Mohammed Erritali

Contribution à la sécurisation des réseaux ad hoc véhiculaires

EDILIVRE

بسم الله الرحمن الرحيم

ربنا عليك توكلنا و إليك أنبنا و إليك المصير

رَبِّ اشْرَحْ لِي صَدْرِي وَيَسِّرْ لِي أَمْرِي و احلل عقدة من لساني يفقهوا قولي

Résumé

L'évolution progressive des technologies sans fil a donné naissance à une nouvelle génération des réseaux utilisée dans les communications véhicule à véhicule ou véhicule à infrastructure afin d'améliorer la sécurité routière via l'échange des messages d'alerte entre les véhicules de voisinage ou encore afin d'offrir de nouveaux services de confort aux usagers des routes. Ces types de réseaux sont très dynamiques avec des architectures fortement décentralisées et dont les services sont organisés de manière autonome.

Le problème dans ces réseaux consiste à déterminer le protocole de routage le plus adapté à cet environnement, et ensuite à le sécuriser afin de fournir un acheminement optimal et sécurisé pour les données.

Dans cette thèse, nous avons proposé quelques solutions de sécurité pour les réseaux ad hoc véhiculaire à savoir: la sécurisation du protocole de routage Greedy Perimeter Stateless Routing, une méthode hybride qui utilise les deux algorithmes de datamining Random Forest et Naïve Bayes pour la construction d'un système de détection comportementale et une définition formelle d'une intrusion par la mise en œuvre d'une ontologie de détection d'intrusions dans les réseaux ad hoc véhiculaire.

Mots clés : Réseaux ad hoc véhiculaires (VANETs), protocole de routage, routage sécurisé, système de détection d'intrusion, Random Forest and Naïve Bayes, ontologie de détection d'intrusion.

Abstract

The technological advancement in Wireless network has give the birth to a new generation of networks used in vehicle-to-vehicle or vehicle to road side unit communications to improve road safety by exchanging warning messages between neighbor vehicles or to offer new comfort services to road users.

These types of networks are highly dynamic with highly decentralized architectures and whose services are organized independently.

The problem in these networks is to determine the best routing protocol suited to this environment characterized by rapid topology changes, then secure it to provide a safe and optimal route to data.

In this thesis, we propose some security mechanisms for vehicular ad hoc networks, first, two cryptographic security mechanisms have been proposed to secure the geographic routing protocol GPSR, secondly we have examined and classified intrusion detection systems then we proposed to use a combination of two data mining algorithms Random Forest and Naive Bayes in our IDS architectures to prevent from complex and distributed attacks. Finally, we propose a formal definition of an intrusion by the development of an ontology for intrusion detection in vehicular ad hoc networks.

Keywords : Vehicular Ad hoc networks (VANET), routing protocol, secure routing, intrusion detection system, Random Forest and Naive Bayes, Ontology intrusion based intrusion detection system.

Avant-propos

Les travaux présentés dans le mémoire ont été effectués au sein du laboratoire de recherche en informatique (L.R.I) à la Faculté des Sciences de Rabat.

J'exprime mes sincères remerciements au M. **Bouabid EL OUAHIDI** professeur à la Faculté des Sciences de Rabat, Université Mohammed V – Agdal, pour avoir accepté de diriger cette thèse. Je tiens à le remercier aussi pour son suivi et ses encouragements tout au long de ce travail de thèse de doctorat.

Je remercie aussi M. **Bouabid EL OUAHIDI** pour l'honneur qu'il m'a fait en acceptant de présider le jury de ma thèse.

Ensuite, je tiens à remercier M. **Mourad EL BELKACEMI** professeur à la Faculté des Sciences de Rabat, M. **Mourad GHARBI** professeur à la Faculté des Sciences de Rabat et M. **Mohamed FAKIR** professeur à la Faculté des Sciences et Techniques de Béni Mellal, pour avoir consacré du temps à lecture de cette thèse ainsi pour avoir soumis leur précieux jugement sur la qualité et le contenu de ce travail.

