Analyse des attaques et des mécanismes de sécurité dans les protocoles de routage des réseaux mobiles Ad Hoc

Dr Karim KONATE et Abdourahime GAYE

Département de Mathématiques et Informatique
Université Cheikh Anta DIOP Dakar
{kkonate911, agaaye}@yahoo.fr

RÉSUMÉ. Ce présent travail a pour vocation d'étudier les attaques et les mécanismes de sécurité proposés dans les protocoles de routage des réseaux mobiles ad hoc. La première partie constituée par l'introduction de cet article résume l'état de l'art sur les réseaux mobiles ad hoc. La deuxième partie fait une analyse de quelques attaques et les mécanismes utilisés pour les contrer dans les MANETs. En fin un tableau qui résume les failles relatives aux mécanismes proposés a été présenté et une simulation de certaines attaques en utilisant le logiciel de NS2.

MOTS-CLÉS : réseaux mobile ad hoc, routage, sécurité, attaques, simulation.

.

1. Introduction.

Un réseau **Ad Hoc** constitue un regroupement d'une grande population d'unités de calculs portables (laptops, PDA…) interconnectés par une technologie sans fil se déplaçant dans un territoire quelconque, formant un réseau décentralisé, sans infrastructure fixe [01].

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

Le problème de ce type réseau consiste à trouver l'investissement de moindre coût en capacités nominales et de réserves qui assure le routage du trafic nominal et garantit sa fiabilité en cas de n'importe quelle panne d'arc ou de nœud. C'est pourquoi plusieurs familles de protocoles de routage se sont rapidement dégagées. Chaque protocole peut ainsi être classifié en tant que réactif comme AODV (Ad hoc On Demand Distance Vector) et DSR (Dynamic Source Routing), proactif comme OLSR (Optimized Link State Protocol), ou hybride comme ZRP (ou Zone Routing Protocol) [01].

2. Analyse des attaques et des mécanismes dans les MANETs

Les attaques de sécurité peuvent être classées en deux catégories selon la nature de l'attaquant : les Attaques passives ou actives. Elles sont nombreuses et variées dans ces MANET.

Blackhole attack qui consiste à laisser tomber certains messages de routage que le nœud reçoit [01, 02, 03, 04, 05]. Elle s'est déclinée en plusieurs variantes plus ou moins proches, ayant des objectifs différents, parmi lesquelles nous pouvons citer : routing loup (boucle de routage), qui permet à un nœud de créer des boucles dans le réseau, gray hole (trou gris), qui ne laisse passer que les paquets de routage et détourne les données, Black mail (courrier noir), qui permet à un nœud attaquant d'isoler un autre nœud. Plusieurs solutions existent pour contrer ces types d'attaques, parmi lesquelles nous pouvons citer la Technique d'estimateur de relation. Dans ce mécanisme les auteurs ont classifié la relation parmi les nœuds et leurs voisins sur trois cas : **Inconnu** (le nœud x n'a jamais envoyé (reçu) de messages au (du) nœud y et la probabilité du comportement malveillant est très haute), **Connu** (le nœud x a envoyé (reçu) quelques messages au (du) nœud y et la probabilité du comportement malveillant doit être observée) et **Ami** (le nœud x a envoyé (reçu) en abondance des messages au (du) nœud y et la probabilité du comportement malveillant est très moindre. Ce mécanisme est implémenté dans le protocole de routage **RDSR (Relationship enhanced DSR protocol)** [06]. Le Seuil du numéro de séquence consiste à faire une vérification pour

