UNIVERSITE DES SCIENCES ET DE LA TECHNOLOGIE HOUARI BOUMEDIENE (USTHB)

FACULTE D'ELECTRONIQUE ET D'INFORMATIQUE

MÉMOIRE

Présenté pour l'obtention du diplôme de :

MAGISTER

en Informatique

Option : Informatique Mobile

Par :

Mr. Boualouache Abdelwahab

Sujet:

SÉCURITÉ ET VIE PRIVÉE DANS LES RÉSEAUX VÉHICULAIRES

Mr. Y.ZAFFOUNE	**Maître de Conférences A (USTHB)**	**Président**
Mme S.MOUSSAOUI	**Professeur (USTHB)**	**Directrice de mémoire**
Mme N. NOUALI	**Directrice de Recherche (CERIST)**	**Examinatrice**
Mlle C.BENZAID	**Maître de Conférences B (USTHB)**	**Invitée**

قال الله تعالى :

وَقُل رَّبِّ زِدْنِي عِلْمًا ﴿١١٤﴾

سورة طه

Remerciements

On remercie **Allah** le tout puissant, qui m'a donné la force et la patience pour l'accomplissement de ce travail.

Je tiens à remercier chaleureusement ma promotrice, **Madame Samira MOUSSAOUI**, de m'avoir proposé ce projet, en me faisant confiance, et d'avoir dirigé ce travail avec ses orientations, ses précieux conseils et remarques. Je vous remercie infiniment Madame pour le temps que vous avez consacré à ce travail, pour votre disponibilité, votre gentillesse, votre patience et votre modestie. J'ai eu le grand plaisir de travailler sous votre direction et j'espère pouvoir continuer à travailler avec vous.

Mes remerciements s'adressent également **aux membres du jury** pour l'immense honneur qu'ils m'ont fait en acceptant d'évaluer ce travail.

Je remercie énormément mes **très chers parents**, mes frères et le reste de la famille pour m'avoir apporté du réconfort et pour m'avoir soutenu dans tous mes efforts

Mes sincères remerciements vont à **Mlle Hayet ZERROUKI** et **Mr Badreddine ALLOUCHE** pour leurs aides et leurs encouragements.

Mes remerciements s'adressent également à tous mes **amis**, à tous mes **collègues de PG informatique** et à tous mes **collègues d'équipe DataWareHouse (OoredoO)** pour leur gentillesse, leur compréhension et l'ambiance.

Enfin, que tous ceux qui ont contribué de prés ou de loin, par leurs encouragements et conseils à l'accomplissement de ce travail, trouvent ici l'expression de ma profonde reconnaissance.

Boualouache Abdelwahab

<< Life is a journey
of learning ... >>

Résumé

Les réseaux ad hoc véhiculaires (*VANET*) ont été développés essentiellement pour améliorer la sûreté de conduite et assurer le confort aux conducteurs et aux passagers. Cette technologie offre une variété d'applications très prometteuses, s'étendant de la sécurité routière (par exemple, la diffusion des messages d'urgence) au confort (l'information non critique) (par exemple, l'échange des vidéos).

Dans les applications liées à la sécurité routière, chaque véhicule a besoin de diffuser périodiquement un message authentifié de sûreté. Ce message contient des informations qui concernent le statut du véhicule tel que l'identité, la position, la vitesse, et l'accélération. Bien que ces messages puissent aider à empêcher des accidents, ils peuvent également être utilisés par les attaquants pour une poursuite non autorisée d'un véhicule. En effet, vu la nature des communications sans fil, un attaquant peut facilement écouter tous les messages diffusés et déterminer ainsi les emplacements visités par les véhicules sur une certaine période de temps. Ce qui compromet la vie privée des conducteurs puisqu'il y a généralement une forte corrélation entre un véhicule et son conducteur. D'où, la protection de la vie privée est importante car ce manque de protection peut perturber ou obstruer le grand déploiement de la technologie des réseaux véhiculaires.

