Les systemes de transport intelligent (STI)

Benyamina Zakaria, Bounaama Fateh
Dept. Technologie, Université de Tahri Mohamed
Laboratoire d'Energarid
Bechar, Algérie

Benahmed khelifa
Dept. Science Exacte, Université de Tahri Mohamed
Laboratoire d'Energarid
Bechar, Algérie

Abstrait— La ville intelligente (smart city) désigne une ville utilisant les technologies de l'information et de la communication (TIC) pour améliorer la qualité des services urbains ou encore réduire ses couts. Dans ces villes intelligentes on trouve Les « systèmes de transport intelligents » (STI) qui sont des applications ou services avancés associant l'ingénierie des transports, les technologies de la communication, de l'information et du positionnement géographique. Il existe plusieurs types de réseaux informatiques assurant la communication entre les différents composants d'un STI, tel que la technologie de l'information et de communication à l'intérieur des véhicules et l'infrastructure des transports va révolutionner la manière de voyager aujourd'hui. Ces applications vous permettent la diffusion et la collecte d'informations utiles entre les véhicules et entre infrastructures et véhicules transport dans le cadre d'aider les conducteurs à voyager en toute sécurité et confortablement. L'objectif de ce travail est la présentation du travail compte tenu du temps réel et de communication fiable pour les réseaux véhiculaires.

Mot clès — Sécurité, communication; véhicule;Sous-Systeme; Système de Transport Intelligent

I. INTRODUCTION

Systèmes de transport évoluent vers les systèmes de transport intelligents (STI) et la dépendance des transports routiers dans nos vies quotidiennes a augmenté massivement au cours des dernières années, en ligne avec les problèmes découlant de son utilisation : la congestion sur les routes et les centres urbains, les pertes d'énergie, les émissions de CO2 avec pour conséquence l'impact sur la santé publique et des taux élevés d'accidents sur les réseaux routiers.

Des recherches récentes montrent que l'incorporation des technologies de l'information et de communication à l'intérieur des véhicules et l'infrastructure des transports va révolutionner la manière de voyager aujourd'hui.

Les technologies habilitantes sont destinées à réaliser les cadres qui stimuleront une gamme d'applications et de cas d'utilisation dans le domaine de la sécurité routière, l'efficacité du trafic et de l'assistance du conducteur. Ces applications vous permettent la diffusion et la collecte d'informations utiles entre véhicules et entre Véhicules et infrastructures de transport dans le cadre d'aider les conducteurs à voyager en toute sécurité et confortablement. Cependant, fiables et la communication en temps réel entre les véhicules et les infrastructures de transport sont encore des défis cruciaux et doivent être abordées pour la réussite de ces applications. Cet article est organisé comme suit. La section 2 fournit les applications de systèmes de transport intelligents (STI). La section 3 discute l'architecture avec les entités qui communiquent. En outre, les deux principales architectures de communication, l'un élaboré par l'Institut « Electrical and Electronics Engineers (IEEE) » et de l'autre par l'Institut «European Telecommunications Standard Institute (ETSI)», sont illustrés. La section 4 examine les défis de la sécurité dans les STI. La section 5 conclut le papier.

II. LES APPLICATIONS

Il y a des millions des véhicules autorisés sur les routes du monde et leur nombre ne cesse d'augmenter. Par conséquent, l'efficacité du trafic, réduisant la congestion et réduire les dommages liés aux accidents est devenu un défi majeur dans les villes. Cela a été progressivement amélioré dans la dernière décennie en employant les systèmes de transport intelligents (STI) et de l'information et de la communication (TIC). Dans STI systèmes véhicules peuvent communiquer avec d'autres véhicules à l'aide de véhicule à véhicule (V2V) de la technologie de communication ou par l'intermédiaire de l'Infrastructure technologies (V2I). Il existe deux types principaux d'STI applications notamment la sécurité et l'efficacité du trafic [1, 2]:

A. Les applications de sécurité routière

visent à réduire le risque d'accidents de voiture et à minimiser les dommages résultant d'accidents inévitables. Ces applications imposent des exigences, nécessitant un matériel fiable dédié ainsi que des communications fiables et opportunes. Ces applications comprennent la sensibilisation des coopératives, par exemple les applications de gestion des progrès, l'avertisseur de sortie de voie et à la gestion de la vitesse, ainsi que les applications de détresse, par exemple la détection des dangers et les mauvaises conditions météorologiques [3].

