Contributions to Wireless multi-hop networks : Quality of Services and Security concerns

Abderrezak Rachedi

Université Paris-EST

École Doctorale MSTIC
Mathématiques et Sciences et Technologies de l'Information et de la Communication

Habilitation à diriger des recherches

Discipline : Informatique

présentée par

Abderrezak Rachedi

Contributions to Wireless multi-hop networks : Quality of Services and Security concerns

---

Soutenue publiquement le 04/12/2015
devant le jury composé de :

M. André-Luc Beylot	Professeur INPT/ENSEEIHT	Rapporteur
M. Marcelo Dias De Amorim	DR CNRS -LIP6	Rapporteur
M. Samuel Pierre	Professeur Ecole Polytechnique Montreal	Rapporteur
Mme Francine Krief	Professeure ENSEIRB	Examinatrice
Mme Lynda Mokdad	Professeure Université Paris-Est (UPEC)	Examinatrice
M. Gilles Roussel	Professeur Université Paris-Est (UPEM)	Examinateur

Résumé

Ce document résume mes travaux de recherche conduits au cours de ces 6 dernières années. Le principal sujet de recherche de mes contributions est la conception et l'évaluation des solutions pour les réseaux sans fil multi-sauts en particulier les réseaux mobiles adhoc (MANETs), les réseaux véhiculaires ad hoc (VANETs), et les réseaux de capteurs sans fil (WSNs). La question clé de mes travaux de recherche est la suivante : « comment assurer un transport des données efficace en termes de qualité de services (QoS), de ressources énergétiques, et de sécurité dans les réseaux sans fil multi-sauts ? » Pour répondre à cette question, j'ai travaillé en particulier sur les couches MAC et réseau et utilisé une approche inter-couches.

Depuis l'an 2000, l'introduction de nouvelles normes de communication sans fil utilisant les bandes de fréquence ISM (Industriels, Scientifiques, Médicales) contribue au développement des réseaux informatiques sans fil. Aujourd'hui, c'est principalement l'accès à Internet qui est fourni via les technologies sans fil, telles que WiFi (IEEE802.11), WiMax (IEEE802.16), et UMTS/LTE (norme 3GPP) sur les terminaux (Smartphones, Tablettes, Ordinateurs portables, etc). Les mécanismes de base proposés par ces technologies permettent une communication sans fil à un seul saut entre le terminal et l'infrastructure réseau (Point d'accès). Un autre mode de communication appelé communication sans fil multi-sauts existe également et utilise des nœuds relais. Les communications sans fil multi-sauts représentent une part importante des technologies réseaux sans fil émergentes telles que les futurs réseaux sans fil de cinquième génération (5G) et l'Internet des Objets (IoT). Contrairement au système cellulaire conventionnel où toutes les communications passent par la station de base, un nouveau type de communication appelé communication d'objet-à-objet est introduit. Selon la portée radio, la communication entre les objets est assurée par une connexion directe ou bien par plusieurs relais. Les réseaux sans fil multi-sauts sont considérés comme une solution prometteuse pour étendre l'infrastructure du réseau sans fil sans déployer d'infrastructure supplémentaire d'une part ; et pour réduire l'important trafic réseau généré par les différents terminaux en utilisant le concept « offload » d'autre part. De plus, ils permettent d'améliorer la résilience du réseau, en particulier lorsque l'infrastructure n'est pas disponible, en cas de catastrophe naturelle ou de guerre par exemple. Nous distinguons deux types de communications sans fil multi-sauts : 1) les nœuds relais font partie de l'infrastructure et ils sont planifiés à l'avance (comme LTE, WiMax) ; 2) les nœuds relais ne font pas partie de l'infrastructure et jouent à la fois le rôle de routeur et de terminal. Nous ne nous sommes pas concentrés sur le premier type de réseau mais sur le deuxième.

Les réseaux sans fil multi-sauts présentent plusieurs problèmes liés à la gestion des ressources et au transport des données capable de supporter un grand nombre de nœuds, et d'assurer un haut niveau de qualité de service et de sécurité.

Dans les réseaux MANETs, l'absence d'infrastructure ne permet pas d'utiliser l'approche centralisée pour gérer le partage des ressources, comme l'accès au canal.

Contrairement au WLAN (réseau sans fil avec infrastructure), dans les réseaux Ad hoc les nœuds voisins deviennent concurrents et il est difficile d'assurer l'équité et l'optimisation du débit. La norme IEEE802.11 ne prend pas en compte l'équité entre les nœuds dans le contexte des MANETs. Bien que cette norme propose différents niveaux de transmission, elle ne précise pas comment allouer ces débits de manière efficace. En outre, les MANETs sont basés sur le concept de la coopération entre les nœuds pour former et gérer un réseau. Le manque de coopération entre les nœuds signifie l'absence de tout le réseau. C'est pourquoi, il est primordial de trouver des solutions pour les nœuds non-coopératifs ou égoïstes. Enfin, la communication sans fil multi-sauts peut participer à l'augmentation de la couverture radio. Les nœuds de bordure doivent coopérer pour transmettre les paquets des nœuds voisins qui se trouvent en dehors de la zone de couverture de la station de base.

Dans les réseaux VANETs, la dissémination des données pour les applications de sureté est un vrai défi. Pour assurer une distribution rapide et globale des informations, la méthode de transmission utilisée est la diffusion. Cette méthode présente plusieurs inconvénients : perte massive des données due aux collisions, absence de confirmation de réception des paquets, non maîtrise du délai de transmission, et redondance de l'information. De plus, les applications de sureté transmettent des informations critiques, dont la fiabilité et l'authenticité doivent être assurées.

Dans les réseaux WSNs, la limitation des ressources (bande passante, mémoire, énergie, et capacité de calcul), ainsi que le lien sans fil et la mobilité rendent la conception d'un protocole de communication efficace difficile. Certaines applications nécessitent un taux important de ressources (débit, énergie, etc) ainsi que des services de sécurité, comme la confidentialité et l'intégrité des données et l'authentification mutuelle. Ces paramètres sont opposés et leur conciliation est un véritable défi. De plus, pour transmettre de l'information, certaines applications ont besoin de connaître la position des nœuds dans le réseau. Les techniques de localisation souffrent d'un manque de précision en particulier dans un environnement fermé (indoor), et ne permettent pas de localiser les nœuds dans un intervalle de temps limité. Enfin, la localisation des nœuds est nécessaire pour assurer le suivi d'objet communicant ou non. Le suivi d'objet est un processus gourmand en énergie, et requiert de la précision.

Pour répondre à ces défis, nous avons proposé et évalué des solutions, présentées de la manière suivante : l'ensemble des contributions dédiées aux réseaux MANETs est présenté dans le deuxième chapitre. Le troisième chapitre décrit les solutions apportées dans le cadre des réseaux VANETs. Enfin, les contributions liées aux réseaux WSNs sont présentées dans le quatrième chapitre.

Mots-clefs

Réseaux mobile ad hoc (MANETs), Réseaux ad hoc véhiculaires (VANETs), Wireless Sensor Networks (WSN), QoS, Accès au canal de communication, Protocoles de routage, Modèle de confiance, Security, nodes malicieux et égoïstes.

Contents

Chapter 1

Introduction

The aim of this document is to summarize my research work conducted during the last six years. The main research topic of my contributions is the design and evaluation of protocols and models for wireless multi-hop networks particularly Mobile Ad hoc Networks (MANETs), Vehicular Ad hoc Networks (VANETs), and Wireless Sensor Networks (WSNs). The key question underlying my research is: how to design an efficient data transportation protocols while ensuring quality of service (QoS), energy saving and security in wireless multi-hop networks? To answer this question, I particularly focus on MAC and routing layers using a cross-layer approach.

1.1 Research context and motivations

Since 2000, the introduction of new wireless communication standards using ISM (Industrial, Scientific, Medical) bands contributes to the development of wireless computer networks. Nowadays Internet access is mainly provided through wireless technologies such as Wifi (IEEE802.11), WiMAX (IEEE802.16), UMTS/ LTE (3GPP standards) on user terminals like smartphone, tablets, and laptops, etc. The basic mechanisms provided by these technologies enable wireless communication over single hop, between user terminal and network infrastructure (access point). Another communication mode named multi-hop wireless communication exists through relayed nodes.

The wireless multi-hop communications are taking an important part of the emerging wireless networks technologies such as: future fifth generation wireless networks (5G) and Internet of Things (IoT). Unlike the conventional cellular system where all communications are enabled through the base station, a new kind of communication has been introduced and is a direct device-to-device communication. According to the communication range, the communication between devices is performed by direct connection or through multiple hop relays [1]. Wireless multihop networks are considered as promising solutions to extend the wireless network infrastructure without any additional infrastructure deployment, on the one hand; and to reduce the massive network traffic generated by different devices (smartphone, tablets, and sensors, etc) using offload concept on the other hand. Moreover, they can improve the resilience of the network particularly when the infrastructure is unavailable due to many reasons like natural disaster, etc. We distinguish two kinds of wireless multi-hop communications: 1) relayed (routers) nodes belong to network infrastructure and they are planned in advance (eg. LTE or WiMAX), 2) relayed nodes do not belong to any infrastructure, and they play the role of terminals and router at the same time. In the first case, an operator controls these wireless networks, which depend entirely on an infrastructure planned and deployed in advance. We do not focus on this

kind of networks, but on the second one.
A wireless multi-hop network is seen as a collection of fixed and/or mobile terminals that communicate over a shared channel without requiring a fixed wireless infrastructure. Unlike conventional cellular systems, there is no master-slave relationship between the nodes such as base station to mobile stations. According to the communication range, the communication between stations is performed by a direct connection or through multiple hop relays.

Several advantages of wireless multi-hop communication can be summarized as follows:

— *Interference reduction:* it is due to the reduction of transmission power (PTX) where nodes use close neighboring nodes to relay packets instead of increasing PTX. This enables to reduce the number of competitor nodes sharing the same channel (link).

— *Spectrum reuse increase:* it is due to the short communication range where the spectrum can be reused more frequently. The spectral efficiency increases when the coverage area decreases. Thus, the availability of frequency channels per unit area increases the system capacity.

— *Radio coverage extension:* it is guaranteed by relayed nodes through multi-hop communication, and it enables to reduce the nodes' isolation.

— *Traffic load balancing:* it is due to the different potential paths to reach the destination. This enables to avoid the congested nodes/links and to select non-congested nodes in order to ensure load balancing between them.

— *Power consumption reduction:* it is due to short-range communication where nodes reduce their transmission power and select relayed neighboring nodes to forward packets to their destination.

We focus on three multihop wireless networks that have attracted a growing attention: Mobile Ad hoc Networks (MANETs), Vehicular Ad Hoc Network (VANETs), and Wireless Sensor Networks (WSNs).

Mobile Ad hoc Networks (MANETs):
MANETs are characterized by their self-configuration, open peer-to-peer network architecture, shared wireless medium, resource constraints, and highly dynamic network topology. Each node acts as router and terminal at the same time, and it must take part in forwarding/routing process of network traffic unrelated to its own use. In addition, nodes are free to move to any direction, and to join or to leave the network. They make the network topology dynamic, and it is more complex to manage the network resources. MANETs are considered as complementary for wireless networks with infrastructure like Wireless LAN (WLAN).

Vehicular Ad Hoc Networks (VANETs):
VANETs are a particular case of MANETs, which has the constraint of fast topology changes due to the high node mobility [2]. With the increasing number of vehicles equipped with computing technologies and wireless communication devices, inter-vehicle communication is becoming a promising field of research, standardization, and development. VANETs enable a wide range of applications, such as prevention of collisions, safety, blind crossing, dynamic route scheduling, real-time traffic condition monitoring, etc. Another important application of VANETs is providing Internet connectivity to vehicular nodes.

Wireless sensor networks (WSN):
In the last decade, sensor networks have emerged, and gained significance in multiple fields including industrial applications. WSNs are composed of low-power sensor nodes equipped with sensing board, processing, and wireless communication capabilities [3]. Sensor

nodes collaborate to collect and to relay sensed information to the collector node named sink node using multi-hop communication. These networks can be applied to different applications such as healthcare, military, industrial, and natural environment monitoring (fire detection, pollution, earthquake, etc.). The advanced technology on the sensing board device enables the apparition of new applications like video surveillance, people and object tracking, etc [4] [5]. WSN can be named Wireless Multimedia Sensor Networks (WMSNs), when nodes are equipped with small cameras and microphones in order to capture and retrieve multimedia contents. In addition to the common characteristics shared with WSN, the WMSN have special features: high bandwidth demand, specific QoS requirements, sector sensing range, etc. Recently, IP-based sensor networks are attracting more attention, and are enabling the development of the Internet of things (IoT) [6]. However, energy consumption continues to remain a challenge in many sensor network applications that require long lifetimes.

1.2 Challenges

The wireless multi-hop networks face some issues mainly related to resource management and data transportation able to support a large number of nodes (scalability), Quality of Services (QoS), and security.

Rate adaptation and fairness issues in MANETs

MANETs are a set of mobile nodes sharing wireless medium, and able to communicate without any existing infrastructure using a multi-hop communication mode. However, the lack of infrastructure makes the centralized approach not suitable to manage shared resources like channel access. Unlike Wireless LAN (WLAN), in ad hoc networks the neighboring nodes become competing nodes without any regulation aiming at ensuring fairness and throughput optimization between them. IEEE 802.11 standard does not take into account fairness in the context of MANET. Although the standard presents various transmission rates, it does not specify how to efficiently allocate these rates. Generally speaking, the effectiveness of a rate adaptation scheme hinges on how it is coping with the impact of transmission failures which may occur due to channel errors or packet collisions. In literature, a wide set of rate adaptation schemes have been proposed [7, 8, 9, 10]. Unfortunately, none of them can be applied to MANETs.

Coverage extension using integrated MANETs

The coverage extension area in wireless networks aims at increasing the network connectivity without increasing the infrastructure. The coverage extension issue requires the cooperation of border mobile nodes to relay the packets of neighboring nodes that are located outside the base-station area. The mobility of relayed nodes has to be taken into account in order to be close to reality. In literature, many solutions proposed to extend the wireless coverage mainly focusing on throughput enhancement without considering the incentive approach [11]. The incentive approach is important, because the relayed nodes must share their resources (eg. throughput) with other neighboring nodes that can impact their own packets' transmission. In addition, the energy consumption of the relayed nodes is more important than the one of other non-relayed nodes. They do not only transmit their own packets but also the packets of other neighboring nodes. Therefore, the user of potential relayed nodes can disable the cooperative functionality in order to keep the performance in terms of QoS only for its own transmission. That is why the incentive

strategy for potential mobile relay nodes has to be taken into account in the cooperation protocol design.

Greedy and non-cooperative nodes detection in MANETs

In addition, MANETs are a set of nodes based on the cooperation aspect to form and manage a network. The nodes act as router and terminal at the same time and a lack of cooperation between them implies the absence of any network. That is why it is important to deal with the non cooperative or selfish nodes problem. The problem of selfish nodes is that they keep their energy to transmit and route their own packets. In other words, the selfish nodes refuse to route and forward the packets of other nodes. This misbehavior can negatively impact not only communication in MANETs, but also the coverage extension in wireless networks like WLAN [12]. Therefore, it's important to detect these nodes, and an efficient monitoring mechanism is required. However, in MANETs the monitoring mechanisms have a serious issues, particularly when a collision occurs at the monitor node during the monitoring process. This situation significantly increases the false positive rate, and it makes the detection process inefficient.

Data dissemination and transportation in VANETs

VANET applications can be divided mainly into two categories: infotainment applications and safety applications [13]. Among safety applications: road traffic data collection and sharing, accident alert, traffic jam notification, and real time traffic condition. These applications provide information directly related to users' safety, in order to reduce road accidents, and better manage the road traffic. VANETs' characteristics make them more complex than their predecessor Mobile Ad hoc Networks (MANETs). Indeed, the high node velocity range, the extended geographic set up area, and the large size of the network, lead to frequent topology changes, and result in sporadic connections between nodes. In order to ensure a quick and global distribution of information, the transmission method used is broadcast. The broadcast protocol poorly prepared, with an excessive number of broadcasts, flood the network with duplicate messages and causes infinite loops of retransmissions. In addition, this method suffers from burst loss due to collisions (particularly at Control Channel (CCH) in IEEE802.11p/1609.4), because of the lack of acknowledgments in the IEEE standard 802.11-2012 [14], which includes the IEEE standard 802.11p [15] dedicated to VANETs. Therefore, a sender is not able to know if a packet is well received or not, and which vehicle(s) did not receive it. Moreover, the importance of the content information is not the same for all nodes. For instance, the location of vehicles, data profile, and time of collection are important parameters, which can be considered in the broadcast process.

