الجمـــهوريـــة الجـــزائريـــة الديـمقراطيـــة الشعبيـــة
RÉPUBLIQUE ALGÉRIENNE DÉMOCRATIQUE ET POPULAIRE
وزارة التعـلـيـــم العـالـــي و البـــحث العلـــــمي
MINISTÈRE DE L'ENSEIGNEMENT SUPÉRIEUR ET DE LA RECHERCHE SCIENTIFIQUE
جـــامعـة عمـــار ثليـجي بالأغـــواط
UNIVERSITÉ AMMAR TELIDJI LAGHOUAT

كـلـيـــــة العلـــــوم
FACULTÉ DES SCIENCES
قسم الريـــاضـيات و الإعـــلام الألـــي
DÉPARTEMENT DE MATHEMATIQUE ET INFORMATIQUE

MÉMOIRE DE MASTER

DOMAINE : MATHÉMATIQUES ET INFORMATIQUE **(MI)**
FILIÈRE : INFORMATIQUE
OPTION. : RÉSEAUX, SYSTÈMES ET APPLICATIONS RÉPARTIS **(ReSar)**

Présenté par :
GUIDJELLI FEDWA

Thème :

VERIFICATION DE POSITION DANS LES RESEAUX VANETS

Soutenu publiquement devant le jury composé de :

L.OULEDJDID	Maître-assistant	U. Laghouat (Président)
F. BOUSBAA	Maître-assistant	U. Laghouat (Examinatrice)
N. CHAIB	Maître-assistant	U. Laghouat (Examinateur)
M. YAGOUBI	Maître de Conférences	U. Laghouat (Rapporteur)
K.TAHARI	Maître de Conférences	U. Laghouat (Co-Rapporteur)

ANNÉE UNIVERSITAIRE 2011/2012

Résumé :

Les réseaux ad hoc de véhicules constituent un nouveau type de réseaux issu des réseaux ad hoc mobiles (MANET). La communication peut être entre véhicules ou bien avec une infrastructure.

Les réseaux véhiculaires sont vulnérables aux attaques menaçant la vie des usagers, donc la sécurité de ces réseaux est un pré-requis pour leurs déploiements. Nous avons fait une représentation des réseaux VANETs, comment localisée les nœuds dans ce réseau, comme on s'intéresse par le problème de la sécurité ou la détection des nœuds malicieux dans un réseau VANET on a été représenté les types d'attaque existant pour ce réseaux et nous avons voir les principales approches existantes pour la vérification de position, leurs avantages et leurs inconvénients. Et nous avons choisi deux techniques parmi les techniques présentés et les simuler, l'une est ce base sur la puissance de signal et l'autre de l'authentification.

Abstract:

Vehicular Ad hoc Networks is a new type of network from the mobile Ad hoc networks (MANET). The communication can be between vehicules or with an infrastructure.

Vehicular network are vulnerable to attacks threatening the lives of users and property, therefore the security of these networks is a prerequisite for their deployements. We made a representation of networks VANETs, how localized the nodes in this network, as we are interested in the problem of the security or the detection of malicious nodes in a VANET, we represented the existing types of attacks for this network and we see the main existing approaches for checking position, their advantages and disadvantages. And we choose among the two techniques provide technical and simulating, the one is based on signal strength and the other for authentification.

ملخص:

VANET نظام الشبكات للسيارات هو نوع جديد من شبكات المحمول المخصص (MANET)
ويمكن أن تكون الاتصالات يبن المركبات أو بنية تحتية.

شبكات المركبات VANET هي عرضة لهجمات تهدد حياة المستخدمين و الممتلكات, و بالتالي أمن هذه الشبكات هو شرط أساسي. قمنا بتقديم VANET, و كيفية تحديد العقد في هذه الشبكة, ونحن مهتمون في هذه المشكلة بالأمن أو العقد الخبيثة في شبكة VANET, وقد شرحنا بعض المواضيع المتعلقة بالهجوم في هذه الشبكات, وأظهرنا مزايا و عيوبها. و نختار من بين الطرق المشروحة طريقتين و قمنا بإظهار النتائج, و يستند أحدهم على قوة الإشارة و الأخر على المصادقة.

Remerciement

Je tiens à remercier mon Dieu, le tout puissant, de m'avoir donné la santé, le courage et la patience jusqu'à l'achèvement de ce travail.

Je tiens tout d'abord à exprimer mes sincères remerciements à Mr. Mohamed YAGOUBI et Mr. Abed Elkarim TAHARI pour d'avoir dirigé mon mémoire.

J'exprime ma profonde reconnaissance et mes vifs remerciements à Mr. Nasreddine LAGRAA pour leurs aides sans limite et leurs précieux conseils.

Merci pour les aides permanentes reçues du personnel du laboratoire, de l'informatique et de mathématiques. Je remercie en particulier Melle. Fatima BOUSBAA et Melle. Sarah BENKOUIDER, qui ont été disponibles à chaque fois que j'ai eu besoin d'une aide.

Je remercie les membres de jury qui ont accepté de juger ce travail

Enfin, tous mes remerciements `a tous ceux qui ont contribué de près ou de loin à l'élaboration de ce mémoire, qu'ils trouvent ici l'expression de ma profonde sympathie.

Dédicaces

Je dédie ce travail à tous ceux qui me sont chers...

Mes chers parents pour son amour, son dévouement et l'encouragement durant la rédaction de ce mémoire et tout au long de mes études.

Mes sœurs et mes frères;

Toutes mes amies;

Et à tous ceux que j'aime et qui m'aiment.

Fedwa…

Table des matières

Table des figures

Introduction Générale

Le développement technologique qu'a vu le monde d'aujourd'hui a touché tous les domaines, particulièrement le secteur de la communication qui connaît une évolution considérable par l'apparition de la technologie sans-fil.

Avec l'adoption des technologies de télécommunication sans fil, de nouvelles utilisations et perspectives ont vu le jour. L'évolution rapide de cette technologie a permis la manipulation de l'information à travers des unités de calculs portables (téléphones portables, ordinateurs portables..., etc.). Ces unités ont des caractéristiques particulières (une faible capacité de stockage, une source d'énergie autonome..., etc.) peuvent accéder aux réseaux à travers une interface de communication sans fil.

Les réseaux Ad hoc considéré comme étant une classe de réseaux sans fils, peuvent être utilisés à des endroits où l'installation d'infrastructures est trop couteuse ou impossible. L'une de leurs caractéristiques clés est leur topologie très dynamique, du fait de la mobilité des nœuds du réseau. Ils ont une large gamme d'applications et plusieurs types, dont les réseaux véhiculaires ad hoc (VANets : Vehicular Ad hoc Network).

Les réseaux ad hoc de véhicules (ou VANet) sont perçus par ailleurs comme un bon exemple d'application du concept des réseaux ad hoc. Ils permettent à des véhicules de communiquer entre eux et d'échanger des informations ; Vu l'importance des informations échangées entre les véhicules et l'ouverture de l'environnement VANET, un attaquant peut émettre des messages d'alerte dont le contenu est falsifié, on indique une fausse position, envoyer des fausses informations sur l'état de la route ou empêcher l'acheminement d'un message légitime.

Parmi les solutions proposées pour améliorer la sécurité dans les VANETs est la vérification de la position qui permet de détecter les nœuds malicieux dans les réseaux. Dans ce travail, on étudiera les principales méthodes proposées pour la vérification de position dans les VANETs.

Le reste de ce mémoire est composé de cinq chapitre : le premier chapitre est une introduction aux réseaux VANETs ; le second représente les techniques de localisation des nœuds; le troisième est une vue général des différent types d'attaques existants dans ces réseaux; le quatrième est une conclusion des différentes techniques de vérification de position proposées; et enfin le cinquième chapitre qui représente l'analyse des résultats de simulation effectues ; et on terminera le mémoire par une conclusion.

Introduction aux réseaux ad hoc de véhicules (VANET)

1.1 Introduction:

Les réseaux ont connu dans les 3 dernières décennies un essor fulgurant marqué en particulier par la généralisation des communications sans fil. Le succès de ces communications, porté dans un premier temps par la transmission séparée de la voix et des données, puis dans un second temps par toute la panoplie des applications multimédias, a été tel qu'en l'espace de peine une décennie, le nombre de terminaux sans fil dans le monde a plus que supplanté le nombre de terminaux fixes [TCH08].

On peut classifier les réseaux sans fils selon l'architecture en trois grandes familles que sont: les architectures de réseaux à infrastructure dans lesquelles les terminaux communiquent obligatoirement par l'intermédiaire d'un nœud fixe relié au réseau filaire, les architectures de réseaux ad-hoc dans lesquelles les terminaux communiquent directement entre eux ou indirectement par l'intermédiaire d'autres terminaux, et les architectures hybrides ou ad-hoc hybrides qui sont la résultante de la combinaison des deux premières familles d'architectures [TCH08].

Il est attendu que les réseaux véhiculaires soient déployés dans des configurations ou combinaisons de configurations mêlant réseaux à infrastructure, réseaux ad-hoc et réseaux hybrides.

Dans ce chapitre, on représente les réseaux VANETS, ses caractéristiques, ses applications, et ses architectures.

1.2 Les réseaux VANETS:

Ces dernières années, les réseaux MANETS (Mobile Ad hoc Network) ont eu un grand intérêt de la part des chercheurs, que ce soit du milieu industriel ou académique. Ces réseaux qui étaient initialement proposés pour l'utilisation dans les domaines militaires, aujourd'hui montrent de plus en plus de potentielle pour les applications civiles. Un réseau MANET est un ensemble de nœuds interconnectés entre eux par le moyen de communication radio. Ces réseaux sont d'une nature totalement distribuée et totalement dynamique, dans lesquels chaque nœud doit être capable de s'auto-configurer sans la nécessité d'aucune gestion centralisée, ni d'aucune infrastructure préalablement déployée. [LSK06]

Des réseaux semblables aux réseaux MANETS sont nés pour donner un champ d'application plus large et plus important dans notre quotidien. Ces nouveaux réseaux sont les réseaux VANETs pour (vehicular ad hoc network).

Les réseaux Vehicular Ad hoc Network (VANET) facilitent la communication entre véhicules et entre eux et les infrastructures (cf. fig 1.1) et peuvent aussi améliorer la sécurité routière. Ces réseaux, malgré qu'ils se dérivent des réseaux MANETS, ils ont leurs propres caractéristiques.

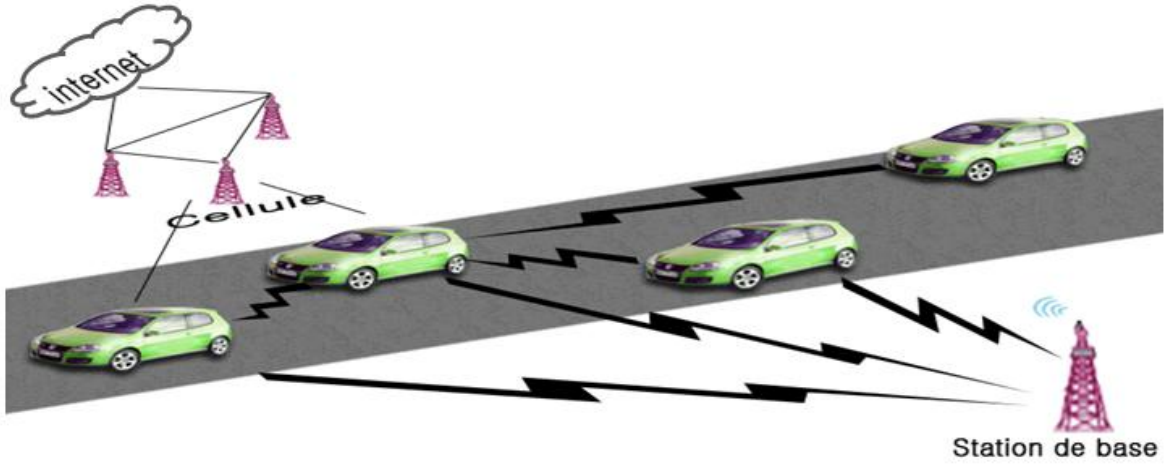


Fig. 1.1 Exemple d'un réseau VANET

1.2.1 Types de communication dans les VANETS :

Dans ces réseaux de véhicules, les services proposés permettent de distinguer plusieurs communications possibles, comme vous pouvez le constater sur la figure 1.2

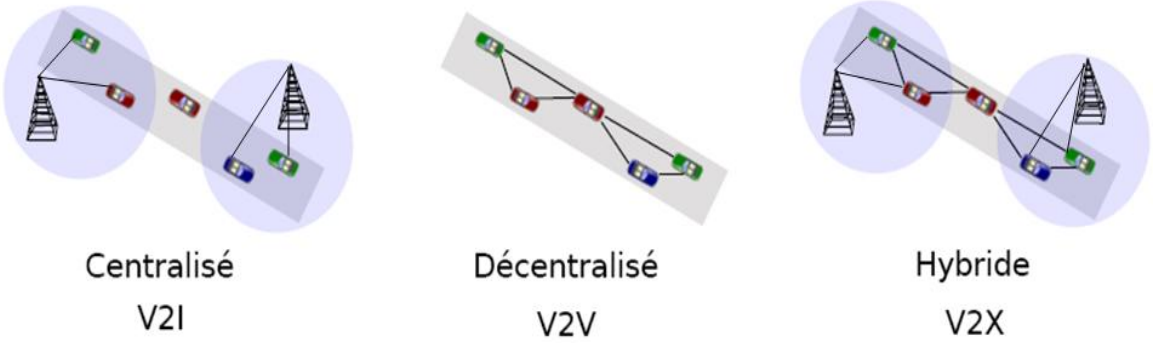


Fig. 1.1 Types de communication dans un réseau de véhicules

- **Communications de Véhicule à Véhicule (V2V):**

Les services et les applications qui sont basées sur la simple communication inter-véhicule et n'impliquant pas d'infrastructure fonctionnent seulement dans le cas où un taux de pénétration suffisant de véhicules équipés des composants et interfaces nécessaire avoir été

atteint. En raison des longs cycles de vie des véhicules, un taux de pénétration approprié peut seulement être atteint après plusieurs années, même si toutes les voitures nouvellement produites ont été équipées en juste proportion. C'est pourquoi, les constructeurs automobiles doivent penser aux stratégies d'introduction graduelles du marché. [BEN09]

- **Communications de Véhicule à Infrastructure (V2I):**

Nous ne nous concentrons pas donc seulement sur des simples systèmes de communications inter-véhicules, mais prenons aussi en compte des applications qui utilisent des unités installées au bord de la route (road side units ou RSUs). Ceux-ci démultiplient les services grâce à des portails Internet communs. [BEN09]

Des services à base d'infrastructure (accès à Internet, échange de données par exemple de voiture à domestique, communications de voiture à parking pour le diagnostic distant, ...) profitent aux clients et peuvent motiver des conducteurs à investir dans l'équipement sans fil supplémentaire pour leurs véhicules.

- **Communications hybrides :**

La combinaison de ces deux types de communications permet d'obtenir une communication hybride très intéressante. En effet, les portées des infrastructures étant limitées, l'utilisation de véhicules comme relais permet d'étendre cette distance. Dans un but économique en évitant de multiplier les bornes à chaque coin de rue, l'utilisation de sauts par véhicules intermédiaires prend toute son importance.

1.2.2 Caractéristiques des réseaux VANETS :

Les réseaux véhiculaires se distinguent des réseaux sans fil traditionnels par un certain nombre de caractéristiques spécifiques dont on peut citer:

- **Le potentiel énergétique et la capacité de calcule:** À la différence des réseaux sans fil traditionnels où la contrainte d'énergie représente un facteur limitant important, les entités des réseaux véhiculaires disposent de grandes capacités énergétiques qu'elles tirent du système d'alimentation des véhicules. Même en cas d'arrêt du moteur et donc d'arrêt du système d'alimentation, il est toujours possible pour une plateforme embarquée de recourir à l'important dispositif de batteries dont seul un véhicule du fait de sa taille, peut disposer. La plate forme embarquée dans les véhicules étant pleinement alimentées, elles peuvent,

tout aussi pleinement, tirer parti de capacités de calcul plus massives et de multiples interfaces de communication. [TCH08]

- **L'environnement de communication et le modèle de mobilité**: Alors que les environnements de communications dans les réseaux sans fil traditionnels se résument généralement à des espaces complètement ouverts et sans obstacles ou à des espaces clos en intérieur, les réseaux véhiculaires imposent la prise en compte d'une plus grande diversité environnementale. Du fait de la mobilité des véhicules, il est en effet possible de passer d'un environnement urbain caractérisé par de nombreux obstacles à la propagation des signaux, à un environnement périurbain ou autoroutier présentant des caractéristiques différentes. En plus de cette diversité environnementale, les réseaux véhiculaires se distinguent également des réseaux sans fil ordinaires par un modèle de mobilité dont une des traductions les plus évidentes est l'importante vitesse des nœuds qui réduit considérablement les durées de temps pendant lesquelles les nœuds peuvent communiquer [HKL10].
- **Le modèle de communication:** Les réseaux véhiculaires ont été imaginés principalement pour les applications liées à la sécurité routière (exemple. diffusion de messages d'alerte). Dans ce type d'application, les communications se font presque exclusivement par relayages successifs d'une source vers une multiplicité de destinataires. Le modèle de transmission en Broadcast ou en Multicast est donc appelé à dominer largement dans les réseaux véhiculaires, ce qui n'est par exemple pas sans conséquence sur la charge du réseau et le modèle de sécurité à mettre en œuvre [TCH08].
- **La taille du réseau:** Étant donné les avancées importantes réalisées dans le domaine des communications sans fil et les bas coûts des équipements associés, les véhicules qui intègrent déjà massivement des systèmes GPS et des équipements Bluetooth, seront très probablement équipés et ce tout aussi massivement de plate forme de communication leur permettant de constituer de véritables réseaux. Ce faisant, et compte tenu de l'importance sans cesse grandissante de la densité et du parc des véhicules, on peut s'attendre à ce que la taille des réseaux véhiculaires dont les déploiements restent encore très confidentiels, soit d'une tout autre ampleur [TCH08].

1.2.3 Application des VANETS:

Selon l'U.S Département de Transportation (U.S DOT), en 2005, plus de 43.000 personnes ont été tuées et plus de 2,6 millions ont été blessés dans des accidents de voiture aux États-

Unis. Le nombre élevé de décès et de blessures coûtent des milliards de dollars en soins de santé, plus que tout autre type de blessure ou de maladie. Ces questions font de la sécurité routière une préoccupation majeure pour les organismes gouvernementaux et les constructeurs automobiles, ainsi que des chercheurs dans des domaines connexes [GKC07].

