MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE

وزارة التعليم العالي والبحث العلمي

BADJI MOKHTAR-ANNABA UNIVERSITY
UNIVERSITE BADJI MOKHTAR-ANNABA

جامعة باجي مختار – عنابـة

Faculté des Sciences de l'Ingéniorat
Département d'Informatique

Année : 2013/2014

THÈSE

Présentée en vue de l'obtention du diplôme de
Doctorat 3ème cycle

La sécurisation des réseaux sociaux mobiles

Filière : Informatique

Spécialité : Réseaux et Sécurité Informatique

Par

Mohamed Amine FERRAG

Devant le jury :

Directeur	M. Salim GHANEMI	Maitre de Recherche à l'Université d'Annaba
Présidente	Mme. Nacira GHOUALMI-ZINE	Professeur à l'Université d'Annaba
Examinateur	M. Yacine GHAMRI-DOUDANE	Professeur à l'Université de La Rochelle
Examinateur	M. Okba KAZAR	Professeur à l'Université de Biskra
Invité	M. Mehdi NAFA	Maitre de conférences à l'Université d'Annaba

Dédicace

Je dédie cet humble travail,

A ma chère maman, qui a toujours été là pour moi, m'a toujours soutenu, compris et fait tout ce qu'il faut pour me faciliter la vie, merci maman,

A mon adorable papa, sans qui je ne serai jamais arrivé en Doctorat, cet homme qui a toujours su être présent pour moi, à tout moment et en toutes circonstances, faisant ainsi tout les sacrifices, soucieux toujours de me propulser vers le meilleur, un très grand merci papa,

A mon frère avec qui j'apprends toujours de la vie, des acquis que je n'aurais jamais su avoir sans toi, merci Abdelhamid,

A mes 2 petites sœurs, merci Fatima Zohra - Amina Aya,

A vous mes camarades de parcours les précieux amis du Laboratoire Réseaux et systèmes.

Encore merci du fond du coeur,

Mohamed Amine

Remerciement

Ce travail de thèse n'aurait jamais aboutit sans l'aide, les encouragements et l'implication de certaines personnes à qui j'exprime à travers ces quelques phrases modestes toute ma gratitude, en particulier :

Je suis très reconnaissant envers Madame Nacéra Ghoualmi-Zine, Professeur à l'Université de Badji Mokhtar- Annaba (Algérie) pour m'avoir fait l'honneur d'être la présidente du jury.

Je remercie chaleureusement Monsieur Yacine Ghamri-Doudane, Professeur à l'Université de La Rochelle (France), Monsieur Okba KAZAR, Professeur à l'Université de Biskra (Algérie), pour m'avoir fait l'honneur de juger ma thèse et de rapporter mon travail je vous remercie pour toute l'attention portée durant cette évaluation.

Toute ma gratitude va à mes encadreurs Monsieur Mehdi Nafa, Docteur à l'Université de Badji Mokhtar-Annaba (Algérie) ainsi que Monsieur Salim Ghanemi, Docteur à l'Université de Badji Mokhtar-Annaba (Algérie) pour m'avoir permis de réaliser cette thèse dans les bonnes conditions. Je les remercie aussi pour m'avoir donné toute ces idées, ainsi que pour toutes les riches réunions de travail, sans quoi je ne serai jamais arrivé à bout de cette thèse, je ne vous remercierai jamais assez pour m'avoir fait profiter de votre expérience et de m'avoir témoigné tant de bienveillance.

Je remercie mon père Y. Ferrag pour avoir bien voulu faire une relecture critique de ce manuscrit.

الملخص

في السنوات الأخيرة على شبكة الإنترنت، نشهد ظاهرة حقيقية هي الشبكات الاجتماعية. يتم تطوير هذه الشبكات للوصول إلى الملايين من المستخدمين في جميع أنحاء العالم، حيث يمكننا خلق مساحة شخصية لمشاركتها مع أصدقائنا الحقيقين أو الإفتراضين أيامنا، أيضا مناقشتهم، اللعب معهم أو التعرف على أشخاص جدد مثل الفيسبوك، تويتر و جوجل. ومع ذلك ، وجدت الشبكات الاجتماعية قبل فترة طويلة من الإنترنت من حولنا في أماكن العمل و الأسر والجماعات الاجتماعية. عموما ، الشبكة الإجتماعية هي في الواقع ليس أكثر من مجموعة من الناس أو المنظمات مترابطة بواسطة تفاعلها الاجتماعي. اليوم ، 72 ٪ من الشركات التي شملتها الدراسة الآن ، الشبكات الاجتماعية تشكل تهديدا لأمنها. وفقا لتقارير شركات الأمن الدولي ، أصبحت الشبكات الاجتماعية ملعب جديد للهجمات الخبيثة مدعي للقلق في عام 2013 . مستخدمي الانترنت يقضون المزيد من الوقت على الشبكات الاجتماعية، و إيصال المعلومات الشخصية الحساسة في بعض الحالات قيمة، و هذا يعتبركنز لمتسللين. بالإضافة إلى ذلك، خدمة الشبكات الاجتماعية سرعان ما انتشرة إلى منصات المتحركة حيث يرتديها الناس محتوى الوسائط المتعددة في الأجهزة الشخصية القوية، مثل أجهزة الكمبيوتر المحمولة ، الهاتف الذكي ، المساعد الشخصي الرقمي ، و ترغب في مشاركتها مع أصدقائهم أو العثور على الأشخاص لذيهم مصالح مماثلة . يمكن تصنيف الشبكات الاجتماعية على أجهزة الهاتف النقال إلى فئتين : مع البنية التحتية و دون البنية التحتية. في هذه الأطروحة ، ونحن نركز على الشبكات الاجتماعية في بيئة دون البنية التحتية ، أي شبكات خاصة "ادهوك".

الارتفاع الأخير والإعتماد الواسع النطاق جزأ لا يتجزأ من تطبيقات الشبكات اللاسلكية لأنظمة الاتصالات المتنقلة العديد من الرؤى لعالم يتزايد بالشبكية والتفاعلية. هذا المقترح في السنوات الأخيرة هو المخصص لشبكة الاسلكية الخاصة (مانيه)، حيث يتم تشكيلها من قبل مجموعة من الأفراد الذين ينظمون أنفسهم بسفة اللامركزية و بشكل كامل، وبالتالي تشكيل شبكة مستقلة وديناميكية تقوم على لا سلكي دون البنية التحتية . المضيفين قد تكون ثابتة أو متحركة. تطبيقات هذه الشبكات عديدة وبشكل رئيسي المناطق حيث البنية التحتية السلكية غير متوفرة أو غير مرغوب فيها. وهذا هو الحال على سبيل المثال في المناطق التي دمرتها الكوارث الطبيعية حيث الإغاثة لديها الحاجة كبيرة للاتصال. يخضع تصميم بروتوكولات الاتصالات لشبكات الإعلان مخصص أساسا من ثلاثة عوامل هي: الطاقة محدودة، الاستقلالية في اتخاذ القرار، والبنية الديناميكية. في السنوات الأخيرة، تم إجراء الكثير من البحوث على دراسة الميزات الفريدة من مانيت لمعالجة مشاكل الأمن والخصوصية في الشبكة من طرف المتطفلين، ولكن اتخذت قليل منها الخصائص الاجتماعية للمانيت بعين الاعتبار. في الشبكة مانيت، يتم تدريب العقد عادة في البيئة الحضرية، ولذا فإننا يمكن أن نتصور أن تنقل العقد يعكس بشكل مباشر على الأفضليات الاجتماعية من السائقين والمهام اليومية، على سبيل المثال، حيث عادة ما تذهب للتسوق أو وظيفة. بسبب هذه العوامل البشرية في الشبكة مانيت، تتعلق ليس فقط إلى التطبيقات الأمنية، ولكن أيضا سوف التطبيقات غير المتعلقة بالسلامة لها ميزات اجتماعية.

نتائج البحوث في أطروحة يجب أن تكون مفيدة لتنفيذ أمن وخصوصية الشبكات الاجتماعية المتنقلة.

Abstract

In recent years on the Internet, we are witnessing to a real phenomenon the growing of social networks. These networks are developed to reach millions of users around the world, where we can create a personal space or to share with our friends - real or virtual - our days, our photos, our interests, but also discuss, play with them or meet new people such as Facebook, Twitter, Twitter, Google+, LinkedIn and MySpace. However, social networks existed long before the Internet around us in workplace and in families, and social groups. Generally, a social network is in fact nothing more than a group of people or organizations interconnected by social interaction they maintain. Today, 72% of companies surveyed now believe that social networks are a threat to their security. According to the reports of international security companies, social networks have become a new playground for malicious attacks, reaching a level considered worrisome in 2013. Internet users spend more time on social networks, communicating sensitive personal information in some cases valuable, and hackers have struck a rich vein. In addition, the social networking service quickly spread to mobile platforms where people wear their multimedia content in powerful personal devices, such as laptops, Smartphone, PDA and want to share with their friends or find people who similar interests. Social networking on mobile equipment can be classified into two categories depending on the architecture: with infrastructure and without infrastructure. In this thesis, we focus on social networks in an environment without infrastructure, i.e., ad hoc networks.

The recent rise and widespread adoption of wireless networked embedded systems for mobile communication applications has sparked numerous visions of an ever more networked and interactive world. One such vision proposed in the past years is wireless ad hoc network (MANET), where it is formed by a set of hosts that are organized only and totally decentralized thus forming an autonomous and dynamic network without infrastructure. These hosts may be fixed or mobile. The applications of these networks are numerous and mainly areas where wired infrastructure is unavailable or undesirable. This is, for example, the case in areas devastated by natural disaster where relief has a great need for communication. The design of communication protocols for ad hoc networks is mainly governed by three factors: the limited energy, decision-making autonomy, and dynamic topology. In recent years, much research has been done on examining the unique features of MANET to addressing problems of security and privacy in MANETs, but few of them have taken the social characteristics of MANET into consideration. In MANETs, the nodes are usually trained in an urban environment, so we can imagine that the mobility of nodes directly reflects the social preferences of drivers and daily tasks, for example, where they usually go shopping or working. Because to these human factors in MANETs, not only related to security applications, but also non-security related applications will have social features.

In this thesis, we focus on the social characteristics of ad hoc networks and introduce the concept of mobile social network applications where both security and non-security related MANETs are influenced by human factors. In particular, we draw on the research of ad hoc social networks and address the challenging security and privacy issues related to them. The main contributions are, i) to compare with our work, we examine the five security and confidentiality protocols recently proposed for vehicular social networks, i.e., SPRING, SPF, PCS, FLIP and Pi. For each protocol, we present the network model, threat model, and design goals. Then, we present the protocol operation followed by the security analysis; ii) To address both security and performance challenges in ad hoc social, we propose an Efficient Conditional Privacy preservation scheme with Demand Response, called ECPDR, for ad hoc social communications. With the proposed EPCDR scheme, each node user can be privacy-preserving authenticated before joining other nodes using routing protocol. We improve the AODV routing protocol basing on some concepts of social theory to be suitable for ad hoc social communications, i.e., degree centrality, closeness centrality, and betweenness centrality. To validate the efficiency and effectiveness of the proposed ECPDR, we integrate in the AODV implementation, being the modified protocol designated AODV-ECPDR. Extensive simulation results in the first scenario show that the proposed ECPDR scheme can detect the black hole attack more in the configuration where attack is launched on a number of more hops. Thus, in the second scenario, we focus on the transmission delay of ECPDR at the node with extensive performance evaluation, which further convinces its practicality; iii) To address both security and privacy challenges in mobile P2P social network (MP2PSN), we propose an intelligent Secure Detection scheme with strong Privacy-Preserving, called SDPP, which allows a user to securely share his information's with ones who have the same similar interests in MP2PSN. To guarantee the security of MP2PSN, we propose an efficient certificate framework, where the trusted authority begins to initialize the system. Then, for the node Nui, the mobile proxy issues the private key and the certificate. The node Nui can verify the certificate and can also re-signs the certificate using the proxy re-signature cryptography technology. To detect the routing attacks, we propose an efficient cooperative neighbor neighbor (CNN) detection scheme, which is an intelligent secure detection based on two phases {response requested & demand response}. To achieve privacy-preserving of message, we propose employs the homomorphic encryption. We analyze the security properties of the proposed SDPP scheme to validate its security in the random oracle model and simulate in two different scenarios. Extensive simulation results in the first scenario show that the proposed SDPP scheme can detect the black hole attack more in the configuration where attack is launched on a number of more hops and the average Detectreq reporting delay (DRD) of sociable users is obviously less than those of unsociable users. Thus, in the second scenario, we focus on the transmission delay of SDPP at the mobile proxy with extensive performance evaluation, which further convinces its practicality.

The research results of the thesis should be useful to the implementation of secure and privacy-preserving mobile social networks.

Résumé

Depuis quelques années sur Internet nous assistons à un véritable phénomène grandissant des réseaux sociaux. Ces réseaux se sont développé pour toucher des millions d'internautes à travers le monde, où sur lesquels nous pouvons, créer un espace personnel ou partager avec nos amis - réels ou virtuels - notre quotidien, nos photos, nos centres d'intérêt, mais aussi discuter, jouer avec eux ou faire de nouvelles rencontres tels que Facebook, Twitter, Skyrock, Google+, LinkedIn et MySpace. Cependant, les réseaux sociaux existaient bien avant Internet autour de nous au lieu de travail ainsi que dans les familles et les groupes sociaux. En règle générale, un réseau social n'est en effet rien d'autre qu'un groupe de personnes ou d'organisations reliées entre elles par les échanges sociaux qu'elles entretiennent. Aujourd'hui, 72% des entreprises sondées jugent maintenant que les réseaux sociaux constituent pour elles une menace de sécurité. Selon les rapports des sociétés internationales de sécurité, les réseaux sociaux sont devenus un nouveau terrain de jeu pour les attaques malveillantes, atteignant un niveau jugé inquiétant en 2013. Les internautes passent plus de temps sur les réseaux sociaux, en communiquant des informations personnelles sensibles dans certains cas précieuses, et les pirates ont trouvé le filon. En outre, le service de réseautage social se propager rapidement aux plates-formes mobiles où les gens portent leur contenu multimédia dans des dispositifs personnels puissants, tels que les ordinateurs portables, Smartphone, PDA et veulent partager avec leurs amis ou trouver des gens qui ont des intérêts similaires. Le réseautage social sur l'équipement mobile peut être classé en deux catégories en fonction de l'architecture: avec une infrastructure et sans infrastructure. Dans cette thèse, nous nous intéressons à des réseaux sociaux dans un environnement sans infrastructure, i.e., les réseaux ad hoc.

La hausse récente et l'adoption généralisée des systèmes embarqués en réseau sans fil pour les applications de communication mobile ont suscité de nombreuses visions d'un monde de plus en plus en réseau et en interactive. Une telle vision proposée dans les dernières années est le réseau sans fil ad hoc (MANET), où il est formé par un ensemble d'hôtes qui s'organisent seuls et de manière totalement décentralisée, formant ainsi un réseau autonome et dynamique ne reposant sur aucune infrastructure filaire. Ces hôtes peuvent être fixes ou mobiles. Les applications de ces réseaux sont multiples, et concernent principalement les zones où une infrastructure filaire est indisponible ou non désirable. C'est par exemple, le cas dans les zones sinistrées par un désastre naturel, où les secours ont un grand besoin de communication. La conception de protocoles de communication pour les réseaux ad hoc est principalement soumise à trois facteurs : l'énergie limitée, l'autonomie de décision, et la topologie dynamique. Au cours de ces dernières années, beaucoup de recherches ont été effectuées sur l'examen des caractéristiques uniques du MA-

NET en abordant certains problèmes de sécurité et de confidentialité dans MANETs, mais peu d'entre elles ont pris les caractéristiques sociales des MANET en considération. Dans les MANETs, les nœuds sont généralement entraînés dans un environnement urbain, et donc nous pouvons imaginer que la mobilité des nœuds reflète directement les préférences sociales des conducteurs et les tâches quotidiennes, par exemple, les endroits où ils vont habituellement faire du shopping ou de travail. En raison de ces facteurs humains dans MANETs, non seulement les applications liées à la sécurité, mais aussi les applications non liées à la sécurité auront des caractéristiques sociales.

Dans cette thèse, nous intéressons sur les caractéristiques sociales des réseaux ad hoc MANET et introduisons le concept du réseau social mobile, où les applications à la fois de sécurité et de non-sécurité liés aux MANETs sont influencées par des facteurs humains. En particulier, nous portons sur la recherche des réseaux ad hoc sociaux, et abordons les questions de sécurité et de confidentialités difficiles qui leur sont liées. Les principales contributions sont, i) Pour comparer avec nos travaux, nous examinons les cinq protocoles de sécurité et confidentialité récemment proposés pour les réseaux sociaux véhiculaires, i.e., SPRING, SPF, PCS, FLIP et Pi. Pour chaque protocole, nous présentons le modèle du réseau, du nœud, de menace, et les objectifs de conception. Ensuite, nous présentons le fonctionnement du protocole, suivi par l'analyse de sécurité ; ii) pour faire face à des défis en matière de sécurité et de performance dans les réseaux sociaux mobiles, nous introduisons un schéma efficace préservant la confidentialité conditionnelle avec la stratégie d'une réponse à la demande, appelé ECPDR. Avec ce schéma ECPDR proposé, chaque nœud utilisateur peut préserver la vie privée et être authentifié avant de rejoindre les autres nœuds en utilisant le protocole de routage. Pour valider l'efficacité de la proposition ECPDR, nous l'intégrerons dans l'implémentation du protocole de routage AODV. Les résultats des simulations approfondies dans le premier scénario du schéma ECPDR proposé peut détecter l'attaque du trou noir de plus dans la configuration où l'attaque est lancée sur un nombre de plus de saut. Ainsi, dans le second scénario, nous nous concentrons sur le délai de transmission du schéma ECPDR au niveau du nœud avec une vaste évaluation de la performance, qui convient davantage à sa pratique ; iii) Pour sécuriser le type de réseau social mobile « P2P » qui est actuellement utilisé, sur Internet, à la fois pour la vidéo sur demande et les services de streaming en temps réel comme l'IPTV tels que UUSee, SopCas, TVants et Joost, nous introduisons un schéma de détection intelligent et sûr avec avec la forte préservation de la confidentialité, appelé SDPP, qui permet à un utilisateur de partager en toute sécurité des informations avec ceux qui ont les mêmes intérêts similaires MP2PSN. Pour garantir la sécurité du MP2PSN, nous proposons un cadre de certification efficace utilisant la technologie de cryptographie re-signature proxy. Puis, afin de détecter les attaques de routage, nous proposons un système de détection coopératif efficace voisin × voisin (cooperative neighbor × neighbor (CNN)), qui est une détection intelligente et sûre basée sur deux phases {réponse demandée et réponse à la demande} et pour atteindre la confidentialité du message, nous utilisons le chiffrement homomorphique. Les résultats de simulation étendus dans le premier scénario montrent que le schéma SDPP proposé peut détecter l'attaque du trou noir plus dans la configuration où l'attaque est lancée sur un cer-

tain nombre de plus de saut et le délai moyen de rapport du Detectreq (DRD) des utilisateurs sociables est évidemment moins que ceux utilisateurs qui ne sont pas sociables. Ainsi, dans le deuxième scénario, nous nous concentrons sur le délai de transmission du SDPP au proxy mobile avec une évaluation approfondie de la performance, qui convient en outre à son aspect pratique.

Les résultats de la recherche de la thèse devraient être utiles pour l'implémentation de la sécurité et la confidentialité des réseaux sociaux mobiles.

Table des matières

Dédicace i
Remerciement ii
الملخص iii
Abstract iv
Résumé vi
Liste des figures xiii
Liste des algorithmes xv
Liste des tableaux xvi
Chapitre 1 Introduction 1
1.1 Les réseaux mobiles MANETs 1
1.1.1 Caractéristiques et applications 2
1.1.2 Menaces de sécurité 2
1.1.3 Besoins de sécurité 3
1.2 Les réseaux ad hoc sociaux mobiles 4
1.2.1 Motivations et objectifs 4
1.2.2 Contributions de la thèse 6
1.2.3 Structure du document 7
Chapitre 2 Etat de l'art : Le routage, la théorie sociale, la cryptographie et les travaux de recherche connexes 9
2.1 Le routage dans les réseaux ad hoc 9
2.2 Classification des protocoles de routage 10
2.2.1 Proactif 11
2.2.2 Réactif 13
2.2.3 Hybride 15
2.3 Les concepts de base de la théorie sociale 17

2.4 La cryptographie 19
2.4.1 Rappels de mathématiques pour la cryptographie 19
2.4.2 Outils cryptographiques 23
2.5 Travaux de recherche connexes 33
2.6 Conclusions 34
Chapitre 3 Les protocoles SPRING, SPF, PCS, FLIP et Pi pour la sécurisation et la confidentialité des communications véhiculaires ad hoc sociaux 35
3.1 Le protocole SPRING 36
3.1.1 Modèles et objectifs de conception 37
3.1.2 Fonctionnement du protocole SPRING 40
3.1.3 Analyse du protocole SPRING 42
3.2 Le protocole SPF 44
3.2.1 Modèles et objectifs de conception 45
3.2.2 Fonctionnement du protocole SPF 46
3.2.3 L'analyse du protocole SPF 50
3.3 Le protocole PCS 51
3.3.1 Modèles et objectifs de conception 53
3.3.2 Fonctionnement du protocole PCS pour la confidentialité de l'emplacement 55
3.3.3 Performances du protocole SPF 64
3.4 Le protocole FLIP 64
3.4.1 Modèles et objectifs de conception 65
3.4.2 Fonctionnement du protocole FLIP 67
3.4.3 L'analyse du protocole 69
3.5 Le protocole Pi 69
3.5.1 Modèles et objectifs de conception 70
3.5.2 Fonctionnement du protocole Pi 73
3.5.3 L'analyse du protocole 76
3.6 Conclusions 76
Chapitre 4 ECPDR: La stratégie d'une réponse à la demande pour la sécurisation et la confidentialité des réseaux sociaux mobiles 77
4.1 Introduction 77
4.2 Modèle du système et objectifs de la recherche 79

4.2.1 Le modèle du système 79
4.2.2 Les objectifs de la recherche 80
4.3 Préliminaires 81
4.3.1 Les chaînes de hachages sécurisées 81
4.3.2 La technique de couplage bilinéaire 81
4.3.3 La technique de signature courte 83
4.4 Notre schéma ECPDR proposé 83
4.4.1 L'initialisation du système 83
4.4.2 Le pseudo identité, la clé privée et le certificat délivré par le TA 84
4.4.3 L'update du certificat 84
4.4.4 La signature et la vérification des messages 86
4.4.5 La réponse demandée 86
4.4.6 La réponse à la demande 89
4.5 Analyse de la sécurité 90
4.5.1 Les oracles 90
4.5.2 La confidentialité du contenu orienté 90
4.5.3 La confidentialité conditionnelle du certificat 93
4.5.4 La robustesse 93
4.6 Evaluation des performances 93
4.7 Comparaison avec autres protocoles de sécurisation 100
4.8 Conclusions 102
Chapitre 5 SDPP : Un schéma de détection intelligent avec la forte préservation de la confidentialité pour la sécurisation des réseaux sociaux P2P 103
5.1 Introduction 103
5.2 Modèles du système et objectifs de la recherche 105
5.2.1 Le modèle du système MP2PN 105
5.2.2 Le modèle de routage 106
5.2.3 Le modèle de menace 107
5.2.4 Les objectifs de recherche 107
5.3 Préliminaires 108
5.3.1 Les chaines de hachage 108
5.3.2 Le chiffrement homomorphique 108

5.3.3 Le couplage bilinéaire 108
5.3.4 La signature basée sur l'identité 108
5.4 Notre schéma SDPP pour le réseau social peer-to-peer mobile 109
5.4.1 L'initialisation du système 109
5.4.2 Les certificats délivrés par le MP 110
5.4.3 La détection d'attaques 110
5.4.4 L'évolution du certificat 111
5.5 L'analyse de sécurité 114
5.5.1 La sécurité sémantique 115
5.5.2 Le SDPP fournit la forte préservation de la confidentialité du message 116
5.5.3 Le SDPP fournit l'évolution des certificats des utilisateurs 117
5.6 Evaluation des performances 117
5.7 Comparaison avec autres protocoles de sécurisation 126
5.8 Conclusions 127
Chapitre 6 Conclusions et travaux futurs 128
6.1 Nos contributions 128
6.2 Nos travaux futurs de recherche 129
6.3 Remarques finales 130
Références 131
Annexe A1. Liste des publications 136
Annexe A.2.Glossaire 138

Liste des figures

Figure 1:1 Mobile Ad hoc Social Network [J2] 5
Figure 2:1 Le chemin utilisé dans le routage entre la source et la destination 10
Figure 2:2 Classification des familles de protocoles ad hoc 11
Figure 2:3 Avantage de l'utilisation des MPR 13
Figure 2:4 Exemple d'établissement de route entre 1 et 5 15
Figure 2:5 Zone de routage de rayon=2 du nœud 2 et 10 16
Figure 2:6 Le degré, la proximité, et betweenness centralités dans les réseaux sociaux [20] .. 18
Figure 2:7 La relation entre les propriétés de la fonction de hachage [33] 24
Figure 2:8 Les principes de base d'utilisation de MAC 28
Figure 2:9 La structure de HMAC 30
Figure 2:10 Signature numérique 31
Figure 3:1 Vehicular Ad hoc Network (VANET) [20] 35
Figure 3:2 La relation entre VANET et MANET [20] 36
Figure 3:3 Modèle de véhicule DTN avec le déploiement RSU sociale, proposé par Ru *et al.* [20] 37
Figure 3:4 Le modèle du système sous considération pour SPF, proposé par Ru *et al.* [64] .. 45
Figure 3:5 La technique socialspot pour améliorer le rendement de la transmission de paquets, proposé par Ru *et al.* [64] 46
Figure 3:6 Le format de paquet dans le protocole SPF, proposé par Ru *et al.* [64] 48
Figure 3:7 L'établissement d'un canal sécurisé entre Vi et un RSU de confiance, proposé par Ru *et al.* [64] 49
Figure 3:8 Le lien pseudonyme en raison de l'évolution des pseudonymes à l'occasion incorrect, proposé par Ru *et al.* [65] 52
Figure 3:9 Les points sociales, l'intersection de la route et un parking gratuit 54
Figure 3:10 Le modèle KPSD pratique pour la confidentialité de l'emplacement dans les VANETs, proposé par Ru et al. [65] 56
Figure 3:11 Le changement de pseudonyme à une intersection, proposé par Ru et al. [65] ... 59
Figure 3:12 Le changement de pseudonyme dans un parking gratuit, proposé par Ru et al. [65] 60
Figure 3:13 Le diagramme de temps, proposé par Ru et al. [65] 61
Figure 3:14 Le modèle du système sous considération pour FLIP, proposé par Ru *et al.* [66] 65
Figure 3:15 Le protocole de préservation de la confidentialité d'intérêt, proposé par Ru et al. [66] 68
Figure 3:16 Un exemple de l'architecture de la pièce en couches, proposé par Ru et al. [67] 73
Figure 3:17 Un routage opportuniste, proposé par Ru et al. [67] 74
Figure 4:1 Le modèle du système ADSocial 79

Figure 4:2 ADSocial sous consideration $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ 80
Figure 4:3 L'organigramme de la mise à jour du certificat 85
Figure 4:4 Réponse demandée et réponse à la demande 88
Figure 4:5 . Taux de détection de liaison de trou noir pour les différentes tailles de réseau .. 94
Figure 4:6 Précision de détection de la liaison d'un trou noir pour les différentes tailles de réseau 94
Figure 4:7 Le délai moyen de transmission tr variant avec le taux moyen d'arrivé λ, où 1 ≤ λ ≤ 100 98
Figure 4:8 Le délai moyen de transmission tr variant avec p et n, où 1% ≤ p ≤ 80% et 1 ≤ n ≤100 99
Figure 5:1 Le modèle du système MP2PSN 105
Figure 5:2 Le mécanisme de détection basé sur la coopération CNN 111
Figure 5:3 La probabilité de k voisins d'un adversaire Pk. neigh. adversary avec $\mathrm{S} = 200 \times 200\ \mathrm{m2}$, $\mathrm{R} = 5\mathrm{m}, 10\mathrm{m}, 15\mathrm{m}, 20\mathrm{m}$, $\mathcal{V} = 100$, et $1 \leq \mathrm{k} \leq 20$ 118
Figure 5:4 Le taux de détection d trou noir Dr variant avec la longueur du tunnel. 119
Figure 5:5 Le taux de détection de trou noir Dr variant selon l'intervalle d'émission HELLO THello (s) et les différentes durées de l'attaque du trou noir 120
Figure 5:6 Le taux moyen du DRD pour les différents rapports sociaux dans 100 min 121
Figure 5:7 Le délai moyen de transmission tr variant avec le taux moyen d'arrivée λ, où 1 ≤ λ ≤ 100 124
Figure 5:8 Le délai moyen de transmission tr variant avec p et n, où 1% ≤ p ≤ 80% et 1 ≤ n ≤100 125

Liste des algorithmes

Algorithme 3:1 Transmission des paquets dans les véhicules DTN [20] 42
Algorithme 3:2 La détection des attaques du trou noir (grey) [20] 43
Algorithme 3:3 L'algorithme d'enregistrement du véhicule, proposé par Ru *et al.* [64] 47
Algorithme 3:4 L'algorithme de transfert du paquet, proposé par Ru *et al.* [64] 48
Algorithme 3:5 Changement de pseudonyme à la stratégie des points sociales, proposé par Ru *et al.* [65] 59
Algorithme 3:6 L'algorithme d'enregistrement du véhicule dans FLIP, proposé par Ru *et al.* [66] 67
Algorithme 3:7 L'algorithme de transfert du paquet dans Pi, proposé par Ru *et al.* [67] 75
Algorithme 3:8 L'algorithme de dégagement du crédit et réputation dans Pi, proposé par Ru *et al.* [67] 75
Algorithme 4:1 Demande pour détection 87
Algorithme 4:2 Notification des attaques 88
Algorithme 4:3 La réponse à la demande de détection d'attaque 89
Algorithme 5:1 Demande de détection dans SDPP 112
Algorithme 5:2 Vérfication des demandes dans SDPP 113
Algorithme 5:3 La réponse de la détection d'attaque demandée dans SDPP 113
Algorithme 5:4 Notification des attaques dans SDPP 114
Algorithme 5:5 L'information collaborative basée sur le réseau social dans SDPP 114

Liste des tableaux

Tableau 2:1 La comparaison des paramètres du SHA 26
Tableau 4:1 Les notations utilisées dans ECPDR 82
Tableau 4:2 Le format du message signé « Detectreq » 84
Tableau 4:3 Le coût des opérations nécessaires 95
Tableau 4:4 Le coût des opérations nécessaires dans ECPDR 96
Tableau 4:5 La comparaison de notre schéma ECPDR avec les autres schémas 101
Tableau 5:1 Format du message signéDetectreq, Detectrep 109
Tableau 5:2 Le coût en temps des opérations nécessaires 122
Tableau 5:3 Le coût en temps des opérations nécessaires dans SDPP 122
Tableau 5:4 La comparaison de notre schéma SDPP avec d'autres schémas 126

Chapitre 1 Introduction

Après le déploiement réussi de la connexion Wi-Fi et les réseaux cellulaires dans la dernière décennie, les systèmes sans fil et mobiles de communication sont devenus le secteur le plus dynamique de l'industrie de la communication où il existe différents réseaux basés sur la zone de couverture : Le réseau personnel sans fil[1] (ou Wireless Personal Area Network, WPAN), le réseau local sans fil[2] (ou Wireless Local Area Network, WLAN), le réseau métropolitain sans fil[3] (ou Wireless Metropolitan Area Network, WMAN) et les réseaux étendus sans fil[4] (ou Wireless Wide Area Network, WWAN). La vision d'être connecté partout et à tout moment n'est plus seulement une idée, elle est devenue une réalité en raison de la combinaison d'appareils mobiles avec les technologies de communication sans fil. Presque toutes les entreprises qui s'appuient sur les réseaux sans fil et mobiles attendent la même chose ou un niveau de sécurité, de confidentialité et de confiance similaire à celles qui existent dans les réseaux câblés pour assurer l'intégrité et la confidentialité des communications entre les terminaux, les réseaux, les applications et les services [B1].

Il existe une autre famille de réseaux sans fils, apportant davantage de flexibilité, de facilité de construction et de déplacement, et qui se différencie de tous les réseaux par l'absence de toute infrastructure fixe préexistante. Ces réseaux sont formés d'un ensemble de nœuds mobiles interconnectés par des liaisons sans fil. Leurs architectures évoluent au gré de l'apparition et du mouvement des nœuds. Ils sont appelés réseaux spontanés ou réseaux ad hoc. Les environnements adaptés à leur utilisation sont donc caractérisés par l'absence (ou la détérioration) d'infrastructure de réseaux préexistante, telles les opérations de secours après un sinistre, les missions d'exploration ou les applications militaires [B1] [B2] [B3].

1.1 Les réseaux mobiles MANETs

Un réseau ad hoc est un système autonome constitué de nœuds mobiles. Ces derniers communiquent avec leur voisin par des liaisons sans fil point à point. Quand les zones d'émission/réception de deux nœuds en communication sont disjointes, les nœuds intermédiaires sont alors sollicités pour assurer le routage. A travers cette définition, nous allons pré-

[1] Le WPAN généralement mis en œuvre dans un espace d'une dizaine de mètres, i.e., réseau domestique ou réseau individuel.
[2] Le WLAN est un réseau permettant de couvrir l'équivalent d'un réseau local d'entreprise, soit une portée d'environ une centaine de mètres.
[3] Les WMAN sont basés sur la norme IEEE 802.16, et offrent un débit utile de 1 à 10 Mbit/s pour une portée de 4 à 10 kilomètres. Ce type de connexion est principalement destiné aux opérateurs de télécommunication.
[4] Les WWAN sont connus sous le nom de réseaux cellulaires mobile. Il s'agit des réseaux sans fil les plus répandus puisque tous les téléphones mobiles sont connectés à un réseau étendu sans fil. Comme le réseau GSM et 3G.

ciser et définir les caractéristiques, les applications, les menaces et les besoins de sécurité dans les réseaux MANETs.

1.1.1 Caractéristiques et applications

Les caractéristiques principales qui différencient un réseau ad hoc d'un réseau doté d'une architecture fixe, ci-après [4] [5] [7] [8] [20] [B1] [B2] [B3]:

- *La mobilité de tous les nœuds* est une caractéristique intrinsèque des MANET. Le déplacement des nœuds provoque des modifications aléatoires et non prédictibles de l'architecture du réseau. De ce fait, les techniques de routage des réseaux classiques, basées sur des routes préétablies par des équipements spécialisés et dédiés, ne peuvent plus fonctionner correctement. Par exemple dans l'application VANET, la vitesse des véhicules dans les villes varie de 0 à 60 km / h, et la vitesse moyenne peut atteindre jusqu'à 100 km / h sur une autoroute.
- *Les ressources énergétiques des nœuds mobiles* alimentés par des sources d'énergies autonomes (batteries) sont limitées.
- *Les liaisons physiques* s'appuient sur les technologies de communications sans fil, indispensable à la mise en place d'un réseau ad hoc.
- *L'absence de serveur centralisé* rend complexe le contrôle et la gestion d'une architecture qui se forme et évolue au gré de l'apparition et des déplacements des nœuds.
- *L'équivalence des nœuds* est une spécificité des MANET. Dans un réseau classique, il existe une distinction nette entre les nœuds terminaux (stations, hôtes) qui supportent les applications et les nœuds internes du réseau (routeurs), chargés de l'acheminement des données. Cette différence n'existe pas dans les réseaux ad hoc, car tous les nœuds peuvent être amenés à assurer des fonctions de routage.
- *Le nombre de nœuds mobiles* présents dans un MANET varie selon les besoins ou la position de chaque nœud. D'une façon plus générale aucune limitation n'est faite sur la taille ou le nombre de nœuds d'un réseau ad hoc.

Les MANETs (Mobile Ad-hoc NETworks) sont utiles dans de nombreux environnements (catastrophe naturelle, communication en combat, réseau de capteurs) et n'ont nul besoin d'infrastructure. Aussi, les communications dans les régions plus restreintes peuvent être mise en place grâce aux MANETs.

1.1.2 Menaces de sécurité

Les réseaux ad hoc tel que conçus manquent de contrôles de sécurité, ce qui augmente le risque d'attaques qui peuvent être orchestrées par des nœuds externes ou internes en tenant compte du positionnement du nœud malhonnête par rapport au réseau [7] [J1] [C2] [C3] [B1] [B2] [B3].

- Les attaquants externes sont des nœuds qui ne font pas partie du réseau.
- Les attaquants internes sont des nœuds faisant légitimement partie du réseau.

Quelque soit sa position (interne ou externe), le nœud malhonnête utilise plusieurs techniques pour perturber le bon fonctionnement du réseau, i.e., le protocole de routage. La combinaison de ces techniques peut aboutir à une attaque plus élaborée. Ces techniques sont présentées ci-après:

- *Rejeu de messages :* l'attaquant enregistre une séquence de trafic qu'il réinjecte ensuite dans le réseau.
- *Modification de messages* : l'attaquant modifie un ou plusieurs champs du message avant de le retransmettre.
- *Suppression de messages* : l'attaquant supprime des messages.
- *Fabrication de messages* : l'attaquant fabrique un message et l'injecte dans le réseau.

Nous présentons dans ce qui suit trois types d'attaques dans les réseaux ad hoc proposées dans [7]. Lors de ces attaques, les attaquants se basent sur une ou plusieurs techniques.

Attaques contre la confidentialité. L'action de l'attaquant peut se résumer à écouter ou surveiller les transmissions. Le but est d'obtenir les informations qui transitent soit directement, soit après une analyse. Ce type de comportement est très difficile à détecter puisque l'attaquant n'altère pas les messages échangés et ne participe pas en envoyant des messages supplémentaires. Par exemple, l'attaque par privation de sommeil (sleep deprivation torture).

Attaques contre la disponibilité. Les attaquants peuvent s'attaquer à la disponibilité des nœuds. Cette technique consiste à consommer leurs ressources en sollicitant de manière continue le nœud cible (en fabriquant des messages inutiles à destination de la cible ou en modifiant des paquets pour que les messages passent par la cible) ce qui provoque des traitements supplémentaires. Par exemple, l'attaque par consommation des ressources (resource consumption attack), et l'attaque par privation de sommeil (sleep deprivation torture).

Attaques contre l'intégrité. En s'attaquant à l'intégrité des messages, un attaquant fausse la table de routage. Son action repose sur des actions élémentaires. Par exemple, l'attaque du trou de ver (wormhole attack), l'attaque par pollution de la table de routage (routing table poisoning), et l'attaque par détour (detour attack).

1.1.3 Besoins de sécurité

Afin de protéger les MANET contre les menaces mentionnées ci-dessus, les mécanismes de sécurité utilisés dans les MANET doivent satisfaire aux besoins de sécurités suivantes [20] :

- *Authentification*: L'authentification est la capacité de déterminer qu'une chose est bien celle qu'elle prétend être. L'authentification des messages est d'une importance vitale dans MANETs car elle garantit que le message reçu est en effet envoyé à partir d'un nœud légitime et autorisé dans les réseaux.
- *Intégrité*: L'intégrité est la capacité d'assurer que les messages échangés entre les nœuds n'ont pas fait l'objet de modifications, ajouts ou suppressions.
- *Non-répudiation*: La non-répudiation est la capacité d'empêcher un nœud autorisé de nier l'existence ou le contenu du message envoyé par lui-même.

- *Contrôle d'accès*: le contrôle d'accès est nécessaire pour assurer les opérations fiables et sécurisées.
- *Confidentialité:* La confidentialité est la capacité de protéger les renseignements personnels d'un tiers non autorisé. Par exemple dans les VANETs qui est un type de réseau MANET, l'identité réelle d'un véhicule individuel est seulement aveugle à d'autres véhicules et les unités de bord de route, mais doit être transparent pour une autorité de confiance (TA). Cette exigence de sécurité est aussi appelée «la préservation de la confidentialité conditionnelle»

1.2 Les réseaux ad hoc sociaux mobiles

1.2.1 Motivations et objectifs

Aujourd'hui, tout le monde sur Internet connaît le mot "réseau social". Les réseaux sociaux se sont adaptés au monde de l'entreprise mieux que quiconque aurait pu imaginer. Le réseautage social a commencé une fois dans l'espace en ligne tels que Facebook, Myspace, Youtube, Flickr avec des centaines de millions d'utilisateurs [20]. Bien que le réseautage social est un mot populaire dans Internet, les réseaux sociaux sont partout autour de nous au lieu de travail ainsi que dans les familles et les groupes sociaux, où les utilisateurs peuvent changer les jeux, rumeurs, et trouver des gens qui ont des intérêts semblables en utilisant leurs appareils mobiles à courte portée avec des interfaces sans fil formant un réseau ad hoc social. En outre, le service de réseautage social se propager rapidement aux plates-formes mobiles où les gens portent leur contenu multimédia dans des dispositifs personnels puissants, tels que les ordinateurs portables, Smartphone, PDA et veulent partager avec leurs amis ou trouver des gens qui ont des intérêts similaires. Le réseautage social sur l'équipement mobile peut être classé en deux catégories en fonction de l'architecture: avec une infrastructure et sans infrastructure. Dans cette thèse, nous nous intéressons à des réseaux sociaux dans un environnement sans infrastructure, i.e., les réseaux ad hoc. Dans les réseaux ad hoc, les nœuds sont généralement dictés par les citoyens dans un environnement urbain ou bien par des soldats dans un environnement militaire. Donc, nous pouvons imaginer que la mobilité des nœuds reflète directement les intentions des gens. Alors, puisque les intentions des gens (facteurs humains) sont impliquées dans les réseaux ad hoc, non seulement les applications liées à la sécurité, mais aussi les applications non liées à la sécurité montreront quelques caractéristiques sociales. En conséquence, nous sommes motivés pour étudier les caractéristiques sociales et leurs impacts sur les réseaux ad hoc, i.e., MANET, VANET, et P2P.

Quelle est la question des réseaux ad hoc sociaux ?

Le réseau ad hoc social est un réseau ad hoc qui prend les «facteurs humains» en considération, comme le montre la figure 1.1. Pour illustrer le concept des réseaux ad hoc sociaux clairement, nous considérons les aspects suivants [20] :

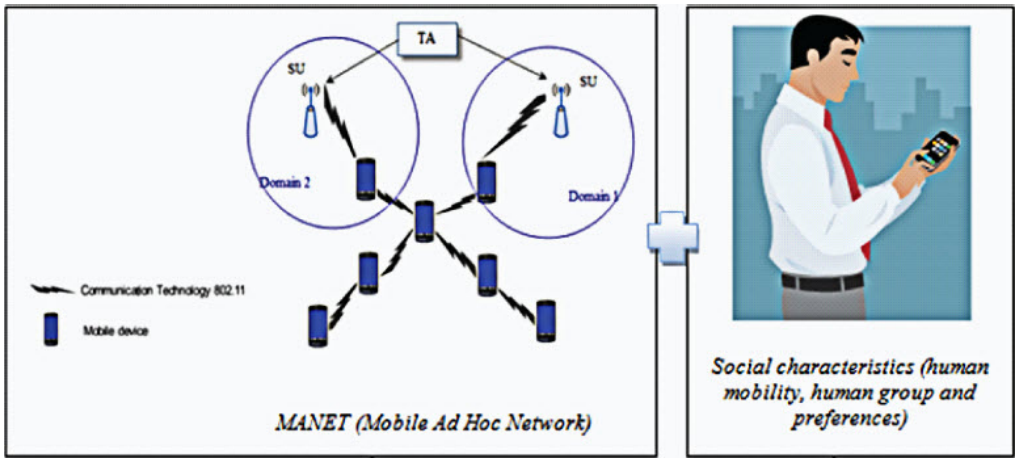


Figure 1:1 Mobile Ad hoc Social Network [J2]

- *Le modèle de mobilité humain*: Dans les réseaux sociaux mobiles, les nœuds sont conduits par des personnes. Donc, le modèle de mobilité n'est plus un point de cheminement aléatoire. Au lieu de cela, certains modèles de mobilité humaine réalistes dans un environnement urbain peuvent être adoptés, i.e., le mouvement du plus court chemin basé sur une carte, le modèle de mobilité basé sur une communauté, et le modèle de mobilité variant dans le temps.
- *Le statut humain égoïste*: Dans les réseaux sociaux mobiles, les nœuds sont entraînés et commandés par des entités rationnelles - des êtres humains. Comme tous les gens dans la réalité sont non-égoïstes, certains nœuds se comportent égoïstement et peuvent ne pas être disposés à participer dans des applications non liées à la sécurité. Par exemple, afin de préserver les ressources de tampons et de l'informatique, un nœud égoïste peut être réticent à la coopération qui n'est pas directement bénéfique pour lui, ce qui pourrait rendre un protocole de routage bien conçu dans MANET inutile. Par conséquent, l'égoïsme est une question très difficile pour des applications non liées à la sécurité dans les réseaux sociaux mobiles.
- *Les préférences humaines*: Dans les réseaux sociaux mobiles, un grand nombre de nœuds conduits par des personnes se déplacent entre la maison et le bureau pour une heure ou plus chaque jour. Ces trajets prennent généralement les personnes sur les routes et d'autres corridors fréquentés, ils sont très prévisibles et réguliers. Jour après jour, les mêmes personnes empruntent les mêmes routes en même temps. Ensuite, en fonction de leurs préférences, ils pourraient former des communautés virtuelles pour discuter de certains sujets intéressants.

D'une part, le routage est une fonction primordiale dans les réseaux ad hoc où chaque entité mobile joue le rôle d'un routeur et participe activement dans la transmission des paquets de données. D'autre part, depuis que les caractéristiques sociales (mobilité humaine, l'état égoïste, et les préférences) sont prises en compte dans les réseaux sociaux mobiles, l'étude de ces réseaux devient plus prometteuse et plus riche que celle du MANET pur. Par exemple, de nombreux protocoles sociaux basés sur le routage MANET et les applications non liées à la sécurité peuvent être développés dans les réseaux sociaux mobiles. Néanmoins, comme dans

les réseaux sociaux en lignes traditionnelles et MANET, les questions de sécurité et de confidentialité également élevées dans les réseaux sociaux, en particulier de la confidentialité.

Les vulnérabilités des réseaux sans fil sont par nature plus sensibles aux problèmes de sécurité. Pour les réseaux ad hoc, le principal problème ne se situe pas tant au niveau du support physique mais principalement dans le fait que tous les nœuds sont équivalents et potentiellement nécessaires au fonctionnement du réseau. Les possibilités de s'insérer dans le réseau sont plus grandes afin de divulguer la vie privée des personnes. En outre, dans le réseau social mobile, le modèle de mobilité humain peut être utilisé pour concevoir des protocoles de routage efficaces. Cependant, les protocoles de routage ad hoc tel que conçus manquent de contrôles de sécurité. Toutefois, s'ils sont mal traités, le modèle de mobilité pourrait divulguer l'emplacement de la vie privée des gens. Plus précisément, le favori des gens est évidemment une question de vie privée, parce que il n'est pas réaliste pour une personne de divulguer son / ses favoris à tout le monde sur un espace publique. Par conséquent, les exigences de sécurité, notamment l'authentification, l'intégrité, la non-répudiation, le contrôle d'accès et la confidentialité devraient être payés plus d'attention dans le réseau social mobile.

Dans cette thèse, nous allons étudier les applications qui se basent sur les facteurs humains dans les réseaux sociaux mobiles, et résoudre les problèmes difficiles de sécurité et de confidentialité.

1.2.2 Contributions de la thèse

La recherche dans cette thèse se concentre sur l'évaluation d'une suite de protocoles récemment proposés et le développement de deux protocoles pour faire face à la sécurité et la confidentialité dans les réseaux sociaux mobiles. Plus précisément, nos contributions se présentent comme suit :

- Premièrement, pour comparer les différents protocoles de sécurité récemment proposés avec nos deux schémas proposés pour les réseaux sociaux mobiles, nous examinons les cinq protocoles de sécurité et confidentialité pour les réseaux sociaux véhiculaires, i.e., SPRING [62], SPF [64], PCS [65], FLIP [66] et Pi [67]. Pour chaque protocole, nous présentons le modèle du réseau, du nœud, de menace, et les objectifs de conception. Ensuite, nous présentons le fonctionnement du protocole, suivi par l'analyse de sécurité.
- Deuxièmement, pour faire face à des défis en matière de sécurité et de performance dans les réseaux sociaux mobile, nous introduisons un schéma efficace préservant la confidentialité conditionnelle avec la stratégie d'une réponse à la demande, appelé ECPDR. Avec ce schéma ECPDR proposé, chaque nœud peut préserver la confidentialité et être authentifié avant de rejoindre les autres nœuds en utilisant le protocole de routage. Nous commençons avec la formalisation du modèle du système où nous considérons les caractéristiques sociales (la mobilité humaine, le groupe humain et les préférences) dans un réseau ad hoc qui se compose d'une autorité de confiance (TA), une certaine unité stationnaire sociale (SU) déployée à l'espace social, et un grand nombre de mobile équipé de la technologie sans fil en mouvement sur un espace so-

cial. Puis, nous proposons un schéma de certificat efficace, où le TA délivre la clé privée SK_{n_i} et le certificat $\mathrm{Cert}_{\mathrm{TA},n_i}$ utilisant l'algorithme de signature Schnorr. Le nœud n_i peut vérifier le certificat $\mathrm{Cert}_{\mathrm{TA},n_i}$ par la procédure $S.check$ et ne peut pas utiliser ce certificat directement dans la communication ad hoc sociale. Basé sur la technologie cryptographique proxy re-signature, le nœud demande la clé de re-signature depuis S_x et puis re-signe les certificats délivrés par le TA. Avec cette méthode de distribution des clés, le schéma garantie la confidentialité de l'identité du nœud. Après, nous fournissons la préservation conditionnelle de la vie privée pour les nœuds avec une réponse à la demande. Pour valider l'efficacité de la proposition ECPDR, nous l'intégrerons dans l'implémentation du protocole de routage AODV. Les résultats des simulations approfondies dans le premier scénario du schéma ECPDR proposé peut détecter l'attaque du trou noir de plus dans la configuration où l'attaque est lancée sur un nombre de plus de saut. Ainsi, dans le second scénario, nous nous concentrons sur le délai de transmission du schéma ECPDR au niveau du nœud avec une vaste évaluation de la performance, qui convient davantage à sa pratique.

- Troisièmement, pour sécuriser le type de réseau social mobile « P2P » qui est actuellement utilisé, sur Internet, à la fois pour la vidéo sur demande et les services de streaming en temps réel comme l'IPTV tels que UUSee, SopCas, TVants et Joost, nous introduisons un schéma de détection intelligent et sûr avec une forte préservation de la confidentialité, appelé SDPP, qui permet à un utilisateur de partager en toute sécurité des informations avec ceux qui ont les mêmes intérêts similaires MP2PSN. Nous commençons avec la définition d'un réseau P2P social mobile (MP2PSN), qui fournit une plateforme pour les utilisateurs qui ont les mêmes intérêts similaires pour agir à la fois comme fournisseurs et consommateurs de ressources. Pour garantir la sécurité du MP2PSN, nous proposons un cadre de certification efficace utilisant la technologie de cryptographie re-signature proxy. Puis, afin de détecter les attaques de routage, nous proposons un système de détection coopératif efficace voisin × voisin (cooperative neighbor × neighbor (CNN)), qui est une détection intelligente et sûre basée sur deux phases {réponse demandée et réponse à la demande} et pour atteindre la confidentialité du message, nous utilisons le chiffrement homomorphique. A la fin, nous analysons les propriétés de sécurité du schéma SDPP proposé pour valider sa sécurité dans le modèle de l'oracle aléatoire et simuler dans deux scénarios différents. Les résultats de simulation étendues dans le premier scénario montrent que le schéma SDPP proposé peut détecter l'attaque du trou noir plus dans la configuration où l'attaque est lancée sur un certain nombre de plus de saut et le délai moyen de rapport du Detectreq (DRD) des utilisateurs sociables est évidemment moins que ceux des utilisateurs qui ne sont pas sociables. Ainsi, dans le deuxième scénario, nous nous concentrons sur le délai de transmission du SDPP au proxy mobile avec une évaluation approfondie de la performance, qui convient en outre à son aspect pratique.

1.2.3 Structure du document

La suite de ce manuscrit est structurée en six chapitres. Après ce chapitre 1 introductif, le chapitre 2 rappelle les différentes notions de base, y compris le routage dans les réseaux ad

hoc, la théorie sociale, les outils cryptographiques et les travaux de recherche connexes. Le chapitre 3 présente l'évaluation de cinq protocoles pour la sécurité et la confidentialité des réseaux véhiculaires ad hoc sociaux, y compris SPRING, SPF, PCS, FLIP et Pi. Le chapitre 4 présente le schéma ECPDR pour la sécurisation des communications ad hoc sociales. Le chapitre 5 présente le schéma SDPP pour la sécurisation des réseaux P2P sociales. Enfin, les conclusions et les futurs travaux de recherche sont décrits dans le chapitre 6.

Chapitre 2 Etat de l'art : Le routage, la théorie sociale, la cryptographie et les travaux de recherche connexes

Dans ce chapitre, nous introduisons les différentes notions de base que nous avons étudié pour le besoin de cette thèse : le routage dans les réseaux ad hoc, la théorie sociale, les outils cryptographiques et les travaux de recherche connexes. Ceci nous permettra surtout de nous positionner par rapport à ces divers aspects faisant intervenir plusieurs domaines desquels nous nous sommes inspirés pour mener à bien nos travaux.

2.1 Le routage dans les réseaux ad hoc

Lors de la transmission d'un paquet de données d'une source vers une destination, il est nécessaire de faire appel à un protocole de routage qui acheminera correctement le paquet par le meilleur chemin.

Dans un réseau à architecture fixe, les routes vers les différents réseaux sont prédéfinies et maintenues par les équipements d'interconnexion fixes, appelés routeurs. L'architecture dynamique d'un réseau ad hoc, qui résulte du mouvement, de l'apparition des nœuds ou de l'état de la connexion physique, nécessite une mise à jour régulière des tables de routage situées dans chaque nœud. Pour acheminer un paquet entre deux nœuds mobiles d'un réseau ad hoc, le mécanisme de base est l'inondation. Celle-ci consiste à transmettre le paquet à l'ensemble des nœuds du réseau. L'inondation est réalisée par diffusions successives à l'ensemble des voisins de chaque nœud [15][B1].

Les protocoles de routage viseront, eux, à limiter la propagation des paquets par inondation. Selon le rôle joué par les nœuds dans la diffusion des messages, nous pouvons réaliser une première différenciation des protocoles de routage :

- ✓ Lorsque tous les nœuds ont des fonctionnalités identiques, le protocole est qualifié d'*uniforme*,
- ✓ Si certains nœuds ont des fonctionnalités particulières dans la diffusion des messages, le protocole dit *non uniforme*.

Nous limitons notre présentation aux protocoles de routage point à point, encore appelés protocoles de routage *unicast*.

Exemple [1] : Si on suppose que les coûts des liens sont identiques, le chemin indiqué dans la figure 2.1 est le chemin optimal reliant la station source et la station destination. Une bonne stratégie de routage utilise ce chemin dans le transfert des données entres les deux stations.

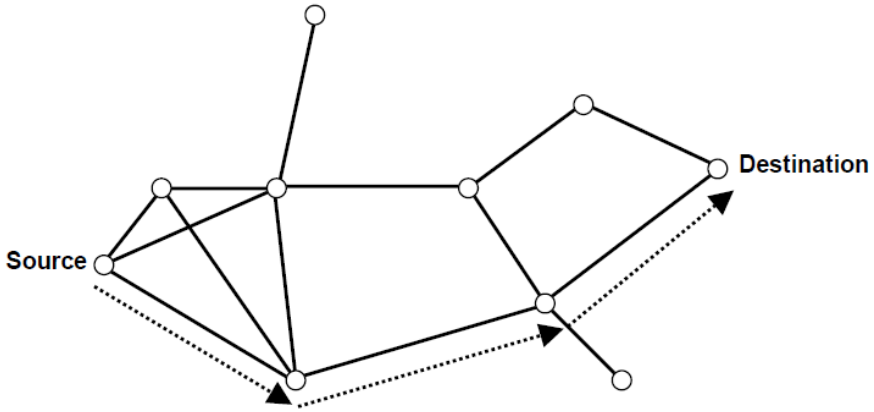


Figure 2:1 Le chemin utilisé dans le routage entre la source et la destination

Le problème qui se pose dans le contexte des réseaux ad hoc est l'adaptation de la méthode d'acheminement utilisée avec le grand nombre d'unités existant dans un environnement caractérisé par de modestes capacités de calcul et de sauvegarde et de changements rapides de topologies. Il semble donc important que toute conception de protocole de routage doit étudier les problèmes suivants :

- Minimiser la charge du réseau ;
- Offrir un support pour pouvoir effectuer des communications multipoints fiables ;
- Assurer un routage optimal ;
- Offrir une bonne qualité concernant le temps de latence.