Security and trust in VANETs

We know that the content of dissemination information in VANET is both time and security sensitive. Each content alteration can cause accidents, as in the case where a malicious vehicle disseminates false information. Integrity, authentication, timeliness, and cooperation are the basic requirements for safety applications. However, VANETs are characterized by an open architecture that raises tremendous vulnerabilities [16, 17]. Therefore providing information security is a serious challenge in VANETs. Introduce security mechanisms such as: public keys distribution, certificates revocation, and trust model requires a centralized third party with is not suitable in VANETs. The only possible

communications with infrastructures take place with Road Side Units (RSUs) which are not always deployed along the roads. Another issue is related to high dynamic topology cause by the speed of vehicles, consequently, the communications between the vehicles are short in time and it is difficult to form an experience history between peers. This makes the monitoring process of vehicles more complex, and reliability of trust model less efficient. In addition, security mechanism must be scalable providing the same achievement independently on the density of vehicles in the network.

QoS, energy efficient, and security aware in WSNs

The development of WSNs enables the increasing of the number of application fields. These applications require not only significant network resources particularly throughput, and energy, but also security services are needed like the end-to-end data confidentiality between the sensors and the sink, the mutual authentication, and the data integrity. However, the characteristics of WSNs such as: the limited resources (bandwidth, energy, memory and processing), the wireless link and mobility make the design of efficient communication protocols a real challenge [4]. In literature, the major proposed solutions consider QoS, energy, and security separately. In addition, it has been shown that it is difficult to offer the end-users multiple levels of security while offering a high level of QoS, because security and QoS are opposite parameters.

Nodes localization and Tracking algorithms in WSNs

The design of routing protocol must take into account not only the characteristics of WSN but also the requirements of the application. Some applications need the position information of sensor nodes. The sensor nodes require knowing their positions in order to track the objects and to route the packets by using the geographic routing [18]. The issue of localization is widely dealt with in order to improve localization accuracy where many techniques and technologies are used [19]. However, many military and civilian applications require to confine the localization time which is not an easy task. Another challenge related to localization issue is target tracking in WSN is tricky problem. We distinguish two kinds of targets: communicating and non-communicating targets (Object without communication module). Mobile target tracking is defined as a two-stage application: detecting the presence of the target in the monitoring area and reporting its position along the trajectory. It is considered as a costly application due to its resources requirements, mainly the energy. Moreover, the sensors should collaborate to efficiently and dynamically select the succeeding sensor to relay the tracking when the target leaves the sensing field of the current sensor. Therefore, the design of mobile tracking algorithm must consider not only the accuracy of the node' trajectory, but also the energy efficiency, and the generated overhead.

1.3 Contributions

Our contributions to the challenges presented above are organized as follow:

MANETs (Chapter 2)

In this chapter, we focus on the contribution related to MANETs. First, we propose a Relative Fairness and Optimized Throughput named REFOT for IEEE 802.11-based DCF (Distributed Coordination Function) mode to ensure fairness and to allow each

node to adapt its transmission rate and contention window to its channel quality [20, 21]. REFOT allows for reaching the appropriate transmission rate level, without crossing all the intermediate levels. This operation helps in avoiding scenarios where the network capacity could be underutilized or overused, allowing the system to reach its stability faster. Second contribution focuses on the nodes cooperation in the context of wireless coverage extension. We propose a new protocol based on an incentive approach and a scheduling algorithm in order to reward cooperative nodes. The cost of cooperation can be prohibitively expensive in terms of QoS and energy consumption, which does not motivate some nodes to cooperate. Therefore, we introduce a percentage of cooperation and QoS parameters in the scheduling algorithm called CEI in order to incite potential mobile relaying nodes to cooperate and in turn extend the wireless areas [22, 23]. Third contribution mainly targets the problem of monitoring and detection of selfish, and non-cooperative nodes in MANETs. The non-cooperative (selfish) nodes can affect the quality of services (QoS) delivered by the network. We propose a new monitoring mechanism named MIMODog based on Multi-Input and Multi-Output (MIMO) technology to detect this kind of malicious nodes without false alarm and without affecting the QoS [24]. We propose a monitoring capacity analysis using graph theory particularly Conflict Graph (CG), and asymptotic study. Finally, we propose a model based on mechanism design from game theory that will incite nodes to launch their monitoring process and to contribute to security management in MANETs [25, 26]. This mechanism will motivate new unknown nodes to participate by giving them incentives in the form of trust, which can be used for cluster's services. Here, we consider the tradeoff between security and resource consumption by formulating the problem as a nonzero-sum noncooperative game between the confident nodes and attacker.

VANETs (Chapter 3)

This chapter is dedicated for our contributions in VANETs context. We classify these contributions into two main axes: 1) efficiency of data dissemination and transportation algorithms; 2) reliability and security mechanisms for these algorithms. Our first contribution named ADCD (Advanced Diffusion of Classified Data) is proposed to significantly reduce the generated overhead, to avoid network congestions as well as long latency to data dissemination in VANETs [27, 28]. The concept of ADCD is based on the characterization of sensed information (i.e. based on its importance, location and time of collection) and the diffusion of this information accordingly.
As demonstrated in the literature, such behavior leads safety messages to suffer from synchronous collisions at the start of the Control CHannel (CCH) interval in IEEE 802.11p/1609.4 protocol, as well as from high end-to-end delays caused by the queue-up during the SCH intervals. To address these issues, we proposed a Distributed MAC Scheduler named DMS, which relies on the Optimal Stopping Theory to evenly balance the channel load by introducing tolerated deferring delays before sending a message [29, 30]. This ensures a higher reception probability and lower collision risks, while complying with Enhanced Distributed Channel Access (EDCA) access categories (ACs).

The second part of this chapter is focusing on reliability and security aspects, particularly the presence of misbehaving nodes, which can have a negative impact on network performance. We deal with the presence of malicious nodes, which spread false and forged data; and selfish nodes, which cooperate only for their own benefit. We propose a Distributed Trust Model (DTM^2), adapted from the job market-signaling model [31, 32, 33]. Another approach based on fuzzy sets to evaluate the honesty of vehicles is proposed [34]. Another contribution related to the trust model is presented [35], which consists in the study of the trust metric variation and its stability in the

context of VANETs. We propose a Markovien model which takes into account not only the dynamic trust metric variation according to the vehicles behaviors, but also the constraints related to the monitoring process. Finally, in another contribution related to security management, we propose a secure and distributed public key infrastructure for VANETs based on an hybrid trust model, and cluster-based architecture to manage trust and certificates [36].

WSNs (Chapter 4)

This chapter focuses on our contributions related to WSN. We distinguish two parts: 1) the quality of services (QoS), the energy efficiency and the security aware for routing and data transportation. 2) Efficient nodes localization, and tracking algorithms.

In the context of routing protocols, we focus on the coexistence between security and Quality-of-Services (QoS) guarantee in WSNs. The idea is to integrate the security services (eg. authentication, integrity, confidentiality, etc) with QoS guarantee. We propose a new model based on PID (Proportional Integral Derivative) controller in order to dynamically select the security level adapted to QoS requirements while considering the energy consumption [37, 38]. Finally, we proposed a new mechanism named EDES (Efficient Dynamic Selective Encryption Framework) ables to ensure adaptive security level, QoS and energy efficiency in the case of multimedia traffic in WSN [39]. The capacity function is proposed to evaluate the possibility to increase or decrease the security level using a cross-layer approach.

In second part, we investigate the accuracy of RSSI-based localization algorithms using spatial diversity in WSN. We consider well known trilateration and multilateration localization techniques with different kinds of single and multiple antenna systems: SISO [1], SIMO [2], MISO [3], and MIMO [4] [40, 41]. In another contribution, we focus on the localizability of the network and the delay of nodes/network localization. We proposed a distributed and time bounded localization algorithm based on Multidimensional Scaling (MDS) method in WSN called D-MDS [42]. In the third contribution, we focus on the mobile node tracking issue using WSN. We consider two kinds of target nodes: communicating and non-communicating nodes. In the case of communicating targets, we use a deployment strategy based on virtual forces (VFA) [5] associated to a distributed tracking algorithm implemented in a cluster-based network [43]. Secondly, we handle a more complex and more frequent case of non-communicating targets. The objective is to detect the presence of such target using movement sensors. We propose the deployment of an heterogeneous wireless sensor networks composed of movement sensors used to detect the target and camera sensors used to locate it [5][44]. Finally, as our last contribution, we focus on the target mobility prediction to perform the tracking process with less energy consumption [45, 46]. We use the Extended Kalamn filter as prediction model combined with a change detection mechanism named CuSum (Cumulative Summuray). This mechanism allows to efficiently compute the future target coordinates, and to select which sensors to activate.

The taxonomy graph of our contributions, the theoretical tools used, the challenges, and the performances metrics is given in figure 1.1.

1. Single Input Single Output
2. Single Input Multiple Output
3. Multiple Input Single Output
4. Multiple Input Multiple Output
5. VFA: Virtual Forces Algorithm

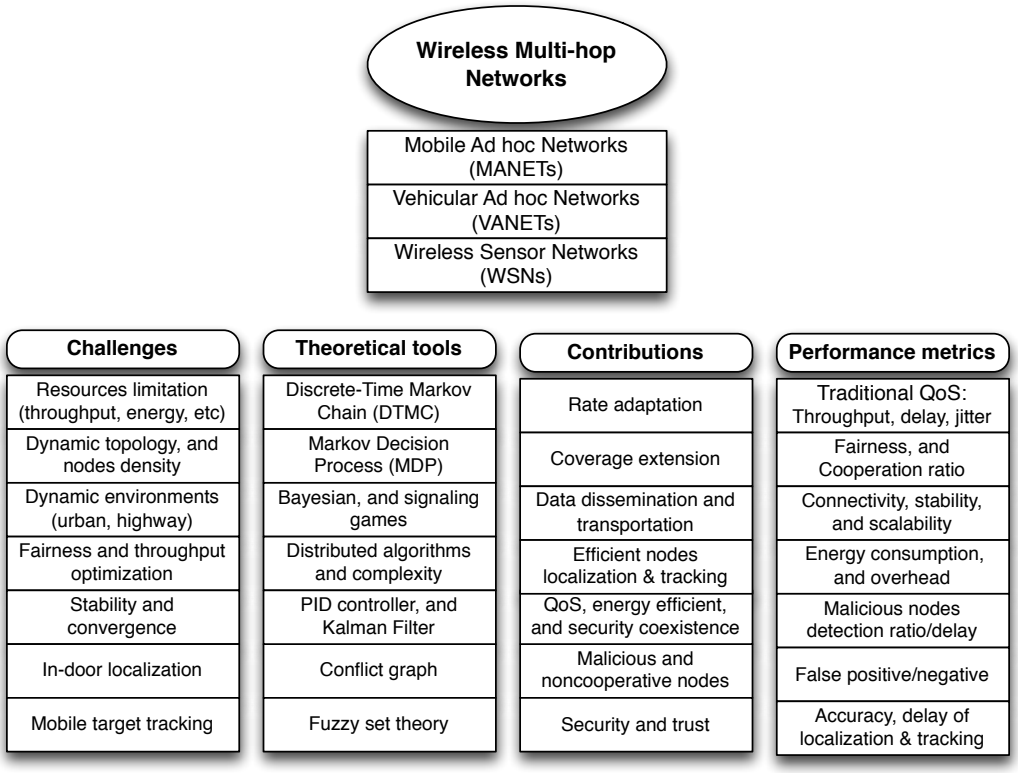


Figure 1.1 – The taxonomy of our contributions.

1.4 Document organization

This document is divided into two parts. A first part dedicated to research activities and a second part composed of a detailed curriculum vitae. The research activities part is divided into five chapters. After having introduced our main contributions in this chapter, Chapter 2 focuses on our results related to Mobile Ad hoc Networks (MANETs) context. Then, the chapter three is dedicated to our contributions for Vehicular ad hoc networks (VANETs). The chapter four describes our contributions in Wireless sensors networks (WSNs). Finally, Chapter 5 summarizes our conclusions and details our main perspectives.

Chapter 2

MANETs

In this chapter, we present our contributions related to resource management, and security issues in MANETs through the following questions: "*How to perform rate adaptation with fairness and throughput optimization?*", "*How to extend the coverage network without negatively impacting the relayed nodes?*", "*How to efficiently detect non-cooperative (selfish) nodes?*", and "*How to incite nodes to cooperate and to prevent misbehavior?*" We have provided answers to these questions through the four contributions classified into two main topics: QoS and security.

In the QoS topic, two main contributions are proposed: First, we propose a REFOT (Relative Fairness and Optimized Throughput) mechanism that is able to improve the overall throughput through rate adaptation while maintaining fairness among nodes[20][21]. Second, in the context of wireless coverage extension we propose an incentive scheduler algorithm called CEI to distinguish between relayed and non-relayed nodes in the resource allocation process [22][23]

Our contributions for security issue particularly misbehaving nodes (eg. greedy, selfish, and non-cooperative nodes) are presented with two approaches: 1) monitoring and detection mechanisms, 2) incentive mechanisms. In order to improve the detection mechanism, we focus on the monitoring process which consists in overhearing the nodes' activities. We propose a new monitoring mechanism called MIMODog based on Multi-Input Multi-Output (MIMO) technology, and particularly a SPACE-MAC protocol to significantly reduce the potential interferences at the monitor (detector) nodes and to enhance the accuracy of the monitoring results [47][24]. Finally, we contribute to incite nodes to cooperate and to avoid selfish and malicious behaviors by proposing incentive mechanism based on mechanism design from game theory [26][25].

2.1 Rate adaptation scheme

2.1.1 Research context

Unlike WLAN, which acquires a centralized control unit, MANET networks lack such unit; which makes the resources management an important challenge in the case of MANETs. We focus on QoS provisioning for competitor nodes particularly rate adaptation, and resource allocation at MAC layer with fairness and throughput optimization issues. As a matter of fact, a MANET node cannot adapt its rate without taking into account the other competitive nodes. Moreover, competing nodes do not necessarily have the same channel conditions. They may, therefore, experience different

channel qualities. If a given node does not take into account its competitive neighbors in its rate adaptation operation, an unfair situation is likely to occur.

IEEE 802.11 standard does not take into account fairness in the context of MANET. Although the standard presents various transmission rates, it does not specify how to efficiently allocate these rates. Generally speaking, the effectiveness of a rate adaptation scheme hinges on how it is coping with the impact of transmission failures, which may occur due to channel errors or packet collisions. In literature, a wide set of rate adaptation schemes have been proposed [48, 8, 9, 10]. Unfortunately, none of them is applicable to MANETs. The drawback of these schemes is that the sender does not care about other competing nodes and adapts its rate without taking them into account. Therefore, most existing schemes, if not all, do not jointly consider fairness, throughput efficiency, and transmission rate adaptation in MANET. Some consider only fairness; others consider only rate adaptation, while only a few methods consider both but in WLAN and not MANET.

2.1.2 REFOT algorithm and model description

We propose a new mechanism called REFOT (Relative Fairness and Optimized Throughput) that increases the overall throughput via rate adaptation while maintaining fairness among nodes. According to their access probability, nodes, competing for a particular channel, update their initial contention window size. Adjusting contention window and adapting the transmission rate shall enable nodes to have a certain fairness related to their perceived channel quality without compromising the system throughput. In addition the modeling of REFOT using a 3-dimension discrete-time Markov chain is done.

REFOT scheme is proposed for IEEE 802.11 with DCF mode in the context of MANETs. The goal of the REFOT scheme is to ensure relative fairness among competing nodes without compromising the throughput. The key idea is based on the channel quality and on the assessment of transmission failures and transmission successes. In addition, the probability to access a channel is introduced in the BEB (Binary Exponential Backoff) algorithm while taking into account the set of competing nodes.

Before a node selects its rate for the data transmission, it assesses the number of its consecutive failure transmissions (n) and the number of consecutive successful transmissions (s). However, when the number of consecutive transmission failures reaches a certain threshold value P_{th}, the RTS/CTS mechanism is activated for the next data transmission. Thus the RTS/CTS mechanism is efficiently used. We distinguish two cases for decreasing the transmission rate. If the current rate is the lowest, when n the number of consecutive transmission failures reaches m ($m \geq N_{th}$), the next attempts for transmissions continue with the same lowest rate. However, in higher transmission rates, when n reaches N_{th} the transmitting node decreases its rate by selecting the lower rate from the set (R_dt) and resets counter n. If the number of consecutive successful transmissions (s) reaches a certain threshold number M_{th}, the transmitting node selects the next higher rate in set R_dt. Then, the transmitter computes its probability to access the channel and adapts the size of the backoff window. According to the value of the backoff window, the transmitter will choose a new transmission stage.