On peut classifier les applications dans les réseaux VANETS en deux catégories une selon leurs nature (sécurité ou commerciale) ou bien selon leurs exigence à la localisation des nœuds qui est représenté dans la figure 1.3:

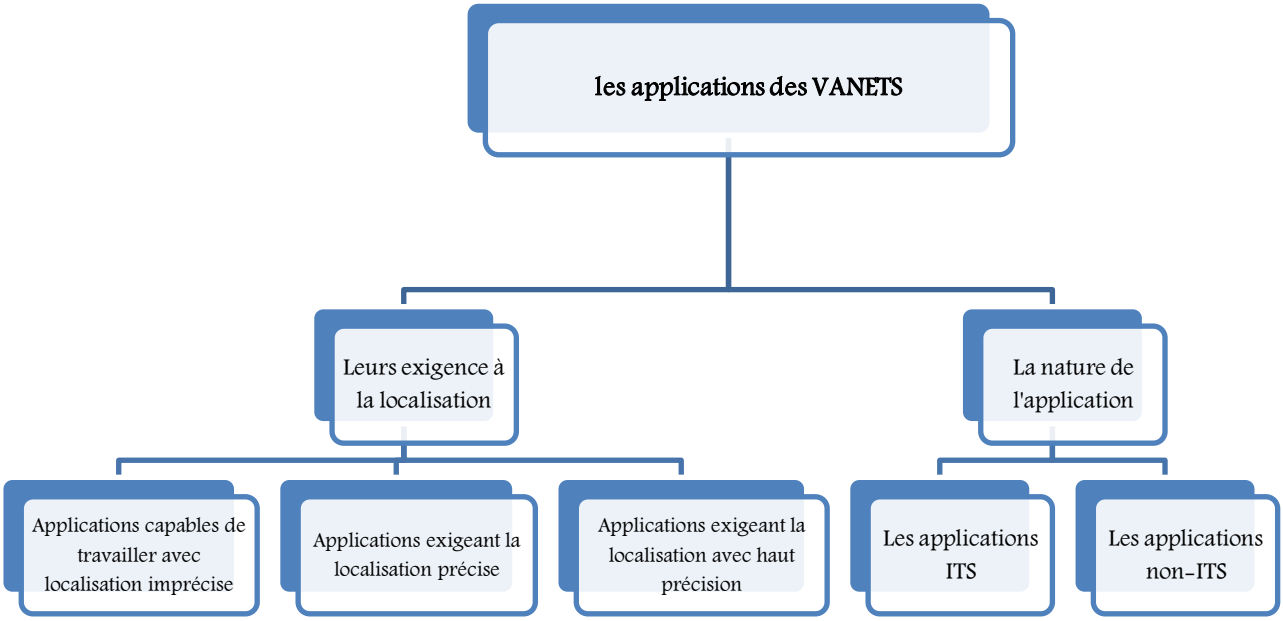


Fig. 1.2 Classification des applications dans VANET

a) La première classification:

Il est attendu que les réseaux véhiculaires soient l'instrument de la fourniture d'une très grande variété d'applications au rang desquelles on peut citer les alertes (accident, de ralentissement, de déviation, de travaux, d'intempéries), la conduite coopérative, la surveillance de l'état des véhicules, la localisation des véhicules, la gestion de flotte de véhicules, la messagerie instantanée, les jeux en réseau, l'accès Internet, les paiements automatiques, etc. On répertorie ces applications suivant 2 grandes classes à savoir:

- **Les applications ITS (Intelligent Transportation System) :** Ce sont des applications liées à la sécurité routières (i.e. des applications impactant directement la sécurité des personnes et des biens) et visant à bâtir un système de transport

intelligent. En d'autres termes, l'objectif ultime de ces applications est de réduire l'accidentologie routière et d'améliorer les conditions de circulation. Ces applications ont constitué dans les différents travaux de recherche et projets gouvernementaux menés à travers le monde, le fondement premier du concept de réseau véhiculaire. Du point de vue du modèle de communication (cf. Fig. 1.4).

- **Les applications non-ITS:** Ce sont des applications commerciales, de confort, de divertissement ou plus généralement toutes les autres applications ne faisant pas partie de la catégorie des applications ITS. Si ces applications ont émergées conceptuellement à la suite des applications ITS, leur mise en œuvre concrète a en revanche pris le pas sur les premières. Cette avance est principalement due à la préexistence d'un certain nombre d'infrastructures sur lesquelles ces applications sont déployées et à leur potentiel commercial beaucoup plus important (cf. Fig. 1.4).

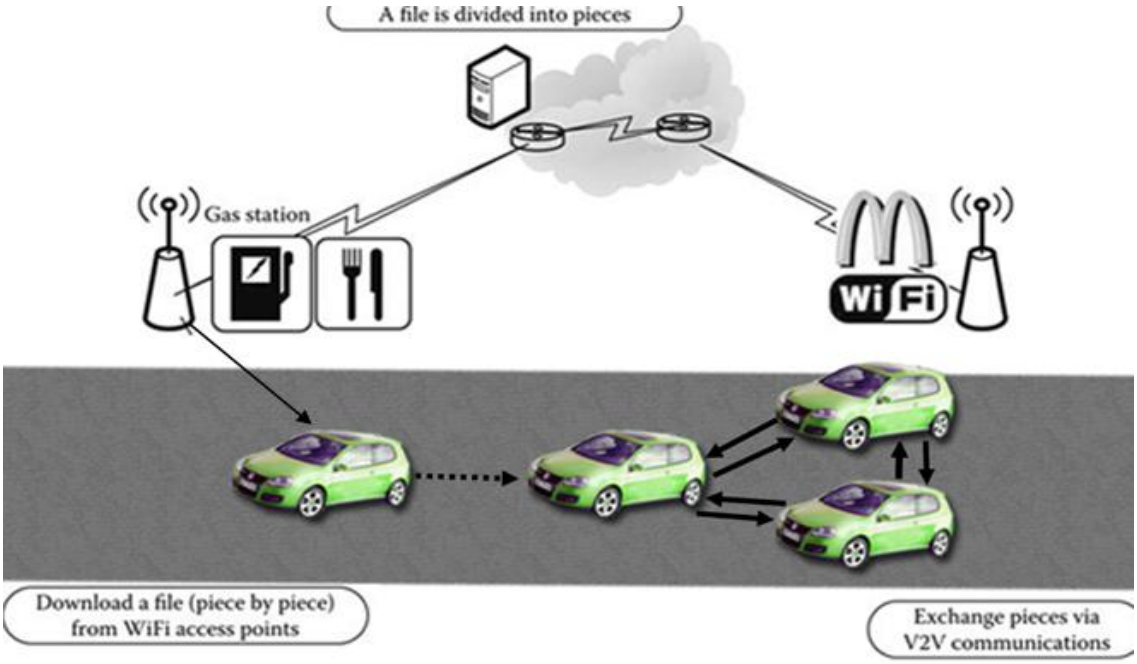


Fig. 1.3 Exemple des applications de VANETS

b) La deuxième classification

On s'intéresse dans notre projet par la position des nœuds dans VANET; alors on peut aussi trouver une classification des applications de VANETS selon leurs exigences à la localisation des nœuds (la précision des positions) qu'est divisé en trois groupes principaux selon leurs exigences de localisation.

- **Applications capables de travailler avec localisation imprécise:** La plupart de ces applications sont liées à la communication de véhicules, qui inclut la communication

de véhicule à véhicule (V2V) et de véhicule à infrastructure (V2I), et fournissent des services comme l'acheminement d'informations et la dissémination de données d'accidents, etc. [BEN09].

- **Applications exigeant la localisation précise:** Les applications dans ce groupe sont habituellement des applications de conduite coopérative, où les véhicules échangent des messages entre eux pour conduire et partager en collaboration l'espace disponible sur la route [BEN09].
- **Applications exigeant la localisation avec haute précision**: La plupart de ces applications sont des applications critiques de sécurité comme les systèmes d'avertissement de collision de véhicule (Collision Warning Systems CWS) et d'autres applications d'aide au conducteur.

Conclusion

Comme nous avons vu dans les réseaux VANETS, les nœuds (véhicules) peuvent communiquer entre eux et avec des infrastructures. VANET peut assurer une meilleure sécurité des conducteurs, prévenir des dangers de la route (ex.: Accidents; Anticipation du trafic (fluidité), prévention d'un véhicule prioritaire; et anticipation d'un danger quelconque..).

On s'intéresse dans notre travail à la sécurité dans les VANETS; qui est un domain de recherche dans VANETS; et les applications de sécurité dépendent de délai des informations de position fiable. Alors, on peut remarquer que la position joue un rôle très important dans la sécurité des réseaux VANETs.

Pour cela, on va voir dans le deuxième chapitre les différentes techniques de localisation utilisées dans les VANETS. Car dans ce projet on va étudier la vérification des positions données pour améliorer la sécurité dans les VANETS.

Chapitre 2

Localisation des nœuds dans les réseaux VANETS

2.1 Introduction:

Les Communications entre les véhicules constituent un réseau Ad hoc de véhicules (VANET). Contrairement à MANET, dans un VANET, les nœuds qui sont des véhicules peuvent se déplacer avec une vitesse élevée et généralement doivent communiquer rapidement et sûrement.

La localisation est un des problèmes fondamentaux de la robotique mobiles et de la navigation des véhicules routiers. Le problème de la localisation de véhicules routiers consiste à répondre à la question "*Où suis-je?*" du point de vue d'un véhicule. Le terme "*localisation*" signifie donc, la connaissance de la pose du véhicule dans un référentiel connu, c'est-à-dire sa position et son orientation par rapport à son environnement.

Dans ce chapitre, nous présentons les méthodes de localisation et les différentes techniques de localisation dans les réseaux sans fils appliquées aux VANETS.

2.2 Les techniques utilisées pour la localisation:

2.2.1 Trilatération:

La trilatération est une méthode mathématique permettant de déterminer la position relative d'un point en utilisant la géométrie des triangles tout comme la triangulation. Mais contrairement à cette dernière qui utilise les angles et les distances pour positionner un point, la trilatération utilise uniquement les distances [CAP08].

En se basent sur la figure 2.1. En connaissant la distance d_1 par rapport au point de référence B_1, on déduit que l'objet cherché se trouve sur le cercle de rayon d_1. En ajoutant d_2, la distance par rapport au point B_2, la position cherchée se réduit à deux points M et M'. Finalement, en ajoutant la distance d_3 par rapport au point B_3, la seule localisation possible de l'objet reste le point M.

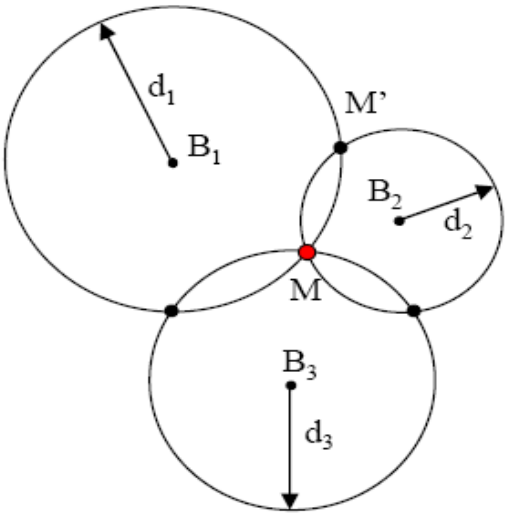


Fig.2.1 Principe de Trilatération

En raison des limitations des récepteurs GPS, ces derniers ne sont utilisés que dans les applications VANET qui n'exigent pas l'information précise et fiable.

2.2.2 Technique basée sur la puissance des signaux reçus

C'est l'une des techniques traditionnelles qui se base sur l'estimation de la distance entre le mobile et les stations de base à partir de la puissance du signal direct reçu du mobile par les stations de base.

En effet, la puissance du signal direct reçu par un récepteur est fonction de la distance *d* séparant l'émetteur et le récepteur. Elle est donnée par la formule suivante [WAS05]:

$$P_r(d)[dBm] = P_t[dBm] - Pe(d)[dB] + G_t[dB] + G_r[dB]$$

Où Pt est la puissance du signal émis, Pe(d) est l'atténuation du milieu en fonction de la distance d, G_t et G_r sont les gains respectifs des antennes de l'émetteur et du récepteur par rapport à une antenne isotrope. L'atténuation du milieu Pe, fonction aussi de la distance d, [WAS05]:

$$Pe(d)[dB] = \overline{Pe}(d_0)[dB] + 10n\log\left(\frac{d}{d_0}\right) + X_\sigma[dB]$$

Où Pe(d_0) représente la moyenne de l'atténuation à une distance de référence d_0 , n le coefficient d'atténuation du milieu considéré et X_σ est une variable aléatoire Gaussienne (en dB) de valeur moyenne nulle et d'écart-type σ . Le coefficient n indique le taux d'atténuation

en fonction de la distance et X_σ représente la variation aléatoire de l'atténuation autour de la moyenne.

En résumé, la puissance du signal du mobile reçu est donnée par la relation suivante [WAS05]:

$$P_r(d)[dBm] = P_t[dBm] - \overline{Pe}(d_0)[dB] - 10n\log\left(\frac{d}{d_0}\right) - X_\sigma[dB] + G_t[dB] + G_r[dB]$$

Les paramètres n et σ sont spécifiques à chaque milieu et peuvent varier lorsque des modifications sont apportées à ce milieu.

Si plusieurs stations se trouvent à la portée de transmission, il est alors possible d'utiliser une méthode de multilatération pour estimer la position de l'objet. Précisément, Comme illustré dans la figure 2.2, nous obtenons ainsi *n* cercles de rayon R_1, R_2, ..., R_n qui correspondent à la distance d_i $(i=1..n)$ et ayant comme centre la station de base T_i dont les coordonnées sont (X_i, Y_i). Dans un plan orthonormé, on en déduit que la position de l'objet X_p et Y_p est donnée par les équations linéaires ci-dessus.

$$(X_p - X_1)^2 + (Y_p - Y_1)^2 = R_1^2$$
$$(X_p - X_2)^2 + (Y_p - Y_2)^2 = R_2^2$$
$$\dots$$
$$(X_p - X_n)^2 + (Y_p - Y_n)^2 = R_n^2$$

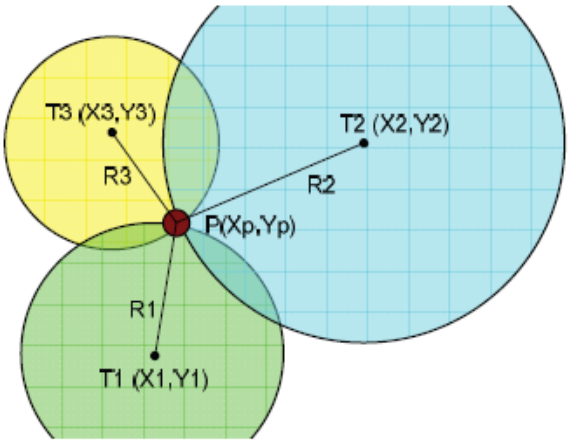


Fig. 2.2 Principe de multilatération

2.2.3 Technique basée sur le temps d'arrivée des signaux reçus:

Les ondes électromagnétiques voyagent à une vitesse constante dans l'espace libre (vitesse de la lumière c ≈ 3×10^8 m/s). On peut donc facilement connaître la distance d séparant un émetteur d'un récepteur en connaissant le temps t mis par le signal direct pour arriver de l'émetteur au récepteur par l'expression suivante [WAS05] :

$$d=c*t$$

Tout comme la technique de localisation basée sur la puissance des signaux reçus, cette technique utilise une simple triangulation avec un minimum de 3 stations de base pour déterminer la position du mobile. L'illustration de cette technique est la même que celle faite sur la figure 2.2**.**

Pour connaître le temps exact d'arrivée du signal aux stations de base, il faut que ces dernières soient parfaitement synchronisées entre elles et avec le mobile afin de connaître le temps exact de transmission du signal par le mobile. Un défaut de synchronisation conduit à des erreurs dans l'estimation du temps pris par le signal direct pour arriver aux stations de base, et donc à des erreurs de localisation importantes.

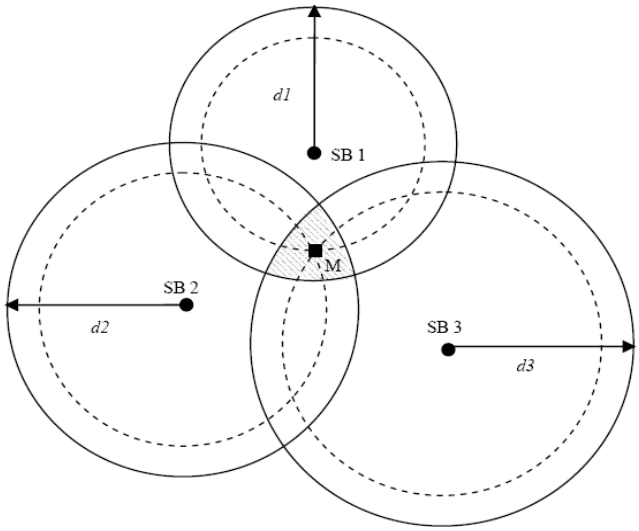


Fig. 2.3 Technique de radiolocalisation basée sur la puissance du signal reçu

2.2.4 Technique basée sur la différence des temps d'arrivée des signaux reçus:

Une variante de la technique décrite précédemment à la section 2.2.3 est celle basée sur la différence des temps d'arrivée des signaux reçus. Elle vise à éviter la synchronisation entre le mobile et les stations de base. Des paires de stations de base synchronisées entre elles sont utilisées. La différence du temps d'arrivée du signal émis par le mobile à chaque paire de stations de base est mesurée. Dans un espace à 2 dimensions, l'ensemble des positions possible du mobile pour avoir une même différence de temps d'arrivée (donc une différence constante en valeur absolue entre les distances séparant le mobile des deux stations car la vitesse du signal est identique) à une paire de stations de base donnée est une hyperbole dont l'équation est donnée par l'expression suivante [WAS05]:

$$\frac{x^2}{a^2} - \frac{y^2}{b^2} = 1$$

Où **x** et **y** sont les coordonnées du mobile et les constantes **a** et **b** sont des constantes liées aux distances séparant le mobile des deux stations de base. C'est la raison pour laquelle cette technique est aussi appelée technique hyperbolique de radiolocalisation. Une simple triangulation faite avec au moins trois paires de stations de base (SB) est nécessaire à la localisation du mobile. Tout comme les autres techniques, des erreurs et des incertitudes sur les mesures de la différence des temps d'arrivée font que l'on obtient, au lieu de la position exacte du mobile, une région d'incertitude où se trouve le mobile. Cette technique est illustrée sur la figure 2.4.

Les hyperboles en pointillé sont celles qui auraient été obtenues si tous les temps d'arrivée avaient été mesurés avec exactitude. Leur intersection donne la position exacte du mobile (M). Mais comme des erreurs sont presque toujours faites, la technique basée sur la différence des temps d'arrivée des signaux reçus, tout comme les autres techniques décrites ci-haut, situe le mobile plutôt dans une région hachurée comme montré sur la figure 2.4.

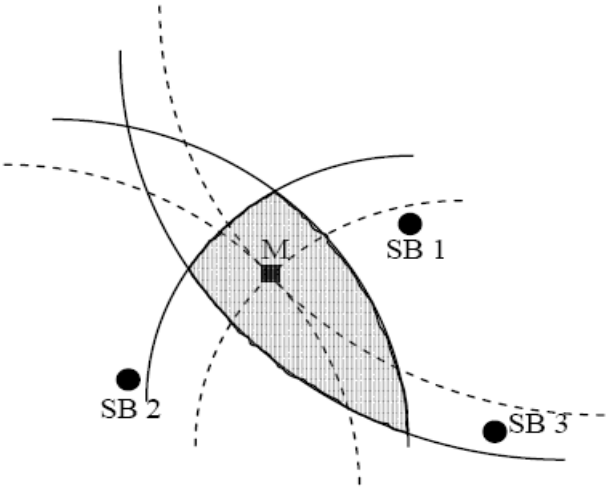


Fig. 2.4 Technique de localisation basée sur la différence des temps d'arrivée des signaux des trajets directs reçus

2.2.5 Technique basée sur l'angle d'arrivée des signaux reçus :

Une autre technique traditionnelle utilise des antennes directionnelles ou encore un réseau d'antennes aux stations de base pour mesurer la direction d'arrivée du signal provenant du trajet direct, émis par le mobile. En utilisant une simple triangulation, deux stations de base suffisent pour localiser le mobile. Cette technique est illustrée sur la figure 2.4. Les directions en pointillé sont les directions réelles du trajet direct qui font respectivement un angle de $\alpha_1$et

α_2 par rapport à un axe prédéfini aux stations de bases SB1 et SB2. Leur intersection donne la position exacte du mobile [WAS05].

Mais, puisque les antennes de réception disposent d'une marge d'erreur s ±θ, alors chaque station de base localise le mobile plutôt dans un faisceau équivalent à la direction mesurée plus ou moins la marge d'erreur. Le mobile se trouve ainsi dans la région hachurée formée par l'intersection des deux faisceaux. D'autres techniques statistiques de positionnement directes ou itératives sont utilisées pour déterminer plus précisément le mobile dans cette région.

On remarque que plus le mobile est éloigné des stations de base, plus grande est la zone d'intersection. La précision de cette technique se dégrade donc au fur et à mesure que le mobile s'éloigne des stations de base. On remarque aussi que lorsque le mobile se trouve sur la droite reliant les deux stations de base, il devient difficile de détecter la position du mobile. Pour ces raisons, plus de deux stations de base sont généralement utilisées pour augmenter la précision de cette technique [EVE07].

