer le contrôle du trafic ou le trafic des données. Cependant, plusieurs études de recherche ont été entreprises dans le but de créer un système de détection d'intrusion (IDS) robuste et efficace (Iwendi et al., 2020) (Nayyar Mahapatra, 2020) (Mahin et al., 2019). Parmi les techniques modernes utilisées pour la création de celles-ci, l'adoption des techniques de la classification est très intéressante, notamment l'utilisation du Machine Learning.

Cette technique nécessite deux elements principaux ; tout d'abord, un ensemble de données (pour la formation et les tests) et un classificateur pour donner un sens à l'énorme quantité de données disponibles.

Des méthodologies supervisées et non supervisées (Kumar et al, 2007) sont utilisées pour faire une classification des données. De plus, dans la méthode supervisée, dite prédictive, toutes les classes possibles sont connues à l'avance contrairement à la méthode non supervisée dite descriptive ou indirecte.

Dans cette recherche, nous appliquons la technique des arbres de décision et spécialement les forêts aléatoires, avec une sélection des caractéristiques les plus importantes, sur les paquets MANET entrants pour classer les données de manière efficace afin de prédire correctement s'il s'agit d'un paquet provenant d'une attaque ou non.

La contribution majeure de ce travail est de sélectionner les caractéristiques les plus appropriées (M-best features) en calculant l'influence de chaque caractéristique sur la précision totale. Les caractéristiques qui ont une grande influence seront sélectionnées comme les meilleures caractéristiques et seront utilisées dans la phase d'apprentissage.

IV.2 Etat de l'art

Les réseaux MANET sont exposés à plusieurs types d'attaques en raison de leur vulnérabilité causée par l'absence d'infrastructure fixe. D'autre part, plusieurs recherches ont été faites pour

remédier ce problème. Dans ce qui suit, un ensemble de ces recherches est présenté.

Le protocole hybride est une combinaison du protocole BDD-AODV et du protocole MI-AODV (khamayseh et al., 2011). Le protocole MI-AODV a un champ de confiance indiquant si la fiabilité du nœud de réponse . Le protocole hybride a deux tables : une table de confiance et une table noire. De plus, chaque nœud source du réseau possède une table de comptage.

(Saurabh et al., 2017) ont proposé une méthode basée sur le clustering pour la détection et la prévention des attaques de trous noirs dans le protocole de routage AODV dans les réseaux MANET. Ce modèle suggère que les caractéristiques physiques sont similaires pour tous les nœuds. Les nœuds approuvés par défaut sont le nœud de destination et les nœuds prédécesseurs. Tout nœud abandonnant la moitié du nombre total de paquets est considéré comme un nœud trou noir. Le chef de cluster est choisi comme un nœud situé au centre du cluster. Pour détecter la différence exclusive entre le nombre de paquets de données reçus et transmis par les nœuds. Chaque membre de l'unité envoie une fois un ping à la tête du cluster. Si le défaut est perçu, tous les nœuds masqueront les nœuds contagieux du réseau. Les expériences sont faites sur NS-2 en comparant le PDR, l'énergie, le débit et le délai de bout en bout.

(Behzad, 2018) ont proposé une alarme de protocole DSR pour se défendre contre les attaques de trous noirs dans les réseaux MANET. Il s'appelle AIS-DSR (Système Immunitaire Artificiel DSR) et utilise l'AIS (*Artificial Immune System DSR*) qui s'inspire du mécanisme du système immunitaire humain. L'objectif est de pouvoir identifier les nœuds isolés et de les retirer du routage en fonction du comportement des nœuds du système. Des simulations approfondies sur l'environnement NS-2 ont été développées pour évaluer cet algorithme. Les résultats de l'AIS-DSR sont excellents d'environ 20 % par rapport au DSR en termes de PDR, de débit et de délai de bout en bout.

(Mahin et al., 2019) proposent une approche pour l'interception et la détection des attaques par trou noir dans le protocole DYMO. Leur méthode se résume en trois phases : plantation, détection et interception. Plusieurs classifieurs ont été utilisés, notant l'arbre de décision, la machine à vecteur de support, K plus proches voisins et le réseau de neurones. Le travail a été simulé dans MATLAB et les résultats ont révélé que les classificateurs SVM donnaient plus de précision que les autres.

(Khamayseh et al., 2019) ont proposé deux protocoles, à savoir BDD-AODV et un protocole Hybride, qui ont été construits en modifiant l'AODV original. Dans le protocole BDD-AODV, chaque nœud MANET possède trois tables : une table de confiance comprenant les nœuds

de confiance des réseaux, une table noire comprenant les nœuds malveillants et une table de comptage, qui contient toutes les statistiques concernant le RREP. Ce protocole utilise le jeu de données BDD (Yassein et al., 2016) DPAA-AODV est une technique proposée par (Albalas et al., 2019) pour la détection et la prévention contre les attaques actives telles que le trou noir et le trou gris. Cette méthode comporte deux phases. La première phase (phase hors ligne) contient les modules suivants : sélection des données, sélection des fonctionnalités et détection. Dans le module de sélection des fonctionnalités, l'algorithme de classification ReliefF (Albalas et al., 2019) est utilisé sur le jeu de données BDD (choisissez les fonctionnalités les plus pertinentes et éliminez les redondances pour augmenter le taux de détection). Dans la deuxième phase (phase en ligne), si les caractéristiques précédentes sont fréquemment détectées pour les nœuds du réseau et dépassent un seuil prédéfini. Ce nœud sera perçu comme un nœud Black-Hole et sera exclu et évité des routes.

Les méthodes classiques de cryptographie sont devenues limitées pour la détection d'intrusion dans les MANET. Pour y parvenir, plusieurs recherches récentes se basent sur le deep learning pour garantir la sécurité et éliminer les intrus. Pour faciliter le choix d'un algorithme DL, (Laqtib et al., 2019) ont fait une comparaison entre plusieurs d'entre eux notant, notamment CNN, Inception-CNN, Bi-LSTM et GRU. Ces algorithmes ont été appliqués sur le jeu de données NSL-KDD.

(Iwendi et al., 2020) ont proposé une méthode avec des classificateurs d'ensemble (Bagging et Adaboost) qui a une haute précision, un taux de détection de paquets élevé et un faible taux de fausses alarmes, pour améliorer le système de détection d'intrusion . Les auteurs ont construit des modèles d'ensemble d'apprentissage automatique avec des classificateurs de base (Random Forest, Reptree et J48). Une classification multiclasse et binaire a été effectuée (appliquée) pour les jeux de données KDD99 et NSLKDD. Toutes les attaques ont été considérées comme une anomalie et un trafic normal. Cinq attaques majeures sont étiquetées, à savoir le déni de service (DoS), la sonde, les attaques utilisateur-racine (U2R), les attaques racine-local (R2L) et les attaques de classe normale.

(Nayyar Mahapatra, 2020) ont proposé une méthode de classification des données entrantes dans les MANET et de réduction de l'ensemble de données à l'aide de la technique RF/ET (Random Forest/Ensembl Tree). Cette approche facilite une classification spécifique de la grande masse de données (données ingérables).

L'évaluation a été appliquée sur l'ensemble de données NSL-KDD et les résultats ont indiqué

que le modèle proposé a atteint un niveau de précision de 86 % dans la gestion des paquets de données dans les MANET.

(Xu, 2021) a collecté son propre ensemble de données en effectuant des simulations sur GloMoSim2 pour trois attaques, dont Blackhole, Flood et Packet Loss. Ensuite, il s'est appliqué sur plusieurs algorithmes d'apprentissage automatique. L'analyse des résultats a montré que les perceptrons multicouches, la régression logistique et les machines à vecteurs de support ont un niveau de détection plus élevé. (Liu Shi, 2019) proposent un classificateur de forêt aléatoire optimisé pour la détection d'intrusion. L'optimisation consiste en la sélection de fonctionnalités. Ils ont opté pour l'utilisation d'algorithmes génétiques pour la sélection des caractéristiques. Le modèle proposé est testé sur deux ensembles de données différents ; NSL-KDD et UNSW-NB15. Les résultats obtenus en termes d'exactitude, F1-Score, Rappel et précision sont respectivement de 96,12%, 88,25%, 86,35%, 90,23% pour NSL-KDD et 92,06%, 94,27%, 96,26%, 92,36% pour UNSW-NB15. Dans ce travail, un classificateur de forêt aléatoire optimisé est également proposé. Ce modèle est basé sur la sélection des caractéristiques les plus importantes en mesurant leur impact.