trouver si le RREP_seq_no est plus élevé que la valeur seuil. La valeur seuil est dynamiquement mise à jour dans chaque intervalle de temps. Comme la valeur de RREP_seq_no s'avère plus élevée que la valeur seuil, on suspecte le nœud pour être malveillant et on l'ajoute à la liste noire. Ce mécanisme est implémenté dans le protocole de routage DPRAODV (Detection, Prevention and Reactive AODV) [07]. Le Watchdog ou surveillance qui permet d'identifier les nœuds malicieux. Le Watchdog assigne des valeurs positives à un nœud qui expédie des paquets avec succès et une valeur négative après qu'un niveau seuil de mauvais comportement ait été observé. Il est implémenté dans SWAN (Secure Watchdog for mobile Ad hoc Network) [08]. Le Pathrater ou évaluateur de parcours qui permet au protocole d'éviter les nœuds corrompus inscris dans une liste noire [[08]. La solution Cross checking qui consiste à compter sur les nœuds fiables (les nœuds par lesquels le nœud source a routé des données) pour transférer des paquets de données [09,10].

Wormhole attack qui consiste à mettre un tunnel entre deux nœuds, souvent deux attaquants [01,03]. Pour contrer les attaques Wormhole certains auteurs ont proposé d'utiliser la notion d'analyse du saut compté. Dans ce mécanisme, une route qui a un saut le plus bas ou le plus haut compté est considérée comme non utilisable. Un si bas saut compté peut impliquer une attaque de trou de ver; tandis qu'un saut si aussi haut peut ralentir la transmission. Le protocole Multipath Hop-count Analysis (MHA) implémente ce mécanisme et aussi le protocole AODV-WADR (AODV-Wormhole Attack Detection Reaction) [12,13]. Le paquet de trace ou variante (leash) qui peut être géographique qui assure que le destinataire du paquet est dans à certaine distance de l'expéditeur ou temporelle qui assure que le paquet a un supérieur c'est-à-dire un nœud expéditeur qui s'occupe de sa durée de vie. Les protocoles LAR (Location-Aided Routing) et AODV-WADR (AODV-Wormhole Attack Detection Reaction) [01,11] et aussi les antennes directionnelles (Directional antenna) qui consiste à utiliser la direction des paquets d'arrivée pour détecter si les paquets proviennent de leurs propres voisins. Cette solution est implémentée dans DREAM (Distance Routing Effect Algorithm for Mobility [15].

Rushing attack qui consiste à envoyer des demandes d'itinéraires (RREQs) au destinataire beaucoup plutôt que (plus rapide que) d'autres demandes itinéraires provenant des autres nœuds intermédiaires. Il y a une probabilité de forcer les itinéraires à passer par lui [01,03]. Certaines solutions ont été proposées parmi lesquelles nous pouvons citer la notion de sélection au hasard (**randomized selection**) qui consiste à admettre une sélection aléatoire des messages de demande de route. Ainsi un nœud attend jusqu'à collecter un nombre **seuil** de demandes de route. Suivant ce nombre de demandes collectées, le nœud peut choisir aléatoirement une demande à transférer parmi les demandes reçues. Les auteurs ont proposé de l'implémenter sous **DSR** [11]. Il y a aussi la Détection de voisin sûr (**Secure Neighbor Detection**) qui permet à chaque nœud de vérifier que l'autre voisin se trouve à la portée maximale de transmission. Elle

est réalisée par l'observation du délai de réponse défi (challenge response delay) pour évaluer la distance à un nœud et de vérifier si le nœud peut être un voisin. . En autre il existe une solution appelée délégation de route sure (**Secure route Delegation**) qui permet à chaque nœud de vérifier que toutes les étapes de détection de voisinage ont été exécutées entre toute paire de nœuds adjacents, c'est-à-dire vérifier que les nœuds soient en effet des voisins. Un message de délégation de route est échangé (**Route Delegation / Accept**). Ce mécanisme est implémenté dans **RAP** (Rushing Attack Prevention) [11].