2.2 Classification des protocoles de routage

Depuis leurs apparitions, les protocoles de routages dans les réseaux ad hoc sont classés en trois grandes familles: (a) les proactifs (b) les réactifs, et (c) les hybrides (Figure 2.2) [B1]. Dans ce qui suit, nous allons présenter en détail un protocole de routage pour chacune des familles précédemment citées.

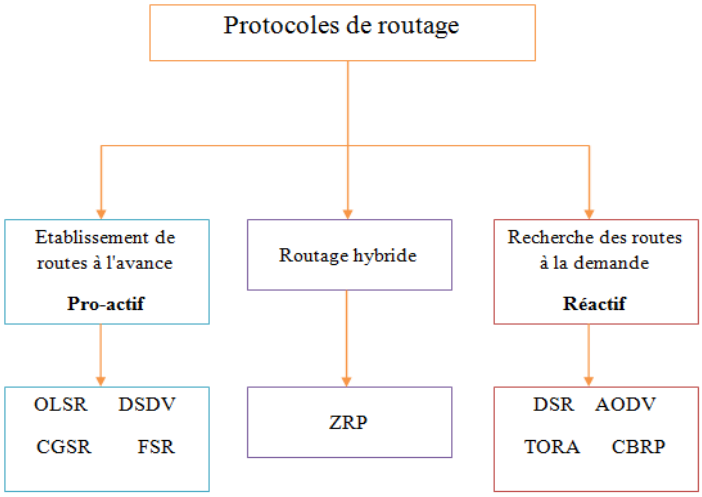


Figure 2:2 Classification des familles de protocoles ad hoc

2.2.1 Proactif

Dans ce type de routage, chaque nœud construit une table de routage par la découverte d'autres nœuds dans tout le réseau, une opération coûteuse pour le réseau a haute dynamique, parmi ces protocoles OLSR [3] et DSDV [2].

a. OLSR (Optimized Link-State Routing)

Un des protocoles proactifs les plus utilisé dans la communauté ad hoc, OLSR [3] est proposé par des chercheurs de l'INRIA et a fait l'objet de travaux de standardisation depuis 2003 au sein de IETF dans le groupe MANET [4]. C'est un protocole proactif basé sur une approche modifiée, dont la version originale ou chaque nœud propage des informations sur l'état des liens à tous les nœuds du réseau. L'altération apportée par OLSR consiste à réduire l'overhead en ne diffusant cette information que par quelques nœuds du réseau [5].

Les définitions suivantes sont utilisées dans la description du protocole [3]:

- **Nœud :** l'hôte d'un réseau ad hoc implémentant le protocole OLSR.
- **Interface :** le point d'accès au réseau ad hoc. Un nœud peut avoir plusieurs interfaces, chacune ayant une adresse IP propre.
- **Voisin immédiat :** le nœud X est un voisin immédiat du nœud Y si Y est à portée du nœud X (une des interfaces de X peut envoyer des messages sur l'une des interfaces de Y).
- **MPR (*MultiPoint Relay*) :** un nœud sélectionné par un de ses voisins immédiat (appelé MS, MPR *Selector*) pour retransmettre ses messages de mise à jour. L'ensemble des MPR d'un nœud est choisi parmi les voisins immédiats, de manière à permettre d'atteindre tous les nœuds situés exactement à 2 sauts.
- **Lien :** la coupe d'interfaces capables de communiquer (i.e recevoir des messages). L'état d'un lien peut être :
  - ✓ Symétrique *SYM*, si les deux interfaces peuvent s'entendre,

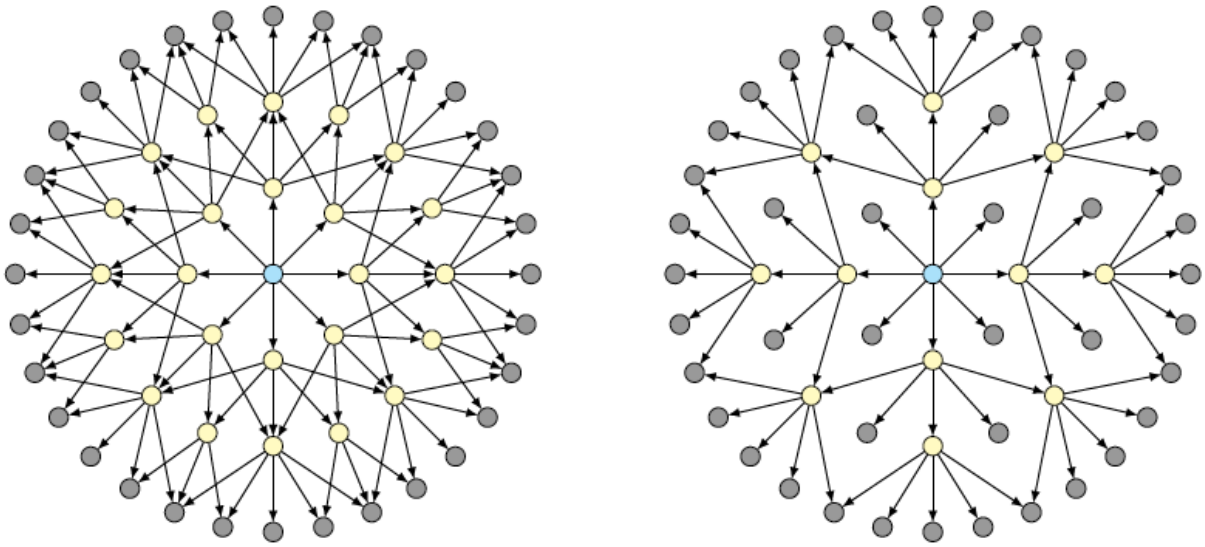
- ✓ Asymétrique *ASYM* ou *HEARD*, si les nœuds ont des puissances d'émission différentes,
- ✓ MPR, si l'émetteur a sélectionné le nœud comme MPR, dans ce cas le lien doit être symétrique.
- ✓ Lost, quand le lien est perdu.

Dans ce protocole, chaque nœud doit détecter les nœuds voisins avec lesquels il a un lien direct et bidirectionnel. Les incertitudes sur la propagation radio peuvent rendre certains liens unidirectionnels. Par conséquent, tous les liens doivent être contrôlés dans les deux directions, afin d'être considérés comme valides. Pour accomplir cela, chaque nœud diffuse périodiquement ses messages Hello contenant les informations sur ses voisins et leur état de lien. Ces messages de contrôle sont transmis dans le mode de diffusion. Ils sont reçus par tous les voisins situés à un saut, mais ils ne sont pas relayés à des nœuds supplémentaires [6] [B1].

Un des messages Hello contient [3] [6]:

- La liste des adresses des voisins pour lesquels il existe un lien bidirectionnel valide.
- La liste des adresses des voisins qui sont entendues par ce nœud (un Hello a été reçu), mais le lien n'est pas encore validé comme bidirectionnel : si un nœud trouve sa propre adresse dans un message Hello, il considère le lien du nœud expéditeur comme bidirectionnel.

Comme nous l'avons cité, le protocole de routage OLSR permet de minimiser l'inondation du réseau en diminuant les retransmissions redondantes dans la même région du réseau et réduit la taille des paquets échangés. Pour cela, il utilise un algorithme de sélection de relais multipoints MPR (Multi Point Relay). L'ensemble des relais d'un nœud N donné est construit à partir de l'ensemble minimal des voisins à un saut de N. De telle sorte que chaque voisin à deux sauts de N ait au moins un même MPR. Chaque nœud dans OLSR choisi indépendamment ses relais multipoints. La seule connaissance dont il a besoin est celle relative à ses voisins à deux sauts [3][6][B1] (voir la figure 2.3).



a. Routage par inondation (24 transmissions pour atteindre tous les nœuds à 3 sauts)

b. Routage avec les nœuds MPR (12 transmissions pour atteindre tous les nœuds à 3 sauts)

Figure 2:3 Avantage de l'utilisation des MPR

Quand un nœud diffuse un message, tous ses voisins le reçoivent. Les MPR n'ayant pas reçu ce message auparavant le rediffusent. Donc, l'overhead causé par l'inondation diminue considérablement dans OLSR. Le nœud diffuse périodiquement l'information sur l'état des liens avec leurs MPRs dans le réseau. La périodicité de l'envoi de ces messages est sujette à la détection du changement de l'ensemble des MPRs. Dans ce cas précis, la période prend alors sa valeur minimale. Dans le cas contraire cette valeur augmente jusqu'à ce qu'elle atteigne la valeur de l'intervalle de rafraichissement (refresh interval). Chaque nœud reçoit, en plus, une information sur la topologie du réseau et construit alors sa table de routage grâce au message d'état de lien. Ce routage utilisé dans OLSR n'inclus que les MPR comme nœud intermédiaire entre deux nœuds donnés [5].

Le protocole OLSR est vulnérable à différents types d'attaques. Dans [J1] [8] , nous avons étudié l'attaque du trou de noir et du trou de ver qui demeurent des attaques sévères et non complètement résolues, particulièrement dans une configuration de réseau ad hoc où le protocole OLSR est utilisé comme protocole de routage. Puis, nous avons proposé une méthode plus efficace pour détecter et prévenir ces deux attaques contre l'OLSR. Son principe de détection se base sur l'utilisation de quatre message *« HELLOreq, HELLOrep, Probing, ACK-prob* ». Cette méthode proposée est facile à déployer, et ne nécessite pas de synchronisation de l'heure ou l'emplacement de l'information; pas plus qu'elle ne nécessite pas de calcul complexe ou matériel spécial. Les performances de cette méthode montrent un taux élevé de détection selon divers scénarios.

2.2.2 Réactif

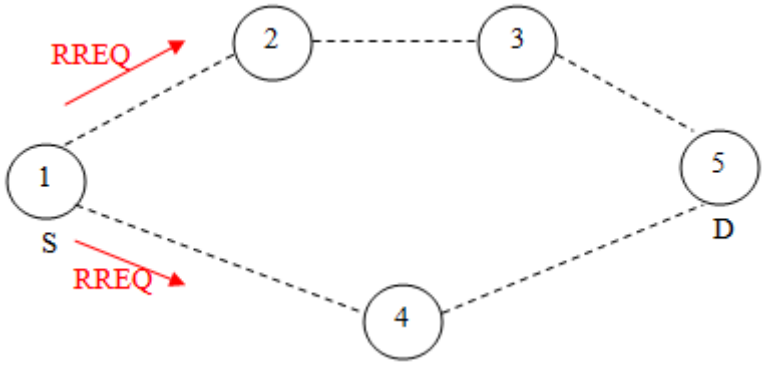
Dans ce type de routage, chaque nœud construit une table de routage lorsqu'un nœud en effectue la demande. Il ne connaît pas la topologie du réseau, il détermine le chemin à prendre pour

accéder à un nœud du réseau lorsqu'on lui demande. Parmi ces protocoles DSR [10] et AODV [9].

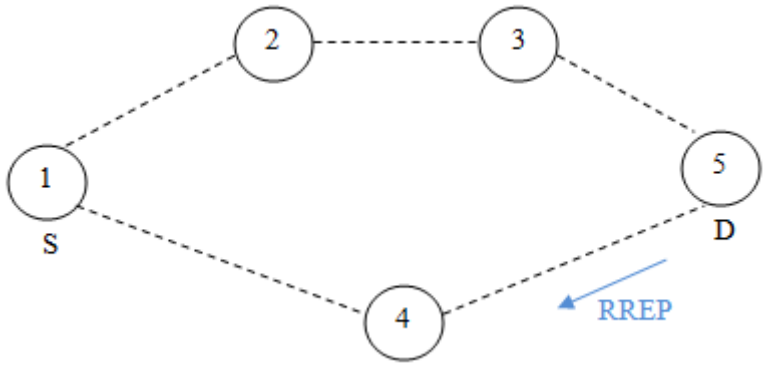
a. AODV (Ad hoc On-Demand Distance Vector Routing)

Dans la famille des routages réactifs, le protocole AODV [9] est l'un des plus célèbres. Dans cette approche, quand un nœud source S a des données à envoyer au nœud destination D (e.g. le nœud 1 dans la figure 2.4 désire envoyer des données au nœud 5), mais ne possède pas tout le cheminement vers celle-ci, il doit lancer une Route REQuest (RREQ) en *broadcast* (voir la figure 2.4.a). Ce message contient un identifiant (RREQ_ID) associé à l'adresse de la source (@SRC) qui servira à identifier de façon unique une demande de route. Le nœud source 1 enregistre cet identifiant de paquet RREQ ([RREQ_ID, @SRC]) dans son historique (*buffer*) et l'associe à un *timer* qui décomptera sa durée de vie au-delà de la quelle cette entrée sera effacée.

Quand un nœud intermédiaire (cas des nœuds 2 et 4 dans la figure 2.4.a) qui n'a pas de chemin valide vers la destination reçoit le message RREQ, il ajoute ou met à jour le voisin duquel le paquet a été reçu. Il vérifie ensuite qu'il ne l'a pas déjà traité en consultant son historique des messages traités. Si le nœud s'aperçoit que la RREQ est déjà traitée, il l'abandonne et ne la rediffuse pas. Sinon, il met à jour sa table de routage à l'aide des informations contenues dans la requête afin de pouvoir reconstruire ultérieurement le chemin vers la source. Il incrémente ensuite le nombre de saut HC (Hop Count) dans la demande de route et la rediffuse. A la réception d'un paquet RREQ, la destination 5 ajoute ou met à jour dans sa table de routage un chemin vers le nœud voisin duquel il a reçu le paquet (nœud 4) ainsi qu'un chemin vers la source 1. La destination génère ensuite une réponse de route RREP qu'elle envoie en *unicast* vers le prochain saut en direction de la source (voir la figure 2.4.b). Il est à noter qu'un nœud intermédiaire peut aussi générer un RREP si la requête l'autorise à le faire. Ces nœuds intermédiaires qui reçoivent la RREP (cas du nœud 4 dans la figure 2.4.b) vont mettre à jour le chemin qui mène à la destination dans leurs tables de routage et retransmettre en *unicast* le message (après avoir incrémenté le nombre de sauts) vers le nœud suivant en direction de la source sachant que cette information a été obtenue lors du passage de la RREQ. Enfin, lorsque la réponse de route atteint la source (nœud 1 dans la figure 2.4.a), un chemin bidirectionnel est établi entre la source et la destination, et la transmission de paquets de données peut débuter [B1] [7].



a. Le nœud 1 initialise une demande de route pour obtenir un chemin vers 5



b. La destination 5 initialise une réponse de route

Figure 2:4 Exemple d'établissement de route entre 1 et 5

Le protocole AODV est vulnérable à différents types d'attaques. Dans [C3], nous avons présenté la taxonomie des attaques et leurs influences sur les propriétés des sécurités dans les réseaux sociaux totalement mobiles (MASN) utilisant l'AODV comme protocole de routage. Ensuite, nous avons introduit un nouveau réseau social, appelé AODV avec MASN. A la fin, nous avons présenté notre nouveau mécanisme de sécurité basé sur l'utilisation de deux messages *DetectReq, DetectRep* et les signatures numériques *Champ_sig* pour détecter des liens malveillants.

2.2.3 Hybride

Ce type de protocole combine les avantages du routage proactif et réactif, ce qui offre un bon compromis entre persistance de la route et surcharge du réseau. En général, les propositions hybrides exploitent la hiérarchisation du réseau en utilisant des protocoles réactifs et proactifs et sont alors intégrés à différents niveaux de la hiérarchie. Historiquement, le premier protocole de routage ad hoc hybride est ZRP [11].

a. ZRP (Zone Routing Protocol)

Ce protocole, proposé par Haas et al. [11] en 2002, combine les deux approches vues précédemment, proactive et réactive, pour en tirer le maximum d'avantages et combler ainsi les

désavantages de chacune par les points forts de l'autre. ZRP utilise deux approches, proactive (IARP) pour le routage dans la même zone (*InterA-zone Routing Protocol* [12]) et réactive (IERP) entre les zones (*IntEr-zone Routing Protocol* [13]). L'IARP maintien une information sur l'état de lien des nœuds à une distance *d*. Dans le cas ou le nœud source et la destination sont dans la même zone, la route est alors disponible immédiatement. La plupart des protocoles proactifs existants pourraient être utilisés en tant que IARP dans ZRP. Dans le reste de cette sous section, nous allons présenter un exemple (voir figure 2.5) d'établissement de route utilisant ZRP comme protocole de routage.

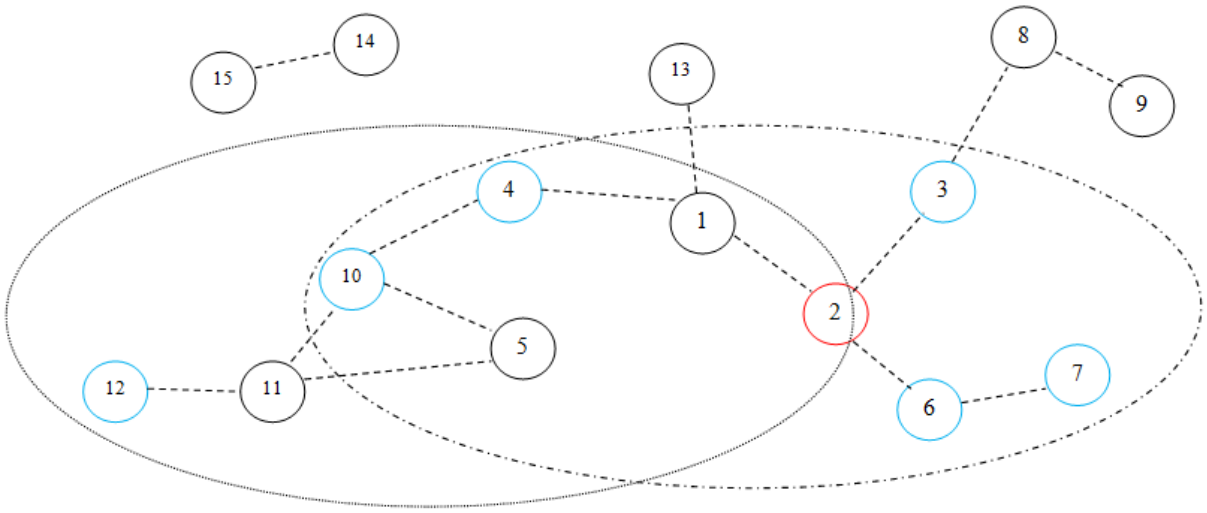


Figure 2:5 Zone de routage de rayon=2 du nœud 2 et 10

Si un nœud n'a pas de chemin vers la destination, l'IERP prend le relais pour la recherche de routes en dehors de la zone dans laquelle le nœud se trouve. Ainsi, une demande de route est créée et envoyée aux nœuds périphériques de la zone de routage (opération appelée *Bordercast*). Par exemple, les noeuds 3, 4, 6, 7, 10 et 12 sont des nœuds périphériques de la zone de routage du nœud 2 dans la figure 2.5. Les demandes de route créées sont acheminées vers la périphérie de la zone en utilisant le protocole BRP [14] (*Bordercast Resolution Protocol*). Ce dernier se base sur la topologie obtenue grâce à l'IARP pour la construction d'un arbre multicast (*Bordercast Tree*) donnant les différents chemins pour atteindre les noeuds périphériques d'une zone [7].

Ce protocole présente l'avantage de diminuer le temps de latence pour trouver de nouvelles routes. Il est à noter que d'autres protocoles hybrides existent mais rares sont ceux qui ont abouti à au moins un draft déposé dans l'IETF[5] (Internet Engineering Task Force). Nous citons à titre d'exemple ZHLS [16] qui se base sur la division du réseau en zones géographiques fixes et chaque noeud peut se localiser dans une zone grâce à ses coordonnées GPS (Global Positioning System).

[5] L'IETF est un groupe international qui participe dans l'élaboration de standards pour l'Internet. Cet organisme produit la plupart des nouveaux standards d'Internet. http://www.ietf.org/

2.3 Les concepts de base de la théorie sociale

Le réseau social mobile (AdSocial) utilise certaines propriétés sociales pour étudier les communications mobiles, nous examinons d'abord quelques notions de base en théorie sociale [17] [18] [19] [20] [J2].

- *Propinquity:* En théorie sociale, « propinquity » est défini que, dans des conditions égales, si deux nœuds sont géographiquement proches les uns des autres, ils sont plus susceptibles d'être connecté.
- *Homophyly:* « homophyly » est défini comme ayant un ou plusieurs attributs sociaux communs, comme la même organisation, et les favoris. Au niveau individuel, les personnes sont plus susceptibles d'avoir une connexion, d'amitié ou d'association, s'ils ont des attributs communs.
- *Le degré de centralité (Degree centrality) :* Dans le réseau ADSocial, un nœud central est celui qui se rapporte à une grande quantité par rapport aux autres nœuds du réseau. Par conséquent, dans [J2], nous avons proposé que les groupes se forment autour des nœuds avec le quartier le plus dense, c'est à dire que le nœud qui possède le plus grand nombre de sauts symétrique du voisin est considéré comme le centre du groupe. De cette façon, nous sommes sûrs que le centre du groupe est le nœud qui couvre le plus grand nombre de nœuds dans le groupe. Ainsi, le degré du nœud n_i est égal à la somme des messages RREQ reçues. La centralité du nœud n_i est calculée par:

$$C_D(n_i) = d(n_i) = \sum_{\forall i \neq j} e_{ij}$$

où $C_D(n_i)$ est le degré de centralité du nœud n_i; $d(n_i)$ est le degré du nœud n_i; e_{ij} est 1 si un message de route request RREQ envoyé par j au nœud i; sinon 0. Cependant, nous avons distingué trois états dans [J2], ci-après:

  - Etat (1): $C_D(n_i) = 0$, le noeud n_i est passé, ou il vient de quitter son groupe et n'a aucun voisin dans son voisinage.
  - Etat (2): $C_D(n_i) \neq 0$ et avec une faible densité, le noeud n_i est un des membres du groupe.
  - Etat (3): $C_D(n_i) \neq 0$ et avec une forte densité, le noeud n_i est le centre du groupe.

- *La proximité de centralité (Closeness centrality) :* Un nœud qui est le centre d'un groupe peut atteindre les autres nœuds ou des groupes à l'aide de chemins disponibles dans ADSocial. Par conséquent, la définition classique de la proximité de centralité modélise la diffusion de l'information à travers l'utilisation des chemins les plus courts. En supposant que le réseau est bien connecté, la proximité de centralité du nœud n_i est mesurée par :

$$C_c(n_i) = \left[\sum_{\forall i \neq j} dr(n_i, n_j)\right]^{-1}$$

où $C_c(n_i)$ la proximité de centralité du nœud n_i et $dr(n_i, n_j)$ est le chemin entre les deux nœuds n_i et n_j.

- *Le betweenness de centralité (Betweenness Centrality) :* Cette mesure a été introduite par Freeman en 1978 [21] comme une mesure pour quantifier le contrôle d'un être humain en communication entre les êtres humains. Dans le réseau ADSocial, le betweenness se concentre sur les nœuds qui se trouvent sur le chemin entre les autres nœuds. Le nœud communique dans le protocole de routage avec un autre nœud en utilisant sa table de routage pour envoyer des messages sur le chemin le plus court. Par conséquent, dans [J2] , nous avons suggéré que si d'autres voies sont disponibles dans le protocole de routage , les nœuds qui ont une forte probabilité de se produire sur un plus court chemin choisi au hasard entre deux nœuds ont une forte betweenness. Plus précisément, la formule betweenness de centralité d'un nœud est défini par:

$$C_b(n_i) = \sum_{i \neq j \neq k \in G} \frac{g_{jk}(n_i)}{g_{jk}}$$

où $C_b(n_i)$ est le betweenness de centralité du nœud n_i , $g_{jk}(n_i)$ est le nombre des chemins les plus courts à partir du nœud n_j au nœud n_k et g_{jk} est le nombre de ces chemins qui passent par n_i.

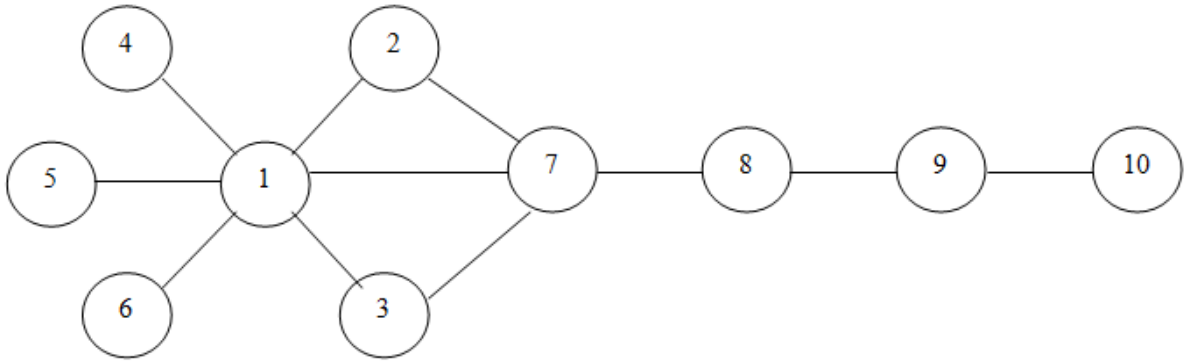


Figure 2:6 Le degré, la proximité, et betweenness centralités dans les réseaux sociaux [20]

La figure 2.6 [20] montre les différences entre le degré, la proximité, et le betweenness de centralité dans les réseaux sociaux. Selon le degré de centralité $C_D(n_i) = \sum_{\forall i \neq j} e_{ij}$, le nœud n_1 a le plus haut degré centralité, c'est à dire qu'il a des connexions les plus directes, servant de "Connecteur Central" ou "hub" dans le réseau; tandis que de la proximité de centralité $C_c(n_i) = \left[\sum_{\forall i \neq j} dr(n_i, n_j)\right]^{-1}$, les nœuds n_2 et n_3 ont la plus forte proximité de centralité, c'est à dire qu'ils ont les chemins les plus courts à tous les autres ; et à partir de betweenness

de centralité $C_b(n_i) = \sum_{i \neq j \neq k \in G} \frac{g_{jk}(n_i)}{g_{jk}}$, le nœud n_7 a la plus forte betweenness de centralité, c'est à dire qu'elle joue un rôle de «courtier» dans le réseau, ayant une grande influence sur ce qui circule dans le réseau. Dans cette thèse, nous suggérons utiliser ces propriétés sociales dans les réseaux sociaux mobiles (AdSocial) pour améliorer l'efficacité, la sécurité et la vie privée [J2].

2.4 La cryptographie

Au cours des vingt dernières années, la cryptologie a répondu à la plupart de ces questions, notamment par l'introduction, en 1976, de la cryptographie à clé publique par Diffie et Hellman [22]. Dans cette section, nous présentons des rappels de mathématiques pour la cryptographie, puis nous examinons les outils cryptographiques de bases, et ainsi les outils cryptographiques avancées.

2.4.1 Rappels de mathématiques pour la cryptographie

Nous allons présenter les principaux outils mathématiques que nous utiliserons dans cette thèse. Un lecteur souhaitant aller plus loi pourra se référer à [23] [24].

2.4.1.1 Les groupes bilinéaires

Soit $\mathbb{N} = \{1,2,3, \dots\}$ l'ensemble des entiers positifs. Si x est une chaîne, alors $|x|$ désigne sa longueur, tandis que si $\mathbb{S}$ est un ensemble alors $|\mathbb{S}|$ désigne sa taille. Si $k \in \mathbb{N}$ alors 1^k désigne la chaîne avec k. Si $\mathbb{S}$ est un ensemble alors $s \leftarrow \mathbb{S}$ désigne l'opération de choisir un élément aléatoire s de $\mathbb{S}$ uniformément.

2.4.1.1.1 Les groupes bilinéaires d'ordre premier q

Soit $\mathbb{G}$ un groupe additif cyclique et $\mathbb{G}_T$ être un groupe multiplicatif cyclique du même ordre premier q. Nous supposons que les problèmes logarithme discret dans $\mathbb{G}$ et $\mathbb{G}_T$ sont difficiles. Un groupe bilinéaire d'ordre premier est un mappage $e: \mathbb{G} \times \mathbb{G}_T \rightarrow \mathbb{G}_T$ qui satisfait les propriétés suivantes [25] [30]:

1. Calculable : Il existe un algorithme efficace pour calculer $e(P, Q)$ pour tout $P, Q \in \mathbb{G}$.
2. Bilinéaire : Pour tout $P, Q \in \mathbb{G}$ et $a, b \in \mathbb{Z}_q^*$, nous avons $e(aP, bQ) = e(P, Q)^{ab}$.
3. Non-dégénérée : Il existe $P \in \mathbb{G}$ et $Q \in \mathbb{G}$ de tel sorte que $e(P, Q) \neq 1_{\mathbb{G}_T}$.

Définition 2.1 *(Générateur bilinéaire) Un générateur de paramètre bilinéaire* Gen *est un algorithme de probabilité qui prend un paramètre k de sécurité en entrée et délivre en sortie un* $(q, P, \mathbb{G}, \mathbb{G}_T, e)$*, où* q *est un nombre premier* k *bits,* $(\mathbb{G}, +)$ *and* $(\mathbb{G}_T, +)$ *sont deux groupes avec le même ordre* q*,* $P \in \mathbb{G}$ *est un générateur, et* $e: \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$ *est une application bilinéaire recevable.*

Dans ce qui suit, nous définissons la notion quantitative des hypothèses de complexité, y compris le Problème du Logarithme Discret (DL), Problème Diffie-Hellman Calculatoire (CDH), Hypothèse CDH, Problème Diffie-Hellman Décisionnel (DDH), Hypothèse Diffie-

Hellman Décisionnel (DDH), Problème Diffie-Hellman Bilinéaire (BDH)), Hypothèse BDH, Problème Décisionnel linéaire (DLIN), Problème q-Diffie-Hellman Flexible q - (SDH), Problème Diffie-Hellman Fort (SDH2), et Hypothèse SDH2.

Définition 2.2 *(Problème du Logarithme Discret (DL)) : Soient* $\mathbb{G}$ *un groupe d'ordre premier* p *et* g *un générateur de ce groupe. Etant donnée un élément* y *de* $\mathbb{G}$*, le problème DL dans* $\mathbb{G}$ *est de trouver* $x \in \mathbb{Z}_p$ *tel que* $y = g^x$ *. L'entier* x *est appelé le logarithme discret de* y *en base de* g*.*

Définition 2.3 *(Problème Diffie-Hellman Calculatoire (CDH)) : Soient* $\mathbb{G}$ *un groupe d'ordre premier* p *et* g *un générateur de ce groupe. Etant donné* (g^a, g^b) *avec a et b choisis aléatoirement dans* $\mathbb{Z}_p$*, le problème CDH dans* $\mathbb{G}$ *est de calculer* g^{ab}*.*

Définition 2.3 *(Hypothèse CDH) : Soit A un adversaire qui prend en entrée* $(P, aP, bP) \in \mathbb{G}$ *pour les inconnues* $a, b \in \mathbb{Z}_q^*$*, et retourne* abP*. Nous considérons l'expérience aléatoire suivante.*

Expérience $\mathbf{Exp_A^{CDH}}$

$a, b \overset{R}{\leftarrow} \mathbb{Z}_q, \alpha \leftarrow A(P, aP, bP)$

si $\alpha = abP$, alors $\beta \leftarrow 1$, sinon $\beta \leftarrow 0$

retourne β

Nous définissons la probabilité de réussite de A dans la résolution du problème CDH via

$$\mathbf{Succ_A^{CDH}} = \mathbf{Pr}[\mathbf{Exp_A^{CDH}} = \mathbf{1}]$$

Soit $\tau \in \mathbb{N}$ *et* $\epsilon \in [0, 1]$*. Nous disons que le CDH est* (τ, ϵ) *sécurisé si aucun algorithme polynomial A exécuté dans le temps* τ *a du succès* $\mathbf{Succ_A^{CDH}} \geq \epsilon$ *.*

Définition 2.4 *(Problème Diffie-Hellman Décisionnel (DDH)) : pour* $a, b, c \in \mathbb{Z}_q^*$*, étant donné* $P, aP, bP, cP \in \mathbb{G}$*, décide si* $c = ab \in \mathbb{Z}_q$*. Le problème DDH est facile en* $\mathbb{G}$*, depuis nous pouvons calculer* $e(aP, bP) = e(P, P)^{ab}$ *et décide si* $e(P, P)^{ab} = e(P, P)^c$*.*

Définition 2.5 *(Hypothèse Diffie-Hellman Décisionnel (DDH)) : l'hypothèse Diffie-Hellman décisionnel implique que quel que soit l'adversaire probabiliste, en temps polynomial, cherchant à distinguer les distributions* (g^a, g^b, g^c) *et* (g^a, g^b, g^{ab})*, la différence de sa probabilité de réussite avec ½ est négligeable*[6] *[24].*

Définition 2.6 *(Problème Diffie-Hellman Bilinéaire (BDH)) : étant donné* $P, aP, bP, cP \in \mathbb{G}$ *pour les inconnus* $a, b, c \in \mathbb{Z}_q^*$*, calculer* $e(P, P)^{abc} \in \mathbb{G}_T$ *.*

[6] En mathématiques, la notion de prépondérance ou de négligeabilité exprime le fait qu'une fonction numérique « l'emporte » localement sur une autre. On dit que la première fonction est prépondérante devant la deuxième ou que la deuxième fonction est négligeable devant la première. (Source : Wikipédia)

Définition 2.7 *(Hypothèse (BDH)) : Soit A un adversaire qui prend en entré* $P, aP, bP, cP \in \mathbb{G}$ *pour les inconnus* $a, b, c \in \mathbb{Z}_q^*$*, et retourne* $e(P,P)^{abc}$ *. Nous considérons l'expérience aléatoire suivante [20].*

$$\textbf{Expérience } \mathbf{Exp_A^{BDH}}$$

$a, b, c \overset{R}{\leftarrow} \mathbb{Z}_q, \alpha \leftarrow A(P, aP, bP, cp)$

si $\alpha = e(P,P)^{abc}$, alors $\beta \leftarrow 1$, sinon $\beta \leftarrow 0$

retourne β

Nous définissons la probabilité de réussite de A dans la résolution du problème BDH via

$$\mathbf{Succ_A^{BDH}} = \mathbf{Pr}[\mathbf{Exp_A^{BDH}} = \mathbf{1}]$$

Soit $\tau \in \mathbb{N}$ *et* $\epsilon \in [0,1]$*. Nous disons que le BDH est* (τ, ϵ) *sécurisé si aucun algorithme polynomial A exécuté dans le temps* τ *a du succès* $\mathbf{Succ_A^{BDH}} \geq \epsilon$*.*

Définition 2.8 ***(****Problème Décisionnel linéaire (DLIN))* : Soit $(q, \mathbb{G}, \mathbb{G}_T, g, e)$ un environnement bilinéaire symétrique avec p premier. Etant donnée $(u, v, w, u^a, v, ^b\ w^c)$ avec u, v, w choisis aléatoirement dans $\mathbb{G}$ et a, b, c choisi aléatoirement dans $\mathbb{Z}_q$, le Problème Décisionnel Linéaire consiste à décider si $w^c = w^{a+b}$ [24].

Définition 2.9 ***(****Problème q-Diffie-Hellman Flexible q - (SDH)): Soit* $(q, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, g, e)$ *un environnement bilinéaire avec q premier. Etant donné* $(g_1, g_2, g_2^x, g_2^{x^2}, \dots, g_2^{x^q})$ *avec x choisi aléatoirement dans* $\mathbb{Z}_q$*, le problème q-Diffie-Hellman flexible consiste à trouver un couple* $(c, g_1^{\frac{1}{x+c}})$ *avec* $c \in \mathbb{Z}_q$ *[20].*

Définition 2.10 ***(****Problème Diffie-Hellman Fort (SDH2)): Soit P un élément de* $\mathbb{G}$*. Etant donné* $(xP, yP, \frac{1}{x+y}P)$ *pour les inconnues* $x, y \in \mathbb{Z}_q$*,* l_1 *distinct le tuple* $(c_i, \frac{1}{x+c_i}P)$ *, où* $c_i \in \mathbb{Z}_q$*,* $i \in \{1,2,\dots,l_1\}$*, et un tuple* $(y^2P, \dots, y^{l_2}P)$*, calcule le nouveau tuple* $(m, \frac{1}{y+m}P)$*, où* $m \in \mathbb{Z}_q$ *[20].*

Définition 2.11 *(Hypothèse (SDH2)) : Soit A un adversaire qui prend en entré* $P, xP, yP, \frac{1}{x+y}P, c_1, \frac{1}{x+c_1}P, \dots, c_{l_1}, \frac{1}{x+c_{l_1}}P$ *pour certains inconnus* $x, y, c_1, \dots, c_{l_1} \in \mathbb{Z}_q$*, et un autre tuple* $(y^2P, \dots, y^{l_2}P)$*, retourne le nouveau tuple* (c, α)*. Nous considérons l'expérience aléatoire suivante [20].*

$$\textbf{Expérience } \mathbf{Exp_A^{SDH2}}$$

$$x, y, c_1, .., c_{l_1} \overset{R}{\leftarrow} \mathbb{Z}_q$$

$$(m, \alpha) \leftarrow A\left(\begin{array}{c} P, xP, yP, \frac{1}{x+y}p \\ c_1, \frac{1}{x+c_1}P, c_2, \frac{1}{x+c_2}P, \dots, c_{l_1}, \frac{1}{x+c_{l_1}}P \\ y^2P, \dots, y^{l_2}P \end{array}\right)$$

si $\alpha = \frac{1}{y+m} P$ alors $b \leftarrow 1$ sinon $b \leftarrow 0$

retourne b

Nous définissons la probabilité de réussite de A dans la résolution du problème SDH 2 via

$$\mathbf{Succ}_{\mathbf{A}}^{\mathbf{SDH2}} = \mathbf{Pr}[\mathbf{Exp}_{\mathbf{A}}^{\mathbf{SDH2}} = \mathbf{1}]$$

Soit $\tau \in \mathbb{N}$ *et* $\epsilon \in [0,1]$. *Nous disons que le SDH2 est* (τ, ϵ) *sécurisé si aucun algorithme polynomial A exécuté dans le temps* τ *a du succès* $\mathbf{Succ}_{\mathbf{A}}^{\mathbf{SDH2}} \geq \epsilon$.

2.4.1.1.2 Les groupes bilinéaires d'ordre composite

Soit p, q deux grands nombres premiers distincts, et $n = pq$. Les groupes $(\mathbb{G}, \mathbb{G}_T)$ d'ordre composite n sont appelé *groupes bilinéaire d'ordre composite* est un mappage $e: \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$ qui satisfait les propriétés suivantes [25-30]:

a) Calculable : Il existe un algorithme efficace pour calculer $e(P, Q) \in \mathbb{G}_T$ pour tout $P, Q \in \mathbb{G}$.
b) Bilinéaire : $e(P^a, Q^b) = e(P, Q)^{ab}$ pour $(P, Q) \in \mathbb{G}^2$ et $a, b \in \mathbb{Z}_n$.
c) Non-dégénérée : Il existe $P \in \mathbb{G}$ de tel sorte que $e(P, P)$ est d'ordre n dans $\mathbb{G}_T$.

Définition 2.12 ***(****Un générateur bilinéaire composite): le générateur bilinéaire composite* $CGen$ *est un algorithme de probabilité qui prend en entré le paramètre de sécurité, et en sortis*$(n, \mathbb{G}, \mathbb{G}_T, g, e)$, *où* $n = pq$ *et* p, q *sont deux k-bit,* $\mathbb{G}, \mathbb{G}_T$ *sont deux groupes avec* $n, g \in \mathbb{G}$ *est un généraeur, et* $e : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$ *est une application bilinéaire non-dégénérée et facilement calculable.*

Soit g un générateur de $\mathbb{G}$, alors $\mathrm{g} = \mathrm{g}^{\mathrm{q}} \in \mathbb{G}$ peut générer le sous groupe $\mathbb{G}_{\mathrm{p}} = \{\mathrm{g}^0, \mathrm{g}^1, \ldots, \mathrm{g}^{\mathrm{p}-1}\}$ d'ordre q en $\mathbb{G}$. Dans ce qui suit, nous définissons la notion quantitative de complexité du problème de décision du sous groupe (SD) [28].

Définition 2.13 ***(****Problème de Décision du sous-groupe SD): Soit* $(n, \mathbb{G}, \mathbb{G}_T, g, e)$ *un environnement bilinéaire avec* $n = pq$, *p et q premiers. Soient* $\mathbb{G}_P$ *le sous groupe de* $\mathbb{G}$ *des éléments d'ordre* p *sans résidu d'ordre* q, *c'est-à-dire* $\forall a \in \mathbb{G}_p, a^p = \mathbb{I}_{\mathbb{G}}$ *et* $\mathbb{G}_p$ *le sous groupe de* $\mathbb{G}$ *des éléments d'ordre* q *sans résidu d'ordre* p, *c'est-à-dire* $\forall a \in \mathbb{G}_q, a^q = \mathbb{I}_{\mathbb{G}}$. *Le probleme SD consiste à décider si un élément donné à été choisi aléatoirement dans* $\mathbb{G}$ *ou dans un de ses sous-groupes.*

Définition 2.14 ***(****Hypothèse SD):Soit A un adversaire qui prend en entré* h *à partir de* $\mathbb{G}$ *ou sous groupe* $\mathbb{G}_P$, *et retourne le bit* $b' \in \{0, 1\}$. *Nous considérons l'expérience aléatoire suivante [20].*

Expérience $\mathbf{Exp_A^{SD}}$

$b' \leftarrow \{0,1\}$

si $b' = 0$, alors $h \overset{R}{\leftarrow} \mathbb{G}_P$; sinon si $b' = 1$ alors $h \overset{R}{\leftarrow} \mathbb{G}$

$b' \leftarrow A(e, \mathbb{G}, \mathbb{G}_T, n, h)$

retourne 1 si $b' = b$, 0 sinon

Nous définissons l'avantage de A dans la résolution du problème SD via

$$\mathbf{Adv_A^{SD}} = |\mathbf{Pr}[\mathbf{Exp_A^{SD}} = \mathbf{1}|\mathbf{b} = \mathbf{0}] - \mathbf{Pr}[\mathbf{Exp_A^{SD}} = \mathbf{1}|\mathbf{b} = \mathbf{1}]| \geq \epsilon$$

Soit $\tau \in \mathbb{N}$ et $\epsilon \in [0,1]$. Nous disons que le SD est (τ, ϵ) sécurisé si aucun algorithme polynomial A exécuté dans le temps τ a l'avantage $\mathbf{Adv_A^{SD}} \geq \epsilon$.

2.4.2 Outils cryptographiques

Dans cette sous section, nous allons présenter les principaux outils cryptographiques que nous utiliserons dans cette thèse.

2.4.2.1 Fonction à sens unique

La cryptographie moderne est fondée sur les fonctions à sens unique. En général, une fonction à sens unique est une fonction qui peut être aisément calculée, mais qui est difficile à inverser. La définition formelle d'une fonction à sens unique est comme suit [24]:

Définition 2.15 *(Fonction à sens unique): Soit $f: E_1 \rightarrow E_2$, on dit que f est à sens unique si f suit les deux propriétés suivantes.*

1. *Efficacité : il existe un algorithme efficace qui, pour tout $x \in E_1$, retourne $f(x)$.*
2. *A sens unique : Pour tout algorithme efficace qui, pour tout élément $= f(x) \in E_2$, la probabilité de trouver $x' \in E_1$ telque $y = f(x')$ est négligeable.*

2.4.2.2 Fonction de hachage cryptographique

Une fonction de hachage cryptographique est une fonction de hachage qui calcule l'emprunte d'un message avec pour objectif de pouvoir résister aux différentes attaques cryptographiques. Elle permet de ramener une chaîne de bit de taille quelconque $\{0,1\}^*$ en un condensé de taille fixe $\{0,1\}^\lambda$ avec λ est un paramètre de sécurité. Une fonction de hachage $\mathcal{H}$ est dite cryptographiquement sûre si elle vérifie les trois propriétés de sécurité suivantes.

1. Résistance à la pré-image. Etant donné $y \in \{0,1\}^\lambda$, quel que soit l'adversaire A , sa probabilité de trouver x tel que $\mathcal{H}(x) = y$ est négligeable.
2. Résistance à la seconde pré-image. Etant donné $x \in \{0,1\}^*$, quel que soit l'adversaire A , sa probabilité de trouver $x' \neq x$ telle que $\mathcal{H}(x) = \mathcal{H}(x')$ est négligeable.
3. Résistance aux collisions. Quel que soit l'adversaire sa probabilité de trouver un couple (x, x') tel que $\mathcal{H}(x) = \mathcal{H}(x')$ et $x' \neq x$ est négligeable. L'expérience qui correspond à cette propriété définit un adversaire A qui a accès à un oracle $\mathcal{O}.\mathcal{H}(m)$. A la

fin de l'expérience, l'adversaire A retourne le couple (x_1^*, x_2^*) son succès dans cette expérience est :

$$\mathbf{Succ}^{\mathcal{H}}_{\mathbf{CollRes,A}}(\boldsymbol{\lambda}) = \mathbf{Pr}[\mathcal{H}(x_1^*) = \mathcal{H}(x_2^*) \textbf{ avec } x_1^* \neq x_2^*]$$

Une fonction de hachage $\mathcal{H}$ est dite résistance aux collisions si quel que soit l'adversaire polynomial A, son succès $\mathbf{Succ}^{\mathcal{H}}_{\mathbf{CollRes,A}}(\boldsymbol{\lambda})$ est négligeable.

$$\mathbf{Succ}^{\mathcal{H}}_{\mathbf{CollRes,A}}(\boldsymbol{\lambda}) < \epsilon \text{ , avec } \epsilon \text{ négligeable}$$

La figure 2.7 montre les relations entre les trois propriétés de résistance. Une fonction qui est résistante à la collision est également résistante à la deuxième pré-image, mais l'inverse n'est pas nécessairement vrai. Une fonction peut être résistante à la collision mais non résistante à la pré-image et vice versa. Une fonction peut être résistante à la collision mais non résistante à la deuxième pré-image et vice versa.

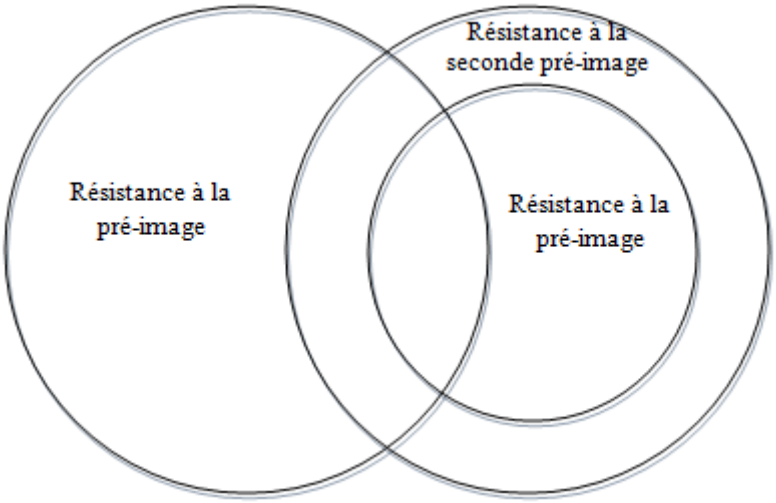


Figure 2:7 La relation entre les propriétés de la fonction de hachage [33]

Dans cette thèse, et spécialement dans [J1] [J2], nous avons utilisé les deux types de hachage suivantes : *Hachage caméléon et Algorithme de hachage SHA-2*.

a. Hachage caméléon :

Ce type de hachage proposé par H. Krawczyk et T.Rabin [31] est associé à une paire de clés publiques et privées, et possède les propriétés suivantes.

1. Quiconque connaît la clé publique peut calculer la fonction de hachage associée.
2. Pour ceux qui ne connaissent pas la trappe de la fonction est résistant à la collision dans le sens habituel à savoir, il est impossible de trouver deux entrées qui sont mappés à la même sortie.

3. Toutefois, le détenteur de l'information de trappe peut facilement trouver des collisions pour chaque entrée donnée.

D'une manière formelle, une fonction de hachage caméléon est associée à un utilisateur R qui a publié une clé publique, notéeHK_R, et détient la clé secrète correspondante (la trappe pour trouver des collisions), notée CK_R. La paire de clés publique et secrète est générée par R en fonction d'un algorithme de génération de donnée. La clé publique HK_R définit une fonction de hachage caméléon, notée $CHAM - HASH_R(\cdot,\cdot)$, qui peut être calculer efficacement la valeur de HK_R. Sur l'entrée d'un message m et une chaîne aléatoire r, cette fonction génère une valeur de hachage $CHAM - HASH_R(m,r)$ qui satisfait les propriétés suivantes:

1. Uniformité. Tous les messages m induis la même distribution de probabilité sur $CHAM - HASH_R(m,r)$ pour r choisi uniformément au hasard.
2. Résistance aux collisions. Il n'existe pas un algorithme efficace sur l'entrée de la clé publique HK_R peut trouver les paires m_1, r_1 et m_2, r_2 où $m_1 \neq m_2$ de telle sorte que $CHAM - HASH_R(m_1, r_1) = CHAM - HASH_R(m_2, r_2)$. L'expérience qui correspond à cette propriété définie un adversaire A connaissant la clé publique de la fonction de hachage caméléon HK_R et qui a accès à un oracle $\mathcal{O}.\mathcal{H}.Forge(m', m, r, h)$. $\{m_i', m_i\}_{i\in[1,n]}$ est l'ensemble des m' et m des requêtes à l'oracle $\mathcal{O}.\mathcal{H}.Forge$ et $\{r_i\}_{i\in[1,n]}$ les réponses correspondantes. A la fin de l'expérience l'adversaire retourne un quintuplet $(HK_R, m^*, r^*, \tilde{m}^*, \tilde{r}^*)$, à condition que $(m^*, r^*) \notin \{(m_i', r_i')\}_{i\in[1,n]}$, $(\tilde{m}^*, \tilde{r}^*) \notin \{(m_i', r_i')\}_{i\in[1,n]}$ et $(m^*, r^*) \neq (\tilde{m}^*, \tilde{r}^*)$. Le succès de l'adversaire dans cette expérience est :

$$\mathbf{Succ}^{CHAM}_{\mathbf{CollRes,A}}(\boldsymbol{\lambda}) = \mathbf{Pr}[CHAM - HASH_R((m^*, r^*) = CHAM - HASH_R(\tilde{m}^*, \tilde{r}^*)]$$

Une fonction de hachage $CHAM$ est dite résistance aux collisions si le succès $\mathbf{Succ}^{CHAM}_{\mathbf{CollRes,A}}(\boldsymbol{\lambda})$ de tout adversaire polynomial A est négligeable.

$$\mathbf{Succ}^{CHAM}_{\mathbf{CollRes,A}}(\boldsymbol{\lambda}) < \epsilon \text{ , avec } \epsilon \text{ négligeable}$$

b. Algorithme de hachage SHA-2 :

Ces dernières années, la fonction de hachage le plus utilisée a été le Secure Hash Algorithm (SHA). SHA a été développé par National Institute of Standards and Technology[7] (NIST). SHA est basé sur la fonction de hachage MD4, et sa conception modélise étroitement MD4. SHA-1 est également spécifiée dans la RFC 3174, qui reprend essentiellement le matériau dans la norme FIPS 180-1, mais ajoute une mise en œuvre du code C. SHA-1 produit une valeur de hachage de 160 bits. En 2002, le NIST a produit une version révisée de la norme, la norme FIPS 180-2, qui a défini trois nouvelles versions de SHA, avec des longueurs de ha-

[7] National Institute of Standards and Technology est une agence du département du commerce des États-Unis. Son but est de promouvoir l'économie en développant des technologies, la métrologie et des standards de concert avec l'industrie. (Source : Wikipédia)

chage de la valeur de 256, 384 et 512 bits, connus sous le nom SHA-256, SHA-384 et SHA - 512, respectivement. Collectivement, ces algorithmes de hachage sont connus comme SHA-2. Ces nouvelles versions ont la même structure sous-jacente et utilisent les mêmes types d'arithmétique modulaire et les opérations logiques binaires comme SHA-1. Un document révisé a été publié sous FIP PUB 180-3 en 2008, qui a ajouté une version 224 bits (tableau 2.1). SHA-2 est également spécifié dans la RFC 4634, qui reprend essentiellement le matériau dans la norme FIPS 180-3, mais ajoute une mise en œuvre du code C.

	SHA-1	SHA-224	SHA-256	SHA-384	SHA-512
La taille du message condensé	160	224	256	384	512
La taille du message	$<2^{64}$	$<2^{64}$	$<2^{64}$	$<2^{128}$	$<2^{128}$
La taille du bloc	512	512	512	1024	1024
La taille du mot	32	32	32	64	64
Le nombre d'étapes	80	64	64	80	80

Remarque : Toutes les tailles sont mesurées en bits.

Tableau 2:1 La comparaison des paramètres du SHA

SHA-2, en particulier la version 512 bits, semble apporter la sécurité inattaquable. Cependant, SHA-2, partage la même structure et les opérations mathématiques que ses prédécesseurs, et c'est une cause de préoccupation. Parce qu'il faudra des années pour trouver un remplaçant adéquat pour SHA-2, si elle devient vulnérable, le NIST a décidé de commencer le processus d'élaboration d'une nouvelle norme de hachage. En conséquence, le NIST a annoncé en 2007 une compétition pour produire la fonction de hachage NIST de la prochaine génération, appelé SHA-3. Pour plus de détail sur le fonctionnement du SHA, le lecteur pourra se référer à [33].

2.4.2.3 Fonction pseudo-aléatoire

Une fonction pseudo-aléatoire FPA, est une fonction déterministe qui associe à tout couple $(k, m) \in \{0,1\}^k \times \{0,1\}^k$ un élément dans $\{0,1\}^n$ où k est la clé secrète. Cette fonction doit suivre les deux propriétés suivantes [24].

1. Sens unique. FPA doit être une fonction facile à évaluer mais difficile à inverser en ses variables.
2. Pseudo-aléatoire. Même si nous connaissons m, il doit être calculatoirement impossible de distinguer une sortie de $FPA(*, m)$ d'une chaîne de n bits aléatoires. L'expérience qui correspond à cette propriété définit un adversaire A face à un oracle $FPA.Challenge(m)$ qui retourne une sortie de FPA sur le message m si $b = 0$ et une chaîne aléatoire sinon. A la fin de l'expérience, l'adversaire retourne un bit b^* , son avantage dans cette expérience est [24] :

$$\mathbf{Adv}^{\mathbf{FPA}}_{\mathbf{Ps-Aléa,A}}(\boldsymbol{\lambda}) = |\mathbf{Pr}[\mathbf{b} = \mathbf{b}^*] - \mathbf{1/2}|$$

Une fonction pseudo-aléatoirement FPA est dit pseudo-aléatoire si l'avantage $\mathbf{Adv}^{\mathbf{FPA}}_{\mathbf{Ps-Aléa,A}}(\boldsymbol{\lambda})$ de tout adversaire polynomial A est négligeable.

$$\mathbf{Adv}^{\mathbf{FPA}}_{\mathbf{Ps-Aléa,A}}(\boldsymbol{\lambda}) < \epsilon \text{ , avec } \epsilon \text{ négligeable}$$

2.4.2.4 Les codes d'authentification de message

2.4.2.4.1 MAC (Message Authentication Code)

Le code d'authentification de message (MAC, Message Authentication Code) est un code accompagnant des données dans le but d'assurer l'intégrité de ces dernières, en permettant de vérifier qu'elles n'ont subi aucune modification. L'émetteur et le destinateur partagent une clé secrète commune qu'ils utilisent pour générer et vérifier le code d'authentification du message. Plus formellement, un MAC se présente sous la forme suivante.