(Mohammed Gbashi, 2021) ont proposé un système de détection d'intrusion utilisant un réseau neuronal profond (DNN) et un réseau neuronal récurrent (RNN) pour la classification avec élimination récursive de certaines fonctionnalités. La technique proposée a été testée à l'aide de l'ensemble de données NSL-KDD, qui a fourni un taux de précision élevé allant jusqu'à 94 %.

Deux approches ont été mises en œuvre en (Belgrana et al., 2021). La première consiste à utiliser CNN pour réduire le nombre de packages dans NSL-KDD puis réduire le nombre d'attributs par une sélection de caractéristiques pertinentes. Les attributs sélectionnés sont 22 sur 42. La deuxième approche est appelée réseau de neurones RBF adaptatif. Il est utilisé pour la sélection des attributs via sa fonction objectif.

IV.3 Modele proposé

La solution proposée peut se résumer en deux phases avant apprentissage : une phase de normalisation des données et une phase de sélection des meilleures fonctionnalités.

IV.3.1 Artcitecture du modèle proposé

La figure IV.1 présente le processus général du notre modèle. Aprés importation des données, elles doivent être normalisés. Les données d'apprentissage passeront sur une étape de sélection des d'attributs/caractéristiques les plus importantes afin d'avoir un efficace ; ce qui engendre la génération d'un modèle robuste. Dans ce qui suit, nous donnerons plus de détaille pour chaque phase du modèle.

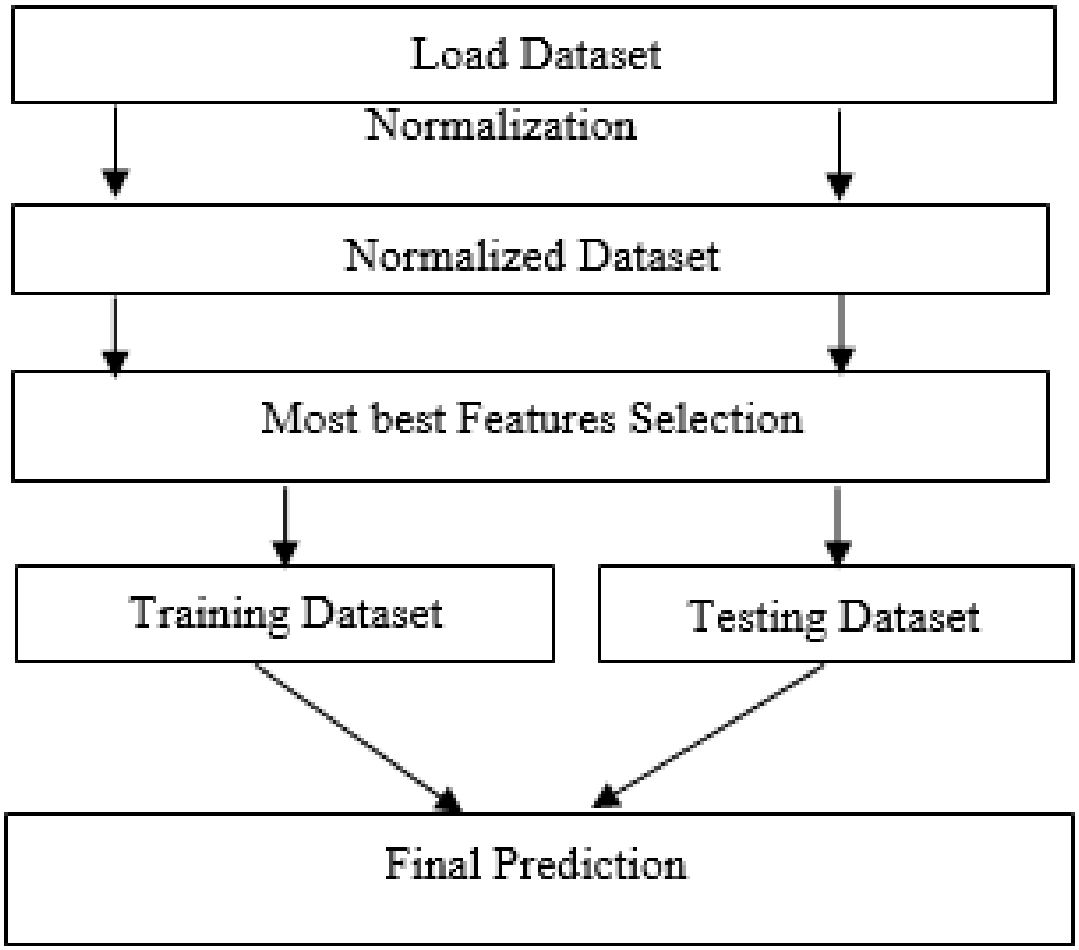

Figure IV.1 – Modèle proposé

IV.3.2 Normalisation

Il existe plusieurs méthodes de normalisation, dans cette recherche. La normalisation min-max est utilisée. C'est l'un des moyens les plus courants de normaliser les données. Son principe est assez simple. La valeur minimale de chaque caractéristique est transformée en 0 et sa valeur

maximale est transformée en 1. Par conséquent, toutes les autres valeurs sont transformées en un nombre décimal compris entre 0 et 1 avec la formule suivante :

$$\frac{Valeur - Min}{Max - Min} \tag{IV.1}$$

Par exemple, si la valeur minimale d'une caractéristique était de 10 et la valeur maximale de 50, alors 10 serait transformé en 0, 50 serait transformé en 1 et 30 deviendrait 0,5 (c'est à mi-chemin entre 10 et 50).

Après application de cette technique, toutes les caractéristiques sont dans le même périmètre et ont la même pondération.

IV.3.3 Algorithme Random Forest

C'est une technique couvrant une grande partie des problèmes de Machine Learning compte tenu de sa simplicité d'interprétation et de sa stabilité. Il a généralement une bonne précision et peut être utilisé pour des tâches de régression ou de classification.

Dans Random Forest (breiman, 2001), il y a d'abord le mot « Forest » qui sous-entend que cet algorithme sera basé sur des arbres appelés arbre de décision.

Les arbres de décision (Jehad et al, 2012) incarnent une approche de classification supervisée. L'idée est venue de la structure arborescente ordinaire qui est composée d'une racine et de nœuds (les positions où les branches se divisent), de branches et de feuilles. De manière similaire, un arbre de décision est construit à partir de nœuds qui représentent des cercles et les branches sont représentées par les segments qui relient les nœuds. Un arbre de décision part de la racine, se déplace vers le bas et est généralement dessiné de gauche à droite. Le nœud à partir duquel l'arbre commence est appelé un nœud racine. Le nœud où se termine la chaîne est appelé nœud « feuille ». Deux branches ou plus peuvent être étendues à partir de chaque nœud interne, c'est-à-dire un nœud qui n'est pas un nœud feuille. Un nœud représente une certaine caractéristique tandis que les branches représentent une plage de valeurs. Ces plages de valeurs agissent comme des points de partition pour l'ensemble des valeurs de la caractéristique donnée. La figure IV.2 décrit la structure d'un arbre. Le regroupement des données dans l'arbre de décision est basé sur les valeurs des attributs des données. Un arbre de décision est réalisé à partir des données pré-classifiées. La division en classes est décidée en fonction des caractéristiques qui divisent le mieux les données. Les éléments de données sont divisés en fonction des valeurs de