B. Les applications de l'efficacité du trafic

L'objectif principal de l'application efficacité du trafic est l'amélioration de la fluidité du trafic en réduisant le temps de déplacement et de congestion du trafic. Les avantages économiques et environnementaux peuvent également être obtenus. Ces

applications fournissent des informations sur le trafic à l'utilisateur, généralement diffusés par des infrastructures. Par ex. la gestion des véhicules de transport de marchandises dangereuses. Bien que ces demandes ne présentent pas les exigences de fiabilité et de délai strict, leur qualité se dégrade gracieusement avec l'augmentation du retard et la perte de paquets [4].

III. ARCHITECTURE

A. Sous-Systeme

Selon [5] Il existe quatre types d'entités qui communiquent dans le S-STI ((sous-systèmes-STI) (Fig. 1) :

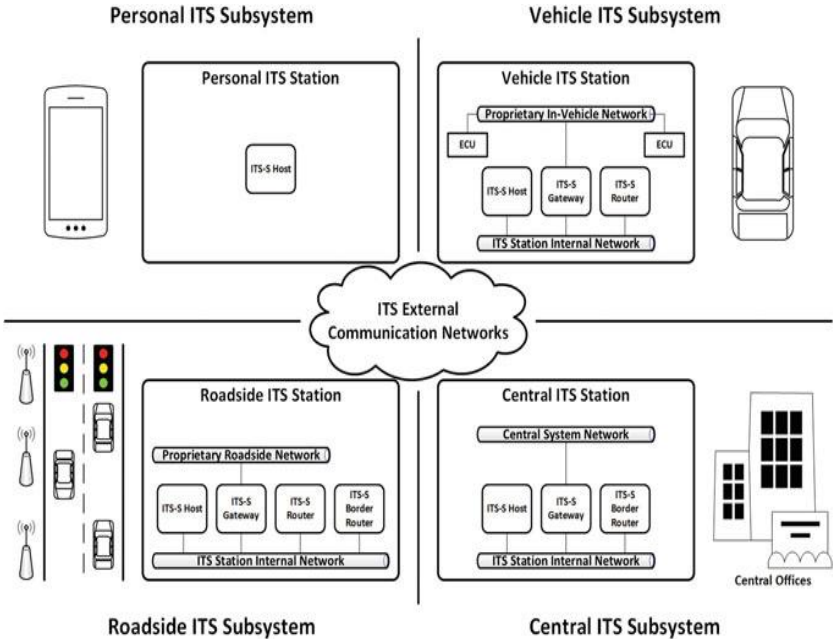

Figure 1. La communication de sous-systèmes européenne

- Vehicle: L'équipement à bord du véhicule (on board unit ou OBU) qui accueille ses applications. Ces applications peuvent recueillir des renseignements sur le véhicule et son environnement, de recevoir et/ou fournir des informations pour le conducteur, en partie ou entièrement contrôler le véhicule dans les situations critiques.
- Central : L'équipement Utilisé pour maintenir, surveiller et fournir des fonctionnalités pour les applications STI.
- Roadside: L'équipement installé sur le bord de la rue qui accueille les applications STI (RoadSide unit ou RSU). Ces applications peuvent recueillir des renseignements sur le flux de trafic routier et de l'environnement (par ex. météo), le contrôle de l'équipement de la route (p. ex., feux de circulation) et de communiquer avec le véhicule de S-STI pour fournir/recueillir de l'information.
- ITS station hôte : permet d'accéder à les applications STI à des fins personnelles, l'utilisateur (par ex. Smartphone avec un guidage routier application).