Définition 2.16 ***(****Code d'authentification de message MAC) : Un code d'authentification de message est une fonction* $MAC : \{0,1\}^{\lambda} \times \{0,1\}^{*} \rightarrow \{0,1\}^{\lambda}$ *, avec* λ *et* λ' *deux paramètres de sécurité. Par abus de langage, on appelle MAC du message* m *avec la clé secrète et la valeur* $MAC(K, m)$*. Le schéma de MAC constitué de trois algorithmes, ci-après :*

- ***Génération de clé :*** *un algorithme probabiliste qui retourne une clé aléatoire k prise dans l'ensemble des clés possibles.*
- ***Génération de MAC :*** *un algorithme déterministe ou probabiliste qui prend en entrée un message clair* $m \in \{0,1\}^{*}$ *et retourne un tag* $\tau \in \{0,1\}^{t} \cup \perp : \tau = m_k(m)$.
- ***Vérification :*** *un algorithme déterministe qui prend en entrée un tag* $\in \{0,1\}^{t}$ *, un message* m *et retourne un bit selon la validité du tag pour ce message.*

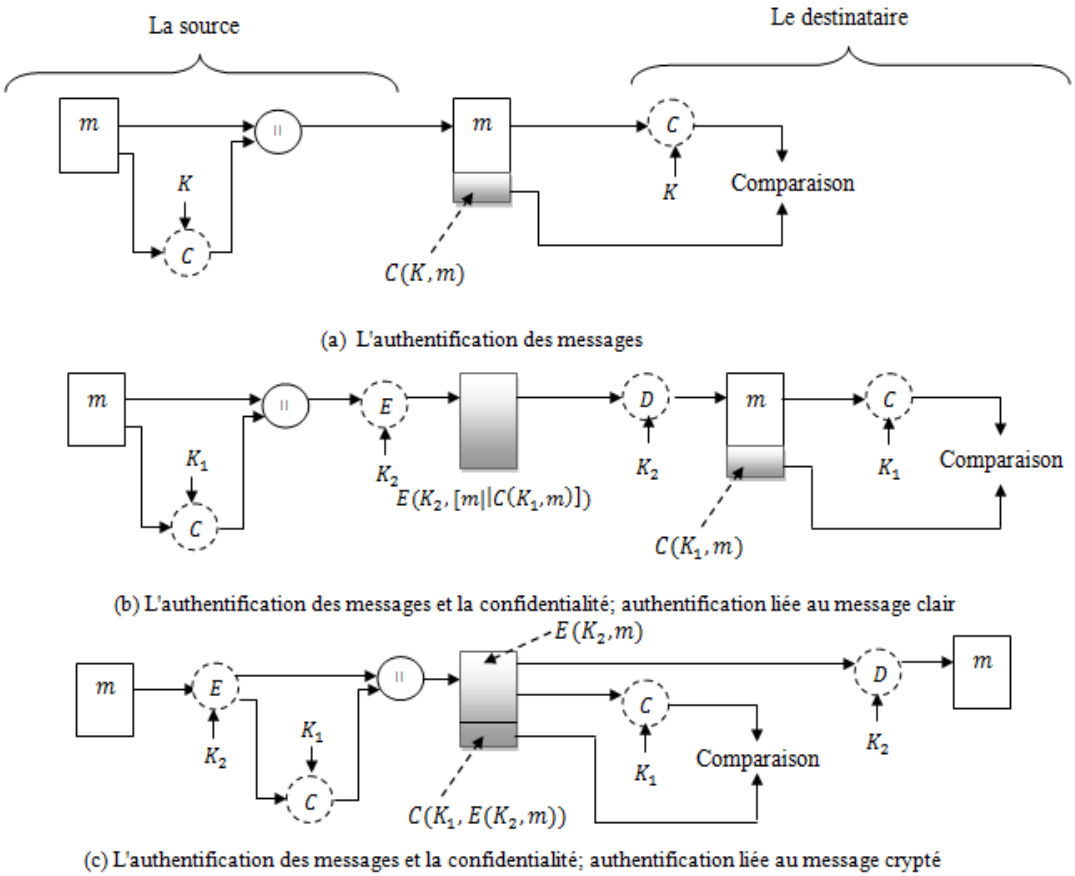


Figure 2:8 Les principes de base d'utilisation de MAC

La figure 2.8 présente les principes de base d'utilisation du MAC. Le processus décrit dans la figure 2.8a fournit une authentification mais pas la confidentialité, car le message dans son ensemble est transmis en clair. La confidentialité peut être assurée en effectuant le chiffrement des messages, soit après (voir figure 2.8b) ou avant (voir figure 2.8c) de l'algorithme MAC. Dans ces deux cas, les deux clés sont nécessaires, chacun étant partagé entre la source et le destinateur. Dans le premier cas, le MAC est calculé avec le message en entré et ensuite concaténé au message. Le bloc entier est ensuite crypté. Dans le second cas, le message est d'abord chiffré. Ensuite, le MAC est calculé en utilisant le texte chiffré résultant et est concaténé au texte chiffré pour former le bloc transmis. En règle générale, il est préférable de lier l'authentification directement au message en clair [33].

2.4.2.4.2 HMAC (Keyed-Hash Message Authentication Code)

Au cours des dernières années, il y a eu un intérêt accru pour l'élaboration d'un MAC dérivé d'une fonction de hachage cryptographique. Les motivations de cet intérêt sont:

1. Les fonctions cryptographiques, comme MD5 et SHA qui s'exécutent généralement plus rapidement dans le logiciel de chiffrement par blocs symétriques tels que DES.
2. Le code de la bibliothèque de fonctions de hachage cryptographique est largement disponible.

Avec le développement de l'AES[8] et la plus grande disponibilité du code des algorithmes de chiffrement, ces considérations sont moins importantes, mais MAC basés sur le hachage continue à être largement utilisé. Une fonction de hachage comme SHA n'a pas été conçue pour être utilisée comme un MAC et ne peut être utilisée directement à cet effet, car elle ne repose pas sur une clé secrète. Il y a eu un certain nombre de propositions pour la constitution d'une clé secrète dans un algorithme de hachage existant. L'approche qui a reçu le plus de soutien est HMAC [34]. HMAC a été publiée en tant que RFC 2104, ainsi choisie comme obligatoire à mettre en œuvre MAC pour la sécurité IP, et est utilisée dans d'autres protocoles Internet, tels que SSL. HMAC a également été publiée en tant que norme NIST (FIPS 198)[9] et en tant que norme IETF (RFC 2104)[10].

L'algorithme de HMAC

Figure 2.9 illustre le fonctionnement global de HMAC. Les termes et expressions utilisés sont définis comme suit :

- H = une fonction de hachage embarqué (par exemple, MD5, SHA-2)
- IV = la valeur initiale pour la fonction de hachage
- m = le message d'entrée
- Y_i = i-ème bloc du , $0 \leq i \leq (L-1)$
- L = le nombre de bloc dans m
- b = le nombre de bits dans un bloc
- n = la longueur du code de hachage produite par la fonction de hachage
- K = la clé secrète ; la longueur recommandée est $\geq n$; si la longueur de clé est $> b$, la clé est introduite dans la fonction de hachage pour produire une clé de n bits
- K^+= K complétée par des zéros sur la gauche afin que le résultat est b bits en longueur
- ipad = 00110110 (36 en hexadécimal) répété b / 8 fois
- opad= 01011100 (5C en hexadécimal) répété b / 8 fois
  Puis HMAC peut être exprimée comme suit :

$$\text{HMAC}(K, m) = \text{H}[(K^+ \oplus \text{opad})||\text{H}[(K^+ \oplus \text{ipad})||m]]$$

Les étapes de l'algorithme HMAC est définit comme suit :

1. Ajouter des zéros à l'extrémité gauche de K pour créer une chaîne de b-bits K^+ .
2. XOR (bitwise exclusive-OR) K^+avec ipad pour produire le b-bit bloc S_i.
3. Ajouter m à S_i.
4. Appliquer H pour le flux généré à l'étape 3.

[8] AES (Advanced Encryption Standard) est un algorithme de chiffrement symétrique. Il remporta en octobre 2000 le concours AES, lancé en 1997 par le NIST et devint le nouveau standard de chiffrement pour les organisations du gouvernement des États-Unis. Il a été également approuvé par la NSA (National Security Agency) pour les informations top secrètes. (Source : Wikipedia)
[9] http://csrc.nist.gov/publications/PubsFIPS.html#198-1
[10] http://www.ietf.org/rfc/rfc2104.txt

5. XOR K^+avec opad pour produire le b-bit bloc S_0.
6. Ajouter le résultat de hachage à partir de l'étape 4 à S_0 .
   Appliquer H au flux généré à l'étape 6 et sortir du résultat.

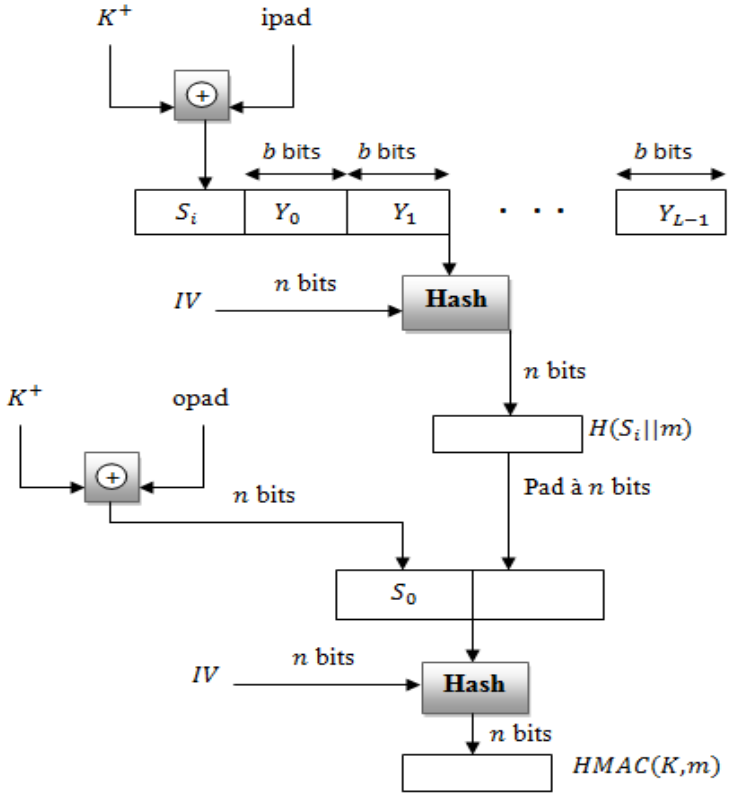


Figure 2:9 La structure de HMAC

2.4.2.5 Signature numérique

La signature numérique est un mécanisme assurant l'intégrité d'un message ainsi que l'authentification de la source de celui-ci. Ceci est possible grâce à la cryptographie asymétrique [7] [24]. La définition suivante est due à Goldwasser, Micali et Rivest [37], et qui est devenue la définition standard de sécurité pour les schémas de signature.

Définition 2.17 *(Schéma de signature) :* $G(\cdot)$, $Sign_{(\cdot)}$, $Verify_{(\cdot)}(\cdot,\cdot)$ *sont des algorithmes polynomiaux probabilistes, où* G *est l'algorithme de génération de clé,* $Sign$ *est l'algorithme de signature et* $Verify$ *est l'algorithme de vérification, constitue un schéma de signature numérique pour une famille (indexée par la clé publique pk) des espaces de message* $\mathcal{M}_{(\cdot)}$ *si :*

Exactitude. *Si un message* m *est dans l'espace de message pour une clé publique* pk*, et* sk *est la clé secrète correspondante, la sortie de* $Sign_{sk}(m)$ *est toujours acceptée par l'algorithme de vérification* $Verify_{pk}$*. Plus formellement, pour toutes les valeurs* m *et* k*:*

$$\Pr[(pk, sk) \leftarrow G(1^k); \sigma \leftarrow Sign_{sk}(m): m \in \mathcal{M}_{pk} \wedge \neg Verify_{pk}(m, \sigma)] = 0$$

Sécurité. *Même si un adversaire a accès à l'oracle de l'algorithme de signature qui fournit les signatures sur les messages du choix de l'adversaire, l'adversaire ne peut pas créer une signature valide d'un message si'il n'est pas explicitement interrogé. Plus formellement, pour toutes les familles de probabiliste polynomial oracle machine de Turing* $\{A_k^{(\cdot)}\}$ *, il existe une fonction négligeable* $v(k)$ *de telle sorte que*

$$\Pr[(pk, sk) \leftarrow G(1^k); (Q, x, \sigma) \leftarrow A_k^{Sign_{sk}(\cdot)}(1^k) : Verify_{pk}(m, \sigma) = 1 \wedge \neg (\exists \sigma' \,|(m, \sigma') \in Q)] = v(k)$$

Par exemple, lorsqu'une source désire transmettre des données à une destination, elle applique la fonction de hachage sur le message à envoyer et le condensé obtenu est chiffré avec sa clé privée. Le résultat obtenu constitue la signature et est envoyé avec le message. La destination utilise la clé publique de la source pour déchiffrer le condensé et le compare avec le condensé obtenu en appliquant la fonction de hachage sur le message reçu. Ainsi, la destination garantit que le message vient de la source et non pas d'un nœud usurpant son identité et garantit aussi que le message n'a pas été altéré lors du transfert. (voir la figure 2.10)

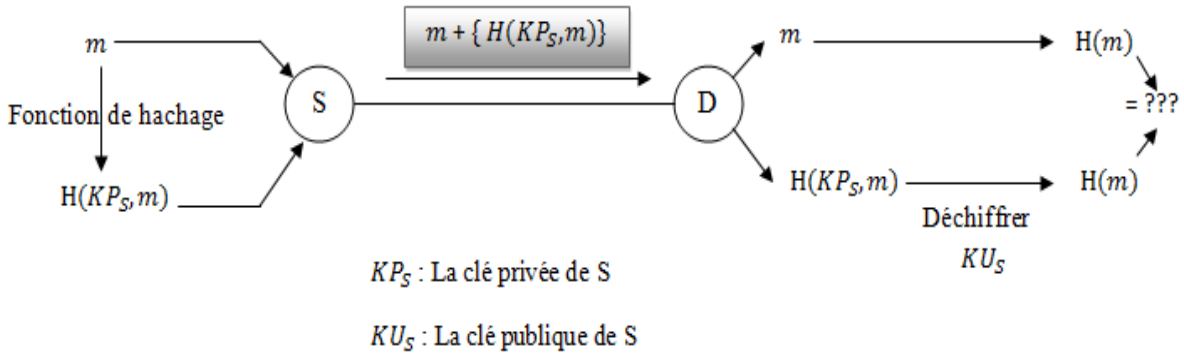


Figure 2:10 Signature numérique

Dans cette thèse, nous avons utilisé le schéma de signature digital *Schnorr*, qui est basé sur des logarithmes discrets [35]. Le schéma de *Schnorr* minimise la quantité dépendant de messages de calcul nécessaire pour générer une signature. L'essentiel du travail pour la génération de signature ne dépend pas sur le message et peut être fait pendant le temps d'inactivité du processeur. La partie de message dépend de la génération de signature et nécessite la multiplication d'un nombre entier $2n$-bits avec n-bit entier. Le schéma est basé sur l'utilisation d'un premier module p, avec $p-1$ ayant un q facteur premier de taille appropriée; qui est $p-1 \equiv (\mathrm{mod}\, q)$. Typiquement, nous utilisons $p \approx 2^{1024}$ et $\approx 2^{160}$. Ainsi, p est un nombre de 1024-bit, et q est un nombre de 160-bit, qui est aussi la longueur de la valeur de hachage SHA-1.

La première partie de ce schéma est la génération d'une paire de clés privée / publique, qui se compose de ces étapes suivantes :

1. Choisir des nombres premiers p et q, tel que q est un facteur premier $p-1$.
2. Choisir un entier a, tels que $a^q = 1 \bmod q$. Les valeurs a, p, et q comprennent une clé publique globale qui peut être commune à un groupe d'utilisateurs.
3. Choisir un nombre aléatoire s avec $0 < s < q$. C'est la clé privée de l'utilisateur.
4. Calculer $v = a^{-s} \bmod p$. C'est la clé publique de l'utilisateur.

Un utilisateur avec la clé privée s et la clé publique v génère une signature comme suit.

1. Choisir un nombre aléatoire r avec $0 < r < q$ et calculer $= a^r \bmod p$. Ce calcul est une étape de prétraitement indépendant du message à signer.
2. Concaténer le message avec x et le résultat de hachage pour calculer la valeur de e :

$$e = \mathrm{H}(m||x)$$

3. Calculer $= (r + se) \bmod q$. La signature est constitué du pair (e, y).

Un autre utilisateur peut vérifier la signature comme suit.

1. Calculer $x' = a^y v^e \bmod p$.
2. Vérifier que $= \mathrm{H}(m \,||\, x')$.

Il est à noter qu'ils existent des signatures particulaires. Dans le reste de cette sous section, nous allons présenter deux types de signatures particulaires.

a. Signatures Camenisch-Lysyanskaya

La signature « Camenisch-Lysyanskaya » est appelée ainsi en référence aux auteurs qui l'introduite [36]. En plus des propriétés usuelles d'un schéma de signature, ce schéma particulier doit assurer les propriétés particulières suivantes [24]:

- Le signataire peut signer un engagement sans pour autant connaitre les valeurs engagées de telle façon qu'il soit possible, par la suite, de construire une preuve ans révéler ni la signature, ni l'ensemble des valeurs engagées.
- Le signataire peut signer un message m décomposé en blocs $m = m_1 || \cdots ||m_l$ de telle façon qu'il soit possible, par la suite, de construire une preuve que l'on connaît la signature du message contenant le bloc m sans révéler ni la signature, ni le message complet.

De manière plus formelle, un schéma de signature « Camenisch-Lysyanskaya » se déroule de la façon suivante [36].

Définition 2.18 *(Schéma de signature Camenisch-Lysyanskaya) : Un schéma de signature «* Camenisch-Lysyanskaya » est composé de trois algorithmes, ci-après :

La génération des clés. *Exécuter l'algorithme Setup pour générer* $(q, G, \mathrm{G}, g, \mathrm{g}, e)$. *Choisir* $x \leftarrow \mathbb{Z}_q,\ y \leftarrow \mathbb{Z}_q,\ z \leftarrow \mathbb{Z}_q$. *Soit* $X = g^x,\ Y = g^y$ *et* $Z = g^z$. *Fixer* $sk = (x, y, z),\ pk = (q, G, \mathrm{G}, g, \mathrm{g}, e, X, Y, Z)$.

Signature. *Le message d'entrée*(m, r)*, la clé secrète* $k = (x, y, z)$ *, et la clé publique* $pk = (q, G, \mathrm{G}, g, \mathrm{g}, e, X, Y, Z)$. *Effectuer :*

- *Choisir un aléatoire* $a \leftarrow G$.
- *Soit* $A = a^z$.
- *Soit* $b = a^y$, $B = A^y$.
- *Soit* $c = a^{x+xym} A^{xyr}$.
- *Sortie* $\sigma = (a, A, b, B, c)$.

Vérification. *En entré* $k = (q, G, \mathrm{G}, g, \mathrm{g}, e, X, Y, Z)$ *, le message* (m, r)*, et signature présumée* $\sigma = (a, A, b, B, c)$ *, vérifier les points suivants:*

- *A a été formé correctement:* $e(a, Z) = e(g, A)$.
- *b et B ont été formés correctement:* $e(a, Y) = e(g, b)$ *et* $e(A, Y) = e(g, b)$.
- *c a été formé correctement :* $e(X, a) \cdot e(X, b)^m \cdot e(X, B)^r = e(g, c)$.

b. Signatures de groupes

Les signatures de groupes, introduites par Chaum et Heyst dans [38], permettent d'assurer l'anonymat des signataires. Tout membre du groupe peut signer des messages, mais la signature résultante conserve l'identité du secret signataire. Dans certains systèmes, il y a un tiers qui peut tracer la signature, ou annuler son anonymat, à l'aide d'une trappe spéciale. Certains systèmes appuient la révocation [39] [40] où l'appartenance au groupe qui peut être désactivée de manière sélective sans affecter la capacité de signer des membres non révoqués. Actuellement, la construction la plus efficace se fait à l'aide des groupes bilinéaires introduit par Jens Groth [41].

2.5 Travaux de recherche connexes

Dans cette section, nous passons en revue quelques-uns de ces travaux existants [45] [46] [50] [53] [54] [55] [56]. Généralement, pour atteindre la confidentialité contextuelle, les approches existantes peuvent être classées en deux types: l'une est par la confidentialité de l'emplacement de la source, et la deuxième par la confidentialité de l'emplacement de la destination.

- *Par la confidentialité de l'emplacement de la destination* qui se compose de deux techniques pour la localisation de la confidentialité: 1) la technique de génération de paquets reconnus dans lequel une destination crée des faux sources à chaque fois où un émetteur informe la destination qu'il a des données à envoyer; 2) le routage sur un seul chemin, qui réalise la localisation de la confidentialité en faisant chaque paquet généré par une source sur un chemin aléatoire avant d'être livré à la destination. Une autre technique pour protéger la confidentialité de l'emplacement de la source est présentée par Ozturk et al. [45] où il nécessite un nœud source à envoyer chaque paquet à travers de nombreux chemins vers une destination pour rendre difficile à un adversaire de remonter à la source.

- *Par la confidentialité de l'emplacement de la destination*, Deng et al. [53] décrit une technique pour protéger les lieux de destinations à partir d'un espion locale en hachant les champs d'identification en-têtes de paquets, après dans [46] il presente quatre techniques pour protéger la confidentialité de la localisation de la destination à partir d'un espion local qui est capable d'effectuer la corrélation temporelle et le suivi des taux. Une autre technique pour protéger la vie privée de l'emplacement de destination est présentée dans [54] où ils proposent un protocole de routage de confidentialité de la localisation (LPR) pour la confidentialité de l'emplacement de la destination. L'algorithme LPR offre la confidentialité à la destination avec l'aide de sauts redondants et les faux paquets lorsque les données sont envoyées à la destination.

Le schéma de confidentialité a été amélioré pour les différents types de réseau. Yipin et al [55] propose un schéma efficace d'authentification pseudonyme avec une forte protection de la vie privée, appelé PASS, pour les communications véhiculaires. Contrairement aux systèmes traditionnels d'authentification pseudonymes, la taille de la liste de révocation de certificats (CRL) dans PASS est linéaire avec le nombre de véhicules. Pour la réalisation de la préservation de la vie privée de l'utilisateur du véhicule tout en améliorant l'efficacité de la mise à jour clé des services basés sur la localisation dans les réseaux ad hoc véhiculaires, Lu et al. [56] propose un système de gestion de clés préservant la vie privée dynamique, appelée DIKE. Une autre étude liée à la vie privée, mais pour les communications de réseaux intelligents (smart grid), où Lu et al. [50] propose un schéma d'agrégation efficace en préservant la vie privée, appelé EPPA. EPPA utilise un super-séquence croissante pour structurer les données multidimensionnelles, et crypter les données structurées par la technique cryptographique *homomorphe paillier*, et pour réduire le coût de l'authentification, il adopte la technique de vérification par lots. Enfin, nous évaluons d'autres techniques de confidentialité dans le chapitre suivant.

2.6 Conclusions

Dans ce chapitre, nous avons discuté sur certains travaux connexes, y compris le routage dans les réseaux ad hoc, les concepts de base de la théorie sociale, et les principaux outils cryptographiques. Dans les chapitres suivants, nous examinons cinq protocoles SPRING [62], SPF [64], PCS [65], FLIP [66] et Pi [67] pour la sécurisation des réseaux ad hoc sociaux afin de les comparer avec nos deux contributions proposées dans le chapitre 4 et 5.

Chapitre 3 Les protocoles SPRING, SPF, PCS, FLIP et Pi pour la sécurisation et la confidentialité des communications véhiculaires ad hoc sociaux

Avec les appareils de communication sans fil équipés en véhicules (également connu sous le nom unités embarquées (On-Board Units (OBU)) et les unités de contrôle routier (Roadside Units- RSUs), un réseau auto-organisé peut être formé, qui est appelé un réseau ad hoc véhiculaires (VANET). Les VANETs est un cas particulier des réseaux ad hoc mobiles (MANETs) [B1], où les nœuds mobiles sont instanciés avec des véhicules équipés de dispositifs de communication OBU, comme indiqué dans la figure 3.1. Par conséquent, les réseaux VANETs ont des caractéristiques uniques différentes de MANET (voir figure 3.2). Récemment, un projet similaire à notre thèse réalisé en 2012 par Rongxing Lu[11] dans [20] , où il a étudié la sécurité et la confidentialité dans les réseaux véhiculaire ad hoc sociaux (VSNs) avec la proposition de cinq protocoles SPRING [62], SPF [64], PCS [65], FLIP [66] et Pi [67] afin de sécuriser les VSNs. Dans ce chapitre, nous examinons ces cinq protocoles afin de les comparer avec nos deux contributions proposées dans le chapitre 4 et 5.

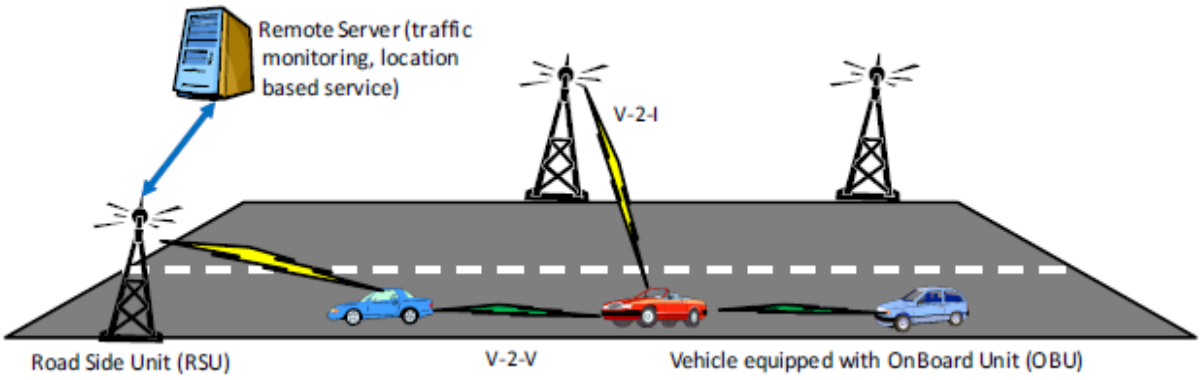


Figure 3:1 Vehicular Ad hoc Network (VANET) [20]

[11] Rongxing Lu : http://www.ntu.edu.sg/home/rxlu/ (Dernière consultation le 13 novembre 2013)

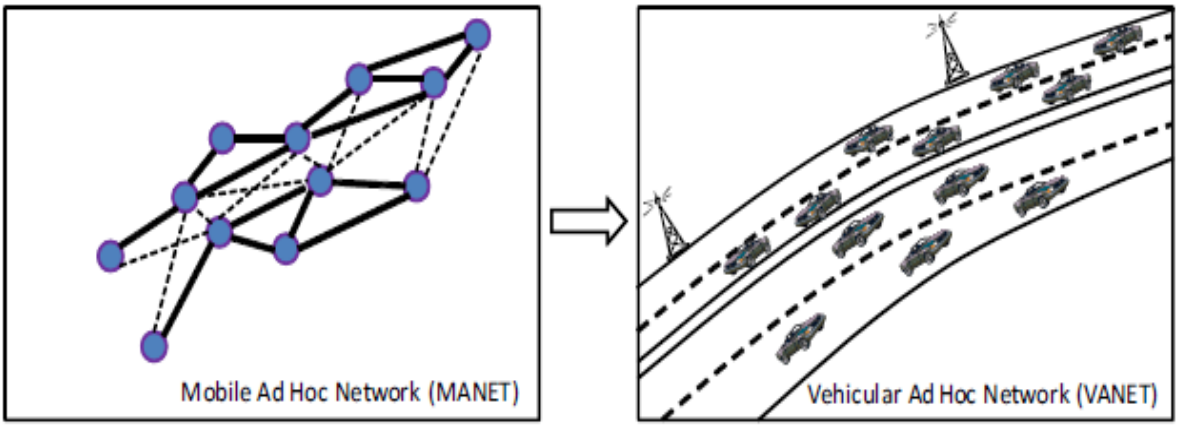


Figure 3:2 La relation entre VANET et MANET [20]

3.1 Le protocole SPRING

Au cours des dernières années, les véhicules d'un réseau ad hoc, comme un cas particulier de DTNs[12] et également connu comme véhicules DTN, est devenu de plus en plus attrayant pour le public en raison de sa capacité prometteuse d'améliorer la sécurité routière et la fluidité du trafic. Dans les réseaux véhiculaires, une variété d'applications peut être activée par véhicule-à-véhicule (V-2-V) et-à un véhicule infrastructure (V-2-I) communications pour améliorer les systèmes de transport. Dans [62], Lu et *al.* proposent un protocole en préservant la confidentialité des transmission de paquets pour les véhicules DTNs, appelé SPRING. Le protocole proposé se caractérise par le déploiement des RSUs aux intersections sociales élevées pour aider la transmission de paquets entre les véhicules en stockant temporairement les paquets à travers la communication V-2-I au cours de la période où les véhicules du prochain saut de ces paquets ne sont pas disponibles. Avec ce genre d'assistance du RSU, la probabilité de perte de paquet est réduite et par conséquent une grande fiabilité de transmission de paquets dans DTNs véhicules peut être atteinte. Plus précisément, les contributions de cette proposition sont de trois ordres.

- Premièrement, les auteurs définissent le degré heuristique social des intersections dans DTNs véhicules. Basé sur les informations sociales, ils mettent RSUs à ces intersections sociales élevées.
- Deuxièmement, les auteurs proposent le protocole de SPRING, un protocole préservant la confidentialité de transmission par paquets sociaux pour DTNs véhicules. Dans SPRING, parce que les unités d'actions restreintes fixes sont déployées à l'intersection sociale élevée, un grand nombre de véhicules passera par ses RSUs. Puis, les RSUs peuvent apporter une assistance considérable pour stocker temporairement certains paquets et en aidant la transmission de paquets de parvenir à une haute fiabilité de

[12] Au cours des dernières années, le réseau tolérant aux délais (Delay tolerant network DTN), telles que la communication de l'espace et de réseautage dans les zones peu peuplées, et les réseaux véhiculaires ad hoc, ont fait l'objet d'importants d'efforts de recherche. Contrairement aux réseaux traditionnels attachés comme l'Internet, un DTN est un réseau mobile clairsemé où la connexion entre les nœuds du réseau change au fil du temps, et à la suite de la communication souffre constamment des retards supérieurs et déconnexions [20].

transmission. En outre, le protocole SPRING peut également atteindre la préservation conditionnelle de la vie privée et de résister à la plupart des attaques existantes dans DTNs véhicules, tels que (packet analysis attack, packet tracing attack, and black (grey) hole attacks), qui sont essentiels à la réussite de ces réseaux.

- Troisièmement, les auteurs développent un simulateur pour montrer l'amélioration substantielle du protocole SPRING en termes de fiabilité élevée, la résistance contre l'attaque du traçage du paquet et l'attaque du trou noir (gris). Les résultats de simulation démontrent son efficacité et sa sécurité.

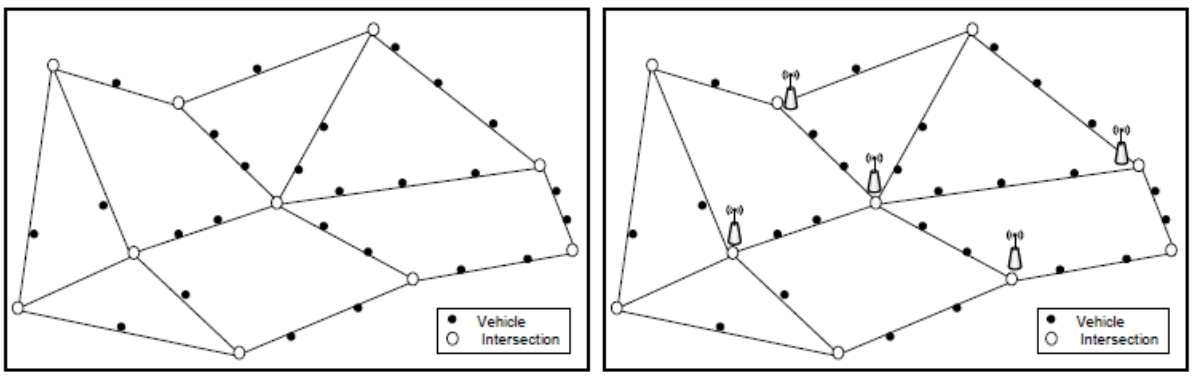
Le reste de cette section est organisé comme suit. Dans la sous section 3.1.1, nous présentons les modèles et les objectifs de conception. Ensuite, nous présentons le protocole SPRING dans la sous section 3.1.2, suivie par notre analyse à la sous section 3.1.3.

3.1.1 Modèles et objectifs de conception

Dans cette sous section, nous présentons le modèle de réseau, le modèle du nœud et le modèle de menace, et nous identifions les objectifs de conception du protocole SPRING [62].

3.1.1.1 Le modèle de réseau basé sur les graphes aléatoires

Soit un grand nombre de véhicules $\mathcal{V} = \{v_1, v_2, \dots\}$ se déplacent dans une ville cartographique en suivant l'algorithme de routage du plus court chemin. Ensuite, un véhicule DTN peut être représenté par un graphe orienté au hasard $\mathcal{G}(\mathcal{V}^*, \mathcal{E})$, comme présenté dans la figure 3.3, où $\mathcal{V}^*$ est une union entre l'ensemble des nœuds du véhicule $\mathcal{V}$ et un ensemble de noeuds d'intersection $\mathcal{C} = \{c_1, c_2, \dots\}$, i.e., $\mathcal{V}^* = \mathcal{V} \cup \mathcal{C}$, et $\mathcal{E}$ est l'ensemble des arêtes orientées au hasard entre toutes intersections $c_i, c_j \in \mathcal{C}$, où $i \neq j$.



(a) (b)

Figure 3:3 Modèle de véhicule DTN avec le déploiement RSU sociale, proposé par Ru *et al.* [20]

Le degré d'interaction du sommet $c_i \in \mathcal{C}$ est le nombre de routes avec c_i comme leur sommet terminal, et il est noté $KI_i = \sum_{j \in \mathcal{C}} \sigma_{ji}$. Out-degré d'interaction du sommet $c_i \in \mathcal{C}$ est le nombre de routes avec c_i comme sommet initial, et il est noté $KO_i = \sum_{j \in \mathcal{C}} \sigma_{i,j}$. Parce que $\sigma_{ji} = \sigma_{ij}$, nous avons $KI_i = KO_i$. Généralement, dans un graphe orienté, « in-degré » et « out-degré » d'un sommet peut capturer son impact dans l'ensemble du graphe. Cependant, dans le

graphe orienté aléatoire, l'impact d'une interaction sommet c_i est subordonné au nombre de contacts entre c_i et d'autres nœuds véhicules dans $\mathcal{V}$. A cet égard, le degré social d'interaction du sommet est introduit.

Le *degré social* d'intersection du sommet $c_i \in \mathcal{C}$ est défini comme suit

$$SD_i = \frac{\sum_{v_j \in \mathcal{V}} \delta_j (c_i)}{\sum_{v_j \in \mathcal{V}} \delta_j}$$

où δ_j est le nombre de chemins les plus courts qu'un nœud véhicule $v_j \in \mathcal{V}$ marche au cours d'une unité de temps, et $\delta_j(c_i)$ est le nombre de chemins les plus courts qui passe par l'intersection du sommet c_i.

Le *déploiement du RSUs*. Soit ST désigne le *seuil social* d'un graphe orienté aléatoire $\mathcal{G}(\mathcal{V}^*, \mathcal{E})$. L'ensemble de sommets élevés d'intersection sociaux est choisit comme suit

$$HS = \{c_i \in \mathcal{C} | SD_i \geq ST\}$$

Il est à noter qu'en ajustant le seuil social , nous pouvons déterminer la cardinalité du HS. Après la détermination du HS, un RSU R_i est placé à chaque intersection $c_i \in HS$, comme présenté dans la figure 3.3 (b). Après, chaque RSU a une capacité sociale élevée et peut effectivement aider les véhicules à stocker d'avance les paquets dans les DTNs véhicules.

3.1.1.2 Le modèle du nœud

Les véhicules DTNs sont caractérisés par deux types de nœuds DTN, à savoir, les véhicules et les RSUs, et chaque type a des caractéristiques uniques.

- *Les véhicules*: en dehors de la mobilité, chaque nœud véhicule conduit par des personnes avec des ressources limitées, i.e., les contraintes du mémoire tampon. En général, un nœud véhicule permettra de transmettre les paquets quand il a un stockage disponible. Cependant, une fois que la mémoire est insuffisante, le nœud véhicule ne sert plus le nœud relais pour aider le transfert.
- *Les unités routières (RSUs)*: différentes du nœud véhicule, chaque nœud RSU est stationnaire mais a une capacité de stockage énorme. Une fois qu'il est déployé à un carrefour, chaque nœud RSU peut aider temporairement à stocker des paquets. Cependant, comme chaque RSU est coûteux, il est impossible d'ériger des nœuds RSU à toutes les intersections, notamment au déploiement rapide des VANETs.

Soit T_R et T_V , où $T_R > T_V$, la porté de transmission du RSU et le nœud véhicule, respectivement. Ensuite, les interfaces sans fil entre les nœuds véhicules sont bidirectionnels, c'est à dire, si v_i entend la transmission de v_j, alors v_j est également capable d'entendre v_i. Cependant, les interfaces sans fil entre le nœud véhicule et le nœud RSU sont généralement unidirectionnelle, sauf s'ils sont très proches les uns des autres.

3.1.1.3 Le modèle de menace

Dans le modèle de menace proposé dans le protocole SPRING, les nœuds RSU sont dignes de confiance, et ne peuvent être compromis. Cependant, une petite fraction de nœuds véhicules pourrait être compromise. Il est considéré qu'un adversaire extérieur global (global external adversary) avec une capacité de contrôle limitée, où

- *Global* montre l'adversaire $\mathcal{A}$ à une information complète du trafic des véhicules DTN.
- *External* désigne l'adversaire $\mathcal{A}$ peut généralement seulement capturer les communications entre les nœuds DTN, mais n'a aucune idée de l'information interne stockée dans ces nœuds.
- *Limited control* signifie que l'adversaire $\mathcal{A}$ peut contrôler une très petite fraction (moins de 0,1), de nœuds véhicules pour lancer certains types d'attaques actives.

En particulier, il est considéré que l'adversaire $\mathcal{A}$ peut lancer les attaques suivantes soit pour subvertir la confidentialité ou dégrader les performances de l'ensemble du nœud véhicule DTN, ci-après :

- L'attaque d'analyse des paquets (packet analysis attack) : Après l'écoute d'un paquet, l'adversaire $\mathcal{A}$ tente d'identifier l'identité de la source par l'analyse du paquet, c'est à dire de récupérer le contenu du paquet, et en déduire la source.
- L'attaque du traçage des paquets (packet tracing attack) : L'adversaire espionne la transmission d'un seul paquet lorsqu'il traverse autour du DTN véhiculaire. De cette façon, les emplacements source et destination du paquet peuvent être tracées. Il est à noté que l'adversaire$\mathcal{A}$ n'a pas besoin de récupérer le contenu des paquets pour déduire la source et la destination des flux.
- L'attaque du trou noir (black hole attack) : Dans le véhiculaire DTN, l'adversaire $\mathcal{A}$ transmet premièrement les paquets en affirmant qu'il peut contribuer à faire progresser les véhicules de leur destination. Cependant, tous les paquets sont en fait diminué par l'adversaire $\mathcal{A}$. De toute évidence, l'attaque du trou noir est une sorte de déni de service (DoS), ce qui peut largement affecter les performances de l'ensemble des véhicules DTN, surtout quand l'adversaire $\mathcal{A}$ contrôle certains nœuds véhicules DTN compromis pour lancer l'attaque.
- L'attaque du trou grey (grey hole attack) : l'attaque trou grey est une variante de l'attaque d'un trou noir dans le véhicule DTN, où l'adversaire $\mathcal{A}$ envoie de façon sélective certains paquets, mais pas tous les paquets. Ce genre d'attaque est à peine à détecter car il est impossible de distinguer le cas de chute de paquet normal lorsque le DTN véhiculaire est pauvrement connecté.

3.1.1.4 L'objectif de conception

L'objectif de conception dans le protocole SPRING est de développer un protocole préservant la confidentialité de transmission par paquets sociale pour les véhicules DTNs. Plus précisément, le protocole SPRING atteint trois objectifs, ci-après :

- *Optimisation des véhicules DTN avec l'aide du RSU*. Dans un grand nombre de véhicules DTN, lorsque la densité de véhicule est clairsemée, la possibilité de contacter avec des nœuds véhicule du DTN est faible, ce qui entraînera le ratio de distribution faible en véhicules DTN, surtout lorsque la technique de copie unique est adoptée. Afin de prévenir la dégradation de la performance globale, les auteurs [20] introduisent le déploiement haut du RSU sociale dans les véhicules DTNs. Parce que les RSUs ont des capacités de stockage énormes, ils peuvent stocker temporairement des paquets lorsque le nœud véhicule du prochain saut n'est pas disponible.
- *Résister aux attaques liées à la confidentialité sur les nœuds véhicules DTN*. Parce les véhicules DTN sont habituellement mis en œuvre dans les scénarios civils, où les emplacements des nœuds véhicules sont étroitement liés à des citoyens qui les conduisait. Si le véhicule DTN divulgue l'information des citoyens, c'est à dire, l'identité et localisation sur la confidentialité, le véhicule DTN ne peut pas être largement accepté par le public. Par conséquent, la vie privée des citoyens doit être protégés afin d'une large adhésion du public.
- *La réalisation de la préservation conditionnelle de la confidentialité*. Si l'adversaire $\mathcal{A}$ lance l'attaque du trou noir / gris en contrôlant une petite fraction de nœuds véhicules compromis, ces attaques sont difficiles à résister, parce que ces nœuds compromis ont leurs matériaux clés valides. Par conséquent, la préservation absolue de la confidentialité est insuffisante, et la préservation de confidentialité conditionnelle est attendue. En particulier, une fois un nœud véhicule compromis lance l'attaque, une autorité de confiance (TA) doit avoir la capacité d'identifier le nœud compromis et punir selon la loi applicable.

3.1.2 Fonctionnement du protocole SPRING

Dans cette sous section, nous présentons le fonctionnement du protocole SPRING [62], qui se compose principalement de deux phases: la phase d'initialisation du système et la phase de transfert de paquets RSU assistée par l'opportunisme.

3.1.2.1 La phase d'initialisation du système

Supposons qu'il existe une autorité de confiance dans le système, qui initialise l'ensemble du système. Soit le paramètre de sécurité k et les paramètres bilinéaires $(n, g, \mathbb{G}, \mathbb{G}_T, e)$ généré par $\mathcal{CG}en(k)$. Le TA commence à choisir deux éléments $(g, u) \in \mathbb{Z}_n^*$, h un générateur du $\mathbb{G}_q$, deux exposants aléatoires $\alpha, a \in \mathbb{Z}_n^*$, une fonction de hachage résistante aux collisions $H : \{0,1\}^* \to \mathbb{Z}_n^*$, et un algorithme de chiffrement symétrique sécurisé $Enc()$. Après ceux-ci, le TA fixe la clé principale (g^α, a, q) et les paramètres publics du système

$$params = (\mathbb{G}, \mathbb{G}_T, e, n, g, u, e(g,g)^\alpha, A = g^\alpha, h, H, Enc()).$$

Pour chaque véhicule $v_i \in \mathcal{V} = \{v_1, v_2, \dots\}$, le TA choisit un nombre aléatoire $x_i \in \mathbb{Z}_n^*$ de telle sorte que $a + x_i \neq 0$ comme la clé secrète, et calcule $A_i = g^{\frac{1}{a+x_i}} \in \mathbb{G}$, $B_i = \mathrm{g}^{x_i} \in \mathbb{G}_T$, où $\mathrm{g} = e(g,g)$. Puis, le TA autorise $B_i \in \mathbb{G}_T$ comme la clé publique du v_i.

Pour un domaine spécifique, le TA enquête premièrement sur l'ensemble de nœuds d'intersection $\mathcal{C} = \{c_1, c_2, ...\}$ et calcule le degré social SD_j du chaque intersection c_j. Puis, en fixant un seuil social ST, le TA dérive un ensemble de nœuds de haute intersection sociaux $HS = \{c_j \in \mathcal{C} | SD_j \geq ST\}$. A chaque intersection sociale élevée, le TA place un RSU et autorise une clé secrète $x_j \in \mathbb{Z}_n^*$ et la clé publique correspondante $C_j = \mathrm{g}^{x_j} \in \mathbb{G}_T$ pour le RSU. Il est à noté que la clé publique C_j ici est associé avec l'intersection c_i attesté avec le certificat délivré par le TA.

3.1.2.2 La phase de transfert de paquets RSU assistée par l'opportunisme

Supposons que le nœud source v_1 va envoyer un message sensible $m \in \mathbb{G}_T$ au nœud destination v_2, où la localisation L_2 du v_2 est supposée fixe et connue par v_1 . Pour s'acquitter de cette transmission de paquets sensibles dans les véhicules DTN, les étapes suivantes seront exécutées.

- **Etape (1)** : Le nœud source premièrement utilise la clé publique du nœud destination $B_2 = \mathrm{g}^{x_2}$ et deux nombres aléatoires $k_0, k_1 \in \mathbb{Z}_n^*$ pour encrypter le message m comme suit

$$M = (\alpha_0, \beta_0, \alpha_1, \beta_1) = (m.B_2^{k_0}, \mathrm{g}^{k_0}, B_2^{k_1}, \mathrm{g}^{k_1}) \qquad (3.3)$$

- **Etape (2)** : Quand un passage par le nœud véhicule v_i est prêt à aider la transmission du message M, le nœud source v_1 et le nœud v_i vont exécuter les opérations interactives suivantes.
  - Le véhicule v_i premièrement obtient l'horodatage actuel T_i et calcule g^{x}, où x est aléatoirement choisi dans $\mathbb{Z}_n^*$. Puis, v_i utilise la technique CPPA[13] [63] pour construire CPPA($T_i||\mathrm{g}^{\mathrm{x}}$) et l'envoyer au nœud source v_1.
  - Après la vérification de la validité du CPPA($T_i||\mathrm{g}^{\mathrm{x}}$) , v_1 choisi un autre nombre aléatoire $y \in \mathbb{Z}_n^*$, encrypte l'emplacement du destination L_2 comme $D = (\alpha_2, \beta_2) = (L_2.\mathrm{g}^{\mathrm{xy}}, \mathrm{g}^{\mathrm{y}})$, et envoie $M||D$ vers le véhicule de passage v_i.
  - Après la réception de l'emplacement du destination L_2 depuis $D = (\alpha_2, \beta_2)$ comme $\frac{\alpha_2}{\beta_2} = \frac{L_2.\mathrm{g}^{\mathrm{xy}}}{\mathrm{g}^{\mathrm{xy}}} = L_2$, le véhicule de passage v_i essaie de son mieux pour aider à transmettre le message M proche du destination.

- **Etape (3)** : Une fois le véhicule v_i porte le message M pour une période de temps, la destination L_2 n'est plus sur la voie du véhicule v_i. Ensuite, v_i invoque l'algorithme 3.1

[13] La technique d'authentification de préservation de la confidentialité conditionnelle (The Conditional Privacy-preserving Authentication (CPPA)) est une sorte de signature de groupe, qui est dédié aux communications véhiculaires pour réaliser l'authentification préservant la confidentialité conditionnelle.

procedure PACKET FORWARDING
    when the vehicle node v_i thinks it cannot help carrying message packet M any more, it will first set a *holding time to wait next-hope node* (T_h) and try to forward M to the next-hop DTN node within T_h
    if v_i detects an RSU located in a nearby intersection **then**
        v_i will drive close and forward the message M to the RSU
    else if v_i detects an available vehicle node v_j nearby **then**
        v_i will forward the message M to v_j
    else if no next-hop node is available **then**
        the message M has to be discarded
    end if
end procedure

Algorithme 3:1 Transmission des paquets dans les véhicules DTN [20]

pour transmettre le message M à un approprié du prochain saut. Parce que T_R la portée de transmission du RSU est large que la portée de transmission du véhicule T_V et s'il existe un RSU à un carrefour à proximité sur son chemin, le véhicule v_i peut premièrement le détecter. Ensuite, v_i conduira à proximité du RSU et transférera le message M avec la communication V-2-I.

- **Etape (4)** : Si le message $M = (\alpha_0, \beta_0, \alpha_1, \beta_1)$ n'est pas tombé, il finira par être relayé au nœud destination v_2 dans l'emplacement L_2. Ensuite, le nœud destination v_2 peut utiliser ses clés secrètes x_2 pour récupérer m par les opérations suivantes :

$$m_0 = \frac{\alpha_0}{{\beta_0}^{x_2}}, \qquad m_1 = \frac{\alpha_1}{{\beta_1}^{x_2}} \tag{3.4}$$

Si $m_0 \neq 1$ et $m_1 = 1$, le nœud destination accepte m_0 comme un texte en clair valide m ; sinon, le message $M = (\alpha_0, \beta_0, \alpha_1, \beta_1)$ est invalide et il sera rejeté.

Exactitude (Correctness). Supposons que $M = (\alpha_0, \beta_0, \alpha_1, \beta_1)$ est temporairement conservé à RSU qu'une seule fois, et il a la forme $(m \cdot B_2^{k_0+k_1.k_0'}, g^{k_0+k_1.k_0'}, B_2^{k_1.k_1'}, g^{k_1.k_1'})$. Après,

$$\frac{\alpha_0}{{\beta_0}^{x_2}} = \frac{m \cdot B_2^{k_0+k_1.k_0'}}{(g^{k_0+k_1.k_0'})^{x_2}} = m; \frac{\alpha_1}{{\beta_1}^{x_2}} = \frac{B_2^{k_1.k_1''}}{g^{k_1.k_1''}} = 1 \tag{3.5}$$

Si $M = (\alpha_0, \beta_0, \alpha_1, \beta_1)$ a été stocké dans RSUs plus d'une fois, avec une simple déduction, l'exactitude de récupérer le texte en clair m peut également être vérifiée.

3.1.3 Analyse du protocole SPRING

Le protocole SPRING peut résister à quatre types d'attaques, i.e., l'attaque d'analyse des paquets, l'attaque du traçage des paquets, l'attaque du trou noir; et l'attaque du trou grey.

- Le nœud source v_1 a encrypté le message sensible m dans $M = (\alpha_0, \beta_0, \alpha_1, \beta_1)$. Sans connaitre la clé secrète x_2 du nœud destination v_2, l'adversaire ne peut pas récupérer m avec l'analyse du paquet. En outre, parce que le protocole CPPA d'authentification

est adopté, aucune information sur l'identité ne sera divulguée. Donc, le protocole SPRING proposé peut résister à l'attaque de l'analyse des paquets.

- Parce que la destination est encryptée dans chaque intersection, l'adversaire ne peut pas savoir l'information de la destination. En outre, dans le protocole SPRING proposé, depuis que le RSU est placé dans les intersections du « *high social* », un grand nombre de véhicules passent et certains paquets seront temporairement enregistrés dans RSU, le RSU peut naturellement servir comme un mix serveur. Puis, pour un paquet de message spécifique, uniquement s'il a été temporairement enregistré dans le RSU « *high social* » au moins une fois, l'adversaire ne peut pas tracer par l'écoute. Donc, le protocole SPRING proposé peut résister à l'attaque du traçage des paquets.

procedure BLACKGREYHOLEATTACKDECTION
With the chain tracking in Fig. 3.5, the TA can obtain each vehicle node v_i's packet dropping number, denoted as X_i.
Compute the mean $\overline{X}$ of all vehicle nodes $\mathcal{V} = \{v_1, v_2, \cdots\}$ as $\overline{X} = \frac{1}{|\mathcal{V}|}\sum_{i=1}^{|\mathcal{V}|} X_i$, where $\mathcal{V}$ is the cardinality of $\mathcal{V}$.
Compute the distance of each X_i to the mean $\overline{X}$ as $d(X_i) = |X_i - \overline{X}|$.
Define the thresholds T_B, T_G for black hole attack and grey hole attack, respectively.
for each vehicle node $v_i \in \mathcal{V} = \{v_1, v_2, \cdots\}$ **do**
  if $d(X_i) > T_B$ **then**
    v_i is considered as a black hole attacker.
  else if $d(X_i) > T_G$ **then**
    v_i is considered as a grey hole attacker.
  else
    v_i is considered as a normal vehicle node.
  end if
end for
end procedure

Algorithme 3:2 La détection des attaques du trou noir (grey) [20]

- A cause du protocole d'authentification CPPA, les attaques du trou noir (grey) lancées par un adversaire externe peut résister dans le protocole SPRING proposé. Comme présenté dans l'algorithme 3.1, si aucun nœud de prochain saut n'est pas disponible, le paquet de messages peut également être diminué. Par conséquent, le processus de détection dans l'algorithme 3.2 proposé dans le protocole SPRING où les nœuds qui ont lancé les attaques des trous noir (grey) peuvent être identifiés. De plus, dans l'algorithme 3.2, les seuils T_B et T_G doivent être soigneusement défini. Sinon, faux positifs et faux négatifs pourrait être élevés.
- Les auteurs du protocole SPRING ont évalué l'effet de la détection où ils ont considéré 4 attaquants du trou noir et un attaquant du trou grey (avec une probabilité de chute de paquets (PDP) = 50%) parmi le total des 50 nœuds véhicules dans les simulations. Les résultats ont montrés que , i) quand plusieurs RSUs sont déployés, le moyen d'événement chuté va diminuer ; ii) le déploiement RSU basé sur la relation social est faiblement moyenne dans les évènements de chutes que dans le déploiement RSU aléatoire. Cependant, avec le bon choix des seuils appropriés T_B et T_G dans l'algorithme 3.2, les attaquants du trou noir (grey) peuvent être détectés.

3.2 Le protocole SPF

Comme nous avons vu dans la section précédente, le protocole SPRING peut non seulement améliorer la fiabilité avec les communications V-2-V et V-2-I, mais aussi atteindre la préservation conditionnel de l'identité véhicule et résister aux attaques des trous noirs (gris) dans la transmission de paquets. Cependant, l'emplacement de la destination est supposé fixe et connu à la source, dans le protocole SPRING, et comme résultat, l'emplacement de la vie privée du récepteur n'est pas protégée. A cet égard, les auteurs du protocole SPRING ont étudié comment protéger la confidentialité de l'emplacement du récepteur dans la demande de transfert de paquets et ont proposé le protocole SPF [64].

Le lieu (l'emplacement) de la confidentialité est une des conditions importantes de la confidentialité dans VANET depuis que les emplacements des véhicules sont étroitement liés aux pilotes. Cependant, si le réseau VANET ne protège pas la confidentialité de l'emplacement du véhicule, il ne peut pas être accepté par le public. Dans [64], Lu et *al.* proposent un protocole efficace basé sur la transmission de paquets *socialspot*, appelé SPF, où les *socialspots* sont désignés comme les emplacements dans un environnement urbain que de nombreux véhicules se rendent souvent comme un centre commercial, un restaurant ou un cinéma. Ce protocole se base sur la technique « Sacrificing the Plum Tree for the Peach Tree[14] ». Depuis les socialspots sont généralement faibles et sensibles aux véhicules, les auteurs ont utilisé le socialspot comme un nœud relais pour la transmission de paquets. De cette manière, la performance de livraison de paquets peut être considérablement améliorée. En attendant, puisque de nombreux véhicules visitent le même socialspot, le socialspot ne peut pas être utilisé pour tracer d'autres sites sensibles d'un véhicule spécifique. Par conséquent, la tactique socialspot peut protéger la confidentialité de l'emplacement du véhicule dans VANETs. Plus précisément, les contributions de cette proposition sont de deux ordres.