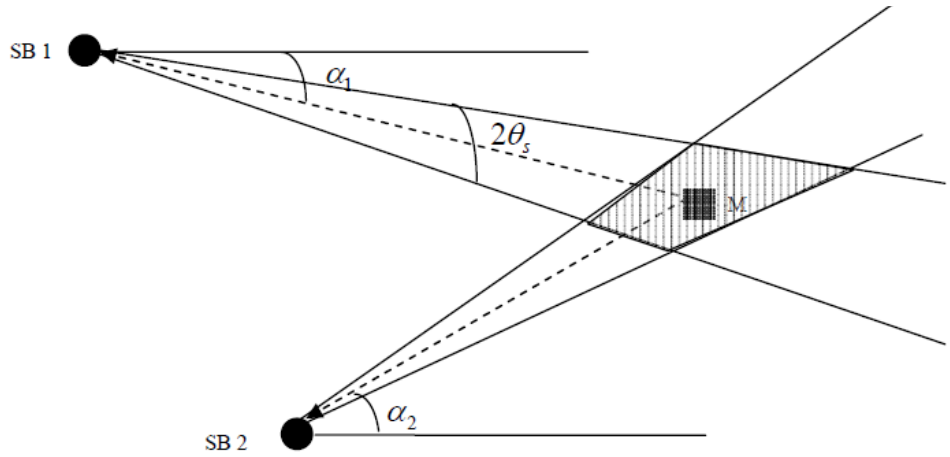


Fig. 2.5 Technique de radiolocalisation basée sur l'angle d'arrivée des signaux des trajets directs

2.3 Les techniques de localisation:

Les techniques proposées pour localiser les nœuds mobiles sont présentés dans cette partie. La plupart des techniques décrites ci-dessus sont appliquées facilement pour localiser les nœuds dans les réseaux VANETS.

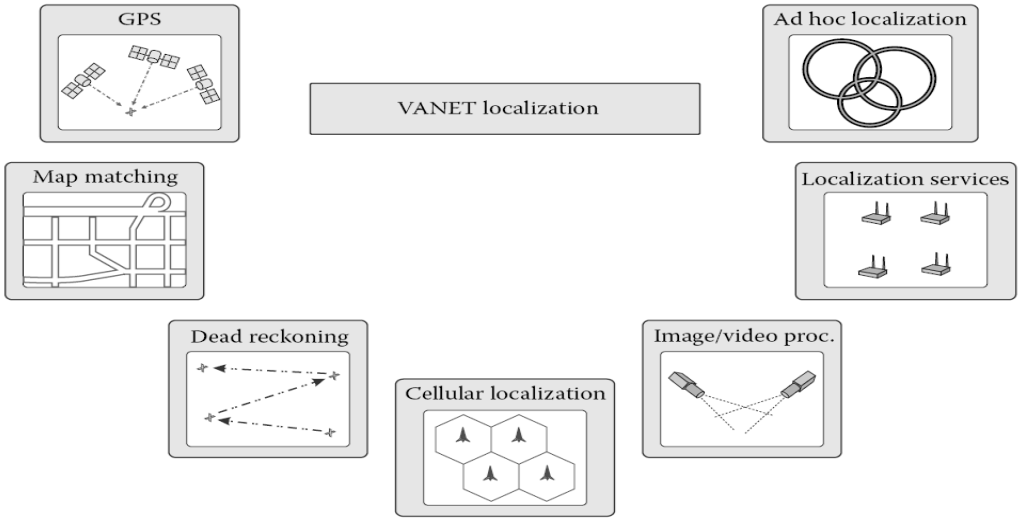


Fig. 2.6 Techniques de localisation appliquées dans VANET

2.3.1 Le Système de Positionnement Global (GPS)

Le système GPS est l'un des systèmes de radiolocalisation les plus connus mondialement. Il a été conçu au début des années 1970 par le Département de la défense des États-Unis. Son entretien est également assuré par ce dernier. Ce système comprend 24 satellites qui gravitent autour de la terre à une altitude d'environ 20200 km et qui assurent une couverture mondiale (cf. Fig. 2.6) [CER93].

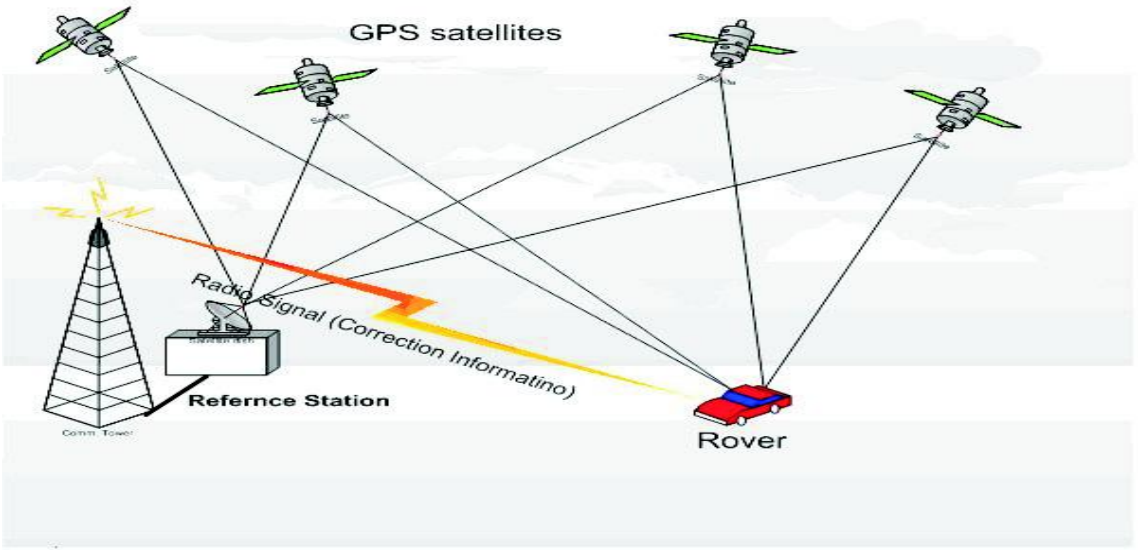


Fig. 2.7 Les différents services de GPS

Un récepteur GPS est nécessaire au niveau du mobile pour connaître sa position. La technique de radiolocalisation utilisée est celle basée sur le temps d'arrivée des signaux reçus. Chaque satellite transmet au récepteur GPS un signal contenant un code qui lui est propre.

Une réplique de ce code est générée simultanément (en même temps qu'au satellite) par le récepteur. Le temps mis par le signal pour aller du satellite au récepteur GPS est normalement égal au décalage temporel que doit subir la réplique du code générée au niveau du récepteur pour coïncider avec le code réel reçu dans le signal. Mais en réalité, puisque les horloges du récepteur GPS et du satellite ne sont pas parfaitement synchronisées, une erreur est commise sur le temps de propagation du signal trouvé. L'erreur se produit parce que, entre autres facteurs, les horloges de récepteurs ne sont pas aussi précises que les horloges atomiques des satellites. Il serait beaucoup trop cher d'installer les horloges atomiques dans les récepteurs. Puisqu'il n y a que 24 satellites GPS, l'installation d'horloges atomiques dans les satellites est faisable. Puisqu'il faut multiplier le temps de propagation par la vitesse de la lumière (c = 3×108 m/ s) pour trouver la distance séparant le mobile du satellite, une erreur par exemple d'une microseconde correspond à une erreur en distance de 300 m. Une bonne synchronisation entre les satellites et le récepteur GPS est donc absolument indispensable. La précision d'une horloge atomique peut être réalisée au récepteur GPS, cependant, avec l'utilisation d'un quatrième satellite. Pour cette raison, au lieu d'utiliser trois satellites pour déterminer les coordonnées x, y et z du mobile, le récepteur GPS utilise plutôt quatre satellites pour déterminer les coordonnées x, y et z du mobile et le décalage temporel de son horloge par rapport à celle du satellite. Quand la distance au satellite est mesurée, la quatrième sphère n'interceptera pas avec les trois premiers, ceci est du à la synchronisation imprécise du récepteur. Le récepteur tient compte de cette anomalie et ajuste son horloge afin qu'il soit synchrone avec ceux des satellites. La précision de localisation obtenue est actuellement d'environ 10 m pour le GPS civil. Cette précision est améliorée avec l'utilisation de plus de quatre satellites [CER93].

La limite du système GPS réside essentiellement dans le fait qu'il ne peut être utilisé que si l'antenne du récepteur GPS a une vue directe avec les satellites. Pour cette raison, il ne peut pas être utilisé dans les environnements internes et externes urbains où les grands buildings obstruent le signal des satellites [CER93].

2.3.2 Map matching:

Les études actuelles [OMW09], [BON07] dans les systèmes d'information Géographiques (SIG) ont permis la collection et le stockage, aussi bien que l'accès à des données géographiques très précises même pour des dispositifs moins puissants. Cette technologie a

été avec succès appliquée pour stocker les informations de carte de ville dans des systèmes de carte de localisation récemment développés pour la navigation des véhicules. Dans la technique Map Matching, plusieurs positions obtenues périodiquement peuvent être utilisées pour créer une trajectoire évaluée. Cette trajectoire est alors comparée aux données de la carte numérique pour trouver la géométrie du chemin la plus appropriée sur la carte qui correspond à la trajectoire. En utilisant cette technique, les informations de position peuvent être précisément représentées sur la carte [BEN09].

2.3.3 Dead Reckoning:

La position actuelle d'un véhicule peut être calculée en se basant sur sa dernière position connue et en utilisant les informations de mouvement comme la direction, la vitesse, l'accélération, la distance, le temps,… etc. Dans les VANETS, le Dead Reckoning peut être utilisé seulement pendant des périodes courtes dans le cas de l'absence de GPS. Puisque le Dead Reckoning accumule rapidement des erreurs, on l'utilise seulement comme un système de secours et ceci pendant la non disponibilité des informations GPS [BEN09], [BON07].

2.3.4 Localisation cellulaire :

La localisation cellulaire profite de la présence d'infrastructure cellulaire mobile dans la plupart des milieux urbains pour évaluer la position d'un objet. Les applications connues de cette technologie incluent la localisation des téléphones portables, le suivi des animaux domestiques et la localisation des véhicules. (RSSI) utilise la force des signaux reçus pour délivrer la distance aux stations de base. On peut délivrée la distance d'après le temps qu'il prend un signal émis par l'expéditeur pour parvenir à la station de base (ToA), on peut aussi utiliser l'angle d'arrivée (AoA). La localisation cellulaire est d'habitude moins précise que le GPS. L'exactitude dépend d'un certain nombre de facteurs comme le milieu urbain actuel, le nombre de stations de base détectant le signal, l'algorithme de positionnement utilisé,…etc. [BEN09], [OMW09].

2.3.5 Traitement d'image/vidéo :

Des sources d'information d'image et de vidéo et des techniques de traitement de données peuvent être aussi utilisées pour des buts de localisation, particulièrement dans des systèmes de guidage de robot mobiles [BON07]. Dans certains cas, des caméras sont disponibles dans les systèmes de sécurité mis en œuvre dans des parkings et des tunnels. Ces techniques de

traitement d'image/Vidéo sont utilisées pour alimenter des algorithmes de fusion de données pour évaluer et prévoir (suivent à la trace) l'emplacement d'un véhicule. En fait, les informations d'image et de vidéo sont des sources réelles que l'on peut utiliser pour calculer les paramètres d'emplacement d'un véhicule [OMW09].

2.3.6 Localisation relative distribuée:

Des cartes de position relatives et locales peuvent être construites par un véhicule en évaluant les distances entre ses voisins et en échangeant cette information de distance par une communication multi-sauts. Avec cette carte de position dynamique, un véhicule peut se localiser par rapport aux véhicules voisins et aussi de localiser les véhicules dans son voisinage. Ce type de localisation relative a été utilisé surtout dans les réseaux Ad hoc et les réseaux de capteurs; mais il est proposé dans un certain nombre de solutions pour les VANETs. L'algorithme de localisation distribuée pour aider des véhicules non équipés de GPS à évaluer leurs positions en exploitant les informations venant des véhicules voisins équipés de GPS. Un véhicule non équipé de GPS doit communiquer avec au moins trois véhicules équipés de GPS dans son voisinage pour évaluer les distances et calculer sa position [BEN09].

2.4 Les protocoles de localisation relative: [BEN09]

A. Benslimane a proposé une nouvelle technique de localisation des nœuds.

Sa solution proposée est basée sur la coopération entre les véhicules équipés de GPS pour aider les véhicules non équipés de GPS à obtenir leurs positions. Bien que la connaissance de la position exacte ne soit pas toujours possible, le véhicule non équipé de GPS peut obtenir une certaine information utile comme la direction de conduite et la distance le séparant de l'accident.

Conclusion:

Dans les réseaux ad hoc de véhicules, la connaissance de la position des nœuds en temps réel est une supposition faite par la plupart des protocoles, des algorithmes et des applications.

Dans ce chapitre on a décrit, les principes de base, les différentes approches, et les principales techniques avec le système de localisation global GPS.

Dans le chapitre suivant, on va représenter les différents types d'attaques existants dans les réseaux VANETs.

Chapitre 3:

Les différents types d'attaques dans VANET

3.1 Introduction:

Dans les réseaux VANET le trafic est accessible à tout le monde comme on ait déjà vu dans le premier chapitre, en conséquent toutes les attaques sur les réseaux WLAN sont possibles. La sécurité des réseaux véhiculaires est encore aujourd'hui un champ d'investigation assez peu exploré.

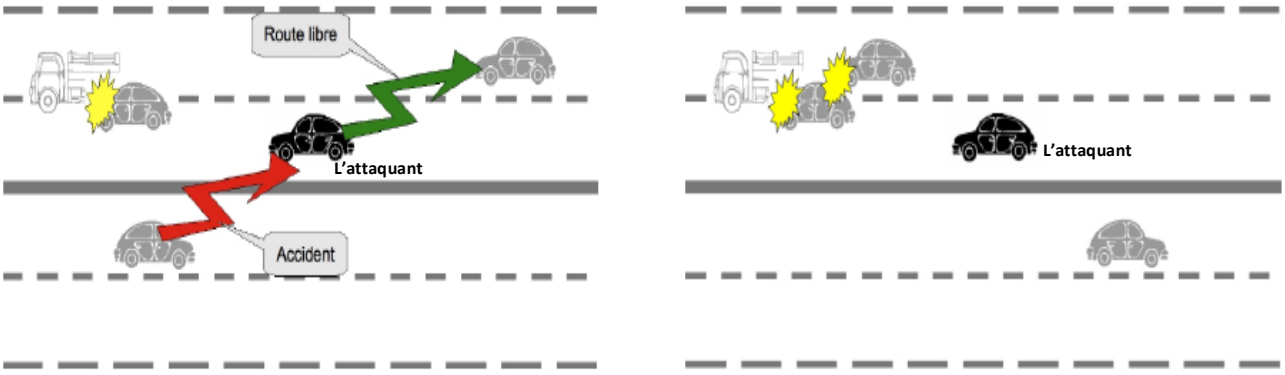
Dans ce chapitre, on va voir les différents types d'attaques dans VANET avec quelques exemples d'attaques. Et précisément les attaques liées aux fausses positions ou bien les attaques Sybil.

3.2 La sécurité dans les VANETS:

Les communications transitant dans un réseau de véhicules ainsi que les informations concernant les véhicules et leurs conducteurs doivent être protégées et sécurisées pour assurer le bon fonctionnement d'un système de transport intelligent.

La sensibilité des données véhiculées par un réseau VANET démontre un besoin fort en sécurité. En effet, l'importance de la sécurité dans ce contexte est concluante vue les conséquences critiques qui résultent d'une violation ou d'une attaque. De plus, avec un environnement fortement dynamique caractérisé par des arrivées et des départs de voitures quasi instantanés, et des connexions de courtes durées, le déploiement d'une solution de sécurité doit faire face à des contraintes et configurations spécifiques. Bien que le besoin de solutions sécurisées pour la transmission des données dans VANET a été préssenté dès leur apparition. Ce n'est que récemment que cette problématique a suscité un grand intérêt, et que quelques solutions ont été élaborées [GKS10].

Les réseaux de véhicules utilisent des communications sans fil, les données sont donc diffusées sur un médium partagé et non sûr. Il est alors très simple pour un nœud malicieux d'intercepter et de modifier des données, ou d'injecter de faux messages. Une injection de données peut provoquer des collisions dans un convoi de véhicules, comme le montre la figure 3.1. La nature ouverte des VANETS rend la sécurisation des communications difficile.



(a) Interception, injection (b) Collision

Fig. 3.1 Un exemple d'attaque par injection dans un VANET.

2.2 Les types d'attaques dans les réseaux véhiculaires:

Dans cette partie, on donne une classification générique des attaques recensées ou à venir dans les réseaux véhiculaires. On illustre ensuite cette classification par quelques exemples concrets.

2.2.1 Types des attaques

La sécurisation des réseaux véhiculaires passe par la détermination d'une typologie des attaques dans ces réseaux. Compte tenu de la diversité des applications que l'on peut y opérer et de celle des environnements d'opération, il est aisé d'imaginer que ces réseaux feront l'objet de nombreuses attaques dont certaines pourront même relever du terrorisme. On définisse 4 grandes déclinaisons pour toute attaque dans ces réseaux [TCH08].

- **Interne ou Externe:** Une attaque est dite interne si elle est instiguée par une entité identifiée comme légitime par les autres nœuds du réseau. De manière courante, une entité sera déclarée légitime si elle est authentifiée dans le réseau. Les attaques internes font partie des attaques les plus dangereuses puisque l'attaquant est injustement considéré comme étant de confiance et a généralement accès aux services du réseau. Une attaque externe est, quant à elle, menée par une entité à priori considérée et reconnue comme illégitime. L'attaquant dans ce cas n'est généralement pas authentifié dans le réseau et n'a pas accès aux services de ce réseau. Il est donc de ce fait limité dans la diversité des attaques qu'il peut entreprendre.
- **Intentionnelle ou Non intentionnelle:** Une attaque est dite intentionnelle si elle est instiguée par une entité malveillante visant délibérément à remettre en cause le bon fonctionnement du réseau. Ce type d'attaque est à distinguer d'une attaque non

intentionnelle ou involontaire qui peut par exemple être le fait d'une erreur de transmission radio ou d'une erreur protocolaire dans le réseau.

- **Active ou Passive:** Une attaque est dite active lorsque l'attaquant injecte, modifie ou supprime du trafic dans le réseau. Au contraire, dans une attaque passive, l'attaquant ne fait qu'écouter et collecter le trafic pour une éventuelle utilisation malveillante ultérieure.
- **Indépendante ou Coordonnée:** Une attaque est dite indépendante lorsqu'elle est menée de manière isolée par un seul attaquant. Elle est en revanche dite coordonnée lorsque plusieurs attaquants partageant le même dessein se concertent pour la mener.

2.3 Exemples d'attaques:

En raison de l'impossibilité d'envisager toutes les attaques possibles dans les réseaux véhiculaires, on se limite ici à la présentation et à la déclinaison dans la taxonomie introduite plus haut, de quelques exemples parmi les plus significatifs:

- **Attaque sur l'intimité numérique:** [TCH08] Dans cette attaque, l'entité malveillante essaie d'obtenir l'identité ou des informations personnelles d'un utilisateur du réseau. Il peut également s'agir pour l'attaquant de tracer l'activité et les déplacements de cet utilisateur. Pour identifier et tracer une victime, l'attaquant peut utiliser toute chaîne de caractères identificatrice dont la récurrence est constatée dans les échanges de la victime. Cette chaîne de caractères peut être une adresse IP, une adresse MAC, des informations d'identification d'un certificat, etc. Au-delà des chaînes de caractères, l'empreinte radio de la victime peut également être utilisée: on parle alors d'attaque de la couche physique. La Figure 3.2illustre une attaque sur l'intimité numérique et en particulier une identification non-autorisée. D'après la taxonomie des attaques qui a été définie, cette attaque peut être interne ou externe, intentionnelle, passive et indépendante.