- Electronic control unit (ECU) : des petits ordinateurs responsables de la sécurité du véhicule et des passagers. Il gère donc des défauts sur ses capteurs et sur ses actionneurs.
- ITS station gateway: Permettent la connexion à des réseaux propriétaires, (par exemple, les réseaux du véhicule)
- ITS Station Routeur : Les routeurs S-STI S'interconnecter deux piles de protocoles STI différents au niveau de la couche 3 de modèle OSI, et sont capables de convertir les protocoles. Ils assurent la liaison avec d'autres S-STI (p. ex. vehicle ITS-S et roadside ITS-S)
- STI Station Border Router : les routeurs S-STI frontière près de fournir les mêmes fonctionnalités que les routeurs S-STI avec la différence que le réseau externe ne peut pas prendre en charge les mêmes principes de gestion et sécurité.

L'architecture de S-STI suit les principes du modèle OSI [6] Pour les protocoles de communication, et il a été étendu pour inclure les applications STI. L'architecture S-STI est illustrée à la Fig. 2.

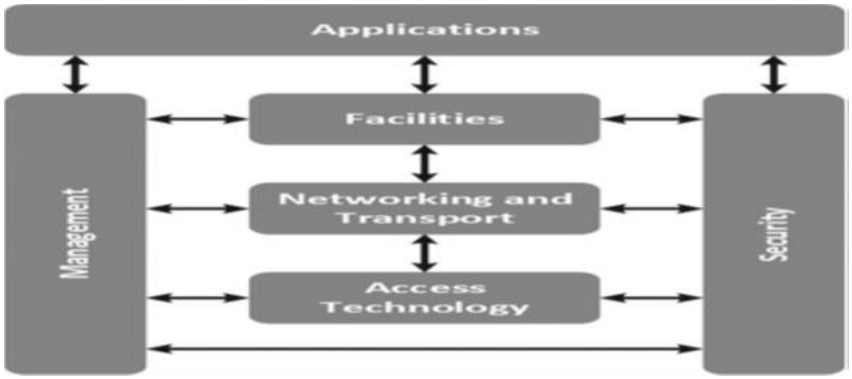

Figure 2. L'architecture S-STI

Dans L'architecture S-STI, les fonctionnalités des couches OSI 1 et 2 est représenté par le bloc "access", les couches 3 et 4 par le bloc "Networking & Transport", et des couches 5, 6 et 7 par les du bloc "Facilities".

Le bloc "Applications" représente les applications S-STI. Ceux-ci peuvent utiliser les services d'autres couches pour se connecter à d'autres applications S-STI .Ils fournissent des services à l'utilisateur de S-STI.

Le Bloc "Management" est en charge de la gestion des communications au sein de la station S-STI alors que l'entité "Sécurité" offre des services de sécurité

B. Réseaux

Les stations STI comptent sur des réseaux de communication pour la communication et la coopération. L'architecture réseau de STI est composée de réseaux internes et externes. Les types les plus pertinents de réseaux externes sont illustrés à la Fig. 3 [5].

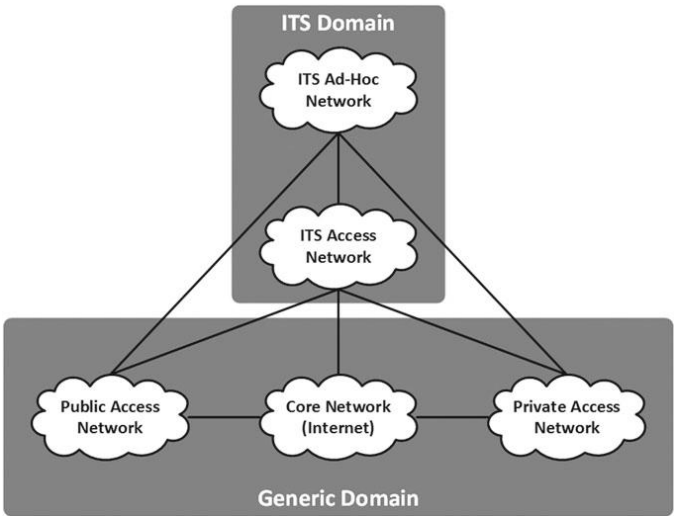

Figure 3. des réseaux S-STI externes.