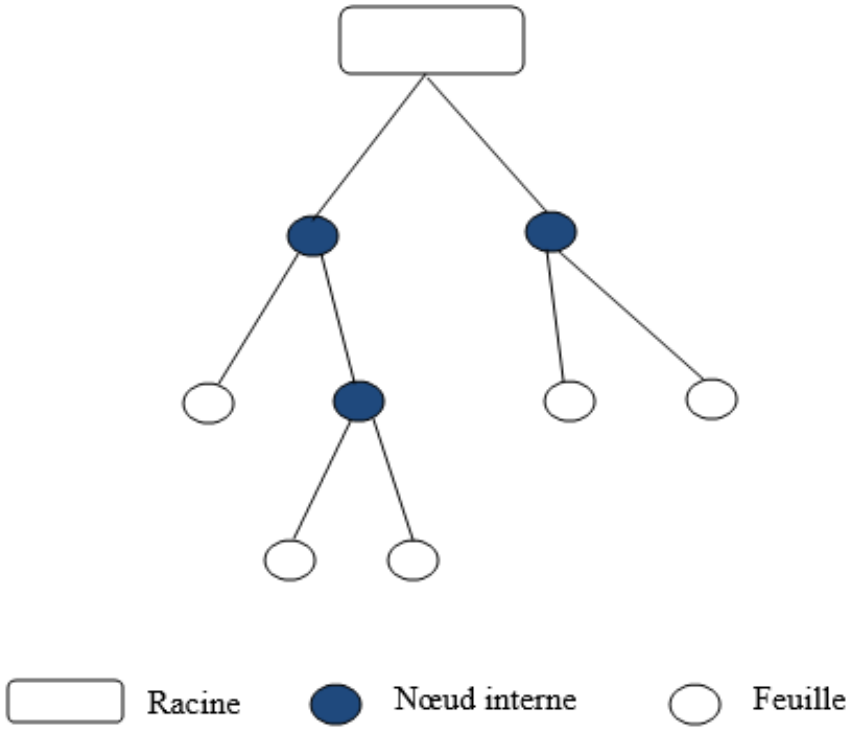

Figure IV.2 – Structure d'un arbre de décision

ces caractéristiques. Ce processus est appliqué à chaque sous-ensemble divisé des éléments de données de manière récursive. Le processus se termine dès que tous les éléments de données du sous-ensemble actuel appartiennent à la même classe.

Finalement, un arbre de décision aide à prendre une décision grâce à une série de questions (aussi appelées tests) dont la réponse (oui/non) conduira à la décision finale. Sur l'arbre, chaque question correspond à un nœud, c'est-à-dire à un endroit où une branche se scinde en deux branches. A chaque nœud, l'algorithme demande quelle question à poser.

Les forêts aléatoires peuvent être constituées de plusieurs dizaines voire centaines d'arbres. Le nombre d'arbres est un paramètre généralement ajusté par validation croisée (c'est une technique d'évaluation d'un algorithme de Machine Learning consistant à entraîner et tester le modèle sur des morceaux du jeu de données de départ).

Chaque arbre est formé sur un sous-ensemble de l'ensemble de données et donne un résultat. Les résultats de tous les arbres de décision contribuent à une réponse finale. Chaque arbre "vote" (oui ou non) et la réponse finale détermine celui qui a obtenu le vote majoritaire. (C'est ce qu'on appelle une méthode d'ensachage). De cette façon, nous construisons un modèle robuste à partir de plusieurs modèles qui ne sont pas nécessairement aussi robustes.

On peut résumer les étapes impliquées dans l'algorithme random forest comme suit :

Étape 1 : Dans la forêt aléatoire, un nombre n d'enregistrements aléatoires est extrait de l'ensemble de données contenant un nombre k d'enregistrements.

Étape 2 : Des arbres de décision individuels sont construits pour chaque échantillon.

Étape 3 : Chaque arbre de décision générera une sortie.

Étape 4 : Le résultat final est considéré sur la base du vote à la majorité ou de la moyenne pour la classification et la régression respectivement (Dans notre cas la majorité). La figure IV.3 illustre le fonctionnement de l'algorithme.

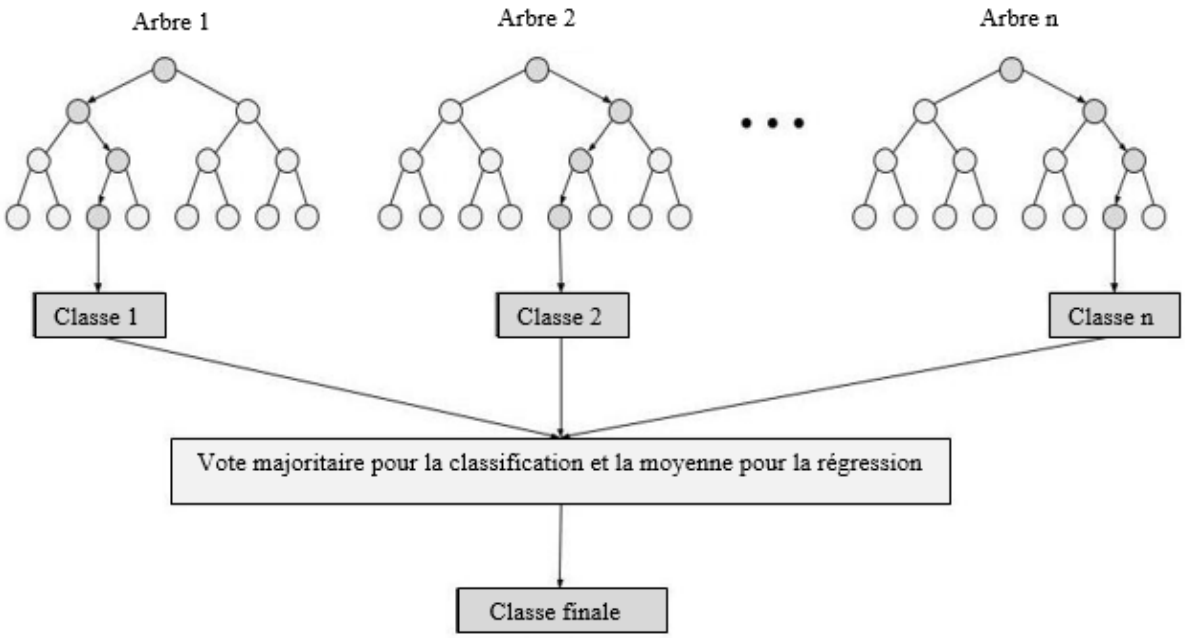

Figure IV.3 – Principe de l'algorithme Random Forest

Cet algorithme permet aussi de faire du pré-traitement, notament la sélection efficace des caractéristiques (Attributs/Features) importantes (Saarela M al,2021). Dans ce qui suit, nous proposons une technique pour la sélection des attributs les plus importants. Pour conclure, cet algorithme est très apprécié pour sa capacité à combiner les résultats de ses arbres pour obtenir un résultat final plus fiable. Son efficacité lui a permis d'être utilisé dans de nombreux domaines, dont la détection d'intrusion.

IV.3.4 Sélection des attributs

Le terme importance de la caractéristique est utilisé pour décrire l'importance de la caractéristique pour les performances de classification d'un modèle. Elle est référée à l'importance des caractéristiques en tant que mesure de la contribution individuelle de la caractéristique correspondante pour un classificateur particulier ou à l'effet de la caractéristique pour le modèle. Cela signifie que l'importance des caractéristiques des données d'entrée dépend du modèle de classification correspondant et qu'une caractéristique importante pour un modèle peut être sans importance pour un autre modèle.

Généralement, les importances des caractéristiques peuvent être divisées en importances modulaires globales et locales. Alors qu'une importance de caractéristique globale modulaire mesure l'importance de la caractéristique pour l'ensemble du modèle, une importance locale mesure la contribution de la caractéristique pour une observation spécifique.

Dans cette étude, la méthode adoptée pour la sélection des caractéristiques consiste à mesurer directement l'influence de chaque caractéristique sur l'exactitude (Accuracy) du modèle.

Le principe général est que la valeur de chaque caractéristique est permutée, puis on mesure dans quelle mesure cette permutation diminue la précision du modèle (Khalladi et al,2022). Puisque, nous avons déja fait une normalisation des données, toutes les valeurs sont compromises ente 0 et 1. D'ou La fonction f est définie par

$$f(x) = 1 - x$$

. On a alors

$$f(x) = 0 \iff x = 1 \tag{IV.2}$$

Évidemment, pour les variables importantes, la permutation diminue considérablement l'accuracy du modèle. En revanche, la permutation des variables moins importantes n'aura aucun effet ou un effet minime.

$$\delta = \frac{Accuracy_{Nouvelle}}{Accuracy_{Totale}} \tag{IV.3}$$

Nous proposons de ne conserver que les meilleures caractéristiques (Most best features), et de supprimer les autres caractéristiques qui ont un impact inférieur ou égal à un seuil d'impact

sur l'exactitude totale selon la formule (IV.3) (Khalladi et al,2022).

Le seuil delta est utilisé pour sélectionner les meilleures caractéristiques en le comparant à l'influence de chaque caractéristique sur la valeur de précision totale. Nous avons opté pour une valeur delta = 10 %.