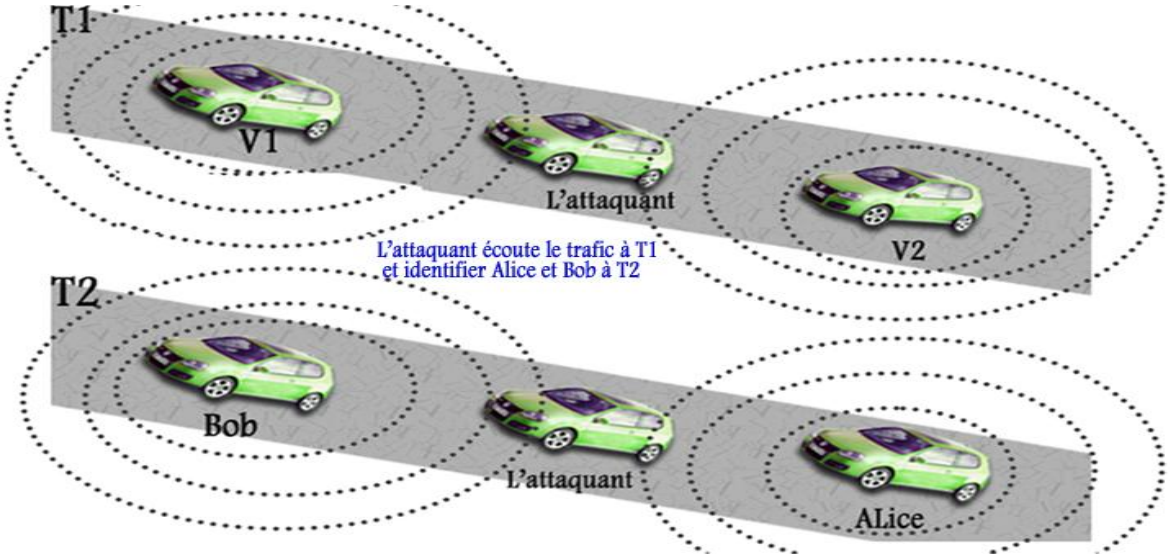


Fig. 3.2 Identification non autorisée

- ✓ **Attaque sur la cohérence de l'information:** [TCH08] Dans cette attaque, l'entité malveillante porte atteinte à la cohérence des informations acheminées dans le réseau en les modifiant ou en injectant des informations erronées. L'intention de l'attaquant peut être d'altérer la perception qu'ont ses victimes, de sa position, de sa vitesse, de sa direction, et plus généralement des conditions de circulation. L'attaquant peut par exemple provoquer un changement d'itinéraire de ses victimes. Sur la Figure 3.3 un attaquant diffuse des informations de trafic erronées et sur la Figure 3.4 des attaquants indiquent de fausses données de localisation amenant les victimes à admettre l'existence d'un bouchon qui en réalité n'existe pas. L'attaque de la Figure 3.3 est interne ou externe, intentionnelle, active et indépendante alors que celle de la Figure 3.4 est interne ou externe, intentionnelle, active et coordonnée.

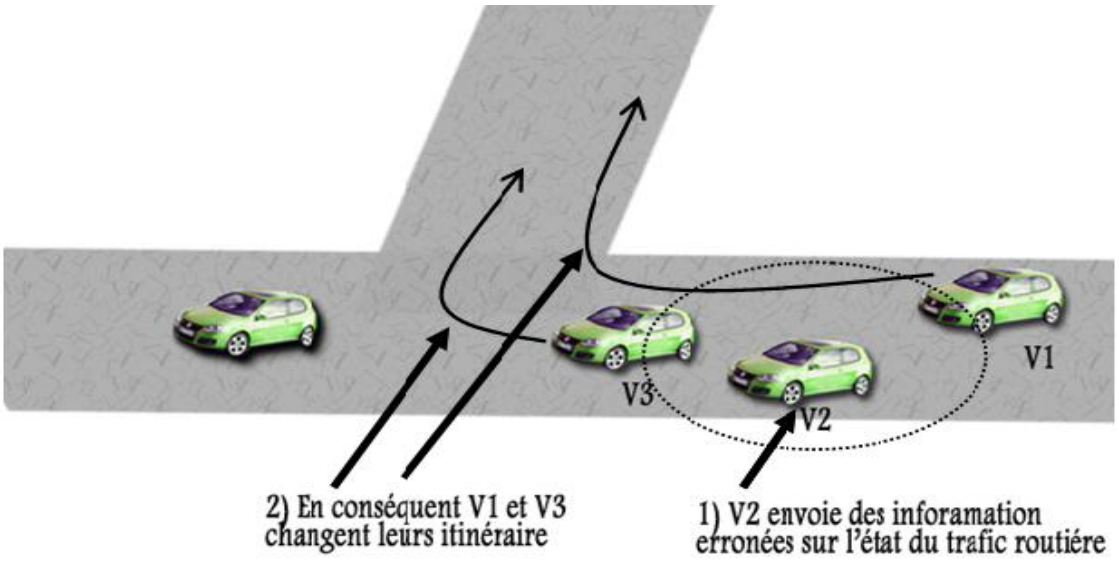


Fig. 3.3 Injection d'informations de trafic erronées

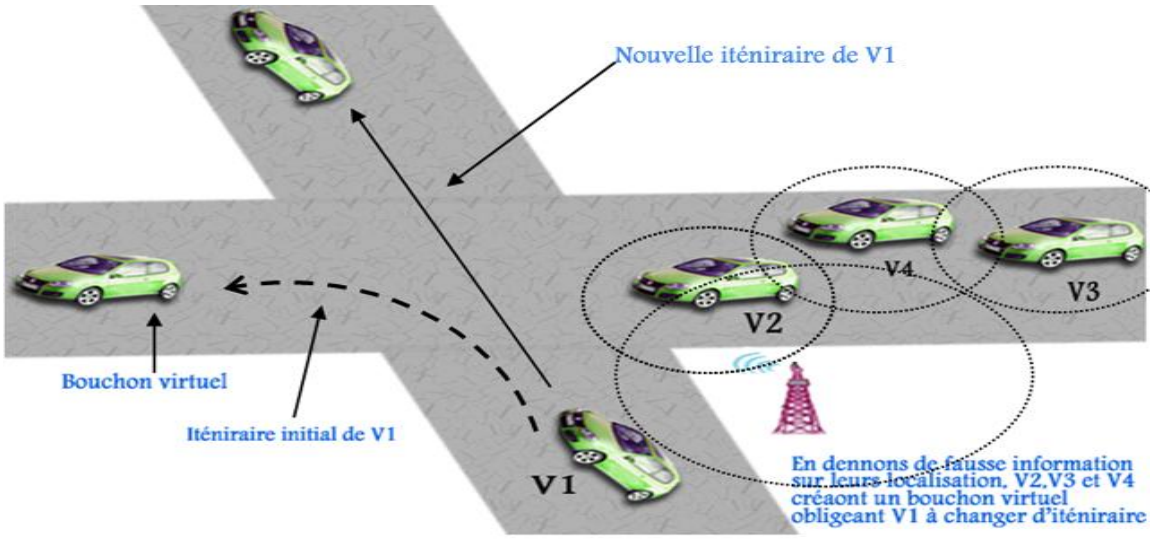


Fig. 3.4 Fausses déclarations de localisation

- **Usurpation d'identité ou de rôle:** Dans cette attaque, l'entité malveillante utilise une fausse identité ou de fausses lettres de créance pour se faire passer pour une entité légitime ou pour jouir des privilèges de cette dernière. La Figure 3.5 illustre un cas d'usurpation d'identité. L'attaque illustrée peut être Interne ou Externe, Intentionnelle, Active et Indépendante. Une de ces attaques est l'attaque Sybil [TCH08].

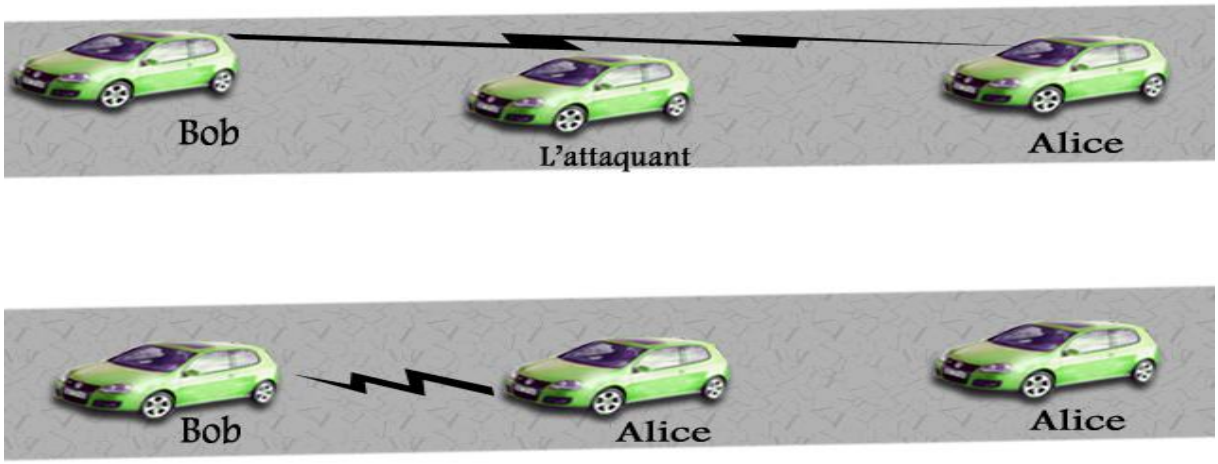


Fig. 3.5 Usurpation d'identité

- **Déni de service:** Dans ce type d'attaque, l'entité malveillante empêche l'accès normal aux services du réseau. Ce type d'attaque peut être monté en brouillant le canal radio, en surchargeant et en épuisant les ressources du réseau par des requêtes abondantes, en exploitant la vulnérabilité des protocoles, en ayant une attitude non coopérative (ex. refus de relayer des paquets), etc. La Figure 3.6 illustre une attaque par déni de service aboutissant à une collision, où l'attaquant empêche l'échange de messages critiques entre des véhicules s'apprêtant à prendre une intersection. Cette attaque peut être Interne ou Externe, Intentionnelle, Active et Indépendante.

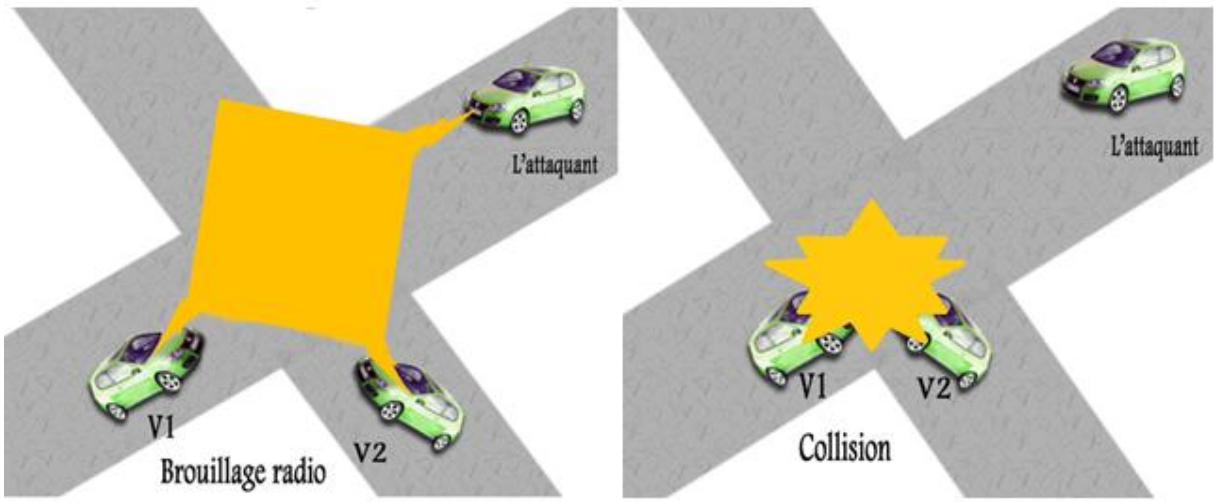


Fig. 3.6 Déni de service par brouillage du canal radio

- **Écoute du réseau:** Dans cette attaque, l'entité malveillante collecte les données transmises dans le réseau afin d'en extraire une information dont elle pourrait tirer profit. La Figure 3.8 illustre une telle attaque dans laquelle l'attaquant pionne une transaction commerciale, typiquement un paiement électronique, en vue d'en extraire un mot de passe. Cette attaque peut être Interne ou Externe, Intentionnelle, Passive et Indépendante.

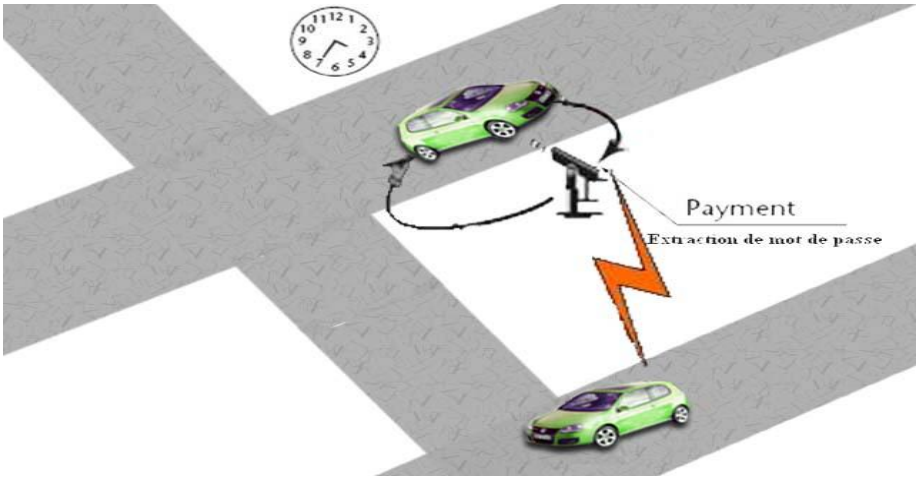


Fig. 3.7: Extraction du mot de passe d'une transaction commerciale

Comme nous sommes intéressés par les attaques Sybil ou les attaques de falsification de position qui sont une partie de l'usurpation des identités, on va les montrer dans les sections suivantes.

3.3 Les attaque Sybil et classification:

Sybil est une attaque de type d'attaque usurpation, où un attaquant usurpe l'identité d'un autre nœud dans le réseau et, par conséquent, tous les messages adressés à ce nœud victimes sont reçues par l'attaquant. Il existe différentes formes d'attaques telles que l'usurpation d'identité volée, l'attaque de nœud invisible et l'attaque Sybil. Dans une attaque Sybil, le nœud qui usurpe l'identité des autres nœuds est appelé nœud malveillant / attaquant Sybil et les nœuds dont les identités sont usurpes sont appelés nœuds Sybil. Une attaque typique Sybil est représentée sur la figure 3.8. Dans ce scénario, l'attaquant Sybil essaie de créer une illusion de la congestion routière sur la route. Le nombre de nœuds Sybil créé par l'attaquant Sybil dépend des ressources de communication, de stockage et de calcul de l'attaquant. [GKS10]

Les attaques Sybil peuvent être classées en trois catégories selon le type de communication, d'identité et de leur participation dans le réseau, comme suit [MDI10] :

- **Communication directe vs communication indirecte :**
    - Dans une communication directe, les nœuds Sybil communiquent directement avec les nœuds légitimes.
    - Dans une communication indirecte, les nœuds Sybil peuvent communiquer à travers un ou plusieurs nœuds malveillants se proclamant capables de les atteindre.
- **Identités fabriquées vs identités volées :**
    - Un nœud Sybilpeut fabriquer une nouvelle identité.
    - Un nœud Sybil peut voler l'identité d'un nœud légitime
- **Simultanéité** :
    - L'attaquant peut faire participer toutes ses identités Sybil de façon simultanée dans le réseau.
    - L'attaquant peut alternativement présenter seulement une partie de ses identités sur une période de temps donné.

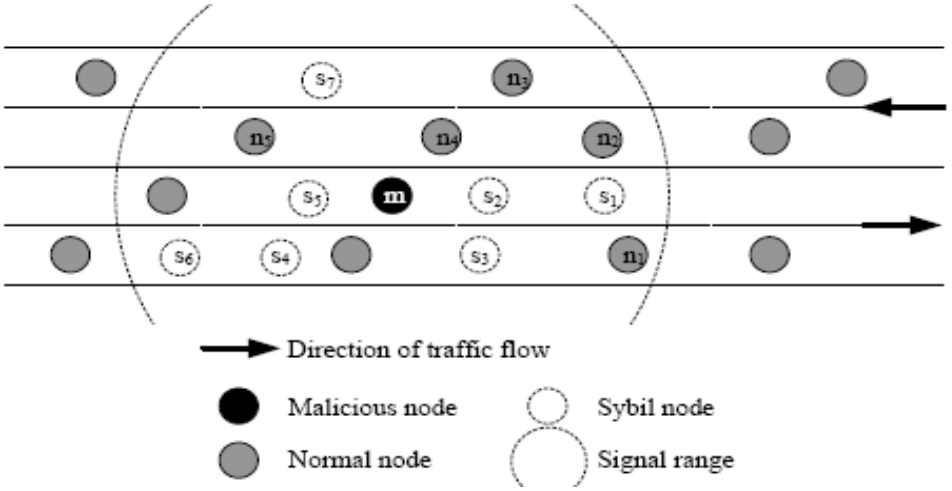


Fig. 3.8 Les attaques Sybil

Conclusion:

Dans ce chapitre nous avons présenté les différents types d'attaques possibles dans les réseaux VANETS avec quelques exemples; ou on a présenté le risque de chaque attaque.

La position est un élément clé de l'information échangée entre les véhicules des réseaux VANETs. La détection de l'information de fausse position réduit le risque d'attaque, cette détection est la clé de la réussite de VANET.

Dans notre travail, nous nous intéressons aux attaques liées à la falsification de position comme les attaques Sybil.

Dans le chapitre suivant, on va présenter les différentes techniques de vérification de position dans les réseaux VANETs.

Chapitre 4

Les techniques de vérification de position dans les VANETS

Introduction:

La sécurité pose un problème majeur dans les réseaux véhiculaire (VANETS), et parmi les attaques les plus dangereuses dans ces réseaux est la falsification de la position.

Dans le chapitre précédent nous avons représenté les attaques Sybil. Comme nous avons déjà vue ces attaques représentent un grand problème pour la sécurité dans les VANETS, dans ce qui suit on va représenter les techniques qui nous a permet d'éviter ces attaques et les détecter. Ainsi que les différentes techniques de vérification de position dans les VANETS, pour une meilleure sécurité contre les attaques Sybil.

4.2 Les techniques de vérification:

Pour améliorer la sécurité routière on trouve plusieurs techniques, parmi ces techniques on a des techniques qui sont basées sur la vérification de la position des nœuds dans les réseaux VANETS.

4.2.1 Détection et localisation des nœuds Sybil dans VANETS

Un régime de sécurité léger pour détecter et localiser les nœuds Sybil dans les VANETs, basé sur l'analyse statistique de la distribution force du signal été représenté dans [BBC06]. Ce régime est une approche distribuée et localisée, dans laquelle chaque véhicule sur une route peut effectuer la détection de véhicules Sybil à proximité en vérifiant leurs positions revendiquées.

Dans ce régime on suppose qu'il ya un certain nombre de véhicules qui circulent sur la route et la plupart des nœuds peuvent faire confiance. Seuls quelques véhicules peuvent effectuer des attaques Sybil afin d'atteindre leurs objectifs malveillants. Chaque véhicule est équipé de même module radio et dispositifs GPS, et les positions GPS sont censées être exactes. Et que les stations de base en bordure de route sont peu déployées le long des routes et l'infrastructure d'authentification d'identité.

Ce régime est basé sur la vérification de position par le contrôle de la puissance du signal des messages périodiques. Pour plus de clarté de la description, on définit trois catégories de rôles des nœuds: claimer, witness, et verifier. Chaque nœud serait périodiquement jouerait tous ces rôles.

- **Claimer:** Chaque nœud périodiquement diffuse un message de *Beacon* dans l'intervalle t_b, pour découvrir son voisinage. Le message de la balise contient son identité et la position GPS en ce moment.

- **Witness:** *(témoins*) Tous les nœuds voisins, au sein de la portée du signal du claimer, recevraient le message de *Beacon* précédent. Ils mesurent la force du signal et enregistrent les informations correspondantes dans leur mémoire. La prochaine fois qu'ils diffusent un message de *Beacon*, ils attachent leur liste de voisins, qui contient les mesures du signal pour chaque message reçu, au message de *Beacon*.
- **Verifier:** Après avoir reçu un message de *Beacon,* un nœud attend un intervalle de vérification, $t_{v,}$ au cours de laquelle il recueille suffisamment de mesures d'intensité de signal sur le message de *Beacon* précédent des témoins voisins. t_v peut être un peu grand que l'intervalle $t_{b,}$ puisque, après un autre intervalle $t_{b,}$ chaque témoin voisins devrai avoir diffusé une *Beacon* contenant des mesures attendues. Avec les mesures collectées, le nœud peut localement calculer une position estimée du claimer, par exemple, en effectuant MMSE (Minimum Mean Square Error-) sur la force du signal collecté et un modèle de radio prédéfinie. On appelle le nœud qui effectuer la vérification le VERIFIER.

Pour obtenir la position estimée, on calcule d'abord l'erreur quadratique moyenne:

$$MSE(p) = \frac{\sum_{i=1}^{k}(Sr(Wi) - Sm(Wi,p))^2}{k}$$

Où p est une position potentielle de claimer; k est le nombre des witnesses; S_r est la puissance du signal reçu au w_i witness, S_m est la force du signal calculé au w_i obtenus à partir de modèle de propagation radio.