"ITS ad-hoc networks" activer la communication directe entre les véhicules, RSU et les stations STI personnels au moyen de technologies sans fil à courte portée (EEE 802.11p). Ce type de réseau permet une plus grande mobilité et flexibilité sans la nécessité d'une entité de coordination.

"ITS access networks" habituellement déployées par les opérateurs privés, qui donnent accès à certains services et applications STI. Les véhicules peuvent communiquer entre eux via les stations routières qui sont reliés entre eux, au lieu d'utiliser un réseau ad hoc.

STI nécessite la communication sans fil entre véhicules et entre les véhicules et l'infrastructure routière. Les systèmes de communication des véhicules peuvent être plus efficaces pour prévenir les accidents de la route que le cas où les véhicules travailler individuellement pour atteindre le même objectif. Cela est dû à la coopérative des techniques qui peuvent être exploitées lorsque les véhicules et les stations routières ont l'information disponible sur d'autres parties (par exemple l'emplacement, la vitesse et la position). Comme un exemple de cette catégorie d'applications de sécurité, la chaîne collisions pourrait être évitée si les informations concernant le premier crash sont diffusées par tous les autres nœuds dans le secteur de l'accident. [5]

Les communications à courte portée (DSRC) est une technologie sans fil qui a été conçu pour soutenir une variété d'applications basées sur véhicule à véhicule (V2V) et l'infrastructure (V2I) des communications. Communications des véhicules pris en charge par les systèmes de DSRC fonctionnent dans la bande de fréquences 5.9GHz réservés et ont une portée maximale de 1000 m. Il y a deux principales architectures de protocole pour la communication, l'un élaboré par l'Institute Electrical and Electronics Engineers (IEEE), l'autre de l'Institut Telecommunications Standard Institute (ETSI), comme illustré en Fig. 4 [7].

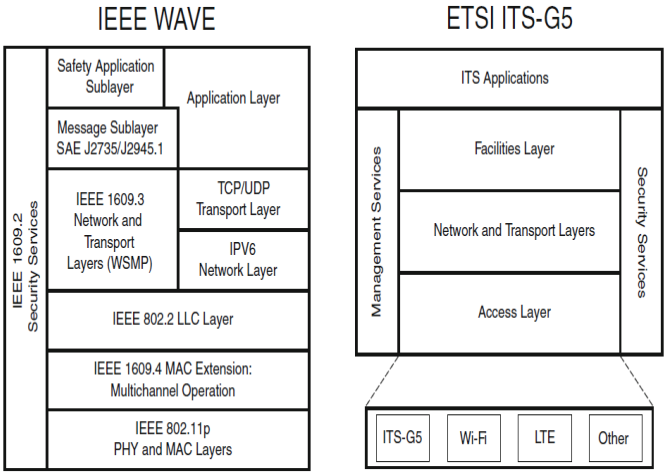

Figure 4. Les protocoles IEEE WAVE et ETSI ITS-G5.

Le développement de STI a été tiré par les scénarios d'usage que voir une grande mesure d'utilisation de la technologie des ondes radio, comme représenté dans Fig. 5.

Figure 5. Les scénarios STI [8].