- Premièrement, basé sur la technique « socialspot », les auteurs proposent un protocole efficace SPF visant à l'application de transfert de paquets dans VANETs, et aussi procéder à l'analyse complète de sécurité pour valider sa sécurité afin de protéger la confidentialité de l'emplacement du récepteur dans VANETs.
- Deuxièmement, les auteurs ont développé un simulateur personnalisé construit en Java pour examiner la performance du protocole SPF proposé. Les résultats des simulations approfondies montrent que la stratégie socialspot peut obtenir de bonnes performances de transmission de paquets en termes de taux de livraison de paquets et de retard moyen dans VANETs.

Le reste de cette section est organisé comme suit. Dans la sous section 3.2.1, nous présentons les modèles et les objectifs de conception. Ensuite, nous présentons le fonctionnement du protocole SPF dans la sous section 3.2.2, suivie l'analyse du protocole à la sous section 3.2.3.

[14] "Sacrificing the Plum Tree for the Peach Tree" est l'un des trente-six stratégies de la chine ancienne, ce qui signifie sacrifier quelque chose de non-critique afin d'assurer l'intérêt général.

3.2.1 Modèles et objectifs de conception

Dans cette sous section, nous présentons le modèle du système, le modèle de confidentialité, et les objectifs de conception.

3.2.1.1 Le modèle du système

Dans [64], Ru *et al.* considèrent un réseau VANET contenant une autorité de confiance TA, un grand nombre de véhicules et quelque *socialspots* dans un environnement urbain, comme présenté dans la figure 3.4.

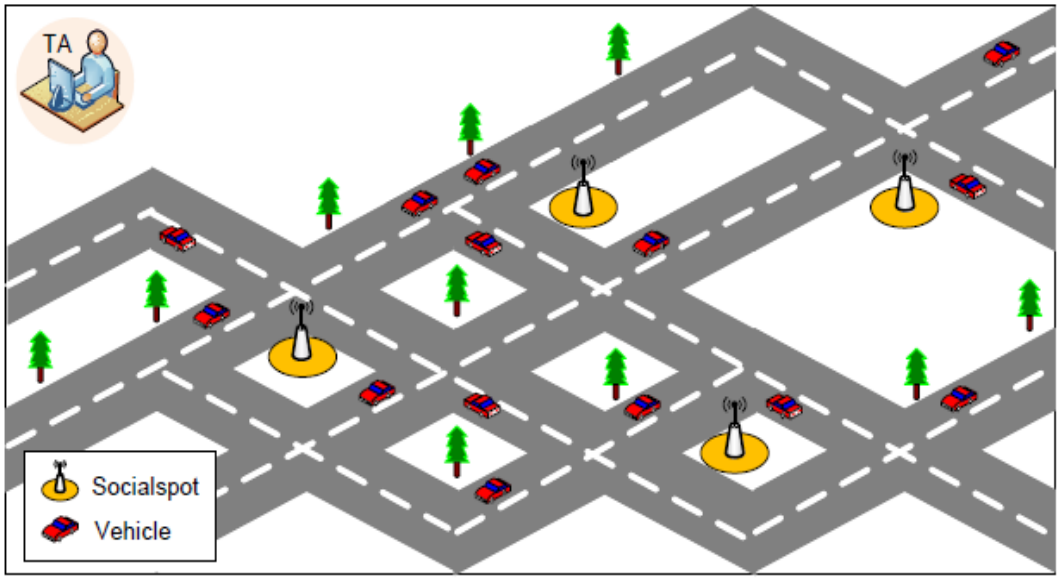


Figure 3:4 Le modèle du système sous considération pour SPF, proposé par Ru *et al.* [64]

- L'autorité de confiance (TA) : Le TA est une entité de confiance et puissante, dont les fonctions comprennent l'initialisation du système, le déploiement du RSUs à certains socialspots, et l'immatriculation des véhicules par l'octroi d'une famille de pseudo-IDs et les clés correspondantes.
- Les socialspots $S = \{ss_1, ss_2, \cdots\}$: Les socialspots sont désignés comme les lieux où de nombreux véhicules vont visiter, par exemple, un centre commercial, un restaurant ou un cinéma.
- Les véhicules $V = \{V_1, V_2, \cdots\}$: Chaque véhicule $V_i \in V$ est équipé avec l'appareil OBU qui leur permet de communiquer les uns avec les autres ainsi que les unités d'actions restreintes aux socialspots pour la livraison de paquets coopératifs dans VANET.

3.2.1.2 Le modèle du système

Dans le modèle de confidentialité proposé dans [64], les auteurs considèrent comment protéger la vie privée de localisation d'un récepteur du véhicule contre l'adversaire externe, global, et passive $\mathcal{A}$, où l'adversaire $\mathcal{A}$ ne peut pas compromettre les RSUs ou les véhicules, mais il a une vue complète d'écoute de tous les paquets transitaires dans VANET. Il est à noté que

l'adversaire $\mathcal{A}$ peut lancer des attaques actives telles que l'attaque du trou noir, l'attaque du trou gris pour dégrader les performances dans la demande de livraison de paquets coopérative.

3.2.1.3 Les objectifs de conception

Avec l'utilisation de la stratégie socialspot, l'objectif principal du protocole SPF est la protection de la confidentialité de l'emplacement du récepteur dans VANETs. Plus précisément, car tous les endroits dans la trajectoire $\mathrm{Tr}_i = \{\mathrm{tr}_1, \mathrm{tr}_2, \cdots\}$ d'un véhicule V_i sont sensible à cela, il est possible de révéler un socialspot non sensible que V_i rend souvent comme un nœud de relais stationnaire de sorte que la performance de livraison de paquets peut être améliorée. Dans le même temps, puisque de nombreux véhicules se rendent souvent dans le même socialspot, le RSU au socialspot peut servir de serveur de mélange (a mix server), alors l'adversaire $\mathcal{A}$ ne peut pas lier un paquet spécifique à son récepteur.

3.2.2 Fonctionnement du protocole SPF

Dans cette partie, nous présentons la technique socialspot puis le fonctionnement du protocole SPF.

3.2.2.1 La technique socialspot

Dans la réalité, les emplacements dans le trajet du conducteur sont presque fixés. Par exemple, un conducteur peut souvent conduire vers son domicile, à l'école, ou à un centre commercial. Comme pour un conducteur, de son domicile et l'école pourraient être des lieux de la vie privée, qui sont sensibles à lui, tandis que le centre commercial est un socialspot, qui n'est généralement pas pris en charge. Cependant, il est possible d'appliquer la technique « Sacrificing the Plum Tree for the Peach Tree » pour révéler le socialspot d'un récepteur comme un nœud de relais stationnaire pour améliorer les performances de transmission de paquets dans VANET tout en protégeant les autres endroits de la vie privée du récepteur, comme indiqué dans la figure 3.5.

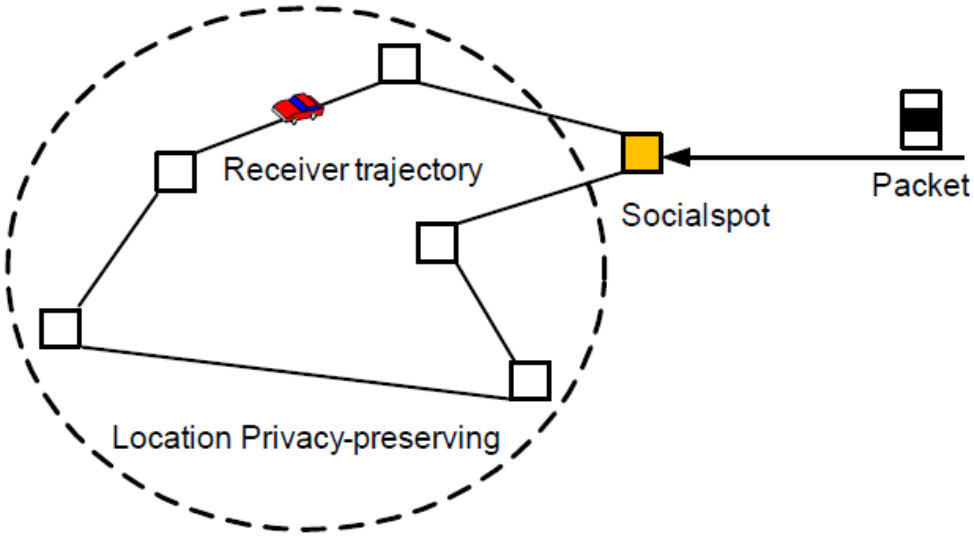


Figure 3:5 La technique socialspot pour améliorer le rendement de la transmission de paquets, proposé par Ru *et al.* [64]

3.2.2.2 La description du protocole SPF

Le protocole SPF se compose de quatre phases: la phase d'initialisation du système, la phase de génération des paquets, la phase de transfert des paquets et la phase de réception des paquets.

La phase d'initialisation du système

Dans la phase d'initialisation du système, le TA premièrement configure les paramètres du système, choisi les scialspots dans un environnement de centre-ville, et enregistre les véhicules dans le système. Plus précisément, le TA exécute les étapes suivantes.

Etape(1). Soit le paramètre de sécurité k, les paramètres bilinéaires $(\mathbb{G}, \mathbb{G}_T, e, P, q)$ sont d'abord généré en exécutant $\mathcal{G}en(k)$, où $e: \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$, P est le générateur de $\mathbb{G}$ et q est le grand nombre premier avec $|q| = k$. Après, le TA choisi un élément aléatoire $Q \in \mathbb{G}$, et un nombre aléatoire $s \in \mathbb{Z}_q^*$ comme la clé master, et calcule la clé publique du système correspondante $P_{pub} = sP$. Aussi, le TA choisi deux fonctions de hachages cryptographiquement sécurisées $\boldsymbol{Enc}()$**.** A la fin, le TA définit les paramètres publics du système $(\mathbb{G}, \mathbb{G}_T, e, P, q, Q, P_{pub}, \mathcal{H}_0, \mathcal{H}_1, Enc())$.

Etape(2). Le TA choisi l'ensemble de socialspots $S = \{ss_1, ss_2, \cdots\}$dans un environnement urbain. Après , à chaque socialspot $ss_i \in S$, un stockage énorme de RSU est placé, qui peuvent être identifiés en passant par les véhicules.

Etape(3). Supposons que la trajectoire d'un véhicule $V_i \in V$ est $\mathrm{Tr}_i = \{\mathrm{tr}_1, \mathrm{tr}_2, \cdots\}$ et que $\mathrm{Tr}_i \cap S \neq \emptyset$, i.e., au moins il existe un endroit $\mathrm{tr_a} = ss_b$, avec $\mathrm{tr_a} \in \mathrm{Tr}_i$ et $ss_b \in S$. Quand V_i enregistre lui-même, il affirme son identité et le socialspot ss_b au TA. Ensuite, le TA accorde une famille de pseudo-ID $\mathrm{PID} = \{\mathrm{pid}_0, \mathrm{pid}_1, \cdots\}$ et les clés correspondantes pour V_i en invoquant l'algorithme 3.3. De cette manière, V_i peut utiliser pid_0 au socialspot ss_b et changer constamment ses pseudo-ID $\mathrm{pid_j} \in \mathrm{PID},\ \mathrm{j} \geq 1$.

1: **procedure** VEHICLEREGISTRATION
Input: a vehicle $V_i \in \mathcal{V}$ and a socialspot $\mathrm{ss}_b \in \mathcal{S}$
Output: a family of pseudo-IDs and the corresponding pseudo-ID based key materials
2: choose a family of unlinkable pseudo-IDs $\mathrm{PID} = \{\mathrm{pid}_0, \mathrm{pid}_1, \cdots\}$
3: compute the private key $S_0 = \frac{1}{s+\mathcal{H}_0(\mathrm{pid}_0 \| \mathrm{ss}_b)} Q$ with respect to the pseudo-ID $\mathrm{pid}_0 \in \mathrm{PID}$ and the socialspot ss_b
4: **for** other pseudo-ID $\mathrm{pid}_j \in \mathrm{PID}$, $j \geq 1$ **do**
5: compute the corresponding private key $S_j = \frac{1}{s+\mathcal{H}_0(\mathrm{pid}_0)} Q$
6: **end for**
7: **return** all tuples (pid_j, S_j) to V_i
8: **end procedure**

Algorithme 3:3 L'algorithme d'enregistrement du véhicule, proposé par Ru *et al.* [64]

La phase de génération des paquets

Supposons qu'une source fixe veut envoyer un message M à un véhicule $V_i \in V$ dans un environnement urbain et que la source ne connaît pas l'emplacement exact de V_i, la source exécute les étapes suivantes pour générer le paquet sur M.

Etape(1). La source choisit premièrement le nombre aléatoire $x \in \mathbb{Z}_q^*$, et calcule $k = e(P,Q)^x$, et C_1, C_2, C_3 où

$$\begin{cases} C_1 = x(P_{pub} + \mathcal{H}_0(\mathrm{pid}_0||ss_b)P) \\ C_2 = \mathcal{H}_1(k||0), C_3 = \mathrm{Enc}(k, M) \end{cases}$$

(C_1, C_3) est un texte chiffré du chiffrement basé sur l'identité anonyme (identity-based encryption), qui donc peut atteindre l'anonyme de l'identité du récepteur.

Etape(2). La source emballe le paquet $\mathcal{P}$ avec le format comme présenté dans la figure 3.6, où Head := C_1, Auth := C_2, Encrypted-Payload := C_3, et Socialspot := ss_b, et attend des véhicules pour aider à transférer le paquet $\mathcal{P}$ à ss_b.

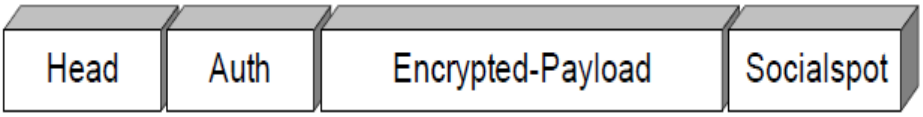


Figure 3:6 Le format de paquet dans le protocole SPF, proposé par Ru *et al.* [64]

La phase de transfert des paquets

Dans cette phase, la source demandera au véhicule passant pour aider à la réalisation du paquet $\mathcal{P}$ au socialspot ss_bou d'autres socialspots près du ss_b. Plus précisément, la source invoque l'algorithme 3.4 pour transférer le paquet $\mathcal{P}$.

1: **procedure** PACKETFORWARDING
2: When a vehicle is passing-by the source, the source asks for the help. If vehicle can forward $\mathcal{P}$ to ss_b or other socialspots close to ss_b, the source forwards $\mathcal{P}$ to the vehicle.
3: **end procedure**

Algorithme 3:4 L'algorithme de transfert du paquet, proposé par Ru *et al.* [64]

Si le paquet $\mathcal{P}$ est transmis avec succès au socialspot ss_b, cette phase est terminée. Sinon, lorsque le paquet est transmis à d'autres socialspots proche de ss_b, alors le RSU au socialspot sera temporairement stocker le paquet $\mathcal{P}$, et aussi invoque l'algorithme 3.4 pour aider à transférer $\mathcal{P}$ à ss_b.

La phase de réception des paquets.

Une fois le paquet $\mathcal{P}$ atteint le socialspot ss_bet est stocké dans le RSU, le véhicule V_i peut ramasser le paquet $\mathcal{P}$ par les étapes suivantes.

Etape(1). Le véhicule V_i établit premièrement un canal sécurisé avec le RSU par les interactions suivantes, comme présenté dans la figure 3.7.

- V_i envoie son pseudo-ID pid_0 au RSU ;
- Le RSU choisit un nombre aléatoire $r \in \mathbb{Z}_q^*$, calcule la clé de session $\text{sk} = e(P,Q)^r$, et envoie le défi $\text{Cha} = r(P_{pub} + \mathcal{H}_0(\text{pid}_0||ss_b)P)$ au V_i ;
- Après la réception du défi Cha , V_i calcule premièrement $\text{sk}' = \text{e}(\text{S}_0, \text{Cha})$, et la réponse $\text{Res} = \text{Enc}(\text{sk}', T)$, où T est le nombre aléatoire avec le significatif l bits $[T]_l = 0^l$, et après envoie Rep à RSU.
- Dès la réception de la réponse Res, le RSU récupère T depuis Res, et vérifie que le significatif l bits $[T]_l ? = 0^l$. S'il est vrai, V_i est authentifié ; et le canal sécurisé avec la clé de session $\text{sk} = \text{e}(\text{P}, \text{Q})^{\text{r}}$ est établit. Le correctness est comme suit

$$\begin{aligned}\text{sk}' &= e(\text{S}_0, \text{Cha}) \\ &= e(r(P_{pub} + \mathcal{H}_0(\text{pid}_0||ss_b)P, \frac{1}{s + \mathcal{H}_0(\text{pid}_0||\text{ss}_\text{b})} Q) \\ &= e(P,Q)^r = \text{sk}\end{aligned}$$

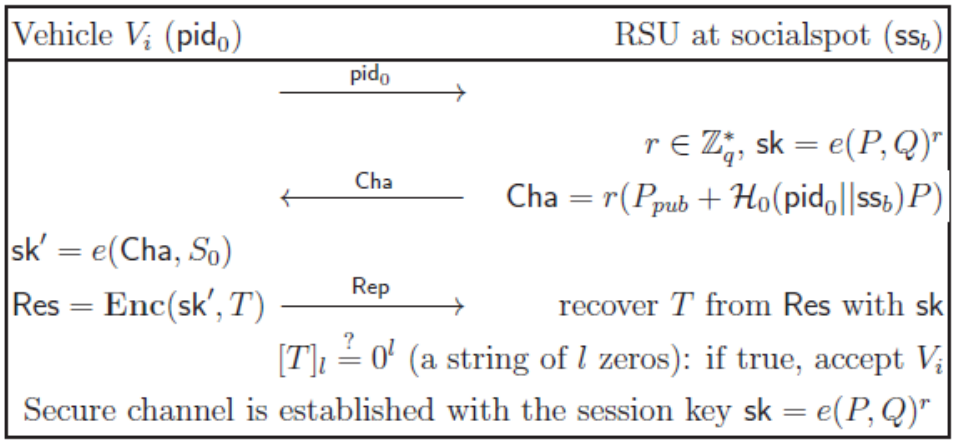


Figure 3:7 L'établissement d'un canal sécurisé entre V_i et un RSU de confiance, proposé par Ru *et al.* [64]

Etape(2). Une fois que le canal sécurisé est établi, le véhicule V_i prend chaque paquet Head et Auth depuis RSU par la verfication de la relation

$$\text{Auth} = C_2 ? = \mathcal{H}_1(k'||0), \text{ où } k' = e(\text{Head}, \text{S}_0)$$

Si la relation est vraie, V_i prend le paquet de Encrypted-Payload depuis RSU et récupère le message M avec k' depuis le encrypted-payload $C_3 = \mathrm{Enc}(k, M)$. Le correctness est comme suit

$$\begin{aligned} \mathrm{k}' &= e(\mathrm{Head}, S_0) \ = \mathrm{e}(C_1, S_0) \\ &= e(x(P_{pub} + \mathcal{H}_0(\mathrm{pid}_0||ss_b)P, \frac{1}{s + \mathcal{H}_0(\mathrm{pid}_0||\mathrm{ss_b})} Q) \\ &= e(P, Q)^r = \mathrm{k} \end{aligned}$$

De cette façon, le message M est reçu avec succès par le récepteur V_i, et le protocole SPF se termine. Il est à noter que, parce que le récepteur V_i est mobile, quand V_i veut changer l'emplacement de la source stationnaire, V_i peut aussi établir un canal sécurisé avec la source et il obtient directement le message M .

3.2.3 L'analyse du protocole SPF

Le protocole SPF peut protéger la confidentialité de l'identité du récepteur et peut aussi protéger la confidentialité de la session du récepteur.

- Depuis Head et $\mathrm{Encrypted} - \mathrm{Payload}$ dans le paquet $\mathcal{P}$ est (C_1, C_3) , où

$$\begin{cases} C_1 = x(P_{pub} + \mathcal{H}_0(\mathrm{pid}_0||ss_b)P) \\ C_3 = \mathrm{Enc}(k, M) \end{cases}$$

  est un texte chiffré du chiffrement basé sur l'identité anonyme, (C_1, C_3) est prouvablement sécurisé et ne divulguera pas l'identité du récepteur. Au même temps, le Auth est $C_2 = \mathcal{H}_1(k||0)$, où $k = e(P, Q)^x$ est aussi relative à l'identité du récepteur pid_1. A l'égard de ces deux raisons, le paquet $\mathcal{P}$ peut protéger la confidentialité de l'identité du récepteur, qui est nécessaire pour protéger la confidentialité de l'emplacament du récepteur.
- Parce que le RSU est déployé au socialspot, il stockera les paquets de nombreux véhicules. Si la clé de session est sécurisée, il est difficile pour un adversaire de lier un paquet à un récepteur. Basé sur le DBDH hypothèse (the DBDH assumption[15]), Ru *et al.* ont prouvé la clé de session $\mathrm{sk} = e(P, Q)^r$ est sémantiquement sécurisé, qui sert comme la condition nécessaire à la confidentialité de la session du récepteur.
- Ru *et al.* [64] ont évalué les performances du protocole SPF utilisant un simulateur personnalisé construit en Java. Les indicateurs de performance calibrés à l'évaluation sont le taux moyen de livraison de paquets(DR) et le retard moyen des paquets (AD), où le DR est défini comme le taux moyen des paquets réussit à atteindre leurs destinations par rapport à ceux générés par les sources dans un laps de temps donné, et le AD est défini comme le moyen entre le moment où un paquet est généré à la source et lors de sa livraison avec succès à sa destination. Les résultats montrent :

[15] Decisional Bilinear Diffie-Hellman assumption

- Qu'avec l'augmentation du temps, le DR augmentera en conséquence. Quand le nombre de socialspots S est fixe, le DR dans $N = 80$ est supérieure à celle dans $N = 40$. La raison est que, quand plusieurs véhicules se déplacent dans la région, plus de paquets peuvent être effectués aux socialspots, puis les récepteurs peuvent obtenir leurs paquets quand ils visitent les socialspots. Par conséquent, quand le nombre de véhicule N est fixé, le DR dans le cas $S = 5$ est plus faible que dans le cas $S = 3$ au stade initial et sera plus élevé à la fin du stade. La raison de ces phénomènes est qu'au stade initial, le nombre de génération des paquets est faible, moins de paquets doivent être effectués aux socialspots. Quand $S = 5$, les récepteurs ont une fréquence inférieure à visiter les socialspots pour ramasser leurs paquets. En outre, le DR est inférieur à celui dans le cas $S = 3$. Cependant, à la fin de l'étape, le nombre de paquets générés est plus grand. Quand $S = 5$, les véhicules peuvent transporter plus de paquets aux socialspots. En conséquence, lorsque les récepteurs visitent les socialspots, ils peuvent recevoir plus de paquets. Donc, le DR est plus grand que celle dans le cas $S = 3$.
- Qu'avec l'augmentation du temps, le AD sera également augmenté, mais le retard accru peut améliorer le DR. Lorsque le nombre de socialspots S est fixé, 80 véhicules peuvent transporter des paquets plus rapidement aux socialspots que 40 véhicules. En conséquence, le AD dans le cas $N = 80$ est inférieure à celle dans le cas $N = 40$. Pendant ce temps, lorsque le nombre de véhicules N est fixé, les véhicules devront visiter plus de sites en $S = 5$ que dans le cas $S = 3$. Enfin, le AD dans $S = 3$ est inférieure à celle dans le cas $S = 5$, mais le DR correspondant est également plus faible.

Comme résultat de ce protocole SPF [64] par rapport au protocole précédant SPRING [62], le protocole SPF considère le modèle de mobilité plus réaliste, qui non seulement protège la vie privée de l'emplacement du récepteur, mais aussi améliore la performance de livraison de paquets. Dans les deux sections suivantes, nous examinons le protocole PCS [65] et le protocole FLIP [66] proposé par Ru *et al.*

3.3 Le protocole PCS

Dans le protocole SPF [64], chaque véhicule possède une famille de pseudo-IDs, l'une est publique et utilisée à la tache sociale pour recevoir efficacement les paquets, et d'autres sont constamment modifiées par le véhicule pour atteindre la vie privée d'identité et son emplacement. Les auteurs de ce protocole considéré ceci : « *Quand et où le véhicule change ces pseudo-IDS? Et est ce qu'il est en train de changer les pseudonymes efficaces ?* » . Pour répondre à ces deux questions, les auteurs ont proposé un protocole de pseudonyme efficace d'évolution à la stratégie de socialespots afin d'atteindre la confidentialité de l'emplacement de haut niveau [65].

Parce qu'un véhicule utilise les différents pseudonymes sur la route, l'unlinkability des pseudonymes ne peut pas garantir la confidentialité du lieu d'un véhicule. Cependant, si le véhicule change ses pseudonymes dans une occasion incorrecte ; changer les pseudonymes n'a

aucune utilité pour protéger la confidentialité de l'emplacement, car un adversaire peut toujours associer un nouveau pseudonyme avec l'ancien. Comme présenté dans la figure 3.8,

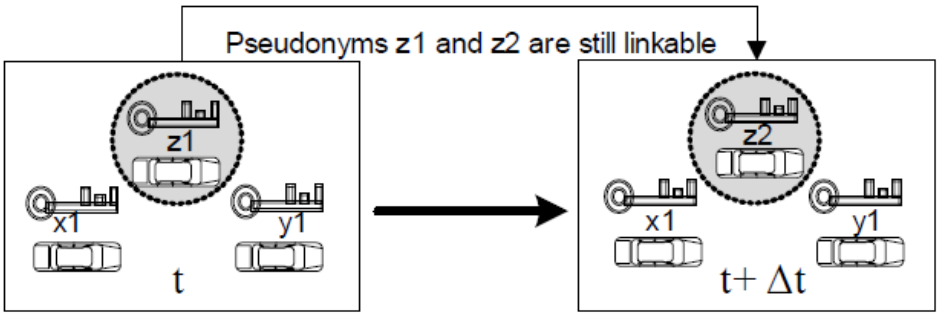


Figure 3:8 Le lien pseudonyme en raison de l'évolution des pseudonymes à l'occasion incorrect, proposé par Ru *et al.* [65]

lorsque trois véhicules sont exécutés sur la route, si un véhicule change ses pseudonymes pendant Δt , un adversaire peut encore suivre le lien de pseudonymes. Même si les trois véhicules changent leurs pseudonymes simultanément, l'emplacement et la vitesse intégrée dans les messages de sécurité pourraient encore fournir un indice à l'adversaire pour relier les pseudonymes, faisant de la protection de la vie privée échouer. Par conséquent, il est impératif d'exploiter l'exactitude de la confidentialité de l'emplacement réalisée par un changement fréquent des pseudonymes dans les VANETs. Soit $\vec{F} = \{F_1, F_2, F_3, \cdots\}$ peut représenter les facteurs $\{\text{Temps}, \text{Emplacement}, \text{Vitesse}, \cdots\}$. Dans certains cas spécifiques, un adversaire a la capacité de contrôler un sous-ensemble $\vec{F}_n = \{F_1, F_2, F_3, \cdots, F_n\} \subset \vec{F}$ et l'utiliser pour identifier le processus de changement d'un pseudonyme du véhicule. Supposons $\overrightarrow{b_0} = (x_1, x_2, x_3, \cdots, x_n)$ et $\overrightarrow{b_1} = (y_1, y_2, y_3, \cdots, y_n)$ sont les vecteurs caractéristiques de pseudonyme de deux véhicules changeant des processus observés par un adversaire. Ensuite, la similarité cosinus basée entre $\overrightarrow{b_0}$ et $\overrightarrow{b_1}$ peut être donnée par :

$$\cos\left(\overrightarrow{b_0}, \overrightarrow{b_1}\right) = \frac{\overrightarrow{b_0} \odot \overrightarrow{b_0}}{\left|\overrightarrow{b_0}\right| \cdot \left|\overrightarrow{b_1}\right|} = \frac{\sum_{i=1}^{n} x_i \cdot y_i}{\sqrt{\sum_{i=1}^{n} {x_i}^2} \cdot \sqrt{\sum_{i=1}^{n} {y_i}^2}}$$

Évidemment, quand $\overrightarrow{b_0}$ et $\overrightarrow{b_1}$ sont identiques, $\cos\left(\overrightarrow{b_0}, \overrightarrow{b_1}\right) = 1$. En raison de l'inexactitude de surveillance, si $|1 - \cos\left(\overrightarrow{b_0}, \overrightarrow{b_1}\right)| \leq \epsilon$, pour une petite valeur de confusion $\epsilon > 0$, deux pseudonymes changeant les processus peuvent être considérés comme impossibles à distinguer à l'œil de l'adversaire. Par conséquent, afin de protéger la confidentialité de l'emplacement de haute qualité, un véhicule doit choisir un scénario approprié où un plus grand nombre possible de pseudonymes indiscernables changeant les processus sont intervenus simultanément. Pour faciliter les véhicules à atteindre la confidentialité de l'emplacement de haut niveau dans VANETs , dans [65], Lu et *al.* proposent un protocole efficace de pseudonymes qui se change à la stratégie de socialspots, appelé PCS. Dans le protocole PCS, les socialspots sont les lieux où se rassemblent de nombreux véhicules temporairement, par exemple, l'inter-

section de la route lorsque le feu passe au rouge, ou un parking gratuit à proximité d'un centre commercial. Si tous les véhicules changent leurs pseudonymes avant de quitter les lieux, le premier diffuse un message de sécurité comprenant des informations impossibles à distinguer *Lieu = social spot*, *vitesse = 0*, et *Pseudonyme non couplées*. Ensuite, le socialspot devient naturellement une zone de mélange et la confidentialité de l'emplacement peut être réalisée. Plus précisément, les contributions de cette proposition sont de trois ordres.

- Premièrement, les auteurs utilisent la particularité des lieux sociaux (socialspot), c'est à dire, de nombreux véhicules s'arrêtent temporairement à l'endroit social, pour proposer la stratégie de PCS. Puis, ils proposent un modèle d'auto-délégation pratique de pseudonyme des clés isolées (KPSD), qui génère solidement de nombreux clés à la demande qui ont une courte durée de vie et peut atténuer les risques dus au vol du véhicule.
- Deuxièmement, les auteurs prennent la taille de l'ensemble de l'anonymat (ASS) comme la métrique de confidentialité pour mesurer la qualité de la vie privée (QoP) réalisée dans la stratégie PCS.
- Troisièmement, afin de garantir la stratégie PCS pour être effectivement adoptée dans la pratique, les auteurs utilisent les techniques simplifiées de la théorie des jeux pour prouver formellement la faisabilité de la stratégie de PCS. En conséquence, la stratégie de PCS peut vraiment guider les véhicules pour changer intelligemment leurs pseudonymes pour une meilleure confidentialité de l'emplacement au bon moment et dans le bon lieu.

Le reste de cette section est organisé comme suit. Dans la section 3.3.1, nous présentons les modèles et les objectifs de conception. Ensuite, nous présentons le fonctionnement du protocole PCS dans la section 3.3.2, suivie par l'analyse du protocole à la section 3.3.3.

3.3.1 Modèles et objectifs de conception

Dans cette sous section, nous présentons le modèle du système, le modèle de menace, et les objectifs de conception.

3.3.1.1 Le modèle du système

Dans [65], Ru *et al.* considèrent un réseau VANET dans une zone urbaine, qui se compose d'un grand nombre de véhicules et une collection de points sociales (socialspot).

- Les véhicules : dans la zone urbaine, un grand nombre de véhicules sont en cours d'exécution sur la route tous les jours. Chaque véhicule est équipé d'un appareil d'un dispositif embarqué (OBU), ce qui permet au véhicule de communiquer avec d'autres véhicules pour le partage des informations de trafic local afin d'améliorer l'ensemble de la sécurité des conditions de conduite.
- Les points sociales (Social Spots): les points sociales dans la zone urbaine se rapportent aux lieux où se rassemblent de nombreux véhicules, par exemple, une intersection de la route lorsque le feu de circulation est rouge ou un parking gratuit à proximité du

centre commercial, comme indiqué dans la figure 3.9[16]. Depuis la session du feu rouge est généralement de courte durée, (soit 30 ou 60 secondes), l'intersection de la route est appelée le petit point social. Comme un centre commercial fonctionne habituellement pendant une journée entière, en indiquant qu'un certain nombre de véhicules de clients s'arrêtera au parking pour une longue période, le parking gratuit à proximité du centre commercial est donc appelé le grand point social.

Figure 3:9 Les points sociales, l'intersection de la route et un parking gratuit

3.3.1.2 Le modèle de menace

Les auteurs du protocole PCS considèrent un adversaire externe global $\mathcal{A}$ équipé d'appareils radio pour tracer les emplacements des véhicules, où

- *Global* signifie que l'adversaire $\mathcal{A}$ a la capacité de surveiller et de collecter toutes les consignes de sécurité dans le réseau avec des appareils de radio ainsi que certaines infrastructures d'écoute spéciales, où chaque message de sécurité comprend *Temps, Emplacement, Vitesse, Contenu* ainsi que *Pseudonyme*. Depuis le *Pseudonyme* est non couplées et le *Contenu* pourrait être défini comme non pertinent, l'adversaire $\mathcal{A}$ suit principalement un véhicule en termes de *Temps, l'Emplacement, la Vitesse*, c'est à dire, d'une manière spatio-temporelle.
- *Externe* désigne que l'adversaire $\mathcal{A}$ peut seulement passivement espionner les communications, mais il ne tente pas de compromettre les véhicules d'exécution.

[16] Une image capturée avec : https://maps.google.dz/

3.3.1.3 Les objectifs de conception

L'objectif de conception dans le protocole PCS est de développer un protocole de pseudonyme efficace d'évolution à la stratégie de socialespots. Plus précisément, le protocole PCS atteint trois objectifs, ci-après :

- Chaque véhicule doit utiliser un pseudonyme à la place de la véritable identité pour diffuser les messages. En dissimulant l'identité réelle, la confidentialité de l'identité peut être atteinte.
- Chaque véhicule doit également changer périodiquement ses pseudonymes pour réduire la relation entre l'ancien emplacement et le second emplacement. En outre, les pseudonymes changeants doivent être effectués à l'heure et à l'endroit approprié pour s'assurer que la confidentialité de l'emplacement est atteinte.
- La confidentialité de l'emplacement devrait être conditionnelle dans les réseaux VANETs. Si un message de sécurité est diffusé en litige, l'autorité de confiance (TA) peut divulguer l'identité réelle, c'est-à-dire que le TA a la capacité de déterminer l'emplacement où un véhicule spécifique a diffusé un message de sécurité contesté.

3.3.2 Fonctionnement du protocole PCS pour la confidentialité de l'emplacement

Dans cette section, nous présentons le fonctionnement du protocole PCS pour la confidentialité de l'emplacement. Ru et *al.* [65] ont développés deux modèles analytiques de l'anonymat pour enquêter sur le niveau de la confidentialité de l'emplacement réalisés dans le protocole PCS, puis ont utilisé des techniques théoriques de jeu simplifiées pour discuter sa faisabilité.

3.3.2.1 Le modèle KPSD pour le protocole PCS

Comme le montre la figure. 3.10, dans le modèle KPSD, le TA fournit la clé anonyme autorisée à l'utilisateur (le propriétaire du véhicule). L'utilisateur stocke généralement la clé anonyme autorisée dans un environnement sécurisé, par exemple, à la maison. Le modèle KPSD se base sur les groupes bilinéaires asymétriques, la signature courte de Boneh-Boyen, et la technologie d'authentification de la préservation de confidentialité conditionnelle. Le KPSD proposé se compose principalement de ces quatre parties suivantes: l'initialisation du système, la génération des clés, la génération d'auto-délégué du pseudonyme et l'emplacement conditionnel :

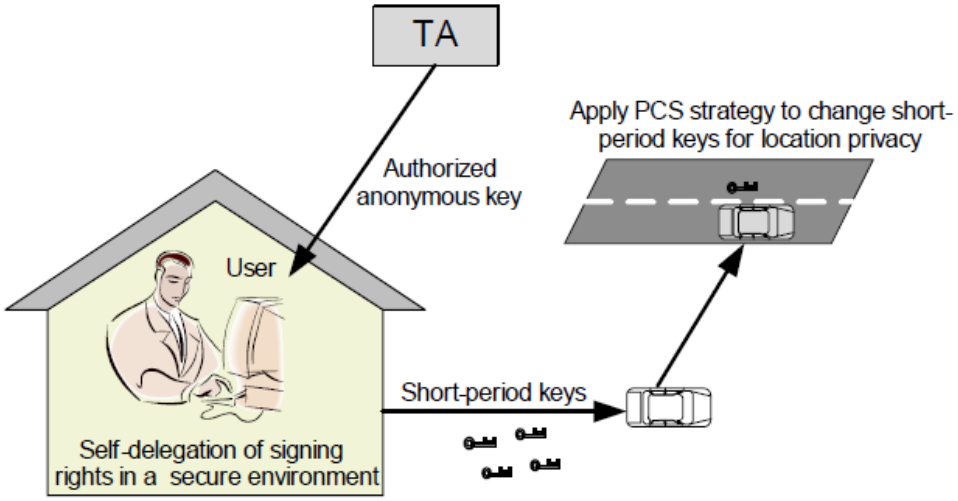


Figure 3:10 Le modèle KPSD pratique pour la confidentialité de l'emplacement dans les VANETs, proposé par Ru et al. [65]

L'initialisation du système :

Soit k un paramètre de sécurité, $\mathbb{G}$, $\mathbb{G}'$ et $\mathbb{G}_T$ trois (multiplicatif) des groupes cycliques du même grand ordre premier q généré par $\mathcal{G}en(k)$, où $|q| = k$. Supposons que $\mathbb{G}$, $\mathbb{G}'$ et $\mathbb{G}_T$ sont équipé avec un appariement, i.e., une application bilinéaire non-dégénérée et facilement calculable $e: \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$ où $e(g_1^a, g_2^b) = e(g_1, g_2)^{ab} \in \mathbb{G}_T$ pour tout $a, b \in \mathbb{Z}_q^*$ et tout $g_1 \in \mathbb{G}$, $g_2 \in \mathbb{G}$. φ est noté l'isomorphisme depuis $\mathbb{G}'$ à , que nous supposons être à sens unique (facile à calculer, mais difficile à inverser). Le TA choisi premièrement deux variables aléatoires $u, v \in \mathbb{Z}_q^*$ comme la clé master et calcule $U_1 = g_1^u$, $U_2 = g_2^u$, et $V_1 = g_1^v$. Le TA choisi aussi une fonction de hachage résistante aux collisions publique :$H: \{0,1\}^* \to \mathbb{Z}_q^*$. A la fin, le TA publie les paramètres du système

$$params = (q, \mathbb{G}, \mathbb{G}', \mathbb{G}_T, e, g_1, g_2, U_1, U_2, V_1, H)$$

La génération des clés :

Quand l'utilisateur U_i avec l'identité ID_i rejoint le système, le TA premièrement choisi un nombre aléatoire $s_i \in \mathbb{Z}_q^*$ comme $s_i + u \neq 0 \bmod q$, calcule $A_i = g_1^{\frac{1}{s_i+u}}$. Puis, le TA stock (ID_i, A_i^u) dans la liste de suivi et retourne $ASK_i = (s_i, A_i = g_1^{\frac{1}{s_i+u}})$ comme une clé anonyme autorisée à l'utilisateur.

La génération d'auto-délégué du pseudonyme :

Après la réception de la clé anonyme autorisée à l'utilisateur (par exemple, à la maison), le U_i commence à se déplacer dans la ville. Après, il exécute les étapes suivantes pour générer les clés anonymes requises de courte durée de vie utilisées pour le voyage, ce qui est très analogue à l'alimenter d'un véhicule avant un voyage.

Etape(1). U_i d'abord choisi l et les nombres aléatoires $x_1, x_2, \cdots, x_l \in \mathbb{Z}_q^*$ comme les clés privées de courte durée de vie et calcule les clés publiques correspondantes $Y_j = g^{x_j}$, pour $j = 1,2,\cdots, l$ pour le voyage.

Etape(2). Pour chaque clé publique de courte durée de vie Y_j, le U_i calcule le certificat auto-délégué anonyme $Cert_j$ comme suit

- Choisir aléatoirement $\propto, r_\propto, r_x, r_\delta \in \mathbb{Z}_q^*$ et calcule $T_U, T_V, \delta, \delta_1, \delta_2, \delta_3$, où

$$\begin{cases} T_U = U_1^{\alpha}, T_V = A_i.V_1^{\alpha}, \delta = \alpha \cdot x_i \bmod q \\ \delta_1 = U_1^{r_\propto}, \delta_2 = T_U^{r_x}/U_1^{r_\delta} \\ \delta_3 = e(T_V, g_2^{r_x})/e(V_1, U_2^{r_\alpha} \cdot g_2^{r_\delta}) \end{cases}$$

- Calcule $c = H(U_1||V_1||Y_j||T_U||\delta_1||\delta_2||\delta_3$ et $s_\alpha, s_x, s_\delta \in \mathbb{Z}_q^*$, où

$$\begin{cases} s_\alpha = r_\alpha + c.\alpha \bmod q, s_x = r_x + c.x_i \bmod q \\ s_\delta = r_\delta + c.\delta \bmod q \end{cases}$$

- Mettre $Cert_j = \{Y_j||T_U||T_V||c||s_\alpha||s_x||s_\delta\}$ comme un certificat.

Etape(3). Après la génération de tout les certificats d'auto-délégué anonyme $Cert_j$, $j = 1,2,\cdots, l$, le U_i les installe sur le véhicule, i.e., implémenter tout $x_j||Y_j||Cert_j$, $j = 1,2,\cdots, l$ dans l'équipement OBU.

Après, quand U_i est en cours de conduire le véhicule dans la ville, il peut utiliser une clé à vie courte $x_j||Y_j||Cert_j$ pour authentifier un message M en signant $\sigma = g_2^{\frac{1}{x_j + H(M)}}$, et diffuse

$$msg = (M||\sigma||Y_j||Cert_j)$$

Lors de la réception du $msg = (M||\sigma||Y_j||Cert_j)$, tout le monde peut vérifier la validité par les deux étapes suivantes

- Si le certificat $Y_j||Cert_j$ n'a pas été vérifié, le vérificateur calcule d'abord

$$\begin{cases} \delta_1' = \dfrac{U_1^{s_\alpha}}{T_U^c}, \delta_2' = \dfrac{T_U^{s_x}}{U_1^{s_\delta}} \\ \delta_3' = \dfrac{e(T_V, g_2^{s_x}.U_2^c)}{e\left(V_1, U_2^{s_\alpha}.g_2^{s_\delta}\right)e(g_1, g_2^c)} \end{cases}$$

et vérifie si

$$c = H(U_1||V_1||Y_j||T_U||T_V||\delta_1'||\delta_2'||\delta_3')$$

S'il la vérification est bonne, le certificat $Y_j||Cert_j$ passe la vérification. Les corrections sont les suivantes:

i. $\delta_1' = \frac{U_1^{sx}}{T_U^c} = \frac{U_1^{r\alpha+c.\alpha}}{U_1^{c.\alpha}} = \delta_1$;

ii. $\delta_2' = \frac{T_U^{sx}}{U_1^{s\delta}} = \frac{T_U^{r\alpha+c.x_i}}{U_1^{r\delta+c\delta}} = \delta_2$;

iii. $\delta_3' = \frac{e(T_V, g_2^{sx}.U_2^c)}{e\left(V_1, U_2^{sx}.g_2^{s\delta}\right)e(g_1, g_2^c)} = \frac{e(T_V, g_2^{rx})}{e\left(V_1, U_2^{r\alpha}.g_2^{r\delta}\right)} = \delta_3$.

- Une fois le certificat $Y_j||Cert_j$ passe la vérification, le vérificateur contrôle

$$e\left(Y_j.g_1^{H(M)}, \sigma\right) ? = e(g_1, g_2)$$

S'il la vérification est bonne, le message M est accepté, sinon, M est rejeté.

L'emplacement conditionnel :

Une fois qu'un message M accepté sous le certificat $Cert_j = \{Y_j||T_U||T_V||c||s_\alpha||s_x||s_\delta\}$, le TA utilise la clé master pour calculer

$$\frac{T_V^u}{T_U^v} = \frac{A_i^u.V_1^{u\alpha}}{U_1^{v\alpha}} = \frac{A_i^u.g^{uv\alpha}}{g^{uv\alpha}} = A_i^u$$

puis peut suivre efficacement l'identité réel ID_i en recherchant l'entrée (ID_i, A_i^u) dans la liste de cheminement.

Depuis que la signature courte et l'authentification préservant la confidentialité conditionnelle sont sécurisé, la sécurité de ce schéma KPSD peut être garantit, i.e., il peut effectivement réaliser l'authentification anonyme avec un suivi conditionnel pour répondre aux exigences de la confidentialité de l'emplacement. De plus, le schéma KPSD proposé peut aussi atténuer les risques dus au vol du véhicule, puisque la clé anonyme autorisé ASK_i est une clé isolée, i.e., il est stocké dans un environnement sécurisé, puis les voleurs de véhicules ne peuvent pas obtenir ASK_i du véhicule volé, et par conséquent, il ne peut pas générer de nouvelles clés d'auto-délégué de courte durée de vie arbitrairement.

3.3.2.2 L'analyse du jeu de l'anonymat pour la confidentialité de l'emplacement réalisée

Avec le schéma ci-dessus KPSD, chaque véhicule peut contenir un certain nombre de pseudonymes sur la route, alors il peut appliquer la stratégie de PCS, comme indiqué dans l'algorithme 3.5, pour protéger sa confidentialité de l'emplacement. Pour évaluer les avantages de la stratégie de PCS, Ru et al [65] développent deux modèles analytiques d'anonymat pour enquêter sur la confidentialité de l'emplacement réalisés dans les petits points sociales et les grands points sociales, respectivement.

1: **procedure** PCS STRATEGY
2: **Case 1:** Small social spot
3: A vehicle V_i stops at road intersection when the traffic light turns red. When the traffic light turns to green, V_i changes its pseudonym.
4: **Case 2:** Large social spot
5: A vehicle V_i stops at a free parking lot near a shopping mall. When leaving the parking lot, V_i changes its pseudonym.
6: **end procedure**

Algorithme 3:5 Changement de pseudonyme à la stratégie des points sociales, proposé par Ru *et al.* [65]

L'analyse du jeu de l'anonymat à de petits points sociaux

Comme présenté dans la figure 3.11, lorsque le feu passe au rouge, l'intersection de la route peut être considérée comme un petit point social, car une flotte de véhicules s'arrête à l'intersection. Les auteurs considèrent que tous les véhicules auront simultanément changé leurs pseudonymes lorsque le feu passe au vert. Donc, l'intersection de la route devient naturellement une zone de mélange. Soit S_a le nombre de véhicules arrêtés à l'intersection et la taille de l'ensemble de l'anonymat (ASS) $= S_a$. Soit $T_s = t$, où $t = 30{,}60$ seconde , la période de temps d'arrêt fixe d'un croisement de route spécifique. Soit l'arrivée du véhicule

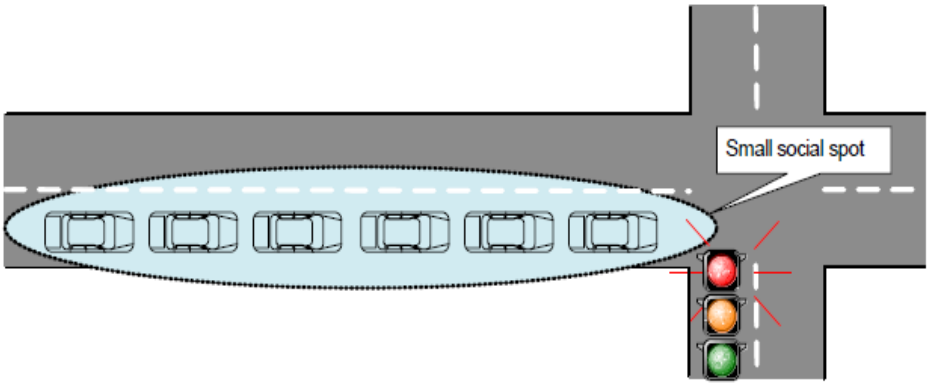


Figure 3:11 Le changement de pseudonyme à une intersection, proposé par Ru et al. [65]

(VA) à l'intersection de la route un processus de Poisson[17], et t_a le temps inter-arrivée à VA, où t_a a une distribution exponentielle avec la moyenne $\frac{1}{\lambda}$. .Soit X la variable aléatoire des véhicules arrivant à l'intersection de la route au cours de la période T_s. Ensuite, la probabilité $X = x$ durant $T_s = t$ peut être exprimée comme

$$\Pr[X = x | T_s = \mathrm{t}] = \frac{(\lambda t)^x}{x!} e^{-\lambda t}$$

[17] Un processus de Poisson, nommé d'après le mathématicien français Siméon Denis Poisson et la loi du même nom, est un processus de comptage classique dont l'équivalent discret est la somme d'un processus de Bernoulli. C'est le plus simple et le plus utilisé des processus modélisant une file d'attente. (Source : wikipedia)

et le nombre attendu de X peut être calculé comme

$$E(X|T_s = t] = \sum_{x=1}^{\infty} x\Pr[X = x|T_s = t] = \lambda t$$

Comme tous les véhicules quittent l'intersection après le feu passe au vert, la taille de l'ensemble de l'anonymat ASS est

$$ASS = S_a = \mathrm{E}[X|T_s = t] = \lambda t$$

L'analyse du jeu de l'anonymat à de grands points sociaux

Comme le montre la figure 3.12, un grand point social pourrait être un parking gratuit à proximité d'un centre commercial. Parce qu'un parking tient habituellement de nombreux véhicules, et chaque véhicule reste au hasard sur le parking selon la volonté propore de l'utilisateur, un tel stationnement devient aussi naturellement une zone de mélange si tous les utilisateurs changent leurs pseudonymes dans le stationnement et quittent le parking après un délai aléatoire.

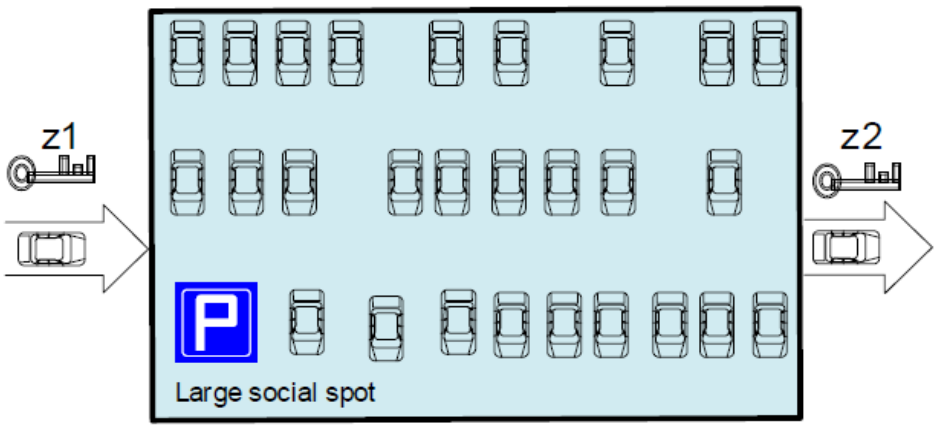


Figure 3:12 Le changement de pseudonyme dans un parking gratuit, proposé par Ru et al. [65]

Soit S_a le nombre de véhicules dans le stationnement lorsque le véhicule est prêt à partir et la taille de l'ensemble de l'anonymat dénote ASS $= S_a$. Pour un véhicule $\mathcal{V}$ spécifique qui a entré au parking à coté d'un centre commercial pour changer pseudonymes, nous considérons la période de l'heure d'ouverture du centre commercial, par exemple, 8 :00 AM, au moment de quitter le véhicule V après le changement des pseudonymes, T_S, comme présenté dans la figure 3.13, est distribué de façon exponentielle avec la fonction de densité $f(t)$, la moyenne $\frac{1}{\mu}$, et la transformée de Laplace $f^*(s) = (\frac{\mu}{\mu+s})$. Soit X la variable aléatoire de véhicules arrivant

au parking pendant la période de temps T_s. Ensuite, la probabilité $X = x$ durant la période $T_s = t$ suit $\Pr[X = x|T_s = t] = \frac{(\lambda t)^x}{x!} e^{-\lambda t}$, et pour $t \geq 0$,

$$\Pr[\mathrm{X} = \mathrm{x}] = \int_{\mathrm{t}=0}^{\infty} \Pr[X = x|T_s = t]\, f(t)dt$$

$$= \int_{\mathrm{t}=0}^{\infty} \frac{(\lambda t)^x}{x!} e^{-\lambda t}\, f(t)dt$$

$$= \left(\frac{\lambda^x}{x!}\right) \int_{\mathrm{t}=0}^{\infty} t^x e^{-\lambda t} f(t)dt$$

$$= \left(\frac{\lambda^x}{x!}\right) \left[(-1)^x \frac{d^x f^*(s)}{ds^x}\right]$$

$$= \frac{\mu \lambda^x}{(\mu + \lambda)^{x+1}}$$

et le nombre attendu de X peut être calculé comme

$$\mathrm{E}(X) = \sum_{x=1}^{\infty} x \Pr[X = x] = \frac{\lambda}{\mu}$$

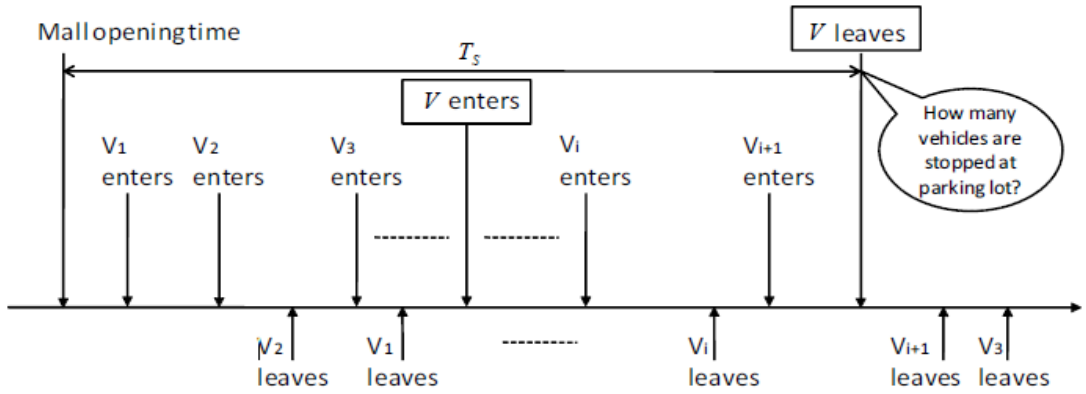


Figure 3:13 Le diagramme de temps, proposé par Ru et al. [65]

Soit χ la période de temps entre le moment où un véhicule arrive sur le parking et le moment où le véhicule V spécifique quitte le parking après le changement des pseudonymes. Depuis T_s est distribué de façon exponentielle, la fonction de densité $\sigma(\chi)$ pour la distribution χ peut être exprimée sous la forme

$$\sigma(\chi) = \mu \int_{t=\chi}^{\infty} f(t)dt = \mu[1 - F(t)]\Big|_{t=\chi} = \mu e^{-\mu\chi}$$

Au cours de la période T_s, de nombreux véhicules peuvent quitter le parking avant le départ de $\mathcal{V}$, c'est à dire, $t_u < \chi$. Supposons que Y est le nombre de véhicules qui sont quitté le parking avant $\mathcal{V}$, alors la probabilité Pr $[Y = y|X = x]$ peut être calculé comme suit

$$\Pr\,[\mathrm{Y} = y|X = x] = \binom{x}{y} (\Pr[t_u < \chi])^y (\Pr[t_u \geq \chi])^{x-y}$$

Ensuite, la probabilité $\Pr[t_u \geq \chi]$ peut être calculée comme suit :

$$\Pr[t_u \geq \chi] = \int_{t_u=0}^{\infty} \int_{\chi=0}^{t_u} \mu e^{u\chi} d\chi f_u(t_u) dt_u$$

$$= \int_{t_u=0}^{\infty} (1 - e^{-ut_u}) f_u(t_u) dt_u$$

$$= 1 - \int_{t_u=0}^{\infty} f_u(t_u) e^{-ut_u} dt_u = 1 - f_u^*(\mu)$$

et $\Pr[t_u < \chi]$peuvent être dérivés de $\Pr[t_u \geq \chi]$ comme

$$\Pr[t_u < \chi] = 1 - \Pr[t_u \geq \chi] = 1 - \left(1 - f_u^*(u)\right) = f_u^*(u)$$

Par conséquent, la taille attendue du jeu de l'anonymat ASS pour les pseudonymes changés du véhicule spécifique $\mathcal{V}$ est

$$ASS = S_a = \mathrm{E}[X] - \mathrm{E}[Y]$$

$$= \frac{\lambda}{\mu} - \sum_{x=1}^{\infty} \left\{ \left\{ \sum_{y=1}^{x} y \binom{x}{y} \left(f_u^*(u)\right)^y (1 - f_u^*(u))^{x-y} \right\} \times \left[\frac{\mu \lambda^x}{(\mu + \lambda)^{x+1}} \right] \right\}$$

3.3.2.3 Analyse de faisabilité du protocole PCS

Les analyses d'ensemble de l'anonymat ci-dessus sont sous l'hypothèse que tous les véhicules changent leurs pseudonymes. Dans cette sous section, nous présentons l'utilisation des techniques de la théorie des jeux simplifiées proposé par Ru et al. [65] pour démontrer la faisabilité du protocole PCS. Plus précisément, nous présentons que chaque véhicule est vraiment prêt à changer le pseudonyme à des endroits sociales pour la réalisation de sa confidentialité de l'emplacement dans la pratique.

