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

N° d'ordre : .....

UNIVERSITE DE M'SILA

FACULTE DES MATHEMATIQUES ET DE L'INFORMATIQUE

Département d'Informatique

MEMOIRE de fin d'étude

Présenté pour l'obtention du diplôme de MASTER

Domaine : Mathématiques et Informatique
Filière : Informatique
Spécialité : Réseaux

Par : Mouloud sariak

SUJET

Sécurité de Routage dans les réseaux ad hoc : cas du protocole AODV

Soutenu publiquement le : 15/06/2015 devant le jury composé de :

Dr Lamiche Chaabane	**Université de M'sila**	**Rapporteur**
Mr Mohamed Kamel	**Université de M'sila**	**président**
Mr Mohamed Sahraoui	**Université de M'sila**	**Examinateur**

Promotion : 2014 /2015

Sommaire

Introduction générale

Au cours des dernières années, de nombreuses normes de connectivité et de technologies sans fil ont vu le jour pour répondre à la hausse constante des besoins en mobilités. Dans un future proche, ces technologies constitueront le socle d'environnements persuasifs (ubiquitaires) dans lesquels les utilisateurs pourront accéder à des services, communiquer, travailler avec l'autre usagers en tout lieu, à tout instant et depuis n'importe quel équipement mobile.

Les réseaux mobiles ad hoc (MANET) représentent une composante clé de cette évolution et leurs fondements seront inévitablement intégrés aux futures générations de réseaux sans fil.

Les réseaux mobiles sans fil, peuvent être catégorisés en deux classes : les réseaux avec infrastructure qui utilisent généralement le modèle de la communication cellulaire, et les réseaux sans infrastructure ou les réseaux ad hoc qui font l'objet de notre étude.

Un réseau ad hoc peut être défini comme une collection d'entités mobiles interconnectées par une technologie sans fil formant un réseau temporaire sans l'aide de toute administration ou de support fixe.

Les caractéristiques des réseaux ad hoc, comme l'absence d'infrastructure et l'utilisation d'un canal radio rendent la sécurité un véritable défi technologique auquel nous sommes confrontés.

Le sujet de notre thèse entre dans le cadre de l'étude du problème de la sécurité du routage dans les réseaux mobiles ad hoc

Ce projet de fin d'étude contient cinq chapitres organisé comme suit :

Le premier chapitre présente les différents types de réseaux sans fil ainsi qu'une classification de ces réseaux. Le deuxième chapitre représente une analyse de sécurité dans laquelle nous avons énuméré les attaques et les menaces possibles sur les réseaux ad hoc, nous allons présenter les attaques reliées aux protocoles de routage dans le troisième chapitre. Une présentation générale de protocole AODV avec une étude de l'attaque Blackhole avec des solutions proposées fait l'objectif du quatrième chapitre. Le dernier chapitre contient les résultats de notre travail de ce qui concerne la simulation.

Conclusion générale

Les réseaux ad hoc semblent avoir un bon avenir dans les prochaines années puisqu'ils permettent la présence de l'information d'une manière distribuée. Cependant, Le problème de la sécurité dans les réseaux ad hoc a un impact décisif à son avenir, les données transmises sont potentiellement sensibles et il est souvent facile de les intercepter ou de les manipuler.

Deux aspects sont critiques et importants : la sécurité des données transmises et en particulier la sécurité du routage ad hoc qui est vulnérable à plusieurs attaques.

Dans ce mémoire de fin d'étude, nous avons étudié et présenter les caractéristiques des réseaux ad hoc, ensuit nous avons fait une analyse de sécurité dans laquelle nous avons énuméré les différentes attaques etrisques liés à la sécurité des réseaux ad hoc. Ces derniers sont vulnérables aux attaques à cause de leurs caractéristiques (utilisation d'un canal radio pour la transmission de données, absence d'infrastructure, l'absence d'une relation de confiance préalable, la mobilité).

Notre travail focalisait sur la sécurisation du routage, dans le but de proposer des solutions de sécurité léger et efficace qui nous permette de préserver les performances globales du réseau contre les attaques possibles au niveau de routage. Un exemple spécifique de l'une de ces attaques est l'attaque Blackhole. Ce type d'attaque peut représenter une menace importante pour le bon fonctionnement du réseau.