The selfish attack qui consiste à ne pas collaborer pour le bon fonctionnement du réseau. Les nœuds **égoïstes** sont des entités économiquement rationnelles dont l'objectif est de maximiser leurs bénéfices**.** Pour prévenir la non coopération des nœuds plusieurs solutions ont été proposées. Une solution basée sur l'**Algorithme de choix négatif: Negative Selection Algorithm (NSA).** Il est basé sur les principes de la discrimination de soi/non-soi dans le système immunitaire (définir le soi comme une collection S d'éléments dans un espace caractéristique X, une collection qui a besoin d'être surveillée) [16]. La **détection d'anomalie** vise à distinguer un nouveau modèle comme une partie de soi ou non-soi, donné un modèle de système de soi (données normales) [16]. **Le GA structuré** (SGA) est un type d'algorithme évolutif qui incorpore le matériel génétique redondant, qui est contrôlé par un mécanisme d'activation de gène. Il utilise les structures génomiques multicouches pour son chromosome c'est-à-dire que tout le matériel génétique (exprimé ou pas) « est structuré » dans un chromosome hiérarchique. Le mécanisme d'activation active et désactive ces gènes codés. Le problème d'espace, dénoté par X dans un espace dimensionnel n; l'ensemble de soi est dénoté S et N soit l'espace complémentaire de S. Cette solution est implémentée dans **AODV** [16]. Une solution basée sur la **réputation** (CORE et CONFIDANT) qui consiste à collecter des informations sur un ancien comportement de l'entité éprouvé par d'autres [17, 18,19]. Une solution basée sur le **payement** (Nuglet) qui exige aux nœuds qui profitent des ressources du réseau (émetteurs et / ou récepteurs) de payer aux nœuds « fournisseurs de services » (nœuds intermédiaires) [20,21] et une solution basée sur la **localisation** (antennes directionnelles).

Sleep deprivation qui consiste à faire en sorte que le nœud soit obligé de rester en état d'activité et de lui faire consommer toute son énergie [04]. Pour lutter contre la privation de sommeil nous avons recours à certaines solutions. Une qui est basée sur la **sélection d'énergie avisée** et qui prend en compte les considérations énergiques dans le choix du meilleur chemin. Chaque nœud calcule son propre statut énergique et déclare une prévision appropriée. Le choix de la prévision est basé sur la capacité de la batterie et la durée de vie prévue d'un nœud. Le rapport entre énergie réelle et initiale d'un nœud est utilisé pour mesurer la capacité de batterie. Ce mécanisme est implémenté dans le protocole **EEAOMDV**: **E**nergy **E**fficient **A**d Hoc **O**n Demand **M**ultipath **D**istance **V**ector Routing Protocol [22]. Une qui est basée sur l'**Énergie efficace pour le routage**; elle nécessite une commutation dynamique sur les états des nœuds entre le

mode veille et le mode actif. Les nœuds entrent dans ces états à des intervalles fixes afin d'assurer l'expédition des messages avec succès, les nœuds actifs peuvent devoir retransmettre des messages un certain nombre de fois avant que le nœud de destination soit en écoute ou en activité. Ce mécanisme est implémenté dans **BECA** : **B**asic **E**nergy-**C**onserving **A**lgorithm [23]. Une qui est basée sur **PARO** (contrôle de puissance du routage) qui est une technique de contrôle de puissance du routage pour les MANETs où tous les nœuds sont situés dans la portée maximale de transmission de l'un de l'autre c'est-à-dire l'énergie dépend de la distance qui sépare la source et la destination [24]. Celle qui se base sur **PAA** (Alternation du contrôle de puissance) qui consiste à éliminer l'activité réseau d'un ensemble de nœuds durant une certaine période afin de conserver leur énergie tout en gardant leur présence dans le réseau par une délégation [25].

Location disclosure qui consiste à révéler des informations sur l'emplacement des nœuds intermédiaires ou la structure du réseau [26]. Pour prévenir les attaques de divulgation d'emplacement l'algorithme RNI **: Random Node Identification** (Identification aléatoire de nœud) a été proposé. Il est basé sur l'utilisation d'identifiant aléatoire du nœud pour dissocier un vrai identifiant du nœud de l'information d'emplacement, les auteurs ont proposé d'implémenter la solution du RNI dans le protocole AODV (Ad hoc On-demand Distance Vector) [04].