Algorithm 2 Features Selection

Require:
Original set of features F={ $F_1, F_2, ...F_n.$}
Delta // Threshold
Output : Most-Best Features
Start
Calculate Accuracy Total // Accuracy Total of dataset
For i = 1 **to** n **Do**
Permute Value ( ) // Permute the value of feature i
Calculate Accuracy (Permuted value ( ))
If Accuracy (Permuted value ( )) / Accuracy Total <= Delta
F ← F - { F_i}//Remove the feature that has minimal or no impact
Else F ← F // No feature removed
End.

IV.4 Expérimentations

IV.4.1 Ensemble de données

Depuis 1999, KDD Cup 99 (Tavallaee M al,2009) est utilisé comme un ensemble de données dans les systèmes de détection d'intrusion. Chaque paquet (instance) se compose de 41 champs et est étiqueté comme paquet normal ou paquet anormal avec des types d'attaque, notant que 37 sont des champs de type numérique et 4 sont des champs de type non numérique. KDD99 contient 37 types d'attaques répartis en quatre grandes classes : DOS, U2R, R2L et Probes.

DOS (Denial of service attaks) : sont des attaques qui visent à miner la disponibilité des services en saturant les ressources de la machine cible, du serveur ou du réseau. Ces attaques réussies dans les réseaux ont pour conséquence immédiate le blocage du trafic réseau.

Probes : vise à recueillir des informations sur la cible susceptible d'aider l'attaquant à lancer une attaque. Il existe de nombreux types d'attaques par sondes.

R2L (Remote To Local) : ces attaques contournent ou usurpent les paramètres d'authen-

tification d'une cible afin d'exécuter des commandes. La plupart de ces attaques proviennent de l'ingénierie sociale.

U2R (User To Root) : Ce type d'attaque vient de l'intérieur. L'attaquant usurpe le mot de passe du super administrateur et par conséquent des autres utilisateurs. La plupart de ces attaques résultent de la saturation du buffer provoquée par les erreurs de programmation.

NSL-KDD est un ensemble de données proposé pour résoudre certains des problèmes inhérents à l'ensemble de données KDD'99 (Tavallaee M al,2009). De plus, le nombre d'enregistrements dans les ensembles d'apprentissage (*training*) et de test (*testing*) NSL-KDD est raisonnable. Cet avantage rend abordable l'exécution des expériences sur l'ensemble complet sans qu'il soit nécessaire de sélectionner au hasard une petite partie. Par conséquent, les résultats d'évaluation des différents travaux de recherche seront cohérents et comparables. NSL-KDD est toujours appliqué comme un ensemble de données de référence efficace pour aider les chercheurs à comparer différentes méthodes de détection d'intrusion.

IV.4.2 Paramètres d'évaluation

Dans le domaine de l'apprentissage automatqiue, il est nécessaire de savoir que l'apprentissage ne se fait pas sur tout l'ensemble de données. Les données sont divisés en deux sous ensemble : ensemble pour l'apprentissage (Généralement 80% des données) et le reste pour le test. Il est évident de savoir que les données utilisées pour le test ne sont pas les mèmes utilisées dans la phase d'apprentissage. Un modèle d'appretissage est evalué selon plusieurs métriques. Nous présentront ici, les métriques les plus populaires.

TP (True Positives) : cas où la prédiction est positive et la valeur réelle est effectivement positive.

TN (True Negatives) : cas où la prédiction est négative et la valeur réelle est effectivement négative.

FP (False positif) : cas où la prédiction est positive, mais la valeur réelle est négative.

FN (False Negative) : cas où la prédiction est négative, mais la valeur réelle est positive.

$$ConfusionMatrix = \begin{pmatrix} TP\ FP \\ FNTN \end{pmatrix} \tag{IV.4}$$

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \tag{IV.5}$$

$$Precision = \frac{TP}{TP + FP} \tag{IV.6}$$

$$Recall = \frac{TP}{TP + FN} \tag{IV.7}$$

$$F1 - Score = \frac{2 * Precision * Recall}{Precision + Recall} \tag{IV.8}$$

$$FalsePositiveRate(FPR) = \frac{FP}{FP + TN} \tag{IV.9}$$

IV.5 Résultats & discussion

Dans cette section, nous montrerons a travers les résultats obtenus, l'impact de la normalisation et la selection des attributs importants dans l'apprentissage. Puis, nous les comparerons avec d'autres modéles.

IV.5.1 Impact de la normalisation des données et de la sélection des Attributs

Pour tester l'efficacité du modèle proposé, trois (3) scénarios ont été lancés sur Python en utilisant le même jeu de données, et basés sur le même algorithme (Random Forest). Nous avons appliqué le classifieur Random Forest directement à l'ensemble de données sans prétraitement (normalisation). Le deuxième scénario consiste à normaliser le jeu de données avant l'application de Random Forest. Enfin, nous avons appliqué Random Forest avec sélection des caractéristiques importantes sur l'ensemble de données normalisé.

La normalisation de l'ensemble de données a entraîné une augmentation de l'accuracy d'environ 7,7 %. Ainsi, la sélection des attributs sur l'ensemble de données normalisé a donné une accuracy de 99,66 %, ce qui est presque parfait en termes de détection efficace.

Le tableau 1 indique que les autres mesures notant la précision, le recall et le F1-score ont également été améliorées.

	RF with Based Dataset	RF With Normalized Dataset	RF with Normalized DataSet &M-best features Selection
Accuracy	85,92%	93,63%	99,66%
Precision	95%	99%	99,85%
F1-Score	85%	95%	99,84%
Recall	77%	91%	99,83%

Table IV.1 – Impact de la normalization et la sélection des attributs sur Random Forest

IV.5.2 Comparaison

Le tableau 2 révèle une comparaison entre le modèle proposé et d'autres modèles discutés dans (Laqtib et al., 2019). Il est clair que RF / M-Best Features fournit les meilleurs résultats en termes d'Accuracy, de précision, de Recall et de F1-Score.

	RF/ M-best	CNN	Inc-CNN	Bi-LSTM	GRU
Accuracy	99,66%	85,99%	89,03%	84,33%	78,98%
Precision	99,85%	90,90%	85,08%	93,98%	81,08%
F1-Score	99,84%	85,76%	85,33%	89,82%	84,20%
Recall	99,83%	81,17%	85,58%	86,01%	87,56%

Table IV.2 – Comparaison du modèle proposé.

	RF/ M-best	GA-RF	SVM/Fselect	DNN(4 LAyer)
Accuracy (%)	99,66	96.12	98.27	94
Precision (%)	99,85	90.23	97.80	91
F1-Score (%)	99,84	88.25	97.64	92
Recall (%)	99,83	86.35	97.49	77
FPR (%)	1,08	2,91	1,7	6

Table IV.3 – Comparaison du modèle proposé (La sélection des attributs)

	RF/ M-best	KNN	CNN	C4.5	IBK	RBF
Accuracy (%)	99,66	87,45	95,54	87,95	88,03	94,28
FPR (%)	1,08	3,07	4,64	2,75	3,25	4,64
Processing Time (s)	5,07	165	2,5	12	124	-

Table IV.4 – Comparaison d'Accuracy, FPR et Time processing pour la selection des attributs importants.

Les tableaux 3 et 4 présentent une comparaison des performances entre le modèle proposé et d'autres méthodes basées sur la sélection des caractéristiques ((Liu & Shi, 2019), (Mohammed & Gbashi, 2021), (Belgrana et al., 2021)). Tous les modèles sont testés sur le jeu de données NSL-KDD. RF / M-Best donne plus d'efficacité par rapport aux autres avec une précision de 99,66 %.

IV.6 Conclusion

L'utilisation de l'apprentissage automatique dans le domaine de la détection d'intrusion dans les réseaux MANET est devenue une question d'actualité. Cependant, plusieurs techniques ont été abordées dans ce chapitre.

Nous avons proposé l'utilisation du Random Forest avec une normalisation des données et une sélection automatique des meilleurs attributs. Ces derniers ont été soigneusement sélectionnées en fonction de leur impact sur l'accuracy totale. Seules les attributs ayant un fort impact seront sélectionnés. Les expériences sont effectuées sur python en utilisant le dataset NSL-KDD qui a donné respectivement 99,66 %, 99,85 %, 99,93 % et 99,84 % pour l'accuracy, la précision, le recall et le F1-score.

Dans un futur travail, plusieurs perspectives sont envisageables notant l'application de RF/M-Best sur d'autres jeux de données, l'implémentation de la solution proposée dans un environnement NS2/NS3 (Entrainer les noeuds a l'aide du modèle d'apprentissage généré).