Soit la taille de l'ensemble de l'anonymat ASS être $N = n + 1$, où $n \geq 0$, aux points sociales, qui peut être estimée par l'analyse de la série de l'anonymat ci-dessus.. Aux points sociales, chaque véhicule V_j, $1 \leq j \leq N$ a deux actions possibles: le changement (C) du pseudonyme avec une probabilité p_j et garder (K) le pseudonyme avec la probabilité $1 - p_j$. Si V_j conserve son pseudonyme au point social, il peut toujours être suivi avec une probabilité de 1. Quand V_j change ses pseudonymes au point social, s'il y a d'autres véhicules qui prennent la même action, la taille de l'ensemble de l'anonymat deviendra S. Après ce point social, V_j reste étant suivi seulement avec une probabilité $\frac{1}{S}$. La perte de la confidentialité de l'emplacement dans le cas présent se réduit à $-\frac{d_j}{S}$. Soit $c_j \in (0,1)$ le coût normalisé de changer un pseudonyme du véhicule V_j, de sorte que le gain de cette action est $-\frac{d_j}{S} - c_j$. Pour tous les véhicules, sauf V_j , soit p_m le minimum de toutes les probabilités $\{p_i | 1 \leq i \leq N, i \neq j\}$. Quand V_j est prêt à changer son pseudonyme à des points sociales, la limite basse de l'anonymat moyenne définie comme

$$S = \sum_{i=0}^{n} \binom{n}{i} . p_m^i . (1 - p_m)^{n-1} . (i + 1) = np_m + 1$$

Comme résultat, la fonction de gain (Payoff) de véhicule V_j peut être résumée comme suit

$$(\text{Payoff}) = \begin{cases} -\dfrac{d_j}{np_m + 1} - c_j, & \text{si l'action C est prise;} \\ -d_j, & \text{sinon si l'action K est prise.} \end{cases}$$

Depuis le véhicule V_j est rationnelle et son but est de protéger sa confidentialité de l'emplacement, la condition que V_j change son pseudonyme au point social est

$$-\frac{d_j}{np_m + 1} - c_j > -d_j \Rightarrow c_j < \frac{np_m d_j}{np_m + 1}$$

Avec le schéma de KPSD adopté, tous les véhicules génèrent leurs pseudonymes par eux-mêmes, ils peuvent générer suffisamment de pseudonymes avant un voyage, alors le coût du changement pseudonyme peut être très faible. Cependant, les auteurs définissent pour chaque véhicule V_j , la fonction du gain de la confidentialité de l'emplacement (*location privacy gain (LPG))* comme suit

$$LPG_j = -\frac{d_i}{np_m + 1} - (-d_i) = \frac{np_m}{np_m + 1} . d_j$$

En outre, LPG_j est une fonction d'augmentation en terme de p_m. Quand $p_m = 1$, i.e., tous les véhicules changent leurs pseudonymes aux points sociales, LPG_j peut atteindre son gain maximal $\frac{n}{n+1} . d_j = \frac{(N-1)}{N} . d_j$. Comme chaque véhicule est rationnel pour maximiser son gain de confidentialité de l'emplacement, il serait une situation gagnant-gagnant quand ils chan-

gent tous leurs pseudonymes. Comme résultat, la faisabilité de la stratégie de PCS dans la pratique est montrée.

3.3.3 Performances du protocole SPF

Ru *et al.* [65] ont évalué les performances du protocole SPF utilisant un simulateur personnalisé construit en C++. Les indicateurs de performance calibrés à l'évaluation sont la taille du jeu de l'anonymat (ASS) et le gain de la confidentialité de l'emplacement (LPG). Les résultats montrent que pour atteindre un endroit de haut niveau de confidentialité, par exemple, un grand carrefour avec un trafic élevé est un bon choix pour les véhicules.

Pour évaluer le niveau de la confidentialité de l'emplacement réalisé au large point social, les auteurs considèrent un parking gratuit à proximité d'un centre commercial. Les résultats montrent que la simulation et l'analyse correspondentes sont correctes, ce qui justifie la précision du modèle analytique. Aussi, les résultats indiquent qu'un véhicule peut changer ses pseudonymes souvant dans la journée pour une meilleure confidentialité de l'emplacement au grand point social, quel que soit durant la matinée ou l'après-midi.

3.4 Le protocole FLIP

Le t'chat des véhicules est l'une des applications les plus prometteuses dans les réseaux VANETs, qui permet aux véhicules circulant sur la même route pour discuter les uns avec les autres sur certains sujets d'intérêt commun dans le but de passer le temps pendant le trajet ou pour demander l'aide sur la route. Cependant, le succès de ce type d'application dans VANETs s'articule encore des questions de problèmes de sécurité et de confidentialité, par exemple, la confidentialité de l'identité (où la vie privée d'identité), la confidentialité de l'emplacement et la confidentialité d'intérêt. Parce les réseaux VANETs sont généralement mises en œuvre dans les scénarios civils, où les emplacements des véhicules sont étroitement liés à ceux qui les animent, si l'application t'chat du véhicule révèle la confidentialité de l'identité du véhicule et la confidentialité de l'emplacement, il ne peut pas être acceptée par le public. Pour faciliter les véhicules à atteindre la confidentialité d'intérêt, comme une exigence particulière de la vie privée dans l'application t'chat du véhicule, dans [66], Lu et *al.* proposent un protocole efficace préservant la confidentialité d'intérêt, appelé FLIP, qui permet à deux véhicules avec l'intérêt commun pour identifier les uns les autres et d'établir une clé de session partagée, et en même temps, protéger leurs intérêts personnels (Interest-Privacy (IP)) depuis les autres véhicules qui n'ont pas le même intérêt sur la route. Plus précisément, les contributions de cette proposition sont de deux ordres.

- Premièrement, les auteurs proposent le protocole FLIP efficace préservant l'IP visant à l'application du t'chat véhicule dans les réseaux VANETs et officialisent son modèle de sécurité aussi bien. Ensuite, ils appliquent la technique de sécurité prouvable pour valider sa sécurité dans le modèle défini.
- Deuxièmement, les auteurs développent un simulateur personnalisé construit en Java pour mesurer la relation entre le niveau IP-préservation et le délai pour trouver le véhicule du même esprit. Les résultats des simulations approfondies

montrent que, après avoir atteint un niveau IP de préservation requis, un véhicule peut trouver le véhicule du même esprit dans un délai prévu.

Le reste de cette section est organisée comme suit. Dans la sous section 3.4.1, nous présentons les modèles et les objectifs de conception. Ensuite, nous présentons le fonctionnement du protocole FLIP dans la sous section 3.4.2, suivie par l'analyse du protocole à la sous section 3.4.3.

3.4.1 Modèles et objectifs de conception

Dans cette sous section, nous présentons le modèle du système, les objectifs de conception, et le modèle de sécurité.

3.4.1.1 Le modèle du système

Dans [66], Ru *et al.* considèrent un réseau VANET dans une zone urbaine, qui se compose d'un grand nombre de véhicules $\mathcal{V} = \{v_1, v_2, v_3, \cdots, \}$ et une seule autorité de confiance (TA), comme indiqué dans la figure. 3.14. Puis ils limitent le problème au scénario où les véhicules trouvent des véhicules partageant les mêmes idées avec intérêt commun sur la route sans l'aide d'unités d'actions restreintes. Les auteurs n'incluent pas UAR dans le modèle actuel, mais ils sont toujours déployés pour soutenir la communication V-2-I.

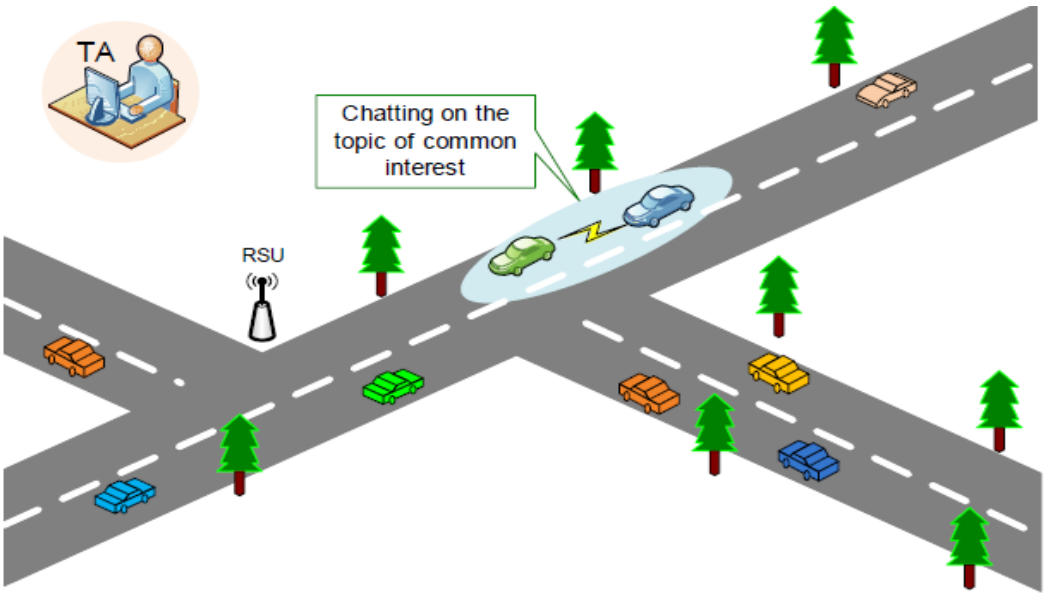


Figure 3:14 Le modèle du système sous considération pour FLIP, proposé par Ru *et al.* [66]

- L'autorité de confiance (Trust Authority (TA)): le TA est une entité digne de confiance et puissante. La responsabilité de TA est la gestion de l'ensemble du réseau, par exemple, l'initialisation du système, l'enregistrement des véhicules dans le système en attribuant un ensemble fini de pseudo-IDs et les clés correspondant à chaque véhicule. il est à noter que TA est une entité ligne, qui n'est pas directement impliqué dans la communication V-2-V.

- Les véhicules $\mathcal{V} = \{V_1, V_2, \cdots\}$: Chaque véhicule $V_i \in \mathcal{V}$ est équipé avec l'appareil OBU, qui leur permet de communiquer les uns avec les autres pour partager des informations d'intérêt commun. Différent des nœuds mobiles dans le général du réseau ad hoc, l'appareil OBU dans VANET n'a pas de problème de puissance sous contrainte et en même temps, il est équipé de capacités puissantes de calcul et de communication. Le support utilisé pour les communications entre les véhicules voisins est de 5,9 GHz communications spécialisées à courte portée (Dedicated Short Range Communication (DSRC)) identifié comme IEEE 802.11p, et la portée de transmission de chaque véhicule est 300 m. Quand deux véhicules V_a, et $V_b \in \mathcal{V}$ sont dans leur gamme de transmission, ils peuvent discuter sur les sujets d'intérêt commun sur la route.

3.4.1.2 Les objectifs de conception

Sans la garantie de la confidentialité des véhicules, y compris la confidentialité de l'identité, la confidentialité de l'emplacement et la confidentialité d'intérêt, l'application de t'chat du véhicule ne peut pas être largement acceptée par le public. Par conséquent, il est essentiel de protéger la confidentialité de véhicule. Plus précisément, les exigences de sécurité suivantes doivent être assurées en application de t'chat de véhicule: i) l'identité réel de véhicule doit être protégée ; ii) la confidentialité du véhicule doit être garantie; et iii) les intérêts du véhicule doivent être protégés contre d'autres personnes qui ne disposent pas de l'intérêt commun.

Pour satisfaire aux exigences de sécurité ci-dessus, L'objectif de conception dans le protocole FLIP est de développer un protocole efficace préservant la confidentialité d'intérêt. Plus précisément, avec FLIP, les véhicules qui ont l'intérêt commun peuvent établir une clé de session partagée sans violer IP à d'autres qui n'ont pas un intérêt commun.

3.4.1.3 Le modèle de sécurité

Ru et al. [66] définissent le modèle de sécurité de FLIP en empruntant des idées à partir du modèle de sécurité du protocole d'échange des clés authentifiées (AKE) [68] pour décrire certaines attaques possibles. Plus précisément, dans le modèle de sécurité, les véhicules ne s'écartent pas le protocole FLIP, tandis que l'adversaire $\mathcal{A}$ dont les capacités d'attaque sont modélisés par un ensemble de requêtes oracle prédéfinies, qui peuvent surveiller passivement et/ou contrôler activement les communications inter-véhicules. Supposons que deux véhicules V_a et V_b participent dans FLIP pour des intérêts communs $I_\alpha \in \mathcal{I} = \{I_1, I_2, \cdots, I_k\}$. Chacun d'entre eux dispose de plusieurs instances appelées oracles impliqués dans des exécutions distinctes du FLIP, où l'intérêt commun I_α varie dans différentes exécutions. On note une instance s de $V_i \in V_a, V_b$ par $\prod_{V_i}^{s}$ pour un entier $s \in \mathbb{N}$, et utilise la notation $\prod_{V_a,V_b}^{s}$ pour définir le $s-$ième instance V_a exécute avec V_b sur l'intérêt commun I_α^s , où $\alpha \in \mathbb{N}$ et $1 \leq \alpha \leq k$.

3.4.1.4 Le modèle de l'adversaire

Supposons qu'il permet à l'adversaire $\mathcal{A}$ d'accéder à toutes transcriptions dans le protocole FLIP. Tous les oracles communiquent uniquement les uns avec les autres via $\mathcal{A}$. L'adversaire $\mathcal{A}$ peut rejouer, modifier, retarder ou supprimer des transcriptions. Cependant, la sécurité du

FLIP est définie utilisant le jeu suivant, joué entre $\mathcal{A}$ et une collection d'oracle $\prod_{V_a,V_b}^{s}$ pour les véhicules V_a, V_b et $s \in \mathbb{N}$, où V_a, V_b sont le pseudo-ID affecté et les clés correspondant.

- Dans le jeu, $\mathcal{A}$ peut poser des questions et récupérer les réponses des oracles correspondants.
- A certain moment, $\mathcal{A}$ questionne la requête Test pour un nouvel oracle, et sortir son estimation (guess) α' pour α, où $1 \leq \alpha \leq k$, et β' pour le bit β dans la requête Test.

3.4.2 Fonctionnement du protocole FLIP

Dans cette section, nous présentons le fonctionnement du protocole FLIP pour la confidentialité d'intérêt, qui se compose principalement de deux parties: l'initialisation du système et la confidentialité d'intérêt sur la route.

3.4.2.1 L'initialisation du système

Dans la phase d'initialisation du système, l'autorité de confiance (TA) initialise premièrement l'ensemble du système en exécutant les étapes suivantes. Soit le paramètre de sécurité l, le TA génère un groupe de courbes elliptiques $\mathbb{G} =< P >$, où le générateur P a un grand nombre premier q avec $|q| = l$. Ensuite, le TA choisi un nombre aléatoire $s \in \mathbb{Z}_q^*$ comme la clé master et calcule la clé publique du système correspondante $P_{pub} = sP$. Aussi, le TA choisi quatre fonctions de hachage $\mathcal{H}, \mathcal{H}_0, \mathcal{H}_1$, et $\mathcal{H}_2$, où $\mathcal{H}: \{0,1\}^* \rightarrow \mathbb{G}$ et $\mathcal{H}_i: \{0,1\}^* \rightarrow \mathbb{Z}_q^*$, pour $i = 0,1,2$. A la fin, le TA publie les paramètres publiques du système

$$params = \{\mathbb{G}, P, q, P_{pub}, \mathcal{H}, \mathcal{H}_0, \mathcal{H}_1, \mathcal{H}_2)$$

et garde secrètement la clé master.

Quand un véhicule $V_i \in \mathcal{V}$ demande l'enregistrement au système, le TA vérifie d'abord la validité du véhicule V_i. Si V_i est valide, le TA génère une famille de pseudo-IDs et les clés correspondantes pour V_i utilisant l'algorithme 3.6. De cette façon, V_i peut constamment changer ses pseudo-ID pour atteindre la confidentialité de l'identité et la confidentialité de l'emplacement sur la route.

```
1: procedure VehicleRegistration
   Input: a verified vehicle V_i ∈ V
   Output: a family of pseudo-IDs and the corresponding key materials
2:     choose a family of unlinkable pseudo-IDs PID = {pid_1, pid_2, ···}
3:     for each pseudo-ID pid_j ∈ PID do
4:         randomly choose a private key x_j ∈ Z_q^*
5:         compute the corresponding public key Y_j = x_j P
6:         assert (pid_j, Y_j) with certificate cert_j signed by TA with s
7:     end for
8:     return all tuples (pid_j, x_j, Y_j, cert_j) to V_i
9: end procedure
```

Algorithme 3:6 L'algorithme d'enregistrement du véhicule dans FLIP, proposé par Ru *et al.* [66]

3.4.2.2 La confidentialité d'intérêt

Quand le véhicule $V_a \in \mathcal{V}$ est sur la route et veut trouver un véhicule $V_b \in \mathcal{V}$ au même esprit avec l'intérêt commun I_α à proximité, comme le montre la figure. 3.15, ils vont exécuter les étapes suivantes pour établir une clé de session partagée sk pour l'intérêt commun I_α.

Etape(1). V_a premièrement fixe un intérêt fixé $\mathcal{I}$, qui se compose de k types d'intérêts $\{I_1, I_2, \cdots, I_k\}$, où V_a l'intérêt réel I^+est impliqué. Ensuite, V_a choisi un nombre aléatoire $x \in \mathbb{Z}_q^*$, calcule $X = x\mathcal{H}(I^+)$ et utilise l'algorithme ECDSA pour générer une signature $\sigma_a = \text{ECDSA}(\mathcal{I}||X)$ sur $\mathcal{I}||X$ avec le pseudo-ID pid_a et le certificat cert_a. A la fin, V_a diffuse la requête $\mathcal{I}\|X\|\sigma_a\|\text{pid}_\text{a}\|\text{cert}_\text{a}$ pour les véhicules à proximité.

Etape(2). Lors de la réception de la requête $\mathcal{I}\|X\|\sigma_a\|\text{pid}_\text{a}\|\text{cert}_\text{a}$, un véhicule à proximité V_a premièrement vérifie la validité du σ_a avec $\text{pid}_\text{a}\|\text{cert}_\text{a}$.

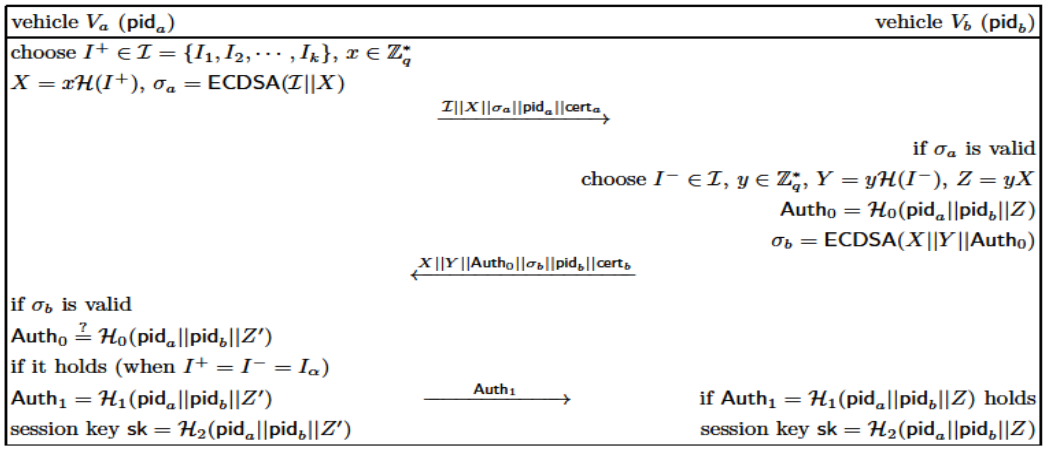


Figure 3:15 Le protocole de préservation de la confidentialité d'intérêt, proposé par Ru et al. [66]

Si elle est valide, V_b néglige la demande. Dans le cas contraire, V_b choisit son intérêt $I^- \in \mathcal{I}$ et le nombre aléatoire $y \in \mathbb{Z}_q^*$, calcule $Y = y\mathcal{H}(I^-)$, $Z = yX$, et $\text{Auth}_0 = \mathcal{H}_0(\text{pid}_\text{a}\|\text{pid}_\text{b}\|\text{Z})$. Ensuite, V_b fait une signature $\sigma_b = \text{ECDSA}(X||Y\|\text{Auth}_0)$ sur $X\|Y\|\text{Auth}_0\|\sigma_b\|\text{pid}_\text{b}\|\text{cert}_\text{b}$ avec le pseudo pid_b et le certificat cert_b , et retourne la réponse $X\|Y\|\text{Auth}_0\|\sigma_b\|\text{pid}_\text{b}\|\text{cert}_\text{b}$ à V_a . Il est à noté que dans le protocole, V_b est autorisé seulement à effectuer au plus une réponse de la même demande.

Etape(3). Après la réception de la réponse $\|Y\|\text{Auth}_0\|\sigma_b\|\text{pid}_\text{b}\|\text{cert}_\text{b}$, le demandeur V_a vérifie d'abord la validité de σ_b avec $\text{pid}_\text{b}\|\text{cert}_\text{b}$. S'elle est invalide, V_a néglige la réponse. Dans le cas contraire, V_a calcule $Z' = xY$, et vérifie si $\text{Auth}_1 = \mathcal{H}_1(\text{pid}_\text{a}\|\text{pid}_\text{b}\|\text{Z}')$ à V_b, et calcule la clé de session $\text{sk} = \mathcal{H}_2(\text{pid}_\text{a}\|\text{pid}_\text{b}\|\text{Z}')$.

Etape(4). Quand V_b reçois $\text{Auth}_1 = \mathcal{H}_1(\text{pid}_\text{a}\|\text{pid}_\text{b}\|\text{Z}')$, il vérifie si $\text{Auth}_1 = \mathcal{H}_1(\text{pid}_\text{a}\|\text{pid}_\text{b}\|\text{Z})$. Si il détient, V_b calcule la clé de session $\text{sk} = \mathcal{H}_2(\text{pid}_\text{a}\|\text{pid}_\text{b}\|\text{Z})$. Si $I^+ = I^- = I_\alpha$ pour certain $1 \leq \alpha \leq k$, V_a et V_b disposent la clé de session partagé sk, i.e., le véhicule V_a a trouvé le véhicule V_b au même esprit sur la route. Si les intérêts I^+ et I^- sont identiques, i.e.,$I^+ = I^- = I_\alpha \in \mathcal{I}$, alors

$$\mathcal{H}(I^-) = \mathcal{H}(I^+)\ ,\ \mathrm{Z}' = xY = xy\mathcal{H}(I_\alpha) = yx\mathcal{H}(I^+) = yX = Z$$

et les deux authentificateurs $\mathrm{Auth}_0 = \mathcal{H}_0(\mathrm{pid_a}\|\mathrm{pid_b}\|\mathrm{Z})$, $\mathrm{Auth}_1 = \mathcal{H}_1(\mathrm{pid_a}\|\mathrm{pid_b}\|\mathrm{Z}')$ et la clé de session sk sont valides. Cependant, si $I^+ \neq I^-$, alors $\mathcal{H}(I^-) \neq \mathcal{H}(I^+)$ et

$$\mathrm{Z}' = xY = xy\mathcal{H}(I^-) \neq yx\mathcal{H}(I^+) = yX = Z$$

ce qui indique que Auth_0 et Auth_1 ne sont pas valides, et la clé de session sk partagée ne peut être établie.

3.4.3 L'analyse du protocole

- Ru et *al.* dans [66] ont prouvé que la confidentialité d'intérêt (Interest-Privacy (IP)) peut être protégée contre les véhicules non partageant les mêmes idées sans collusion dans le protocole FLIP proposé.
- La métrique de performance utilisée dans l'évaluation [66] est le délai moyen pour trouver le véhicule d'esprit commun, noté par FD, qui est définie comme le temps moyen entre le moment où le demandeur V_a envoie une requête et lorsque le V_b trouve avec succès le véhicule V_a sur la route. Les auteurs considèrent un nombre large de véhicule $\mathcal{V} = \{V_1, V_2, V_3, \cdots\}$ se déplacent sur une même route de direction multivoies avec une vitesse variant de 40km/h à 80km/h. Aussi, ils considèrent d'autres véhicules qui passent par le véhicule $V_a \in \mathcal{V}$ suit un processus de Poisson, et l'inter passant par le temps t_a a une distribution exponentielle avec la moyenne $1/\lambda$. Dans la simulation, le véhicule V_a diffusera la demande avec intérêt fixé $\mathcal{I}$ de taille différente $|\mathcal{I}|$ variant de 1 à 10, pour trouver le véhicule au même esprit. Avec l'exécution de la simulation 10.000 fois, les résultats ont montré que la moyenne FD peut être réduite avec l'augmentation de λ.

3.5 Le protocole Pi

Comme nous avons vu dans la section précédente, le protocole FLIP peut garantir la confidentialité d'intérêt dans les réseaux sociaux véhiculaires. Toutefois, en raison des contraintes de ressources, certains véhicules pourraient se comportent comme des égoïstes dans les réseaux sociaux véhiculaires. Pour résoudre ce problème, les auteurs du protocole FLIP ont proposé un nouveau protocole d'incitation pratique, appelé Pi [67], pour les applications de transmission de paquets dans les réseaux véhiculaires DTNs.

En raison des caractéristiques uniques de DTNs, tels que le manque de chemin contemporain et la forte variation dans les conditions du réseau, il est difficile de détecter des comportements égoïstes des nœuds DTN ou prédéterminer le chemin de routage. Par conséquent, ces défis dans DTNs font les protocoles d'incitation en vigueur, qui s'appuient généralement sur un routage simultané. Pour améliorer la performance de DTNs en termes de taux de livraison élevé et le délai moyen faible, Ru et *al.* dans [67] proposent le protocole d'incitation pratique, appelé Pi, pour résoudre le problème de l'égoïsme dans DTNs. Dans le protocole Pi, lorsque le nœud source DTN envoie un paquet, il ne fixe pas un chemin de routage à l'avance, mais a

seulement besoin d'attacher une certaine incitation sur le paquet. Ensuite, les nœuds DTN égoïstes sur la route pourraient être incités à aider à transmettre le paquet pour améliorer le taux de livraison et de réduire le délai moyen des réseaux DTNs entiers. Les contributions de cette proposition sont de trois ordres.

- Ru et *al.* dans [67] commencent à proposer un modèle d'incitation équitable dans lequel les nœuds DTN égoïstes sont stimulés pour aider les paquets avec l'incitation à base de crédit ainsi que d'incitation basé sur la réputation.
- Afin de garantir la faisabilité du modèle d'incitation équitable, les auteurs utilisent le modèle de pièce en couches et des techniques de signature vérifiable cryptées pour fournir l'authentification et la protection de l'intégrité dans le protocole Pi.
- Afin de confirmer l'efficacité du protocole Pi, les auteurs développent également un simulateur personnalisé construit en Java où il a montré nettement que le protocole Pi peut atteindre le ratio élevé de livraison et le faible délai moyen de DTNs lorsque la grande incitation est fournie.

Le reste de cette section est organisée comme suit. Dans la sous section 3.5.1, nous présentons les modèles et les objectifs de conception. Ensuite, nous présentons le fonctionnement du protocole Pi dans la sous section 3.5.2, suivie l'analyse du protocole à la sous section 3.5.3.

3.5.1 Modèles et objectifs de conception

Dans cette sous section, nous présentons le modèle de réseau, le modèle de nœud, et les objectifs de conception.

3.5.1.1 Le modèle de réseau

Les réseaux DTNs se caractérisent généralement par la connectivité non garantie et la faible fréquence des rencontres entre une paire de nœuds au sein du réseau. Dans le modèle proposé dans [67], les auteurs considèrent un réseau DTN comme un graphe direct $= (V, E)$, où V et E représente l'ensemble de nœuds du DTN et d'arêtes de contact opportunistes, respectivement. Dans le DTN, un nœud source S peut délivrer des paquets à la destination D via le mouvement des nœuds DTN avec l'algorithme de transfert correct des données.

3.5.1.2 Le modèle de nœud

En DTNs, les comportements égoïstes des nœuds DTN sont naturellement provoqués par des entités humaines qui les contrôlent. Dans le modèle proposé [67], afin d'étudier les nœuds DTN égoïstes d'une manière non abstraite, les auteurs prennent le réseau ad hoc des véhicules comme un réseau à tolérance de retard, où chaque nœud DTN est instancié par un véhicule conduit par des gens qui courent dans une ville avec une certaine vitesse.

Dans les véhicules DTNs, chaque véhicule est équipé avec un dispositif de communication OBU, qui permet à différents véhicules de communiquer les uns avec les autres sur la base du protocole 802.11p. Il est à noter que la couche physique 802.11p offre des débits différents, allant de 3 à 27 Mbps, à partir de laquelle le dispositif OBU peut choisir. Par conséquent, lorsque deux véhicules sont dans la portée de transmission, par exemple, à 300 mètres, ils peuvent échanger des paquets. En général, un véhicule a presque des ressources illimitées,

tandis que le dispositif de communication OBU équipé est considéré avec des ressources limitées, i.e., un tampon et des contraintes de puissance de calcul. Cependant, il peut exister plusieurs nœuds DTN égoïstes dans les réseaux. Afin d'économiser de l'espace tampon, ces nœuds DTN égoïstes peuvent être très réticents à la coopération qui n'est pas directement bénéfique pour eux. En conséquence, l'égoïsme serait contraire à l'objectif de la DTN véhicules à livrer en collaboration avec un paquet de sa source S à la destination D. Par conséquent, la probabilité de coopération d'un nœud DTN égoïste peut être modélisée comme suit

$$P_c = \alpha P_s + (1-\alpha)P_u = \alpha P_s + 1 - \alpha$$

où $0 \leq \alpha \leq 1$ est le facteur égoïste, $P_s < 1$ est la probabilité de coopération dans des conditions égoïste, i.e.,$P_s = 0.01$, tant que $P_u = 1$ désigne la probabilité de coopération désintéressée. En clair, si $\alpha = 0$, un nœud DTN est désintéressé, i.e., il est toujours prêt à aider avec le transfert avec une probabilité $P_c = 1$. Au contraire, si $\alpha = 1$, le noeud DTN est égoïste, la probabilité de coopération est juste $P_c = P_s = 0{,}01$. Par conséquent, plus le facteur égoïste α est petit, plus la coopération est meilleure dans DTNs.

3.5.1.3 Les objectifs de conception

L'objectif de conception est de développer un protocole pratique d'incitation pour stimuler les nœuds DTN égoïstes afin d'améliorer la coopération de probabilité P_c dans les réseaux véhiculaires. Plus exactement, les deux objectifs souhaitables suivants seront atteints dans le protocole Pi.

- *Améliorer les performances de DTN avec stimulation*: Afin d'éviter la dégradation de la performance globale, i.e., le taux faible de livraison et le délai moyen élevé, en raison des nœuds DTN égoïste dans DTNs, la stratégie d'incitation à base de crédit est adoptée.
- *Équité (Fairness)* : Dans le protocole pratique d'incitation, l'équité est également envisagée. Concrètement, les nœuds DTN de transfert intermédiaires peuvent recevoir des crédits si et seulement si le nœud de destination reçoit les paquets, ce qui est juste pour le nœud source.

Stratégie d'encouragement

Pour atteindre les objectifs ci-dessus, Ru et *al.* [67] adoptent la stratégie d'incitation hybride suivante :

- Dans le DTN véhicules, un véhicule peut communiquer avec TA pour l'autorisation quand il entre en contact avec certains RSUs. Pour chaque nœud DTN, PCA (Personal Credit Account) stocke ses crédits, tandis que PRA (Personal Reputation Account) enregistre sa réputation de valeur dynamique comme suit: soit $R_{IP(n-1)}$ la valeur de réputation du nœud DTN au temps T_{n-1}. La nouvelle valeur de réputation $\mathrm{R}_{IP(n)}$ au temps T_n est formulée comme $\mathrm{R}_{IP(n)} = e^{-\lambda T_i} \cdot \mathrm{R}_{IP(n-1)} + C_{T_i}$, où $T_i = T_n - T_{n-1}$, λ est la vitesse à laquelle la valeur de la réputation diminuerait, et C_{T_i} représente

la fonction cumulative de réputation, qui est la somme des valeurs nouvelles de la réputation acquise dans la période de temps T_i .

- Il n'est pas obligatoire pour le nœud DTN intermédiaire de transmettre les paquets. Tous les nœuds intermédiaires dans le réseau DTN peuvent déterminer son opinion si oui ou non pour participer dans le transfert de paquet. Cependant, une fois un nœud DTN intermédiaire participe au transfert du paquet, il peut obtenir les crédits du nœud source ainsi que les valeurs de la réputation du TA.
- Si le groupe n'arrive pas au nœud destination, le nœud source ne sera pas besoin de payer des crédits. Toutefois, ces nœuds intermédiaires qui ont participé avant peuvent toujours obtenir de bonnes valeurs de la réputation du TA.

La conception du calcul de la récompense est le pivot d'un protocole pratique d'incitation, qui devrait guider les nœuds DTN égoïstes de suivre le protocole pour aider au transfert des paquets. Ru et *al.* dans [67] proposent le calcul de récompense, ci-après :

$$\text{Reward}_\text{i} = \begin{cases} Dis_i.\,\text{C}_{IP} + Dis_i.\,\text{R}_{IP}, \text{si B arrive au D;} \\ Dis_i.\,\text{R}_{IP}, \text{sinon.} \end{cases}$$

où C_{IP} est l'unité de crédit d'incitation fournie par la source S, R_{IP} est la valeur de l'unité de réputation défini par TA pour l'optimisation du réseau. Supposons que C_F est le coût des ressources de l'unité utilisée pour le transfert, les auteurs définissent le *facteur gagnant* du nœud DTN N_i comme suit

$$\zeta_i = \frac{Dis_i.\,\text{C}_{IP} - Dis_i.\,\text{C}_F}{Dis_i.\,\text{C}_F} = \frac{\text{C}_{IP}.\,\text{C}_F}{\text{C}_F}$$

et la probabilité de coopération du N_i avec sa valeur de réputation R_{IP} comme suit

$$P_c = \begin{cases} 1, si\ R_{IP} < R_{th}; \\ sinon\ si\ R_{IP} \geq R_{th}; \\ 1,\ \ \alpha_i - \zeta_i \leq 0; \\ (\alpha_i - \zeta_i)P_s + 1 - (\alpha_i - \zeta_i),\ \alpha_i - \zeta_i > 0 \\ end\ if \end{cases}$$

Enfin, avec la probabilité de coopération P_c, le nœud DTN N_i est intéressé à aider le transfert du paquet.

Modèle de la pièce en couches (Layered Coin Model)

Pour garantir le bon fonctionnement de la stratégie incitative, l'incitation doit être sécurisée. Par conséquent, dans l'implémentation du protocole Pi, les auteurs utilisent la pièce couchée pour stimuler la diffusion des paquets. La pièce couchée se compose généralement d'une couche de base formée par le nœud source et de multiples couches approuvées formées par les nœuds intermédiaires. Fig. 3.16 montre un exemple de l'architecture de la pièce en couches, où $(S, L_s), (D, L_d), (N_i, L_i)$ sont le nœud source et son emplacement, le nœud de destination et de son emplacement, et le i-ème nœud intermédiaire et l'emplacement qu'il entre en contact avec le i + 1-ième nœud, respectivement.

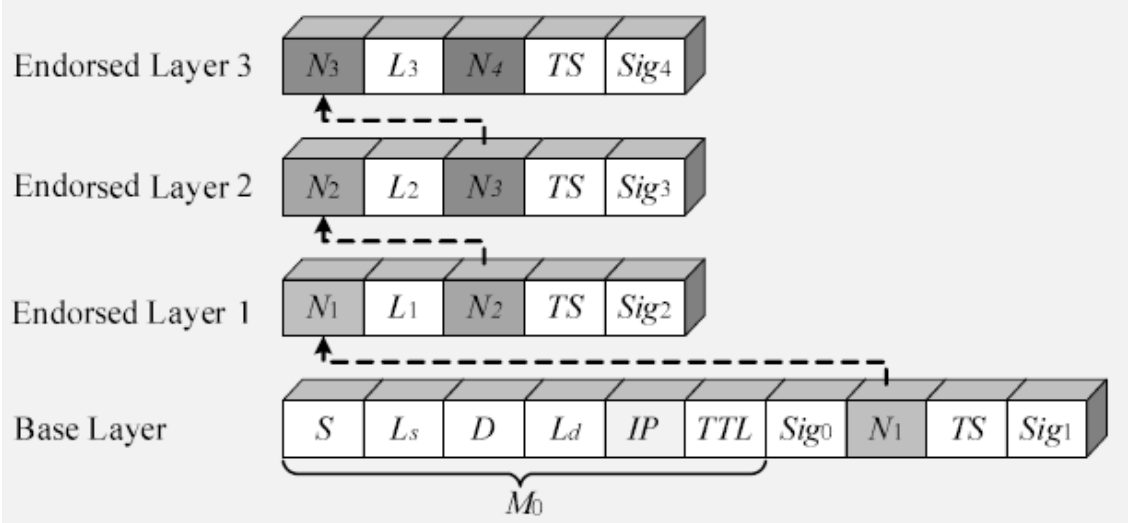


Figure 3:16 Un exemple de l'architecture de la pièce en couches, proposé par Ru et al. [67]

3.5.2 Fonctionnement du protocole Pi

Dans cette sous section, nous allons présenter le fonctionnement du protocole Pi pour résoudre le problème de l'égoïsme dans DTNs, qui se compose principalement de quatre parties: l'initialisation du système, la génération du paquet, le transfert du paquet, et le charge et le récompense.

3.5.2.1 L'initialisation du système

Soit tous les nœuds $\mathcal{N} = \{N_1, N_2, \cdots\}$ et le TA utilisent une suite de paramètres du système. Soit le paramètre de sécurité k, les paramètres bilinéaires $(q, g, \mathbb{G}, \mathbb{G}_T, e)$ sont d'abord générés en exécutant $\mathcal{CG}en(k)$. Après, une fonction de hachage résistante aux collisions $:\{0,1\}^* \rightarrow \mathbb{Z}_n^*$, et un algorithme de chiffrement symétrique sécurisé $Enc()$. A la fin, le paramètre du système $params = (q, g, \mathbb{G}, \mathbb{G}_T, e, h, Enc)$ sera publié.

Chaque nœud DTN avec son identité unique $N_i \in \mathcal{N}$ choisi un nombre aléatoire $x_i \in \mathbb{Z}_n^*$ comme ses clés privés et calcule sa clé publique correspondante comme suit $y_i = g^{x_i}$. A chaque moment, chaque nœud DTN $N_i \in \mathcal{N}$ aussi enregistre son compte de crédit personnel (Personal Credit Account (PCA)) et le compte de crédit de réputation (Personal Reputation Account (PRA)) pour le TA. Il est à noter que toutes les clés publiques dans le système seront certifiées par les certificats de clé publique délivrés par l'autorité de compétente. En outre, la valeur de réputation de chaque nœud DTN R_{IP} durant la période est signée par le TA et où chacun peut la vérifier.

3.5.2.2 La génération du paquet

Quand le nœud source S avec la paire clé privée $(x_s, y_s = g^{x_s})$ au emplacement L_s va envoyer le paquet m au nœud de destination D avec la paire clé $(x_d, y_d = g^{x_d})$ au emplacement L_s, S va exécuter les étapes suivantes :

Etape(1). Calcule la clé statique du partage $k_{sd} = y_d^{x_s} = g^{x_s x_d}$ entre S et D, et encrypte le paquet m dans B $= Enc(m)$ pour achever la confidentialité.

Etape(2). Détermine le IP, et vérifie la signature encryptée σ_0 sur $M_0 = S||L_s||D||L_d||IP||TTL$ et B comme $\sigma_0 = y_d^{(H(M_0||B)+x_s)^{-1}}$.

Etape(3). Vérifier la validité du ACK[18] par la vérification de l'équation $(\sigma_1^*, g^{H(M_0||N_1||L_s||TS)}.y_1)? = e(g,g)$. Si elle est valide, S génère la signature σ_1 sur $M_0||N_1||L_s||TS$ comme $\sigma_1 = g^{(H(M_0||N_1||L_s||TS)+x_s)^{-1}}$. Sinon, *S* néglige le ACK.

Etape(4). Régler la couche de base en tant que BL $= (M_0||\sigma_0||N_1||TS||\sigma_1)$ et transfert le paquet B conjointement avec la couche de base BL au nœud intermédiaire N_1 comme suit :

$$S \rightarrow N_1 : \text{B}, \text{BL}$$

Après la vérification du $\sigma_1 = g^{(H(M_0||N_1||L_s||TS)+x_s)^{-1}}$ en vérifiant $e(\sigma_1, g^{H(M_0||N_1||L_s||TS)}.y_s)\ ? = e(g,g)$, N_1 commence à transmettre le paquet.

3.5.2.3 Le transfert du paquet

Quand le paquet s'approche du l'emplacementL_1, le nœud intermédiaire N_1 estime qu'il ne peut pas porter le paquet B à proximité du noeud destination D et transmet le paquet au prochain saut du noeud DTN en exécutant l'algorithme 3.7. De même, chaque nœud de retransmission ultérieure utilise également l'algorithme 3.7 pour transmettre les paquets. Sans perte de généralité, le paquet B arrive au niveau du nœud de destination D avec un routage opportuniste $S \longrightarrow N_1 \longrightarrow N_2 \longrightarrow \cdots \longrightarrow N_l \longrightarrow D$, comme présenté dans la figure 3.17. Plus de détail sur cette étape, les lecteurs peuvent se rapporter à l'article de la référence [67].

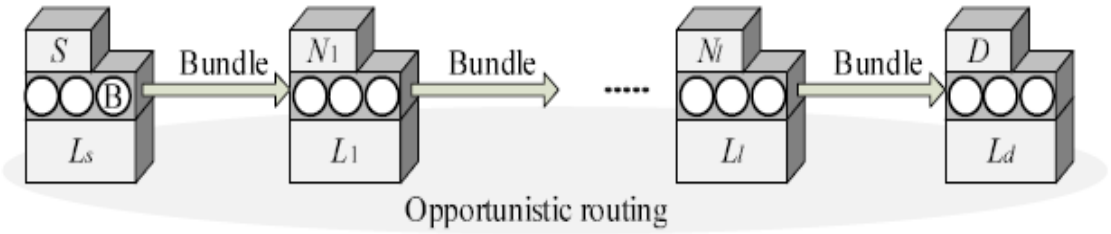


Figure 3:17 Un routage opportuniste, proposé par Ru et al. [67]

[18] L'accusé de réception de l'intérêt (Interest Acknowledgement (ACK))

Data: When approaching to the location L_1, the node N_1 sets a *holding time to wait next-hop node* (T_h), and tries to forward the bundle B to the next-hop DTN node within T_h
procedure BUNDLE FORWARDING
  if a DTN node N_2 is interested in forwarding within T_h **then**
    N_1 checks the possible location L_2 that N_2 can carry the bundle B to
    if location L_2 is closer to the destination D than L_1 **then**
      N_1 forwards the bundle B to N_2
    else
      N_1 continues to wait other DTN node which is interested in forwarding
    end if
  else
    when there is no DTN node which is interested in forwarding the bundle at location L_1, N_1 has to drop the bundle packet, since the next-hop route is not immediately available
  end if
end procedure

Algorithme 3:7 L'algorithme de transfert du paquet dans Pi, proposé par Ru *et al.* [67]

3.5.2.4 La charge et le récompense

Lorsque le dernier nœud intermédiaire N_i dispose d'une connexion rapide disponible avec TA, N_i envoie ses rapports $(\sigma_1, \dots, \sigma_l)$ au TA. Après, le TA effectue l'autorisation de crédit et la réputation juste en exécutant que les étapes suivantes.

Etape(1). Le TA vérifie la fraîcheur et la validité de $(\sigma_1, \dots, \sigma_l)$. Si elles sont fraîches et valides, le TA continue, sinon l'opération se termine.

Etape(2). Basé sur les emplacements $(L_s, L_1, \dots, L_l, L_d)$ dans les signatures, le TA mesure la distance de relais réelle de chaque nœud intermédiaire. Ensuite, conformément à la politique d'incitation en IP, le TA enregistre les crédits mérités et les valeurs de réputation à chaque nœud intermédiaire de PCA et PRA, et retire les valeurs de crédit correspondant du PCA du nœud source, comme présenté dans l'algorithme 3.8.

Data: The TA obtains valid signatures $(\sigma_1, \cdots, \sigma_l)$ from the last intermediate node N_l
procedure CREDIT AND REPUTATION CLEARANCE
  get the location information $(L_s, L_1, \cdots, L_l, L_d)$ from these signatures
  measure each intermediate node N_i's actual relay distance Dis_i, where $Dis_1 = |L_1 - L_s|$, $Dis_l = |L_d - L_l|$ and $Dis_i = |L_i - L_{i-1}|$, where $2 \leq i \leq l$
  for $i = 0$ to l **do**
    according to the incentive policy in IP, withdraw $C_i = L_i \times C_{\text{IP}}$ from the source node S's PCA, and store the merited credits C_i in N_i's PCA
    store $R_i = Dis_i \times R_{IP}$ reputation values in N_i's PRA based on the reputation calculation
  end for
end procedure

Algorithme 3:8 L'algorithme de dégagement du crédit et réputation dans Pi, proposé par Ru *et al.* [67]

Si le paquet n'atteint pas le nœud de destination D, chaque nœud intermédiaire $N_i \in \mathcal{N}$, qui a aidé le transfert, peut encore obtenir la bonne valeur de la réputation en soumettant σ_i et σ_{i+1}^*. Plus de détail sur cette étape, voir l'article de la référence [67].

3.5.3 L'analyse du protocole

- Ru et *al.* dans [67] ont prouvé que le protocole Pi offert la motivation ainsi résistant à l'attaque de parasitisme, l'attaque de suppression des couches, et l'attaque de l'ajout des couches.
- La métrique de performance utilisée dans l'évaluation [67] est : i) le rapport de livraison, qui est la fraction de messages générés qui sont correctement livrés à la destination finale dans une période de temps donnée; ii) le retard moyen, qui est défini comme le temps moyen entre le moment où un message est généré au niveau d'une source et lorsqu'il est remis avec succès à sa destination. Utilisant un simulateur personnalisé construit en Java et avec l'exécution de la simulation 10.000 fois, les résultats ont montré le rapport de la livraison sans incitation est très faible, en particulier lorsque le rapport égoïste $\rho = 90\%$.

3.6 Conclusions

Dans ce chapitre, nous avons examiné cinq protocoles SPRING [62], SPF [64], PCS [65], FLIP [66] et Pi [67] afin de les comparer avec nos deux contributions proposées dans le chapitre 4 et 5. Dans le chapitre suivant, nous présentons notre modèle de sécurité ECPDR pour résoudre certains problèmes de sécurité et de confidentialité dans les réseaux sociaux mobiles.

Chapitre 4 ECPDR: La stratégie d'une réponse à la demande pour la sécurisation et la confidentialité des réseaux sociaux mobiles

Dans le chapitre précédent, nous avons examiné cinq schémas pour la sécurisation et la confidentialité des réseaux véhiculaires ad hoc sociaux. Dans ce chapitre, nous introduisons le schéma ECPDR [J2] où nous allons nous concentrer sur la façon de détecter et prévenir une attaque avec la forte protection de la confidentialité en utilisant la stratégie d'une réponse à la demande.

4.1 Introduction

Au cours des dernières années, plusieurs techniques de confidentialité ont été proposées [45] [46], pour les réseaux de capteurs [47], les systèmes de santé en ligne [48], les communications véhiculaires [49], et les communications de réseau intelligent [50]. Toutefois, en raison des caractéristiques uniques du réseau ad hoc social (ADSocial) [B2]; ces schémas ne sont pas applicables aux attaques de routage dans ADSocial. Une des raisons est que ces schémas ne considèrent pas la vie privée de l'utilisateur requise dans ADSocial. Aussi, ces schémas n'ont pas non plus tenu compte des caractéristiques des réseaux Ad hoc, i.e., la topologie dynamique où les nœuds sont libres de se déplacer arbitrairement, de sorte que la topologie du réseau peut changer aléatoirement et rapidement à n'importe quel moment, et peut consister deux liaisons unidirectionnelles ou bidirectionnelles. Cette évolution a naturellement un impact sur la morphologie du réseau et peut modifier le comportement du canal de communication. Par conséquent, il est nécessaire de concevoir un système sûr et efficace préservant la confidentialité pour le réseau social dans un environnement ad hoc.

Dans ce chapitre, nous introduisons un schéma efficace préservant la confidentialité conditionnelle avec la stratégie d'une réponse à la demande, appelé ECPDR, pour les communications ad hoc sociales,dans le but de faire face à des défis en matière de sécurité et de performance dans les réseaux sociaux ad hoc. Avec le schéma ECPDR proposé, chaque nœud utilisateur peut préserver la confidentialité et être authentifié avant de rejoindre les autres nœuds en utilisant le protocole de routage. Les contributions de ce chapitre sont de quatre ordres.

- Premièrement, nous formalisons le modèle du système où nous considérons les caractéristiques sociaux, i.e., la mobilité humaine, le groupe humain et les préférences dans un réseau ad hoc qui se compose d'une autorité de confiance (TA), des unités stationnaires sociales (SU) déployées à l'espace social, et un grand nombre de mobiles équipés de la technologie sans fil en mouvement sur un espace social.
- Deuxièmement, nous proposons un schéma de certificat efficace, où le TA délivre la clé privée SK_{n_i} et le certificat $\mathrm{Cert}_{\mathrm{TA},n_i}$ utilisant l'algorithme de signature *Schnorr* [35]. Le nœud n_i peut vérifier le certificat $\mathrm{Cert}_{\mathrm{TA},n_i}$ par la procédure $S.check$ et il ne peut pas utiliser ce certificat directement dans la communication ad hoc sociale. Basé sur la technologie cryptographique proxy re-signature [52], le nœud demande la clé de re-signature depuis S_x et puis re-signe les certificats délivrés par le TA. Avec cette méthode de distribution des clés, le schéma garantie la confidentialité de l'identité de l'utilisateur.
- Troisièmement, nous fournissons la préservation conditionnelle de la confidentialité pour les nœuds avec une réponse à la demande. Bien que le SU agir comme des émetteurs de certificats dans ECPDR, les adversaires ne savent pas que les certificats sont détenus par un nœud. Par conséquent, les adversaires ne peuvent pas aussi retracer les nœuds intéressés même s'ils avaient compromis les SUs. Ensuite, pour détecter et prévenir les attaques contre les protocoles de routage , le schéma proposé se base sur trois messages de contrôles $\{Detectreq, Detectrep, Notifreq\}$, chaque nœud initie une demande de réponse et envoie $Detectreq$ signé aux nœuds voisin à 1-saut, et attend la réponse à sa demande pour exécuter la phase de notification. Après avoir reçu une réponse à la demande, le nœud vérifie sa signature. Si la signature est *valide* et $TDetect_{n_i} < 0$, il considère que le lien avec le noeud est prouvé. Sinon, il retourne *suspect* et commence la phase de notification.
- Finalement, pour valider l'efficacité de la proposition ECPDR, nous l'intégrerons dans l'implémentation du protocole de routage AODV. Les résultats des simulations approfondies dans le premier scénario du schéma ECPDR proposé peut détecter l'attaque du trou noir de plus dans la configuration où l'attaque est lancée sur un nombre de plus de saut. Ainsi, dans le second scénario, nous nous concentrons sur le délai de transmission du schéma ECPDR au niveau du nœud avec une vaste évaluation des performances, qui convainc davantage sa pratique.

Le reste de ce chapitre est organisé comme suit. La section 4.3 présente le modèle du système, et les objectifs de la recherche. La Section 4.4 donne quelques préliminaires, y compris la fonction de hachage sécurisée, les appariements bilinéaires et la technique des signatures courtes. Ensuite, la section 4.5 présente le schéma ECPDR proposé, suivie par l'analyse de la sécurité et de l'évaluation de la performance dans les sections 4.6 et 4.7, respectivement. Nous comparons notre proposition avec d'autres protocoles dans la section 4.8. Enfin, la section 4.9 attire notre conclusion.

4.2 Modèle du système et objectifs de la recherche

Dans cette section, nous formalisons le modèle du système et les objectifs de la recherche.

4.2.1 Le modèle du système

Les réseaux mobiles ad hoc (MANET) disposent d'un large éventail d'applications. En fait, ils sont robustes, peu coûteux et adaptables à la fois en milieu urbain et en zones rurales. Parmi les applications, on inclut: les applications militaires, les opérations de sauvetage, les applications commerciales, les réseaux véhiculaires (VANET) ou les réseaux sociaux véhiculaires (VSN). Dans notre travail, nous considérons les caractéristiques sociales (la mobilité humaine, le groupe humain et les préférences) dans un MANET typique qui se compose d'une autorité de confiance (TA), certaines unités sociales stationnaires (SU) déployées dans l'espace social, et un grand nombre de mobiles équipés de la technologie sans fil se déplaçant sur un espace social, comme le montre la Fig. 4.1.