Overflow qui consiste pour un nœud malicieux de provoquer le débordement des tables de routage des nœuds servant de relais [04]. Pour parer à cette attaque la solution nommée **Trust evaluation (évaluation de confiance)** a été proposée. Elle se base sur l'évaluation de confiance pour assurer un routage sûr dans les MANETs. Le succès d'une communication à travers un nœud augmentera l'indice de confiance de ce nœud et l'échec par ce nœud diminuera l'indice de confiance. Si cette valeur atteint zéro ce nœud est inscrit dans une liste noire et nous avertissons les autres voisins de ce nœud. TRP (Trust-based Routing Protocol) implémente cette solution [27].

Ad hoc flooding attack qui permet pour un adversaire d'effectuer un DoS en saturant le support avec une grosse quantité de messages en broadcast, en réduisant le débit des nœuds, et au pire, les empêchant de communiquer [28]. Pour prévenir cette attaque deux principales approches ont été proposées. Une approche basée sur les **relations** (**Relationship)**, dans ce mécanisme, tous les nœuds dans un réseau ad hoc sont classés par catégories, soit comme *amis*, *connaissances* ou *étrangers*, basées sur leurs rapports avec leurs nœuds voisins. Cette solution est implémentée dans le protocole AODV) [29]. Une approche basée sur la monnaie virtuelle (Virtual currency) qui utilise la notion de crédit ou de micro paiement pour compenser le service d'un nœud [20]. Une approche basée sur la méthode de suppression voisine (FAP) [20]. Quand l'attaquant diffuse un grand nombre de paquets de RREQs, les nœuds voisins de l'attaquant enregistrent la cadence de demandes d'itinéraires. Une fois que le seuil est dépassé, les nœuds voisins nient tous les futurs paquets de demande de l'attaquant.

Replay attack qui consiste à propager les vieux messages de routage, qui ne reflètent pas la topologie courante, dans le réseau pour affecter des itinéraires. Pour prévenir ce type d'attaque le mécanisme de Sequence Number (numéro de séquence) a été proposé et ils permettent de faire la distinction entre les anciens et les nouveaux paquets transmis, DSDV (Dynamic Destination-Sequence Distance-Vectore) et AODV (Ad hoc On-demand Distance Vector) implémentent ce mécanisme [01].

Tableau 2 : tableau récapitulatif des attaques et les protocoles

Protocoles de routage / Attaques	SWAN	LAR	RAP	CORE	CONFIDANT	Nuglet	PARO	PAA	TRP	FAP	DSDV	AODV	WRP	DREAM	RDSR	DPRAODV	MHA
boucle de routage	oui	non	oui	oui	oui	non	non	non	Oui	non	oui	oui	oui	oui	oui	oui	non
trou Gris	oui	non	non	oui	oui	non	non	non	Oui	non	non	non	oui	oui	oui	oui	non
Courrier Noir	oui	non	oui	**non**	non	non	non	non	non	non	non	non	non	non	oui	non	non
Trou Ver	non	oui	oui	non	non	non	oui	non	non	non	non	oui	oui	oui	non	non	oui
Précipitation	non	non	oui	non	non	oui	non	non	non	non	non	non	non	non	non	non	oui
Non Coopération	non	oui	oui	oui	oui	oui	oui	oui	oui	oui	non	non	non	oui	oui	non	non
Privation de sommeil	non	non	non	non	non	oui	oui	oui	non	oui	non	non	non	non	non	non	non
divulgation d'emplacement	oui	non	non	non	non	non	non	oui	non	non	non	non	non	non	non	non	non
débordement des tables de routage dû aux nœuds fictifs	non	non	oui	**non**	non	oui	oui	non	oui	non	non	non	non	non	non	non	non
Blackhole coopérative	non	non	non	**non**	non	non	non	non	non	non	non	non	oui	oui	non	non	non
Saturation de la bande passante	non	oui	non	non	non	oui	non	oui	non	oui	non	non	non	non	non	oui	non

3. Simulation des attaques dans les MANETs

Pour évaluer le comportement malheureux des attaques dans ce type de réseau nous avons utilisé le logiciel de ns2. Les paramètres de notre simulation sont donnés dans le tableau suivant.