La sécurité de protocoles de routage a été pleinement étudiée et plusieurs solutions ont été proposées, nous avons basés sur des technique de prévention qui nous donne la possibilité de sécurisation de ces protocoles.

Dans ce mémoire,Nous nous sommes intéressés à la sécurité au niveau routage, plus précisément nous avons basé notre étude sur la sécurisation du protocole AODV, nous nous sommes intéressés à l'analyse de l'attaque Blackhole.

Nous avonsproposé un protocole basé sur l'approchede l'IDS qui va permettre d'éviter cette attaque, la solution exploite la communication entre les nœuds au cours de l'envoi des messages decontrôle pourassurer la détection du comportement malhonnête, ce principe permet au protocole étudié de détecte le comportement suspect lié à l'attaque Blackhole.

Pour évaluer les performances du protocole, nous avons implémenté la solution sous le simulateur ns-2. Ensuite, nous sommeseffectuésdessimulations de scénarios proposéset nous avons présenté et interprété les résultats obtenus.

Ce projet nous a offert l'occasion de travailler sous l'environnement Linux, découvrir l'outil de simulation des réseaux ns-2, découvrir et enrichir nos connaissances sur des domaines de recherche très vastes, à savoir les réseaux ad hoc, la sécurité des réseaux en général et les systèmes de détection d'intrusionen particulier. Grâce à notre étude, nous avons aussi constaté qu'il ne peut y avoir une sécurité absolue. Cela est dû au nombre important des facteurs qui conditionnent les performances des réseaux et des protocoles utilisés.

Un mémoire ou une thèse :

[1] K.ayad,Sécurité de routage dans les réseaux ad hoc mobiles,(magistere),oued smar Alger,2012.

[2] O.cheikhrouhou,Sécurité des réseaux ad hoc,(license), Sfax, Tunisie,2005.

[6] A.Hajami. Sécurité du routage dans les réseaux sans fil spontanés : cas du protocole OLSR ,(Doctorat),maroc 2011.

[13] H.Hafi, Protocole pour la sécurité des réseaux sans fil, (magistere), ouargla, 2011.

Un site web :

[3] Comment ça marche http://www.commentcamarche.net/ consulté le 21/04/2015.

Un ouvrage :

[4] K.kadima,Mise en place sur le point d'accès d'un réseau wifi.2010.

[5] Van ,Hybridation entre les modes ad-hoc et infrastructure dans les réseaux de type Wi-Fi,bruxelle,2006.

[7] ValérieGayraud, LoutfiNuaymi, Francis Dupont, Sylvain Gombault, and Bruno Tharon, « La Sécurité dans les Réseaux Sans Fil Ad Hoc ».

[8] Paul Mahlethan, « 802.11 et les réseaux sans fil », livre Edition Eyrolles, 2002.

[9] Yingshu Li, My T. Thai, Weili Wu, «Wireless Sensor Networks and Applications» , 2008.

[10] Chris Karlof, David Wagner, «Secure routing in wireless sensor networks: attacks and countermeasures», Ad Hoc Networks, 2003.

[11] L. Lazos, R. Poovendran, C. Meadows, P. Syverson, , L.W. Chang : "Preventing wormhole attacks on wireless ad hoc networks.March 2005.

[12] R.Abdellaoui.une nouvelle sollution pour le protocole OLSR.

[14] M.Abdelhaq.al, "Security Routing Mechanism forBlack Hole Attack over AODV MANET Routing Protocol",Australian Journal of Basic and Applied Sciences, 5(10):1137-1145, 2011 University Kebangsaan Malaysia, 2011.

[15] K.LakSBmi, al. "Modified AODV Protocol against Black hole Attacks in MANET", International Journal of Engineering and Technology Vol.2 (6), 2010, 444 -449, 2010.

[16] Deng H., Li W. and Agrawal, D.P., "Routing security in wireless ad hoc networks" Communications Magazine,IEEE, October 2002.

[17] Al-Shurman, M., Yoo, S. and Park, S, "Black hole Attack in Mobile Ad Hoc Networks", ACM Southeast Regional Conference, 2004.