Si la position estimée d'un claimer est loin de sa position revendiquée, on considère ce nœud en tant que nœud suspect. En raison de la nature instable et irrégulière de RF (Radio Frequency), on ne peut pas affirmer, sur la base des résultats de ce calcul simple, qu'une attaque Sybil peu se passer.

Le message de Beacon peut être dans le format suivant:

{NodeID, Beacon #, Position, NebList, Signature}

NebList: {NodID$_i$, Beacon#$_i$, RSS$_i$}

Où NodeID est l'identité du claimer, Beacon # est un numéro de séquence des messages de *Beacon*, *Position* est la position d'expéditeur revendiquée, *NebList* est la liste de l'expéditeur voisin le plus récent contenant des mesures de force de signal, *Signature* est la signature

numérique pour l'ensemble du paquet. Dans chaque élément de *NebList*, RSS_i est la puissance de signal reçu des messages de *Beacon* $Beacon_i$ récemment reçu $NodeID_i$ des nœuds voisins.

4.2.2 Les méthodes de vérification de position pour les réseaux ad hoc véhicule

Dans [LSK06], pour la vérification de la position, il est seulement nécessaire de trouver des capteurs appropriés qui peuvent être utilisés pour détecter des informations de position falsifié. Fondamentalement, il existe deux catégories de capteurs de vérification de la position. Les capteurs de la première espèce qui travaille de manière autonome sur chaque nœud et contribuent par leurs résultats à l'ensemble des cotes de confiance voisins. La deuxième catégorie comprend des capteurs qui fonctionnent uniquement en coopération avec d'autres nœuds entourant le nœud voisin en question.

Tous les capteurs ont ne s'appuient pas sur les informations fournit couche de routage de toute façon, il n'y a pas de matériel supplémentaire en cause. En outre, seuls les nœuds normaux formant les VANETs sont inclus. Ne pas plus besoin d'une infrastructure dédiée.

Combinaison de capteurs vérification:

L'accumulation des observations au cours du temps et des capteurs est tenue de fournir la décision de savoir si un nœud doit être considéré comme étant malveillant ou non. Sachant aussi que les observations de certains capteurs sont plus fiables que les observations de ceux d'autres, on utilise un modèle de confiance qui offre les capacités nécessaires pour tenir en compte des observations provenant de capteurs différemment pondérés pendant une certaine période de temps.

Lorsqu'on indique la n^{ième} observation du capteur S par σ_n^S le modèle de confiance peut être décrite comme suit:

- ✓ Tous les nœuds magasin de confiance des valeurs r ϵ [-1, 1] pour tous les voisins directs. r = 0 est équivalente à la confiance neutre, r ϵ] 0, 1] signifie qu'un nœud est digne de confiance, et r ϵ[-1; 0[signifier qu'un nœud n'est pas digne de confiance.
- ✓ Chaque observation σ_n^S est stockée avec horodateur t_n^S.
- ✓ A l'arrivée d'une nouvelle observation, la valeur de confiance pour un nœud voisin est recalculée en fonction des observations recueillies à ce nœud.
- ✓ Toutes les observations sont stockées pendant un temps T maximum et jetés par la suite.

Le facteur de pondération a été d'une σ_n^S, l'observation est choisie en fonction de la fiabilité du capteur fournissant, par exemple, les observations d'un capteur plus fiable peut être considérée comme plus précieuse que les observations d'une autre moins fiables, comme le capteur Mobility Grade Threshold (MGT). En outre, les observations peuvent également être pondérées de façon dynamique (par exemple, si un capteur offre une observation avec différentes fiabilité).

L'horodateur t_n^S d'une observation σ_n^S est utilisé pour calculer le facteur temps de l'observation wt(t, t_n^S):

$$wt(t, t_n^S) = 1 - \left(\frac{t - t_n^S}{T}\right)^x$$

Où *x* représente le facteur exponentiel vieillissement des observations. *x* = 1 correspond à un processus linéaire de vieillissement, et les valeurs *x*> 1 sont équivalentes à une plus que les processus de vieillissement linéaire de l'observation respective.

Enfin, la r_t valeur de confiance d'un nœud voisin à un instant t est calculée en multipliant les observations disponibles par leur facteur de poids et de leur facteur temps, puis résume les résultats et la fin de la normalisation à [-1; 1].

Infractions détectée sont pondérées plus élevés que les observations d'un comportement normal; ainsi, une fois les informations de position falsifiée sont détectées, il faut plusieurs messages de balise correcte pour compenser le niveau de confiance.

Dans le protocole de routage, les informations de localisation est distribué entre les nœuds au moyen de balises de position. Afin de prévenir les abus du système de vérification, les balises doivent être authentifiés et horodaté par leur expéditeur. Quand un nœud reçoit un phare position d'un autre nœud, qui se prétend à une certaine position, les capteurs deviennent actifs afin de vérifier si cette revendication est susceptible d'être correcte ou non.

4.2.3 Une sécurité Fournir pour VANET par vérification de position

Le projet [GKC07] a étudie les aspects de sécurité de la communication de véhicule à véhicule en utilisant le GPS et le radar. Le but de ce travail est de fournir un milieu fermé pour une topologie VANET et de construire un réseau sécurisé pour les applications. On utilise un radar et on suppose que le nombre des voisins est limité en raison de la limitation de la portée de transmission radar, un véhicule peut «voir» entourant les véhicules et d'entendre des rapports sur leurs coordonnées GPS. En comparant ce qui est vu et entendu, un véhicule peut déterminer la position réelle des voisins et d'isoler les menteurs (attaquants Sybil) pour assurer la sécurité.

Dans ce projet les véhicules sont supposés être dotés des caractéristiques suivantes:

- ✓ Un système de navigation GPS, comme un récepteur GPS, cartes GPS, radar micro-ondes qui peuvent détecter des objets à distance jusqu'à 200 mètres.
- ✓ Un centre informatique, qui permettra le traitement des données, calcul et de stockage;
- ✓ Un émetteur-récepteur sans fil, tels que DSRC qui permettent la communication rapide pour VANET;
- ✓ Un identifiant unique, comme une plaque d'immatriculation électronique qui est donnée par les autorités d'enregistrement ou est stockée dans EDR.

Principe:

Le radar détecte les obstacles à venir. Système de navigation GPS, en particulier le récepteur GPS et des cartes, fournit les coordonnées et la localisation. Pour simplifier le matériel de sécurité, on suppose que tous les appareils sont inviolables, comme une EDR. La figure 4.1 montre la disposition des dispositifs dans un véhicule.

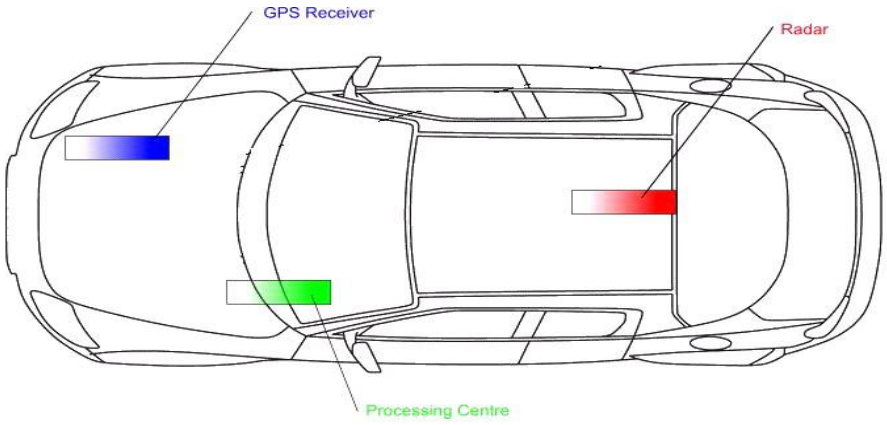


Fig. 4.1 Montre l'agencement des dispositifs dans un véhicule.

Modèle de réseau:

Il existe deux types de cellules : les cellules dynamiques et les cellules basées sur la position. Bien que les cellules dynamiques soient flexibles, ils ne sont pas efficaces. D'autre part, les cellules à base de position, sont crées à l'avance, et les véhicules qui utilisent leurs coordonnées GPS à la carte à leurs cellules respectives. Ces cellules évitaient le processus complexe de formation d'une cellule et l'élection d'un chef de cellule.

On peut configurer la route avec des cellules virtuelles numériques, par exemple tous les 200 mètres d'une cellule sur la route, c'est à dire, le rayon des cellules est de 100 mètres de

telle sorte que tous les véhicules à l'intérieur veut directement envoyer ou recevoir des paquets sans routage. Le rayon des cellules est le même avec la distance de transmission du radar de sorte que tous les voisins à l'intérieur peuvent être directement détecté par le radar. Overlap, qui est zone d'intersection entre deux cellules doit être décidé avant que les cellules sont formées. La taille du chevauchement (Overlap) dépend de la taille des cellules et l'état de la route. Si la taille des cellules est très grande, le chevauchement peut être faible proportion des cellules; si la route est la route nationale, le chevauchement peut être plus grand pour contenir plus de véhicules que les routeurs potentiels. Dans ce projet, ils ont utilisé un scénario de l'autoroute, et les cellules sont de 100 mètres-rayons, par conséquent, ils sélectionnent les chevauchements 20-30 mètres. Lorsque les véhicules sont à proximité de la superposition de deux cellules, ils peuvent choisir que le routage des véhicules. La nécessité pour les routeurs dépend de la portée de transmission. Si la portée de transmission peut atteindre le chef de cellule suivante sans avoir besoin d'un saut intermédiaire, alors il n'est pas nécessaire d'avoir des routeurs cellulaires. Les étapes pour former une cellule du réseau sont:

- ✓ En consultant la carte chargée chiffres, chaque véhicule peut décider de la taille des zones de recouvrement entre deux cellules;
- ✓ Partition la carte numérique dans les cellules, par exemple 100 cellules mètres du rayon, en s'assurant que les chevauchements;
- ✓ Véhicules de décider de ses cellules en fonction de ses coordonnées GPS et le préréglage des cartes numériques;

Chef de cellule : est déterminée pour chaque direction. Un véhicule, à proximité du centre de la cellule serait admissible être le chef de cellule. Chaque véhicule obtiendrait un score de crédit en fonction de la distance de la cellule. Le véhicule avec le score le plus élevé de crédit prendra le relais en tant que chef de cellule et annonce sa nouvelle appellation. Dans les cas où plus d'une voiture ont obtenu le même score, inférieur ID obtiendrait la priorité.

Les véhicules membre régulièrement (toutes les 100ms) envoient des informations de position au chef de cellule. Non seulement le chef de cellule obtient cette information, mais aussi les autres membres du véhicule. On peut réduire les collisions dues à la diffusion périodique en permettant aux véhicules non seulement la diffusion de leurs coordonnées GPS, mais aussi la position des véhicules dans leur ligne de vue directe. Distance et position par rapport au chef de cellule devait décider du temps de transmission suivante. De cette façon, les véhicules voisins ne doivent pas diffuser leurs coordonnées s'ils sont d'accord avec la transmission du véhicule. Le chef de cellule et d'autres membres de l'agrégat de cellules de ces informations et de construire le point de vue du trafic.

Quand un nouveau véhicule entre dans le système, il attend 200ms au cours de laquelle elle entend les informations transmises par les autres membres de la cellule et apprend l'ID de chef de cellule. Le nouveau véhicule active aussi son radar pour détecter ses voisins. À la fin de la tranche de temps, il envoie ses informations de position ainsi que des informations de position de ses voisins. Si ce n'était pas en mesure de détecter le chef de cellule, il envoie une requête demandant l'adresse (ID) du chef de cellule. Si aucune réponse ne vient donc de nouveaux véhicules prennent le relais en tant que chef de cellule et annonce son nouveau rôle.

Sécurité locale:

Une cellule est la plus petite entité qui peut être fixé contre les attaques de position. Tout membre de la cellule peut vérifier les coordonnées GPS reçues de tout autre membre en utilisant le radar. Si le chef diffuse les coordonnées avec les conclusions de radar, le message est accepté. Le chef de cellule diffuse des informations sur ses membres de la cellule toutes les 100ms, ainsi que son point de vue du trafic agrégé. Depuis d'autres membres de la cellule seraient aussi voir la situation des trafics similaires, le chef de cellules malveillantes peut être détecté, en supposant que la plupart des véhicules sont honnêtes. Si un chef de cellule se trouve, les voisins diffusent les informations correctes. Le message peut être capté par le routeur cellulaire, chef de cellule ou de tout véhicule membre en fonction de la distance de transmission et de l'état du trafic. Les véhicules membre réinitialisent le compteur de relais quand ils reçoivent le message. Si un véhicule n'est pas entendu le relais du message avant son expiration de la minuterie, il relaie le message reçu. Le temps de relais suivant dépend de la distance de la source du message.

Position GPS :

Dans le GPS, [2.3.1] lorsque les signaux de radio par satellite sont transmis, ils sont faussés, donc les coordonnées GPS ont une certaine tolérance. $\Delta x = \pm 0{,}25$ m; $\Delta y = \pm 0{,}25$ m. Dans la figure 4.2, nous supposons que Δy et Δx sont toujours égales, marqué comme $\Delta\alpha = \Delta x = \Delta y$. La zone d'ombre est l'ensemble des positions possibles véhicule réel.

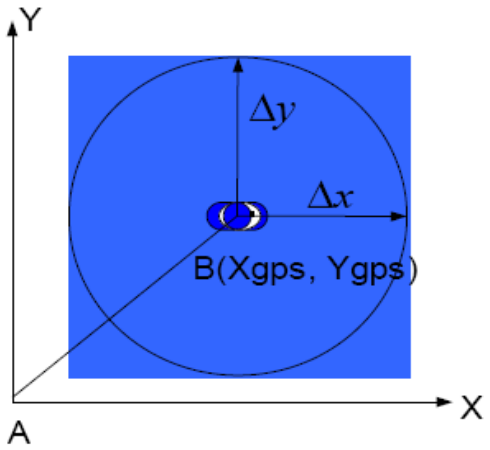


Fig. 4.4 La tolérance GPS pose une série de position GPS réelle, comme la montre l'ombre.

On peut utiliser la formule suivante pour décrire cette région. On utilise (x, y) pour représenter la position réelle du véhicule dans le système GPS.

$$(x-x_{gps})^2 + (y-y_{gps})^2 \leq (\Delta\alpha)^2 \qquad (1)$$

Détection radar

On suppose que la tolérance radar comprend deux parties: la tolérance angle Δq et tolérance Δr rayon, comme (Δq, Δr). Dans la figure 4.3, la région est délimitée par l'ombre HGQFEP. On utilise (x, y) pour représenter la position réelle du véhicule dans le système GPS et marquer les lectures radar (q, r). On peut utiliser les formules suivantes pour décrire deux cercles, cercle D et C le cercle de la figure 4.3.

Sans perdre de généralité, il suppose que le véhicule détecté est au centre de l'ombre:

$$(x-r*\cos(\theta-\Delta\theta))^2 + (y-r*\sin(\theta-\Delta\theta))^2 \leq (\Delta r)^2 \qquad (2)$$

$$(x-r*\cos(\theta+\Delta\theta))^2 + (y-r*\sin(\theta+\Delta\theta))^2 \leq (\Delta r)^2 \qquad (3)$$

Θ : l'angle de détection, on partant du nord de 0 degré ;

r : le rayon de détection (la distance entre un véhicule et le véhicule B) ;

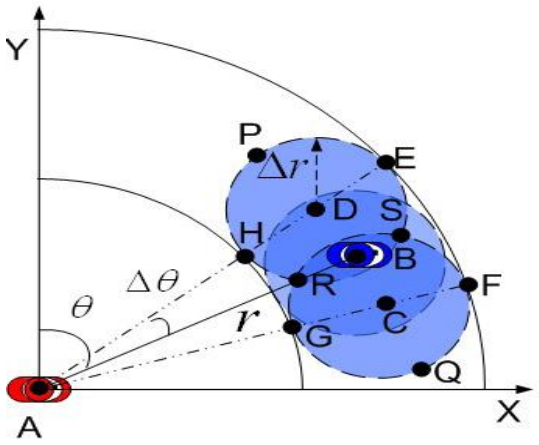


Fig. 4.5 La tolérance (Δq, Δr) du système de radar cause un ensemble de position réelle, montre que l'ombre de la lumière.

On remarque qu'il ya deux petites régions HRG et EBF, où la position réelle d'un véhicule pourrait être, qui ne sont pas décrits par la formule (2) et (3), par exemple la région FGHE à la figure 4.3. C'est pourquoi il utilise la formule (4) pour décrire cette région.

$$\begin{cases} r - \Delta r \leq x^2 + y^2 \leq r + \Delta r \\ \theta - \Delta\theta \leq arctg\frac{x}{y} \leq \theta + \Delta\theta \end{cases} \qquad (4)$$

Région d'intersection :

Sans perdre de généralité, on suppose que le véhicule réel est au centre de la position GPS et la position de radar, comme le montre la zone d'ombre dans la figure 4.3. Si l'une des combinaisons suivantes a une solution, il peut tirer la conclusion que le véhicule détecté est honnête:

Formule (1) et la formule (2)

Formule (1) et la formule (3)

Formule (1) et la formule (4).

Sinon, il est déterminé à être un véhicule compromis. La signification de ces combinaisons est illustrée à la figure 4.4. Si la position GPS réel est en baisse dans la région de position radar réel, c'est à dire si il ya un chevauchement entre l'ombre et l'ombre position GPS position radar, cela signifie que le GPS position réelle est très proche de la valeur qui est détecté par le système radar. C'est pourquoi il affirmé que il ne peut accepter la position GPS.

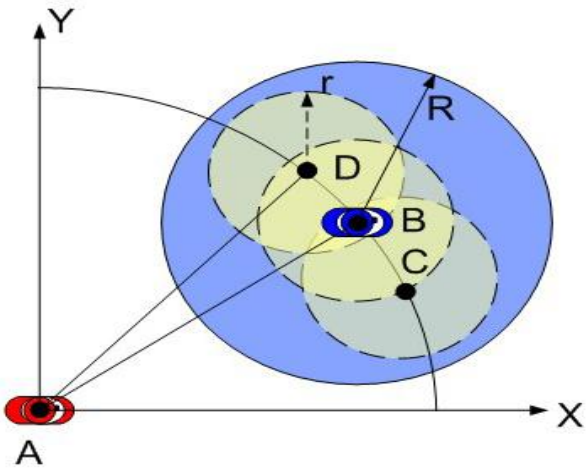


Fig.6.4 S'il ya une zone de chevauchement entre les plus sombres ombres (position GPS) et plus légère ombre (position radar), nous acceptons les coordonnées GPS, sinon jetez-le

Sécurité global

Les messages diffusés par le chef de cellule sont captées par le chef de cellule de la circulation qui est proche plutôt que celle qui a déjà passé cet endroit. Un chef de cellule ou de tout autre membre de la cellule peut envoyer une demande de vérification de deux façons: proactive et réactive. Proactive, un véhicule peut choisir au hasard un enregistrement et la vérification de la demande. Réactif est quand un enregistrement est en litige. Habituellement, un véhicule membre attend le chef de cellule d'envoyer une requête de vérification avant d'envoyer ses propres. Un véhicule dans une cellule voisine aurait plus de chances d'être sélectionnés pour la vérification d'un véhicule qui est loin de la cellule.

Afin d'augmenter la probabilité de vérifier la potentielle position des véhicules malveillants, on garde la trace des mouvements de véhicules. Chaque véhicule dans une cellule connaît la position exacte de tous les autres véhicules dans une cellule par échanger des paquets. Avec les données localement détectées par radar, le radar de la circulation venant en sens inverse a détecté des données et des données fiables voisines dans la main; on applique similitude cosinus à ces données. Si la valeur de similarité est supérieure à un seuil, on accepte les données, sinon il est abandonné. Avec les données acceptées, on construit une histoire des mouvements de véhicules, ou un tableau d'historique. L'idée de base est que l'histoire d'un véhicule sans position n'est pas digne de confiance, tout comme une personne sans antécédents de crédit ne peut pas obtenir un prêt. Lors de la réception d'une annonce position, l'observateur vérifie la table Historique et vérifier la position fondée sur la cohérence

du mouvement. S'il ya divergence, le dossier en particulier est plus susceptible d'être pris pour vérification.