Tableau 8 : paramètres de simulation

Temps de simulation en S	10, 20, 30, 40, 50, 60, 70, 90, 100
Nombre de nœuds	10
Surface	670*670
Vitesse d'exécution	20 mètre/sec
Taille paquet	1000 bytes
Modèle trafic	CBR/UDP
Routage	DSDV
Modèle d'antenne	Omnidirectionnelle
Energie de transmission en J	0,4
Energie de réception en J	0 ,3

Pour étudier les attaques nous nous focalisons sur un certain nombre de paramètres cités ci-dessous pour pouvoir faire notre simulation des attaques car dans le Selfish aussi bien que dans le Blackhole le nombre de paquets envoyés sera inférieur au nombre de paquets à l'arrivée et aussi pour l'attaque Overflow la consommation d'énergie diffère car chaque paquet reçu correspond à une perte d'énergie. Les paramètres sont :

- le nombre de paquets envoyés ;
- le nombre de paquets reçus ;
- le nombre de paquets perdus ;
- la consommation d'énergie.

La figure 1 illustre le changement du débit en fonction du nombre de paquets envoyés dans le temps. Nous avons constaté que le débit est égal à 100 bit/sec lorsque le nombre de paquets reçu est égal à 865 et brusquement le débit chute et atteint les 50 bit/sec, cela trouve son explication dans le fait que le but de l'attaquant est de saturer le réseau rendant ainsi la bande passante non disponible d'où la diminution du débit:

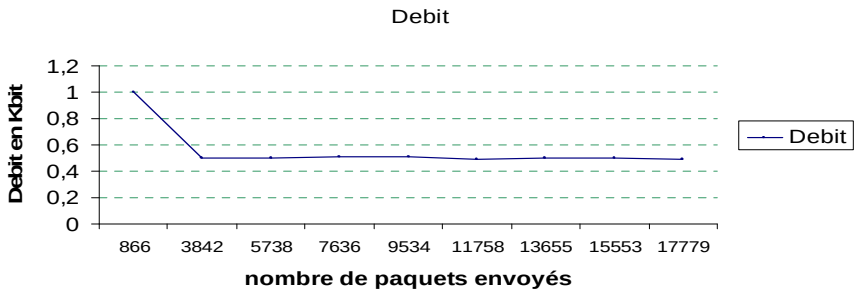

Figure 1 : Changement du débit

La figure 2 calcule le taux de perte des paquets en fonction du nombre de paquets envoyés dans le temps. Nous avons constaté que le taux augmente considérablement et atteint presque les 75% lorsque le nombre de paquets atteint les 800 et ensuite le taux commence à diminuer et atteint les 35%, cela peut s'expliquer du fait que le but de l'attaque Blackhole est de détourner les paquets de données et non pas les paquets de routage et en plus l'attaquant peut décider d'acheminer les paquets ou les mettre dans un trou noir.

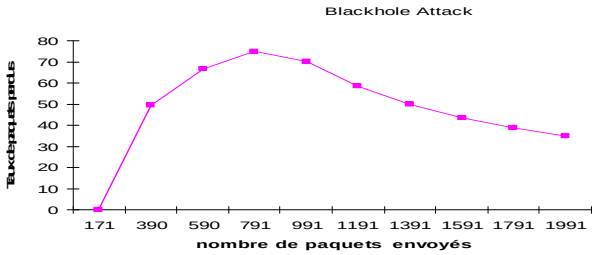

Figure 2 : Effet de l'attaque Blackhole

Les résultats visualisés ci-dessous nous permettent de faire une étude comparative sur le taux de perte de paquets en fonction du temps dans le cas où les nœuds du réseau fonctionnent correctement et dans le cas où le réseau est saturé par l'envoi d'une grande quantité de paquets. Nous avons constaté que si les nœuds sont légitimes, le taux de perte de paquets ne dépasse pas les 5% et reste constant même si le temps augmente, cela peut s'expliquer du fait que la bande passante est partagée et que les nœuds envoient leurs paquets par intervalle de temps régulier car les nœuds écoutent le canal