CONCLUSION GÉNÉRALE ET PERSPECTIVES

Conclusion générale et perspectives

Les réseaux ad-hoc mobiles sont l'option du futur en matière de coûts (sans infrastructure) et en connectivité. A l'opposé de ces avantages, l'inconvénient de la vulnérabilité risque de les anéantir aux diverses formes d'attaques.

Comme nous l'avons souligné au premier chapitre, les problèmes inhérents aux réseaux mobiles ad hoc sont assez sérieux et les touchent sur plusieurs plans laissant comprendre qu'ils resteront un domaine de recherche ouvert allant de leur conception jusqu'à leur exploitation.

L'un des problèmes les plus sérieux dans ces réseaux est la sécurité, vue leurs natute dynamique. Plusieurs techniques ont été présentées et testées, mais elles présentes toujours des faiblesses.

Un système de détection d'intrusion est un processus de surveillance des activités dans le réseaux. Il analyse les informations collectées sur les activités dans les réseaux pour déterminer s'il existe des activités violant les règles de sécurité.

WATCHDOG est présenté comme étant le premier système de détection d'intrusion. Malgré ses faiblesses mais il reste le système de base. Plusieurs schémas ont vu le jour, notant *TWOACK, A3ACK, AACK* mais reste toujours insuffisantes.

Dans le présent travail, un mécanisme visant à améliorer les méthodes décrites précedament a été proposé. SP-AACK vise précisément à la détection rapide et efficace des nœuds malveillants quelques soit leurs nombres et leurs positions dans le réseau. Si l'accusé AACK n'est pas reçu, SP-AACK se declanche. Il divise le chemin en deux sous chemins à chaque fois que l'accusé de réception AACK n'est pas reçu. La division permet d'avoir plusieurs sous-chemins ce qui rend la détection du nœud malveillant facile. Un processus de confirmation des nœuds source et destination est lancé aprés chaque opération de division, cela est nécéssaire pour s'assurer que les nouveaux nœuds sources / destinations ne sont pas malveillants.

Le mécanisme SP-AACK a été testé pour la détection de l'attaque par trou noir (Black Hole attack) qui est l'une des plus severes attaques. Cette dernière a une énorme influence sur le protocole AODV vue le grand nombre de paquets qui sera supprimé ou absorbé par cette attaque. NS2 est l'outil utilisé pour simuler notre approche qui a permis de détecter les attaques

de trous noirs simples et multiples d'ou l'augmentation du PDR de +72% en moyenne. Plusieurs approches ont été proposées, chacune avec ses forces et ses faiblesses. Les résultats obtenus ont montré que SP-AACK est meilleur notamment en PDR et en Débit. En ce qui concerne le délai de bout en bout, il donne de bons résultats en équivalence avec les autres modèles proposés. L'envoi d'accusés de réception peut créer une surcharge, ce qui est une limitation. Par conséquent, des améliorations supplémentaires sont nécessaires pour le réduire.

L'utilisation des techniques de l'intélligence artificielle a aussi eu sa part pour la détection d'intrusion. Notamment, les techniques d'apprentissage automatique qui peuvent être basée sur des réseaux de neurones, la logique floue, des algorithmes génétiques, les réseaux bayésiens ou bien d'autres algorithmes de classification. Ces technologies sont devenues une alternative remarquable pour les analystes de sécurité ainsi que pour les chercheurs afin d'arriver à une solution efficace et optimisée pour l'amélioration de la sécurité dans les environnements MANET.

Dans cette thése, nous avons présenté une nouvelle approche basée sur un modèle d'apprentissage automatique utilisant le puissant classifieur Random Forest sur l'ensemble de donnée NSL-KDD. Cette approche a montré une efficacité pour la détection d'intrusion. L'utilisation aveugle d'un classifieur sur tous les attributs de l'ensemble de données, affaibli un peu le modèle de détection généré. Pour remédier à ce problème, nous avons proposé une méthode de sélection des attributs les plus importants, en calculant l'impact de chacun sur l'exactitude gobale du modèle. Seul les attributs avec un impact élevé seront sélectionnés durant la phase d'apprentissage.

Notre humble expérience, nous a permis d'entrevoir des propositions et des perspectives pour l'avenir entre autres :

- ▷ Une amélioration du SP-AACK concernant la surcharge(Overhead) est nécéssaire pour minimiser les cout d'énergie.
- ▷ Tester SP-AACK pour la détection d'autres attaques.
- ▷ Implementer le modele d'apprentissage sur un environnement NS2/NS3 .
- ▷ Tester le modèle d'apprentissage sur d'autres ensembles de données.
- ▷ Pour conclure, Collecter l'ensemble des paquets résultant du modéle SP-AACK pour créer un nouveau ensemble de donnée récent.

BIBLIOGRAPHIE

A, H. R. (2018). Protocol for multiple black hole attack avoidance in mobile ad hoc networks. *Recent advances in cryptography and network security, Chapter 3 Licensee IntechOpen*, page pp 26–39.

Ahmim A, Maglaras L, F. M. D. M. J. H. (2019). A novel hierarchical intrusion detection system based on decision tree and rules-based models. *2019 15th international conference on distributed computing in sensor systems (DCOSS). IEEE*, page pp 228–233.

Albalas, F., Y. M. . N. A. (2019). Detecting black hole attacks in manet using relieff classification algorithm. *ACM International Conference Proceeding Series*, page 0–5.

Ali, J., Khan, R., Ahmad, N., and Maqsood, I. (2012). Random forests and decision trees. *International Journal of Computer Science Issues (IJCSI)*, 9(5) :272.

Aljawarneh S, Aldwairi M, Y. M. (2018). Anomaly-based intrusion detection system through feature selection analysis and building hybrid efficient model. *J Comput Sci*, 25 :152– 160.

Amaral, J. P., Oliveira, L. M., Rodrigues, J. J., Han, G., and Shu, L. (2014). Policy and network-based intrusion detection system for ipv6-enabled wireless sensor networks. *Proceedings of the IEEE International Conference on Communications (ICC)*.

Augustine, A., . J. M. (2015). International journal of current engineering and technology black hole detection using watchdog. *2738| International Journal of Current Engineering and Technology*, Vol. 5(Issue 4) :1–4.

Bahrololum M, Salahi E, K. M. (2009). Anomaly intrusion detection design using hybrid of unsupervised and supervised neural network. *International Journal of Computer Networks Commun (IJCNC)*, 1(2) :26–33.

Bashah N, Shanmugam IB, A. A. (2005). Hybrid intelligent intrusion detection system. *World Acad Sci Eng Technol*, 11 :23–26.

Behzad, S. (2018). An artificial immune based approach for detection and isolation misbehavior attacks in wireless networks. *Journal of Computers*, 13(6) :705–720.

Belgrana, F.Z., B. N. H. M. C. A. M. . T.-a. A. (2021). Network intrusion detection system using neural network and condensed nearest neighbors with selection of nsl-kdd influencing features. *2020 IEEE International Conference on Internet of Things and Intelligence System (IoTaIS)*, page 23–29.

Bhati, B. S. and Rai, C. (2019). Analysis of support vector machine-based intrusion detection techniques. *Arabian Journal for Science and Engineering*, 45 :2371–2383.

Bhati BS, R. C. (2016). Intrusion detection systems and techniques : a review. *Int J Critical Comput Syst*, 6(3) :173–190.

Bhattacharyya, Bhattacharjee, D. (2011). Different types of attacks in mobile adhoc network : prevention and mitigation techniques. *Department of Computer Science Engineering, Institute Of Engineering Management, Saltlake, 1*, (1).

Bhattacharyya A, Saha HN, B. A. B. D. D. B. (2011). Different types of attacks in mobile adhoc network : prevention and mitigation techniques. *Dep. Comput. Sci. Eng. Inst. Eng. Manag. Saltlake*, vol 1(no 1) :pp 1–11.

Breiman, L. (2001). Random forests. *Machine learning*, 45(1) :5–32.

Butun, I., Morgera, S. D., and Sankar, R. (2014). A survey of intrusion detection systems in wireless sensor networks. *IEEE Commun. Surv. Tutor.*, 16(1) :266–282.

C. Xenakis, C. Panos, S. (2011). Acomparative evaluation of intrusion detection architectures for mobile adhoc networks. *Comput. Secur*, 30(1) :63–80.

