Université de L'Hadj Lakhdar-Batna
Faculté des sciences de l'ingénieur
Département d'informatique

MÉMOIRE DE MAGISTÈRE EN INFORMATIQUE

Option : Informatique industrielle

Intitulé :

De la Sécurité à la E-Confiance basée sur la Cryptographie à Seuil dans les Réseaux sans fil Ad hoc

Présenté par : ***M^r^ Abdesselem BEGHRICHE***

Sous la direction de : ***Dr Azeddine Bilami***

Membre de Jury composé de :

Dr M.K. Kholladi :	M.C Université de Constantine	Président
Dr B. Belattar :	M.C Université de Batna	Examinateur
Dr R. Maamri :	M.C Université de Constantine	Examinateur
Dr A. Bilami :	M.C Université de Batna	Rapporteur

Promotion 2008/2009

A mes chers parents qui m'ont soutenu durant mon existence et ma scolarité. Je leur dédie ce mémoire.

Abdesselem

Remerciements

Au terme de ce travail, Je tiens à remercier :

Merci à Dr Azeddine Bilami, mon encadrant, tu m'as fait bénéficier de ton savoir, de tes compétences scientifiques et de ta passion pour la recherche. Je te remercie également de m'avoir appris à aller jusqu'au bout de mes idées.

Merci très vivement à Dr Mohammed Kheireddine Kholladi, Dr Brahim Belattar et Dr Ramdane Maamri de l'honneur qu'ils m'ont fait en acceptant de siéger à mon jury de magistère.

Mes remerciements vont à tous les membres de ma famille à qui je dois beaucoup, sans leurs aides, ce travail n'aurait pu voir le jour.

Merci à tous ceux qui m'ont aidé sans ménager ni leurs temps, ni leurs encouragements, ni leurs savoirs.

Je tiens tout particulièrement à remercier, mon cher ami Abderrahmane Boumezbeur pour ses conseils et ses aides.

Et enfin, merci à tous les chercheurs que j'ai pu rencontrer lors des conférences et qui sont intéressés à mes travaux.

Abdesselem BEGHRICHE

ملخص :

موضوع هذه المذكرة يركز على الأمن في شبكات المحمول اللاسلكية المخصصة (أد-هوك). نقوم بدراسة أمن هذه الشبكات نظرا لعدم وجود إدارة مركزية، الشيء الذي يجعل من هذه الأخيرة أكثر عرضة للهجوم مقارنة بالشبكات الأخرى (السلكية واللاسلكية). للأسف، بروتوكولات الأمن والحماية الموجودة حاليا ليست مصممة لمثل هذا النوع من الشبكات (محيط ديناميكي متحرك)، أضف إلى ذلك محدودية الطاقة والذاكرة وضعف القدرة على الحساب) وذلك مما يزيد من تعقيد مشكلة الأمن في هذه الشبكات، ونظرا لأهمية إستخدام هذه الشبكات في عدة مجالات مثل العمليات العسكرية، الاتصالات بين الطائرات والسيارات والأفراد وعمليات الإغاثة في حالات الطوارئ والكوارث، وما إلى ذلك)، فإنه من الضروري أن يكون الهدف الرئيسي من هذا العمل هو وضع آلية أمنية مضمونة وذلك من خلال اقتراح بنية هرمية توزيعية والتي تسمح باستخدام هيكل مبني على مفتاح عام. كما يجب دعم هذه البنية للخصائص المختلفة لهذه الشبكات (عدم وجود مركزية لإدارة الشبكة، محدودية الطاقة والذاكرة، الخ) وتحقيقا لهذه الغاية، نقوم بتكييف نموذج للثقة مع هذه البنية لتطوير مستويات الثقة في كل عقدة من الشبكة.

هذا النموذج يؤسّس على مبدأ عتبة الكتابة السرّيّة، ويجمع بين عناصر أمن الشبكات التقليدية والعناصر الجديدة التي نقترحها، بحيث يتغذى هذا النموذج على تفاعلات وسلوك العقدة مع بيئتها.