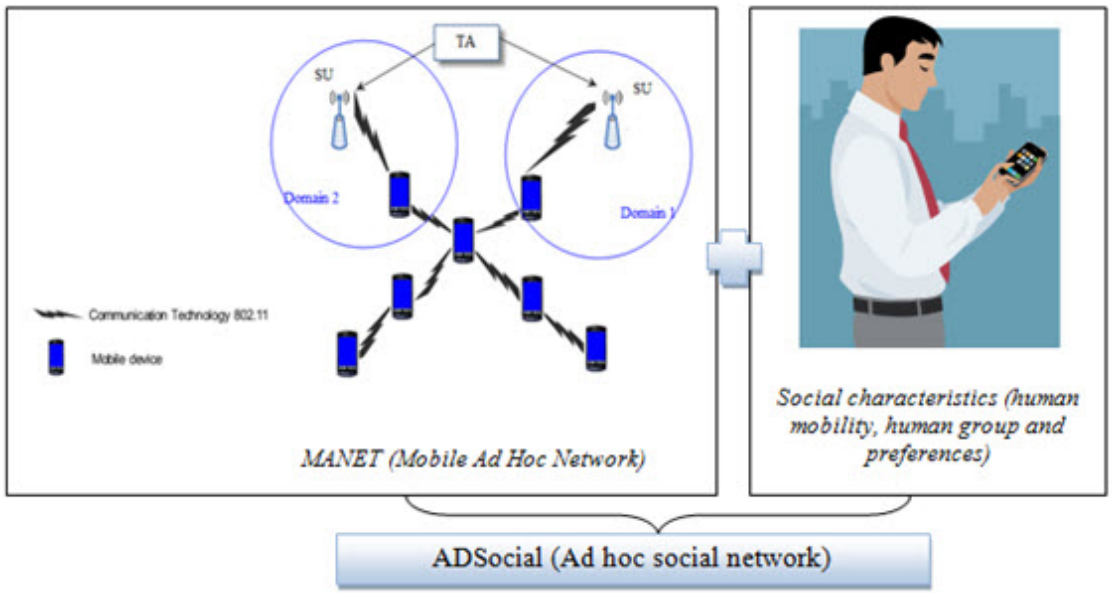


Figure 4:1 Le modèle du système ADSocial

- Le TA est pleinement approuvé par toutes les parties dans le système et en charge de l'enregistrement des SUs et les appareils mobiles. Aussi, le TA est supposé sous tension avec une capacité de stockage suffisante et il est impossible pour n'importe quel adversaire à faire des compromis.
- Le SU se connecte avec le TA par des liaisons filaires dans le système. Ils offrent un service de diffusion de l'information et de certificat à jour.
- Formellement, comme un réseau ad hoc sans fil, le ADSocial peut être représenté comme un graphe non orienté $\mathcal{G} = (\mathcal{V}, \mathcal{E})$, où $\mathcal{V} = \{v_1, v_2, \dots\}$ est l'ensemble de tous les nœuds $\mathcal{N} = \{n_1, n_2, \dots\}$, et $\mathcal{E} = \{(v_i, v_j) | \, v_i, v_j \in \mathcal{V}\}$ est l'ensemble des arêtes (voir la figure. 4.2). Soit $d(v_i, v_j)$ désigne la distance entre v_i et v_j et e_{ij} indique que s'il existe une arête de communication entre deux noeuds v_i et v_j ou pas, est définie comme suit

$$e_{ij} = \begin{cases} 1, & d(v_i, v_j) \leq R; \\ 0, & d(v_i, v_j) > R; \end{cases}$$

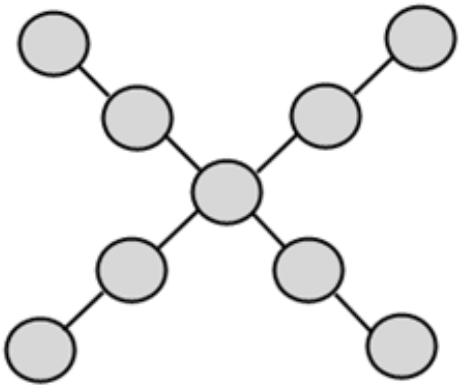


Figure 4:2 ADSocial sous consideration $\mathcal{G} = (\mathcal{V}, \mathcal{E})$

4.2.2 Les objectifs de la recherche

Depuis que le réseau ad hoc social est devennu un scénario de réseau sans fil à grande échelle pour le service public, il est confronté gravement pour la sécurité et les défis de la confidentialité. Dans le schéma ECPDR, nous visons à atteindre la sécurité et les objectifs de protections suivantes :

- **La disponibilité**. Cette propriété implique que les services ou les ressources demandées sont disponibles en temps opportun, même si il y a un problème ou un dysfonctionnement dans le système. Dans notre contexte, il est nécessaire de garantir l'accès au service de routage à tout moment.
- **L'authentification**. Cela comprend l'authentification des utilisateurs et l'intégrité du message. Tous les messages doivent être acceptés par les membres juridiques et délivrés sans changement ou modification.
- **La confidentialité du contenu orienté**. Assurer cette propriété nous mène à atteindre les trois propriétés suivantes:
  - **L'immutabilité**. Cette propriété indique qu'il doit être impossible de modifier une partie du message désigné comme non modifiable par le signataire, tout en conservant une signature valide.
  - **La transparence (confidentialité)**. Il devrait être impossible de déterminer si un message a été désinfecté ou non. Cela peut être utile dans les applications où l'on ne devrait pas pouvoir faire de la discrimination contre les messages produits par le désinfectant. Cette propriété implique aussi la confidentialité. Si l'adversaire contre la confidentialité existante, il est capable de récupérer le message original à partir des messages changés. Ainsi, il sera possible d'utiliser cet adversaire pour construire un adversaire contre la transparence.

- **La responsabilité**. Il devrait être impossible à réaliser, par une personne autre que le signataire, une signature originale ou une signature modifiée. Aussi, en cas de problèmes sur l'origine de la signature, il doit être en mesure de trouver correctement qui est à l'origine de la signature.

4.3 Préliminaires

Dans cette section, nous présentons des préliminaires, y compris les chaînes de hachages sécurisées [57], la technique de couplage bilinéaire [25] [30], et la technique de signatures courtes [26], qui sont les fondements de notre schéma ECPDR proposé. En outre, les notations utilisées dans ce chapitre sont présentées dans le tableau 4.1.

4.3.1 Les chaînes de hachages sécurisées

Une chaîne de hachage est une fonction à sens unique, en particulier, elle permet de réduire une chaîne de bits de n'importe quelle taille $\{0,1\}$ dans un digest de taille fixe $\{0,1\}^{\lambda}$ avec λ un paramètre de sécurité.

Définition 4.1 (Une fonction de hachage cryptographique sécurisée $\mathcal{H}$) : *Une fonction de hachage $\mathcal{H}:\{0,1\}^{*} \rightarrow \{0,1\}^{\lambda}$, avec λ un paramètre de sécurité, est dite crypto graphiquement sûre si elle vérifie les trois propriétés suivantes.*

- ***Résistance à la pré-image**, étant donné $y \in \{0,1\}^{\lambda}$, quel que soit l'adversaire, sa probabilité de trouver x comme $\mathcal{H}(x) = y$ est négligeable. Ceci correspond à la définition d'une fonction à sens unique;*
- ***Résistance à la seconde pré-image**, étant donné $x \in \{0,1\}^{*}$, quel que soit l'adversaire, sa probabilité de trouver $x' \neq x$ telle que $\mathcal{H}(x) = \mathcal{H}(x')$ est négligeable ;*
- ***Résistance aux collisions**, quel que soit l'adversaire, sa probabilité de trouver un couple (x, x') tel que $\mathcal{H}(x) = \mathcal{H}(x')$ et $x' \neq x$ est négligeable.*

4.3.2 La technique de couplage bilinéaire

Soient $\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T$ trois groupes cycliques d'ordre premier q. Un couplage est une application $e : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$ ayant les trois propriétés suivantes.

- Calculable, pour tout $(x, y) \in \mathbb{G}_1 \times \mathbb{G}_2$, il existe un algorithme efficace pour calculer $e(x, y)$;
- Bilinéaire, pour tout $(x, y) \in \mathbb{G}_1 \times \mathbb{G}_2$, et tout $(a, b) \in \mathbb{Z}_q^2, e(x^a, y^b) = e(x, y)^{ab}$;
- Non-dégénérée, il existe g_1 générateur de $\mathbb{G}_1$ et g_2 générateur de $\mathbb{G}_2$ tel que $e(g_1, g_2) \neq 1_{\mathbb{G}_T}$.

Définition 4.2 (Le problème Diffie-Hellman (SDH)): *Soit* $(q, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e, g_1, g_2)$ *un environnement bilinéaire d'ordre premier* q. *Soit* $(g_1, g_2, g_2^x, g_2^{x^2}, \dots, g_2^{x^q})$ *avec* x *choisi aléatoirement dans* $\mathbb{Z}_q$ *, le problème SDH est de trouver le couple* $(c, g_1^{\frac{1}{x-c}})$ *avec* $c \in \mathbb{Z}_q$.

Symbole	Notation
ADSocial	Ad hoc Social Network
n_i	Le nœud i dans ADSocial
$Detectreq$	Le message d'une réponse demandée
$Detectrep$	Le message d'une réponse à la demande
$Notifyreq$	Le message de notification
T	Le temps actuel
$TNormal_{\text{Detectreq}}$	Le temps pour envoyer le message $Detectreq$
K	La clé temporaire
H_1, H_2	Une fonction de hachage
$S.Init$	Générer un environnement bilinéaire
$S.GenK$	Générer la clé privée
$S.Sign(K, SK_{n_i}, Detectreq)$	Signer le message $Detectreq$ avec la clé temporaire K et la clé privée SK_{n_i}
$S.Check\ (Detectreq, \sigma_{n_i,Detectreq}, K)$	Vérifier la signature $\sigma_{n_i,Detectreq}$ du message $Detectreq$ avec la clé temporaire K
$Enc_s\ (.)$	Un algorithme de chiffrement symétrique sécurisé avec la clé secrète s
‖	La concaténation
Send_Request (C)	Envoyer le message C
PID_{n_i}	L'identité pseudo du nœud n_i
SK_{n_i}	La clé privée du nœud n_i
PK_{n_i}	La clé publique du noeud n_i
σ_{TA,n_i}	Une signature signée par TA pour n_i
$\text{Cert}_{\text{TA},n_i}$	Le certificat du noeud n_i délivré par TA
ΔT	L'exigence de la vie privée sur la longueur de la période de validité d'un certificat
S_x	Le x-ième SU
$TDetect_{n_i}$	Le temps de détection des attaques du noeud n_i
R	La transmission maximale
SD	La vitesse de la lumière
$SIMS$	Short Inter-Message Space

Tableau 4:1 Les notations utilisées dans ECPDR

4.3.3 La technique de signature courte

La technique de signature courte est définie par les quatre algorithmes suivants:

- $\boldsymbol{S.Init(1^{\lambda})}$. Cet algorithme génère un environnement bilinéaire $(q, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, g_1, g_2, e, \psi)$. $\mathbb{G}_1, \mathbb{G}_2$ deux groupes d'ordre premier q avec $g_1$est le générateur de $\mathbb{G}_1$ et g_2 le générateur de $\mathbb{G}_2$. ψ est un isomorphism où $g_2 = \psi(g_1)$. Nous notons $S.param$ =$(\lambda, q, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, g_1, g_2, e, \psi)$ comme paramètre d'entré.
- $\boldsymbol{S.GenK(S.param)}$. Cette procédure sélectionne aléatoirement r et r' dans $\mathbb{Z}_q^*$ et calcule $u = g_1^r \in \mathbb{G}_1$ et $v = g_2^{r'} \in \mathbb{G}_2$. Nous notons $z = e(g_1, g_2) \in \mathbb{G}_T$. La clé secrète du signataire est:

$$SK = (S.param, u, v, z)$$

- $\boldsymbol{S.Sign(PK, SK, m)}$. C'est l'algorithme de signature. Il prend en entrée la clé de signataire (PK, SK) et le message m . Le signataire choisi aléatoirement $r \in \mathbb{Z}_q^*$ où $x + m + yr \neq 0 \; mod \; q$ et calcule:

$$A = g_1^{\frac{1}{x+m+yr}}$$

Le signataire obtient la signature $\sigma = (A, r)$ du message m.

- $\boldsymbol{S.check(m, \sigma, PK)}$. Avec cette procédure, le vérificateur vérifie que $\sigma = (A, r)$ est une signature du signataire, désigné par la clé public $PK = (S.param, u, v, z)$ avec la vérification de l'équation suivante:

$$e(A, u \,.\, g_2^m \,.\, v^r) = z$$

Si l'équation (4.4) est valide, il retourne vraie, sinon il retourne faux.

4.4 Notre schéma ECPDR proposé

Dans cette section, nous présentons notre schéma ECPDR, qui se compose de six phases: 1) l'initialisation du système; 2) le pseudo identité, la clé privée et le certificat délivré par le TA; 3) La mise à jour du certificat; 4) la signature et la vérification du message; 5) la réponse demandée; et 6) la réponse à la demande.

4.4.1 L'initialisation du système

Supposons qu'il existe une autorité de confiance TA dans le système, qui initialise l'ensemble du système. Pour le protocole de routage, l'AODV initialise trois messages de contrôles $\{Detectreq, Detectrep, Notifreq\}$, qui ont le même format du message de demande RREQ et comprend trois parties, à savoir, le coûts de signature, le coût de la vérification, et les frais généraux de la communication (y compris le certificat et la signature, comme indiqué dans le tableau 4.2). Ensuite, le TA initialise le système en exécutant les étapes suivantes.

1) Le TA commence à initialiser les paramètres de sécurité en exécutant $S.Init(1^{\lambda})$ pour générer un environnement bilinéaire $(q, \mathbb{G}_1, \mathbb{G}_2, g_1, g_2, e, \psi)$, où (λ, l_1) sont les paramètres de sécurité.

2) Le TA sélectionne r et r' dans $\mathbb{Z}_q^*$ et calcule $u = g_1^r \in \mathbb{G}_1$ et $v = g_2^{r'} \in \mathbb{G}_2$, et choisi un nombre aléatoire $s \in \mathbb{Z}_q^*$ comme une clé master. Puis, il choisi deux fonctions de hachage cryptographique sécurisées H_1, H_2 , où $H_1 : \{0,1\}^* \to \mathbb{G}_1$, $H_2 : \{0,1\}^* \times \mathbb{G}_2 \to \{0,1\}^{l_1}$, et un algorithme de chiffrement symétrique sécurisé $Enc_s(.)$.
3) Le TA choisit ΔT selon les exigences de la vie privée de la plupart des nœuds et fixe la durée de validité du certificat égale à ΔT.
4) Le TA publie dans ADSocial les paramètres du système blics$(q, \mathbb{G}_1, \mathbb{G}_2, g_1, g_2, e, \psi, H_1, H_2, Enc_s(.), \Delta T)$ et conserve la clé master s en secret.

0										1										2							
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7
Type								J	R	G	D	U	Reserved											Hop Count			
Detectreq ID																											
Destination IP Address																											
Destination Sequence Number																											
Originator IP Address																											
Originator Sequence Number																											
Certificate													Signature														

Tableau 4:2 Le format du message signé « Detectreq »

4.4.2 Le pseudo identité, la clé privée et le certificat délivré par le TA

Quand un nouveau noeud n_i désire communiquer avec autres noeuds, pour un SU S_x dans le domaine D_y , le TA délivre la clé privée SK_{n_i} et le certificat $\text{Cert}_{\text{TA},n_i}$ comme suit :

1) Le TA commence à calculer le pseudo identité $PID_{n_i} = Enc_s(ID_{n_i})$ avec la clé master s.
2) Le TA choisi un nombre aléatoire $\in \mathbb{Z}_q^*$, définit la clé secrète$SK_{n_i} = H_1(PID_{n_i})$ et la clé publique $PK_{n_i} = rg_1$.
3) Le TA génère la signature σ_{TA,n_i} utilisant l'algorithme de [35], où $\sigma_{TA,n_i} = S.Sign(s, PK_{n_i})$.
4) Le TA fournit en toute sécuritéPID_{n_i} , SK_{n_i} et $\text{Cert}_{\text{TA},n_i}$à n_i où $\text{Cert}_{\text{TA},n_i}(PK_{n_i}, \sigma_{TA,n_i})$. Ensuite, il stocke le mappage entre le véritable ID_{n_i} et $\text{Cert}_{\text{TA},n_i}$.

Le nœud n_i peut vérifier le certificat $\text{Cert}_{\text{TA},n_i}$ par la procédure $S.check(\sigma_{TA,n_i}, g_{1_{pub}}, PK_{n_i})$. Avec cette méthode de distribution de clés, le ECPDR garantit la confidentialité de l'identité du l'utilisateur.

4.4.3 L'update du certificat

Le schéma ECPDR proposé adopte une stratégie de restauration, où chaque nœud peut obtenir un grand nombre de certificats à partir du TA. Mais il ne peut pas utiliser ces certificats directement dans la communication ad hoc sociale. Dans le domaine D_y, que les certificats délivrés par SU S_x appartenant à ce domaine sont valables. Cependant, ECPDR adopte la technologie

de cryptographie re-signature par proxy [52], il suffit de demander à N_y la clé de re-signature depuis S_x et puis re-signe les certificats délivrés par le TA soient les mêmes que ceux délivrés par lui-même. Étant donné que le temps actuel est TW_k, le noeud n_i peut soumettre les certificats de signature $Scert$ pour demander les clés de re-signature correspondantes depuis S_x. Le processus de certificat de mise à jour est présenté dans la figure 4.3 et la liste qui suit.

1) Le S_x diffuse ses certificats $\text{Cert}_{\text{TA},S_x}$ périodiquement, par exemple chaque 3 s.

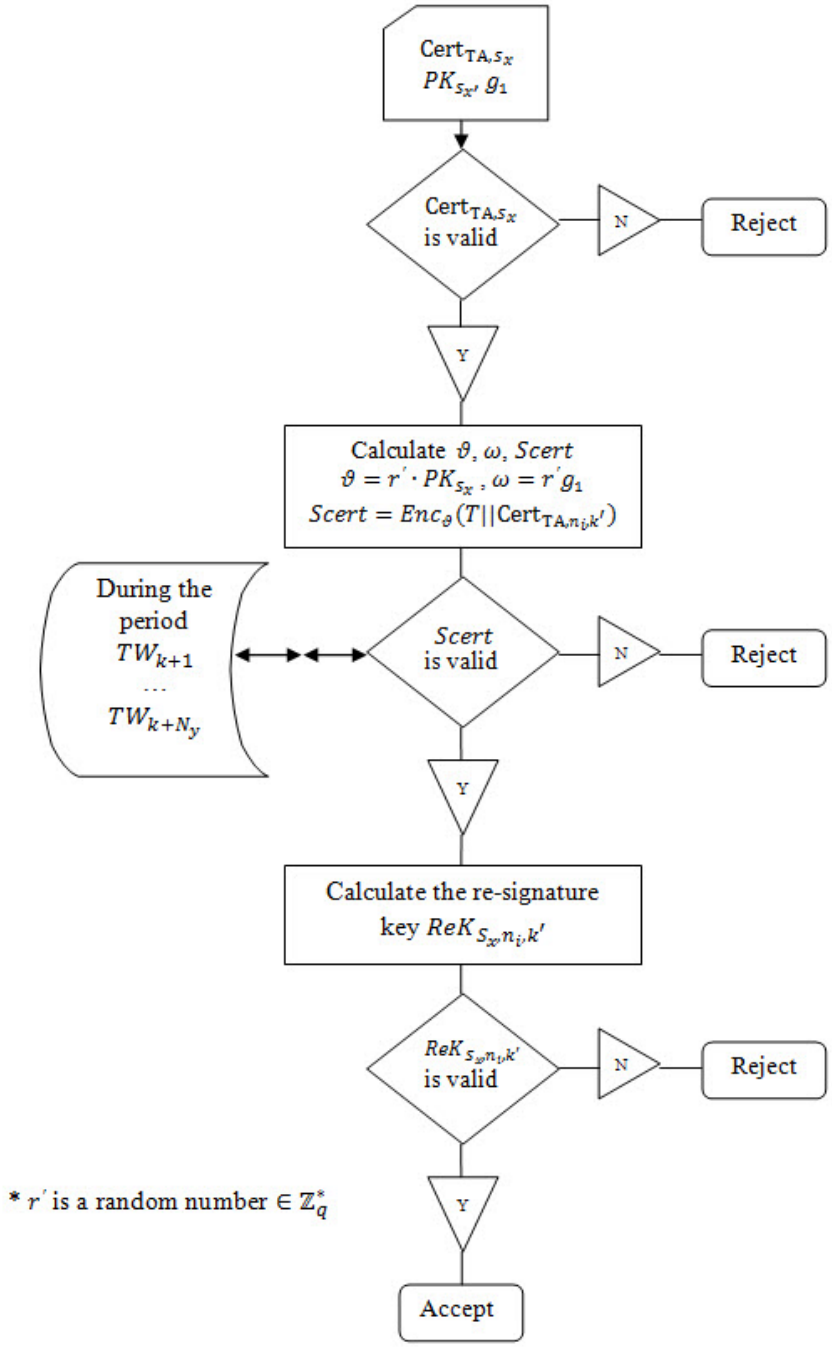


Figure 4:3 L'organigramme de la mise à jour du certificat

2) Le nœud n_i vérifie le certificat $\text{Cert}_{\text{TA},S_x}$. Si $\text{Cert}_{\text{TA},S_x}$ est valide, le nœud n_i sélectionne le nombre aléatoire $r' \in \mathbb{Z}_q^*$ et calcule la clé secrète du partage $\vartheta = r' \cdot PK_{S_x}$ et le soupçon $\omega = r' g_1$.
3) Le noeud n_i calcule les certificats de signature $Scert = Enc_{\vartheta}(T||\text{Cert}_{\text{TA},n_i,k'})$ où $k' \in [k+1, k+N_y]$ et T est l'horodatage, puis envoie le message de demande $(\omega, Scert)$ à S_x.
4) Pour décrypter le message de demande et vérifie si T est frais, l'unité sociale S_x calcule la clé secrète partagée $\vartheta' = \omega \cdot SK_{S_x}$, puis vérifie les certificats de signature $Scert$ durant la période TW_{k+1} à TW_{k+N_y} . Si la vérification est valide, S_x calcule la clé de re-signature $ReK_{S_x,n_i,k'} = \left(\frac{1}{SK_{S_x}}\right).PK_{TA,n_i,k'}$ pour chaque $\text{Cert}_{\text{TA},n_i,k'} \in Scert$.
5) L'unité sociale S_x envoie $\{ReK_{S_x,n_i,k'}\}$ vers le nœud n_i .

Le nœud n_i vérifie chaque clé de re-signature dans $\{ReK_{S_x,n_i,k'}\}$ en vérifiant que $\left(ReK_{S_x,n_i,k'}, PK_{S_x}\right) = e\left(\left(\frac{1}{SK_{S_x}}\right).PK_{TA,n_i,k'}, PK_{S_x} \cdot g_1\right)$.

4.4.4 La signature et la vérification des messages

Pour signer les trois messages $\{Detectreq, Detectrep, Notifreq\}$, le noeud n_i doit utiliser l'algorithme de signature Schnorr, i.e., $S.Sign\left(K, SK_{n_i}, Detectreq\right) \| \sigma_{n_i,Detectreq}$ où $K = H2(T \cdot \text{Cert}_{S_x,n_i})$ est la clé temporaire, $\text{Cert}_{\text{TA},n_i}$ est le certificat du n_i délivré par le TA, et SK_{n_i} est la clé secrète du n_i . Après la réception du message $Detectreq$ depuis n_i , les autres noeuds premierement vérifient si Cert_{S_x,n_i} est valide et puis acceptent le message si $S.Check\ (Detectreq, \sigma_{n_i,Detectreq}, K)$ is vrai.

Sur la base de la puissance d'émission, l'heure d'envoi du message $Detectreq$, et des conditions environnementales, le temps de détection des attaques $TDetect_{n_i}$ du n_i peut être définit comme suit:

$$TDetect_{n_i} = TNormal_{\text{Detectreq}} - \frac{R}{SD}$$

où R est la transmission maximum, SD est la vitesse de la lumière, et $TNormal_{\text{Detectreq}}$ est le temps d'envoie du message $Detectreq$. $TDetect_{n_i}$ doit être calculé avec soin pour éviter des décisions erronées. Si $TDetect_{n_i} < 0$, il y a probablement une attaque. (Voir algorithme 4.1, ligne 10)

4.4.5 La réponse demandée

L'adversaire peut détecter, modifier ou copier les messages de contrôles pour envoyer des faux messages. Cependant, pour détecter et vérifier l'attaque, chaque nœud $n_i \in$ ADSocial

initie une demande (exécute l'algorithme 4.1) pour les nœuds n_j dans sa table de routage à un saut, et attend la réponse de ses demandes pour exécuter la phase de notification.

Algorithm 4.1: Response_requested

Input : The control message $Detectreq$

Output : The link is *proved* or *suspicious*

1: Begin
2: Obtain the current timestamp;
3: Compute the temporary key $K = H2(T \cdot \mathrm{Cert}_{S_x,n_i})$;
4: Compute $C = S.Sign(K, SK_{n_i}, Detectreq) \parallel \sigma_{n_i,Detectreq}$;
5: Obtain the short time $SIMS$ (Short Inter-Message Space);
6: Send_Request (C);
7: When node receive the encrypted control message$Detectrep$,
recover $Detectrep$ from D ;
8: Compute $\gamma = S.Check\ (Detectrep, \sigma_{n_j,Detectrep}, K)$;
9: if $\gamma = true$ then begin
10: Compute $TDetect_{n_i} = TNormal_{\mathrm{Detectreq}} - \frac{R}{SD}$;
11: if $TDetect_{n_i} < 0$ then begin
12: return *suspicious*;
13: end;
14: else return *proved*;
15: end;
16: else Begin
17: return *suspicious*;
18: end;
19: End;

Algorithme 4:1 Demande pour détection

Algorithm 4.2: Notify

Input : The control message $Notifyreq$, the adversary node n_x

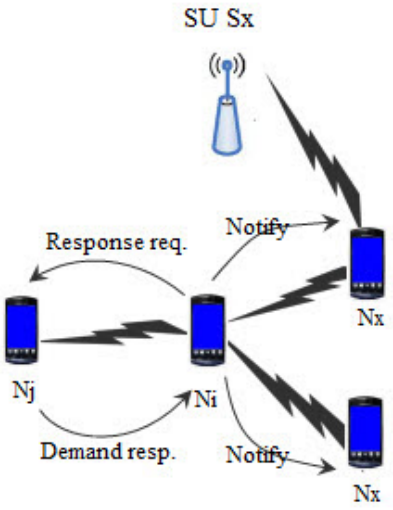
Output : R ready for transmission

1: Begin
2: Compute $R = S.Sign(K, SK_{n_i}, Notifyreq) \parallel \sigma_{n_i,Detectreq}$;
3: if $n_x \in (1 - hop\ of\ n_i)$ then
4: begin
5: remove n_x in the routing table of n_i at 1-hop;
6: return;
7: end;
8: else return;
9: End;

Algorithme 4:2 Notification des attaques

Cette phase d'une réponse demandée est résumée dans les étapes suivantes:

1) Le nœud n_i premièrement signe le message avec la clé privée SK_{n_i}et la clé raire $K = H2(T \cdot \text{Cert}_{S_x,n_i})$. Pour éviter les collisions, il attend l'épuisement du temps $SIMS$. Puis, il envoie à ses voisins à un saut dans sa table de routage. (Voir algorithme 4.1, ligne 1 à 6)
2) Après avoir reçu une demande de réponse envoyée par n_j , le nœud $n_i$récupère depuis R le message de contrôle encrypté $Detectrep$. Puis, il vérifie sa signature. Si elle est valide et $TDetect_{n_i} < 0$, il considère que le lien avec le nœud n_j est prouvé. Sinon, il retourne suspect et commence la phase de notification. (Voir algorithme 4.1, ligne 7 à 19)



Response req.: Send a response request
Demand resp.: Send a demand response
Notify: Send a notification message to its neighbors

Figure 4:4 Réponse demandée et réponse à la demande

3) Si le nœud n_i détermine que le lien avec le nœud n_j est suspect, le n_i commence la phase de notification (Voir l'algorithme 4.2) qui est résumée dans les étapes suivantes:
   3.1) Le noeud n_i prépare un message de notification $Notifyreq$. Puis, il supprime le noeud adversaire n_j dans sa table de routage à un saut.
   3.2) Le nœud n_i envoie un message de notification à ses voisins. Lorsque le nœud voisin reçoit la demande de notification, il supprime le nœud adversaire dans sa table de routage. Et à la fin, le nœud voisin diffuse le message de notification à tous les nœuds dans sa table de routage. (Voir figure 4.4)

Remarques:

- Dans ECPDR, un nœud prend un grand nombre de certificats, mais chaque certificat est seulement valide dans les différentes parties du temps. Donc, il peut limiter l'utilisation abusive d'informations d'identification.
- Avec l'adaptation de la technologie cryptographique [52], le nœud ne peut pas générer une signature correcte pour les certificats faux.
- La phase de notification (Algorithme 4.2) est exécutée après la vérification du message de réponse $Detectrep$.

4.4.6 La réponse à la demande

Quand le nœud n_j reçoit la demande de détection, il exécute Demand_Reponse () (Algorithme 4.3).

Algorithm 4.3: Demand_Reponse

Input : C the encrypted control message$Detectreq$

Output : D the encrypted control message$Detectrep$

1: Begin
2: Obtain the current timestamp ;
3: Compute the temporary key $K = H2(T \cdot \text{Cert}_{S_x,n_j})$;
4: Compute $D = S.Sign\left(K, SK_{n_j}, Detectrep\right) \parallel \sigma_{n_j,Detectreq}$;
5: When node receive the encrypted control message $Detectreq$,
recover $Detectreq$ from C ;
6: Compute $\gamma = S.Check\ (Detectreq, \sigma_{n_i,Detectreq}, K)$;
7: if $\gamma = true$ then Send_reponse (D, n_i) ;
8: Else Response_requested () ;
9: End;

Algorithme 4:3 La réponse à la demande de détection d'attaque

Cette phase de la réponse à la demande est résumée dans les étapes suivantes:

1) Quand le nœud n_j recois le message de controle encrypté $Detectreq$, il récupère C et vérifie sa signature $S.Check\ (Detectrep, \sigma_{n_i,Detectreq}, K)$.
2) Si la signature est valide, le nœud n_j signe la réponse $S.Sign\left(K, SK_{n_j}, Detectrep\right) \parallel \sigma_{n_j,Detectreq}$ et renvoie à n_i . Sinon, le nœud n_j envoie une réponse demandée à n_i.

4.5 Analyse de la sécurité

Dans cette section, nous décrivons d'abord les oracles, et ensuite nous prouvons que le schéma ECPDR proposé préserve la confidentialité axée sur le contenu et la confidentialité conditionnelle du certificat. Enfin, nous discutons de la robustesse du schéma ECPDR contre les attaques élémentaires et les attaques composées.

4.5.1 Les oracles

La sécurité sémantique du $S.Sign(PK, SK, m)$ dans ECPDR est définie à l'aide d'un jeu entre un challenger et un adversaire. Soit un adversaire polynôme $\mathcal{A}$ essayant de gagner l'expérience contre le challenger $\mathcal{C}$. Dans ECPDR, l'adversaire peut utiliser les quatre oracles suivants:

- $\boldsymbol{\mathcal{O}.Sign(m, PK, VAB)}$ permet à l'adversaire $\mathcal{A}$ d'obtenir une signature originale sur un message m de son choix avec la clé publique du signataire PK et la variable VAB du l'adversaire.
- $\boldsymbol{\mathcal{O}.Modify(m, \sigma, ALT)}$ permet à l'adversaire $\mathcal{A}$ de modifier une paire d'un message de signature(m, σ) avec les changements ALT qu'il souhaite. L'oracle retourne une signature modifiée valable si des modifications sont admissibles et $\perp$ en cas d'erreur.
- $\boldsymbol{\mathcal{O}.Prove(m, \sigma, DB)}$ permet à l'adversaire $\mathcal{A}$ d'obtenir la preuve de l'origine d'une paire message-signature (m, σ) selon une base de données $DB = \{ (m_k, \sigma_k)\}_{k\in[1,q]}$.
- $\boldsymbol{\mathcal{O}.Sign/Modify_b(m, \mathbf{VAB}, MOD)}$ permet à l'adversaire $\mathcal{A}$ pour prendre en entrée un message m, VAB et MOD. L'oracle retourne $\perp$ si MOD ne correspond pas à VAB. Si $b = 0$, il renvoie une signature originale du signataire m' (m' est le message correspondant au message m modifié parMOD). Et si $b = 0$, il effectue une signature originale du signataire du message m par VAB et il le modifie par MOD.

4.5.2 La confidentialité du contenu orienté

Dans notre proposition ECPDR, la confidentialité du contenu orienté peut être garantit par la sécurité du $S.Sign(PK, SK, m)$. Si le cryptogramme $S.Sign(PK, SK, m)$ est prouvablement sécurisé, il préserve la confidentialité du contenu orienté dans ECPDR. Par conséquent, nous prouvons la propriété de la sécurité sémantique du $S.Sign(PK, SK, m)$ en utilisant les techniques de sécurité prouvable prouvé par Brzuska et *al.* [51].

Théorème 4.1: Soit $(q, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e, g_1, g_2)$ *un environnement bilinéaire d'ordre premier,* λ *un paramètre de sécurité et* $\mathcal{A}$ *un adversaire polynôme pour acquérir de l'expérience contre le challenger* $\mathcal{C}$. *Cet adversaire peut accéder aux quatre oracles, ci-après:*

- $\mathcal{O}.Sign(m, PK, VAB)$,
- $\mathcal{O}.Modify(m, \sigma, ALT)$,
- $\mathcal{O}.Prove(m, \sigma, DB)$
- $\mathcal{O}.Sign/Modify_b(m, VAB, MOD)$.

Le schéma ECPDR est sécurisé, i.e., il est immuable, transparent et responsable.

Preuve: Nous allons étape par étape à travers les propriétés. La plupart du temps, nous décrivons chaque propriété pour ECPDR.

- **Immutabilité**

Définition 4.3 (ECPDR Immutabilité): *Soit* λ *un paramètre de sécurité,* $S.Init(1^\lambda)$*un algorithme d'initialisation et* $S.GenK$ *un algorithme de génération de clé de signataire* (PK, SK) . *Soit* $\mathcal{A}$ *un adversaire peut accéder à la signature oracle* $\mathcal{O}.Sign(m, PK, VAB)$ *et l'oracle de prouve* $\mathcal{O}.Prove(m, \sigma, DB)$. *Nous considérons l'expérience aléatoire suivante*:

Experiment $\text{EXP}_{\text{Imm},\mathcal{A}}^{\text{ECPDR}}(\lambda)$
$S.param \leftarrow S.Init(1^\lambda)$
$(PK, SK) \leftarrow S.GenK(S.param)$
$(m^*, \sigma^*, PK^*) \leftarrow \mathcal{A}^{Sign,Prove}(S.param, PK)$
if $S.check(m^*, \sigma^*, PK^*)$ = true then $b \leftarrow 1$ else $b \leftarrow 0$
return b

Nous définissons le succès de l'adversaire du polynôme $\mathcal{A}$ dans l'expérience $\text{EXP}_{\text{Imm},\mathcal{A}}^{\text{ECPDR}}(\lambda)$ via:

$$\text{Succ}_{\text{Imm},\mathcal{A}}^{\text{ECPDR}}(\lambda) = \Pr\left[1 \leftarrow \text{EXP}_{\text{Imm},\mathcal{A}}^{\text{ECPDR}}(\lambda)\right]$$

Le ECPDR est dit (λ, t, ϵ) immuable sécurisé, si aucun adversaire $\mathcal{A}$ s'exécute dans le temps t a le succès $\text{Succ}_{\text{Imm},\mathcal{A}}^{\text{ECPDR}}(\lambda) < \epsilon$, avec ϵ négligeable.

- **Transparence (Confidentialité)**

Définition 4.4 (ECPDR Transparence): *Soit* λ *un paramètre de sécurité,* $S.Init(1^\lambda)$ *un algorithme d'initialisation et* $S.GenK$ *un algorithme de génération de clé de signataire* (PK, SK) *et* b *un bit choisit au hasard. Soit* $\mathcal{A}$ *un adversaire avec l'accès aux quatre oracles:*$\mathcal{O}.Sign(m, PK, VAB)$,$\mathcal{O}.Modify(m, \sigma, ALT)$,$\mathcal{O}.Prove(m, \sigma, DB)$ *and* $\mathcal{O}.Signe/Modify_b(m, VAB, MOD)$. *Si* $b = 0$, *l'oracle de défi renvoie une signature ; ou une signature modifiée si* $b = 1$. *Nous considérons l'expérience aléatoire suivante:*

Experiment $\mathrm{EXP}^{\mathrm{ECPDR}}_{\mathrm{Transp},\mathcal{A}}(\lambda)$
$S.param \leftarrow S.Init(1^{\lambda})$
$(PK.SK) \leftarrow S.GenK(S.param)$
$b \leftarrow \{0,1\}$
$b^* \leftarrow \mathcal{A}^{Signe,Modify,Prove,Signe/Modify_b}(S.param, PK)$
if $b^* = b$ then $a \leftarrow 1$ else $a \leftarrow 0$
return a

Nous définissons l'avantage du polynôme de l'adversaire $\mathcal{A}$ dans l'expérience $\mathrm{EXP}^{\mathrm{ECPDR}}_{\mathrm{Transp},\mathcal{A}}(\lambda)$ via:

$$\mathrm{Adv}^{\mathrm{ECPDR}}_{\mathrm{Transp},\mathcal{A}}(\lambda) = |\Pr[1 \leftarrow \mathrm{EXP}^{\mathrm{ECPDR}}_{\mathrm{Transp},\mathcal{A}}(\lambda)] - \frac{1}{2}$$

Le ECPDR est dit (λ, t, ϵ) transparent sécurisé, si aucun adversaire $\mathcal{A}$ s'exécute dans le temps t a l'avantage $\mathrm{Adv}^{\mathrm{ECPDR}}_{\mathrm{Transp},\mathcal{A}}(\lambda) < \epsilon$, avec ϵ négligeable.

- **Responsabilité**

Définition 4.5 (ECPDR Responsable): *Soit λ un paramètre de sécurité, $S.Init(1^{\lambda})$ un algorithme d'initialisation et $S.GenK$ un algorithme de génération de clé de signataire (PK, SK). Soit $\mathcal{A}$ un adversaire avec accès à l'oracle de changement $O.Modify(m, \Sigma, ALT)$ et retourne un quadruplet $(SK^*, \pi^*_{or/ALT}, m^*, \sigma^*)$. Nous considérons l'expérience aléatoire suivante:*

Experiment $\mathrm{EXP}^{\mathrm{ECPDR}}_{\mathrm{Acc},\mathcal{A}}(\lambda)$
$S.param \leftarrow S.Init(1^{\lambda})$
$(PK.SK) \leftarrow S.GenK(S.param)$
$(PK^*, \pi^*_{or/ALT}, m^*, \Sigma^*) \leftarrow \mathcal{A}^{Modify}(S.param, PK)$
Let $(m'_k, \sigma'_k)_{k\in[1,n]}$ the response of the oracle modified
if $S.check(m^*, \sigma^*, PK^*) =$ tru
and $(PK^*, m^*) \neq (PK^*{}_k, m^*{}_k)$ where $k \in [1, n]$
then $a \leftarrow 1$ else $a \leftarrow 0$
return a

Nous définissons le succès de adversaire du polynôme $\mathcal{A}$ dans l'expérience $\mathrm{EXP}^{\mathrm{ECPDR}}_{\mathrm{Acc},\mathcal{A}}(\lambda)$ via:

$$\mathrm{Succ}^{\mathrm{ECPDR}}_{\mathrm{Acc},\mathcal{A}}(\lambda) = Pr[1 \leftarrow EXP^{ECPDR}_{Acc,\mathcal{A}}(\lambda)]$$

Le ECPDR est dit (λ, t, ϵ) responsable sécurisé, si aucun adversaire $\mathcal{A}$ s'exécute dans le temps t a le succès $\mathrm{Succ}^{\mathrm{ECPDR}}_{\mathrm{Acc},\mathcal{A}}(\lambda) < \epsilon$, avec ϵ négligeable.

Ceci termine la preuve. ■

4.5.3 La confidentialité conditionnelle du certificat

Dans le schéma ECPDR, la confidentialité conditionnelle du certificat est préservée par la technologie re-signature où SU S_x agit comme l'émetteur du certificat pour le nœud n_i . En outre, les certificats délivrés par un SU S_x appartenant à ce domaine sont valables. Avec l'utilisation de la technologie de cryptographie re-signature proxy [52], SU S_x n'a aucune idée sur la confidentialité du nœud n_i.

4.5.4 La robustesse

Dans cette sous section, nous discutons de la robustesse du ECPDR. Plus précisément, nous montrons comment l'ECPDR empêche les attaques connues contre les protocoles de routage, comme les attaques élémentaires et les attaques composées.

La résistance contre les attaques élémentaires: Un adversaire peut faire les quatre actions de base suivantes sur les messages:

- Suppression d'un message, l'adversaire ne participe pas au routage, c'est comme s'il ne fait pas partie du réseau social.
- Modification d'un message, l'adversaire peut jouer sur le numéro de séquence de la destination et/ou le nombre de sauts dans les messages de commande en augmentant et en diminuant.
- Fabrication d'un message, l'adversaire peut faire une réponse de route, même si aucun chemin valide vers la destination.
- Réduire le temps, l'adversaire peut réduire le temps de traitement de messages de contrôle et le retransmettre plus vite afin qu'il atteigne la destination plus rapidement. Cela permettra d'assurer pour l'adversaire une place sur le chemin.

Ces attaques ne touchent pas notre schéma ECPDR proposé parce que le nœud vérifié la validité du message reçu avec $S.Check\ (Detectrep, \sigma_{n_j,Detectrep}, K)$. Si le message n'est pas valide, il sera directement éliminé.

La résistance contre les attaques composées: Un adversaire peut combiner des attaques élémentaires pour effectuer des attaques composées potentielles pour atteindre des objectifs plus avancés. Comme l'insertion dans un chemin déjà établi ou n'est pas encore établi, aussi la création d'une boucle de routage ou d'un tunnel. Toutefois, le ECPDR peut détecter et contrôler les attaques composées, puis informer les autres nœuds, par l'utilisation de messages de contrôle ($\boldsymbol{Detectreq}$,$\boldsymbol{Detectrep}$,$\boldsymbol{Notifyreq}$) et l'authentification de ces messages en fonction du pseudo identité, la clé privée et le certificat délivré par le TA.

4.6 Evaluation des performances

Pour évaluer notre schéma ECPDR, nous avons effectué des simulations dans deux scénarios différents. Dans cette section, nous présentons d'abord l'environnement de simulation utilisé et ensuite les résultats de simulations pour chaque scénario.

A) Scénario 1

Dans le premier scénario, nous évaluons l'efficacité du schéma ECPDR contre l'attaque du trou noir sur le routage réactif AODV utilisant le simulateur NS-2 [58] configuré à la norme IEEE 802.11 (11 Mbps et 2 Mbps où ils sont utilisés pour transmettre le trafic de diffusion unicast et broadcast, respectivement). Nous avons généré un certain nombre de topologies aléatoires avec N nœuds sur un terrain carré, où N est compris entre 10 et 100. La taille du champ carré varie de 600x600m à 1500x1500m en fonction de la taille du réseau ADSocial. La portée de transmission maximale de chaque noeud est fixée à 250 m et le modèle de trafic est CBR. La paire de nœud adversaire est choisie au hasard dans ADSocial formé.

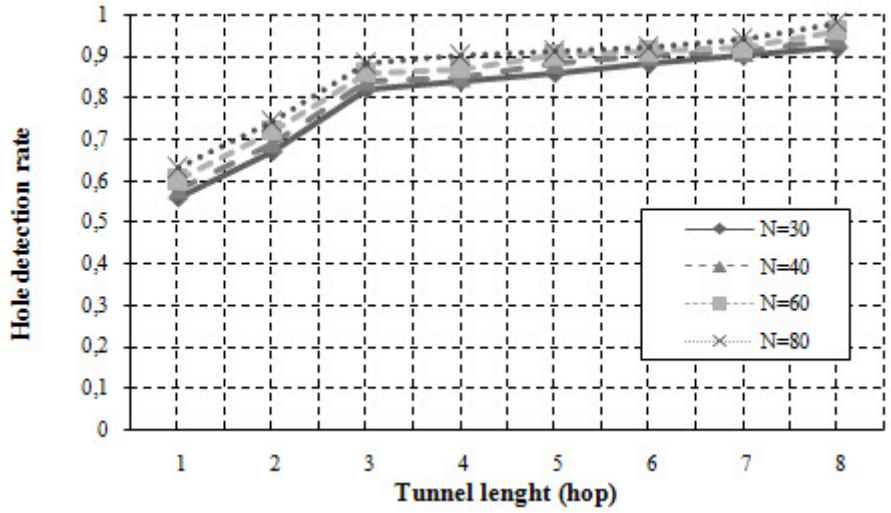


Figure 4:5 . Taux de détection de liaison de trou noir pour les différentes tailles de réseau

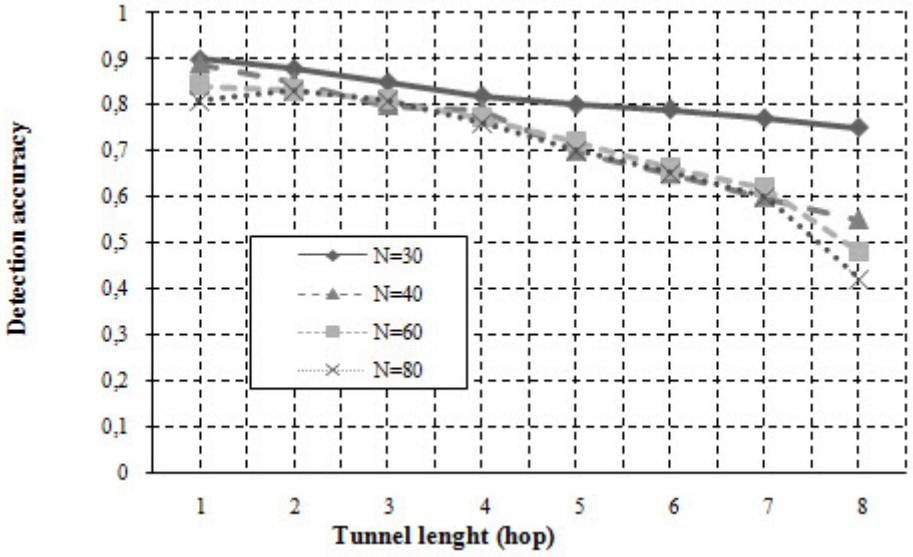


Figure 4:6 Précision de détection de la liaison d'un trou noir pour les différentes tailles de réseau

La figure 4.5 montre le taux de détection du trou noir selon la longueur du tunnel qui est le nombre de sauts entre les nœuds de l'adversaire. Comme on le voit sur la figure 4.4, les trous sont détectés plus dans la configuration où l'attaque est lancée sur un nombre de plus de saut. C'est un fait évident, que par le lien du trou, les paquets sont encapsulés.

La figure 4.6 montre les résultats de précision de la détection d'un trou noir. Nous pouvons observer que la précision de détection dépend de la corrélation entre le nombre de nœuds et la longueur du tunnel. Dans un réseau de 30 noeuds, la précision de détection diminue rarement avec l'augmentation de la longueur du tunnel. Et dans les grands réseaux, où (N = 40, N = 60), la précision de détection diminue considérablement avec l'augmentation de la longueur du tunnel. Mais en réseau (N = 80) où le réseau devient plus grand, le nœud adversaire est plus susceptible d'avoir de nombreux voisins.

A) Scénario 2

Une métrique de performance importante dans les systèmes ADSocial est combien de temps il faut à un nœud pour envoyer les messages, i.e., $Detectreq$ pour atteindre ses noeuds voisins. Dans le second scénario, nous nous concentrons sur le délai de transmission du schéma ECPDR au niveau du noeud. Le coût de calcul du schéma ECPDR notamment, la détection, la vérification et la notification de l'attaque, qui concernent principalement les opérations cryptographiques suivantes: authentification, genk, encrypt, decrypt, multiplication dans Z_q^* et les opérations de hachage. Nous implémentons le type de courbe Tate pairing avec le degré d'intégration k = 2 Cocks-Pinch (CP-80). CP-80 est sur $\mathbb{F}_p$ avec 512 bit d'ordre premier p . Après, Nous implémentons le type de courbe Ate paring avec un degré d'intégration k = 6 Miyaji-Nakabayashi-Takano (MNT-80). MNT-80 est sur $\mathbb{F}_{p^3}$ avec 160 bit d'ordre premier p . Les repères pour l'appariement sélectionné exécuté sur un poste de travail modèrne, où le processeur est 64-bit Intel i5 520M, 2.4GHz. Les résultats des mesures sont donnés dans le tableau 4.3. Sur la base de ces chiffres et le chiffrement des prédicats Inner-Produit adopté (IPE) [59], on peut estimer le coût de calcul en ECPDR, et les résultats pertinents sont donnés dans le tableau 4.4 [60].

Courbe	CP-80		MNT-80	
G_2 type	$\mathbb{F}_p$		$\mathbb{F}_{p^3}$	
K	2		6	
Modulus (bits)	512		160	
Paring	Tate		Ate	
with/without precomp.	w	w/o	w	w/o
GenK	0.207ms	1.020ms	0.663ms	2.239ms
Encrypt	0.366ms	1.695ms	0.194ms	0.767ms
Decrypt 2	1.213ms	2.360ms	1.392ms	3.788ms
Decrypt *	0.834ms	1.991ms	1.043ms	3.383ms

2: 2 pairings / *: multi-pairing

Tableau 4:3 Le coût des opérations nécessaires

Courbe	CP-80		MNT-80	
with/without precomp.	w	w/o	w	w/o
Detectreq authentication	0.207ms	1.020ms	0.663ms	2.239ms
Encrypt (t_e)	0.366ms	1.695ms	0.194ms	0.767ms
Decrypt (t_d)	1.213ms	2.360ms	1.392ms	3.788ms

Tableau 4:4 Le coût des opérations nécessaires dans ECPDR

Ensuite, nous avons

$$\mu = \begin{cases} 169.3/s, \text{w/o pairing precomputation;} \\ 377.3/s, \text{with pairing precomputation.} \end{cases}$$

Nous évaluons le délai de transmission dans ECPDR utilisant le processus M/D/1 [61], où nous considérons l'arrivée moyenne $Detectreq$ au niveau du noeud est un processus de Poisson avec le taux d'arrivée λ , le taux de départ μ , et faire avancer le processus de l'état i à $i + 1$. Le temps de retard moyen de $Detectreq$ avant d'être mis dans le tampon du nœud est t_v ,

$$t_v = \frac{1}{\mu} \cdot \frac{2-\rho}{2-2\rho} \quad \text{, où } \rho = \frac{\lambda}{\mu}$$

Par la diffusion du message $Detectreq$, les deux opérations « crypter et décrypter » peuvent être réduites. Ce mécanisme entraînera le retard de transmission. L'attaque du trou noir va également entraîner le retard de transmission. Soit la probabilité p d'un message $Detectreq$ invalide arrivant au nœud en raison de l'attaque du trou noir. Nous étudions le temps moyen d'attente dans le tampon du nœud comme suit. Nous considérons d'abord combien le temps qu'il prend le i-ème $Detectreq$ dans le nœud pour attendre l'arrivée de la prochaine i + 1 i-ème $Detectreq$. Etant donné que la probabilité d'un message $Detectreq$ invalide est p, lorsqu'un $Detectreq$ valable est mise en mémoire tampon du nœud, le nombre d'authentifications $Detectreq$ au niveau du noeud est une variable aléatoire géométriquement distribuée:

$$P(\text{nombre d'authentification} = k) = p^{k-1}(1-p)$$

où $= 1,2,\cdots$. Nous définissons $t_{i(i+1)}$ comme le temps d'attente moyen,

$$t_{i(i+1)} = \sum_{k=1}^{\infty} \frac{k}{\mu} \cdot p^{k-1}(1-p) = \frac{1}{\mu(1-p)}$$

où $i = 1,2,\cdots,n-1$. Pour le cas $i = n$, $t_{ii} = t_{nn} = 0$. Donc, avant l'envoie du message $Detectrep$, le temps d'attente pour chaque $Detectreq$ dans le buffer du nœud est

$$T_i = \begin{cases} \dfrac{n-i}{\mu(1-p)}, & i = 1,2,\cdots,n-1; \\ 0, & i = n. \end{cases}$$

(4.12)

Et le temps d'attente moyen est

$$t_w = \sum_{i=1}^{n} \frac{1}{n} T_i = \frac{1}{n} \cdot \frac{1}{\mu(1-p)} \cdot \big(1 + 2 + \cdots + (n-1)\big)$$

$$= \frac{1}{n} \cdot \frac{1}{\mu(1-p)} \cdot \frac{n(n-1)}{2}$$

$$= \frac{1}{n} \cdot \frac{n(n-1)}{2\mu(1-p)}$$

$$= \frac{n-1}{2\mu(1-p)}$$

Et le retard de transmission t_r du schéma ECPDR au nœud dans le statut du récepteur est :

$$t_r = t_v + t_w + t_d = \frac{2-\rho}{2\mu(1-\rho)} + \frac{n-1}{2\mu(1-p)} + t_d$$

$$\rho = \frac{\lambda}{\mu} < 1$$

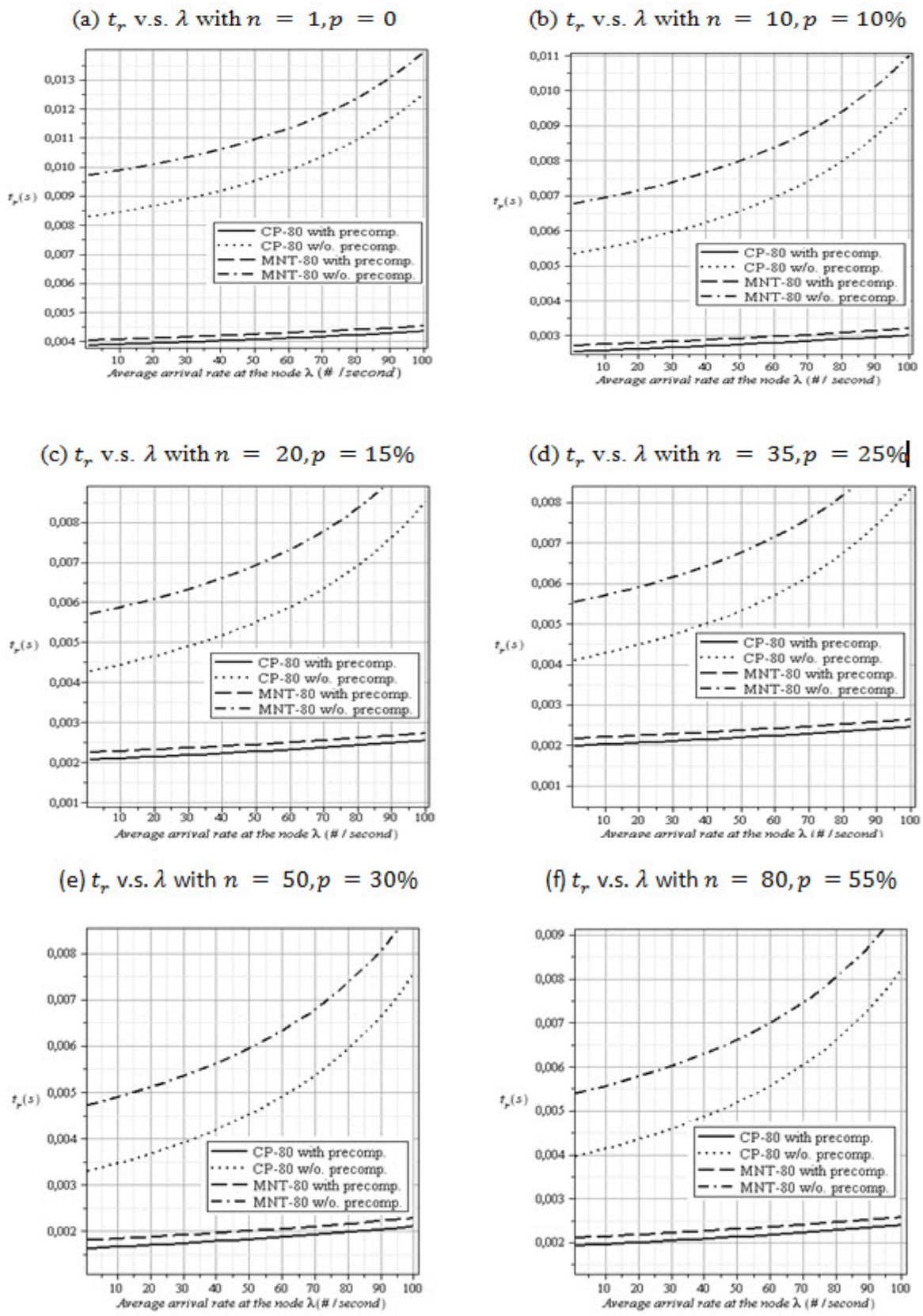


Figure 4:7 Le délai moyen de transmission t_r variant avec le taux moyen d'arrivé λ, où $1 \leq \lambda \leq 100$

Nous fixons les paramètres n et p, Fig. 4.7 (a,b,c,d,e,f) représente le délai moyen de transmission t_r variant avec le taux moyen d'arrivé λ, où $1 \leq \lambda \leq 100$. Comme on le voit dans la figure. 4.7, le retard de transmission t_r augmente avec l'augmentation de λ dans l'ensemble. Aussi, le retard de transmission t_r avec la courbe Cocks-Pinch (CP-80) est inférieur à la courbe Miyaji-Nakabayashi-Takano (MNT-80). Ces résultats indiquent que CP-80 le retard de transmission peut être réduit lorsque la performance du dispositif mobile (noeud) est améliorée. En outre, à partir de la figure. 4.7, nous pouvons également observer à peu près la relation entre t_r et p, n, i.e., avec l'augmentation de p et n, le retard de transmission t_r permettra également d'augmenter.