avant leur transmission et dans cet environnement sans fil les risques de collision sont assez fréquents. Dans le cas où il existe un nœud qui émet volontairement des paquets afin de saturer le réseau le taux de perte de paquets atteint presque les 30%, cela peut s'expliquer du fait que la bande passante est limitée et partagée par l'ensemble des nœuds du réseau. Si le nœud malicieux ne respecte pas les intervalles d'émission, l'envoi des paquets par les nœuds légitimes entraîne une perte.

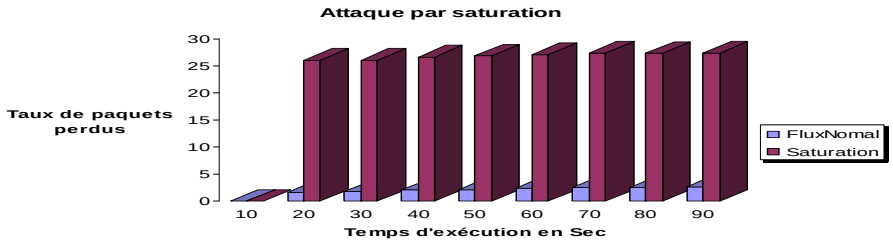

Figure 3 : Effet de l'attaque par saturation

La figure 4 nous permet de faire une comparaison sur la consommation d'énergie en fonction du temps dans le cas où les nœuds coopèrent au bon fonctionnement du réseau et aussi dans le cas il existe des nœuds égoïstes. Dans le fonctionnent normal, la consommation d'énergie augmente avec le temps et atteint presque les 750 J au temps égal à 90 sec tandis que si le nœud est égoïste la consommation d'énergie est de 400 J, ce qui entraîne une réservation de presque de 375 J d'où les nœuds ont tendance à être égoïstes pour rester dans le réseau ou bien d'expédier leur propre paquet car ils ont une autonomie limitée.

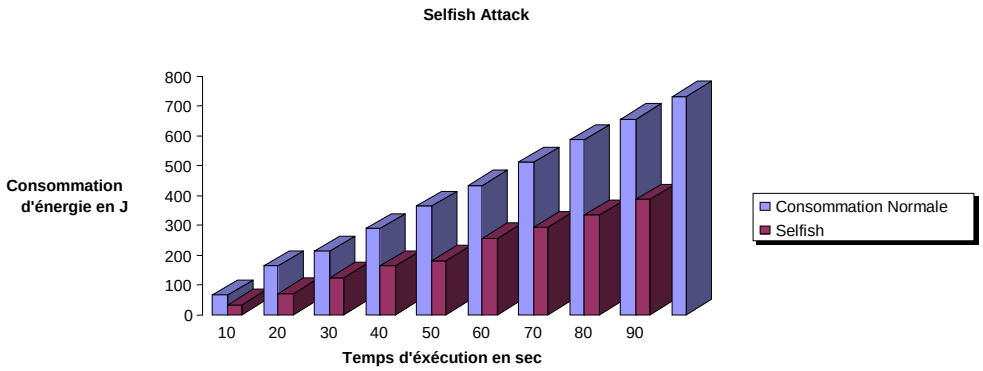

Figure 4 : Consommation d'énergie

4. Conclusion

A l'issu de notre travail nous avons présenté les spécificités des réseaux mobiles ad hoc ainsi que les problèmes de sécurisation des protocoles de routage dans ces types de réseau. Nous avons présenté plusieurs variantes d'attaques rencontrées dans les MANETs, leur mode de fonctionnement ainsi les mécanismes utilisés et les protocoles qui les implémentent pour contrer ces attaques. Nous avons présenté les avantages et les inconvénients pour chaque mécanisme proposé. Ce qui nous permis d'ouvrir des champs de recherche. Nous avons enfin procédé à une simulation de certaines attaques comme la non coopération, sleep deprivation, Blackhole, saturation de la bande passante en utilisant le logiciel de NS2.