كلمات البحث الرئيسية : شبكات المحمول المخصصة (أد-هوك)، أمن الشبكات، خوارزميات توزيعية، أنظمة المراقبة، هياكل المفاتيح العمومية، تفصيص الشبكات، الثقة والسمعة، IEEE 802.11.

Abstract:

This research work is focused on security in Ad hoc mobile networks (MANET: Mobile Ad hoc NETwork). The absence of a central management of the functionalities of the network makes them much more vulnerable to attacks than wireless networks (WLAN) and ordinary wire networks (LAN). Unfortunately, the protocols of security which exist nowadays are not conceived for such environment (dynamics).

They do not take in consideration the shortage of means because not only the environment is dynamic, but means are also restricted (memory, capacity of calculation and especially energy), which make the problems more complicated, as it is known that the resolutions of security are very demanding in term of means. However, owing to the importance of the domains of application of Ad hoc mobile networks in the military (communication between planes, cars and personnel and operations of assistance, urgent situations in case of disaster, etc), therefore, to take up the challenge for the design of a mechanism of infallible security for mobile networks Ad hoc is necessary.

The main objective of this thesis is to study the resolutions that are likely to ensure security in Ad hoc mobile networks, by offering a distributed hierarchic architecture which allows the establishment of dynamic facilities with public key. This architecture must support the different characteristics of these networks (absence of a central processing unit of management of network, dynamic network topology, etc). To this end, a trust model adapted to a dynamic environment, to ensure the evolution of the trust levels of the nodes, is established. This model based on the principle of threshold cryptography and combines at the same time the classical elements of security and the new elements which we suggest, which are nourished by the correlations of entity (node) with its environment.

Key words: Mobile Ad hoc networks, Security, Distributed Algorithms, Public Key Infrastructure (PKI), Mechanism of surveillance, IEEE 802.11, Clustering, Trust and Reputation.

Résumé :

Le sujet de ce mémoire se focalise sur la sécurité dans les réseaux mobiles sans fil Ad hoc (MANET : Mobile Ad hoc NETwork). L'absence d'une gestion centrale des fonctionnalités du réseau rend ces réseaux beaucoup plus vulnérables aux attaques que les réseaux sans fil (WLAN) et filaires (LAN). Malheureusement, les protocoles de sécurité qui existent actuellement ne sont pas conçus pour un tel environnement (dynamique). Ils ne prennent pas la contrainte des ressources en considération car non seulement l'environnement est dynamique, mais les ressources sont aussi limitées (mémoire, capacité de calcul et surtout énergie), ce qui complique davantage la problématique, car on sait bien que les solutions de sécurité sont gourmandes en terme de ressources. Cependant, en raison de l'importance des domaines d'application des réseaux mobiles Ad hoc comme les opérations militaires (communication entre les avions, les voitures et le personnel et opérations de secours, situations d'urgence en cas de sinistre, etc.), il faut relever le défi, car concevoir un mécanisme de sécurité infaillible pour les réseaux mobiles Ad hoc est nécessaire.

L'objectif principal de ce mémoire consiste à étudier les solutions susceptibles d'assurer la sécurité dans les réseaux mobiles Ad hoc, en proposant une architecture hiérarchique distribuée qui permet d'établir une infrastructure dynamique à clé publique. Cette architecture doit supporter les différentes caractéristiques de ces réseaux (absence d'une unité centrale de gestion de réseau, topologie réseau dynamique, etc.). Dans ce but, un modèle de confiance adapté à l'environnement dynamique pour assurer l'évolution des niveaux de confiance des nœuds est établi. Ce modèle basé sur le principe de la cryptographie à seuil, et combine à la fois les éléments classiques de la sécurité et de nouveaux éléments que nous suggérons, et qui sont nourris par les interactions de l'entité (nœud) avec son environnement.

Mots clés : Réseaux mobiles Ad hoc, Sécurité, Algorithmes distribués, Infrastructure à clé publique (PKI), Mécanisme de surveillance, IEEE 802.11, Clustering, Confiance et Réputation.

Liste des figures

Liste des tableaux

Table des matières