In order to define the probability that node d accesses to channel J (Q_d^J), we need to define the probability that transmission fails for node d (P_d^J) which is given by:

$$P_d^J = \frac{\sum_{l \in \Phi_J} P_l r_l}{\sum_{l \in \Phi_J} r_l} \tag{2.1}$$

where Φ_J is the set of nodes competing for channel J, r_l is the transmission rate of Node l, P_l is the probability of failure of node l. Therefore, each node calculates the probability to access the main channel:

$$Q_d^J = \frac{1 - P_d^J}{\sum_{l \in \Phi_J} 1 - P_l^J} \tag{2.2}$$

This probability takes into account the channel conditions of the neighboring nodes. According to this probability, each node respects the other neighbor nodes by introducing their probability to access the communication channel. Then, this probability is incorporated to fix the value CW^*_{min} of the transmitting node as follows:

$$CW^*_{min} = \begin{cases} CW_{min}.(1 - Q_d^J) & \text{if } Q_d^J \neq 1 \\ CW_{min} & \text{Otherwise} \end{cases}$$

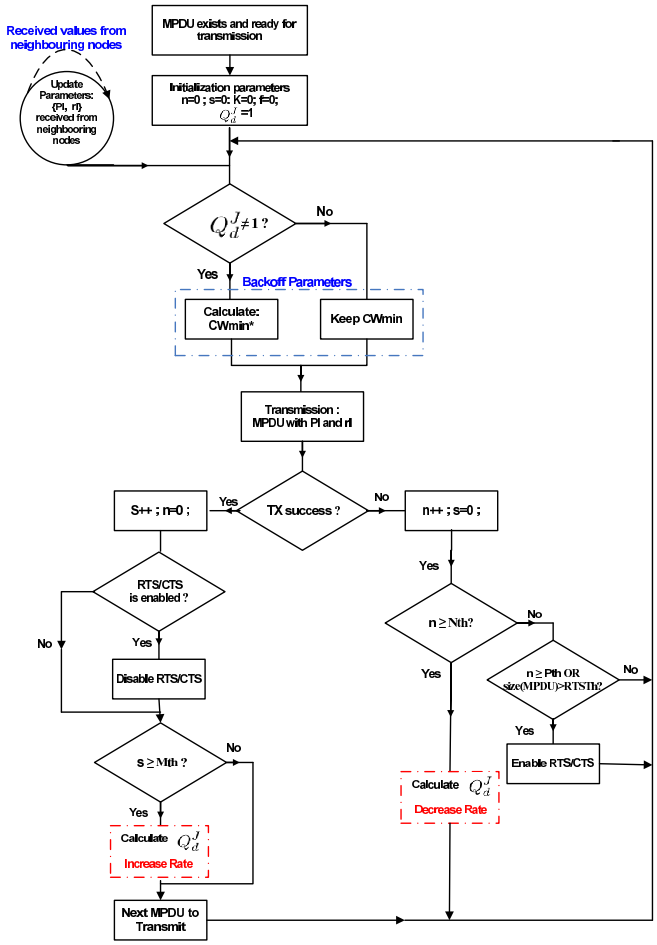


Figure 2.1 – REFOT Flow-chart.

Figure 2.1 summarizes the REFOT flowchart. At the beginning, the access probability Q_d^J is equal to 1 and the parameters $\{n, s, K, f\}$ are set to zero. The first step consists in parameters initialization with RTS/CTS mechanism disabled. The node continuously refreshes the set of parameters $\{P_l, r_l\}$ received by overhearing the transmission of neighboring nodes. Then, it calculates the probability to access the channel (Q_d^J). If this probability is equal to 1 the backoff algorithm is not changed. Otherwise, the node changes the backoff algorithm (BEB) parameters by introducing the new CW^*_{min}. Once

the node finishes this step, it adds its own refreshed parameters in terms of probability and transmission rate in the scheduled packet. In the second step, the node checks the packet transmission. In the case of a transmission failure the counter parameter n is incremented and the counter s is set to zero. According to the threshold N_{th} the decision to decrease the transmission rate is made as illustrated in the flowchart. However, in the case of a transmission success the counter parameters s and n are updated and according to the thresholds M_{th} the transmission rate may be increased. Moreover, the decision to enable the RTS/CTS mechanism is made according to the thresholds P_{th} and RTS_{Th}. RTS_{Th} indicates the threshold of packet size. When size of MPDU exceeds the RTS_{Th}, the RTS/CTS mechanism is enabled to prevent the collision and the hidden nodes problem. The recommended RTS_{Th} value is set to $500bytes$.

Markov Chain Model For REFOT

We developed an analytical model for REFOT based on 3-dimension Markov chain. First, the transmission probability of a single station during a randomly selected time slot τ is studied. Then, the throughput model for the whole network as a function of the variable τ is expressed.
In REFOT the transmitter adjusts its backoff ($CW_{i,j}$) according to the probability to access the channel (Q_d^J) defined by Equation 2.2. However, for modeling reasons, we define four classes of backoff which represent the different rates used by the transmitter. The contention window size ($W_{i,j}$) is then defined as:

$$W_{i,j} = \alpha_j 2^i W_0, \tag{2.3}$$

where $\alpha_j \in \{1, 3/4, 2/4, 1/4\}$, $j \in [0, 3]$ the backoff stage, $i \in [0, m]$ the counter of successful and failed transmissions and $W_0 = CW_{min}$.

We use a $3 - D$ stochastic process $\{u(t), v(t), w(t)\}$ to model REFOT scheme as a discrete-time Markov chain. The first process $u(t)$ represents the current backoff stage ($j \in [0, 3]$). The second process $v(t)$ represents the number of consecutive successful and failure transmissions experienced by a station which is explained hereafter:

- $v(t) = -i$, $i \geq 1$ represents a station that has suffered i consecutive failure transmissions.
- $v(t) = i$, $i \geq 1$ represents a station that has experienced i consecutive successful transmissions.
- $v(t) = 0$, indicates the first step of each rate (j).

The third process $w(t)$ represents the backoff counter for a given station. A discrete and integer time scale is adopted as in Bianchi model [49].

For more details about the resolution of this Markov chain, please refer to this paper [21].

2.1.3 Summary of results

We studied the variation of the average rate during the entire simulation time, with different nodes density, and with and without nodes mobility. We notice that the rates obtained in case of REFOT are better than other schemes (like CARA [48], and DCF). The rate varies from 2Mbps to 11Mbps. However, in case of DCF, the rate remains constant, equal to 2Mbps, due to the lack of rate adaptation mechanisms. In addition, these results show that the nodes have more consecutive successes than consecutive failures, so their rates can rapidly get stabilized. However, this stability is relatively impacted when the nodes mobility is important. In the case of the node mobility, the probability of collision

and the number of consecutive failures when a connection-oriented protocol is used (TCP flows), are relatively low. We deduce that TCP mitigates the impact of mobility in terms of collided packets, so the rate is more stable then the case of UDP flows. We can deduce that the possibility, offered by REFOT, to reduce the rate level of a node allows to adapt the rate level in the event of a critical situation, such as bad channel conditions.

We used the fairness index (FI) as a metric to evaluate the system fairness [50]. The fairness index involves the relative throughput of nodes sharing a medium. Depending on the application and the number of senders, gaining higher fairness values is sometimes worthwhile even at the cost of reduced efficiency. We studied the impact of nodes density on the FI. We used UDP flows (randomly generated) and Random Way Point as mobility model. We notice that REFOT gives best performance in terms of fairness compared to other schemes particularly CARA and DCF. Furthermore, we remark that the fairness value is approximately 40% greater than in CARA and DCF schemes. We can deduce that when the number of nodes increases, the number of collisions may increase and the probability to access the channel will decrease. Then, the fairness index will decrease.

In order to study the impact on the throughput, the obtained simulation results show that the throughput with REFOT stay close to the throughput with CARA mechanism. However, in case of DCF, the throughput is relatively low in comparison with CARA and REFOT. Therefore, we can deduce that taking into account the fairness in adapting the rate among contenders for a channel does not affect the throughput of the network.

2.2 Resource allocation and coverage extension

2.2.1 Research context

In order to incite the relayed nodes to participate in the extension of the coverage area, we propose a new cooperative protocol based on an incentive approach that takes into account the QoS for mobile relayed nodes. We focus on the coverage extension of the Wireless Local Area (WLAN) and particularly of the access point area using the allocation of radio resources while considering a cooperative behavior. However, the proposed solution can be applied to the Mobile Ad hoc Networks (MANETs) context under one condition, that is to use the cluster-based architecture. This approach consists of increasing the priorities of the relayed nodes according to their cooperation rate. The idea is to reward the relayed nodes for their cooperation instead of penalizing them by increasing the cost of cooperation. Consequently, the nodes have no interest in selecting and acting selfishly, by using their throughput only to transmit their own packets. Moreover, the proposed protocol guarantees that the nodes are free to cooperate, because they choose their percentage of cooperation. The proposed solution combines the QoS parameters and cooperation rate using the cross-layer approach with a scheduling algorithm. This solution is called *Coverage Extension based on Incentive scheduling (CEI)*. Moreover, the physical layer information is used in order to take advantage of the time, frequency and multiuser diversity and to optimize the system capacity until it is close to the Shannon limit.

2.2.2 System and scheduler algorithm description

The total available bandwidth is divided into sub-frequency bands or subcarriers. The radio resource is further divided into frames in the time domain. Each frame is itself divided into time slots of constant duration. The time slot duration is an integer multiple of the OFDM symbol duration. Moreover, the frame duration is fixed to a value much smaller than the coherence time (inverse of the Doppler spread) of the channel. With such

assumptions, the transmission on each subcarrier is subject to flat fading with a channel state that can be considered static during each frame.

The elementary Resource Unit (RU) is defined as any (subcarrier, time slot) pair. Transmissions performed on different RUs by different mobiles have independent channel state variations [51]. On each RU, the modulation scheme is QAM with a modulation order adapted to the channel state between the access point and the mobile to which it is allocated. This provides the flexible resource allocation framework required for an opportunistic scheduling.

The system operates using time division duplexing with five subframes: the *control subframe*, the *cell downlink data subframe*, the *cell uplink data subframe*, the *relayed downlink data subframe* and the *relayed uplink data subframe*. The cell uplink and downlink data subframes are used for the transmission of intra-cellular user data while the relayed uplink and downlink data subframes are used for the transmission by the relaying nodes of extra-cellular user data.

The Incentive Scheduler (CEI) Algorithm:
The scheduler, located in the central node like access point or cluster-head node, grants RUs to each mobile as a function of: (1) its channel state, (2) its current cooperation ratio, (3) its network confidence percentage, (4) its traffic backlog.

The CEI scheduling algorithm relies on weights that set the dynamic priorities to allocate the resources. These weights are built in order to satisfy two major objectives: to maximise the system throughput and to encourage the nodes cooperation.

System Throughput Maximization Parameter: The CEI scheduler maximizes the system throughput in a MAC/PHY opportunistic approach. Data integrity requirements of the mobiles are enforced to adapt the modulation scheme and the transmission power to the mobile specific channel state. At each scheduling period, the scheduler computes the maximum number of bits $m_{k,n}$ that can be transmitted in a time slot of subcarrier n if assigned to a mobile k, for all k and all n. This number of bits is limited by two main factors: the data integrity requirement and the supported modulation orders.

Incentive Parameter: The second major objective of the CEI is to incite nodes to participate to frame relay in order to extend the network coverage zone. This is achieved by extending the above cross-layer design to other layers. A new "Incentive Parameter" (IP_k) is introduced based on the current estimation of the cooperation ratio:

$$IP_k = \frac{R_k}{D_k} = \frac{D_k + \sum_{i=0...i=K}^{i} D_{ki}}{D_k}, \tag{2.4}$$

where R_k is the global amount of data transmitted by mobile k. It is the sum between D_k, the amount of data transmitted to mobile k for its own requirement and D_{ki}, the amount of data transmitted to the mobile k for a mobile i (then these data will be relayed to mobile i by mobile k in the relaying subframe). This information could be directly monitored by the access point, or signaled by each mobile to the access point.

We also define the cooperation ratio C_k as the number of packets that mobile k is ready to relay for other mobiles when it receives 100 packets for its own consumption.

Confidence Parameter: We assume that each mobile reveals its R_k and D_k to the access point. Thanks to this information, the CEI scheduler will make adequate resource allocation rewarding the mobile according to its cooperation degree. However in order to block malicious mobiles that could lie on this information, we introduced a last parameter called the confidence parameter. The confidence parameter T_k depends on the correspondence between the announced cooperative ratio and the observed forwarding

ratio. This control is carried out by a monitor node (in our case the AP or cluster-head (CH)) in order to efficiently evaluate T_k. Each T_k varies between 0 and 1 included. When the access point monitoring R_k and D_k corresponds to the announced cooperative ratio, T_k is set to 1. Otherwise, when the mobile does not relay the announced amount of data for which it had previously received more priority, its T_k is set to 0 for one round of scheduling in order to punish it. This ensures a deterrent threat for mobiles that would try to mislead the system.

CEI Algorithm Description:

In the allocation process of a given time slot, the priority of a mobile k for UR n is determined by the magnitude of its CEI parameter:

$$CEI_{k,n} = m_{k,n} \times \frac{R_k}{D_k} \times T_k. \tag{2.5}$$

Based on the $m_{k,n}$ and IP_k factor, the $CEI_{k,n}$ directly takes into account the channel states and the mobile behavior.

The T_k parameter is an additional factor that allows to temperate $CEI_{k,n}$ value function of network confidence. Include T_k parameter allows to be resistant to malicious nodes that would lie on their $\sum_{i=0...i=K}^{i} D_{ki}$.

The probability for a mobile to receive Resource Units depends on the magnitude of its $CEI_{k,n}$ and consequently highly depends on the quantity of data relayed by the mobile to other mobiles in order to contribute to the coverage extension. The higher the cooperation ratio, the higher IP_k and, unlike other schedulers, the higher the probability to receive bandwidth resources and to benefit from a low delay and a high throughput is. Consequently, with CEI algorithm, mobiles are encouraged to cooperate. If they want high priority and high QoS, they must not be selfish.

The CEI scheduling algorithm is detailed in Fig. 2.2. The scheduling is performed subcarrier by subcarrier and on a time slot basis for an improved granularity. In the allocation process of a given time slot, the priority of a mobile is determined by the magnitude of its CEI parameter. In the following items, we describe the proposed scheduling algorithm step by step.

— Step 0: The scheduler refreshes the current $m_{k,n}$ and updates cooperation ratio IP_k, confidence ratio T_k and buffer occupancy BO_k values. Then, it computes the $CEI_{k,n}$ parameter for each mobile and each subcarrier. Then, n and t are initialized to 1.

— Step 1: For subcarrier n, the scheduler selects the mobile k that has the greatest $CEI_{k,n}$ value. If $CEI_{k,n}$ is the same for several mobiles, the scheduler chooses the mobile that has the highest BO_k value.
- Sub-step 1-1: If the virtual buffer occupancy [1] of mobile k is positive, the scheduler goes to Sub-step 1-2. Otherwise, if all virtual buffers are null or negative, the scheduler goes to Step 2. Otherwise, the scheduler selects the next mobile k that has the greatest $CEI_{k,n}$ value and restarts Sub-step 1-1 (if $CEI_{k,n}$ is the same for several mobiles, the scheduler chooses the mobile that has the highest BO_k value).
- Sub-step 1-2: The scheduler allocates time slot t of subcarrier n to mobile k with a capacity of $m_{k,n}$ bits, removes $m_{k,n}$ bits of its virtual buffer and increments the value of t. If t is smaller than the maximum number t_{max} of time slots by subcarrier, go to Sub-step 1-1 to allocate the following time slot. Otherwise, go to the following sub-step.

1. We define the virtual buffer occupancy as the current buffer occupancy of mobile k minus the number of bits already allocated to this mobile.

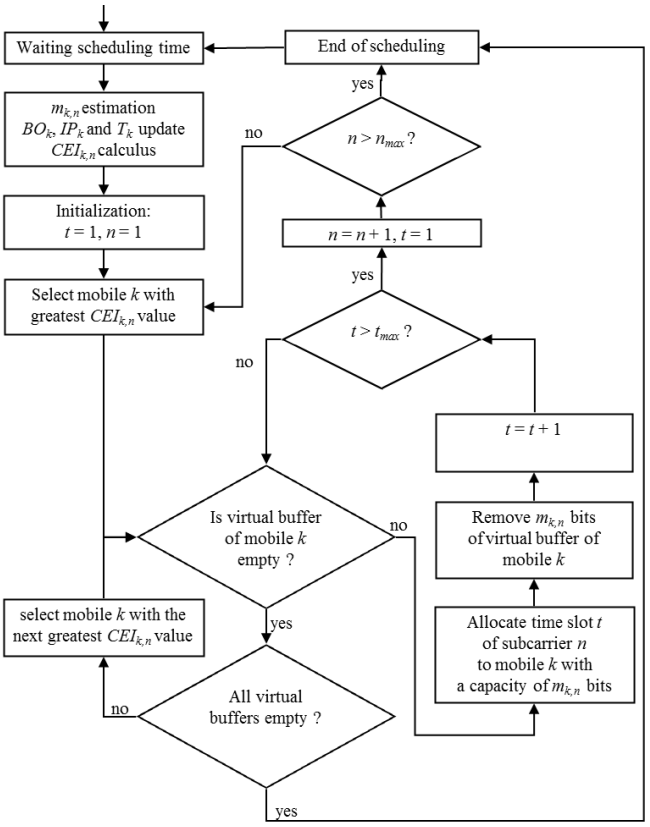


Figure 2.2 – CEI scheduling algorithm flow chart.