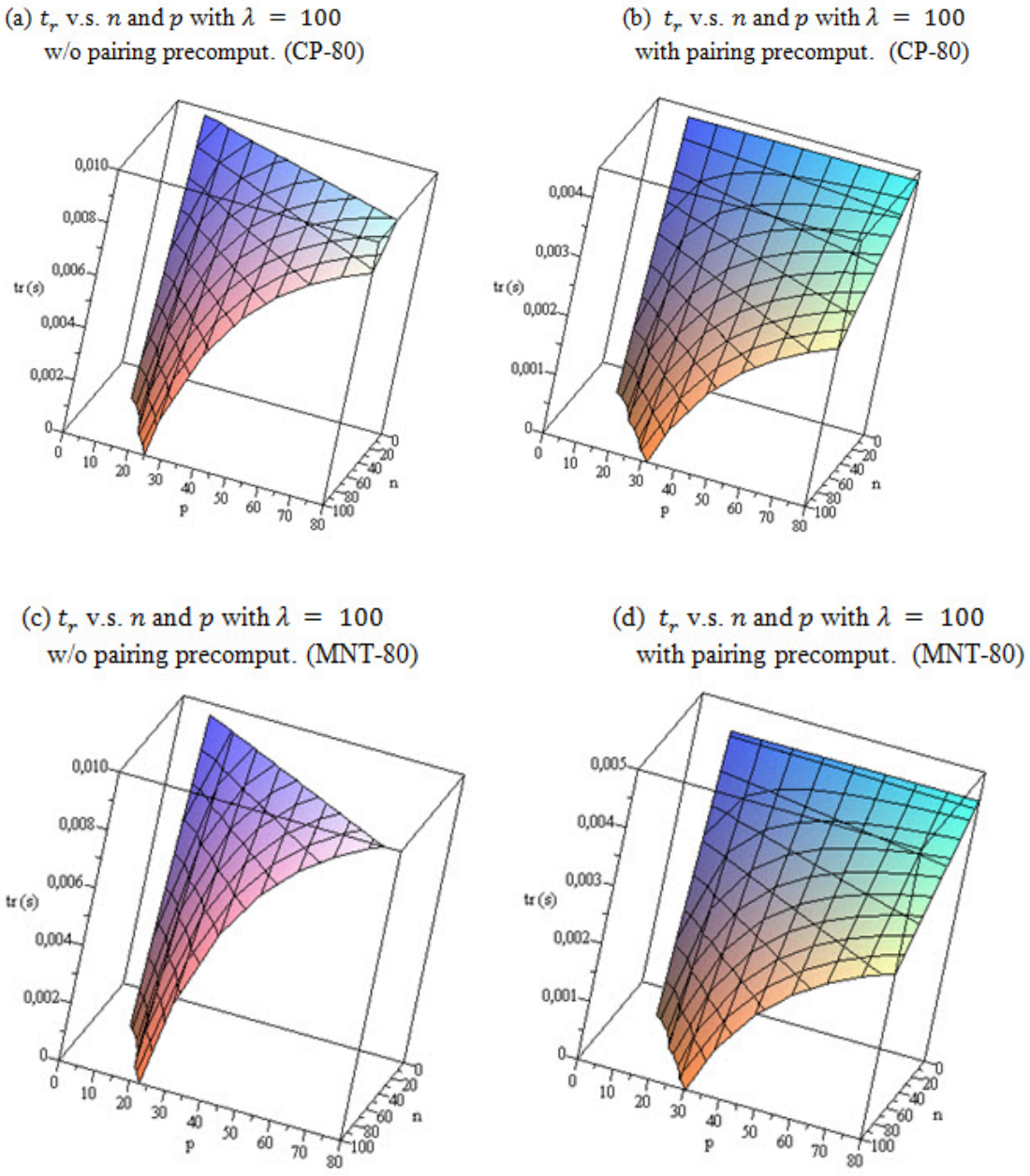


Figure 4:8 Le délai moyen de transmission t_r variant avec p et n, où $1\% \leq p \leq 80\%$ et $1 \leq n \leq 100$

Pour discuter davantage sur la relation subtile, nous traçons t_r variant avec p et n dans Fig. 4.8, où λ est fixé à 100. On peut voir que pour les petits p, le retard de transmission augmente très lentement avec n. Cependant, pour les grands p, le retard de transmission augmente rapidement. Ceci indique que le paramètre , en raison de l'attaque du trou noir, est l'élément déterminant pour le retard de transmission. Par conséquent, pour les petits p, le schéma proposé peut obtenir une bonne performance en termes de délai de transmission. En outre, la différence entre Fig. 4.8(a), Fig. 4.8 (b), Fig. 4.8 (c) et Fig. 4.8 (d) démontre que le précalcul de CP-80 peut réduire le délai de transmission. Enfin, la mise en œuvre des méthodes cryptographiques utilisées par ECPDR sur un autre type de processeur, telles que ARM-série M et Intel Atom, est en cours.

4.7 Comparaison avec autres protocoles de sécurisation

Dans cette section, nous comparons notre schéma ECPDR proposé avec les protocoles examinés dans le chapitre 3, i.e, SPRING, SPF, PCS, FLIP et Pi.

On peut voir dans le tableau 4.5 que tous les schémas réalisent la préservation de la confidentialité. Le schéma SPRING [62] donne l'optimisation des véhicules DTN, peut résister aux attaques liées à la confidentialité sur les nœuds véhicules DTN, et atteint la préservation conditionnelle de la confidentialité. Le schéma SPF [64] réalise la préservation la confidentialité conditionnelle et atteint la protection de la confidentialité de l'emplacement. Le schéma PCS [65] atteint la protection de la confidentialité de l'emplacement et la confidentialité de l'identité. Le schéma FLIP [66] atteint les mêmes objectives de sécurité du schéma [65] et il peut aussi atteint la confidentialité d'intérêt. Le schéma Pi [67] réalise seulement la stimulation des nœuds DTN égoïstes. Notre schéma ECPDR [J2] atteint l'immutabilité, la responsabilité, la détection précoce des attaques de routage, la transparence, l'authentification et l'intégrité du message, et la disponibilité des ressources.

Les schémas proposés / Les objectifs de sécurité et de confidentialité	SPRING [62]	SPF [64]	PCS [65]	FLIP [66]	Pi [67]	ECPDR [J2]
La préservation de la confidentialité	X	X	X	X	X	X
Optimisation des véhicules DTN	X					
Résister aux attaques liées à la confidentialité sur les nœuds véhicules DTN	X					
La préservation de la confidentialité conditionnelle	X	X				X
La protection de la confidentialité de l'emplacement		X	X	X		X
La confidentialité de l'identité			X	X		X
La confidentialité d'intérêt				X		
La stimulation des nœuds DTN égoïstes					X	
L'immutabilité						X
La responsabilité						X
La détection précoce des attaques de routage						X
La transparence						X
L'authentification et l'intégrité du message						X
La disponibilité des ressources						X

Tableau 4:5 La comparaison de notre schéma ECPDR avec les autres schémas

4.8 Conclusions

Dans ce chapitre, nous avons proposé le schéma ECPDR pour sécuriser les communications ad hoc sociaux. ECPDR peut non seulement satisfaire aux exigences de sécurité et de confidentialité des réseaux ad hoc, mais peut aussi détecter, prévenir et informer les attaques élémentaires et les attaques composées. En outre, grâce à l'évaluation vaste des performances, le ECPDR a été démontré comme un schéma désinfecté et efficace pour le protocole de routage AODV contre l'attaque du trou noir et efficace en terme de délai de transmission.

Chapitre 5 SDPP : Un schéma de détection intelligent avec la forte préservation de la confidentialité pour la sécurisation des réseaux sociaux P2P

Précédemment, nous avons présenté le schéma ECPDR pour la sécurisation et la confidentialité des réseaux sociaux ad hoc. Dans ce chapitre, nous introduisons le schéma SDPP [J3] où nous nous concentrons, sur la façon de détecter et de prévenir une attaque avec la forte protection de la vie privée pour la sécurisation et la confidentialité des réseaux sociaux P2P.

5.1 Introduction

Les réseaux sociaux se sont adaptés au monde de l'entreprise mieux que quiconque aurait pu l'imaginer. Le réseautage social a commencé une fois dans l'espace en ligne tels que Facebook, Myspace, Youtube, Flickr avec des centaines de millions d'utilisateurs [20]. Bien que le réseautage social est un mot à la mode populaire dans l'Internet, les réseaux sociaux sont partout autour de nous au lieux de travail ainsi qu'au sein des familles et des groupes sociaux, où les utilisateurs peuvent changer les jeux, rumeurs, et trouver des gens qui ont des intérêts similaires en utilisant leurs appareils mobiles à courte portée avec des interfaces sans fil formant un réseau ad hoc social.

Le réseau P2P (Peer-to-Peer) contribue à une grande quantité de trafic Internet car de nombreux internautes utilisent massivement ou dépendent des applications de partage de fichiers comme BitTorrent, PPStream, et eDonkey. Un grand nombre d'applications P2P sont actuellement utilisées, sur Internet, à la fois pour la vidéo sur demande et les services de streaming en temps réel comme l'IPTV tels que UUSee, SopCas, TVants et Joost [5]. *Et si un Smartphone est l'outil de partage d'informations avec le réseau de P2P?* En raison de la mobilité de l'utilisateur, les utilisateurs peuvent communiquer souvent avec d'autres sur un réseau social ad hoc ou avec le nœud d'échange en réseau P2P. Si deux utilisateurs ont des intérêts similaires, il est possible pour eux de partager leurs différents types de ressources (par exemple, audio, vidéo, jeu, musique, e-books) qui sont facilement accessibles via le modèle de P2P, pour éliminer la solitude. Nous appelons ce genre de contact, le réseau social P2P mobile (MP2PSN).

Au cours des dernières années, plusieurs techniques de la vie privée ont été proposées [45, 46], pour les réseaux de capteurs [47], les systèmes de santé en ligne [48], les communications des véhicules [49], et les communications de réseaux électriques intelligents [50]. Toutefois, en raison des caractéristiques uniques de MP2PSN; ces schémas ne sont pas applicables aux attaques de routage dans MP2PSN. Une des raisons est que ces schémas ne considèrent pas la vie privée de l'utilisateur dans MP2PSN. Autre raison, est que ces schémas n'ont pas non plus tenu compte des caractéristiques d'un réseau ad hoc, i.e., la topologie dynamique, l'exploitation de l'énergie , la bande passante limitée, et la sécurité physique limitée. Ce changement a naturellement une influence sur la morphologie du réseau et peut changer le comportement du canal de communication. Par conséquent, il est essentiel mais difficile de concevoir un schéma efficace préservant la confidentialité pour MP2PSN.

Dans ce chapitre, pour faire face à ces défis cités en matière de sécurité et de performance dans MP2PSN, nous introduisons un schéma de détection intelligent et sûr) avec une forte préservation de la confidentialité, appelé SDPP, qui permet à un utilisateur de partager en toute sécurité des informations avec ceux qui ont les mêmes intérêts similaires dans MP2PSN. Les contributions de ce chapitre sont de quatre ordres :

- Premièrement, nous définissons la notion d'un réseau P2P social mobile (MP2PSN), celui qui fournit une plateforme pour les utilisateurs qui ont les mêmes intérêts similaires afin d'agir comme fournisseurs et consommateurs de ressources.
- Deuxièmement, pour garantir la sécurité du MP2PSN, nous proposons un cadre de certification efficace, où l'autorité de confiance commence à initialiser le système. Ensuite, pour le nœud N_i, le proxy mobile lui envoie sa clé privée et son certificat. Le nœud N_i peut vérifier le certificat et peut également signer de nouveau le certificat en utilisant la technologie de cryptographie re-signature proxy [52].
- Troisièmement, afin de détecter les attaques de routage, nous proposons un système de détection coopératif efficace voisin × voisin (cooperative neighbor × neighbor (CNN)). Ce système peut détecter d'une façon intelligente en basant sur deux phases {réponse demandée et réponse à la demande}. Pour atteindre la confidentialité du message, il utilise le chiffrement homomorphique [69].
- Enfin, nous analysons les propriétés de sécurité du schéma SDPP proposé pour valider sa sécurité dans le modèle de l'oracle aléatoire et simulons dans deux scénarios différents. Les résultats de simulation étendus dans le premier scénario montrent que le schéma SDPP proposé peut détecter l'attaque du trou noir plus dans la configuration où l'attaque est lancée sur un certain nombre de plus de saut et le délai moyen de rapport du Detectreq (DRD) des utilisateurs sociables est évidemment moins que ceux des utilisateurs qui ne sont pas sociables. Ainsi, dans le deuxième scénario, nous nous concentrons sur le délai de transmission du SDPP au proxy mobile avec une évaluation approfondie de la performance, qui conduit en outre vers son aspect pratique.

Le reste de ce chapitre est organisé comme suit. Dans la section 5.2, nous introduisons le modèle du système, le modèle de routage, le modèle de menace, et les objectifs de recherche. Dans la section 5.3, nous donnons des préliminaires sur les chaînes de hachage, le chiffre-

ment homomorphique, le couplage bilinéaire et la signature identitaire. Nous proposons notre système SDPP pour MP2PN à la section 5.4, suivi de son analyse de sécurité dans la section 5.5, et l'évaluation de la performance dans la section 5.6. Nous comparons notre proposition avec d'autres protocoles dans la section 4.7. Enfin, nous apportons des conclusions dans la section 5.8.

5.2 Modèles du système et objectifs de la recherche

Dans cette section, nous présentons le modèle du système MP2PN, le modèle de routage, le modèle de menace, et les objectifs de recherche.

5.2.1 Le modèle du système MP2PN

Nous considérons un réseau MP2PSN, composé d'une seule autorité de confiance (TA), un nœud de communauté P2P, et un grand nombre d'utilisateurs avec de téléphones mobiles $\mathcal{N} = \{N_1, N_2, \ldots\}$ en réseau ad hoc, comme le montre la figure 5.1.

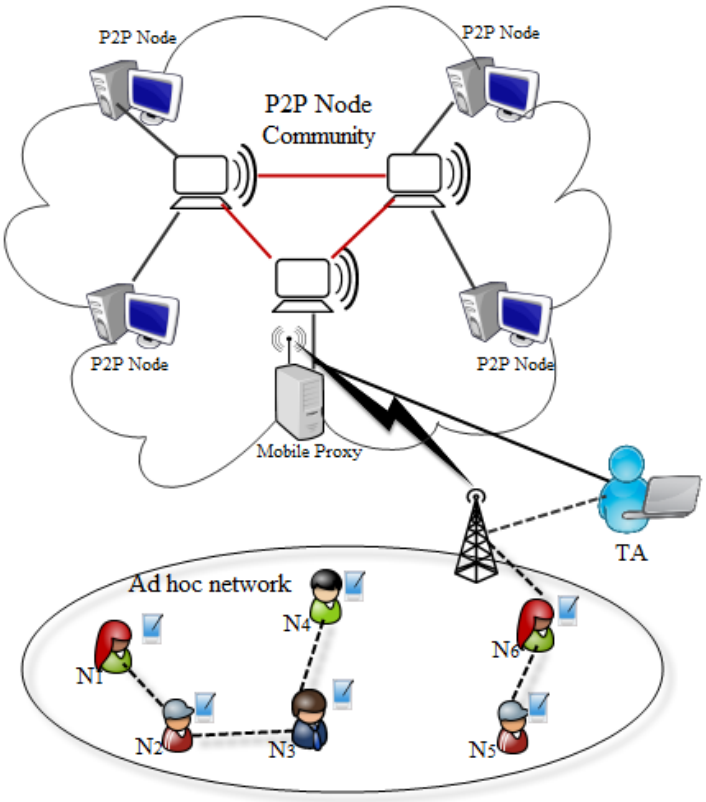


Figure 5:1 Le modèle du système MP2PSN

- L'autorité de confiance (TA): Le TA est entièrement approuvé par toutes les parties dans le système , il est en charge de la gestion de l'ensemble du système de P2P mobile, par exemple, l'initialisation du système P2P mobile, l'enregistrement des utilisateurs au proxy mobile (MP). Les informations des domaines sont disponible pour toutes les entités. En outre, le TA est supposé alimenté avec une capacité de stockage suffisante et il est impossible pour n'importe quel adversaire de faire des compromis.

- Le nœud de communauté P2P (P2P NC): Le P2P NC est une architecture de réseau décentralisée et distribuée, dans laquelle chaque nœud du réseau (appelé «pairs») agit comme des fournisseurs et des consommateurs de ressources.
- Le proxy mobile (MP): Le MP est un pair virtuel connecté au réseau de P2P. Il peut représenter entièrement le dispositif de PDA sans fil vers les nœuds fixes et autres P2P mobiles, même dans la situation où le PDA est hors de portée ou manquant de batterie. En outre, le MP se connecte avec le TA par des liaisons filaires dans le système. Il offre un service de diffusion de l'information et la mise à jour de certificat. Les certificats délivrés par un MP peuvent être utilisés uniquement dans le domaine où le MP est situé.
- Les utilisateurs $\mathcal{N} = \{N_1, N_2, \ldots\}$ sont un groupe d'utilisateurs enregistrés, chaque utilisateur $N_i \in \mathcal{N}$ équipé d'un dispositif de PDA sans fil, où l'utilisateur peut périodiquement se rencontrer et de recevoir les dernières nouvelles, partager des expériences avec d'autres utilisateurs dans le réseau ad hoc ou P2P NC, etc. Contrairement à l'utilisateur à la maison, les utilisateurs $\mathcal{N}$ dans notre modèle sont mobiles et ont leur sociabilité afin qu'un MP2PSN peut être formé.
- Socialité: Dans notre modèle, les utilisateurs ont N socialités différentes. Certains sont actifs, d'autres ne le sont pas. Si les utilisateurs sont actifs, ils peuvent partager leurs informations avec d'autres utilisateurs en réseau ad hoc ou avec le nœud d'échange en P2P CN qui ont des intérêts similaires à partager avec leurs amis ou trouver des gens. Cependant, si les utilisateurs ne sont pas sociables, même s'ils se heurtent souvent aux autres, une relation sociale fondée sur les intérêts similaires reste difficile à établir [70].

  Pour chaque utilisateur $N_i \in \mathcal{N}$, soit $\mathrm{sim}(N_i)$ les intérêts similaires du N_i, et $\mathrm{soc}(N_i)$ N_i's socialité, et définie comme suit

$$\mathrm{sim}(N_i) = \begin{cases} 1, \text{si l'utilisateur est sociable;} \\ 0, \text{ sinon.} \end{cases}$$

  Quand deux utilisateurs $N_i,\ N_j \in \mathcal{N}$ se contactent, les conditions nécessaires à l'établissement d'une relation sociale fondée sur les mêmes intérêts similaires sont les suivants :

$$\begin{cases} \mathrm{soc}(N_i) = \mathrm{soc}(N_j) = 1, & N_i, N_j \text{ sont sociable ;} \\ \mathrm{sim}(N_i) = \mathrm{sim}(N_j), & \text{ont les mêmes intérêts similaires.} \end{cases}$$

5.2.2 Le modèle de routage

Un protocole de routage ad hoc est une convention ou une norme, qui contrôle la façon dont les nœuds décident comment acheminer des paquets entre les nœuds dans le réseau ad hoc. Dans notre modèle de routage, nous choisissons le protocole de routage AODV comme protocole de communication dédié à l'acheminement des paquets entre les nœuds. Plus de détails sur ce protocole de routage, voir la sous section 2.2.1 du chapitre 2.

5.2.3 Le modèle de menace

Nous nommons un nœud *;* un adversaire ou un attaquant s'il s'écarte des protocoles de routage du réseau MP2PSN ou touche la vie privée de l'utilisateur. En outre, nous nous référons à des adversaires qui créent des tunnels de communication privés. L'adversaire peut être un membre authentifié du réseau. Plus précisément, dans notre modèle de menace, nous considérons que l'adversaire pourrait diffuser des informations fausses dans le réseau afin d'affecter le comportement des autres utilisateurs ou de toucher l'infrastructure du réseau MP2PSN, e.g., l'attaque du trou noir, l'attaque d'analyse des paquets, l'attaque de traçage des paquets, l'attaque du trou gris, et l'attaque du trou de ver. Plus de détails sur ces attaques, voir les références [B1] [B2] [B3].

5.2.4 Les objectifs de recherche

Depuis que le réseau MP2PSN est un scénario de réseau sans fil à grande échelle pour le secteur public, il fait face à des défis graves de sécurité et de confidentialité. Dans le schéma SDPP, nous visons à atteindre les objectifs de sécurité et de confidentialité suivante:

- **Disponibilité (Availability):** Cette propriété implique que les services ou les ressources demandés sont disponibles en temps opportun, même si il y a un problème ou un dysfonctionnement dans le système. Dans notre contexte, il est nécessaire d'assurer l'accès à la fonction de calcul d'itinéraire à tout moment.
- **Authentification (Authentication):** Cela comprend l'authentification des utilisateurs et l'intégrité du message. Tous les messages doivent être acceptés par les membres juridiques et livrés sans modification.
- **Détection précoce des attaques de routage (Early detecting the routing attacks):** Quand les attaques sont détectées au plus tôt, plus l'énergie peut être enregistrée dans l'ensemble du réseau.
- **Résistance à l'imitateur (Impersonator resistance)**: La résistance à l'imitateur est précisée que, lorsque deux utilisateurs $N_i,\ N_j \in \mathcal{N}$ exécutent la phase "Réponse demandée", si $\mathrm{soc}(N_i) = \mathrm{soc}(N_j) = 1$ et $\mathrm{sim}(N_i) \neq \mathrm{sim}(N_j)$, la probabilité que N_i estime que N_j a les mêmes intérêts similaires, $\mathrm{sim}(N_i)$ est négligeable.
- **Transparence (Transparency)**: Cette propriété implique la confidentialité. Si l'adversaire contre la confidentialité existe, il est en mesure de récupérer le message d'origine. Ainsi, il sera possible d'utiliser cet adversaire pour construire un adversaire contre la transparence.
- **Résistance au détecteur (Detector resistance)**: La résistance au détecteur est indiquée que, lorsque deux utilisateurs $N_i,\ N_j \in \mathcal{N}$ exécute la phase "Réponse demandée", si $\mathrm{soc}(N_i) = \mathrm{soc}(N_j) = 1$ et $\mathrm{sim}(N_i) \neq \mathrm{sim}(N_j)$, N_j n'a aucune idée sur les intérêts similaires $\mathrm{sim}(N_i)$ que N_i a.
- **Tête d'authentification (Authentication overhead)**: Il s'agit principalement de trois parties dans les messages Detectreq & Detectrep, à savoir, le coût du message de signature, le coût de la vérification et de la communication en tête, qui comprend le certificat et la signature, comme montré dans le tableau 5.1 (voir section 5.4.1).

5.3 Préliminaires

Dans cette section, nous examinons les chaînes de hachage [57], le chiffrement homomorphique [69], le couplage bilinéaire [25] [30], et la signature basée sur l'identité [71], qui servira de base du schéma SDPP proposé.

5.3.1 Les chaines de hachage

Comme présenté dans la sous section 4.4.1 du chapitre précédent, les chaines de hachage sont des fonctions à sens unique, en particulier en permettant de réduire une chaîne de bits de n'importe qu'elle taille $\{0,1\}$ dans un digest de taille fixe $\{0,1\}^{\lambda}$ avec λ un paramètre de sécurité. Plus de détails sur ce type de hachage, voir la sous section 2.3.2.1.1 du chapitre 2.

5.3.2 Le chiffrement homomorphique

Le chiffrement homomorphique (HE) permet à certaines opérations algébriques sur le texte en clair pour effectuer directement sur le texte chiffré. Ce type de chiffrement est habituellement utilisé pour les applications qui préservent la confidentialité (la vie privée). Dans HE, la clé publique est (N, g) , et la clé privée correspondante est $sk(\lambda, \delta)$. Soient $E(\cdot)$, m, et r , la fonction de chiffrement, un message et un nombre aléatoire, respectivement. Le cryptogramme est

$$c = E(m) = g^m \cdot r^N \bmod N^2$$

Le texte en clair est

$$m = D(c) = L\left(c^{\lambda \bmod N^2}\right) \cdot \delta \bmod N$$

Quand la fonction $(x) = (x-1)/N$, l'additif propriété homomorphique est définie comme suit:

$$\begin{aligned} E(m_1) \cdot E(m_2) &= (g^{m_1} \cdot r_1^n)(g^{m_2} \cdot r_2^n) \bmod n^2 \\ &= g^{m_1+m_2} \cdot (r_1 r_2)^n \bmod n^2 \\ &= E(m_1 + m_2) \end{aligned}$$

5.3.3 Le couplage bilinéaire

Comme présenté dans la sous section 4.4.1 du chapitre précédent, un couplage bilinéaire est une application $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$ ayant trois propriétés, i.e., calculable, bilinéaire, et non-dégénérée. Dans la sous section 2.3.1.1 du chapitre 2, voir les détails du couplage bilinéaire.

5.3.4 La signature basée sur l'identité

La signature basée sur l'identité est définie par les quatre algorithmes suivants:

- **L'installation (Setup):** soit le paramètre de sécurité k, le générateur de clé privée (PKG) premièrement choisi deux groupes $\mathbb{G}_1$ et $\mathbb{G}_2$ d'ordre premier $q > 2^k$. Puis PKG choisi le générateur P du $\mathbb{G}_1$ et la clé de master aléatoire $s \in \mathbb{Z}_q^*$ et calcule la clé publique associée

$P_{pub} = sP$. Il prend aussi les fonctions de hachage cryptographiques H_1,H_2 : $\{0,1\}^* \rightarrow \mathbb{G}_1^*$. Les paramètres publics du système sont$(q, \mathbb{G}_1, \mathbb{G}_2, e, H_1, H_2)$.

- **La génération des clés (Keygen):** soit ID est l'identité de l'utilisateur, le PKG calcule $Q_{ID} = H_1(ID) \in \mathbb{G}_1$ et la clé privée associée $d_{ID} = sQ_{ID} \in \mathbb{G}_1$ qui est transmis à l'utilisateur.
- **La signature (Sign):** pour signer un message, l'utilisateur choisit un nombre aléatoire $\in \mathbb{Z}_q^*$, et calcule $U = rP$, $V = d_{ID} + rH_2(ID, M, U)$. La signature sur$M$ est le couple $\sigma =< U, V >$.
- **La vérification (Verify):** pour verifier la signature $\sigma =< U, V >$ sur un message M pour l'identité ID, le vérificateur accepte la signature si $e(P, V) = e(P_{pub}, H_1(ID))$ $e(U, H_2(ID, M, U))$.

5.4 Notre schéma SDPP pour le réseau social peer-to-peer mobile

Dans cette section, nous proposons notre schéma SDPP, qui se compose de quatre parties: l'initialisation du système, les certificats délivrés par le MP, la détection d'attaques, et l'évolution du certificat.

5.4.1 L'initialisation du système

Chaque noeud $\{N_1, N_2, \ldots\}$ dans le MP2PSN initialise deux messages de contrôle $\{Detectreq, Detectrep\}$, ces messages ont le même format de message « demande de route RREQ » [9] qui comprend trois parties, à savoir, le coût de signature, le coût de vérification, et les frais généraux de communication (y compris le soc, le som, le certificat et la signature, comme indiqué dans le tableau 5.1). Soit les paramètres bilinéaires $(q, P, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e)$, le TA initialise le système en exécutant les étapes suivantes.

- ***Etape-1:*** Le TA choisit un algorithme de chiffrement symétrique sécurisé Enc_s (.)avec la clé secrète, e.g., AES, et trois fonctions de hachage sécurisésH_1, H_2 et H_3 , où $H_1 : \{0,1\}^* \rightarrow \mathbb{G}_1$, $H_2 : \{0,1\}^* \rightarrow \mathbb{G}_2$, et $H_3 : \mathbb{G}_T \rightarrow \mathbb{Z}_q^*$. Aussi, le TA choisit un nombre aléatoire r dans $\mathbb{Z}_q^*$, et calcule $Q = rP$ et $\mathcal{P}_{TA} = rH_1(ID_{TA})$, où ID_{TA} est la chaîne d'identité du TA.
- ***Etape-2:*** Le TA choisit ΔT selon les exigences de la confidentialité de la plupart des nœuds et définit la période de validité du certificat égal à ΔT. Ensuite, le TA estime le nombre de certificats qu'un nœud doit mettre à jour à partir d'un MP une fois selon la densité du MP dans chaque domaine.

0										1										2							
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7
Type								J	R	G	D	U	Reserved											Hop Count			
Detectreq ID																											
Destination IP Address																											
Destination Sequence Number																											
Originator IP Address																											
Originator Sequence Number																											
soc																				sim							
Certificate																				Signature							

Tableau 5:1 Format du message signéDetectreq, Detectrep

- ***Etape-3:*** Le TA calcule la clé publique de chiffrement homomorphique (N, g) , et la clé privée correspondante (λ, δ).

- ***Etape-4:*** Le TA publie dans MP2PSN les paramètres du système publique

$$\text{PubParam} = \{(q, P, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e, Q, H_1, H_2, H_3, N, g, Enc_s(.), \Delta T)\}$$

et maintient la clé principale $(\lambda, \delta, s, \mathcal{P}_{TA}, r)$ en secret.

- ***Etape-5:*** Quand $MP_x(x = 1, \dots, n)$ s'enregistre dans le système, le TA calcule la clé privée basée sur l'identité $SK_{MP_x} = rH_1(ID_{TA}||ID_{MP_x})$, où ID_{TA} et ID_{MP_x}sont les chaînes de l'identité de TA et MP_x, respectivement. Ensuite, le TA envoie SK_{MP_x} à MP_x par l'intermédiaire d'un canal sécurisé.

5.4.2 Les certificats délivrés par le MP

Quand un nouveau nœud N_i désir communiquer avec d'autres nœuds dans le domaine D_y , le MP_x délivre la clé privée SK_{N_i} et le certificat Cert_{MP_x,N_i} comme se présente dans la liste qui suit :

- ***Etape-1:*** Le MP_x choisit un nombre aléatoire r_{MP_x} dans $\mathbb{Z}_q^*$ comme la clé principale (master), et calcule l'identité de pseudo $PID_{N_i} = Enc_{r_{MP_x}}(ID_{N_i})$, la clé privée $SK_{N_i} = r_{MP_x}H_1(ID_{MP_x}||PID_{N_i})$, et la clé publique $PK_{N_i} = r_{MP_x}P$, où ID_{N_i} et ID_{MP_x} sont les chaînes de l'identité du N_i et MP_x , respectivement. Ensuite, le MP_x calcule son point privé $Q_{MP_x} = r_{MP_x}P$ et $\mathcal{P}_{MP_x} = rH_1(ID_{MP_x})$.

- ***Etape-2:*** Le MP_x génère le certificat $\text{Cert}_{MP_x,N_i} < PK_{N_i}, V >$, où

$$V = PID_{N_i} + r_{MP_x}H_2(ID_{MP_x}, SK_{N_i}, PID_{N_i})$$

- ***Etape-3:*** Le MP_x envoie SK_{N_i} et Cert_{MP_x,N_i} à N_i via un canal sécurisé.

5.4.3 La détection d'attaques

Comme représenté dans la figure.5.3 (a,b), le SDPP utilise le mécanisme de coopération voisin × voisin (CNN) basé sur deux phases {réponse demandée et réponse à la demande} pour détecter les attaques.

5.4.3.1 Réponse demandée

Comme cité dans la section 5.2.4, l'adversaire peut créer des tunnels de communication privés pour envoyer des faux messages, i.e., l'attaque du trou de ver. Cependant, chaque nœud $N_i \in$ MP2PSN initie une demande de réponse (exécute l'algorithme 5.1) à des nœuds N_j dans sa table de routage à 1-saut, et attend la réponse de sa demande pour exécuter la phase de notification. Cette phase de demande de réponse est résumée dans les étapes suivantes:

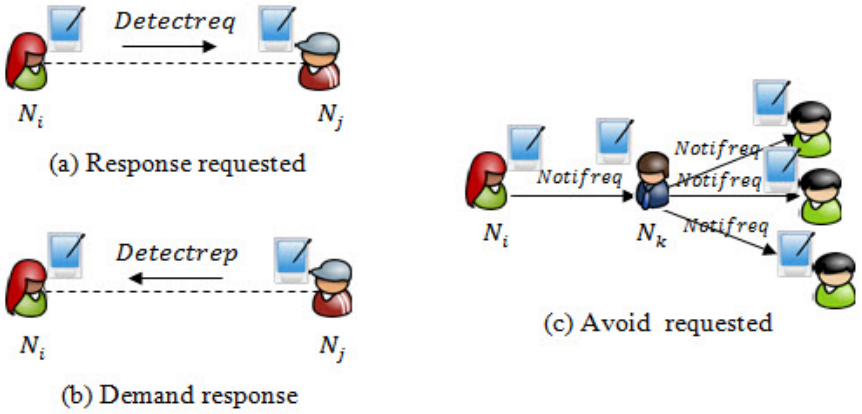


Figure 5:2 Le mécanisme de détection basé sur la coopération CNN

- ***Etape-1:*** Le nœud N_i signe le message $Detectreq$ avec la clé publique $PK_{N_j} < g_{Nj}, N_{Nj} >$ du nœud récepteur N_j et le nombre aléatoire r_{N_i} dans $\mathbb{Z}_q^*$. (Voir l'algorithme 5.1, ligne 1 à 2)
- ***Etape-2:*** Pour éviter les collisions, le nœud N_j attend l'épuisement du temps SIMS. Ensuite, il envoie à tous les noeuds à 1-saut dans sa table de routage. (Voir algorithme 5.1, ligne 4 à 6)
- ***Etape-3:*** Après avoir reçu une réponse de requête envoyée par le nœud N_j , le nœud N_i extrait le message de réponse $Detectrep$ encrypté à partir de D. Ensuite, le nœud N_i extrait Cert_{MP_x,N_j} à partir de $Detectrep$ et vérifie la validité du certificat avec MP_x. (Voir l'algorithme 5.2, ligne 1 à 4)
- ***Etape-4:*** Si le certificat Cert_{MP_x,N_j} est valide, il considère que le lien avec le nœud N_j est prouvé. Sinon, il retourne suspect. (Voir l'algorithme 5.2, ligne 6 à 7)

5.4.3.2 Réponse à la demande

Quand le nœud N_j reçoit la requête de détection, il exécute Demand_Reponse () (Algorithme 5.3). Cette phase de la réponse à la demande est résumée dans les étapes suivantes:

- ***Etape-1:*** Quand le nœud N_j reçoit le message de contrôle $Detectreq$ encrypté, il le récupère à partir du C. Ensuite, le nœud N_j récupère Cert_{MP_x,N_i} à partir de $Detectreq$ et valide le certificat avec MP_x. (Voir l'algorithme 5.3, ligne 1 à 4)
- ***Etape-2:*** Si le certificat Cert_{MP_x,N_j} n'est pas valide, il exécute l'algorithme 1. Sinon, le noeud N_j signe le message $Detectrep$ avec la clé publique $PK_{N_i} < g_{N_i}, N_{N_i} >$ du noeud émetteur N_i et le nombre aléatoire r_{N_j} dans $\mathbb{Z}_q^*$. (Voir l'algorithme 5.3, ligne 7 à 8)
- ***Etape-3:*** Le noeud N_j attend l'épuisement du temps $SIMS$ et envoie le texte chiffré D. (Voir l'algorithme 5.3, ligne 9 à 10)

5.4.4 L'évolution du certificat

Nous étendons la chaîne d'identité ID à $ID||d$, où d représente la date d'expiration. Pour le noeud N_i , la chaîne d'identité $ID_{N_i}||d$ est valable uniquement avant la date d'expiration indiquée d. Après d, le certificat correspondant $\text{Cert}_{MP_x,N_i}||d$ est automatiquement révoqué si un

nouveau certificat n'est pas généré par MP_x. Pour cela, SDPP adopte une stratégie de restauration en utilisant la technologie de cryptographie re-signature proxy [52].

Remarques:

- Si le noeud N_i détermine que le lien avec le nœud N_x est suspect, le noeud N_i supprime le nœud adversaire N_x dans sa table de routage à 1-saut. Ensuite, il envoie à tous ses voisins, comme montré dans figure 5.3 (c). Lorsque le nœud voisin reçoit la demande de notification, il supprime le nœud adversaire N_x dans sa table de routage. A la fin, le nœud voisin envoie le message de notification à tous les nœuds dans sa table de routage (Voir l'algorithme 5.4).
- Une fois le schéma SDPP est réussie, l'utilisateur N_i et N_j peut utiliser l'évolution de certificat pour échanger en toute sécurité ses informations et expériences, et de donner un soutien mutuel à d'autres voisins avec P2P NC. Grâce à ces fonctionnalités prometteuses, MP2PSN peut être largement utilisé par plusieurs utilisateurs. En outre, parce que le point d'accès (AP) n'est pas toujours disponible pour un utilisateur dans un environnement mobile, les utilisateurs actifs, sur la base d'intérêts similaires de relation sociale, peuvent aussi aider leurs amis à relayer leurs informations. De cette manière, le retard d'information peut être réduit [70] (Voir l'algorithme 5.5).

Algorithm 1: Response requested
Input : The control message *Detectreq*
Output : *The ciphertext C*

Begin
  Choose a random number $r_{N_i} \in \mathbb{Z}_q^*$;
    Compute *C the ciphertext of Detectreq*
    $C = E(Detectreq) = g_{Nj}{}^{Detectreq} \cdot r_{N_i}{}^{N_{Nj}} \bmod N_{Nj}{}^2$
      Where $PK_{Nj} < g_{Nj}, N_{Nj} >$
  for each $N_j \in 1 - hop\ of\ N_i$ **do**
    Obtain the Short Inter-Message Space*SIMS* ;
    Send_Request (C , N_j);
  end;
End;

Algorithme 5:1 Demande de détection dans SDPP

Algorithm 2: Demand_verification

Input : *The ciphertext D*

Output : The link is *proved* or *suspicious*

1: **Begin**

2: When the node N_i receive *the ciphertext D*, recover *Detectrep* from D ;

3: $Detectrep = L\left(D^{\lambda \bmod N_{Nj}^2}\right) \cdot \delta \bmod N_{N_i}$;

Where $SK_{N_i} < \lambda, \delta >$

4: Recover Cert_{MP_x,N_j} from *Detectrep* ;

5: Checks the certificate Cert_{MP_x,N_j} with MP_x;

6: **if** Cert_{MP_x,N_j} is valid **then** return *proved* ;

7: **else** return *suspicious* ;

8: **End;**

Algorithme 5:2 Vérfication des demandes dans SDPP

Algorithm 3: Demand_Reponse

Input : *The ciphertext C* , the control message *Detectrep* , and the sender N_i

Output : *The ciphertext D*

1: **Begin**

2: When the node N_j receive *the ciphertext C*, recover *Detectreq* from C ;

$Detectreq = L\left(C^{\lambda \bmod N_{Nj}^2}\right) \cdot \delta \bmod N_{Nj}$;

Where $SK_{Nj} < \lambda, \delta >$

3: Recover Cert_{MP_x,N_i} from *Detectreq*;

4: Checks the certificate Cert_{MP_x,N_i} with MP_x

5: **if** Cert_{MP_x,N_i} is not valid **then** Response_requested ();

6: **else begin**

7: Choose a random number $r_{N_j} \in \mathbb{Z}_q^*$;

8 : Compute *D the ciphertext of Detectrep*

$D = E(Detectrep) = g_{N_i}{}^{Detectrep} \cdot r_{N_j}{}^{N_{N_i}} \bmod N_{N_i}{}^2$

Where $PK_{N_i} < g_{N_i}, N_{N_i} >$

9: Obtain the Short Inter-Message Space*SIMS*

10: Send_Request (D ,N_i);

11: **end;**

12: **End;**

Algorithme 5:3 La réponse de la détection d'attaque demandée dans SDPP

Algorithm 4: Avoid _requested

Input : The control message $Notifreq$, and the adversary N_x

Output : $The\ ciphertext\ E$

1: **Begin**
2: **if** $N_x \in (1 - hop\ of\ N_i)$ **then**
3: remove N_x in the routing table of N_i at 1-hop;
4: Choose a random number $r_{N_x} \in \mathbb{Z}_q^*$;
5: **for** each $N_k \in 1 - hop\ of\ N_i$ **do**
6 : Compute $E\ the\ ciphertext\ of\ Notifreq$

$$E = E(Notifreq) = g_{N_k}{}^{Notifreq} \cdot r_{N_x}{}^{N_{Nk}} \bmod N_{nj}{}^2$$

Where $PK_{N_k} < g_{N_k}, N_{N_k} >$;
7: Obtain the Short Inter-Message Space$SIMS$;
8: Send_Request (E , N_k);
9: **End**;

Algorithme 5:4 Notification des attaques dans SDPP

Algorithm 5: Social-Based Information Collaborative

Input : The status of AP

Output: The information I_i

1: **Begin**
2 User N_i's PDA device periodically collect information I_i ;
3: **if** an AP is available nearby **then**
4: N_i directly report I_i to P2P NC via AP;
5: **else if** another user N_i nearby **then**
6: **if** $\mathrm{soc}(N_i) = \mathrm{soc}(N_j)$ && $\mathrm{sim}(N_i) = \mathrm{sim}(N_j)$ **then**
7: N_i and N_j exchange their information if their PDAs' storages are available. Later, before I_i's expiration, N_j helps I_i when he runs into an available AP; otherwise, I_i will be deleted.
8: **end if**
9: **End;**

Algorithme 5:5 L'information collaborative basée sur le réseau social dans SDPP

5.5 L'analyse de sécurité

Dans cette section, nous analysons les propriétés de sécurité du schéma SDPP proposé en fonction des objectifs de sécurité présentés à la section 5.2.5. Nous analysons d'abord la sécurité du schéma SDPP proposé pour être un schéma sûr, i.e., les exigences de la résistance à l'imitateur et la résistance au détecteur peuvent être satisfaites. Ensuite, nous nous préoccupons de la façon dont SDPP peut atteindre la confidentialité (la vie privée) du message et l'évolution des certificats des utilisateurs.

5.5.1 La sécurité sémantique

Soit un adversaire polynôme $\mathcal{A}$ essaye de gagner l'expérience contre le challenger $\mathcal{C}$. Dans SDPP, l'adversaire$\mathcal{A}$ peut utiliser les quatre oracles suivantes: 1) $\mathcal{O}.Sign(m, PK, VAB)$ permet à l'adversaire $\mathcal{A}$ d'obtenir une signature originale sur le message m de son choix avec la clé publique du signataire PK et la variable VAB que l'adversaire a mis; 2) $\mathcal{O}.Modify(m, c, ALT)$ permet à l'adversaire $\mathcal{A}$ de modifier une paire de message-signature(m, c) avec les changements ALT qu'il souhaite. L'oracle retourne une signature modifiée valable si des modifications sont admissibles et $\perp$ en cas d'erreur; 3) $\mathcal{O}.Prove(m, c, DB)$ permet à l'adversaire $\mathcal{A}$ d'obtenir une preuve de l'origine du paire de message-signature(m, c) selon une base de données $DB = \{(m_k, c_k)\}_{k\in[1,q]}$. 4) $\mathcal{O}.Sign/Modify_b(m, \text{VAB}, MOD)$ permet à l'adversaire $\mathcal{A}$ prenant en entrée un message m, VAB et MOD.. Si $b = 0$, il renvoie une signature originale du signataire m' (m' est le message correspondant au message m modifié par MOD). Et si $b = 1$, il effectue une signature originale du signataire du message m par VAB et le modifie par MOD.

Théorème 1: *Soit* $(q, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e, g_1, g_2)$ *un environnement bilinéaire d'ordre premier,* λ *un paramètre de sécurité et* $\mathcal{A}$ *être un adversaire polynôme dans* SDPP *cherchant à acquérir de l'expérience contre le challenger* $\mathcal{C}$. *Cet adversaire peut accéder aux quatre oracles:*

- $\mathcal{O}.Sign(m, PK, VAB)$,
- $\mathcal{O}.Modify(m, \sigma, ALT)$,
- $\mathcal{O}.Prove(m, \sigma, DB)$
- $\mathcal{O}.Sign/Modify_b(m, VAB, MOD)$.

Le schéma SDPP est sécurisé, i.e., il est résistant imitateur et résistant détecteur.

Preuve: Nous allons pas à pas à travers les propriétés. La plupart du temps, nous décrivons chaque propriété pour SDPP.

Définition 4.1 (SDPP la résistance à l'imitateur (IR)): *Soit* λ *être un paramètre de sécurité,* $\mathcal{G}en(1^\lambda)$ *un algorithme d'initialisation et* $\mathcal{G}enK$ *un algorithme de génération de clé de signataire* (PK, SK) *et* b *un bit choisit aléatoirement. Soit* $\mathcal{A}$ *un adversaire avec l'accès aux quatre oracles:*$\mathcal{O}.Sign(m, PK, VAB)$,$\mathcal{O}.Modify(m, \sigma, ALT)$,$\mathcal{O}.Prove(m, \sigma, DB)$ *et* $\mathcal{O}.Signe/Modify_b(m, VAB, MOD)$. *Si* $b = 0$, *le oracle du challengeur retourne une signature; ou une signature changé si* $b = 1$. *Nous considérons l'expérience aléatoire suivante:*

Experiment $\text{EXP}_{\text{IR},\mathcal{A}}^{\text{SDPP}}(\lambda)$
$param \leftarrow \mathcal{G}en(1^\lambda)$
$(PK.SK) \leftarrow \mathcal{G}enK(param)$
$b \leftarrow \{0, 1\}$
$b^* \leftarrow \mathcal{A}^{Signe,Modify,Prove,Signe/Modify_b}(param, PK)$
if $b^* = b$ then $a \leftarrow 1$ else $a \leftarrow 0$
return a

Nous définissons l'avantage du polynôme adversaire $\mathcal{A}$ dans l'expérience $\text{EXP}_{\text{IR},\mathcal{A}}^{\text{SDPP}}(\lambda)$ via:

$$\mathrm{Adv}_{\mathrm{IR},\mathcal{A}}^{\mathrm{SDPP}}(\lambda) = |\Pr[1 \leftarrow \mathrm{EXP}_{\mathrm{IR},\mathcal{A}}^{\mathrm{SDPP}}(\lambda)] - \frac{1}{2}$$

Le SDPP est dit (λ, t, ϵ) résistant à l'imitateur, si aucun adversaire $\mathcal{A}$ s'exécute dans le temps t a l'avantage $\mathrm{Adv}_{\mathrm{IR},\mathcal{A}}^{\mathrm{SDPP}}(\lambda) < \epsilon$, avec ϵ négligeable.

Définition 4.2 (SDPP la résistance au détecteur DR): *Soit λ un paramètre de sécurité, $Gen(1^{\lambda})$ un algorithme d'initialisation et $GenK$ un algorithme de génération de clé de signataire (PK, SK). Soit $\mathcal{A}$ un adversaire avec accès à l'oracle de changement $\mathcal{O}.Modify(m, \Sigma, ALT)$ et retourne un quadruplet $(SK^*, \pi^*_{or/ALT}, m^*, \sigma^*)$. Nous considérons l'expérience aléatoire suivante:*

Experiment $\mathrm{EXP}_{\mathrm{DR},\mathcal{A}}^{\mathrm{SDPP}}(\lambda)$
$param \leftarrow Gen(1^{\lambda})$
$(PK.SK) \leftarrow GenK(param)$
$(PK^*, \pi^*_{or/ALT}, m^*, \Sigma^*) \leftarrow \mathcal{A}^{Modify}(param, PK)$
Let $(m'_k, \sigma'_k)_{k\in[1,n]}$ the response of the oracle modified
if $S.check(m^*, \sigma^*, PK^*) =$ tru
and $(PK^*, m^*) \neq (PK^*{}_k, m^*{}_k)$ where $k \in [1, n]$
then $a \leftarrow 1$ else $a \leftarrow 0$
return a

Nous définissons le succès de l'adversaire du polynôme $\mathcal{A}$ dans l'expérience $\mathrm{EXP}_{\mathrm{DR},\mathcal{A}}^{\mathrm{SDPP}}(\lambda)$ via:

$$\mathrm{Succ}_{\mathrm{DR},\mathcal{A}}^{\mathrm{SDPP}}(\lambda) = \Pr[1 \leftarrow \mathrm{EXP}_{\mathrm{DR},\mathcal{A}}^{\mathrm{SDPP}}(\lambda)]$$

Le SDPP est dit (λ, t, ϵ) résistant au détecteur, si aucun adversaire $\mathcal{A}$ s'exécute dans le temps t a le succès $\mathrm{Succ}_{\mathrm{DR},\mathcal{A}}^{\mathrm{SDPP}}(\lambda) < \epsilon$, avec ϵ négligeable.

Ceci termine la preuve. ■

5.5.2 Le SDPP fournit la forte préservation de la confidentialité du message

Dans le schéma proposé SDPP, étant donné que les messages de contrôle $\{Detectreq, Detectrep\}$ sont des cryptages chiffré homomorphique [69], l'adversaire $\mathcal{A}$ ne peut pas identifier le message correspondant, même si $\mathcal{A}$ d'espionner le texte chiffré. En outre, étant donné queMP_x ne pas déchiffrer le message, $\mathcal{A}$ ne peut pas faire passer le message, même si $\mathcal{A}$ compromet la base de données du MP_x. Par conséquent, le schéma SDPP fournit la forte préservation de la confidentialité du message.

5.5.3 Le SDPP fournit l'évolution des certificats des utilisateurs

Dans la phase du certificat d'évolution, même si un adversaire $\mathcal{A}$ espionne la communication entre MP_x et N_i, il ne peut pas obtenir les informations sur le certificat généré par la technologie de cryptographie re-signature proxy. D'autre part, même si un adversaire à compromet tout les certificats précédents, il ne peut pas déduire les certificats actuels ou futurs, car le problème du logarithme discret assure la sécurité du certificat. Par conséquent, l'évolution du certificat de sécurité de l'utilisateur est atteinte dans le schéma SDPP proposé.

5.6 Evaluation des performances

Pour évaluer le schéma SDPP, nous avons effectué des simulations dans deux scénarios différents. En introduit tout d'abord l'environnement de simulation utilisé et par la suite nous présentons les résultats de simulation pour chaque scénario. Les mesures de performance utilisées dans l'évaluation sont: i) le taux de détection de trou noir (the black hole detection rate ($\mathrm{D_r}$)); ii) le délai moyen de rapport du Detectreq (the average Detectreq reporting delay (DRD)); et iii) le délai moyen de transmission (the average transmission delay ($\mathrm{t_r}$)).

A) Scénario 1

Dans le premier scénario, nous évaluons l'efficacité du SDPP contre l'attaque du trou noir sur le routage réactif AODV en utilisant le simulateur NS-2 [58] configuré à la norme IEEE 802.11 (11 Mbps etd 2 Mbps ont été utilisés pour transmettre le trafic unicast et broadcast, respectivement). Nous avons généré un certain nombre de topologies aléatoires avec les N noeuds mobiles et 4 points d'accès qui sont régulièrement déployées sur un champ carré variant de 600x600m à 1500x1500m en fonction de la taille du réseau MP2PSN (i.e., nombre de noeud), où N est entre 30 à 80. Dans le cas de 60 nœuds, 30 nœuds ont les mêmes intérêts SI_1 et le groupe de forme $\mathcal{G}_1$, et les autres 30 noeuds ont les mêmes intérêts SI_2 et le groupe de forme $\mathcal{G}_2$. La paire de noeuds d'adversaire est choisie de façon aléatoire parmi les noeuds dans le réseau formé. En outre, la portée de transmission maximale est R^2, le modèle de trafic est CBR. Chaque utilisateur choisit d'abord au hasard une destination dans la région et y arrive en utilisant le chemin le plus court avec la vitesse $v = 1 \pm 0.4\, m/s$.

Soit $P_{k.\mathrm{neigh.adversary}}$ désigne la probabilité qu'il y ait au moins k voisins dans la portée de transmission πR^2 d'un noeud adversaire avec la surface S,

$$\begin{aligned} P_{k.\mathrm{neigh.adversary}} &= P(N \geq k|\pi R^2) \\ &= 1 - P(N < k|\pi R^2) \\ &= 1 - \sum_{i=0}^{k-1} P(N = i|\pi R^2) \\ &= 1 - \sum_{i=0}^{k-1} \binom{|\mathcal{V}|}{i} \left(\frac{\pi R^2}{S}\right)^i \cdot \left(1 - \frac{\pi R^2}{S}\right)^{|\mathcal{V}|-i} \end{aligned}$$

Soit D_r le taux de détection du trou noir,

$$D_r = \frac{1}{T_{detect}}$$

où T_{detect} est le temps de détection de l'attaque

Soit S_r le rapport social d'un groupe, $S_r = \frac{le\ nombre\ d'utilisateurs\ sociables}{le\ nombre\ d'utilisateurs\ dans\ le\ groupe}$ en supposons que les deux SI_1et SI_2 ont le même rapport social S_r = [0, 0.1, 0.2, 0.3].

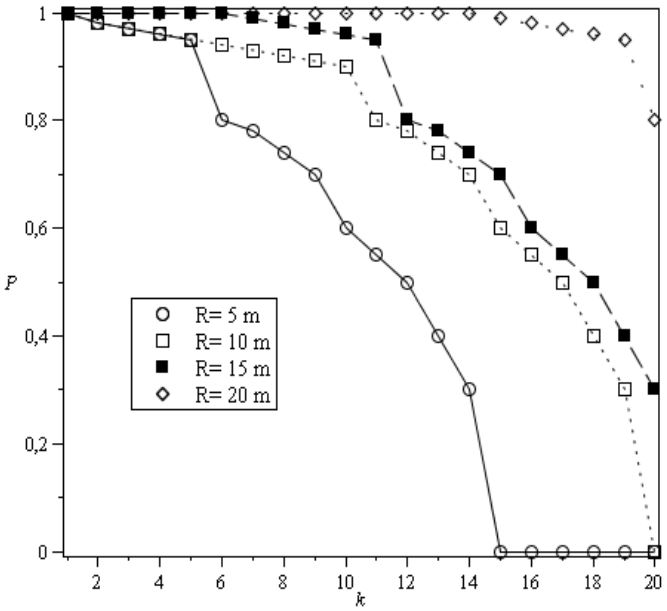


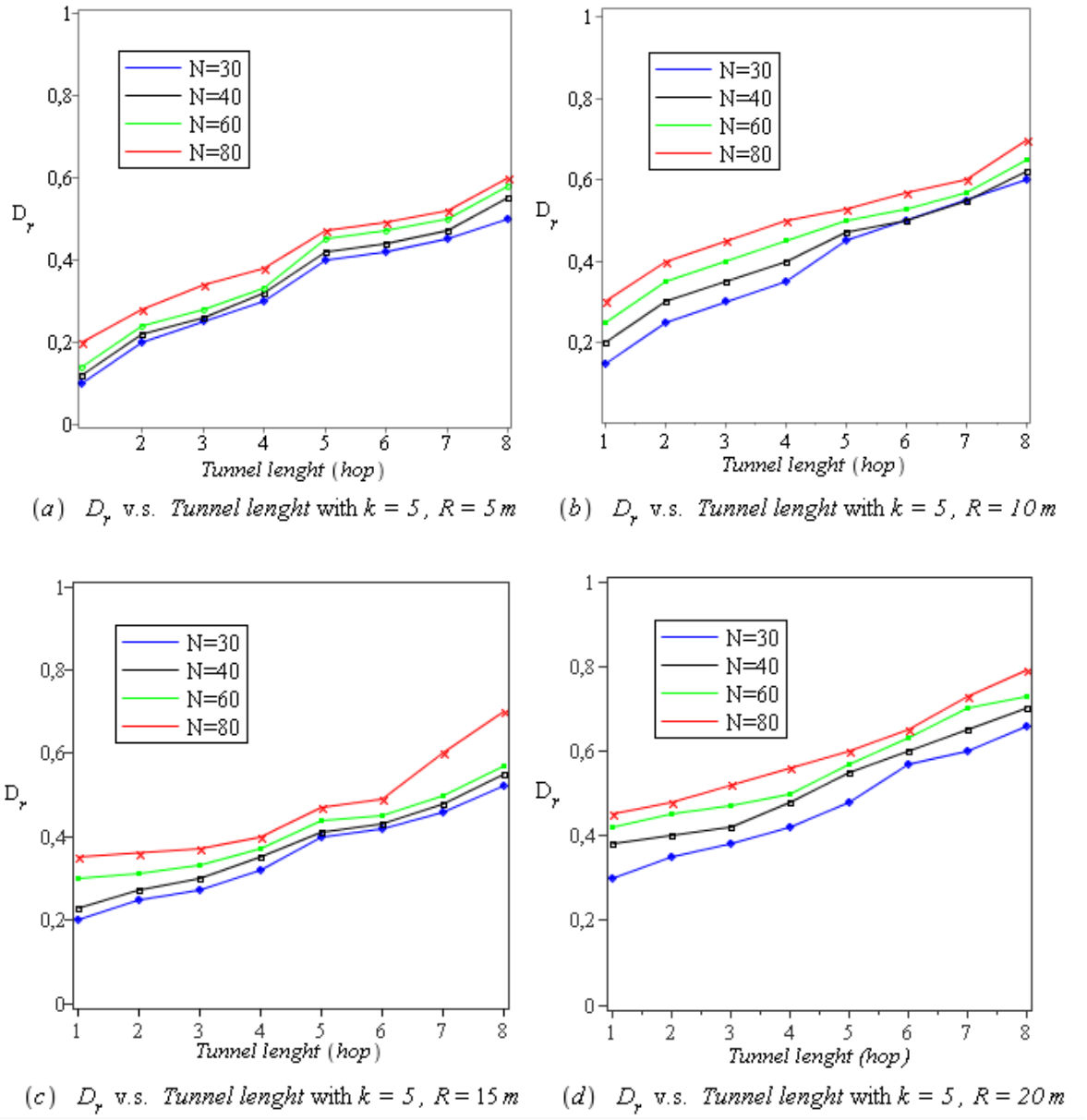
Figure 5:3 La probabilité de k voisins d'un adversaire $P_{k.neigh.adversary}$ avec $S = 200 \times 200\ m^2$, $R = 5m, 10m, 15m, 20m$, $|\mathcal{V}| = 100$, et $1 \leq k \leq 20$

La figure 5.3 présente la probabilité de k voisins d'un adversaire $P_{k.neigh.adversary}$ dans un réseau social sans fil ad hoc avec les différents k, ($1 \leq k \leq 20$). Il est clair que la forte probabilité prévue de l'attaque du trou noir peut être réalisée quand nous choisissons le bon k, i.e., $k \leq 5$.