Une demande de vérification peut être envoyée de deux manières différentes. Premièrement, l'utilisation des véhicules dans la même direction et d'autre part, ce qui rend les véhicules sens inverse de vérifier le véhicule. La circulation message de demande jusqu'à ce qu'elle atteigne le véhicule qui est en ligne directe de la vue du véhicule litigieux. Un message de réponse est alors renvoyé au demandeur. Une réponse positive serait valider le record. La demande et le message de réponse n'est pas nécessaire d'attendre la prochaine transmission de se produire. Ils sont transmis dès qu'ils sont reçus. Pour cette raison le véhicule peut recevoir deux confirmations: celle de véhicules sens inverse et un autre véhicule de même sens.

4.2.4 Évaluation de la performance et la détection des attaques Sybil dans les réseaux Ad-Hoc des véhicules

Dans un système distribué comme VANET, [GKS10] la plupart des applications supposées que chaque entité participante a exactement une identité. Si cette hypothèse est vérifiée, alors il n'ya pas de risque d'attaques d'usurpation d'identité. Ces attaques peuvent être évitées en utilisant l'autorité de certification centrale. Ceci garantit l'autorité que chaque entité n'a qu'une seule identité. Toutefois, en pratique, il est très difficile de déployer ce système sur une grande échelle. Essais de ressources est une autre méthode pour défendre une attaque Sybil.

On suppose que les ressources physiques de chaque nœud sont limitées. Malheureusement, cette méthode ne convient pas pour les réseaux ad hoc car un attaquant peut avoir plus de ressources que les nœuds honnêtes. Test des ressources radio est également difficile à mettre en œuvre. Certains documents, mentionnent que la cryptographie à clé publique peut être utilisée pour résoudre le problème de la sécurité des attaques Sybil et d'introduire l'utilisation, est une solution lourde et difficile qui doit être testé pour évaluer son utilisation possible dans le monde réel en raison de VANET caractéristiques. Dans, la méthode multilatération vérifiables est proposé pour l'exécution à distance de sélection. Diverses solutions de détection d'attaque Sybil sont présentés.

La méthode proposée est dans laquelle tous les nœuds participent à l'observation (plutôt que d'utiliser nœuds de fixes de confiance) tout écart de conduite dans VANET, et chaque nœud vérifie la position de l'expéditeur de paquets en utilisant l'approche vérification de la position.

Chaque nœud du réseau (soit une unité fixe en bord de route ou d'un véhicule) observe et informe sur la circulation des échanges afin d'analyser l'existence d'une attaque Sybil.

Tous les nœuds VANET suivent les uns des autres de manière distribuée et coopérative en prenant aide de preuves d'observation de la circulation (*cf.* figure 4.5).

L'expéditeur reprend sa position et time-stamp dans les paquets. Les positions sont obtenues à partir d'un appareil GPS. Comme un nœud reçoit un paquet de nœuds voisins, il vérifie sa position revendiquée. Le nœud récepteur estime la position de l'expéditeur, soit par la mesure de la puissance du signal reçu (RSS) du paquet reçu ou par une approche de vérification de position basée sur des capteurs multiples. Si la position revendiquée de l'expéditeur et sa position estimée par match récepteur, le récepteur génère l'observation et transmet les paquets à ses nœuds voisins. Sinon, le récepteur rejette le paquet.

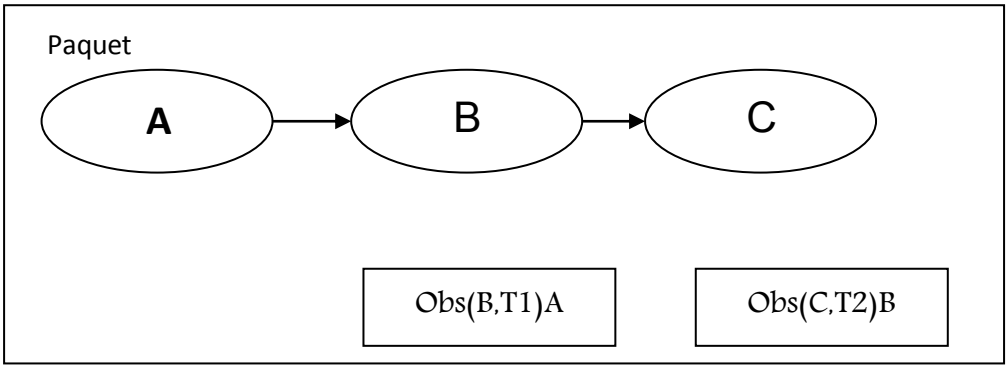


Fig. 4.7 Trois nœuds A, B et C. A envoi un paquet. Obs (B, T1) A représente l'observation du nœud A enregistré par nœud B au temps T1. Obs (C, T2)B représente les observations du nœud B enregistré par C à l'instant T2.

Chaque nœud dans le réseau diffuse ses observations et les enregistré dans une grille d'observation pour ses nœuds de communication. Dans cette grille, les observations d'un nœud donné sont stockées dans une rangée triée par date et heure. Chaque ligne décrit la trajectoire du mouvement de ce nœud. Si deux lignes sont les mêmes, cela implique que l'un de ces nœuds est un attaquant Sybil.

4.2.5 Sécurité et confidentialité dans VANET de réduire les frais d'authentification pour les réseaux d'itinérance rapide

Dans ce travail [MAH10], le système d'authentification est utilisé pour améliorer la sécurité dans les VANETS.

Le régime d'authentification dans les VANETS :

On considère le scénario de communication VANET, comprend des entités communicantes des prestataires de services (SP), les voitures, et les points d'accès (AP) exploités pour le compte des fournisseurs de services. Les (SPs) et les (APs) peuvent communiquer entre eux par certains protocoles propriétaires de la couche application via Internet. Les APs sont déployés le long de la route avec une couverture sans fil raisonnable pour faciliter la communication. Une voiture appartient généralement à un prestataire de services réseau sans fil, et communique avec les APs pour accéder à Internet sur la route qu'il traverse. Quand il se déplace, il se promène aussi dans la couverture sans fil qu'est offerte par d'autres autorités.

Pour rendre le processus d'authentification du temps efficace, les solutions traditionnelles en utilisant le serveur d'authentification centralisée (AS), n'est pas préférable en raison de la grande quantité de messages échangés entre les voitures, les AP et les AS. Si le réseau de recouvrement reliant les AP et l'AS est basé sur l'Internet, le délai pour échanger des messages d'authentification pourrait être prohibitif compte tenu de la brièveté de la durée de communication entre la voiture en mouvement rapide et un individu AP. Ainsi, les protocoles d'authentification sont conçues de telle sorte qu'après la voiture initie les demandes de communication jusqu'à la session de communication est établie, le protocole devrait impliquer les partis les moins possibles en dehors de la voiture et l'AP, et que moins à la demande de communication sur Internet que possible en dehors de la liaison sans fil entre les deux parties qui communiquent. En outre, le nombre de messages échangés pour que l'authentification doit être contrôlée. Dans cette conception, l'authentification des utilisateurs sera effectuée à l'AP, c.-a-d, l'utilisateur devra prouver à l'AP qu'il est légitime.

Une sécurité plus stricte, il faudra l'AP pour prouver qu'elle est légitime et, de manière à avoir une authentification mutuelle.

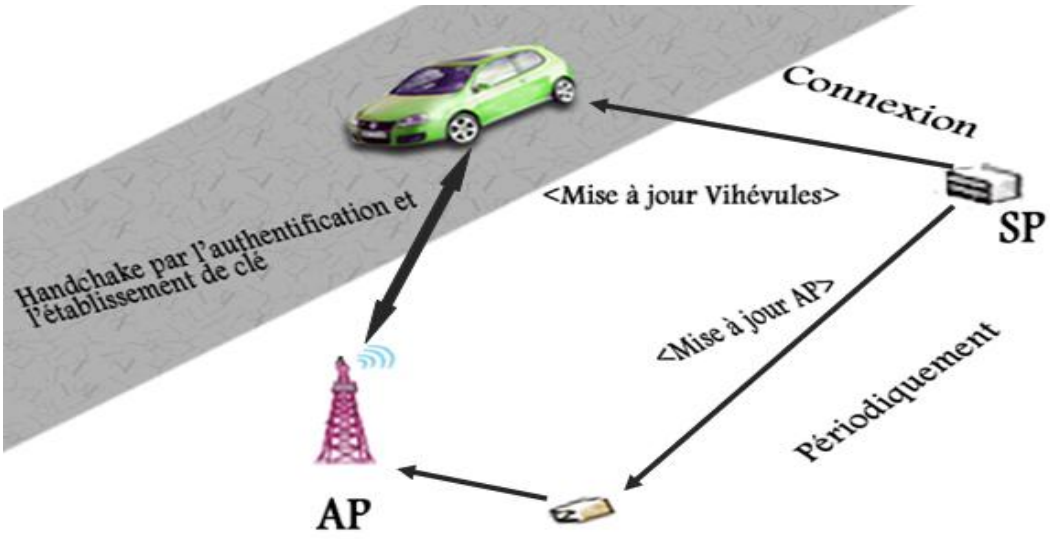


Fig. 4.8 Processus d'authentification générale

Lors de l'authentification, les deux parties négocient une clé de session secrète de la communication par la suite. Les clés de session n'ont pu être établies d'une manière qui synchronise la mise à jour à la fois la voiture et l'AP afin de permettre à des contre-mesures confidentialité de la localisation. Le processus d'authentification générale est représenté sur la figure 4.6.

Proxy ré-cryptage (PRA) dans l'authentification :

Proxy ré-cryptage est un concept introduit par Blaze, permet une entité semi-confiance appelé «proxy» pour convertir les textes chiffrement adressée à une entité B appelé le "délégataire" à une autre entité appelée C le "délégué ", tout en maintenant que le proxy ne peut rien apprendre sur le texte en clair sous-jacentes, et C ne peut rien apprendre sur le texte en clair sous-jacent sans la coopération de la procuration. B présente cette délégation en fournisse une pièce spéciale de l'information, appelé la «recomposition», à la procuration. Proxy ré-cryptage a trouvé des applications diverses telles que le renvoi de courrier électronique sécurisé, etc. Le concept de base du chiffrement nouveau proxy dit que, un texte chiffré à Alice qui est chiffrée par la clé publique d'Alice peut être transformé par une procuration à un texte chiffré pour Bob qui peuvent être déchiffrées par la clé privée de Bob. La procuration ne peut toutefois pas lire le texte chiffré. Dans cette procédure, les délégués Alice son droit de décryptage pour Bob. La clé que le proxy utilise pour réaliser la transformation est appelée clés ré-cryptage $rk_a \rightarrow b$.

En VANET, une voiture doit d'abord abonner auprès d'un fournisseur de services SP. La voiture se voit attribuer une paire de clés publiques et privées à l'inscription. Pour chaque

intervalle de temps le SP a une clé publique PK_{SP} (ti). Selon le contrat d'abonnement, le SP assigner une série de ré-cryptage clés de $ReKey_{CAR}$ (ti) correspondant à des créneaux horaires dans la durée d'abonnement, par lequel la voiture peut recrypter un message crypté à l'origine par la clé publique du SP à générer un texte chiffré par sa propre clé publique.

Le processus d'authentification est représenté dans la figure 4.7. Pour la première étape, la voiture envoie une demande d'authentification à l'AP détectée dans sa gamme. Le message de demande contient juste le temps de t demande et un nombre aléatoire n1: <t1,n1>. Après l'AP reçoit ce message, il compare le temps t1 offert par la voiture de sa propre horloge. Si le temps est considéré comme étant dans l'écart normal, le point d'accès envoie un message à la voiture. Le message constitue un nouveau nombre aléatoire n2 chiffré par la clé publique du SP de l'intervalle de temps correspondant à t1: < (n2) PK_{SP} (t1)>.

Après que la voiture reçoit la réponse, il utilise la clé de nouveau chiffrement correspondant à t1 à ré-crypter le message. Le résultat est donc disponible pour elle à déchiffrer à l'aide de sa propre clé privée, et le n2 est révélé. Il prend alors n1 et n2, les combine par un certain algorithme de cryptographique E connue pour les deux parties pour produire E (N1, N2), et l'utilise comme une clé symétrique pour crypter un mot-clé de succès comme la preuve d'authentification.

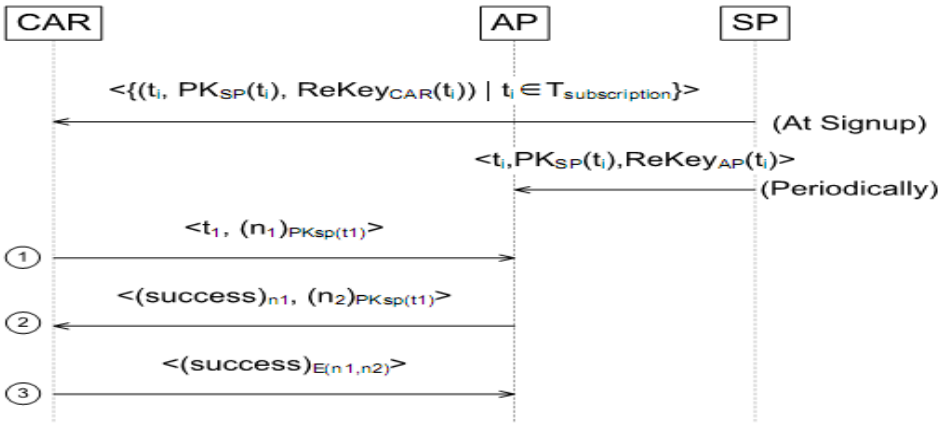


Fig. 4.9 Authentification en utilisant Proxy Ré-cryptage

Le message chiffré est renvoyé à l'AP séparément, ou la voiture peut également choisir de commencer à envoyer des paquets de données, avec la preuve d'authentification greffée au premier paquet de données. Après l'AP vérifie le message par le décryptage en utilisant l'algorithme E (N1, N2), une connexion sécurisée et de confiance est établi. La clé de session E (N1, N2) est utilisée pour sécuriser la transmission des données suivantes.

Pour l'AP à se montrer comme autorisée, elle doit répondre à un défi comme il effectuer à la voiture. A cet effet, l'AP a besoin d'obtenir du temps liés à touches nouveau chiffrement avec des clés publiques du SP de façon périodique. Lorsque la demande d'authentification de voiture initie, en plus de l'horodatage, le nonce n1 est chiffré par la clé publique de la SP comme un défi. Après l'AP reçoit la demande, il peut utiliser de nouveau chiffrement à régler le problème. Dans le message de réponse, outre le message de défi à la voiture, il comprend la preuve de la capacité de ré-cryptage par un tag succès chiffré à l'aide n1 comme une clé symétrique. La voiture peut alors utiliser n1 de révéler le mot-clé et de valider l'AP.

4.2.6 Anonymisation centrale d'utilisateur RSSI pour la Localisation de la confidentialité dans réseaux véhiculaires

Dans cet article la méthode proposée [WCS10] baser sur la puissance de signal reçue RSSI (Received Signal Strength Indicator) base de modèle anonymisation centrée sur l'utilisateur, ce qui peut considérablement améliorer la confidentialité de la localisation et en même temps assurer la sécurité routière.

La méthode proposée :

L'idée d'approches basées sur l'identité anonymat et de rendre les véhicules non identifiables. Il existe deux modèles de base pour les approches basées sur l'identité anonymat: l'un est énorme base clé anonymes " huge anonymous keys based"(HAB), l'autre est une technique de signature de groupe basée (GSB).

En HAB, sur l'unité de conseil "on board unit" (OBU) stocke un grand nombre de touches anonymes, qui sont signées par les CA et utilisées pour signer les messages de sécurité. En changeant la clé de signature en permanence, il devient plus difficile de suivre les véhicules. Le principal avantage de HAB est sa simplicité et sa franchise. Toutefois, il a quelques problèmes: l'un de ces problèmes est que OBU a besoin d'un grand espace de rangement pour les clés anonyme, l'autre est que la gestion des clés va devenir un problème. En outre, le traitement d'une longue liste de révocation de certificats (CRL) prendra un long moment. L'idée maîtresse est de permettre à un membre du groupe de signer des messages de façon anonyme au nom du groupe. Les avantages de la GSB sont de deux ordres: il réduit le nombre de touches anonyme et il a une liste plus courte de révocation. Mais le temps de vérification des messages de sécurité augmente linéairement avec le nombre d'identités révoqué dans la liste de révocation.

En intégrant des approches HAB et GSB, on trouve un système hybride. Dans ce régime, chaque véhicule est équipé d'une clé de signature de groupe et une touche de groupe public. Un véhicule génère son propre jeu de clés anonymes hors ligne. Ces touches sont signées par le propriétaire du véhicule de la clé privée, celle-ci est signée par l'CA afin de garantir sa validation. Avec cette méthode, les touches anonymes du véhicule peuvent être générées à la volée et l'auto-certifié. On a aussi un mécanisme similaire, appelé PKI +, qui a les avantages des méthodes traditionnelles HAB, mais a une taille plus petite de la CRL.

En résumé, l'utilisation des méthodes ci-dessus peuvent assurer la confidentialité et l'intégrité des messages, mais tant que les véhicules ont besoin de diffuser des messages régulièrement pour des raisons de sécurité, elles sont toujours identifiables en surveillant les mouvements et l'identification profil de renseignements sur le véhicule. Par conséquent, HAB et GSB n'assurer pas toujours l'intraçabilité du mouvement du véhicule.

Méthodologie :

Afin de rendre le travail correctement la méthode qui été proposée, comme suit:

- Tous les véhicules sont équipés d'un système de navigation GPS.
- Une infrastructure à clé publique est disponible dans le réseau de véhicules.
- Les pseudonymes ont une durée de validité courte et ne peut pas être réutilisée.
- Les véhicules diffusent régulièrement leurs positions, vitesses et directions au réseau pour des raisons de sécurité et ils enregistrent ces données dans leurs propres Enregistreur de données (EDR).
- Il existe bien des tiers de confiance, qui sont conformes aux politiques de confidentialité et de garder trace de la correspondance entre les pseudonymes et de l'identité réelle du conducteur correspondant.

Le modèle R-anonymat :

L'idée de base du modèle R-anonymat est d'utiliser une méthode de la distance métrique pour préserver la confidentialité de la localisation, tout en maintenant la sécurité routière. La confidentialité est préservée par perturbation sélective des valeurs réelles (basé sur le niveau de risque) des positions des véhicules, les directions et les vitesses. Cette distribution donnée va empêcher précisément l'adversaire qui suive une véhicule ciblé.

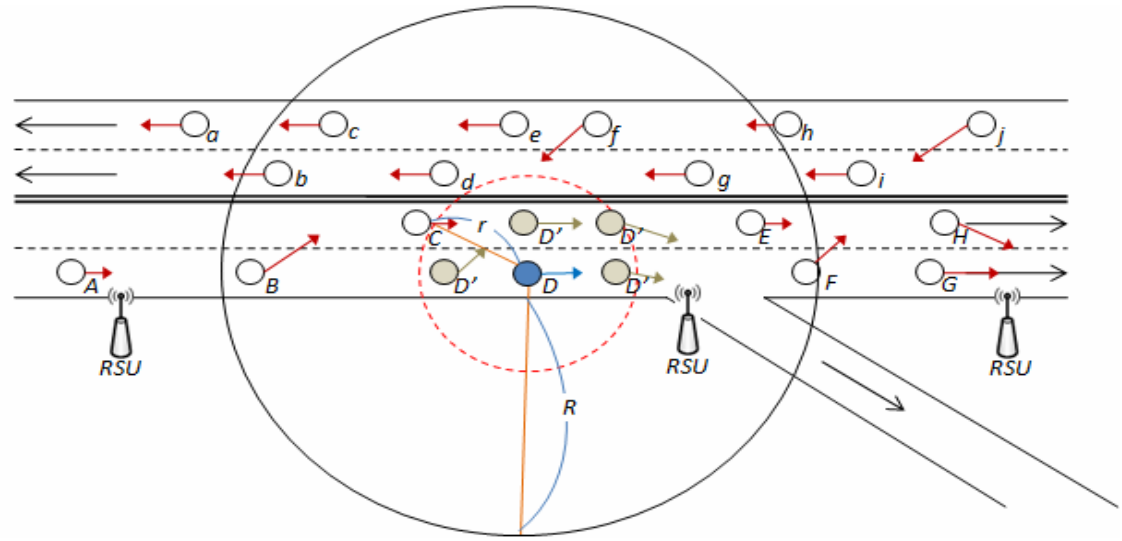


Fig. 4.8 Illustration d'un modèle de R-anonymat dans pseudo position, direction et vélocité

Le diamètre de transmission sans fil de véhicule D est R et C est le véhicule le plus proche du véhicule D avec la distance r. Le poste proposé pseudo D' sera diffusé au lieu de D, où D' est dans le cercle de centre D de diamètre r. La valeur de D' est choisi de manière que la position pseudo n'affectera pas la sécurité de la circulation. Il est clair que plus la distance du véhicule le plus proche, la plus grande plage de variation de pseudo positions on pourrait l'utiliser. Par conséquent, comme on fait il est plus difficile pour l'adversaire de suivre la position correcte, on peut augmenter la confidentialité de la localisation du véhicule D.