Cepheli Ö, Büyükçorak S, K. K. G. (2016). Hybrid intrusion detection system for ddos attacks. *J Electr Comput Eng*, page 152– 160.

Chavan A, Jadhav D, M. N. D. N. (2020). Survey of different countermeasure on network layer attack in wireless network. *Inventive communication and computational technologies*, vol 89 :Springer, Singapore, pp 62–65.

Chitra Gupta, P. P. (2016). Movement based or neighbor based tehnique for preventing wormhole attack in manet. *Symposium on Colossal Data Analysis and Networking (CDAN).*

Deng, H., Xu, R., Li, J., Zhang, F., Levy, R., and Lee, W. (2006). Agent based cooperative anomaly detection for wireless ad hoc networks. *Proceeding of the 12th International Conference on Parallel and Distributed Systems (ICPADS).*

Deng, S., Zhou, A.-H., Yue, D., Hu, B., and Zhu, L.-P. (2017). Distributed intrusion detection based on hybrid gene expression programming and cloud computing in a cyber physical power system. *IET Control Theory Appl.*, 11(11) :1822–1829.

F, L. (2010). Hybrid neural network intrusion detection system using genetic algorithm. *2010 International conference on multimedia technology. IEEE*, page pp 1–4.

F. Sabahi, A. M. (2008). Intrusion detection : a survey. *Proceeding of the Third International Conference on Systems and Networks Communications.*

Fahad Taha AL-Dhief, Naseer Sabri, M. S. S. F. S. A. A. (2018). Manet routing protocols evaluation : Aodv, dsr and dsdv perspective. *MATEC Web of Conferences 150 06024 (2018)*, pages 679–684.

Garcia-Teodoro, P., Diaz-Verdejo, J., Maciá-Fernández, G., and Vázquez, E. (2009). Anomaly-based network intrusion detection : techniques, systems and challenges. *Elsevier J. Comput. Secur.*, 28(1) :18–28.

Giordano, S., . U. A. (2005). Self-organized and cooperative ad hoc networking. *Mobile Ad Hoc Networking.*

Gite, P. (2017). Link stability prediction for mobile ad-hoc network route stability. *International Conference on Inventive Systems and Control*.

Govindarajan M, C. R. (2011). Intrusion detection using neural based hybrid classification methods. *Comput Networks*, 55(8) :1662–1671.

Gupta A, Bhati BS, J. V. (2014). Artificial intrusion detection techniques : a survey. *Int J Comput Network Inform Secur*, 6(9) :51.

G.V. Nadiammai, M. H. (2013). Handling intrusion detection system using snort based statistical algorithm and semi-supervised approach. *Res. J. Appl. Sci. Eng. Technol*, 6(16) :2914–2922.

H, L. (2014). An improved intrusion detection based on neural network and fuzzy algorithm. *J Networks*, 9(5) :1274–1280.

H. Otrok, N. Mohammed, L. W. M. D. P. B. (2008). A game-theoretic intrusion detection model for mobile ad hoc networks. *Comput. Commun.*, 31(4) :708–721.

Hamamreh, R. (2018). Protocol for multiple black hole attack avoidance in mobile ad hoc networks provisional chapter protocol for multiple black hole attack avoidance in mobile ad hoc networks. *Intech*.

H.Ghayvat, S.Pandya, S. S. M. K. (2016). Advanced aodv approach for efficient detection and mitigation of wormhole attack in manet. *Tenth International Conference on Sensing Technology*.

Hoang, X. D., Hu, J., and Bertok, P. (2009). A program-based anomaly intrusion detection scheme using multiple detection engines and fuzzy inference. *J. Netw. Comput. Appl.*, 32(6) :1219–1228.

Iwendi, C., K. S. A. M. M. A. M. . A. M. (2020). The use of ensemble models for multiple class and binary class classification for improving intrusion detection systems. *Sensors*, 20(9) :2559.

Jemili F, Zaghdoud M, A. M. (2009). Intrusion detection based on "hybrid" propagation in bayesian networks. *2009 IEEE international conference on intelligence and security informatics. IEEE*, page pp 137–142.

J-S, L. (2008). A petri net design of command filters for semiautonomous mobile sensor networks. *IEEE Trans Ind Electron*, 55(4) :1835–1841.

K. Manousakis, D. Sterne, N. I. G. L. A. M. (2008). A stochastic approximation approach for improving intrusion detection data fusion structures. *Proceedings of the Military Communications Conference, IEEE, San Diego, USA*.

Kachirski, O. and Guha, R. (2003). Effective intrusion detection using multiple sensors in wireless ad hoc networks. *Proceedings of the 36th Annual Hawaii International Conference on System Sciences (HICSS'03)*.

Kamarudin MH, Maple C, W. T. (2019). Hybrid feature selection technique for intrusion detection system. *Int J High Perform Comput Network*, 13(2) :232–240.

Karthick RR, Hattiwale VP, R. B. (2012). Adaptive network intrusion detection system using a hybrid approach. *2012 fourth international conference on communication systems and networks (COMSNETS 2012). IEEE*, page pp 1–7.

Kaur, H., S. V. . B. M. (2013). A survey of reactive, proactive and hybrid routing protocols in manet : a review. *(IJCSIT) International Journal of Computer Science and Information Technologies,Vol. 4 (3) , 2013, 498-5004(3)*, pages 498–500.

Kavitha T, M. R. (August 2017). Instant route migration during link failure in manets. *International Journal of Mechanical Engineering and Technology (IJMET)*, Volume 8(Issue 8).

Khalid Khan, Amjad Mehmood, S. K. M. A. K. Z. I. W. K. M. (2020). A survey on intrusion detection and prevention in wireless ad-hoc networks. *Journal of Systems Architecture*, Volume 105,2020,101701, ISSN 1383-7621,.

Khalladi, R., Rebbah, M., and Smail, O. (2019). Security against blackhole attacks in manet networks. *8th edition Smart Communications in Network Technologies-IEEE (SACONET 2019)*.

Khalladi, R., Rebbah, M., and Smail, O. (2021). A new efficient approach for detecting single and multiple black hole attacks. *The Journal of Supercomputing*, 77(7) :7718–7736.

Khalladi, R., Rebbah, M., and Smail, O. (2022). Intrusion detection system based m-best features selection in manet. *Journée Scientifique des Mthématiques et de l'Informatique(JSMI22)*.

khamayseh, Y., B. A. M. W. . B. M. (2011). A new protocol for detecting black hole nodes in ad hoc networks. *International Journal of Communication Networks and Information Security*, 3(1) :36–47.

Khamayseh, Y., Y. M. B. . A.-J. M. (2019). Intelligent black hole detection in mobile adhoc networks. *International Journal of Electrical and Computer Engineering*, 9(3) :1968–1977.

Khraisat A, Gondal I, V. P. K. J. A. A. (2020). Hybrid intrusion detection system based on the stacking ensemble of c5 decision tree classifier and one class support vector machine. *Electronics*, 9(1) :173.

Koujalagi, A. (2018a). Considerable detection of black hole attack and analyzing its performance on aodv routing protocol in manet (mobile ad hoc network). *American Journal of Computer Science and Information Technology*, 06(02) :1–6.

Koujalagi, A. (2018b). Considerable detection of black hole attack and analyzing its performance on aodv routing protocol in manet (mobile ad hoc network). *American Journal of Computer Science and Information Technology*, 06(02) :1–6.

Kumar Kollati, V. (2017). Information security journal : A global perspective ibfwa : Integrated bloom filter in watchdog algorithm for hybrid black hole attack detection. *MANET IBFWA : Integrated Bloom Filter in Watchdog Algorithm for hybrid black hole attack detection in MANET*.

Kumar Saxena A, Shukla P, K. S. S. (2019). Enhanced and secure acknowledgement ids in mobile ad hoc network by hybrid cryptography technique. *Data, engineering and applications. Springer, Singapore*, page pp 217–222.

Kumari A, Singhal M, Y. N. (2020). Black hole attack implementation and its performance evaluation using aodv routing in manet. *Inventive communication and computational technologies*, vol 89 :Springer, Singapore, pp 431–433.

Kushwah, R., T. S. . K. A. (2022). A novel technique for gateway selection in hybrid manet using genetic algorithm. *Wireless Pers Commun*.

L. Vokorokos, A. B. (2010). Host-based intrusion detection system. *Proceedings of the IEEE 14th International Conference on Intelligent Engineering Systems, Las Palmas (Spain)*.