- Sub-step 1-3: Increment the value of n. If n is smaller than the maximum number n_{max} of subcarriers, go to Step 1 to allocate the time slots of the next subcarrier. Otherwise, go to Step 2.

— Step 2: All buffers are empty or all time slots of all subcarriers are allocated and the scheduling ends.

2.2.3 Summary of results

The proposed solution called CEI does not only incite the nodes to cooperate but also enhance the QoS by increasing the average throughput and decreasing the delay. The simulation results show that for a high traffic load of $500Kbps$ for each mobile, the scheduler behavior showing the mean cell mobile provided throughput according to their cooperation ratio and the total mean provided throughput out of the cell. It's clearly demonstrated that with RR (Round Robin) and MaxSNR [52] scheduling, there is no interest for a mobile to cooperate. Unlike RR and MaxSNR, there is a significant interest for a mobile to cooperate with CEI. To be friendly induces to decrease its mean packet delay whatever the traffic load on the system but also enables to increase its potential throughput in an overloaded context. Thanks to this new resource allocation strategy, mobiles are not penalized anymore when they cooperate but receive high rewards in terms of QoS which could easily compensate their cooperative energy cost. For a high traffic load of $500Kbps$ for each mobile, the cooperative mobiles can increase their own throughput by around 114% compared to MaxSNR and by around 209% compared to RR resource allocation strategy. The total amount of data transmitted out of the cell in order to extend the coverage can be increased by around 59% compared to other algorithms. Therefore,

this allows a significant coverage extension which was not achieved with RR and MaxSNR strategies and free mobiles.

2.3 Monitoring mechanism with MIMO technology

2.3.1 Research context

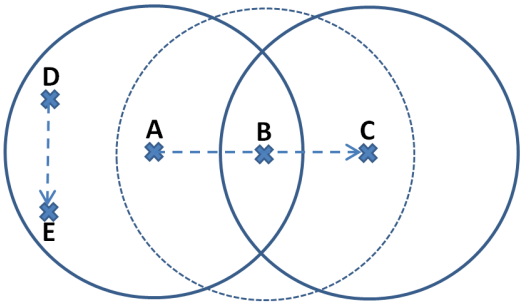
In MANETs, the nodes act as router and terminal at the same time and a lack of cooperation between them implies the absence of any network. That is why it is important to deal with the misbehaving nodes particularly non cooperative or selfish nodes problem. The problem of selfish nodes is that they keep their energy to transmit and route their own packets. In other words, the selfish nodes refuse to route and forward the packets of other nodes. In order to detect these kinds of nodes, and to prevent them in the routing process an efficient detection mechanism is required. However, the interference at the monitor (or detector) nodes makes the detection mechanism inefficient because of mis-monitoring and then false alarms. In order to significantly reduce the potential interferences at the monitor (detector) nodes and to enhance the accuracy of the monitoring results, we propose a new monitoring mechanism called MIMODog based on Multi-Input Multi-Output (MIMO) technology, and particularly a SPACE-MAC protocol [53]. We present the modeling of MIMODog to evaluate the impact of the monitoring process on the network performance. In addition, the proposition of a monitoring capacity analysis based on graph theory particularly conflict graph is done. Finally, an asymptotic study proposed to investigate lower and upper bounds of the number of monitor nodes is proposed.

2.3.2 Model and MIMODog protocol description

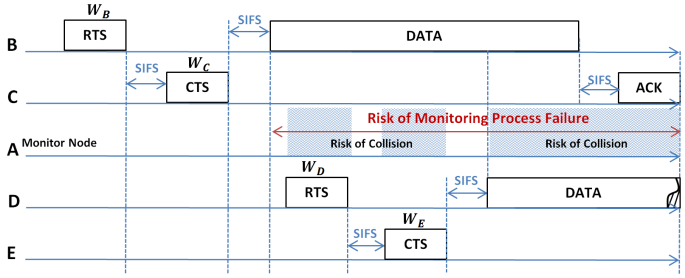
The MIMODog monitoring protocol is based on the Spatial Reuse Using MIMO Channel-Aware MAC called (SPACE-MAC). The SPACE-MAC is a Media Access Control protocol for networks with smart antennas which uses antenna weights to schedule simultaneous transmissions on a single collision domain [53]. Antenna weights are exchanged via control packets (RTS and CTS) [2]. The main idea of SPACE-MAC is the fully distributed MAC protocol that exploits the physical layer characteristics and cross-layer techniques to enable spatial reuse in scatter-rich multi-path environments. The main advantage of SPACE-MAC is that it enables multiple data streams at the same time in the same collision area, thereby increasing the overall capacity of the network.

The SPACE-MAC protocol is not designed for efficient monitoring mechanism. Figure 2.3 illustrates an example of monitoring scenario with SPACE-MAC protocol. Node B wants to forward A's packets to C and D wants to communicate with E. Node B transmits an RTS using the default weight vector, or a random vector. The weight vector used to transmit the RTS will be used to transmit the following data packet and to receive the corresponding CTS and ACK. Once node C receives the RTS, it responds with a CTS packet using the current weight vector. The weight vector used to transmit the CTS will be used to receive the following data packet and to send an ACK. The receiver estimates the SIMO (Single-Input Multi-Output) channel vector $h_{BC} = w_B^H H_{BC}$, where w_B is the weight vector of node B and H_{BC} is $M \times M$ MIMO channel matrix with elements h_{ij} and the superscript H denotes an hermitian operation. In fact, as there is no ongoing communication, nodes C (receiver) and A (monitor) can switch their weight vectors to $w_C = h_{BC}^t$ and $w_A = h_{BA}^t$ which maximize the combined channel and array gain. When

2. RTS: Request to Send / CTS: Clear to Send



(a) An example scenario



(b) SPACE-MAC protocol

Figure 2.3 – Monitoring problem based on SPACE-MAC protocol.

a node other than the designated receiver and the neighbor monitor receive the RTS, say node K, it estimates the effective channel H and adjusts the weight vector so that the signal from the RTS sender is nullified (i.e., $h_{BK}C_K = 0$) for the duration of time specified in the RTS duration field. When a node other than the sender of the RTS (B) receives the CTS, say node L, it estimates the effective channel and stores the weight vector for the duration specified in the CTS duration field. After the RTS/CTS handshaking, node B sends, C receives and A supervises a data frame respectively using the weight vectors w_B, w_C and w_A chosen as described above.

Now let us say node D wants to initiate a transmission toward E. Since node D is not currently aware of the antenna weight used by node B (node D cannot overhear B's RTS and C's CTS), it cannot adjust its weight vectors meeting these conditions: $w_D^H H_{DA} w_A = 0$ (D's signals cannot be nullified by A). Consequently a collision will occur at node A.

MIMODog protocol:

In order to avoid any interference at the monitor node, each new transmitting node must be aware not only of the weight vectors of the existing transmissions in the cover area, but also of the weight vectors used by the monitor nodes. To deal with this issue, we propose MIMODog protocol where, the basic idea is that the monitor nodes simulate a real reception by sending CTS packet control before starting their monitoring process. We use the previous example (see figure 2.3(a)) to illustrate our MIMO MAC protocol functioning.

When monitor node A hears an RTS packet from its forwarding node B:

1. it estimates the SIMO channel vector $h_{BA} = w_B^H H_{BA}$ and switches its weight vector to $w_A = h_{BA}^t$ to well receive B's packets for monitoring;
2. it sends a CTS packet after a SIFS time using a weight vector $\hat{w}_A$ meeting this condition: $\hat{w}_A^H H_{AB} w_B = 0$ (the A's CTS signal is nullified at B to avoid collisions with C's CTS and to ensure that node B will not change its behaviour if it is

malicious). The A's CTS contains the weight vector w_A and transmits using $\hat{w}_A$. The goal of this operation is to make all future transmitters in the neighborhood believe that node A will receive packets and that its weight vector w_A should be considered.

Once it receives the CTS packet from A, each node should estimate the effective channel from A. Now, the transmission of D should ensure that the reception of A is not disturbed. So, it picks W_D meeting $w_D^H H_{DA} w_A = 0$ before transmitting its RTS.

The process is graphically explained in Figure 2.4.

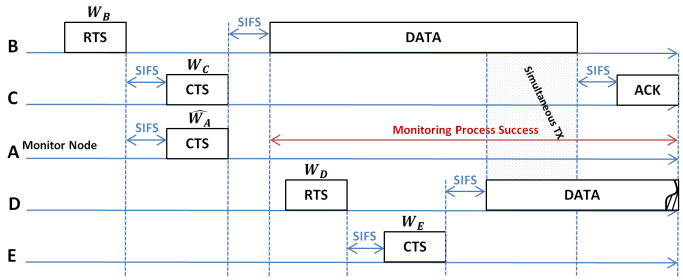


Figure 2.4 – Monitoring mechanism with MIMODog

Complexity analysis:
The proposed solution is designed to be backwardly compatible with the legacy IEEE 802.11 DCF protocol. The aim is to maintain the simplicity of implementation with no added computational complexity.

The additional complexity of MIMODog protocol is due to the selection of the appropriate pre-code weight vectors. This process can be formulated as an optimization problem where our solution can reduce it to eigenvalue problem using the null-space projection method [54]. The time complexity of this method is $O(mn^2)$, where m is the data dimensionality, and n is the sample size related to the channel matrix (H).

Monitoring capacity analysis:
We investigate the monitoring capacity and its impact on wireless multi-hop networks. The monitoring capacity for cooperation can be evaluated by the ability of a monitor (detector) node to listen (overhear) its neighbors activities under interference consideration. In this regard, we focus on:

— the computation of the available capacity on the link between the monitor-forwarding nodes;
— the necessary conditions to correctly perform monitoring.

We use the conflict graph to model the interference relationships between links and called it the Links Conflict Graph LCG. Every link in connectivity graph G is represented by a node in conflict graph LCG. Two nodes in G are connected by an edge if the nodes corresponding to links in G cannot have simultaneous transmissions according to the protocol's interference model.

The main goal of the MIMODog protocol is to avoid transmissions and monitoring under the same DoF within the interference area of the monitor node. Consequently, the link capacity of the monitor-relay nodes is similar to that of the SPACE-MAC protocol.The resulting capacity is due to the reservation of the DoF (Degree of Freedom) for the monitoring process which demonstrates the advantage of MIMODog protocol.

2.3.3 Summary of results

We focus on the impact of the average number of monitor nodes, the number of selfish nodes, and the cost of monitoring process on the network capacity.

The obtained results show that the number of monitor nodes (NMN) increases not only with the network density, but also with the number of network traffic flows. However, the NMN significantly decreases when the degree of neighborhood increases.

In order to analyze the throughput capacity of a given flow in the presence of selfish nodes, we compute the normalized goodput [55]. This metric is based on a route validity time that contains a successful transmission on the one hand, and the additional time required to find a new route without selfish nodes on the other hand. During this additional time, the throughput between a pair of source and destination nodes is null. We remark that when the selfish node density increases, the throughput capacity of flows in the network decreases. This throughput capacity can be greatly enhanced using MIMODog protocol.

To study the impact of monitoring on the capacity, we assume that n nodes are randomly located on the surface of a square flat torus unit area. We use this geometric topology to avoid edge effects, which otherwise complicates the analysis. Each node selects a destination randomly to which is sends $\lambda(n)$ bits/s. The average length of of each source-destination pair in terms of links is $\overline{hopcount} + 1$. The average required capacity over the entire network for $\lambda(n)$ successful delivery is: $\frac{(\overline{hopcount}+2)n\lambda(n)}{M}$ where M is the number of antennas.

We focus on the MIMODog asymptotic study of the lower and upper bound of monitor (detector) nodes' number. We consider a random multi-hop MIMO ad hoc network with n nodes, where each node, equipped with M antennas, is randomly located in a unit square area.
Lower bound of the number of monitor nodes: we demonstrate that in MIMODdog ad hoc networks a number of monitor nodes lower bound of $\Omega(\frac{M}{\sqrt{n \ln n}})$ can be obtained [24].
Upper bound of the number of monitor nodes: we show that in MIMODog ad hoc network, a number of monitor nodes upper bound for all possible routing and scheduling schemes is $O(\frac{M}{\sqrt{n \ln n}})$ with a high probability when $n \to \infty$[24].
Combining the lower and upper bounds of the number of monitor nodes, we can see that the number of monitor nodes in a random multi-hop MIMO ad hoc network with n nodes is $\Theta(\frac{M}{\sqrt{n \ln n}})$.

Finally, the obtained results of the average consumed capacity in the network according to the network density and the average hop count with different models of monitoring mechanism: SISO ($M = 1$), SPACE-MAC, and MIMODog (the number of antennas is set to 2) show that the required capacity in the case of MIMODog is more important than the case of SPACE-MAC particularly when the average hop count increases. However, the worst results are obtained in the case of SISO compared to both models based on MIMO technology. In order to study the impact of the number of antennas (M), we focus on the consumed capacity with different monitoring models. The obtained results illustrate that the gap between the consumed capacity in the case of MIMODog and SPACE-MAC remains constant when the number of antennas increases.

2.4 Incentive models: mechanism design approach

2.4.1 Research context

In this section, we focus on the following question: why do nodes act selfishly and ignore the cooperation aspect? To answer this question, we investigate the motivation of nodes to adopt this misbehavior. First of all, the resources in MANETs are limited in terms of energy, bandwidth, etc. Then, the nodes try to increase their lifetime duration by reducing their energy consumption and the cost of the transmission operation is important in terms of energy. Secondly, when the nodes route and forward the packets of other nodes, this increases the delay of their own packets transmission and reduces their own average throughput. Thus, this operation may be perceived by nodes as punishment and not as global network interest. That's why it's important to not only focus on the detection mechanisms, but also on the incentive mechanisms.

We consider the case of nodes cooperation in the public key distribution mechanism which is one important mechanism, to ensure the security of nodes and data transportation in MANETs. However, the centralized solution is not suitable in this kind of network, because it creates a single point failure for the certificate authority (CA). We proposed a cluster-based architecture to distribute the CA role. The main idea is to distribute the CA role on confident nodes (with high trust level). The aim of confident nodes is to organize the network, and to assume different sensitive roles. In order to increase the clusters stability endangered by the CA mobility, we introduce the concept of secondary role of CA called register authority RA. The problems of such a model are: (1) Clusters with one confident node, CA, cannot be created and thus clusters' sizes are increased which negatively affect clusters' services and stability. (2) Clusters with a high density of RA may cause channel collisions at the CA. (3) Clusters' lifetime is reduced since RA monitors are always launched (i.e., resource consumption). We propose a model based on a mechanism design that will enable clusters with a single trusted node (CA) to be created. Our mechanism will motivate nodes that do not belong to the confident community to participate by giving them incentives in the form of trust, which can be used for cluster's services.

2.4.2 Algorithm and model description

Cluster formation and CA election algorithm:
The CA is selected among confident nodes in each cluster based on node's stability which increases cluster's lifetime. We use Relative Mobility (RM), and the degree of the neighbors nodes (DN) as parameters for CA election. Furthermore, the clustering algorithm ensures the authentication and integrity of the transited data during the election process.

Initially all trusted nodes are playing CA role, and they receive a beacon, from one of their neighbors, they execute clustering algorithm 1 to change its status from cluster-head (CA) to cluster-member [56].

The $Packet - Authentication - Integrity - checking()$ is the function which consists to check the integrity and the authentication of the election packet. $HopCount$ indicates the hop number of the election packet.RM_i is the relative mobility of node i and DN_i is the degree of the neighbors nodes of the node i.