5. Références

[01]: Wiley John: Security for wireless ad hoc networks. Eyrolles, livre 2007, pages 247.

[02]: ADJIDO Idjiwa, BENAMARA Radhouane, BENZIMRA Rebecca, GIRAUD Laurent: Protocole de routage ad hoc sécurisé dans une architecture clusterisée. Université Pierre et Marie Curie (Paris VI) Paris, FRANCE, Novembre 2005, pages 4.

[03]: Curtmola Reza. Security of Routing Protocols in Ad Hoc Wireless Networks. 600.647 – Advanced Topics in Wireless Networks, Février 2007, pages 26.

[04]: Bing Wu, Jianmin Chen, Jie Wu, Mihaela Cardei. A Survey of Attacks and Countermeasures in Mobile Ad Hoc Networks. Department of Computer Science and Engineering Florida Atlantic University, Decembre 2005

[05]: Chen Ruiliang, Snow Michael, Park Jung-Min, M. Refaei Tamer, Eltoweissy Mohamed. Defense against Routing Disruption Denial-of-Service Attacks in Mobile Ad Hoc Networks. Department of Electrical and Computer Engineering Virginia Polytechnic Institute and State University Blacksburg, VA, USA, Novembre 2005, pages 15.

[06]: A.Rajaram, Dr. S. Palaniswami. The Trust-Based MAC-Layer Security Protocol for

Mobile Ad hoc Networks.. (IJCSE) International Journal on Computer Science and Engineering Vol. 02, No. 02, 2010, 400-408. Anna University Coimbatore, India, Mars 2010, pages 9.

[07]: Payal N. Raj, Prashant B. Swadas. DPRAODV: a dyanamic learning system against blackhole attack in aodv based manet, ijcsi International Journal of Computer Science Issues, Vol. 2, Computer Engineering Department, SVMIT Bharuch, Gujarat, India, Septembre 2009, pages 6.

[08]: Xue Xiaoyun. Security mechanisms for ad hoc routing protocols. Computer Science and Network Department, ENST, thesis September 2006, pages 234.

[09]: Ramaswamy Sanjay, Fu Huirong, Sreekantaradhya Manohar, Dixon John and Nygard Kendall: Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks. Department of Computer Science, IACC 258 North Dakota State University, Fargo, ND 58105, Mars 2003, pages 7.

[10]: Hesiri Weerasinghe and Huirong Fu. Preventing Cooperative Black Hole Attacks in Mobile Ad Hoc Networks: Simulation Implementation and Evaluation ; International Journal of Software Engineering and Its Application Vol. 2, No. 3. *Oakland University Rochester MI 48309 USA*, Juin 2008;, *page 16.*

[11]: Hu Yih-Chun, Perrig Adrian, Johnson David B.: Packet Leashes: A Defense against Wormhole Attacks in Wireless Networks, INFOCOM 2003, pages 11

[12]: Emmanouil A. Panaousis, Levon Nazaryan, Christos Politis. Securing AODV Against Wormhole Attacks in Emergency MANET Multimedia Communications, Wireless Multimedia & Networking (WMN) Research Group Kingston University London. Juillet 2009, pages 7.

[13] : Shang-Ming Jen 1, Chi-Sung Laih 1 and Wen-Chung Kuo. A Hop-Count Analysis Scheme for Avoiding Wormhole Attacks in MANET.

[14]: Debdutta Barman Roy, Rituparna Chaki, Nabendu Chaki. a new cluster-based wormhole intrusion detection algorithm for mobile ad-hoc networks. International Journal of Network Security & Its Applications (IJNSA), Vol 1, No 1, West Bengal University of Technology, Kolkata 700064, India. Avril 2009, pages 9.