L'interopérabilité et la capacité de traitement dans STI est basée sur les capteurs du véhicule, Ceux qui contrôlent par l'ECU:

- Radar : c'est un des nouveaux capteurs introduits dans les voitures de Google. Il y a quatre capteurs radar montés sur les boucliers avant et arrière [9]. Les capteurs radar sont utilisés pour l'affichage et de surveillance de la circulation rapide sur l'autoroute.
- Lidar : est le principal capteur utilisé dans la voiture de Google pour générer des cartes et de déterminer sa position et d'éviter ainsi les obstacles. Il s'agit d'un faisceau laser Velodyne 64 qui tourne autour et prend constamment des mesures de distance horizontale de la génération d'une carte en 3D de l'environnement [9]. Ces mesures sont ensuite comparées avec des illusions des cartes et des images prises de l'appareil photo, la génération de modèles de données qui permettent la conduite autonome.
- Ultrasonic sensors : peut être utilisé pour mesurer la distance aux objets à proximité du véhicule en stationnement.

- Un récepteur GPS : monté sur le haut de la voiture Google sans conducteur est utilisé pour déterminer l'emplacement de la voiture de participation des signaux envoyés par les satellites GPS.
- Caméras vidéo : enregistrer des images qui sont utilisées pour détecter des obstacles sur la route, lire les panneaux de signalisation et feux de circulation, de reconnaître des objets en mouvement comme les piétons et les cyclistes, de détecter et de garder la voiture sur la voie.
- Odometer: est utilisé pour mesurer la distance parcourue par le suivi de la position de la roue arrière.
- Onboard compute : est utilisé pour fusionner et analyser les données provenant des capteurs. Les informations générées par les capteurs utilisés pour contrôler le volant, l'accélérateur et les freins.[9]

IV. LES DÉFIS DE LA CYBER-SÉCURITÉ DE STI

A. Les cyber-attaques en STI

L'augmentation en ECUs a créé de nouveaux risques de sécurité. Des recherches antérieures ont démontré comment attaquer un réseau interne de la voiture, y compris la sécurité des éléments critiques tels que les freins et moteur [8][9]. Malgré tout cela, les constructeurs sont résistants et pas disposé à investir de grosses sommes d'argent dans la sécurité sans gains financiers. Exploits récents ont montré que les mécanismes de sécurité fournies par les fabricants de voiture sont de base et inadéquates. L'un des principaux arguments d'ignorer ces attaques, c'est qu'ils sont très peu nombreux comparativement au grand nombre de voitures qui ne sont pas compromis. Aussi certains chercheurs affirment qu'il n'est pas financièrement intéressant d'attaque dans les voitures. Un argument contraire à ceci est que le motive pour les hackers n'est pas seulement financière mais elle peut aussi être d'ordre politique ou de violence.

B. Les cyber-sécurité en STI

Les exigences de Cyber-sécurité sont définies selon les concepts clés suivants :

- Confidentialité : est la propriété de protéger l'information contre des entités, des systèmes ou des particuliers.
- Intégrité des données : est la propriété de maintenir l'exactitude des données provenant d'une source à sa destination.
- Authentification : est la propriété de la validation que les parties impliquées dans une transaction sont bien qui ils prétendent être.
- Disponibilité : est la propriété de fournir l'information à tous les moments où il est nécessaire.
- Le non répudiation : est la propriété de sorte qu'une partie à un contrat ne peut nier l'authenticité de leur signature sur un document.

C. Les menaces de sécurité

Dans cette section, nous décrivons certains exemples de la vulnérabilité connue dans les voitures modernes. Nous donnent un aperçu de la communication sans fil traditionnelles menaces, STI menaces. Initiatives de recherche ont démontré que les attaques sur les freins du véhicule ont été un succès. Le système de freins antiblocage (ABS) empêche la voiture de déraper si c'est dur de freinage. Avec un ABS pompes, le système de la pédale de frein et régule la pression hydraulique pour maintenir le blocage des roues, sans intervention humaine. Dans [10] Les auteurs ont été en mesure de verrouiller les freins individuels et ensembles de freins en envoyant des paquets aléatoires à l'ECU. Certaines voitures fera le freinage automatique préparer l'airbag et serrer la ceinture de sécurité. Toutefois, cela peut être compromis comme démontré dans [11]. Les auteurs ont utilisé un logiciel de surveillance d'isoler ont été en mesure de complètement ralentir ou même arrêter la voiture. En général, un déni de service et de contenu sont les principaux types de cyber-attaques contre des réseaux STI.