Monitor/Detector (RA) nodes selection:
The RA nodes ensure the monitoring packets and network activities to protect the CA

Algorithm 1: Clustering Algorithm ($SDCA$)

When node j receives an election packet from node i;
begin
  Packet-Authentication-Integrity-checking();
  if *($HopCount >= k$)* **then No − Competition**; **Goto**(**end**);
  ;
  else if *($RM_i < RM_j$) OR (($RM_i == RM_j$) AND ($DN_j < DN_i$))* **then**
    Accept node i as CA;
  else if *($RM_j < RM_i$) OR ($DN_j > DN_i$)* **then**
    node j remains as CA candidate;
  else if *($RM_i == RM_j$) AND ($DN_j == DN_i$)* **then**
    apply Lowest-ID;

node from potential attacks. The election of RA nodes depends on the selection criteria function $F()$ which can be expressed by the following Social Choice Function (SCF):

$$SCF = S(C) = \max \sum_{i \in N} F_i \tag{2.6}$$

The selection criteria function has the following parameters:

Trust Level/Metric (Z_1): This metric determines the confident level of nodes which is evaluated by the monitoring mechanism.
Stability Metric (Z_2): RA node's stability is based on the relative mobility according to the CA node (it is the private information of a node).
Residual Energy Metric (Z_3): This metric determines the residual energy level of the nodes. This is also a private information of a node.
Connectivity Degree (Z_4): It is the number of links a node is connected with.

Based on the above four parameters, our selection criteria function F is defined as follows:

$$F = \sum_{i=1}^{4} W_i Z_i \tag{2.7}$$

where W_i is the weight of each parameter i.

The stability and residual energy are the private information, which needs to be truthful in order to have a truthful calculated function F. We give incentive in terms of reputation so that nodes are motivated to participate and reveal their truthful function $F()$. To achieve this goal, the payment should be designed in such a way truth-telling is the dominant strategy for each node.

Game model

We treat the RA election as a game where the N mobile nodes are the agents/players. Each node plays by revealing its own private information (selection criteria function (F)) which is based on the node's type θ_i. The type θ_i is drawn from each player's available type set Θ_i=*{Normal, Selfish}*. Each player selects his own strategy/type according to how much the node values the outcome (i.e., The amount of reputation granted). If the player's strategy is normal then the node reveals the true selection criteria function F. We assume that each player i has a utility function [57]:

$$u_i(\theta_i) = p_i - v_i(\theta_i, \mathbf{o}(\theta_i, \theta_{-i})) \tag{2.8}$$

where,

— θ_{-i} is the type of all the other nodes except i.

— v_i is the valuation of player i of the output $\mathbf{o} \in O$, knowing that O is the set of possible outcomes. In our case, if the node is elected then v_i is the value of the selection criteria function F_i.

— $p_i \in \Re$ is the payment given by the mechanism to the elected node. Payment is given in the form of reputation. Nodes that are not elected receive no payment.

Note that, $u_i(\theta_i)$ is what the player usually seeks to maximize. It reflects the amount of benefits gained by player i if he follows a specific type/strategy θ_i. Players might deviate from revealing the truthful value of the function F if that could lead to a better payoff. Therefore, our mechanism must be strategy-proof where truth-telling is the dominant strategy. To play the game, every node declares its corresponding function F, where each node's reported function value is the input for our mechanism. The goal of our mechanism is to motivate nodes to say the truth and compute the output $\mathbf{o}$ that is equal to the SCF defined in Equation 2.6.

Payment Design: Our mechanism provides payments to the elected *RA*s for running their monitor. The payment is in the form of reputations, which are then used to increase the trust level and allocate the cluster's services. Hence, any node will strive to increase its reputation in order to increase the trust level.

The following design of payment is strategy proof where truth-telling is the dominant strategy:

$$p_i = F_i + \sum_{i \in N} v_i(o*) - \sum_{j \in N} v_j(o*) \tag{2.9}$$

where o^* is the optimal selection of nodes that maximizes the sum of all the agent's declared function value. Here, $\sum_{j \in N} v_j(o*)$ denotes the second maximum summation assuming without node i.

The moderate to robust game model:

We model the game as nonzero-sum noncooperative game with incomplete information about the players where each player has a private information about his/her preferences. In our case, the CA type is known to all the players while the sender type is selected from the type set $\Theta = \{Malicious\ (M),\ Normal\ (N)\}$. Knowing that the sender type is a private information. *Bayesian Equilibrium* [58] dictates that sender's action depends on his/her type θ. We can determine the behavior of the sender at time t_k, the CA can calculate the posterior belief evaluation function $\mu_{t_{k+1}}(\theta_i|a_i)$ using the following Bayes' rule:

$$\mu_{t_{k+1}}(\theta_i|a_i) = \frac{\mu_{t_k}(\theta_i)\ P_{t_k}(a_i|\theta_i)}{\sum_{\theta_i \in \Theta} \mu_{t_k}(\theta_i)\ P_{t_k}(a_i|\theta_i)} \tag{2.10}$$

where $\mu_{t_k}(\theta_i) > 0$ and $P_{t_k}(a_i|\theta_i)$ is the probability that strategy a_i is observed at this stage of the game given the type θ of the node i. It is computed as follows:

$$P_{t_k}(Attack|\theta_i = M) = E_m \times O + F_m(1 - O)$$

$$P_{t_k}(Attack|\theta_i = N) = F_m$$

where O is the probability of attack determined by the CA. F_m is the false rate generated by the CA. E_m is the expected detection rate by a RA (moderate mode).

We define the intruder's pure strategy as $A_i = \{Attack, Not\_Attack\}$. On the other hand, CA strategy is selected from the strategy space $A_{IDS} = \{Robust, Moderate\}$. By solving this game using pure strategy, there is no Nash equilibrium. Thus, mixed strategy

Table 2.1 – Moderate to robust game

Strategy	Robust	Moderate
Attack	$\overline{E_r}V - C_a, \quad E_rV - C_r$	$\overline{E_m}V - C_a, \quad E_mV - C_m$
Not-Attack	$0, -C_r$	$0, -C_m$

is used to solve the game where q is the probability to run in robust mode and p is the probability to attack by the attacker.

In Table 2.1, the game is defined where the utility function of the CA by playing the *Robust* strategy while the attacker plays the *Attack* strategy is defined as $E_r\ V - C_r$. It represents the payoff of protecting the CA node, which values V, from being compromised by the attacker, where $E_r\ V >> C_r$. On the other hand, the payoff of the attacker if the intrusion is not detected is defined as $\overline{E_r}\ V - C_a$. It is considered as the gain of the attacker for compromising the CA node. Additionally, we define $E_m\ V - C_m$ as the payoff of the monitoring mechanism, if strategy *Moderate* is played while the attacker strategy remains unchanged. Conversely, the payoff of the attacker if the intrusion is not detected is defined as $\overline{E_m}\ V - C_a$. Now, if the attacker plays *Not-Attack* strategy and the CA strategy is *Robust* then the losses of the CA is C_r while the attacker gains/losses nothing. Moreover, the payoff of the attacker with the same strategy and CA strategy is *Moderate* is 0 while the losses of the monitoring mechanism is defined as C_m which is the cost of running the CA in moderate mode. For more details, and game resolution you can refer to this paper [25].

2.4.3 Summary of results

We focus on the impact of selfish nodes on the network. The nodes can behave selfishly before the election by refusing to serve as RA. This selfishness has a serious impact on resource consumption of the normal nodes. The obtained results indicates that normal nodes will carry out more the duty of RA and die faster whenever the number of selfish nodes increase. Thus, the presence of selfish node effect the lifetime of the entire network.

We study the performance of the proposed clustering algorithm, and focus on the average number of CA nodes that can create clusters. The obtained results show that as the transmission range increases the number of clusters decreases. The number of CA nodes of our algorithm is greater than others. Hence, we can conclude that the proposed algorithm is flexible with respect to cluster's formation.Thus, nodes' CA service will be enhanced and probability of detecting the misbehaving nodes can be increased since nodes will be distributed over more number of CAs.

Finally, we consider the tradeoff between security and resource consumption by formulating the problem as a nonzero-sum noncooperative game between the CA and attacker. The obtained results are provided to support our solutions. More results details and analysis are presented in these papers [26, 25].

2.5 Conclusion of the chapter

In this chapter, we addressed the resources management, and security issues in MANETs. Our first contribution related to QoS provisioning for competitor nodes particularly rate adaptation scheme called REFOT (Relative Fairness and Optimized Throughput) consider a fully distributed approach [20, 21]. Ensuring the dynamic rate

adaptation with relative fairness guarantee, and with throughput optimization in MANETs is a challenging issue. In this contribution, we answer the following question: Which adapted rate selection enables the throughput and relative fairness optimization? REFOT takes into account not only the QoS in terms of throughput in rate adaptation algorithm, but also the relative fairness between competitor nodes.
We know that MANETs can be used to extend existing infrastructure network (WLAN). In this context, the second contribution attempts to give an answer to this question: how to allocate the network resources to incite relayed nodes to cooperate? In this regard, an incentive scheduler algorithm called CEI is proposed to allocate the resources taking into account not only the QoS parameters but also the cooperation rate of nodes [22, 23]. The main idea is to reward the relayed nodes for their cooperation instead of penalizing them by increasing the cost of cooperation. An analytical model is proposed to perform the CEI algorithm. The simulation results in the trade-off between cooperation rate and QoS parameters with CEI.
In order to detect and mitigate the impact of misbehaving nodes (eg. greedy, selfish, and non-cooperative nodes) in terms of security, we propose two approaches: 1) monitoring and detection mechanisms, and 2) incentive models based on game theory. Our third contribution attempts to answer this question: how to monitor and to detect the misbehaving nodes without any false alarm due to interference? In this regard, we propose a new monitoring mechanism based on MIMO technology particularly the Spatial Reuse Using MIMO Channel-Aware MAC called (SPACE-MAC) called MIMODog [47, 24]. The key idea is to nullify the interference at the monitor (detector) nodes and then increase its observation by using the weight vectors related to antennas of MIMO system. The theoretical study of the monitoring capacity analysis, and the number of monitor nodes using graph theory particularly conflict graph, and an asymptotic approach is proposed.
In our fourth contribution, we answer the following question: how to motivate and to incite nodes to act as monitor of misbehaving nodes? In this regard, we propose an incentive model based on a mechanism design from game theory [26] [25]. We applied our model to the distribution of Certification Authority (CA) role with cluster-based architecture. The proposed mechanism will motivate unknown nodes to participate by giving them incentives in the form of trust, which can be used for cluster's services. We consider the tradeoff between security and resource consumption by formulating the problem as a nonzero-sum noncooperative game between the CA and attacker.

These contributions are the results of collaborations with colleagues: A. Benslimane ([20, 21]), C. Gueguen ([22, 23]), H. Badis ([47, 24], and H. Otrok ([26, 25]).

Chapter 3

VANETs

In this chapter, we address the problem of collaborative data dissemination in VANETs through the following four questions: "*How to perform data dissemination?*", "*When should we do it?*", "*What must be disseminated?*", and "*How to secure it?*" We have provided answers to these questions through the four contributions classified into two main topics: QoS and security.
In the QoS topic, two main contributions are proposed: our first contribution is an *efficient* dissemination strategy called ADCD, specifically tailored to the importance of the exchanged information as well as its lifespan, which is able to avoid the intensive dissemination process that generates network congestion and data redundancy [28, 27]. In the second contribution, we propose a communications channel access scheduler called DMS (Distributed MAC Scheduler), which aims at reducing the number of collisions caused by IEEE 802.11p/1609.4 multi-channel synchronizations, and thus improving the data reception rate[29, 30].
In security topic, we contribute to the *reliability* of the dissemination process, which is obtained by inciting vehicles to cooperate and evicting malicious vehicles from the process. We focus on the distributed trust model, and dynamic trust metric evolution in VANETs [31, 32, 33, 35]. Finally, in the fourth contribution, we focus on a dynamic distributed Public Key infrastructure (PKI), and certificates management for vehicular ad hoc networks [36, 34]. We propose a mechanism to provide anonymous vehicle-to-vehicle communications using pseudonyms.

3.1 Efficient data dissemination protocol (ADCD)

3.1.1 Research context

We focus on data dissemination and distribution based on targeting the concerned nodes, i.e. the nodes that should receive the information and can be interested in its content according to its geo-location, and on the data characteristics like importance, location and time of collection.
Our main motivation comes from the fact that the congestion and the redundancy induced in order to ensure the reception of relevant messages by the concerned nodes, is an important drawback of previous works. Thus, we propose a new protocol for Advanced Diffusion of Classified Data (ADCD). ADCD targets the receiver nodes to avoid both redundancy and network congestion. Therefore, ADCD differentiates the sensed data according to their relevance and period of validity, in order to better predict its importance for the other nodes in the network. Once the first step achieved, the collector node

customizes the diffusion by electing a number of broadcasters from its neighborhood according to the importance of the message, while reducing the redundancy by binding the election process to different criteria (node density, node positions). Finally, the third step consists in verifying whether the limits of the message broadcast, in terms of targeted broadcasting area and content validity in time, had been reached or not. In addition, we propose a new analytical model based on Markov chains for ADCD. This model results the delivery ratio, the overhead, the probability of a complete transmission and the minimal numbers of hops; and allows us to optimally select the ADCD parameters.

3.1.2 ADCD description

ADCD is based on three main parts: (i) data classification, (ii) relayed node election, and (iii) iterative rebroadcast with corresponding scope. It uses an adaptive broadcast algorithm based on the election of a fixed number of relayed nodes to reduce the overhead without neglecting the reception ratio.

Data classification:
We consider that each collected information depends on the region where it was collected. Thus, its diffusion is only useful in its surroundings during a fixed period of time to avoid the transmission of old information. In order to carry out this concept, we characterize information with two parameters: *class* and *mode*. A class represents the importance level of information; it is used to define the broadcasting area within the VANET. The mode is a value in a scale representing the period of validity of the data. ADCD defines an interval $[\sigma_{min}, \sigma_{max}]$ for the classes and modes.

The information is represented by Cxy, where x represents the class and y the mode. The vehicles concerned by particular information are those belonging to the targeted broadcast area and for which we advocate interest in receiving this information. In order to target these vehicles during the transmission, we attribute a diffusion perimeter, as a square centered upon with the coordinates of the collected data. The length of each square side corresponds to the class of data.

Relayed nodes election:
Each vehicle cooperates in the network by sending its collected data to other vehicles. To avoid redundancy, the information is shared only if it meets the following conditions:

— The vehicle has recently collected the data.
— The vehicle can retransmit the data only if the previous message regarding it has reached its time validity and the information is always valid.
— None of the vehicle's neighbors already distributed this information.

In order to avoid the classical broadcast (i.e. flooding), and the broadcast storm, we use the class and the mode associated to the data in the dissemination process. In addition, the election of nodes (called relayed nodes) to transmit the information is required to reduce the impact of the redundancy. The number of elected relayed nodes depends on the information class. For instance, in the case of the number of elected nodes is three, the first elected node is the neighbor of source node with the highest density. Then, the two other elected nodes are chosen according to their rotation angle (Θ) relative to the previous elect and their density. The algorithm 2 summarizes the election process.

Analytical model

We use the discrete-time Markov chain (DTMC) with a Binomial distribution to model the dissemination process. This model is presented by states (i, j), such as $i \in \{0, 1, 2, \ldots, N\}$ and $j \in \{0, 1, 2, \ldots, N - i\}$. The states are represented by the number

Algorithm 2: Relayed nodes election algorithm

Input: elect_ number;
begin
  $\Theta = \frac{360}{elect\_number}$;
  I=0; Y=1;
  Elect_tab[0]=Look_node_highest_density(list_neighbors_sender);
  Delineate_areas_with_angle_according_to($\Theta, coordinates\_of\_Elect\_tab[0]$)
  while $Y < elect\_number$ **do**
    Elect_tab[Y]=Look_node_highest_density(list_of_area(y));
    Y++;
Output: Elect_tab;

of nodes that received the message, and the edges are represented by the probabilities regarding the transition from one state to another. The first dimension i of a state represents the number of nodes, which have already received the message and therefore have transmitted it once at most. The second dimension j is the number of nodes, which have recently received the message among the remaining nodes $N-i$, then able to retransmit it in the next step. Possible state's transactions are from (i,j) to $(i+j,m)$ such as $m \in \{0,1,2,\ldots,N-i-j\}$ and represents the future receiver nodes. To determine the probabilities of this model, we assign a probability P to the existence of a link between two nodes and Q to its non-existence or disappearance. This connectivity graph can be viewed as a Markov chain whose stationary probability for existing link is calculated as follows: $\pi = \frac{P}{P+Q}$, this value represents the probability of reception for a node during one step, and allows to calculate the average node degree by $\pi \times (N-1)$. Figure 3.1 illustrates the Markov chain for ADCD, which has $1 + N(N+1)/2$ states. The initial state $(0,1)$ represents the case where the source is the only holder of the message, the final state $(N,0)$ the case where all the nodes have received the message and there are $(N-1)(N+2)/2$ remaining states representing all the possible transition states (i, j).