[18] Payal N. Raj1 and Prashant B. Swadas2, "DPRAODV: A Dynamic Learning System against Blackhole Attack in AODV based MANET", IJCSI International Journal of Computer Science Issues, 2009.

[19] S. Dokurer, Y. M. Erten and E. A. Can, "Performance Analysis of Ad-Hoc Networks under Black Hole Attacks," Proceeding from SECON'07: IEEE Southeast Conference, Richmond, 22-25 March 2007, pp. 148-153.

[20] Kevin Fall et Kevin Fall et Kannan Varadhan "The ns Manual", 2011.

ملخص:

تطرقنا في هذا العمل المتواضع الى دراسة شبكات اد هوك اللاسلكية المتنقلة وقمنا بدراسة شاملة لمختلف أنواعها كما قمنا بدراسة سبل الحماية في هذا النوع من الشبكات وركزنا في بحثنا على أساليب الحماية على مستوى بروتوكولات توجيه البيانات في الشبكة

قمنا بالتركيز على أحد البروتوكولات من النوع التفاعلي، والتي ترتكز على الربط عند الطلب. البروتوكول المدروس هو البروتوكول AODV، قمنا بالحديث معظم الهجومات المحتملة على هذا البروتوكول، تطرقنا الى دراسة أحد هذه الهجمات وهو هجوم الثقب الأسود. تحدثنا عن بعض الحلول العملية والسهلة من أجل الحماية ضد هذا النوع من الهجمات. كما قمنا في الأخير بمحاكاة هذا الهجوم في شبكة افتراضية باستعمال برنامج المحاكاة NS-2 قمنا كذلك بطرح أحد الحلول الممكنة للحماية وهو عبارة عن نظام لكشف التسلل وقمنا بمحاكاته وتوصلنا الى نتائج مقبولة تسمح بالحصول على حماية مبدئية ضد هذا النوع من الهجومات

الكلمات المفتاحية: شبكات اد هوك. حماية ضد الهجمات. بروتوكول توجيه.AODV.الثقب الاسود.IDS.NS-2.محاكاة

Résumé :

De ce projet de fin d'étude, nous avons étudié les réseaux mobiles de type ad hoc et nous avons fait une étude approfondie des différents types de ces réseaux, nous avons étudiés les moyens de protection dans ce type de réseaux et dans notre recherche nous nous sommes concentrés sur les méthodes de protection au niveau des protocoles de routage. Nous avons nous concentrer sur un seul protocole réactif, qui est basé sur l'approche le lien à la demande. Le Protocole étudié est le protocole AODV, Nous énumérons les attaques les plus potentiels sur ce protocole, Nous avons concentré notre étude sur l'attaque BlackHole .Nous avons parlé de quelques solutions pratiques et faciles pour la protection contre ce type d'attaque. Nous avons simulé cette attaque dans un réseau à l'aide d'un simulateur de réseaux ns-2 nous avons également introduit une solution léger pour la protection contre l'attaque BlackHole ,cette solution est basée sur l'approche de l'IDS, Nous avons acquis des résultats acceptables qui permettent d'effectuer une protection initiale contre ce type d'attaques.

Mots clés : Réseaux ad hoc, Protection des réseaux, Protocoles réactifs, AODV, BlackHole, Simulation, NS-2, IDS.

Abstract:

In this final project of study, we have talked about one of the most popular type of networks, it's the ad hoc mobile networks, we have done a general study for the various types of these networks, we studied how we could level-up the security and protection in this type of networks and in our search, we have focused on routing protocols. We focus on a single reactive protocol, which is based on the approach link on demand. The studied protocol is the AODV protocol, we list the potential attacks on this protocol, and we have focused in our study on the Black Hole attack. We talked about some practical and easy solutions to protect the network against this type of attack. We simulated the attack in a virtual network using the simulator ns-2, we also introduced a lightweight solution to protect against the attack Black Hole, it is based on the IDS mechanism, and we acquired acceptable results that perform Initial protection against such attacks.

Key words: Ad hoc networks, Network protection, reactive protocols, AODV, Black hole, Simulation, NS-2, IDS