Pour remédier à ce problème, une approche connue dans la littérature consiste à utiliser des multiples pseudonymes, au lieu des identifiants statiques. Le véhicule peut alors changer son pseudonyme de façon autonome, pour compliquer la poursuite de ses positions. Cependant, les études récentes basées sur le changement du pseudonyme ont montré une faible efficacité de cette approche en termes du niveau de protection fourni. Cela est dû aux attaques de corrélation des pseudonymes. Pour pallier à ces attaques, plusieurs stratégies ont été proposées dans la littérature afin de fournir un changement de pseudonyme plus fiable. Néanmoins, le développement d'une stratégie efficace de changement du pseudonyme n'est pas toujours réalisable. C'est dans ce cadre qu'on propose une solution qui tente de répondre à ce problème.

Dans ce travail, nous proposons une stratégie pratique de changement du pseudonyme adaptée pour l'environnement urbain, appelée *Silence and Swap at Signalized Intersection (S2SI)*. En particulier, nous proposons deux protocoles, un pour créer les *Silent Mix Zones (SMs)* et un autre pour l'échange des pseudonymes entre les véhicules sous le contrôle de RSUs(Road Side Units), dans les SMs, tout en maintenant la traçabilité par les autorités. Nous évaluons la protection de la vie privée assurée par notre stratégie en développant un modèle analytique d'ensemble anonymat et en réalisant des simulations de la stratégie en utilisant l'entropie d'ensemble d'anonymat comme une métrique primaire.

Mots-clés : *Vehicular Ad hoc Networks (VANETs)*, vie privée, changement du pseudonyme, sécurité.

Abstract

Vehicular ad hoc networks(*VANETs*) are initially designed for enhancing driving safety and convenience in transportation systems. This technology offers a variety of promising applications, ranging from safety (e.g., emergence reporting and collision warning) to non-safety (e.g., infotainment), can be enabled to improve the road safety and better driving experiences.

In safety-related applications, each vehicle needs to periodically broadcast an authenticated safety message. This message is sent with a high frequency. This message includes vehicular status information such as veritable identity, position, speed, and acceleration. Although these safety messages can help to prevent accidents, they may also be used by the attackers for unauthorized location tracking of vehicles.

Due to the nature of the wireless communications, an attacker can easily eavesdrop on all the broadcast messages and determine the locations visited by the vehicles over a period of time, which compromise the privacy of drivers since there is usually a strong correlation between a vehicle and its driver. Thus, protecting the location privacy of vehicles is important because the lack of privacy may hinder the wide acceptance of *VANET* technology.

A common approach to avoid this problem is the use of multiple identifiers called the pseudonyms, instead of static identifiers. Vehicle can then autonomously change their pseudonym, to complicate tracking of their positions. This approach regards anonymity as being untraceable between two successive locations of the target. Since pseudonyms cannot be linked to each other, they can provide a certain degree of privacy. However, recent studies on the effectiveness of pseudonym changes in terms of achieved privacy level have shown the weakness of this approach to provide the required protection due to pseudonyms linking attacks. To combat such attacks, many strategies have been proposed in the literature to provide an efficient pseudonym changing. But the development of an efficient changing pseudonyms strategy is not yet achieved and it still an open problem in literature.

In this work, we propose a practical pseudonym changing strategy adapted for urban environment, called *Silence and Swap at Signalized Intersection (S2SI)*. In particular, we propose two protocols, one for creating Silent *Mix Zones (SMs)* and another allows the exchange of pseudonyms between vehicles under the control of RSU, within these *SMs*, with the maintaining of liability. We evaluate the provided privacy protection of our strategy by developing anonymity set analytic model and by performing a simulative study of the strategy using the entropy of vehicles' anonymity set as the primary metric.

Keywords : *Vehicular Ad hoc Networks (VANETs)*, Privacy, Pseudonyms Changing, Security.

Table des matières