[15]: Hu Lingxuan et Evans David: Using Directional Antennas to Prevent Wormhole Attacks. University of Virginia, California, USA. February 2004, pages 11.

[16]: T.V.P.Sundararajan et Dr.A.Shanmugam. Behavior Based Anomaly Detection Technique to Mitigate the Routing Misbehavior in MANET. Sathyamangalm-638401, Tamilnadu,, India, Mai 2009, pages 14

[17]: Kevin Hoffman, David Zage, and Cristina Nita-Rotaru. A Survey of Attack and Defense Techniques for Reputation Systems. Department of Computer Science and CERIAS, Purdue University. Avril 2008, pages 19

[18]: Pietro Michiardi : Coopération dans les réseaux ad hoc : Application de la théorie des jeux et de l'évolution dans le cadre d'observabilité imparfaite. Institut Eurecom 2229, route des Cretes BP 19306904 Sophia-Antipolis, France, Juillet 2006, pages 17

[19] :Michiardi Pietro and Molva Refik: CORE: A Collaborative Reputation Mechanism to enforce node cooperation in Mobile Ad hoc Networks. European Wireless Conference, Nonvembre 2003, pages 15.

[20]: Hu Jiangyi: Cooperation in Mobile Ad Hoc Networks. Computer Science Department Florida State University, January 11, 2005, pages 23.

[21]: Buttyan Levente and Hubaux Jean-Pierre: Nuglets: a virtual Currency to Stimule Cooperation in Self-Organized Mobile Ad Hoc Networks. Institute for Computer Communications and Applications Department of Communication Systems Swiss Federal Institute of Technology Lausanne, 18 January 2001, pages 15.

[22]: GETSY S SARA, NEELAVATHY PARI.S, SRIDHARAN.D. Energy Efficient Ad Hoc On Demand Multipath Distance Vector Routing Protocol, International Journal of Recent Trends in Engineering, Vol 2, No. 3. Department of Electronics and Communication Engineering, CEG Campus, Anna University Chennai, India November 2009, pages 3.

[23]: Mads Darø Kristensen and Niels Olof Bouvin. Energy Efficient MANET Routing Using a Combination of Span and BECA/AFECA. JOURNAL OF NETWORKS, VOL. 3, NO. 3, New York, USA,MARCH 2008, pages 8.

[24]: S ARVIND, DR.T.ADILAKSHMI. power aware routing for mobile agent in ad-hoc networks. Journal of Theoretical and Applied Information Technology. Department of Computer Science & Engineering, Vasavi College of Engineering, Hyderabad- 500031. Mai 2009, pages 7.

[25]: Idoudi Hanen, Akkari Wafa, Belghith Abdelfatteh, Molnar Miklos: Alternance synchrone pour la conservation d'energie dans les réseaux mobiles ad hoc. IRISA, Centre Universitaire de Beaulieu-35042 Rennes CEDEX-France, Novembre 2006, pages 46.

[26] : Choi Heesook, McDaniel Patrick, La Porta Thomas F.: Privacy Preserving Communication in MANETs. Department of Computer Science and Engineering the Pennsylvania State University, Mars 2007, pages 10.

[27]: Yan Zheng, Zhang Peng, Virtanen Teemupekka. Trust Evaluation Based Security Solution in Ad Hoc Networks. Helsinki University of Technology, Finland, Decembre 2003, pages 14.

[28]: Yi Ping, Dai Zhoulin, Zhang Shiyong, Zhong Yiping: A New Routing Attack in Mobile Ad Hoc Network. Department of Computing and Information Technology, Fudan University, Shanghai, 200433, China, June 2005, pages 12.

[29]: Revathi Venkataraman, M. Pushpalatha, and T. Rama Rao. Performance Analysis of Flooding Attack Prevention Algorithm in MANETs. World Academy of Science, Engineering and Technology 56, Septembre 2009, pages 4.