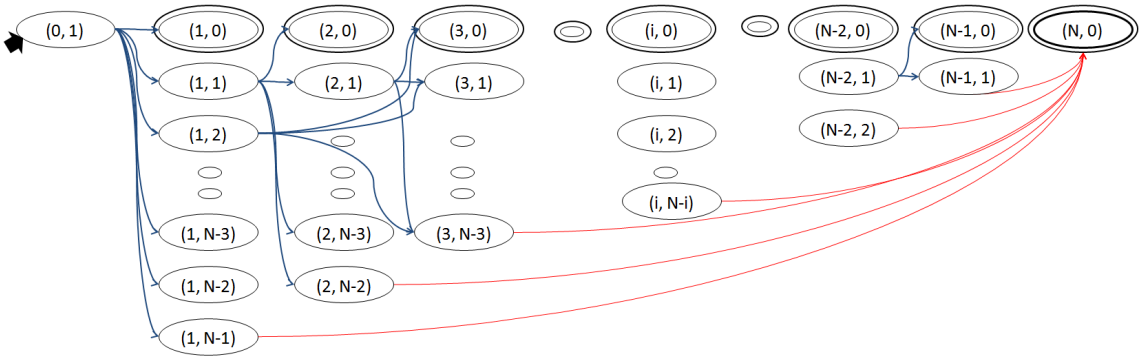


Figure 3.1 – The discrete-time Markov chain for ADCD.

The transition probability from (i,j) state to $(i+j,m)$ state is calculate as fellow:

$$\begin{aligned} P[(i,j)(i+j,m)] &= Pdf_B(m, 1-(1-\pi)^D, N-i-j) \\ &= \left(\frac{(N-i-j)!}{m! \times (N-i-j-m)!}\right) \times (1-(1-\pi)^D)^m \times (1-\pi)^{D(N-i-j-m)} \end{aligned} \tag{3.1}$$

where,

$$D = \begin{cases} Number\ of\ elected\ relayed & If\ D\ >\ j \\ j & Otherwise, \end{cases}$$

We consider this process as a binomial one where we have j attempts to transmit the message to the m nodes. The result can be a success or not between each couple of nodes. This binomial distribution has n and p as parameters, so that $m \sim B(n, p)$, n represents the number of nodes which have not yet received the message, equivalent to $N - i - j$ in our model and p the probability of receiving a message sent by D nodes during the same step. The network connectivity π is considered, and probability to send data with success is $1 - (1 - \pi)^D$ [59].

3.1.3 Summary of results

In order to adapt the number of selected relayed nodes (chosen regarding to the class and mode of information), we study the evolution of the packet delivery ratio (PDR), the number of relayed nodes, and the generated overhead. The obtained results show that 100% of PDR is reached in the case of high priority of the couple (class, mode). However, PDR decreases to reach 60% when we reduce the importance level of the information. We evaluate the impact of the vehicle nodes density on the ADCD performance; and the obtained results show that even if the nodes density increases the percentage of concerned nodes remains stable (and greater than 90%) in the case of ADCD, which is not the case of existing solutions like blind broadcast (without any strategy), and adapted MobEyes [60]. In these existing solutions, the percentage of concerned nodes cannot even reach 50% and 40%, in the case of blind broadcast, and MobEyes, respectively. These results confirm the efficiency of ADCD for the target diffusion even with a small density which can limit the possibilities of rebroadcast in a large area.

In the case of the number of relayed nodes, the results show that there is no significant difference in terms of performance when we exceed a certain number of relayed nodes. This prove that our strategy is appropriate.
Finally, the overhead is significantly reduced by up to 90% compared to other existing protocols. We notice the linear increase of the ADCD overhead compared to the exponential increase experienced by both other evaluated protocols, the Blind broadcast and adapted MobEyes. This mainly due to the selected strategy, where we consider the classification of data to disseminate, and the election of the relayed nodes.

3.2 Distributed MAC Scheduler (DMS)

3.2.1 Research context

The transmission mode used to distribute and disseminate the information in VANETs is the *broadcast* one. In this mode, the sender is not able to know if a packet is well received or not, and which vehicle(s) did not receive it, because of the lack of acknowledgments for broadcast in the IEEE standard 802.11-2012 [14], which includes the IEEE standard 802.11p [15] dedicated to VANETs. In addition, since the contents of the messages are highly important, any congestion problem disturbing the transmission of safety messages can cause unsafe situations on road traffic.

In the IEEE Std 802.11p [15], safety and non-safety messages coexist by using the IEEE 1609.4 multi-channel operations [61] over the 5.9 GHz Dedicated Short Range

Communications (DSRC) spectrum [62], where seven 10 MHz channels are used for both Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communications. In the MAC layer of this architecture, the time is devised into SYNChronization intervals (SYNC) of 100 ms. During the first half (50 ms) of the SYNC interval, all the vehicles tune into the Control CHannel (CCH), dedicated to the transmission of safety and control messages. Then, during the second half (50 ms) of the SYNC interval, each vehicle decides to remain on the CCH or to switch to one of the six available Service CHannels (SCHs), dedicated to the driver and passenger comfort applications. Between channel switches, there is a guard interval that lasts 4 ms, and makes the channel busy for both type of applications.

In the safety application, a vehicle transmits during the CCH interval, the vehicle can only use 46 ms, since the guard interval between channel switching needs to be deducted. Moreover, as demonstrated in the literature [63][64], queuing safety messages during the SCH interval and the guard interval increases heavily the competition for channel access at the beginning of a CCH interval. This causes a burst loss due to collisions, and an uneven use of the channel as illustrated in Fig. 3.2, where 20 nodes are in the same coverage range, sending 1 and 2 messages per SYNC interval. Because of the safety message queuing, and the increase of their end-to-end delay during this period, a large number of messages are sent at the beginning of the CCH interval, thus making it busier than the rest of the time.

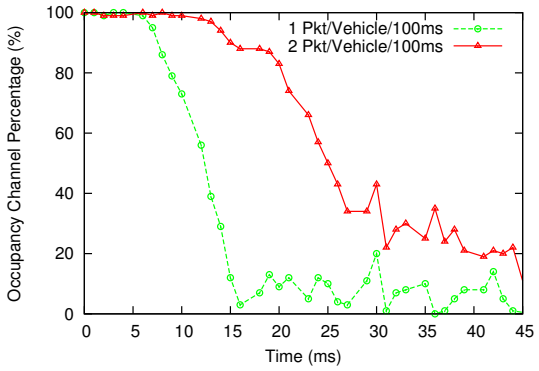


Figure 3.2 – CCH load percentage over time

To tackle the CCH resource management issue, we propose a Distributed MAC Scheduler called DMS to better balance the load during the CCH interval, and to reduce the risk of collisions.

3.2.2 DMS description

The DMS is adapted from the Optimal Stopping Theory [65][66], which provides an answer to the question: *"Is it better to send my packet now or to defer it? And if the decision is to defer it, then how long the deferment should be?"*. The aim is to find a trade-off between delaying messages, and ensuring a high reception probability with respect to performance metrics. The channel load balancing is transformed into a distributed decision problem, where each vehicle takes the decision to either send immediately or to defer its message transmission, with respect to the message AC [1] and to the estimation of future channel load. The objective is to send a message with a high success probability, during its validity time (i.e. relatively to its AC). For the resolution of our model we use a Markov Decision Process (MDP) [68].

1. DMS complies with the Enhanced Distributed Channel Access (EDCA) access categories (ACs) [67]

The vehicle with a message to send expects to maximize the success sending probability of its messages by waiting for the less loaded period in the channel, while at the same time reducing the end-to-end message transmission time. However, in this particular case, the time a vehicle can wait in order to defer the transmission of a message is limited by the validity time of the message VT.

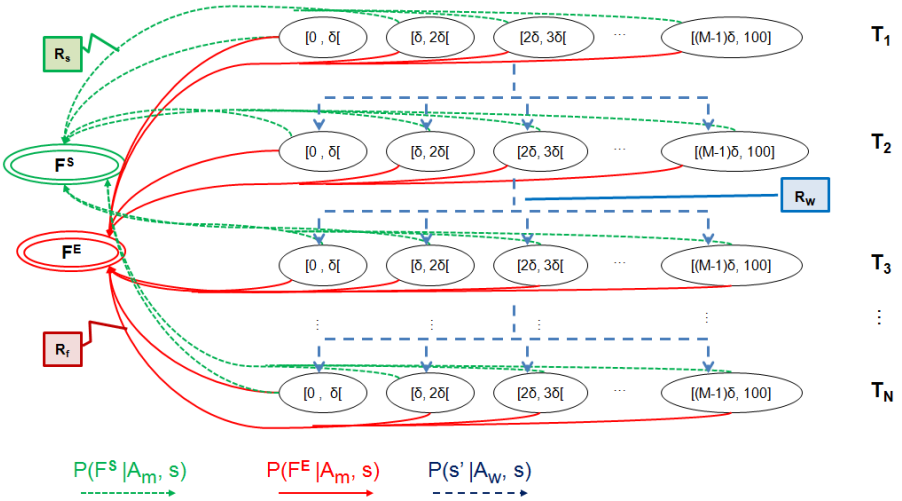


Figure 3.3 – Markov Decision Process for Optimal MAC Transmissions using 1609.4

We formulate the problem as a MDP for a finite horizon process. Indeed, the possible deferring time for a message is divided into a countable time step N that forms a decision period set T, such that the SCH interval and guard interval are removed if encountered during the validity time of the message. The duration of the period t depends on the needed precision for the problem resolution. Figure 3.3 illustrate the proposed MDP.

Decisions period set: $T = T_1, ..., T_N$

Where $N = \frac{VT}{t}$,

$$T_{i+1} - T_i = t + \eta \times T_{SCH} + \upsilon \times T_{guard} \text{ when } i < N$$

$$\eta = \begin{cases} 1 & If \;\; SCH \; interval \; encountered \\ 0 & Else \end{cases}$$

$$\upsilon = \begin{cases} 1 & If \;\; guard \; interval \; encountered \\ 0 & Else \end{cases}$$

A MDP is composed of the process states S, the actions $A_s^{T_i}$, the rewards and costs $R(s'^{T_{(i+1)}}, s^{T_i})$ that depend on two states used as parameters, and the transition probabilities $P(s'^{T_{(i+1)}}|a, s^{T_i})$. A state transition occurs between two states $s'^{T_{(i+1)}}$ and s^{T_i} time-shifted with $(T_{(i+1)} - T_i)$, after taking action a.

The states:

The process states S are divided into two parts, the channel occupancy states C and the absorbing states F. Its formulation is as follows: States: S=C+F

Actions:

At each time step, two actions $A_s^{T_i}$ (A_m, and A_w) can be selected during a time period T_i, and for a state $s \in C$. A_m: a vehicle can send its message immediately. A_w: a vehicle

waits during a time period if the message is still valid in time.

$$A_{s^{T_i}} = \begin{cases} \{A_w, A_m\} & If \;\; s^{T_i} \in C \;\; and \;\; i < N \\ A_m & If \;\; s^{T_i} \in C \;\; et \;\; i = N \end{cases} \tag{3.2}$$

Rewards and costs:
The expected final benefit takes into consideration the different rewards and costs $R(s'^{T_{(i+1)}}, s^{T_i})$ received or deducted during the transitions between the states.

Problem Resolution:
The proposed MDP offers a sequence of actions, where each action corresponds to a time step. This mapping between decided action d_i, and channel occupancy probability at time step T_i, forms a policy $\pi(T_i) = \{d_1, d_2, ..., d_N\}$. In order to find the optimal policy $\pi^\star$, we use dynamic programming algorithm, by performing multiple iterations, until the results converge (i.e. the chosen action for each case remains fixed). The convergence time is considered as non significant (vehicle not limited by the processor capacity). Thus a vehicle can run the model in real-time, or in advance by taking into consideration all the possible combinations.

After obtaining the optimal policy from the actual channel occupancy state, a vehicle follows the actions in it, until it reaches the immediate transmission action A_m. Otherwise, the vehicle delays sending its message during one, two or $(N-1)$ time periods to maximize the chances of a successful sending.

3.2.3 Summary of results

We evaluate the performance of DMS by focusing on its ability to equally balance the channel load over the CCH interval and to avoid synchronous collisions, which generally occur at the beginning of the CCH interval. We measure the performance achieved by the proposed solution, and we compare it to the ones attained in other scenarios using different solutions. We use the following performance metrics: 1) The channel occupancy percentage; 2) The packets loss percentage; 3) The packet Delivery ratio (PDR); and 4) The end-to-end delay. The DMS is compared with existing solutions: Random deferring, and WAB [69]. The WAB solution deals with weak performance of safety applications caused by the channel switching, by dynamically adapting the channel conditions.

In the case of channel occupancy, we remark that when the traffic load is at its maximum, the channel occupancy percentage at the start of the CCH interval is higher than 90% for the Legacy IEEE 1609.4, the Random deferring solution, and WAB. We can clearly notice that when using this three approaches the channel occupancy is unbalanced. At the middle and at the end of the CCH interval, the channel is underutilized when the Legacy IEEE 1609.4 and the Random deferring delay are used, since the channel occupancy is around 50% in the second half of the CCH interval. On the other hand, the occupancy percentage when DMS is deployed is around 85% at the beginning of the CCH interval and remains stable during the entire CCH interval.

The obtained results show that the packets loss at the beginning of the CCH interval are important for the Legacy IEEE 1609.4, the Random deferring solution, and WAB. This is mainly due to synchronous collisions occurring at the beginning of the CCH interval. We also notice some losses at the end of the CCH interval, just before switching to the guard interval. These losses are higher in DMS, and are around 1% of sent packets. Because of the fixed deferment delay for each access category, if a node has not sent its packet, or a node captures a packet to send at the end of the CCH interval, it has to choose between

sending it immediately, even if the channel is already saturated, or waiting more than 54 ms for a new CCH interval.

In the case of packet delivery ratio, the obtained results are opposite to the channel occupancy channel. This clearly shows that when the channel occupancy is lower, the sent packet reception percentage is higher. We notice that both Legacy IEEE 1609.4 and Random deferring approaches have a low reception percentage in the first half of the CCH interval, which varies from around 30% to 80%, and then it increases until reaching 95% in the second half. In contrast, during the second half, since the sent packets are fewer, the channel is underutilized and there are fewer losses and higher reception percentages. The DMS approach enhances the reception percentage by redistributing the traffic load during a SYNC interval. The reception percentage is around 80%.

With end-to-end delay metric, we verify the sent packets are always valid over time, and then to avoid loading the channel with outdated information. DMS fixes a maximum deferment delay for each access category (AC) in order to limit the end-to-end delay. The simulations results show that DMS has an average deferment delay of 40 ms for AC3, the most urgent and important information, 50 ms for AC2, and 60 ms for AC1 and AC0. These delays are considered as reasonable for safety messages in VANETs. In addition, tuning DMS parameters, such as the cost and reward values, we can increase the reception percentage by increasing the maximum deferment delay for ACs.

3.3 Distributed Trust Model

3.3.1 Research context

In vehicular environments, the time to react to a given situation is very critical and a vehicle must be able to accurately check the trust of the received information in real time. The trust and reputation models [70] are proposed as new approaches to circumvent with this constraint and to filter out inaccurate messages and malicious vehicles. Trust establishment is tagged in many existing research works for peer to peer, sensors, and mobile ad hoc networks [70] [71]. However, in vehicular environments it is facing tremendous specific challenges related to their characteristics. The main existing trust models for VANETs are based on the verification of vehicles identities and their legitimacy in the network [72], [73], [74]. They are classified as entity oriented models such as identity-based systems where the trust metric is related to the vehicle credentials and its trustworthiness is static. Other existing trust models are based on a data-oriented approach. Indeed, in VANETs, when the vehicle introduces a new information in the network it will be responsible for the consequences of this information.

The presence of misbehaving nodes can have a negative impact on network performance. In particular, we are interested in dealing with this nasty presence in road safety applications, based on VANETs. We consider as harmful the presence of malicious nodes, which spread false and forged data; and selfish nodes, which cooperate only for their own benefit. To deal with this, first we focus on the trust model that motivate vehicles to well-behave and to cooperate. The first contribution is a Distributed Trust Model based on two approaches: 1) signaling games (which are a type of dynamic Bayesian games); and 2) Fuzzy-based. In the first approach, we propose an incentive model called DTM^2. The main idea consists in allocating *credits* to nodes and securely managing these credits. To motivate selfish nodes to cooperate more, DTM^2 establishes the cost of reception to access data, forcing them to earn credits. Moreover, to detect and exclude malicious nodes, DTM^2 requires the cost of sending, using signaling values inspired form

economics and based on the node's behavior, so that the more a node is malicious, the higher its sending cost, thus limiting their participation in the network. In the fuzzy-based approach, we focus on the decision about honesty of vehicles. This point is sensitive and important because it is responsible on false alarms issue. This technique enables to filters out malicious vehicles with good performance.
In the second contribution, we focus on trust metric variation, and its stability in the context of VANETs. The proposed model takes into account not only the dynamic trust metric variation according to the vehicles behaviors, but also the constraints related to the monitoring process. In our model each vehicle can act as monitor and update the trust metric of its neighbors according to their behavior in the network. In addition, this model can be customized through different parameters like the trust interval and the number of transitions needed to reach the highest trust level. This flexibility enables to adapt the model according to the application context.