Mes remerciements s'adressent également à M. **Abderrahim SEKKAKI** professeur à la Faculté des Sciences Ain Chock Casablanca et **M. Daniel BOURGET** maitre de conférences à Télécoms Bretagne Brest France, membres du jury, qui ont bien accepté de siéger au jury de cette thèse. Qu'ils trouvent ici l'expression de ma reconnaissance !

Il est bon et juste d'évoquer l'appui moral ainsi que la sollicitude trouvée auprès de toute ma famille. Je tiens à exprimer mes sentiments les plus respectueux et ma profonde reconnaissance à ma cher femme Ibtissame, à mes très chers parents, à mes frères et sœurs, pour les

encouragements constants qu'ils ont déployé tout au long de ces années de recherche. Merci à tous les collègues du laboratoire LRI pour leur amitié et bonne humeur qui ont égayé ma vie au laboratoire.

Enfin, je remercie toutes les personnes qui, de près ou de loin, ont apporté leur contribution à ce travail. Je leur exprime ici toute ma reconnaissance et ma sympathie.

Liste des acronymes

AES	Advanced Encryption Standard
AODV	Ad-Hoc On demand Distance Vector
ARIADNE	A Secure On-Demand Routing Protocol for Ad Hoc Networks
A-STAR	Anchor-based Street and Traffic Aware Routing
ASTM	American Society for Testing and Materials
BPSK	Binary Phase Shift Keying
C2C-CC	CAR 2 CAR Communication Consortium
CCH	Control Channel
CHM	Cluster-Head module
CMM	Cluster-Member module
CONFIDANT	COoperation of Nodes Fairness In Dynamic Ad hoc NeTworks
CORE	COllaborative REputation
CW	Contention Window
DAG	Directed Acyclic Graph
DDOS	Distributed Denial of Service
DSR	Dynamic Source Routing
DSRC	Dedicated Short Range Communications
ETSI TC	European Telecommunications Standards Institute Technical Committee
FSR	Fisheye State Routing
FTP	File Transfer Protocol
GACE	Global Aggregation and Correlation Engine
GF	Greedy Forwarding
GG	Global Positioning System
GLS	Greedy Location Service
GPCR	Greedy perimeter coordinator routing

GPS	Global Positioning System
GPSR	Greedy perimeter stateless routing
GRP	Geographic routing protocol
GSR	Geographic source routing
HMAC	Hashed Message Authentication Code
IDS	Intrusion detection system
IEEE	The Institute of Electrical and Electronics Engineers
IP	Internet Protocol.
ITS	Intelligent Transportation Systems
JDK	Java Development Kit
KDD'99	Knowledge Discovery in Databases 1999
LACE	Local Aggregation and Correlation Engine
MAC	En réseau désigne medium allocation control En cryptographie désigne message authentification code
MANET	Mobile Ad-hoc NETworks
MD5	Message Digest 5
MLP	Multi Layer Perceptron
OFDM	Orthogonal Frequency Division Multiplexing,
OLSR	Optimized Link State Routing
OMNET++	Objective Modular Network Testbed in C++
OPNET	Optimized Network Engineering Tool
OTCL	Oriented Tool command Language
PDA	Personal Digital Assistant
PF	Perimeter Forwarding
PHY	Physical Layer
PKI	Public Key Infrastructure
QAM	Quadrature Amplitude Modulation
QLS	Quorum-based location
QPSK	Quadrature Phase-Shift Keying
RERR	Route ERRor
RFC	Request For Comment
RNG	Relative Neighborhood Graph
RREP	Route REPly
RREQ	Route REQuest SN
RS-232	Recommended Standard 232
RSU	Roadside units (infrastructure de bord de la route)
SAODV	Secure Ad-Hoc On demand Distance Vector

SCH	Service Channel
SGPSR	Secure Greedy perimeter stateless routing
SOLSR	Secure Optimized Link State Routing
SRP	Secure routing protocol
TCP	Transport Control Protocol
TESLA	Timed Efficient Stream Loss-Tolerant Authentication
TORA	Temporally-Ordered Routing Algorithm
UWB	Ultra Wide Band
V2I	Véhicule à Infrastructure
V2V	Véhicule à Véhicule
VANET	Vehicular Ad-Hoc NETwork
WAVE	Wireless Ability in Vehicular Environments
ZBIDS	Zone based Intrusion Detection system

Liste des figures