Radio Signal Strength Indication (RSSI)

La méthode de la puissance des signaux reçus (RSSI) est la plus connue pour fournir une estimation de distance entre les véhicules avec un cout faible. Le bénéficier de cette méthode est que son implémentation est très simple, et elle est utiliser par les applications de localisation et de traking avec une estimation d'erreur un peut faible autour de 4.1 m, Comme on a besoin d'un paramètre à être utilisé comme une semence et une équation simple et rapide pour garantir l'anonymat des VANET, le RSSI de proposer un modèle anonymat centrée sur l'utilisateur, que nous appelons R-Anonymat. Parce que les véhicules sont dans le mode de conduite, leur sens de déplacement, vitesse et accélération varient, donc la force des signaux reçus du véhicule sont en constante évolution.

$$\boldsymbol{RSSIij = -(10\,log\,10\,dij + A)}$$

- $RSSI_{ij}$ indique la puissance radio du nœud i au nœud j,
- i est l'émetteur, et j est le récepteur,

- n est l'exposant de perte de trajet selon les caractéristiques de chaque réseau,
- d_{ij} est la distance entre i à j,
- et A est le signal reçu force à 1 mètre de distance.

Pour des fournisseurs différents, la gamme de valeur de RSSI est définie différemment. Par exemple, Cisco utilise une plage de 0 à 100 en leurs appareils, tandis que les chipsets basé Atheros basé utilisent une plage de 0 à 60. De ce dernier il utilise les indicateurs RSSI dans 0 à 1.

Comme $RSSI_{max}$ peut être utilisé pour représenter la distance entre les véhicules trackés et le véhicule le plus proche, il utilise pour calculer une pseudo-valeur pour être utilisées dans le modèle R-anonymat. Autrement dit, le calcul de la pseudo-valeur dépend de la valeur de $RSSI_{max}$. La force radio est inversement proportionnelle à la différence de distance entre la valeur réelle et la pseudo-valeur, ce qui signifie que lorsque la force de radio est faible, il n'ya pas de véhicule, à proximité du véhicule tracké. Ainsi générer la pseudo-valeur avec de grandes différences avec la position réelle pour maintenir ce véhicule difficile à tracker.

$$R_d = X * 10^{-(RSSI_{max})/10n} / C_R \ , \ -1 \leq X \leq 1$$

Dans l'équation (2),

- R_d est le rapport toléré de la distance par rapport à la valeur actuelle $RSSI_{max}$,
- X est une valeur aléatoire entre -1 à 1,
- CR est la portée de transmission maximale d'un dispositif VANET.

Avec le calcul de la R_d, nous pouvons fournir quatre types d'amélioration de la confidentialité: pseudo-position, pseudo-direction, la pseudo-vitesse et la période silencieuse pseudo-aléatoires, nommés respectivement R-pseudo position, R-pseudo direction, la vitesse R-pseudo et R-Random de la période silencieuse.

Conclusion :

Dans ce chapitre on a représenté les différentes techniques qui existes pour la vérification de la position dans les VANETS ;

On peut conclure qu'il ya plusieurs techniques et que chaque technique a ces paramètres, ces avantages et ces inconvénients.

Tous ce qu'on a vue dans ce chapitre est résumer dans un tableau comparatives.

	[BBC06]	[YOW07]	[GKC07]	[GKS10]	[MAH10]	[WCS10]
l'utilisation de GPS	Oui	Non (utilisée d'autre capteurs)	Oui	Oui	Non	Oui
Utilisation des messages périodiques	Oui	Oui	Oui	Oui	Oui	Oui
Nombre des messages	Elevé	Elevé	Elevé	Elevé	Elevé	Elevé
L'authentification	Non	Oui	Non	Non	Oui	Oui
Type de Cryptographie	/	/	/	/	Avec clé public et privé	Avec clé privé et clé public pour l'infrastructure
Principe	il est repose sur le contrôle de la puissance du signal des balises périodiques. Et calcule de la distance réelle et la distance calculer d'après la position revendique.	Cette méthode est basée sur l'utilisation des capteurs telle que ces capteurs va vérifier et décider si un nœud est considérée est malveillant ou non, on utilise un modèle de confiance qui offre les capacités nécessaires pour tenir compte des observations provenant de capteurs différemment pondérés pendant une certaine période de temps.	Dans ce projet on utilise le GPS et le radar. l'utilisation du radar accroîtra sensiblement le montant de confiance qui peut être donnée l'information de positionnement reçues.	Chaque nœuds reçoit un paquet d'un nœud voisin il vérifier la position par une des méthodes de vérification; Si la position revendiquée de l'expéditeur et sa position estimée par match récepteur ; il génère l'observation et transmet les paquets à ses nœuds voisins. Sinon, le récepteur rejette le paquet	Le régime d'authentification dans les VANET dit que chaque nœud doit d'abord abonner auprès d'un fournisseur de services SP. La voiture se voit attribuer une paire de clés publiques et privées à l'inscription. Pour chaque intervalle de temps le PS a une clé publique PKSP(ti).	L'idée d'approches basées sur l'identité anonymat est de rendre les véhicules ne sont pas identifiables. Après on utilise l'approche de vérification de position en utilise la puissance de signal.

Table comparative des techniques de vérification de position étudiée

Chapitre 5

Simulations et analyse

Introduction

Le développement des technologies de l'information et de la communication a mis à la portée du secteur éducatif une très importante diversité de ressources et de supports. De ce fait, exploiter ces différentes ressources nécessite une étude des besoins pour déterminer leur forme d'utilisation.

La simulation permet d'analyser des phénomènes réels et de prévoir des résultats à partir de l'application d'une ou plusieurs théories à un niveau d'approximation donné. Aussi, elle désigne un procédé selon lequel on exécute un programme informatique sur un ordinateur en vue de simuler.

Pour évaluer les performances des techniques présentées dans le chapitre précédent, nous avons effectué des simulations avec le simulateur (Network Simulator) NS2 tout en utilisant un modèle de mobilité de type FREEWAY.

Dans ce chapitre, on donnera une présentation générale du simulateur NS2, et du modèle de mobilité utilisée dans notre travail. Ensuite, nous présenterons les paramètres et les métriques utilisés. Nous terminerons ce chapitre par l'analyse des résultats obtenus avec une comparaison des techniques simulées.

5.2 Network Simulator 2 :

5.2.1 Définition

NS-2 (Network Simulator 2) est un simulateur open source utilisé dans les recherches liées aux réseaux de communication d'ordinateurs. Il est très populaire car il est à accès libre. Cet outil a été proposé par l'université de Californie du Sud en 1995. Il est principalement développé avec les idées de la conception par objets, de réutilisabilité du code et de modularité. Il est devenu aujourd'hui un standard de référence en ce domaine. Le simulateur se compose d'une interface de programmation en tcl et d'un noyau écrit en C++ dans lequel la plupart des protocoles réseaux ont été implémentés.

NS2 utilise le langage OTCL (Object Tools Command Language), dérivé objet de TCL. À travers ce langage, l'utilisateur décrit les conditions de la simulation : topologie du réseau, caractéristiques des liens physiques, protocoles utilisés, communication…etc. La simulation

doit d'abord être saisie sous forme de fichier texte que NS utilise pour produire un fichier trace contenant les résultats.

NS-2 est écrit en C++ avec une interface textuelle (ou shell) qui utilise le langage OTCL. Le langage C++ sert à décrire le fonctionnement interne des composants de la simulation. Pour reprendre la terminologie objet, il sert à définir les classes.

Les principales classes utilisables pour définir l'architecture et la topologie du modèle sont les suivantes :

a. **Nœuds** :

Les nœuds représentent les différentes machines du réseau, qui peuvent être des postes fixes, des routeurs, des nœuds mobiles, …etc. et se créent en tapant : set n0 [$ns node] (pour créer un nœud « n0 »).

b. **Lien :**

Le lien est un autre composant principal du réseau sert à relier les nœuds. Il modélise le système de transmission. Le lien est principalement caractérisé par un délai de propagation et une bande passante. C'est une classe OTCL qui regroupe un ensemble de composants.

c. **Agent** :

Les agents représentent des points terminaux où les paquets de la couche réseau sont produits ou consommés. Cette classe est à la fois dans l'interpréteur et dans le simulateur. C'est la classe de base pour définir des nouveaux protocoles dans NS. Elle fournit l'adresse locale et celle de destination et les fonctions pour générer les paquets. Actuellement NS comporte de nombreux agents citons: UDP, protocoles de routage, différentes versions de TCP, RTP, etc.

5.2.2 Éléments de la simulation:

a. **Simulateur :**

La simulation est configurée, contrôlée et exploitée via l'interface fournie par la classe OTCL Simulator. Elle n'existe que dans l'interpréteur. Un script de simulation commence toujours par créer une instance de cette classe par la commande: set ns_ [new Simulator].

b. Ordonnanceur (scheduler) :

L'ordonnanceur est défini dans le fichier scheduler.{h,cc}. L'ordonnanceur se charge de choisir l'événement le plus proche en termes de temps, d'exécuter les traitements, de faire progresser le temps de simulation et d'avancer à l'événement suivant etc. Un seul événement est traité à la fois. Si plusieurs événements doivent être traités au même instant. Ils sont exécutés en série mais au même instant en termes de temps simulé.

c. Consommation de temps :

Aucun objet dans la simulation ne peut faire avancer le temps. Pour consommer du temps, il faut obligatoirement passer par l'ordonnanceur.

d. Traitement séquentiel en temps simulé :

Le temps de simulation est découplé du temps réel. Si aucun objet ne fait de consommation de temps, vis à vis du temps simulé tous les traitements se font en même temps (mais par rapport au temps réel ils sont exécutés en série). Un simulateur est naturellement une machine pseudo-parallèle.

5.2.3 Le générateur "IMPORTANT" des modèles de mobilité :

Le modèle de mobilité est un facteur très important pour déterminer la performance d'un protocole dans les réseaux mobiles. Le modèle RWP (Random WayPoint) est le plus utilisé dans les simulations des MANET. Le nœud+ mobile utilisant ce modèle se déplace vers une destination avec une vitesse aléatoire sélectionnée entre $[0,V_{Max}]$ où V_{Max} est la vitesse maximale. Lorsque le nœud atteint sa destination, il marque un temps de pause, puis, il reprend son déplacement, jusqu'à la fin de la simulation.

Dans les VANET, les nœuds mobiles (les véhicules) ne se déplacent pas d'une façon aléatoire, mais, en suivant des routes unidimensionnelles ce qui, fait que le modèle RWP n'est pas approprié pour ce type de réseau. Pour cela, un modèle alternatif pour les VANET est nécessaire afin que les simulations dans ce type de réseau soient réalistes. Une équipe de recherche de l'université USC (University of Southern California) a proposé, dans le cadre du projet MARMALADeS (Multicast and Resource Management for Large-Scale Ad-hoc and Sensor Networks), un générateur de mobilité pour les VANET appelé IMPORTANT [HSA05]. Ce générateur est capable de générer beaucoup de modèles pour les VANET comme les modèles Freeway et Manhattan.

5.2.4 Le modèle de mobilité Freeway:

Le modèle Freeway est l'un des modèles qui peut être généré par IMPORTANT, il simule le comportement de mouvement des nœuds véhicules sur une autoroute. Il peut être aussi utilisé dans l'échange de trafic ou dans le suivi d'un véhicule sur une autoroute.

Dans ce modèle, nous utilisons des cartes qui comportent généralement plusieurs autoroutes et chaque autoroute se compose d'une ou plusieurs voies dans les deux directions.

Les différences entre le modèle de mobilité Freeway et les modèles aléatoires sont les suivantes :

- Chaque véhicule est restreint par sa voie de l'autoroute et il ne peut pas la changer durant la simulation.
- La vitesse du véhicule (à l'instant t+1) dépend temporellement de sa vitesse précédente (à l'instant t) selon la formule suivante :

$$vitesse_i\ (t + 1) = vitesse_i\ (t) + random\ () * accélération_i\ (t).$$

- Une distance de sécurité (d) est maintenue pour qu'aucun véhicule ne puisse pas dépasser la vitesse de celui qui le précède. Cette distance est définie comme suit :
  Si $distance_{i,j}\ (t) < d \Rightarrow vitesse_i\ (t) < vitesse_j\ (t)$, Si j est avant i dans sa voie.

En raison de ces caractéristiques, le modèle de mobilité Freeway assure une dépendance spatiale et une haute dépendance temporelle. Il impose également des restrictions géographiques strictes sur le mouvement des nœuds en ne permettant pas à un nœud de changer sa voie.

5.2.3.1 Les étapes de création d'un fichier de mobilité :

Une fois le programme freeway.ccp est compilé et exécuté, il demande à l'utilisateur d'entrer les informations suivantes :

- Le nombre de véhicules participant à la simulation.
- L'accélération de la vitesse des véhicules (par exemple si cette valeur est égale à 10% de la vitesse, donc: l'accélération = vitesse Max* 0.1).
- Le chemin du fichier qui décrit la carte de l'autoroute (voir l'annexe pour le format de ce fichier). Donc, c'est un fichier d'entrée pour le générateur IMPORTANT.

- Le chemin du fichier qui va être créé pour contenir le modèle de mobilité, ce fichier va être utilisé par NS 2 (voir l'annexe pour le format du fichier de mobilité). Donc, ce fichier est un fichier de sortie pour IMPORTANT et un fichier d'entrée pour NS 2.

5.3 Métriques d'évaluations :

Les scénarios de simulation que nous avons utilisée, nous ont permis de proposer et d'utiliser des métriques importantes pour l'évaluation de performances de notre simulation:

5.3.1. Erreur moyenne en mètre (ERRM):

Cette métrique désigne l'erreur moyenne des distances calculées par les coordonnées x ,y et par la puissance de signal au niveau du récepteur. Cette métrique est calculée selon la formule suivante :

$$ERRM = \frac{\sum_{i=1}^{k} ERRi^2}{k},$$

$$ERRi = Dc_{ij} - Dr_{ij}$$

k: Le nombre de nœuds dans le réseau.

Dc_{ij} : La distance entre le nœud « i » et le nœud « j » calculée par leurs positions réelles.

Dr_{ij} : La distance entre le nœud « i » et le nœud «j » calculée par l'utilisation de la puissance du signal reçu.

5.3.3 Nombre des nœuds malicieux (NM) :

Cette métrique désigne le pourcentage des nœuds malicieux dans le réseau. Pour calculer cette métrique on calcule l'erreur entre la distance calculé et la distance réelle et on prend en considération l'erreur de calcule, alors on limite l'erreur entre -10m et +10m comme suit :

$$ERRi = Dc_{ij} - Dr_{ij}$$

$$-10m <= ERRi >= 10m$$

Si $ERRi \in [-10, +10]$ alors le nœud n'est pas malicieux, sinon le nœud est malicieux ; on additionner le nombre des fois où on trouve le nœud est malicieux.

$$NM = \sum_{i=1}^{n} ERRi \quad tlq\ ERRi \notin [-10, +10]$$

N : le nombre des nœuds dans le réseau ;

5.3.4 Nombre de messages envoyés (NbrM) :

Cette métrique définit le nombre de messages "k" nécessaires pour calculer les positions des nœuds. Cette métrique est calculée en utilisant la formule suivante :

$$\sum_{i=1}^{k} Nbr_i$$

Nbr_i : Le nombre de messages envoyés par le nœud « i ».

5.4 Paramètres de simulation :

Nous avons évalué les performances de notre simulation dans différentes configurations : différents nombres de nœuds dans le réseau (20,40, 60, 80,100) et différentes vitesses.

Durant les simulations, nous avons utilisé deux variantes de mobilité. La première est la mobilité faible avec une vitesse entre 80 km/h et 100km/h. La deuxième est une mobilité assez forte avec une vitesse entre 80 km/h et 140 km/h.

Le tableau suivant résume la configuration de notre simulation et les paramètres utilisés :

Nombre des nœuds	20,40, 60, 80,100
Mobilité du réseau [Faible, Forte]	[80-100, 80-140] km/h
Longueur de l'autoroute	1 km
Nombre de voies	2
Portée de transmission	300 m
Modèle de mobilité	Freeway
Modèle de propagation	FREE-SPACE
Temps de simulation	60s
Nombre de nœuds malicieux	Entre 10%-30%

Tableau 5.1. Paramètres de simulation.

5.5 Résultats et analyses :

5.5.1 La puissance de signal :

Dans la simulation de la méthode de la puissance de signal on va simuler la proposition de Bin Xiao, Bo Yu et Chuanshan Gao « detection and localisation of Sybil nodes », cet article est publier le 26.09.2006 a Los Angeles, Californie, USA [BBC06].

Et on est parlée de cette technique dans la section 4 parties 4.2.1 et son détail, et après la simulation on obtiendra les résultats suivants :

5.5.1.1 L'erreur moyenne (ERRM):

Afin d'évaluer les solutions en terme de nombre de nœuds qu'on a pu calculer leurs positions, nous avons fait varié le nombre de nœuds de 20 à 100, et, nous avons obtenu les résultats graphiques ci-dessous :

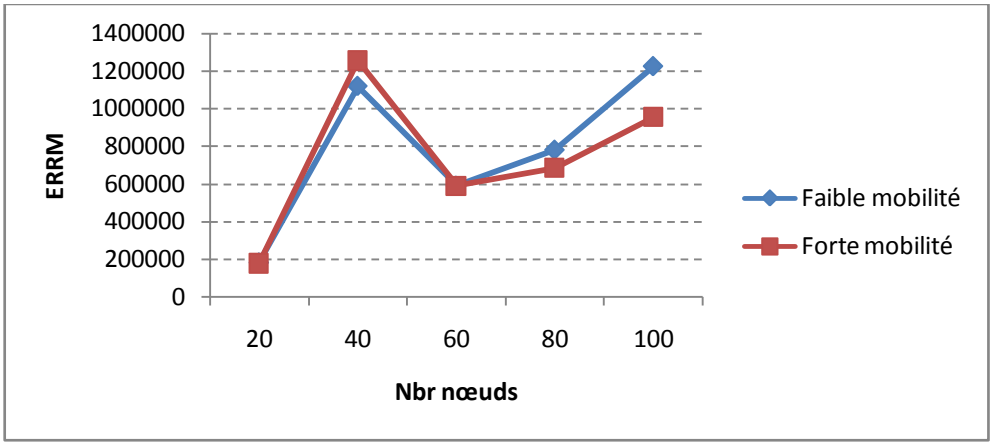


Fig. 5.1 : l'erreur moyenne en fonction de nombre des nœuds

Dans le cas de faible mobilité on remarque que le taux de l'erreur moyenne augmente c-à-dire le nombre des nœuds malicieux augmente pour un réseau de 40 nœuds et diminué pour 60 nœuds après le taux raugmenter pour 80 et 100 nœuds et la même chose pour le cas de forte mobilité.

5.5.1.2 Nombre des nœuds malicieux détecté:

Dans cette partie on est supposée qu'on a 10% des nœuds malicieux, 20%, et 30%.

On a évalue le nombre des nœuds malicieux calculés comme on a déjà vue dans 5.3.3, on obtient les résultats graphique ci-dessus :

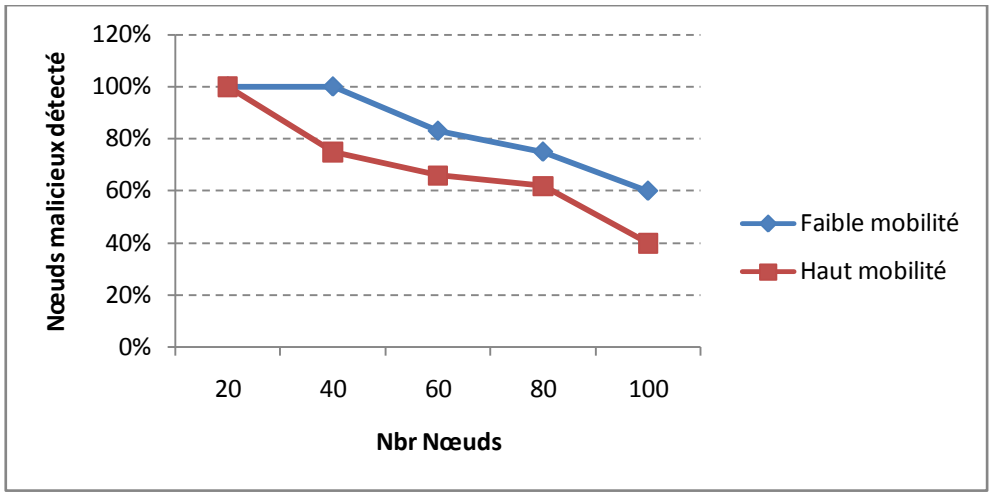


Fig. 5.2 : Nombre des nœuds malicieux en détectés (nœuds malicieux= 10%)

Pour 10% de nœuds malicieux dans le réseau, on a fait les simulations 5 fois avec une charge de réseau différente et pour les deux types de mobilité hautes et faible.