Le déni de service est le principal type de menace dans les communications sans fil. Dans une attaque DOS un réseau peut être rendu indisponible par des inondations et le spamming des paquets avec des faux messages qui absorbent toute la bande passante disponible. Un attaquant peut utiliser des logiciels malveillants d'infecter le réseau avec les logiciels, ou d'utiliser des moyens de gagner plus cupides débit que les autres utilisateurs. Le tableau 1 donne une liste des menaces existantes dans les communications sans fil.

TABLE I. LES MENACES DE COMMUNICATION SANS FIL

Denial of Service	***Autres menaces***
Spamming	False Message Injection
Malwar	Eavesdropping
Flooding	RF Finger printing
Jamming	Message Manipulation
Masquerade	Data sniffing
Blackhole	Wormhole

Des vulnérabilités dans STI et le résultat de ces attaques sont énumérés au tableau 2. Un bon exemple est l'attaque de brouillage GPS, brouilleurs GPS créer une bulle autour du véhicule, ce qui perturbe l'émetteur ou du récepteur.

TABLE II. LES MENACES EN STI

Menaces	***Résultats***
Replay attack	La falsification d'identité (vol)
Sybil Attack	Le vol d'identité
Bogus messages	Fausses alertes
GPS jamming	Faux Situation
Location Tracking	Violation de la vie privée
Denial of Service	Panne réseau
Vehicle sensor spoofing	défectueux des données du capteur
Malicious code Injection	La corruption de données
Man in the middle attack	erronées les données

V. CONCLUSION

STI est un système qui offre de nombreux avantages pour les conducteurs des véhicules, notamment la protection contre les accidents et l'efficacité des trafics routier grâce à la coopération entre les différentes entités du STI. Mais comme n'importe qu'el système, le STI maintient des faiblesses concernant les cybers sécurités, alors ces derniers ont besoin des études à l'avenir.

RÉFÉRENCES

[1] S. An,B.-H. Lee, D.-R. Shin,Asurvey of intelligent transportation systems, Dans la 3em Conférence internationale sur l'intelligence informatique, systèmes de communication et des réseaux, juillet

[2] R. Bossom, Deliverable D31 European ITS Communication Architecture—Overall Framework (2009)

[3] ETSI, ETSI EN302 637-2V1.3.2: Part2: Specification of Cooperative Awareness Basic Service (2014)

[4] ETSI, ETSI EN 302 637-3 V1.3.2: Part3: Specification of Decentralized Environmental Notification Basic Service (2014)

[5] L'ETSI, ETSI EN 302 665 V1.1.1 : Les systèmes de transport intelligents (STI)-Communications Architecture (2010)

[6] L'International Standard Organization. ISO/CEI 7498-1 (1994)

[7] IEEE Standard for Information Technology–Telecommunications and information exchange between systems local andmetropolitan area networks–Specific requirements Part 11:Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, IEEE Std 802.11-2012 (Revision of IEEE Std 802.11-2007), Mar 2012, pp. 1–2793

[8] Institut des télécommunications européen, systèmes de transport intelligents. http://www.etsi.org/ITS.2012

[9] IEEE Experimental security analysis of a modern automobile"In D. Evans and G. Vigna, editors, IEEE Symposium on Security and Privacy. IEEE Computer Society, May 2010.

[10] C. Miller, C. Valasek "Adventures in Automotive Networks and Control Units" illmatics.com/car hacking.pdf Retrieved 15th January 2014.

[11] Spectrum. "How Google's Self-Driving Car Works" spectrum.ieee.org. Retrieved 16th January 2014.