Laqtib, S., E. Y. K. . H. M. L. (2019). A deep learning methods for intrusion detection systems based machine learning in manet. *ACM International Conference Proceeding Series, October*.

Lauf, A. P., Peters, R. A., and Robinson, W. H. (2010). A distributed intrusion detection system for resource constrained devices in ad-hoc networks. *Ad Hoc Netw*, 8(3) :253–266.

Lawrence, E. Ramavel, L. (2016). Fundamentals of mobile ad hoc network.(book).

Lee, S., Kim, G., and Kim, S. (2011). Self-adaptive and dynamic clustering for online anomaly detection. *Expert Syst. Appl.*, 38(12) :14891–14898.

Li, T., Zhang, T., Yu, G., Song, J., and Fan, J. (2019). Minimizing temperature and energy of real–time applications with precedence constraints on heterogeneous mpsoc system. *J. Syst. Arch*, 98(1) :79–91.

Liao, H.-J., Lin, C.-H. R., Lin, Y.-C., and Tung, K.-Y. (2013). Intrusion detection system : a comprehensive review. *J. Netw. Comput. Appl.*, 36(1) :16–24.

Lima MN, Dos Santos AL, P. G. (2009 Jan 3). Guide to wireless ad hoc networks. *IEEE Communications Surveys Tutorials.*, 11(1) :66–77.

Liu, Z., . S. Y. (2019). A hybrid ids using ga-based feature selection method and the random forest. *International Journal of Machine Learning and . . .*, 12(2) :1–14.

Lundin E, J. E. (2002). Survey of intrusion detection research. *Chalmers University of Technology*.

M. Peter, B. R. (2001). Nist special publication on intrusion detection. *National Institute of Standards and Technology, USA*.

M. Tavallaee, E. Bagheri, W. L. and Ghorbani, A. (2009). A detailed analysis of the kdd cup 99 data set. *Submitted to Second IEEE Symposium on Computational Intelligence for Security and Defense Applications (CISDA)*.

M. Zeeshan, H. Javed, S. U. (2017). Discrete r-contiguous bit matching mechanism appropriateness for anomaly detection in wireless sensor networks. *Int. J. Commun. Netw. Inf. Secur. (IJCNIS)*, 9(2) :157–162.

M.A. Aydin, A.H. Zaim, K. C. (2009). A hybrid intrusion detection system design for computer network security. *Comput. Electr. Eng*, 35(3) :517–526.

Mahin, S. H., Taranum, F., Fatima, L., and Khan, K. (2019). Detection and interception of black hole attack with justification using anomaly based intrusion detection system in manets. *International Journal of Recent Technology and Engineering*, 8(2 Special Issue 11) :2392–2398.

Mahin, S. H., T. F. F. L. N. . K. K. U. R. (2019). Detection and interception of black hole attack with justification using anomaly based intrusion detection system in manets. *International Journal of Recent Technology and Engineering*, 8(2 Special Issue 11) :2392–2398.

Malik AJ, Shahzad W, K. F. (2012). Network intrusion detection using hybrid binary pso and random forests algorithm. *Security and Communication Network [online].*

Marti S, Giuli TJ, L. K. B. M. (2000). Mitigating routing misbehavior in mobile ad hoc networks. *Proceedings of 6th Annual International Conference on Mobile Computing and Networking, Boston, MA*, page pp 255–265.

Mbarushimana, C. and Shahrabi, A. (2007). Comparative study of reactive and proactive routing protocols performance in mobile ad hoc networks. *21st International Conference on Advanced Information Networking and Applications Workshops (AINAW'07)*, pages 679–684.

Mehran Abolhasan, Tadeusz Wysocki, E. D. (2004). A review of routing protocols for mobile ad hoc networks. *Ad Hoc Networks*, Volume 2(Issue 1) :Pages 1–22.

Misra S, Woungang I, M. S. e. (2009 Mar 2). Guide to wireless ad hoc networks. *London : Springer Science Business Media.*

Mitra, P. (2020). A mobile ad hoc network routing protocols : A comparative study. *Recent Trends in Communication Networks. IntechOpen.*

Mohammed, B., . G. E. K. (2021). Intrusion detection system for nsl-kdd dataset based on deep learning and recursive feature elimination. *Engineering and Technology Journal*, 39(07) :1069–1079.

Nayyar, A., . M. B. (2020). Effective classification and handling of incoming data packets in mobile ad hoc networks (manets) using random forest ensemble technique (rf/et). *(Eds) Data Management, Analytics and Innovation. Advances in Intelligent Systems and Computing*, 1016 :431–444.

O. Awodele, S. Idowu, O. A. V. J. (2009). A multilayered approach to the design of intelligent intrusion detection and prevention system (iidps). *Issues In- forming Sci. Inf. Technol*, 6 :631–647.

Omari, S.A.K.A., . S. P. (2010). An overview of mobile ad hoc networks for the existing protocols and applications. *An Overview of Mobile Ad Hoc Networks for the Existing Protocols and Applications.*, 2(1) :87–110.

Panda M, Abraham A, P. M. (2011). A hybrid intelligent approach for network intrusion detection. *International conference on communication technology and system design*, page pp 1–9.

R. Janakiraman, M. Waldvogel, Q. Z. I. (2003). a peer-to-peer approach to network intrusion detection and prevention. *Proceedings of the Twelfth IEEE In- ternational Workshops on Enabling Technologies : Infrastructure for Collaborative Enterprises, Linz (Austria).*

Ramasamy Rajeswari, A. (2020). A mobile ad hoc network routing protocols : A comparative study. *Recent Trends in Communication Networks.*, page 87–110.

S. B. Geetha, D. V. C. P. (2015). Elimination of energy and communication tradeoff to resist wormhole attack in manet. *International Conference on Emerging Research in Electronics, Computer Science and Technology.*

S. Sharma, A. K. (2018). A survey on intrusion detection systems and honeypot based proactive security mechanisms in vanets and vanet cloud. *Veh. Commun.*, 12(1) :138–164.

S.A. Onashoga, A.D. Akinde, A. S. (2009). A strategic review of existing mobile agent-based intrusion detection systems. *Issues Inf. Sci. Inf. Technol.*, 6(1) :669–682.

S.A. Razak, S.M. Furnell, N. C. P. B. (2008). Friend assisted intrusion detection and response mechanisms for mobile ad hoc networks. *Ad Hoc Netw.*, 6(7) :1151–1167.

Saarela, M., J. S. (2021). Comparaison des mesures d'importance des caractéristiques comme explications des modèles de classification. *SN Appl. Sci.*, 3(272).

Saika, A., E. K. R. N. A. . H. M. M. (2010, September). Implementation and performances of the protocols of routing aodv and olsr in the ad hoc networks. *2010 5th International Symposium On I/V Communications and Mobile Network*, pages (pp. 1–4). IEEE.

Sarika, S., P. A. V. A. . S. K. (2016). Security issues in mobile ad hoc networks. *Procedia Computer Science*, (92) :329–335.

Saurabh, V. K., S. R. I. R. . S. U. (2017). Cluster-based technique for detection and prevention of black-hole attack in manets. *Proceedings of the International Conference on Electronics, Communication and Aerospace Technology, ICECA 2017, 2017-Janua*, page 489–494.

Saurabh, V. K., Sharma, R., Itare, R., and Singh, U. (2017). Cluster-based technique for detection and prevention of black-hole attack in manets. *Proceedings of the International Conference on Electronics, Communication and Aerospace Technology, ICECA 2017, 2017-January,*, page 489–494.

Saxena, A. K., Shukla, P., and Sinha, S. K. (2019). Enhanced and secure acknowledgement ids in mobile ad hoc network by hybrid cryptography technique. *Data, Engineering and Applications*, page (pp. 217–227). Springer Singapore.

Sbai, O., . E. M. (2018). Classification of mobile ad hoc networks attacks. *Colloquium in Information Science and Technology, CIST, 2018-October*, page 618–624.

Scarfone, K. (2007). Logging and monitoring to detect network. *National Institute of Standards and Technology, USA.*

Shakshuki E, Kang N, S. T. (2013). T eaack–a secure intrusion detection system for manets. *IEEE Trans Ind Electron*, 60(3) :1089–1098.

Sheltami T, Basabaa A, S. E. (2014). A3acks : adaptive three acknowledgments intrusion detection system for manet's. *J Ambient Intell Hum Comput*, 5 :611–620.