Le graphe montre que dans un réseau de 20 et 40 nœuds l'algorithme détecte presque tous les nœuds malicieux, pour un réseau de 60 et 80 nœuds il détecte de 85% a 75% de nœuds malicieux, et pour 100 enivrent de 60% pour faible mobilités.

Et pour la haute mobilité, pour 20 nœuds détecte 100%, 40 a 80 nœuds de 80% a 60%, et pour 100 nœuds 40% des nœuds malicieux détecter. Alors chaque fois que le nombre des nœuds augmente le nombre des nœuds malicieux augmente dans le réseau sa implique que la technique peut détecter un certaine nombre et pas tous les nœuds malicieux du réseau.

Pour 20% de nœuds malicieux dans le réseau, les résultats pour les deux cas mobilités hautes et faibles est représenté dans le graph suivant :

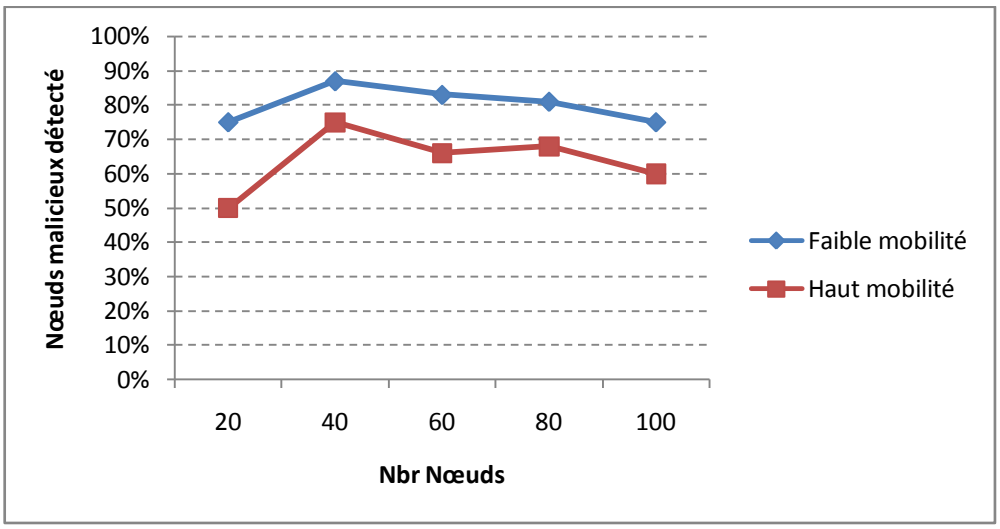


Fig. 5.3 : Nombre des nœuds malicieux en détectés (nœuds malicieux= 20%)

Dans un réseau de 20 et 100 nœuds l'algorithme détecte 75% nœuds malicieux, pour un réseau de40, 60 et 80 nœuds il détecte de 90% a 80% de nœuds malicieux, pour faible mobilités.

Et pour la haute mobilité, pour 20 nœuds détecte 50%, 40 60 et 80 nœuds de 75% a 65%, et pour 100 nœuds 60% des nœuds malicieux détecter.

Pour 30% de nœuds malicieux dans le réseau, les résultats est représenté dans le graph suivant :

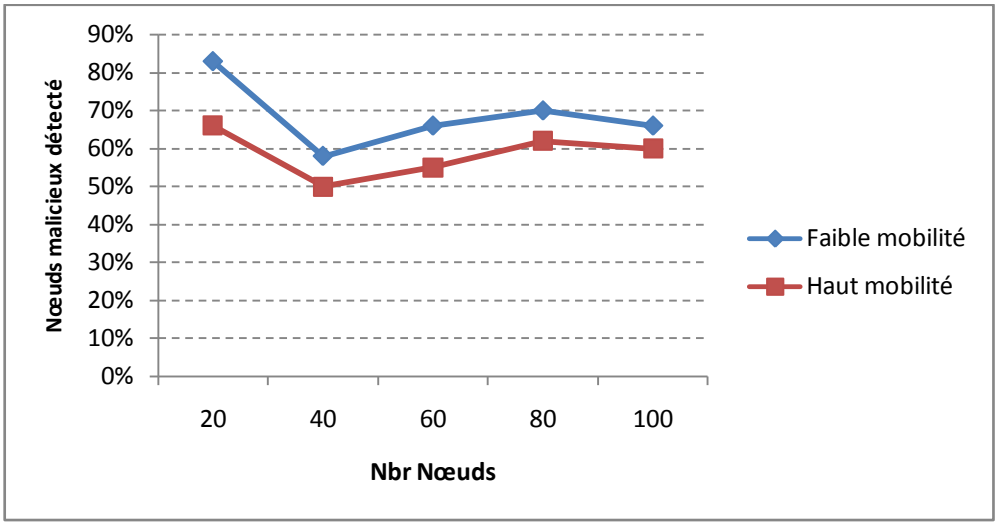


Fig. 5.4 : Nombre des nœuds malicieux en détectés (nœuds malicieux= 30%)

Pour un réseau de 20 nœuds l'algorithme détecte 85% nœuds malicieux, pour un réseau de40 nœuds il détecte de 55% a 60% de nœuds malicieux, et 60,80 et 100noeuds il détecte de 65% a 70%, pour faible mobilités.

Et pour la haute mobilité, pour 20 nœuds détecte 65%, 40, 60, 80 et 100 nœuds il détecte entre 50% et 65% des nœuds malicieux.

5.5.1.3 Nombre des messages envoyés :

Le nombre de messages échangés est un paramètre important qui permet de déterminer les performances d'un protocole. Pour cela, on a mesuré ce paramètre dans les différents scénarios de simulation.

Les courbes de la figure 5.5 montrent pour les deux cas de mobilité que le nombre de messages envoyés augmente à l'augmentation du nombre total de nœuds, ce qui confirme le bon fonctionnement de protocole simulé.

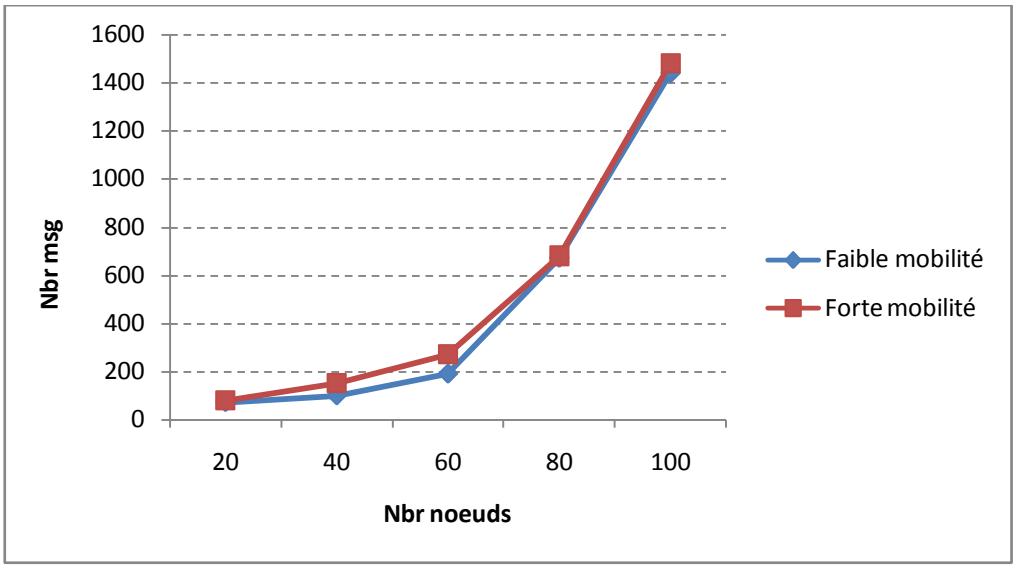


Fig. 5.5 : Nombre des messages envoyé en fonction de nombre des nœuds

D'après l'algorithme, chaque véhicule doit diffuser un massage pour calculer les distances par rapport à ses voisins. Donc, chaque fois qu'on augmente le nombre de véhicules dans l'autoroute le nombre de messages envoyés augmentera aussi.

5.5.2 L'authentification :

Dans la simulation de la méthode de l'authentification on a choisi la technique présenté dans l'article de Surabhi Mahajan et Alka Jindal « Security and Privacy in VANET to reduce Authentication Overhead for Rapid Roaming Networks», Chandigarh, India, 2010 [MAH10].

Le détail de cette technique est représenter dans la section 4 parties 4.2.5. Et on obtiendra les résultats suivants :

5.5.2.1 Nombre des nœuds non authentifié :

D'après la simulation de l'algorithme d'authentification, on a obtenu les résultats graphiques ci-dessous :

On remarque que pour le cas de forte mobilité les résultats de simulation montre que chaque fois on augmente le nombre des nœuds dans le réseau le nombre des nœuds non authentifiés augmente aussi par exemple pour 20 nœuds on a presque 25% de nœuds non authentifier, et aussi la même chose pour le cas de faible mobilité on trouve pour 20 nœuds 10% non authentifier et pour 80 nœuds 20% des nœuds non authentifier.

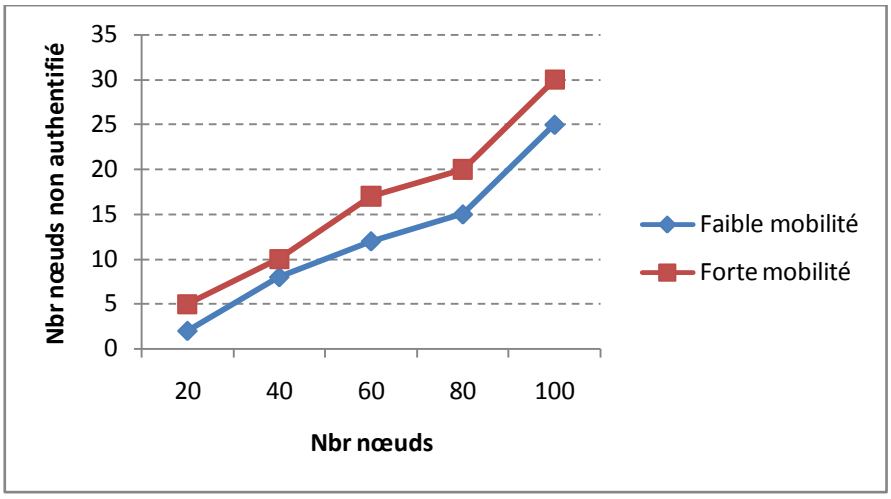


Fig. 5.6 : Nombre des nœuds non authentifié en fonction de nombre des nœuds

5.5.2.2 Nombre des messages envoyés :

Comme tous les protocoles de réseaux le nombre de messages échangés est un paramètre important dans le cas de l'authentification.

Pour cela nous avons représenté le nombre des messages échangés dans cette simulation dans le graphe c'est dessous :

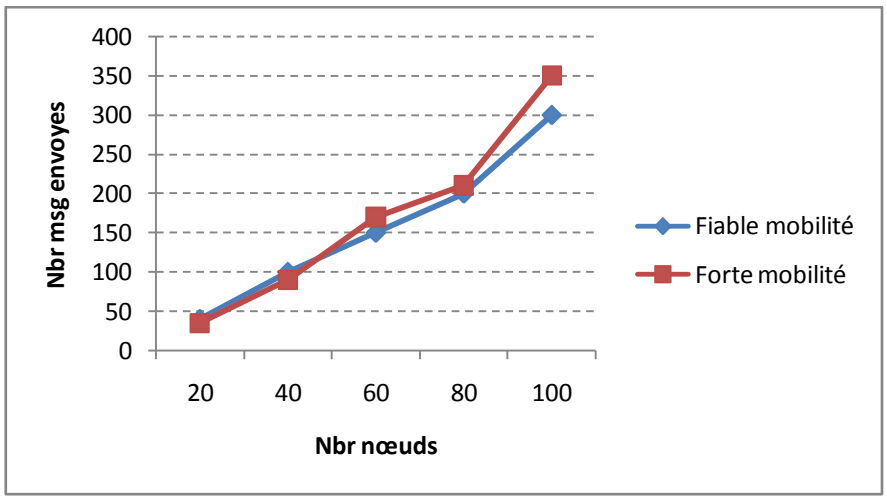


Fig. 5.7 : Nombre des messages envoyé en fonction de nombre des nœuds

On peut voir que le nombre des messages échanger augmenter avec l'augmentation de nombre des nœuds dans les deux cas forts et faible mobilité.s

5.6 Comparaison :

Après les résultats des simulations obtenues on peut résumer les conclusions dans le tableau suivant:

	Authentification	Puissance de signal
Nombre des messages	Élevé	Élevé
Détection des nœuds malicieux	Fiable et détecte presque tous les nœuds malicieux il détecte de 70% a 85% parmi les nœuds malicieux existes	Fiable mais il détecte entre 50% et 70% parmi les nœuds malicieux existes
Vérification de position	Ne vérifier pas la position et ne détecte pas la position de nœuds malicieux	Vérifier la position des nœuds et détecter la position réelle de nœuds malicieux

Conclusion :

D'après les résultats de simulation présentés précédemment, nous pouvons dire que les performances de les algorithmes de puissance de signal et l'authentification, qui peuvent détecter les nœuds malicieux dans un réseau sont très satisfaisantes et qui peuvent être très utile dans des applications qui nécessitent de la sécurité.

Conclusion Générale et perspective

Conclusion :

De nos jours, la voiture prend de plus en plus de place dans notre vie mais reste cependant le moyen de transport le moins sûr. La sécurité des automobiles devient une question importante et les constructeurs recherchent de nouveaux systèmes pour améliorer la sécurité à bord. La communication entre véhicules est une des solutions prometteuse qui va certainement réduire de 50% les accidents sur la route.

Les réseaux ad hoc de véhicules constituent un nouveau type de réseaux issu des réseaux ad hoc mobiles (MANET). Leur particularité provient des communications qui peuvent s'instaurer entre véhicules ou bien avec une infrastructure de stations de base. La mobilité est également largement plus contrainte que dans les réseaux ad hoc traditionnels.

Les réseaux véhiculaires sont vulnérables aux attaques menaçant la vie des usagers et les biens, donc la sécurité de ces réseaux est un pré-requis pour leurs déploiements. Les techniques cryptographiques peuvent assurer les objectifs de l'authentification, l'intégrité et la confidentialité dans une certaine mesure, mais la disponibilité est difficile à assurer car l'aspect décentralisé des réseaux VANET donne la possibilité d'avoir plusieurs attaques.

Dans ce travail, on fait une présentation des réseaux VANETs, comment localisée les nœuds dans ce réseau, comme on s'intéresse du problème de la sécurité et la détection des nœuds malicieux dans un réseau VANET on a représenté les différents types d'attaque existant pour ce réseaux et nous avons vu les principales approches existantes pour la vérification de position, leurs avantages et leurs inconvénients. Et nous avant choisi deux techniques parmis les techniques présenter et les simuler, l'une se base sur la puissance de signal et l'autre sur l'authentification.

Perspective :

Simuler les protocoles de vérification de position en utilisant d'autres techniques de localisation, par exemple au lieu d'utilisé la localisation par la puissance de signal on utilise le map matching ou bien d'autre technique.

Comparer les protocoles simulés avec des approches de même catégorie. Comme les approches qui se basent sur l'authentification on les compare entre. Et qui se base sur la vérification de position par les techniques de localisation…

Tester l'applicabilité des techniques évolutionnaires au problème de vérification des positions comme les réseaux de neurone…

Bibliographie

Bibliographie :

[ABD09] **R.ABDELLAOUI** «SU-OLSR Une nouvelle solution pour la sécurité du protocole OLSR. », École de technologie supérieure l'Université du QUÉBEC, 2009.

[AYB10] **I.Allama, R.Yahyaoui et Benslimane** «VANET : Clustering dans les réseaux de véhicules», l'Université d'Avignon, 2010.

[BBC06] **Bin Xiao, Bo Yu, Chuanshan Gao** «Detection and Localization of Sybil Nodes in VANETs », l'Université de Hong Kong Polytechnique, et l'Université Fudan China, 2006.

[BEN09] **S.Benkouider** « ÉTUDE DU PROBLÈME DE LOCALISATION DANS LES RÉSEAUX VANET », L'Université des Sciences et de la Technologie Houari Boumediene, 2009.

[BON07] **A.Boukerche, H.Oliveira, E.Nakamura et A. Loureiro «** Vehicular Ad Hoc Networks: A New Challenge for Localization-Based Systems», l'Université de Ottawa Canada, 2007.

[CER93] **Caroline Erickson «** Guide pour le positionnement GPS », Ministre des Approvisionnements et Services Canada, 1993.

[CAP08] **C.Cappel** «Localisation des véhicules et détection des obstacles apport d'un modèle virtuel 3D urbain », l'Université de science te technologie s de Lille, 2008.

[CLE09] **S.Clément**, « Quelques contributions dans les réseaux de capteurs sans fil : Localisation et Routage », l'Université d'Avignon, 2009.

[CHA10] **N.CHAIB** «La sécurité des communications dans les réseaux VANET », l'Université Elhadj Lakhder – BATNA, 2011.

[EVE07] **F.Evennou** « Techniques et technologies de localisation avancées pour terminaux mobiles dans les environnements indoor », L'UNIVERSIT´E JOSEPH FOURIER, 2007.

[GKS10] **J.Grover, D. Kumar, M. Sargurunathan, M.S. Gaur, et V.Laxmi** « Performance Evaluation and Detection of Sybil Attacks in Vehicular Ad-Hoc Networks »,Jaipur, India, 2010.

[GKC07] **Gyanesh Kumar Choudhary «** Providing VANET Security through Position Verification », Département d'informatique l'université de Old Dominion , 2007 .

[IWY08] **K.Ibrahim, M.C.Weigle et G.Yan «** Light-Weight Laser-Aided Position Verification for CASCADE», l'Université de Old Dominion Norfolk, 2008.

[LYB10] **N. Lagraa, M. B. Yagoubi1 et S. Benkouider «** Localization technique in VANets using Clustering (LVC) », Laboratoires d'Informatique et Mathématique; Université de Laghouat, Laghouat, Algeria, 2010.

[LSK06] **T.Leinmuller, D.E.Schoch et F.Kargil**, «POSITION VERIFICATION APPROACHES FOR VEHICULAR AD HOC NETWORKS», l'Université d'ULM, 2006.

[MAH10] **S.Mahajan «** Security and Privacy in VANET to reduce Authentication Overhead for Rapid Roaming Networks**»,** Chandigarh, India, 2010.

[PAL08] **N.C.Palomino «**Géo-localisation et poursuite dans un réseau mobile », l'Ecole Nationale Supérieure des Télécommunications, Paris, 2008.

[TCH08] **C.TCHEPNDA «**Authentification dans les Réseaux Véhiculaires Opérés », Paris, 2008.

[WAS05] **G.I.WASSI «** radiolocalisation en milieu confiné non stationnaire », l'Université de LAVAL, 2005.

[WCS10] **Y.Wei, Y.Chen, et H.Shan** «RSSI-Based User Centric Anonymization for Location Privacy in Vehicular Networks», Chunghwa, 2010.

[YOW07] **G.Yan, S.Olariu, et M.C.Weigle**« Providing VANET Security Through Active Position Detection», l'Université d'Old Dominion, 2007.

[EBE08] **L. ELAACHAK, A. BENSLIMANE**. « Communication inter-véhicules », Rapport de projet, Université d'Avignon IUP GMI, 2008.

[MDI10] **Mohamed el mehdi DIOURI** Mémoire d'ingénieur « Réseaux de capteurs sans fil: routage et sécurité » l'INSA de Lyon , 2010

[HKL10] **Hannes Hartenstein Kenneth P Laberteaux** VANET:Vehicular Applications and Inter-Networking Technologies - John Wiley & Sons Ltd, The Atrium, Southern Gate, Chichester, West Sussex, PO19 8SQ,United Kingdom. 2010.