3.3.2 Signaling games-based approach

The DTM^2 is based on the signaling games [75], which is a type of dynamic Bayesian game with incomplete information. This approach forms the basis of multiple solutions in economics to cope with the lack of information between sellers and buyers about the quality of proposed wares. We adapt one of the well-known examples of the signaling games, the Spence model, also known as job market signaling, to a VANET in order to obtain a functional trust and collaborative network.

Spence's model is adaptable to a VANET, since nodes in this kind of networks also suffer from asymmetric information regarding the behavior of each of them. Because of long and infrequent meeting intervals, it is difficult to establish valid and truthful links between nodes only by using a reputation model. Moreover, Spence's model provides a solution to the common problem found in both VANETs and markets, which consists on how to force their members to reveal their real nature to others. This is obtained by encouraging each member to choose the optimal action for it. Therefore, both nodes and the network are able to benefit, without overloading the network, and without requiring a heavy infrastructure in case of VANETs.

The DTM^2 is credit-based technique where the signal value is used in sending message as guarantee of node truthfulness. The signal cost depends on the remaining credit of each node. Upon their first connection to the network, each node receives the same amount of credit. This credit is used to pay the signaling cost when sending a message, and to decrypt received messages. It increases when a sent message is approved by the majority of recipient nodes.

DTM^2 description

Fig. 3.4 illustrates the process of exchanging a message using DTM^2. In this example, node A broadcasts a message, and vehicle B is one of the receivers. First, node A chooses a signaling value Y_A. This value is attached to its message Msg_A, and both of them are sent to its TPM (Trusted Platform Module)The TPM is a hardware device proposed by the TPM groupe [76], and it performs cryptography capabilities, while being tamper-proof. TPM_A uses the credit count of node A, θ_A, to compute the corresponding cost, C_A, of its signal value Y_A, and then subtracts it from the credit count. To ensure the integrity of the mechanism, the TPM signs and encrypts the message, M_A, which contains both the signal value Y_A and the data to share, Msg_A, using its signing and symmetric keys, and then returns it to node A.

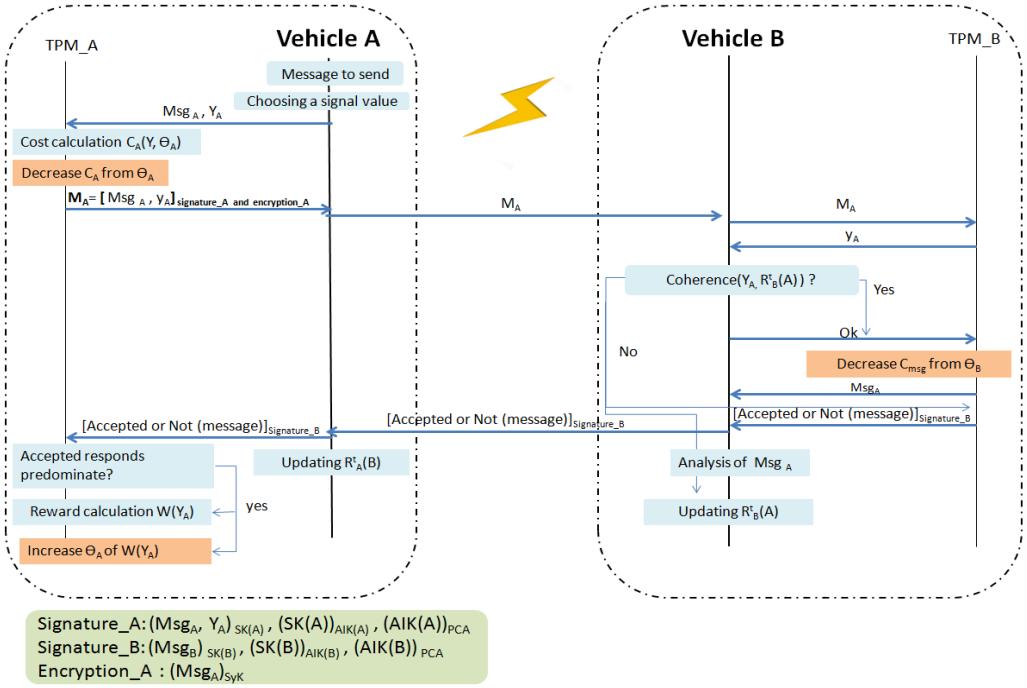


Figure 3.4 – Process for a message exchange using DTM^2, where vehicle A broadcasts a message and vehicle B is one of the receivers.

When node A broadcasts message M_A, node B receives it and asks the TPM, TPM_B, to verify the signature and to decrypt the signal value for it in order to evaluate its coherence with the reputation value it holds on node A, $R^t_B(A)$. If the reputation is coherent, then node B accepts the message and asks TPM_B to decrypt the rest of the message, which contains the data. Then, its TPM subtracts the cost of receiving a message, C_{msg}, fixed by the application; and delivers the decrypted data, while returning a signed acceptance message about the received information to node B, which will be sent to the source node. In case B refuses the message, a signed refusal message from TPM_B is sent to source node A.

In both cases of acceptance and refusal, the reputation values of both nodes A and B are updated, for the sent message of A, and for the acceptance or refusal message of B, as described in [77]. Finally, if node A receives a majority of positive returns from its recipients, then TPM_A increases its credit count by a reward, $W_A(Y_A)$, proportional to its used signal value Y_A.

The signaling cost concept:
The signal Y used by a source node acts as a guarantee about the validity of its messages and its honest behavior. An optimum signal value maximizes the net benefit of a node.

The signaling cost computation is presented in equation (3.3). It uses two positive real coefficients β and α. β in order to normalize the signal value regarding the credit count of a node, and α to have a larger impact on the the credit value in the signaling cost computation, such as the higher α, the greater the difference between the signaling costs for the same signal value, paid by different nodes holding different credits. This can be used to detect malicious nodes more or less quickly.

$$C(Y, \theta) = \frac{\beta \times Y}{\theta^{\alpha}} \tag{3.3}$$

where β, α, θ >0

To avoid cheating or security problems when a node pays a signaling cost, the TPM calculates the cost and deducts it from the node's credit. It then encrypts the message containing both the data to share and the signal value by using its secret key, and returns it to the node.

The reward value:

To motivate nodes to cooperate, DTM^2 proposes incentive rewards to truthful nodes for their sent messages. A reward value depends on the signal used by the source node, which is the node that detects or forwards a detected event. The secondary goal of this reward is to obtain self-selection of the nodes, which we name a *separating equilibrium*, by inciting them to maximize their benefit by not cheating on their used signal value. The advantage of a self-selection is that it copes with frequent changes to the topology, as often found in VANETs.

Since the credit count of a node hints at the real behavior of a node, the reference wage value depends on it to make it proportional to the real behavior of the node. The reference wage is set by dividing the credit of a node by a coefficient σ, so that the higher the value of σ, the stricter application with regard to the final wage. The obtained final equation of the wage shown in (3.4):

$$W(Y) = \left(\frac{\beta \times (\alpha + 1) \times Y}{\sigma^{\alpha}}\right)^{\frac{1}{\alpha+1}} \tag{3.4}$$

The reward value is added to the credit count of a source node by its TPM, providing that its sent message is validated by the majority of recipients.

The optimal signal value:

This model is designed in such a way that a node makes the maximum benefit when it uses the optimum signal value $Y^{\star}(\theta)$ with regard to its credit, θ. DTM^2 incites vehicles to chose their optimal signal value because a signal value is directly observable by all, and mainly because it is directly related to the remaining credits of a vehicle due to its inducing cost. The optimum signal for each node is obtained from equation (3.4), by replacing $W(Y)$ with $\frac{\theta}{\sigma}$. The result is given in equation (3.5).

$$Y^{\star} = \frac{\theta^{\alpha+1}}{\sigma \times \beta \times (\alpha + 1)} \tag{3.5}$$

Received message acceptance process:

The second way to encourage nodes to cooperate is to create the need for holding credits and earning them. For this reason, decrypting the received message is paid in this model. In the case where a node is selfish, its credit decreases slowly because of its non existent or insufficient cooperation. The validation decision of the receiver node is made with respect to the following two criteria:

— The reputation of the source node, held by the receiver.

— The used signal value advertised by the source node.

The used reputation, $R_r^t(s)$, belongs to [0, 1], and is calculated at time t by the Receiver node r with respect to the source node, s. This reputation is local, based on directly observed behavior, and is not shared in the network. If it is too bad, i.e. $R_{r(s)}^t$ is less than a certain threshold ρ, it becomes an elimination criterion for the received message. It's computed as follow:

$$R_r^t(s) = \omega \times R_r^{t-1}(s) + (1 - \omega) \times \psi_r(s) \tag{3.6}$$

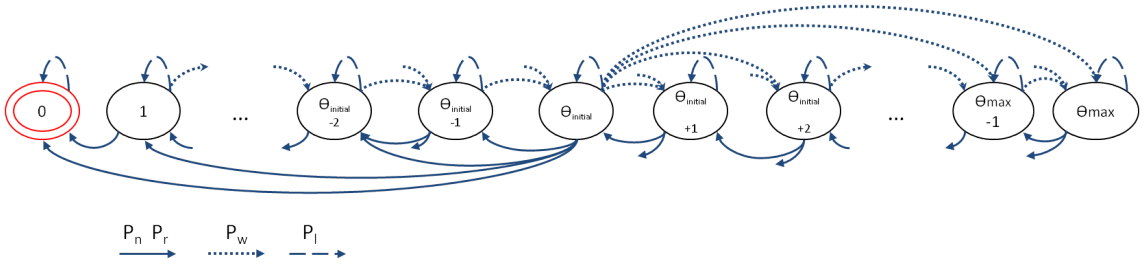


Figure 3.5 – Markov chain for DTM^2

where $\psi_r(s)$ is the value of the last observation made by node r concerning node s, and ω represents a fading factor to give a higher or a lower relevance value to past observation values.

After verifying the reputation criterion, a recipient node can base its acceptance on the signal used by the source. The minimum accepted signal is fixed to $Y^\star(\gamma \cdot \theta_{initial})$, which represents the optimal signal value for a node detaining only $\gamma \cdot \theta_{initial}$ of credits.

The analytical model for DTM^2:
In order to study the optimization parameter of DTM^2, we propose a Markov chain-based model. In this model, we consider the network characteristics, such as message collision probability, the vehicle's transmission range, the event frequency, and the connectivity between the nodes, to model a sufficiently realistic network with DTM^2 set up on it. From this model, we are able to obtain malicious node detection probabilities with its corresponding timing. Moreover, our model provides the detection probabilities of well-behaved and selfish nodes, while the former corresponds to the probability of false positive exclusions in the network.
Indeed, we use a Markov chain to model the credit change for a node in the network, according to its behavior. A state in our model represents a node's credit count value, θ. This value belongs to a range $[0, \theta_{max}]$, so that $(\theta_{max} + 1)$ is the number of states in our Markov chain. The transition probabilities of our model represent all the actions that can modify a node's credit (i.e. increase, decrease or stagnation), such as sending a message and paying a cost, or being rewarded for it.

We model road event detection as a Poisson process $P(x = k)$, with λ as arrival intensity. The initial state in our model is represented by the initial credit that a node receives the first time it joins the application. The final state is reached when the credit runs out and is equal to zero, and therefore the node is excluded from the application. The Markov chain for DTM^2 is illustrated in Fig. 3.5 where, P_n is the probability of credit decrease because of no received reward, P_r is the probability of receiving a message, P_w is the probability of updating credit with a Reward, and P_l is the probability of credit stagnation.

3.3.3 Fuzzy-based approach

We introduce a fuzzy-based approach in the distribute trust model to decide about the honesty of vehicles. We focus an hybrid trust model for evaluating the behavior of vehicles and estimating their corresponding trust metric (Tm). The idea consists on the monitoring and the assessment of the behavior of vehicles in two aspects: their cooperativeness in the network and the legitimacy of the information that they broadcast. Each vehicle must monitor all its 1-hop neighbors and calculate their Tm. In the network, the vehicles broadcast messages related to urgent events occurred on the road which are

called warning messages. Each time a monitor vehicle receives a warning message, it evaluates the cooperation rate of the source. After, it computes the reputation of the event reported in the received message. Then, using a *fuzzy-based* approach the monitor filters out malicious vehicles. Finally, according to the outcome of the monitoring process, it updates the Tm of the source. The $Tm(i)$ is a continuous value in $[0, 1]$. The vehicle is trusted (confident) if its Tm reaches 1. Hereafter, we present the different steps followed by a monitor in order to calculate the Tm of its neighbors.

Gathering information:
In all warning messages broadcasted by each vehicle, an information about the legitimacy of the event is attached to the messages that we call reputation ($Rep_V(E)$: the reputation of event E computed in vehicle V). In fact, around event $E(x, y, t)$ occurring in position (x, y) and at time t, we consider a static geographic zone Z where vehicles are able to directly detect the event using their on board sensors.

Evaluating information:
If vehicle V is beyond Z or it has not an exact information about the reputation of E, it computes $Rep_V(E)$ by aggregating all information about E, which are received from other vehicles in warning messages as follow:

$$Rep_V(E) = \frac{\sum_{i=1}^{i=|S|} Rep_i(E) \times d_i \times T_m(i)}{\sum_{i=1}^{i=|S|} d_i \times T_m(i)} \tag{3.7}$$

Where S is the set of vehicles from which V receives warning messages about E, $Tm(i)$ is the local trust metric of the vehicle i computed by vehicle V, and d_i is the distance between vehicle i and event E. We use the distance between the vehicle and the event because the closer the reporter is to the event location the more accurate its information on the event will be.

Evaluating vehicle behavior:
The behavior is evaluated by the monitor, based on the cooperativeness of the monitored vehicle and the legitimacy of the information that it broadcasts, as follow:

— *The cooperativeness:* a monitor calculates a forwarding rate called F .

$$F = \frac{\text{the number of forwarded messages}}{\text{the total number of transmitted messages}} \tag{3.8}$$

— *The legitimacy of the information:* Monitor V decides the honesty of monitored vehicle i based on $Rep_i(E)$. We use the fuzzy set theory [78] to classify honesty of vehicles. Each vehicle is classified within one of the honesty levels. First, an accordance degree corresponding to each vehicle i in S is calculated by monitor V as follow:

$$A_i = \frac{Rep_i(E)}{Rep_V(E)} \tag{3.9}$$

We define 3 honesty levels represented by fuzzy sets as depicted in figure 3.6. Then A_i is projected into one of the trust levels: (1) malicious (2) +/-malicious or (3) not malicious. As expected in figure 3.6, each fuzzy set F_k has a membership function $\varphi_k : F_k \rightarrow [0, 1]$ determining which honesty level each vehicle is belonging to. Hence, the probability that vehicle V is in honesty level 3 (not malicious) is computed as follows :

$$P_m = \frac{\varphi_3}{\varphi_1 + \varphi_2 + \varphi_3} \tag{3.10}$$

Updating T_m:
The updating process of the T_m is presented in figure 3.7. Initially the monitor affects

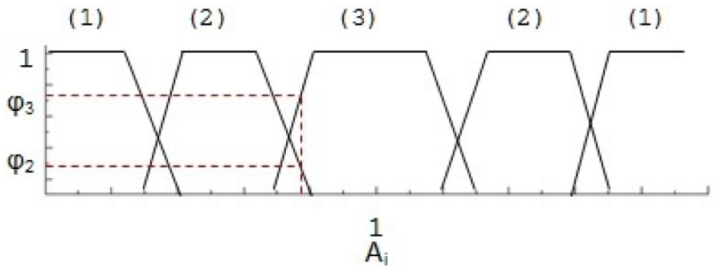


Figure 3.6 – Membership functions

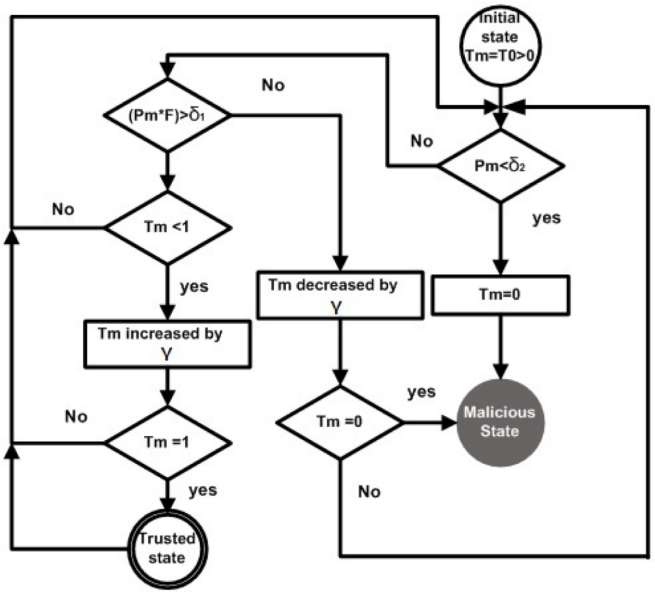


Figure 3.7 – The State-Transition Diagram of the Trust Model

$T_m(i) = T_0(0 < T_0 < 1)$ to monitored vehicle i . Then, according to the outcome of the evaluation of the behavior that monitored vehicle i exhibits, the monitor update $T_m(i)$. If P_m is less than threshold δ_2 , vehicle i will have $T_m(i) = 0$, and it is declared malicious. Otherwise, if the value of $(F \times P_m)$ is greater than threshold δ_1 then $Tm(i)$ increases by γ $(1 mod \gamma = 0)$, otherwise it decreases by γ. If $T_m(i) = 1$, vehicle i is trusted. It is worth mentioning that the values of δ_1, δ_2 and γ are defined as a function of the level of accuracy that we aim to perform towards the evaluation of $T_m(i)$.