Sheltami T, Al-Roubaiey A, S. E. M. A. (2009). Video transmission enhancement inpresence of misbehaving nodes in manets. *Int J Multimed Syst*, 15(5) :273–282.

Shewaye Sirika, S. M. (2016). Survey on dynamic routing protocols. *INTERNATIONAL JOURNAL OF ENGINEERING RESEARCH TECHNOLOGY (IJERT)*, Volume 05(Issue 01).

Singh V, Singh D. A, H. M. M. (2019). Survey : black hole attack detection in manet. ssrn electron. *Proceedings of 2nd International Conference on Advanced Computing and Software Engineering (ICACSE2019)*, page pp 522–525.

Snapp, S. R., Brentano, J., Dias, G. V., Goan, T. L., Heberlein, T., Ho, C., Levitt, K., Mukherjee, B., Smaha, S., Grance, T., et al. (2017). Dids (distributed intrusion detection system) - motivation, architecture, and an early prototype. *Proceedings of the 14th national computer security conference, Sri Lanka*.

Sobh, T. S. (2006). Wired and wireless intrusion detection system : classifications, good characteristics and state-of-the-art. *Elsevier J. Comput. Stand. Interfaces*, 28(6) :670–694.

Thomas Clausen, Philippe Jacquet, C. A. A. L. P. M. e. a. (2003). Optimized link state routing protocol (olsr). *⟨inria-00471712⟩*.

Tong X, Wang Z, Y. H. (2009). A research using hybrid rbf/elman neural networks for intrusion detection system secure model. *Comput Phys Commun*, 180(10) :1795–1801.

V, K. K. (2017). Ibfwa : integrated bloom filter in watchdog algorithm for hybrid black hole attack detection in manet ibfwa. *Inf Secur J Glob Perspect*, 26(1) :49–60.

V. Chandola, A. Banerjee, V. K. (2009). Anomaly detection : a survey. *ACM Comput.Surv. (CSUR)*, 41(3) :1–15.

Vigna, G. and Kemmerer, R. A. (1999). Netstat : a network-based intrusion detection system. *J. Comput. Secur*, 7(1) :37–71.

Wang, W., Man, H., and Liu, Y. (2009). A framework for intrusion detection systems by social network analysis methods in ad hoc networks. *Secur. Commun. Netw.*, 2(6) :669–685.

Xu, Y. (2021). Research on intrusion detection method of industrial internet based on machine learning. *Journal of Physics : Conference Series*, 1802(4) :042029.

Yadav, A. K. (2017). Comparative study of routing protocols in manet. *Oriental journal of computer science and technology*, 10(1) :174–179.

Yasin, A., . A. Z. M. (2018a). Detecting and isolating black-hole attacks in manet using timer based baited technique. *Wireless Communications and Mobile Computing, 2018*, page 1–10.

Yasin, A., . A. Z. M. (2018b). Detecting and isolating black-hole attacks in manet using timer based baited technique. *Wireless Communications and Mobile Computing,2018*, page 1–10.

Yassein, M., K. Y. . A. M. (2016). Feature selection for black hole attacks. *Journal of Universal Computer Science*, 22(4) :521–536.

Yi Lu, Weichao Wang, Y. Z. and Bhargava, B. (2003). Study of distance vector routing protocols for mobile ad hoc networks. *Proceedings of the First IEEE International Conference on Pervasive Computing and Communications. (PerCom 2003)*, pages 187–194.

Zhou, C. V., Leckie, C., and Karunasekera, S. (2010). A survey of coordinated attacks and collaborative intrusion detection. *Comput. Secur.*, 29(1) :124–140.

ANNEXE

N°	Nom de l'attribut	Type	Description
01	duration	Numérique	La durée de connexion
02	protocol_type	Nominal	Protocole utilisé dans la connexion (tcp, udp,icmp)
03	service	Nominal	Service réseau de destination,(http,telnet,ftp_data,etc.)
04	Flag	Nominal	Statut de la connexion :Normal ou Erreur (SF,REJ,S0, S1, etc.)
05	src_bytes	Numérique	Nombre d'octets de donnée transférés de la source à la destination (491, etc.)
06	dst_bytes	Numérique	Nombre d'octets de données transférés de la destination à la source(0, etc.)
07	Land	Binaire	**Si** l'adresse IP de source et destination et le nombre de port sont les mêmes **alors**, *land*=1**sinon***land*=0
08	wrong_fragment	Numérique	Nombre total de fragments erroné dans cette connexion
09	urgent	Numérique	Nombre de parquets urgent
10	Hot	Numérique	Nombre d'indicateurs«Hot»
11	num_failed_logins	Numérique	Nombre de tentative de connexions échouées
12	logged_in	Binaire	**Si** connecté avec success **alors** *logged_in*=1**sinon***logged_in*=0
13	num_compromised	Numérique	Nombre de conditions compromises
14	root_shell	Binaire	1 si le root shell est obtenu,0autrement
15	su_attempted	Binaire	1 **si** la commande "su root" a été tentée ou utilisée,**sinon**0
16	num_root	Numérique	Nombre d'accès "root" ou nombre d'opérations effectuées comme racine dans la connexion
17	num_file_creations	Numérique	Nombre d'opérations de création de fichiers
18	num_shells	Numérique	Nombre d'invites du shell
19	num_access_files	Numérique	Nombre d'opérations sur les fichiers de contrôle d'accès
20	num_outbound_cmds	Numérique	Nombre de commandes sortantes dans une session FTP
21	is_host_login	Binaire	1 **si** la connexion appartient à la liste du «hot»(root ou admin);**sinon**0

22	is_guest_login	Binaire	1 **si** le login est un login«guest»;**sinon**0
23	count	Numérique	Nombre de connexions vers le même hôte de destination que la connexion encours dans les deux dernières secondes
24	srv_count	Numérique	Nombre de connexions vers le même service (N°Port) que la connexion encours dans les deux dernières secondes
25	serror_rate	Numérique	Le pourcentage de connexions qui ont activé le *flag* s0, s1, s2 ous3, parmi les connexions agrégées dans *count*
26	srv_serror_rate	Numérique	Le pourcentage de connexions qui ont active le *flag* s0 , s1 , s2 ou s3, parmi les connexions agrégées dans *srv_count*
27	rerror_rate	Numérique	Le pourcentage de connexions qui ont active le *flag* REJ, parmi les connexions agrégées dans *count*
28	srv_rerror_rate	Numérique	Le pourcentage de connexions qui ont active le *flag* REJ, les parmi les connexions agrégées dans srv_*count*
29	same_srv_rate	Numérique	Le pourcentage de connexions qui sont au même service, parmi les connexions agrégées dans *count*
30	diff_srv_rate	Numérique	Le pourcentage de connexions qui sont aux différents services, parmi les connexions agrégées dans *count*
31	srv_diff_host_rate	Numérique	Le pourcentage de connexions qui sont à différentes machines de destination, parmi les connexions agrégées dans srv_*count*
32	dst_host_count	Numérique	Nombre de connexions ayant la même adresse IP De l'hôte de destination
33	dst_host_srv_count	Numérique	Nombre de connexions ayant le même numéro de port
34	dst_host_same_srv_rate	Numérique	Le pourcentage de connexions qui sont au même service, parmi les connexions agrégées dans *dst_host_count*
35	dst_host_diff_srv_rate	Numérique	Le pourcentage de connexions qui sont aux différents services, parmi les connexions agrégées dans *dst_host_count*
36	dst_host_same_src_port _rate	Numérique	Le pourcentage de connexions qui sont au même port de source, parmi les connexions agrégées dans *dst_host_srv_count*
37	dst_host_srv_diff_host_ rate	Numérique	Le pourcentage de connexions qui sont à différentes machines de destination, parmi les connexions agrégées dans *dst_host_srv_count*
38	dst_host_serror_rate	Numérique	Le pourcentage de connexions qui ont active le *flag* s0, s1, s2 ous3,parmi les connexions agrégées dans *dst_host_count*

39	dst_host_srv_serror_rate	Numérique	Le pourcentage de connexions qui ont active le *flag* s0, s1, s2 ou s3, parmi les connexions agrégées dans *dst_host_srv_count*
40	dst_host_rerror_rate	Numérique	Le pourcentage de connexions qui ont active le *flag* REJ,parmi les connexions agrégées dans *dst_host_count*
41	dst_host_srv_rerror_rate	Numérique	Le pourcentage de connexions qui ont active le *flag* REJ,parmi les connexions agrégées dans *dst_host_srv_count*