La figure 5.4 (a,b,c,d) présente le taux de détection du trou noir D_r variant avec la longueur du tunnel qui est le nombre de sauts entre les noeuds de l'adversaire, où $k = 5$ et $R = 5m, 10m, 15m, 20m$. Comme on le voit dans la figure 5.4, le taux de détection de trou noir D_r augmente avec l'augmentation de R dans l'ensemble du réseau ,et l'attaque du trou noir est détectée plus dans la configuration où l'attaque est lancée sur un certain nombre de plus de sauts. C'est un effet évident, que par le lien du tunnel, les paquets sont encapsulés. Aussi, depuis la figure 5.4, nous pouvons observer à peu près la relation entre D_r et le nombre de nœuds N, i.e., avec l'augmentation de N, le taux de détection du trou noir va également augmenter.

Pour discuter davantage sur le taux de détection du trou noir, la figure 5.5 (a,b,c,d) présente le taux de détection du trou noir D_r variant selon l'intervalle d'émission HELLO T_{Hello} (s) et les différentes durées de l'attaque du trou noir , où $k = 5$ et $R = 5m, 10m, 15m, 20m$. La figure 5.5 montre si la durée de l'attaque du trou noir est plus courte que son taux de détection

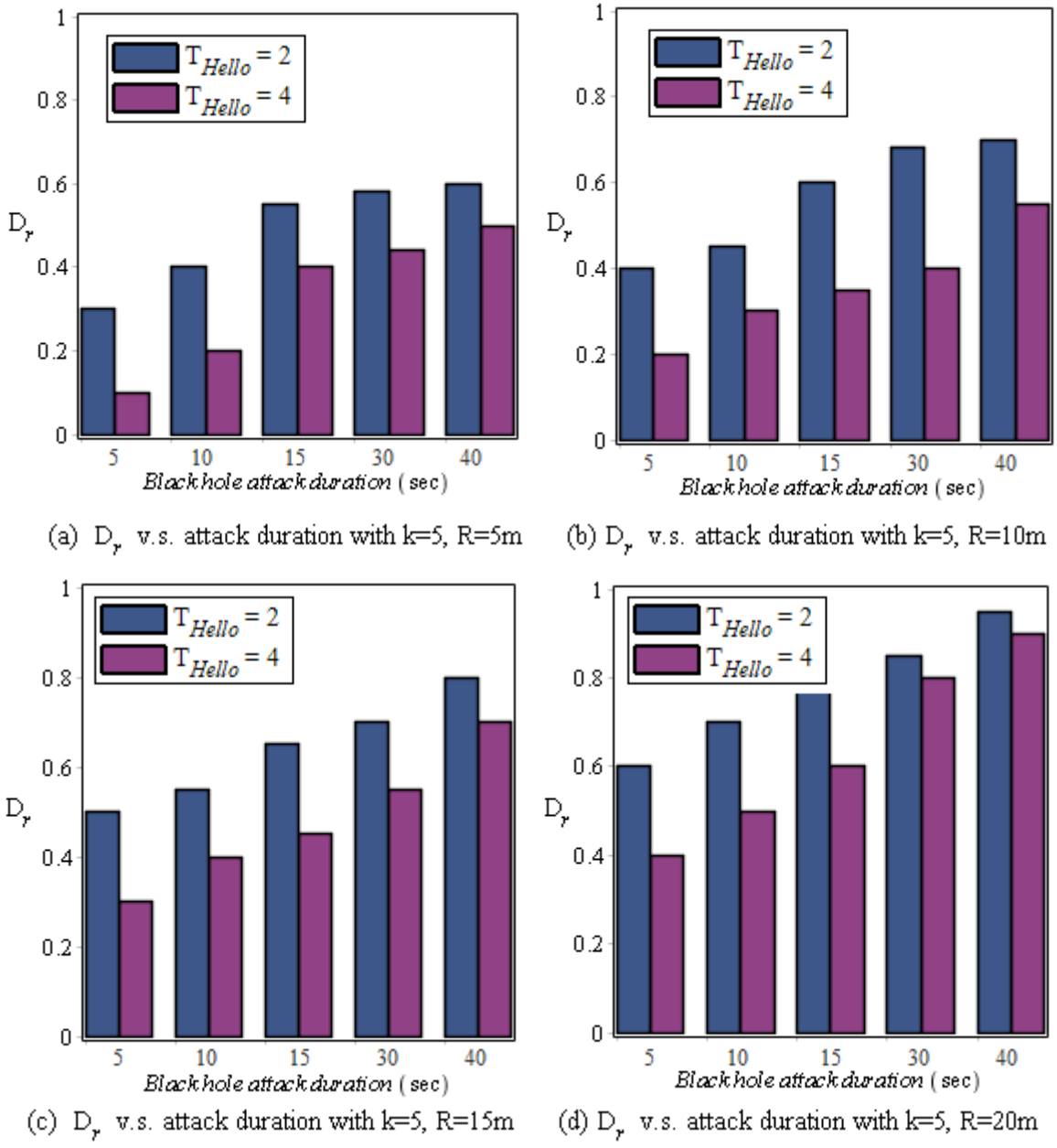
(i.e., moins que 0.6), ceci est dû au fait qu'il existe des noeuds qui n'exécutent pas l'algorithme 5.1 et 5.2. Egalement dans la figure 5.5, le taux de détection du trou noir D_r augmente avec l'augmentation de R dans l'ensemble du réseau. Ce résultat démontre l'impact de T_{Hello} sur le temps de détection. Si l'intervalle d'émission T_{Hello} est assez long, il prend plus de temps à détecter. Par conséquent, le schéma SDPP a besoin d'utiliser de petits intervalles d'émission de message. En outre, plus les attaques des trous noirs sont détectées tôt, plus l'énergie peut être enregistrée dans l'ensemble du réseau



(a) D_r v.s. *Tunnel lenght* with $k = 5$, $R = 5\,m$ (b) D_r v.s. *Tunnel lenght* with $k = 5$, $R = 10\,m$

(c) D_r v.s. *Tunnel lenght* with $k = 5$, $R = 15\,m$ (d) D_r v.s. *Tunnel lenght* with $k = 5$, $R = 20\,m$

Figure 5:4 Le taux de détection d trou noir D_r variant avec la longueur du tunnel.



(a) D_r v.s. attack duration with k=5, R=5m

(b) D_r v.s. attack duration with k=5, R=10m

(c) D_r v.s. attack duration with k=5, R=15m

(d) D_r v.s. attack duration with k=5, R=20m

Figure 5:5 Le taux de détection de trou noir D_r variant selon l'intervalle d'émission HELLO T_{Hello} (s) et les différentes durées de l'attaque du trou noir

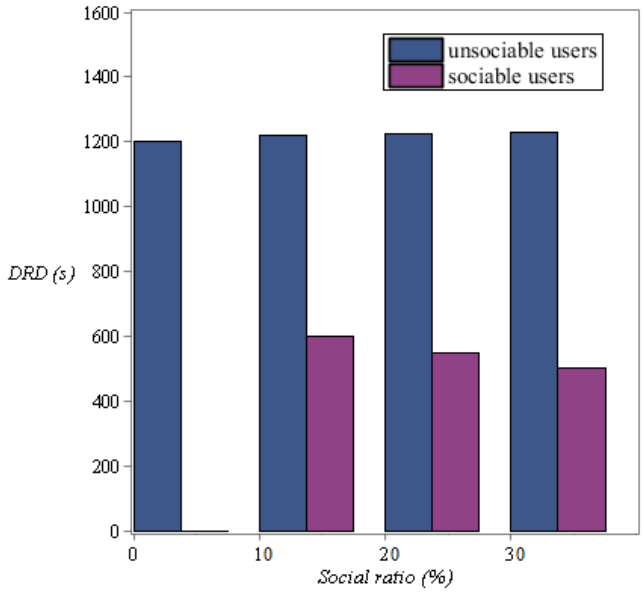


Figure 5:6 Le taux moyen du DRD pour les différents rapports sociaux dans 100 min

La figure 5.6 montre le taux moyen du DRD pour les différents rapports sociaux S_r = [0, 0.1, 0.2, 0.3] dans 100 min. De cette figure, nous pouvons constater que la moyenne DRD des utilisateurs sociables est moindre que ceux des utilisateurs non sociables. Plus le rapport social S_r augmente, plus le DRD diminu. Les résultats présentés ici démontrent que le MP2PSN a un effet positive sur D_r et DRD, et peut être accepté par les utilisateurs mobiles.

B) Scénario 2

Une métrique de performance importante dans les systèmes P2P est le temps qu'il faut pour un nœud d'envoyer un message, i.e., $Detectreq$ pour arriver au P2P NC via le proxy mobile. Dans le second scénario, nous nous concentrons sur le délai de transmission du schéma SDPP au MP. Le coût de calcul du schéma SDPP notamment, la détection, la vérification et la notification de l'attaque, qui concernent principalement les opérations cryptographiques suivantes: authentification, genk, encrypt, decrypt, multiplication dans Z_q^* et les opérations de hachage. Nous implémentons trois types de courbe CP-80, MNT-80, et BN-128. CP-80 est le couplage de Tate avec un degré d'intégration (the Tate pairing) k = 2 Cocks-Pinch courbe sur $\mathbb{F}_p$ avec 512 bit d'ordre premier p . MNT-80 est le couplage de Ate avec un degré d'intégration (the Ate pairing) k = 6 Miyaji-Nakabayashi-Takano courbe sur $\mathbb{F}_{p^3}$ avec 160 bit d'ordre premier p . BN-128 est le couplage de Tate avec un degré d'intégration (the R-ate pairing) k = 12 Barreto-Naehrig courbe sur $\mathbb{F}_{p^2}$ avec 256 bit d'ordre premier p . Les repères pour l'appariement sélectionné est exécuté sur un poste de travail moderne, où le processeur est 64-bit Intel i5 520M, 2.4GHz. Les résultats des mesures sont donnés dans le tableau 5.2. Sur la base de ces chiffres et le chiffrement homomorphique ,et la signature basée sur l'identité [69] [71], on peut estimer le coût de calcul dans SDPP, et les résultats pertinents sont donnés dans le tableau 5.3 [60].

Curve	CP-80		MNT-80		BN-128	
G_2 type	$\mathbb{F}_p$		$\mathbb{F}_{p^3}$		$\mathbb{F}_{p^2}$	
K	2		6		12	
Modulus (bits)	512		160		256	
Paring	Tate		Ate		R-ate	
with/without precomp.	w	w/o	w	w/o	w	w/o
GenK	0.207ms	1.020ms	0.663ms	2.239ms	0.363ms	0.854ms
Encrypt	0.366ms	1.695ms	0.194ms	0.767ms	0.653ms	1.646ms
Decrypt **	1.213ms	2.360ms	1.392ms	3.788ms	4.097ms	4.680ms
Decrypt *	0.834ms	1.991ms	1.043ms	3.383ms	2.533ms	3.106ms

**: 2 pairings / *: multi-pairing

Tableau 5:2 Le coût en temps des opérations nécessaires

Curve	CP-80		MNT-80		BN-128	
with/without precomp.	w	w/o	w	w/o	w	w/o
$Detectreq$ authentication	0.207ms	1.020ms	0.663ms	2.239ms	0.363ms	0.854ms
Encrypt ($t_{encrypt}$)	0.366ms	1.695ms	0.194ms	0.767ms	0.653ms	1.646ms
Decrypt ($t_{decrypt}$)	1.213ms	2.360ms	1.392ms	3.788ms	2.533ms	3.106ms

Tableau 5:3 Le coût en temps des opérations nécessaires dans SDPP

Ensuite, nous avons

$$\mu = \begin{cases} 169.3/s, \text{w/o pairing precomputation;} \\ 377.3/s, \text{with pairing precomputation.} \end{cases}$$

Puis, nous évaluons le délai de transmission dans SDPP. Sur la base de processus M/D/1 [61], nous considérons l'arrivée moyenne $Detectreq$ au niveau du noeud est un processus de Poisson avec le taux d'arrivée , taux de départ μ , et faire avancer le processus de l'état i à $i + 1$. Le temps de retard moyen de $Detectreq$ avant d'être mis dans le tampon du MP est t_v

$$t_v = \frac{1}{\mu}.\frac{2-\rho}{2-2\rho} \quad \text{, where } \rho = \frac{\lambda}{\mu}$$

Par la diffusion du message $Detectreq$, les deux opérations « crypter et décrypter » peuvent être réduites. Cependant, ce mécanisme entraînera le retard de transmission. En outre, l'attaque du trou noir va également entraîner le retard de transmission. Soit la probabilité d'un invalide $Detectreq$ arrivant au MP être p en raison de l'attaque du trou noir. Nous étudions le temps moyen d'attente dans le tampon du MP comme suit. Considérons d'abord combien le temps qu'il prend le i-ème $Detectreq$ dans le nœud pour attendre l'arrivée du prochaine i + 1 i-ème $Detectreq$. Etant donné que la probabilité d'un invalide $Detectreq$ est p, lorsqu'un $Detectreq$ valable est mis en mémoire au tampon du MP, le nombre d'authentifications $Detectreq$ au niveau du MP est une variable aléatoire géométriquement distribuée:

$$P(\text{number of authentication} = k) = p^{k-1}(1-p)$$

où $k = 1,2,\cdots$. Nous définissons $t_{i(i+1)}$ comme le temps d'attent moyen,

$$t_{i(i+1)} = \sum_{k=1}^{\infty} \frac{k}{\mu} \cdot p^{k-1}(1-p) = \frac{1}{\mu(1-p)}$$

Pour $i = 1,2,\cdots,n-1$. Aussi, pour le cas trivial $i = n$, $t_{ii} = t_{nn} = 0$. Donc, avant l'envoie du message $Detectrep$, le temps d'attente pour chaque $Detectreq$ dans le buffer du MP est

$$T_i = \begin{cases} \dfrac{n-i}{\mu(1-p)}, & i = 1,2,\cdots,n-1; \\ 0, & i = n. \end{cases}$$

Et le temps d'attente moyen est

$$t_w = \sum_{i=1}^{n} \frac{1}{n} T_i = \frac{1}{n} \cdot \frac{1}{\mu(1-p)} \cdot \big(1 + 2 + \cdots + (n-1)\big)$$

$$= \frac{1}{n} \cdot \frac{1}{\mu(1-p)} \cdot \frac{n(n-1)}{2}$$

$$= \frac{1}{n} \cdot \frac{n(n-1)}{2\mu(1-p)}$$

$$= \frac{n-1}{2\mu(1-p)}$$

Et le retard de transmission t_r du schéma SDPP au MP dans le statut du nœud récepteur

$t_r = t_v + t_w + t_{decrypt}$

$= \frac{2-\rho}{2\mu(1-\rho)} + \frac{n-1}{2\mu(1-p)} + t_d$, $\rho = \frac{\lambda}{\mu} < 1$

Nous fixons les paramètres n et p, Fig. 5.8 (a,b,c,d,e,f) représente le délai moyen de transmission t_r variant avec le taux moyen d'arrivée λ, où $1 \leq \lambda \leq 100$. Comme on le voit dans cette figure, le retard de transmission t_r augmente avec l'augmentation de λ sur l'ensemble. Aussi, le retard de transmission t_r avec la courbe Cocks-Pinch (CP-80) est inférieur à la courbe Miyaji-Nakabayashi-Takano (MNT-80) et la courbe Barreto-Naehrig (BN-128). Ces résultats indiquent qu'avec le CP-80, le retard de transmission peut être réduit lorsque la performance du dispositif proxy mobile est améliorée. En outre, à partir de la figure. 5.8, nous pouvons également observer à peu près la relation entre t_r et p, n, i.e., avec l'augmentation de p et n, le retard de transmission t_r permettra également d'augmenter.

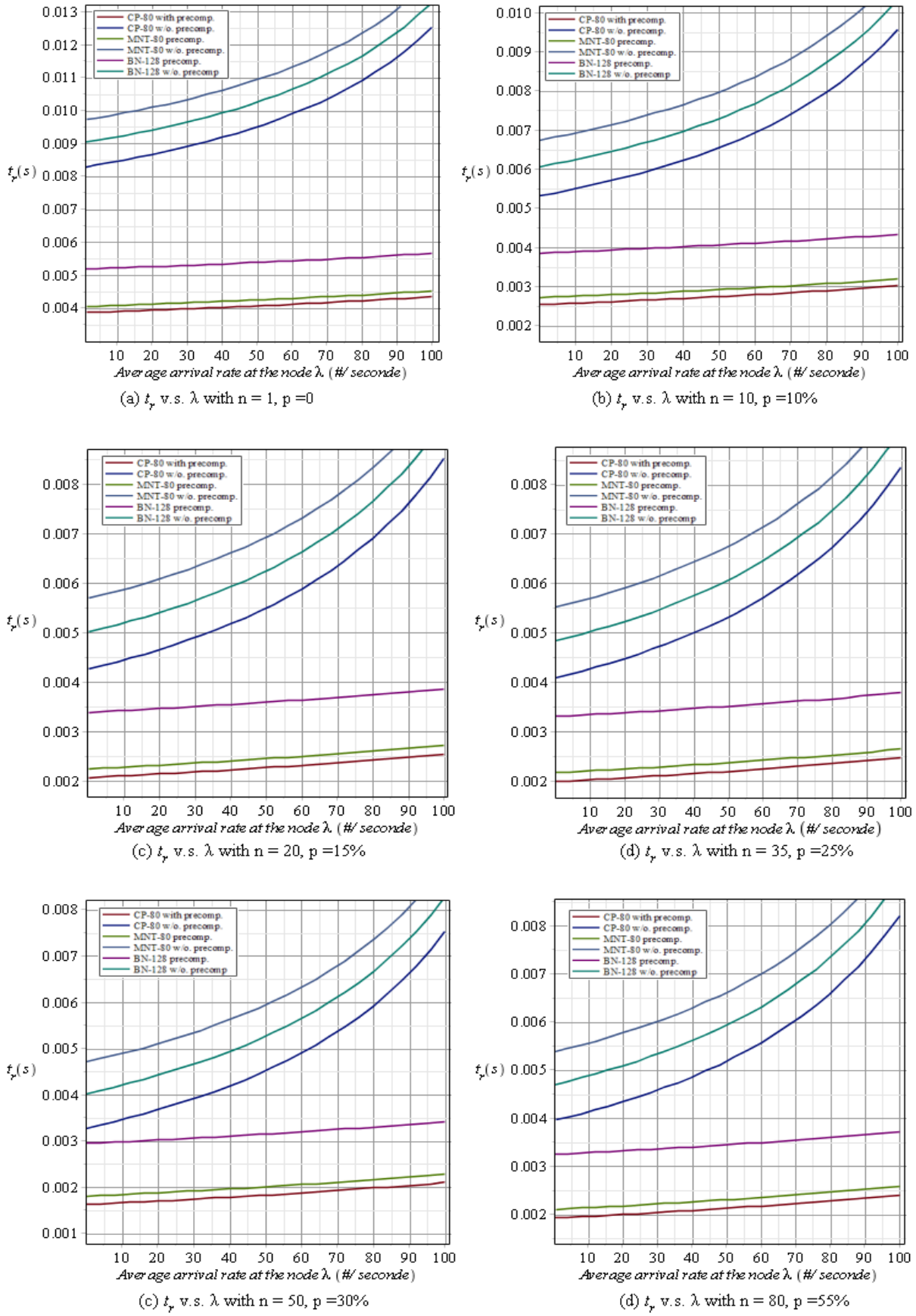
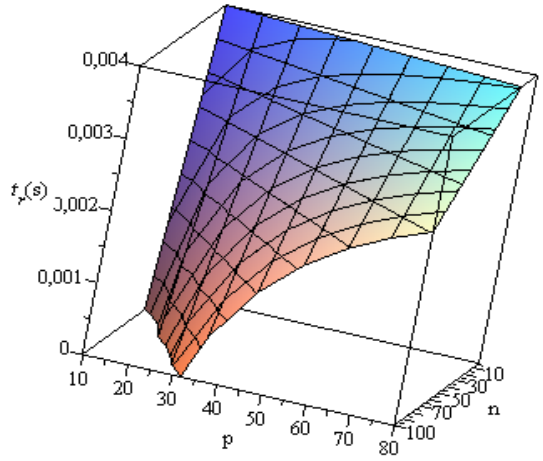
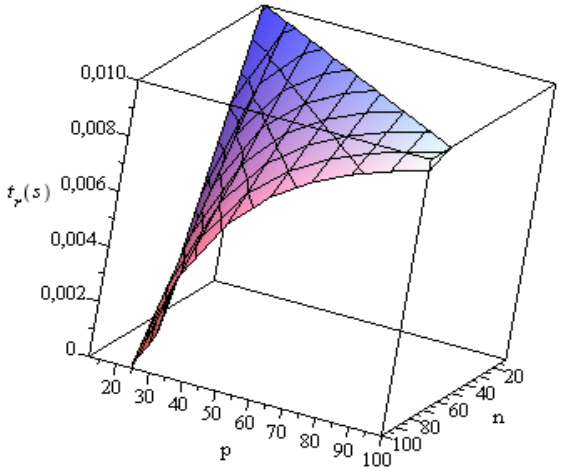


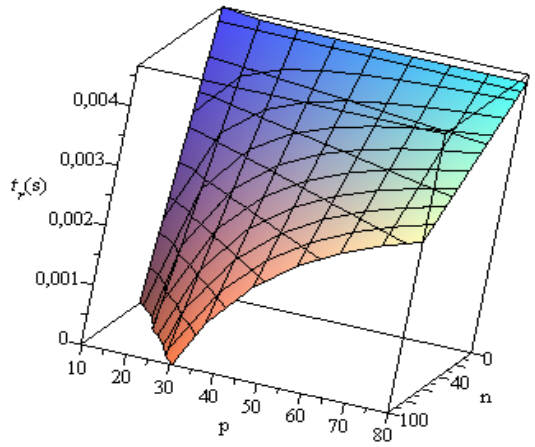
Figure 5:7 Le délai moyen de transmission t_r variant avec le taux moyen d'arrivée λ, où $1 \leq \lambda \leq 100$



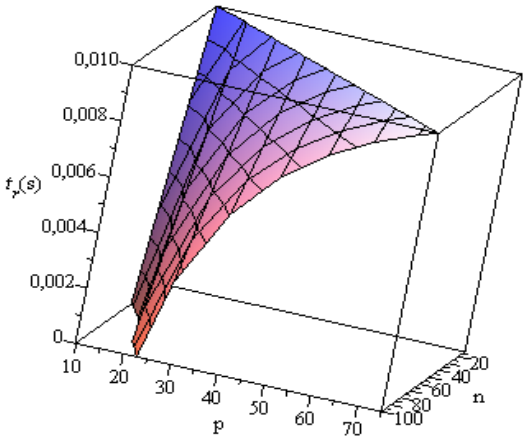
(c) t_r v.s. n and p with λ = 100
with pairing precomput. (CP-80)



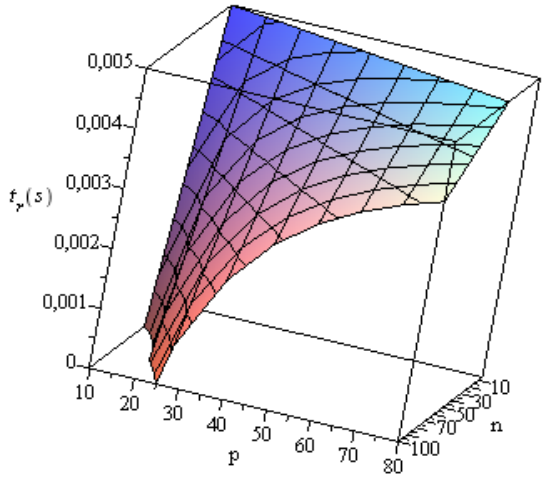
(d) t_r v.s. n and p with λ = 100
w/o pairing precomput. (CP-80)



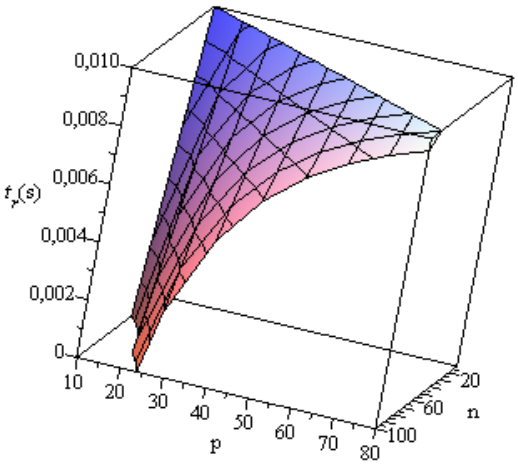
(c) t_r v.s. n and p with λ = 100
with pairing precomput. (MNT-80)



(d) t_r v.s. n and p with λ = 100
w/o pairing precomput. (MNT-80)



(e) t_r v.s. n and p with λ = 100
with pairing precomput. (BN-128)



(f) t_r v.s. n and p with λ = 100
w/o pairing precomput. (BN-128)

Figure 5:8 Le délai moyen de transmission t_r variant avec p et n, où 1% ≤ p ≤ 80% et 1 ≤ n ≤100

5.7 Comparaison avec autres protocoles de sécurisation

Dans cette section, nous comparons notre schéma SDPP [J3] proposé avec les protocoles examinés dans le chapitre 3, i.e, SPRING, SPF, PCS, FLIP et Pi.

Les schémas proposés / Les objectifs de sécurité et de confidentialité	SPRING [62]	SPF [64]	PCS [65]	FLIP [66]	Pi [67]	SDPP [J3]
La préservation de la confidentialité	X	X	X	X	X	X
Optimisation des véhicules DTN	X					
Résister aux attaques liées à la confidentialité sur les nœuds véhicules DTN	X					
La préservation de la confidentialité conditionnelle	X	X				
La protection de la confidentialité de l'emplacement		X	X	X		X
La confidentialité de l'identité			X	X		X
La confidentialité d'intérêt				X		
La stimulation des nœuds DTN égoïstes					X	
La résistance à l'imitateur						X
La résistance au détecteur						X
La détection précoce des attaques de routage						X
La transparence						X
L'authentification et l'intégrité du message						X
La disponibilité des ressources						X

Tableau 5:4 La comparaison de notre schéma SDPP avec d'autres schémas

On peut voir dans le tableau 5.4 que tous les schémas réalisent la préservation de la confidentialité. Le schéma SPRING [62] donne l'optimisation des véhicules DTN, peut résister aux

attaques liées à la vie privée sur les nœuds véhicules DTN, et atteint la préservation conditionnelle de la confidentialité. Le schéma SPF [64] réalise la préservation conditionnelle de la confidentialité et atteint la protection de la confidentialité de l'emplacement. Le schéma PCS [65] atteint la protection de la confidentialité de l'emplacement et la confidentialité de l'identité. Le schéma FLIP [66] atteint les mêmes objectives de sécurité du schéma [65] , et il peut aussi atteindre la confidentialité d'intérêt. Le schéma Pi [67] réalise seulement la stimulation des nœuds DTN égoïstes. Notre schéma SDPP [J3] atteint la protection de la confidentialité de l'emplacement, la confidentialité de l'identité, la résistance à l'imitateur et au détecteur; la détection précoce des attaques de routage, la transparence, l'authentification et l'intégrité du message, ainsi que la disponibilité des ressources.

5.8 Conclusions

Dans ce chapitre, basé sur le chiffrement homomorphique et la technique de certificat d'évolution, nous avons proposé un schéma intelligent de détection (SDPP) avec la protection de la vie privée pour sécuriser le réseau MP2PSN. SDPP peut non seulement satisfaire aux exigences de sécurité et de confidentialité du MP2PSN mais peut aussi détecter, prévenir et informer les attaques élémentaires et les attaques composées. En outre, grâce à l'évaluation de la performance vaste, le SDPP a été démontré qu'il est efficace sous le protocole de routage AODV contre l'attaque du trou noir, également efficace en termes de délai de transmission au proxy mobile.

Chapitre 6 Conclusions et travaux futurs

Dans ce chapitre, nous résumons nos contributions dans cette thèse, et nos travaux futurs de recherche, et enfin nous apportons nos remarques finales.

6.1 Nos contributions

Les principales contributions de cette thèse sont résumées comme suit:

- Premièrement, un nouveau schéma efficace préservant la confidentialité conditionnelle avec la stratégie d'une réponse à la demande, appelé ECPDR, est proposé pour sécuriser les communications ad hoc sociales. Avec le schéma ECPDR proposé, chaque nœud utilisateur peut préserver la vie privée et authentifié avant de rejoindre les autres nœuds en utilisant le protocole de routage. Ce schéma se base sur un schéma de certificat efficace, où le TA délivre la clé privée SK_{n_i} et le certificat $\mathrm{Cert}_{\mathrm{TA},n_i}$ utilisant l'algorithme de signature Schnorr. Le nœud n_i peut vérifier le certificat $\mathrm{Cert}_{\mathrm{TA},n_i}$ par la procédure $S.check$ et il n'utilise pas ce certificat directement dans la communication ad hoc sociale. Basé sur la technologie cryptographique proxy re-signature, le nœud demande la clé de re-signature depuis S_x et puis re-signe les certificats délivrés par le TA. Avec cette méthode de distribution des clés, le schéma garantie la confidentialité de l'identité du nœud. Par conséquent, le ECPDR peut non seulement satisfaire aux exigences de sécurité et de confidentialité des réseaux ad hoc, mais peut aussi détecter, prévenir et informer les attaques élémentaires et les attaques composées. En outre, grâce à la vaste évaluation des performances, le ECPDR a été démontré efficace pour le protocole de routage AODV contre l'attaque du trou noir et efficace en terme de délai de transmission.
- Deuxièmement, pour faire face à des défis en matière de sécurité et de performance dans les réseaux sociaux P2P, un nouveau schéma de détection intelligent et sûr avec une forte préservation de la confidentialité, appelé SDPP, est proposé où nous avons définit la notion d'un réseau P2P social mobile (MP2PSN), qui fournit une plateforme pour les utilisateurs qui ont les mêmes intérêts similaires pour agir comme fournisseurs et consommateurs de ressources. Pour garantir la sécurité du MP2PSN, nous avons proposé un cadre de certification efficace. Pour détecter les attaques de routage, nous avons proposé un système de détection coopératif efficace voisin × voisin (cooperative neighbor × neighbor (CNN)) basé sur deux phases {réponse demandée et réponse à la demande}. Pour atteindre la confidentialité du message, nous avons propo-

sé le chiffrement homomorphique. Enfin, nous avons analysé les propriétés de sécurité du schéma SDPP proposé pour valider sa sécurité dans le modèle de l'oracle aléatoire et avons simulé dans deux scénarios différents. Les résultats de simulation étendus dans le premier scénario montrent que le schéma SDPP proposé peut détecter l'attaque du trou noir plus dans la configuration où l'attaque est lancée sur un certain nombre de plus de saut, et le délai moyen de rapport du Detectreq (DRD) des utilisateurs sociables est évidemment moins que ceux des utilisateurs qui ne sont pas sociables. Ainsi, dans le deuxième scénario, nous sommes concentré sur le délai de transmission du SDPP au proxy mobile avec une évaluation approfondie de la performance, qui conduit en outre vers son aspect pratique.

6.2 Nos travaux futurs de recherche

Avec ces résultats obtenus, nos recherches ont fait des progrès importants dans la sécurisation des réseaux ad hoc sociaux mobiles. Cependant, comme le réseau social est une plateforme prometteuse dans l'environnement de notre vie, il existe encore plusieurs directions de recherche à explorer pour compléter ces travaux. Par conséquent, les deux thèmes de recherche suivants seront étudiés comme une continuation de travail de ma thèse de doctorat.

- *La sécurisation et la confidentialité des réseaux sociaux mobiles utilisant les listes noires* : Dans les réseaux sociaux mobiles, la topologie dynamique élevée et les ressources limitées déployées sur chaque équipement mobile peuvent conduire à des dysfonctionnements de la communication entre les équipements d'une manière temporaire. Donc, ces équipements mobiles ne doivent pas être considérés comme des malicieux, et la révocation immédiate par le gestionnaire de système n'est pas juste envers eux. Alors, si la définition du dysfonctionnement est égale au mauvais déplacement dans un réseau très dynamique, comme MP2PSN, les nœuds valides du P2P peuvent devenir des nœuds malicieux, et finalement le réseau peut s'effondrer. Cependant, comme un de nos futurs travaux, pour les réseaux MP2PSN, nous proposons un nouveau système préservant la sécurité et la confidentialité utilisant les listes noires comme suit :
    - Pour chaque nœud dans le réseau MP2PSN, il maintient une liste noire qui enregistre tous les identifiants des nœuds qu'ils ne peuvent pas communiquer avec succès dans la période précédente. Du point de vue du nœud, les nœuds sur la liste noire sont considérés comme malicieux pour cette période spécifique et il ne sera pas en communication avec eux au cours de cette période.
    - Pour l'administrateur du système, périodiquement, il recueillera les listes noires de tous les nœuds. Si les instants d'apparition sur les différentes listes noires dépassent un seuil prédéfini, l'administrateur du système révoque l'autorité légitime, sinon, le comportement de ce nœud est reconnu comme un dysfonctionnement et l'administrateur du système permettra de clarifier sa validité.
- *La sécurisation et la confidentialité avec un système d'authentification de bande passante pour* le réseau MP2PSN: L'attaque d'injection de données fausses est une grave menace bien connue dans les réseaux sans fils, spécialement pour le réseau MP2PSN,

où un attaquant envoie des rapports faux d'informations afin de gaspiller l'énergie dans les nœuds. En deuxième lieu, nos futurs travaux concerneront les réseaux MP2PSN, où nous étudierons la relation entre la mobilité des utilisateurs, la bande passante, et la vie privée sous l'injection de données fausses afin de proposer un système d'authentification efficace de bande passante pour les réseaux MP2PSN.

6.3 Remarques finales

Dans cette thèse, nous avons présenté une suite de protocole de sécurité et de confidentialité pour sécuriser les communications ad hoc sociaux. En outre, nous avons également identifié deux futurs sujets de recherche pour compléter cette thèse. Nous réaliserons des expériences pour confirmer davantage nos résultats de recherche.

Références

[1] Badache, N., & Lemlouma, T. Le Routage dans les Réseaux Mobiles Ad Hoc. Source : http://opera.inrialpes.fr/people/Tayeb.Lemlouma/Papers/AdHoc_Presentation.pdf (Consulté le 1 juin 2013)

[2] Perkins, C., & Bhagwat, P. (1994). Highly Dynamic Destination Sequenced Distance Vector Routing Protocol (DSDV) for Mobile Computers. *ACM SIGCOMM Computer Communication Review* , 24 (4), 234–244.

[3] Clausen, T., & Jacquet, P. (2003). Optimized link state routing protocol. RFC 3626. IETF.

[4] IETF MANET group. http://datatracker.ietf.org/wg/manet/ (Consulté le 1 juin 2013)

[5] Nafa, M. (2009). *Optimisation des applications de streaming peer to peer pour des réseaux ad hoc mobiles*. France: UNIVERSITÉ D'ÉVRY-VAL-D'ESSONNE.

[6] Optimized link state routing protocol, http://fr.wikipedia.org/wiki/OLSR. (Consulté le 1 juin 2013)

[7] Ayachi, M. A. (2011). *Contributions à la détection des comportements malhonnêtes dans les réseaux ad hoc AODV par analyse de la confiance implicite*. PhD thesis , Université de Rennes 1 / Université 7 Novembre à Carthage.

[8] Ferrag, M. A. (2010). *Sécurisation du protocole de routage OLSR pour les réseaux ad hoc : étude de l'attaque du trou noir* . Thèse de Master, Université Badji Mokhtar Annaba.

[9] Perkins, C., Belding-Royer, E., & Das, S. (2003). Ad hoc On-Demand Distance Vector Routing. http://tools.ietf.org/html/rfc3561. (Consulté le 1 juin 2013)

[10] Johnson, D. (2007). The Dynamic Source Routing Protocol (DSR). http://tools.ietf.org/html/rfc4728. (Consulté le 1 juin 2013)

[11] Zygmunt, J. H., Pearlman, M. R., & Samar, P. (2002). The Zone Routing Protocol (ZRP) for Ad Hoc Networks. Internet-Draft. http ://tools.ietf.org/id/draft-ietf-manet-zone-zrp-04.txt

[12] Haas, Z. J., Pearlman, M. R., & Samar, P. (2002). The intrazone routing protocol (iarp) for ad networks. Internet-Draft. http ://tools.ietf.org/html/draft-ietf-manet-zone-iarp-02. (Consulté le 1 juin 2013)

[13] Haas, Z. J., Pearlman, M. R., & Samar, P. (2002). The interzone routing protocol (ierp) for ad hoc networks. Internet-Draft. http ://tools.ietf.org/html/draft-ietf-manet-zone-ierp-02. (Consulté le 1 juin 2013)

[14] Haas, Z. J., Pearlman, M. R., & Samar, P. (2002). The bordercast resolution protocol (brp) for ad hoc networks. Internet-Draft. http ://tools.ietf.org/html/draft-ietf-manet-zone-brp-02. (Consulté le 1 juin 2013)

[15] Percher, J. M. (2004). *Un modèle de détection d'intrusions distribuée pour les réseaux sans fil Ad hoc*. PhD thesis, L'Université de Versailles Saint Quentin en Yvelines.

[16] Mario, JN. (1999) *Routing Protocol and Medium Access Protocol for Mobile Ad Hoc Networks*. PhD thesis, Polytechnic University, NY, USA.

[17] Batallas, D., & Yassine, A. (2006). Information leaders in product development organizational networks: Social network analysis of the design structure matrix. *IEEE Transactions on Engineering Management*, 53 (4), 570–582.

[18] Opsahl, T., Agneessensb, F., & Skvoretzc, J. (2010). Node centrality in weighted networks: Generalizing degree and shortest path. *Elsevier Social Networks*, 32 (2), 245-251.

[19] Snijders, T., & Borgatti, S. (1999). Non-parametric standard errors and tests for network statistics. *Connections* , 22 (2), 161–170.

[20] Lu, R. (2012). *Security and privacy preservation in vehicular social networks*. PhD thesis, University of Waterloo, Canada.

[21] Freeman, L. C. (1978). Centrality in social networks: conceptual clarification. *Elsevier Social Networks*, 1, 215–239.

[22] Diffie, W., & Hellman, M. (1976). Multiuser cryptographic techniques. *AFIPS National Computer Conference* , 109-112.

[23] Alfred, J., Paul, C., & Scott, A. (1997). *Handbook of Applied Cryptography*. USA: CRC Press.

[24] Jambert, A. (2011). *Outils cryptographiques pour la protection des contenus et de la vie privée des utilisateurs*. PhD thesis, France: Université Bordeaux 1.

[25] Boneh, D., & Franklin, M. (2011). Identity-based encryption from the weil pairing. *Lecture Notes in Computer Science, Advances in Cryptology - CRYPTO 2001*. 2139, pp. 213–229. Springer-Verlag.

[26] Boneh, D., & Boyen, X. (2008). Short signatures without random oracles and the SDH assumption in bilinear groups. *Journal of Cryptology* , 21 (2), 149-177.

[27] Boneh, D., Lynn, B., & Shacham, H. (2004). Short signatures from the weil pairing. *Journal of Cryptology* , 17 (4), 297–319.

[28] Boyen, X., & Waters, B. (2007). Full-domain subgroup hiding and constant-size group. *PKC 2007*, (pp. 1–15).

[29] Liang, X., Cao, Z., Shao, J., & Lin, H. (2007). Short group signature without random oracles. *ICICS*, (pp. 69–82).

[30] Boneh, D., Boyen, X., & Shacham, H. (2004). Short group signatures. *Proceedings of Crypto 2004* (pp. 41–55). LNCS 3152.

[31] Krawczyk, H., & Rabin, T. (2000). Chameleon signatures. *NDSS 2000*. California, USA. http://www.isoc.org/isoc/conferences/ndss/2000/proceedings/042.pdf (Consulté le 1 juin 2013)

[32] Menezes, A. http://math.fau.edu/bkhadka/Syllabi/A%20handbook%20of%20applied%20cryptography.pdf (Consulté le 1 juin 2013)

[33] William, S. (2011). *Cryptography and network security principles and practice*, fifth edition. Prentice Hall.

[34] Bellare, M., Canetti, R., & Krawczyk, H. (1996). Message Authentication using Hash Functions| The HMAC Construction. *RSA Laboratories' CryptoBytes* , 2(1).

[35] Schnorr, C. (1991). Efficient Signature Generation by Smart Cards. *Journal of Cryptology* , 4 (3), 161-174.

[36] Camenisch, J., & Lysyanskaya, A. (2004). Signature Schemes and Anonymous Credentials from Bilinear Maps. *24th Annual International Cryptology Conference* (pp. 56-72). Santa Barbara, California, USA: Springer Berlin Heidelberg.

[37] Goldwasser, S., Micali, S., & Rivest, R. (1988). A digital signature scheme secure against adaptive chosen-message attacks. *SIAM Journal on Computing* , 17 (2), 281–308.

[38] Chaum, D., & van Heyst, E. (1991). Group signatures. *Proceedings of Eurocrypt 1991* (pp. 257–65). Springer-Verlag.

[39] Camenisch, J., & Lysyanskaya, A. (2002). Dynamic accumulators and application to efficient revocation of anonymous credentials. *Proceedings of Crypto 2002* (pp. 61–76). Springer-Verlag.

[40] Ateniese, G., Tsudik, G., & Song, D. (2002). Quasi-efficient revocation of group signatures. *Proceedings of Financial Cryptography 2002*.

[41] Groth, J. (2007). Fully Anonymous Group Signatures Without Random Oracles. *13th International Conference on the Theory and Application of Cryptology and Information Security* (pp. 164-180). Kuching, Malaysia: Springer Berlin Heidelberg.

[42] Bellare, M., Shi, H., & Zhang, C. (2005). Foundations of group signatures: The case of dynamic groups. *The Cryptographers' Track at the RSA Conference 2005* (pp. 136-153). San Francisco, CA, USA: Springer Berlin Heidelberg.

[43] Canard, S., Schoenmakers, B., Stam, M., & Traoré, J. (2006). List signature schemes. *Discrete Applied Mathematics* , 154 (2), 189–201.

[44] Ateniese, G., Camenisch, J., Joye, M., & Tsudik, G. (2000). A Practical and Provably Secure Coalition-Resistant Group Signature Scheme. *Proceedings of 20th Annual International Cryptology Conference* (pp. 255-270). California, USA: Springer Berlin Heidelberg.

[45] Ozturk, C., & Zhang, Y. (2004). Source-location privacy in energy-constrained sensor network routing. *Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks* (pp. 88-93). Washington, USA: ACM New York.

[46] Deng, J., Richard, H., & Shivakant, M. (2006). Decorrelating wireless sensor network traffic to inhibit traffic analysis attacks. *Elsevier Pervasive and Mobile Computing Journal*, 2 (2), 159-186.

[47] Lu, R., Lin, X., Zhu, H., Liang, X., & Shen, X. (2012b). BECAN: a bandwidth-efficient cooperative authentication scheme for filtering injected false data in wireless sensor networks. *IEEE Transactions on Parallel and Distributed Systems*, 23 (1), 32-43.

[48] Lin, X., Lu, R., Shen, X., Nemoto, Y., & Kato, N. (2009). SAGE: a strong privacy-preserving scheme against global eavesdropping for ehealth systems. *IEEE Journal on Selected Areas in Communications*, 27 (4), 365-378.

[49] Liang, X., Li, X., Luan, T., Lu, R., Lin, X., & Shen, X. (2012). Morality-driven data forwarding with privacy preservation in mobile social networks. *IEEE Transactions on Vehicular Technology*, 61 (7), 3209-3221.

[50] Lu, R., Liang, X., Li, X., Lin, X., & Shen, X. (2012a). EPPA: an efficient and privacy-preserving aggregation scheme for secure smart grid communications. *IEEE Transactions on Parallel and Distributed Systems*, 23 (9), 1621-1631.

[51] Brzuska, C., Fischlin, M., Freudenreich, T., Lehmann, A., Page, M., Schelbert, J., et al. (2009). Security of sanitizable signatures revisited. *Proceeding of the 12th International Conference on Practice and Theory in Public Key Cryptography* (pp. 317-336). California: Springer-Verlag Berlin.

[52] Toshiyuki, I., Nguyen, M., & Tanaka, K. (2013). Proxy re-encryption in a stronger security model extended from CT-RSA2012. *Proceedings of The Cryptographers' Track at the RSA Conference* (pp. 277-292). San Francisco,CA, USA: Springer Berlin Heidelberg.

[53] Deng, J., Han, R., & Mishra, S. (2003). Enhancing base station security in wireless sensor networks. CU-CS-951-03: University of Colorado, Department of Computer Science Technical Report.

[54] Jian, Y., Shigang, C., Zhan, Z., & Liang, Z. (2007). Protecting receiver-location privacy in wireless sensor networks. *Proceedings of 26th IEEE International Conference on Computer Communications* (pp. 1955-1963). Anchorage, Alaska, USA: IEEE Computer Society.

[55] Yipin, S., Lu, R., Lin, X., Shen, X., & SU, J. (2010). An efficient pseudonymous authentication scheme with strong privacy preservation for vehicular communications. *IEEE transactions on vehicular technology*, 59 (7), 3589-3603.

[56] Lu, R., Lin, X., Liang, X., & Shen, X. (2012c). A dynamic privacy-preserving key management scheme for location based services in VANETs. *IEEE Transactions on Intelligent Transportation Systems*, 13 (1), 127-139.

[57] Mao, W. (2003). *Modern Cryptography*: Theory and Practice. Prentice Hall.

[58] Information Sciences Institute. http://www.isi.edu/nsnam/ns/

[59] Park, J. H. (2011). Inner-product encryption under standard assumptions. *Springer Designs, Codes and Cryptography* , 58 (3), 235-257.

[60] Scott, M. (2011). On the efficient implementation of pairing-based protocols. *Proceedings of 13th IMA International Conference IMACC* (pp. 296-308). Oxford, UK: Springer Berlin Heidelberg.

[61] Donald, G., John, F. S., James, M. T., & Carl, M. H. (2008). *Fundamentals of queueing theory*. 4th Edition. Wiley.

[62] Lu, R., Lin, X., & Shen, X. (March 2010). SPRING: A social-based privacy-preserving packet forwarding protocol for vehicular delay tolerant networks. *INFOCOM'10* (pp. 1229–1237). San Diego, California, USA: IEEE.

[63] Lu, R., Lin, X., Liang, X., & Shen, X. (2010). Secure provenance: the essential of bread and butter of data forensics in cloud computing. In *ASIACCS*, (pp. 282–292).

[64] Lu, R., Lin, X., Liang, X., & Shen, X. (2010). Sacrificing the plum tree for the peach tree: A socialspot tactic for protecting receiver-location privacy in vanet. In *GLOBECOM*, (pp. 1–5).

[65] Lu, R., Lin, X., Luan, H., Liang, X., & Shen, X. (2012). Pseudonym changing at social spots: An effective strategy for location privacy in vanets. *IEEE Transactions on Vehicular Technology* , 61 (1), 86–96.

[66] Lu, R., Lin, X., Liang, X., & Shen, X. (2010). Flip: An efficient privacy-preserving protocol for finding like-minded vehicles on the road. In *GLOBECOM*, (pp. 1–5).

[67] Lu, R., Lin, X., Zhu, H., Shen, X., & Preiss, B. R. (2010). Pi: a practical incentive protocol for delay tolerant networks. *IEEE transactions on Wireless Communications* , 9 (4), 1483–1493.

[68] Bellare, M., Pointcheval, D., & Rogaway, D. (2000). Authenticated key exchange secure against dictionary attacks. *EUROCRYPT*, (pp. 139–155).

[69] Gentry, C., & Halevi, S. (2011). Implementing Gentry's fully-homomorphic encryption scheme. In *proceedings of the 30th Annual international conference on Theory and applications of cryptographic techniques: advances in cryptology*, (pp. 129-148).

[70] Lu, R., Lin, X., Liang, X., & Shen, X. (2011). A secure handshake scheme with symptoms-matching for mHealthcare social network. *Journal Mobile Networks and Applications - Special issue on Wireless and Personal Communications*, 16 (6), 683-694.

[71] Libert, B. & Quisquater, J. (2004) "The exact security of an identity based signature and its applications," Desponible dans http://eprint. iacr.org/2004/102.pdf.

[72] Azarderakhsh, R., Longa, P., Hu, S., & Jao, D. (2013). Efficient implementation of bilinear pairings on ARM processors. *Springer Selected Areas in Cryptography*, 149-165.

[73] Aranha, D., Karabina, K., Longa, P., Gebotys, C., & López, J. (2011). Faster explicit formulas for computing pairings over ordinary curves. Advances in Cryptology – EUROCRYPT 2011, 6632, 48-68.

[74] Acar, T., Lauter, K., Naehrig, M., & Shumow, D. (2012). Affine pairings on ARM. Pairing-Based Cryptography – Pairing 2012, 7708, 203-209.

Annexe A1. Liste des publications

A.1.1. Revues internationales

[J1] Ferrag, M. A., & Nafa, M. (2011). Securing the OLSR routing protocol for Ad Hoc Networks Detecting and Avoiding Wormhole Attack. *Cyber Journals: Multi-disciplinary Journals in Science and Technology, Journal of Selected Areas in Telecommunications (JSAT)*, April Edition, 2 (4), 51-58. ISSN: 1925-2676.

[J2] Ferrag, M. A., Nafa, M., & Ghanemi, S. (2013). ECPDR: An Efficient Conditional Privacy-Preservation Scheme with Demand Response for Secure Ad hoc Social Communications. *International Journal of Embedded and Real-Time Communication Systems-special issue on Networked Embedded Systems*, 4 (3), 43-71. DOI: 10.4018/ijertcs.2013070103

[J3] Ferrag, M. A., Nafa, M., & Ghanemi, S. (2014). SDPP: An Intelligent Secure Detection Scheme with Strong Privacy-Preserving for Mobile Peer-to-Peer Social Network. *International Journal of Information and Computer Security*, Indersience (1744-1773). Accepté.

A.1.2. Conférences internationals / nationales

[C1] Ferrag, M. A., & Nafa, M. (2011). Un nouveau modèle de mobilité pour les réseaux sociaux totalement mobiles fondé sur la théorie des réseaux sociaux et basé sur "Ontology Profil". *1ers Journées Doctorales du Laboratoire d'Informatique d'Oran*. Oran, Algerie.

[C2] Ferrag, M. A., Nafa, M., & Ghanemi, S. (2012). OlsrBOOK: A Privacy-Preserving Mobile Social Network Leveraging on Securing the OLSR routing protocol. *Proceeding of The 8 th International Scientific Conference eLearning and Software for Education*, (pp. 133-139). Bucharest, Romania.

[C3] Ferrag, M. A., Nafa, M., & Ghanemi, S. (2013). A new security mechanism for ad-hoc on-demand distance vector in mobile ad hoc social networks. *Proceedings of the 7th Workshop on Wireless and Mobile Ad-Hoc Networks (WMAN 2013) in Conjunction with the Conference on Networked Systems NetSys/KIVS*. Stuttgart, Germany: WMAN.

[C4] Ferrag, M. A., Nafa, M., & Ghanemi, S. (2014). ECDF: an efficient-cooperative detection framework with adaptive certificate evolution for secure P2P social communications. (En cours de rédaction)

A.1.3. Livres / Chapitres de livres

[B1] Ferrag, M. A. (2012). *Study of attacks in ad hoc networks*. Germany: LAP LAMBERT Academic Publishing. ISBN-13: 978-3659293672

[B2] Ferrag, M. A., Nafa, M., & Ghanemi, S. (2013). Security and privacy in mobile ad hoc social networks. In D. B. Rawat, B. B. Bista, & G. Yan, *Security, Privacy, Trust, and Resource Management in Mobile and Wireless Communications* (pp. 223-244). USA: IGI Global. DOI: 10.4018/978-1-4666-4691-9, ISBN13: 9781466646919

[B3] Ferrag, M. A., Nafa, M., & Ghanemi, S. (2014). Security and Privacy for Routing Protocols in Mobile Ad hoc Networks. In S. Khan, & J. Mauri, *Security for Multihop Wireless Networks*. USA: CRC Press, Taylo & Francis Group. ISBN : 9781466578036.

Annexe A.2.Glossaire

CA Certificate Authority

CPPA Conditional Privacy-preserving Authentication Technique

DTN Delay Tolerant Network

ECPDR An Efficient Conditional Privacy-Preservation Scheme with Demand Response

FLIP Finding Like-Minded Vehicle Protocol

GPS Global Positioning System

MANET Mobile Ad hoc NETwork

MANET Mobile Ad Hoc Network

MPR MultiPoint Relay

NS-2 Network Simulator 2

OBU On-board Unit

OLSR Optimized Link State Routing protocol

P2P Peer to Peer

P2PSN Mobile Peer-to-Peer Social Network

PCS Pseudonyms Changing at Socialspots Strategy

PKI Public Key Infrastructure

RREP Route REPly

RREQ Route REQuest

RSU Roadside Unit

SDPP An Intelligent Secure Detection Scheme with Strong Privacy-Preserving

SPF Socialspot-based Packet Forward Protocol

SPRING Social-based Privacy-preserving Packet Forwarding Protocol

TA Trust Authority

V-2-I Vehicle-to-Infrastructure Communication

V-2-V Vehicle-to-Vehicle Communication

VANET Vehicular Ad Hoc Network

VSN Vehicular Social Network

WLAN Wireless Local Area Network

WMAN Wireless Metropolitan Area Network

WPAN Wireless Personal Area Network

WWAN Wireless Wide Area Network