

Nom et Prénom : SABIR ZAKARIA

Date de soutenance : 13/11/2021

Directeur de Thèse : AMINE AOUATIF

Sujet de Thèse :

Voitures Connectées pour la Sécurité Routière : Sécurité des Réseaux de Données Nommées (NDN) en utilisant Blockchain

Résumé :

La sécurité routière est devenue un motif de recherche et de nombreux instituts de recherche ont investi dans ce domaine car beaucoup de personnes meurent et beaucoup d'autres sont blessées chaque année à cause des accidents de la route. Ces investissements ont conduit à une intégration continue de la technologie qui vise à améliorer l'efficacité et la qualité de vie dans les grandes agglomérations urbaines, tout en réduisant les coûts de leur gestion. Les villes deviennent de plus en plus intelligentes, ainsi des objets intelligents et différents capteurs sont déployés partout dans les villes.

Les véhicules modernes font partie des objets intelligents qui présentent plusieurs avantages. En effet, les voitures ne seront pas seulement connectées, mais aussi intelligentes, dotées de plusieurs interfaces réseaux, caractérisées par un stockage illimité et capables de traiter localement les données produites par les capteurs embarqués. Le déploiement de technologies de communication sans fil dans les réseaux de véhicules peut considérablement améliorer la sécurité routière. Il peut activer de nouveaux services tels que la gestion de la circulation, la détection des collisions et une facilité de communication supplémentaire entre les véhicules en mouvement. Cependant, les voitures connectées apportent aussi de nouveaux défis comme la mobilité, la diversité d'interfaces et la sécurité des données.

Dans les scénarios ad hoc de communications véhiculaires, il est impossible de supposer la disponibilité ou la dépendance à l'égard de l'infrastructure. De plus, les changements constants de connectivité qui caractérisent l'environnement de véhicules exigent également que les itinéraires soient recalculés et que les sessions soient rétablies à une fréquence assez élevée, ce qui est également considéré comme irréalisable. En revanche, un modèle de communication par demande/réponse utilisant des noms de données ne nécessite pas l'attribution d'adresses, ni la configuration des chemins de transmission des données ni l'établissement de sessions avant la transmission des données.

La communauté de chercheurs a pensé alors qu'un changement du paradigme IP centré sur l'hôte au paradigme ICN (Information-Centric Networking) centré sur le contenu est nécessaire. La famille des réseaux orientés contenus, en particulier l'architecture NDN (Named Data Networking), se considère ainsi comme une direction attrayante pour réussir les communications dans les réseaux véhiculaires. Dans cette famille, les mécanismes de sécurité sont appliqués au contenu lui-même plutôt qu'aux canaux de communication. Par conséquent, la livraison et la mise en cache du contenu ne nécessitent pas obligatoirement une sécurisation des communications.

Cette thèse analyse donc, dans une partie, les avantages et les défis de l'architecture NDN dans le domaine des voitures connectées, et prouve son efficacité contre l'architecture actuelle de l'Internet. Elle vise également à contribuer à la sécurité des communications véhiculaires en proposant un nouveau système qui utilise la technologie Blockchain avec un nouvel algorithme bio-inspiré.

Dans une autre partie, et dans le contexte du projet SAFEROAD lancé en partenariat avec le METLE (Ministère de l'Équipement, des Transports, de la Logistique et de l'Eau) et le CNRST (Centre National pour la Recherche Scientifique et Technique), cette thèse contribue à l'amélioration de la sécurité routière au Maroc en proposant une implémentation complète des communications V2V (Vehicle to Vehicle) et V2I (Vehicle to Infrastructure).

Mots-clés : Voitures Connectées, V2V, V2I, VANET, ICN, NDN, Sécurité, Blockchain, Cryptographie, Optimisation.

Abstract :

Road safety has become a reason for research and many research institutes have invested in this area because many people die and many others are injured every year due to road accidents. These investments have led to a continuous integration of technology that aims to improve the efficiency and quality of life in large urban areas while reducing the costs of managing them. Cities are becoming more and more intelligent, therefore smart objects and various sensors are deployed everywhere in the cities.

Modern vehicles are part of the smart objects that have several advantages. Indeed, cars will not only be connected but also intelligent, equipped with multiple network interfaces, characterized by unlimited storage, and capable of locally processing the data produced by onboard sensors. The deployment of wireless communication technologies in vehicular networks can significantly improve road safety. It can enable new services such as traffic management, collision detection, and additional communication facility between moving vehicles. However, connected cars also bring new challenges such as mobility, interface diversity, and data security.

In ad hoc vehicular communication scenarios, it is impossible to assume availability or dependence on the infrastructure. In addition, the constant changes in connectivity that characterize the vehicular environment also require that routes are recalculated and sessions are re-established at a quite high frequency, which is also considered infeasible. In contrast, a request/reply communication model using data names does not require the assignment of addresses, the configuration of data transmission paths, nor the establishment of sessions prior to data transmission.

The research community then believes that a shift from the host-centric IP paradigm to the content-centric ICN (Information-Centric Networking) paradigm is necessary. The family of content-oriented networks, in particular the NDN (Named Data Networking) architecture, is considered as an attractive direction for successful communication in vehicular networks. In this family, security mechanisms are applied to the content itself rather than the communication channels. Therefore, content delivery and caching do not necessarily require secure communications.

This thesis, therefore, analyzes, on one hand, the advantages and challenges of the NDN architecture in the field of connected cars, and proves its effectiveness against the current Internet architecture. It also aims to contribute to the security of vehicular communications by proposing a new system that uses Blockchain technology with a new bio-inspired algorithm.

On the other hand, and in the context of the SAFEROAD project launched in partnership with the METLE (Ministry of Equipment, Transportation, Logistics and Water) and the CNRST (National Center for Scientific and Technical Research), this thesis contributes to the improvement of road safety in Morocco by proposing a complete implementation of V2V (Vehicle to Vehicle) and V2I (Vehicle to Infrastructure) communications.

Keywords : Connected Cars, V2V, V2I, VANET, ICN, NDN, Security, Blockchain, Cryptography, Optimization.