3.3.4 Trust metric stability approach

In order to study the trust metric variation and its stability in VANTEs, we propose a formalize the trust metric by using a Markovien model. The goal of this modeling is to take into account different parameters related to the robustness, stability and flexibility of the trust model. Unlike static trust models, we propose a dynamic model based on the monitoring of the instantaneous vehicles behaviors in the network. The monitoring process considers the legitimacy of the information and the cooperation rate of the vehicles. We include also the constraints related to the efficiency of the monitoring process, particularly, the probability of false positives and negatives. Furthermore, our model is fully distributed, the assessment of vehicles behavior does not require any type of infrastructure.

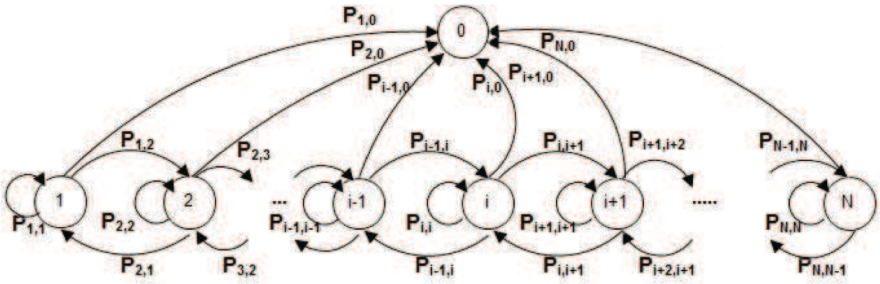


Figure 3.8 – States transitions diagram of the trust metric

The analytical model description

In order to establish a dynamic and distributed trust model where each vehicle called monitor affects a local trust metric T_m to each vehicle from its neighbors called monitored vehicle. In fact, the evaluation of the behavior of the monitored vehicle by the monitor vehicle is based on two main aspects: the reliability of the message sent by the monitored vehicle and its cooperation ratio. Thus, according to the outcome of the monitoring process, the monitored vehicle will have its T_m increased, decreased or unchanged. Additionally, the T_m can change to null, and as presented in figure 3.8, this transition is weighted by a probability related to the honesty of the monitored vehicle when it broadcasts the alert messages, also it depends on the current state of the vehicle.

We model the update process of the T_m at the monitor vehicle using a discrete-time Markov chain with $N+1$ states and a transition matrix $P = (P_{i,j}(t))_{0 \leq i,j \leq N}$ as represented in figure 3.8. Consider a random variable $(X_t)_{t \geq 0}$ which represents the current local T_m corresponding to a given state of a monitored vehicle assigned by a monitor vehicle, the probability of transition from state i to state j is:

$$P_{i,j}(t) = Pr(X_{t=j} | X_{t1=i}) \tag{3.11}$$

The T_m has a value in $[0, 1]$, state 0 is the non trusted state wherein $T_m = 0$ and state N is the highest trusted state where $T_m = 1$. Each vehicle has an initial trust metric $T_0 \in [0, 1]$. The interval [0, 1] is divided into $N + 1$ states, each one represents a step of $\gamma(1 mod \gamma = 0)$.The values of γ and N are determined based on the degree of accuracy assessment and severity towards the T_m of vehicles that we want to achieve with our model. By using these two parameters we aim to make our model flexible in the context wherein it is used.

— *increasing/decreasing of the* T_m: If the current state is i at time t and the vehicle shows a positive behavior, its T_m transits to the state $i + 1$ otherwise it transits to the state $i1$.

— *State sojourn probability*: A vehicle can keep the same Tm for a certain period of time because either it has no message in its buffer to forward or it has not detected events on the road.

— *Trusted state sojourn Probability:* The vehicle keeps the trusted state N ($T_m = 1$) either because it positively cooperates as discussed above or it has no messages in its transmission queue.

— *Transition to the non trusted state:* The monitor vehicle assesses both the cooperativeness of the monitored vehicle and the legitimacy of the information it broadcasts. Thus, according to the outcome of the monitoring process, the

T_m of the monitored vehicle can nullify with a given probability that reflects the legitimacy of its broadcasted messages.

In order to evaluate the cooperation of a monitored vehicle, first, a monitor vehicle calculates a forwarding rate called F.

$$F = \frac{\text{the number of forwarded messages}}{\text{the total number of transmitted messages}} \tag{3.12}$$

The monitor vehicle calculates the probability that the monitored vehicle has a positive cooperation in the network denoted p_c as follows:

$$p_c = F \times P_m \tag{3.13}$$

where P_m is the probability that the monitored vehicle is not malicious.
For details of the model resolution, you can refer to [35].

3.3.5 Summary of results

In the a distributed trust model based on signaling games called DTM^2, we focus on managing a tamper-proof credit count received by nodes at the start of the application. We select three performance metrics to evaluate this solution: 1) The detection malicious node delay; 2) The ratio of received and accepted false messages (false positive); and 3) The ratio of received data.

we compare the simulation results in highway and urban scenarios to the theoretical ones. We noticed that the detection rate reaches 100% gradually, and it's faster in the case of urban scenarios compared to the highway scenarios. The results show that the detection time of all malicious nodes in a network is not automatically multiplied by the event frequency, but can be lower or greater because of the node distribution. In fact, when the shared messages are so frequent, the nodes' reputations are quickly established, which leads to an effective decision for received messages in the network. So, the remaining credits quickly decreases for malicious nodes, and they are rapidly excluded. In addition, the results are better in urban scenarios than in the highway, independently of the network composition. The frequent neighborhood changes in urban scenario allows to retransmit received information more frequently, thus spending or earning more often credits, and holding larger view of the network. DTM^2 gives low average false positive rate around 0.5%. This is mainly due to the credit safeguard, where a node does not accept received messages when its credit level is too low. On other hand, we evaluate the ratio of received data with presence of selfish nodes, and with different scenarios. We noticed that the proposed solution reaches 100% in urban and highway even with the presence of 25% selfish nodes which is not the case where there no deployed solution. However, the negative impact is more important in the case of urban scenarios than highway. Since they have no incentive to cooperate, and no constraint if they refuse, selfish nodes do not cooperate.

In the fuzzy based approach, the obtained results show that this approach contribute in the stability of the trust model by significantly reducing the false alarms. The false alarms are mainly related to mis-estimation of the vehicle behavior.

The trust metric has an important impact in the trust model. That's why, we studied the trust metric and its stability in different scenarios. We proposed an analytical model based on discrete-time Markov chain to study the trust metric, and then to enhance the trust model. We evaluate the convergence of our model which consists in the required time and the needed conditions for a vehicle to reach the trusted state where Tm=1 (called trustworthiness of a vehicle) and to remain in. The obtained results confirm that the

trustworthiness is getting higher for high values of the forwarding rate F. However, the persistence in the trusted state strongly depends on the behavior of the vehicle expressed by Pm. The more positively the vehicle cooperates, the more chance it has to be trusted, and the longer it keeps its trusted state. Moreover, if a vehicle proves a malicious behavior even for a short period of time, this affects its trustworthiness on the network and it is difficult to restore the trusted state. We deduce that the proposed model is incentive. Indeed, the vehicle must be neither selfish nor malicious not only to reach the trusted state but also to remain in.

3.4 Distributed public key and certificates managements

3.4.1 Research context

Vehicular networks are characterized by an open architecture that raises tremendous vulnerabilities [16] [17]. Therefore providing information security is a serious challenge in VANETs. In order to achieve the fundamental security requirements, particularly the authentication, the confidentiality and a reliable vehicle-to-vehicle data exchange, Public Key Infrastructure (PKI) is a good promising choice. It is based on a trust third parti called certification authority (CA) which is responsible for certifying the public keys of vehicles. However, in VANETs, the conception of PKI must take into account the frequent disconnections in the network, and the CA must always be reachable by all vehicles.

In order to make the certification authority (CA) reachable by all vehicles, we propose to distribute its role among a set of dynamically elected vehicles using a cluster-based architecture. Due to the important role of the CA in each cluster and in order to protect it from DOS attacks, we introduce a concept of registration nodes (RA). Their role is to handle the certification requests sent to the CA from unknown vehicles and hence it avoids compromising it.

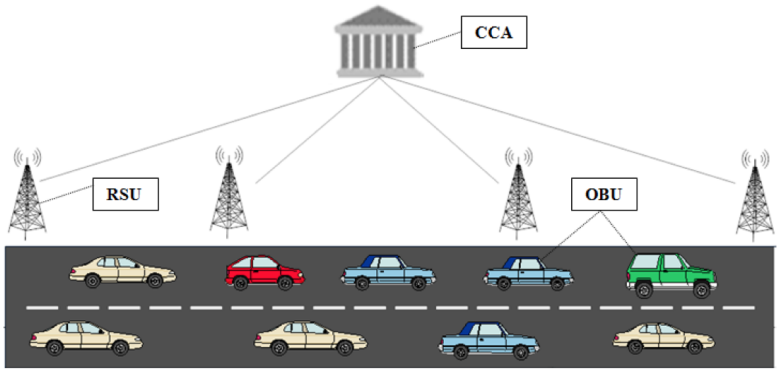


Figure 3.9 – The network model

Figure 3.9 show the used network model. In this model, the central certification authorities called CCAs manages all credentials of the vehicles registered with it. In addition, the road side units (RSU) are connected to the local servers and to the CCAs.

3.4.2 Architecture description

The proposed architecture consists in three main modules as presented in figure 3.10. First, we use a trust model in order to assign to each vehicle a trust level reflecting the

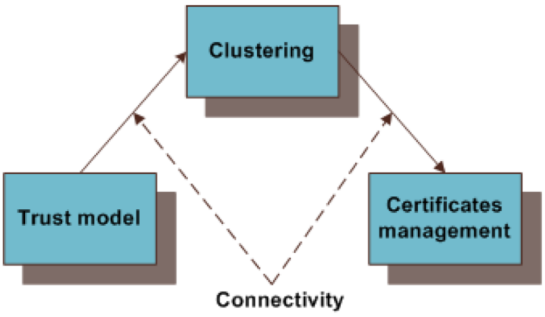


Figure 3.10 – Different modules of the distributed PKI

legitimacy of its behavior. The vehicles which have the highest trust level are considered trusted and they can be candidate to serve as CA. Secondly, in order to elect vehicles that will be the certification authorities in their cluster, a clustering algorithm will be executed. It is based on the trust level of vehicles and on their mobility. The third module consists on the inner processing of the proposed PKI, particularly the certification process and the inter vehicles communications. In order to study the feasibility and the stability of our architecture, we model the inter vehicles connectivity using a set of parameters characterizing of the network such as the transmission range, the inter vehicles distance, the speed, and the number of trusted vehicles.

Certificates management

Cluster configuration: Upon the formation of a cluster the CA_i vehicle should first, generate its pseudo identity PID_i and its pseudo pair of keys short term $(PK^+_{PID_i}, PK^-_{PID_i})$. Next, it generates a certificate associated to the short term pair of keys signed by its long term private key. After, the $CA(PID_i)$ establishes a group key (GK_k) which will be used only by the RA nodes to communicate with CA. In order to secure the communication between CA and RA nodes of the same cluster k, and to hide their identity we use a common pseudonym m_k to which is associated a pair of keys $(K^+_{m_k}, K^-_{m_k})$. However, for security reason each time a RA leaves the cluster, the CA renews the pair of pseudo keys to avoid that it tries to disclose exchanged information after its departure from the cluster. Only nodes belong to two cluster at the same time (called gateway GW) can have two valid pair of keys from both different CAs.

Cross certification:
The cross certification consists in establishing a trust relationship between two CAs which do not share a common root. In fact, a first CA issues a certificate called "cross certificate" to another CA. The CA vehicles generate their own short term certificates and sign them with their long term private keys. However, if a vehicle wants to communicate with another one, it must use its short term pair of keys and the corresponding certificate signed by a CA which is self-certified. Thus, the cross certification takes place each time two vehicles from different clusters will communicate in broadcast and unicast applications.

3.4.3 Summary of results

The proposed architecture performs a set of security services. In fact, the keys and certificates are issued dynamically without storing a large set of keys, also without needing RSUs to request new keys from the central CA. Furthermore, the certificates issued by

CAs are short term in order to avoid tracking vehicles. For purpose of anonymity, vehicles generate short term pairs of key and they request certificates from the CAs in their clusters. We used the RA nodes concept to avoid single point failure (compromising the CA in each cluster), and to authenticate unknown vehicles. Unlike the existing solutions where any vehicle can sign certificates for other vehicles, in our clustering algorithm only trusted vehicles can be elected as cluster head.

We investigate three parameters of the proposed certificates management process. The delay required to join a cluster, the delay during which a vehicle lasts attached to a CA and the average delay of the cross certification. The delay required to join a cluster directly depends on the availability of CA and RA vehicles on the road. Indeed, if there is a sufficient number of CAs to cover the entire network, the time will be reduced to the required time to exchange necessary messages with the correspondent CA to be member of its cluster. The obtained results show that the delay depends on the average number of trusted vehicles in the network which directly affects the average number of RAs. We also notice that the delay decreases when the average number of trusted vehicles increases. We focus on the cross certification, and we remark that the cross certification only lasts some milliseconds which is efficient for VANETs applications and particularly safety applications. We also notice that when the number of trusted vehicles raises, the delay decreases because there are more RA vehicles which are available to route the message to the CA in less time.

3.5 Conclusion of chapter

In this chapter, we addressed the data dissemination, trust model and security issues in VANETs. In our first contribution, we answer the fellowing question: how to improve the data dissemination in terms of redundancy and network congestion? We propose a new protocol based on the classification of data approach called ADCD to targets the receiver nodes [28, 27]. This approach enables to significantly reduce both redundancy and network congestion. ADCD selects the relayed nodes (broadcasters) according to their connectivity degree, while taking into account the data characteristics (location of collection, time validity, importance of data, etc), size of dissemination area, and potential concerned vehicles.

We know that MAC protocol has an important impact on the data dissemination process particularly on the network congestion situation. In our second contribution, we focus on the Control CHannel (CCH) congestion in IEEE 802.11p/1609.4 [61] where safety and non-safety messages coexist. We propose a distributed scheduler called DMS based on the Optimal Stopping Theory [65, 66], which provides an answer to the question: *"When is it better to send a packet?"* [29, 30]. The aim of DMS is to increase a high delivery packet probability with tacking into account the class of the message and the performance metrics. The channel load balancing is transformed into a distributed decision problem, where each vehicle takes the decision to either send immediately or to defer its message transmission. In our third contribution, we answer the following question: how to incite vehicles to well-behave and to contribute in the dissemination process? In this regard, we propose a distributed trust model based on two approaches: signaling games, and fuzzy-based. In the first approach, the trust model is adapted from the job market signaling model, a well-known economic model used in the case where asymmetric information is held between parties called DTM^2 [31, 32]. DTM^2 uses a incentive concept to improve the cooperation level of selfish nodes. We model DTM^2 by using a Markov chain to analysis different model' parameters. The simulation results show that both objectives

(i.e. evicting malicious nodes and encouraging selfish ones to cooperate) are reached. The fuzzy-based approach is used to improve the decision making about the honesty of vehicles [34]. The main obtained results illustrate the impact of the trust metric evolution in the trust model performance. That's why, in [35] we focus on the trust metric stability, and we propose an analytical model based on Markov chain. This model takes into account different parameters related to the robustness, stability and flexibility of the trust model. In order to perform the security services in VANETs, it's important to introduce a distributed architecture able to dynamically manage the keys and certificates. In this regard, we propose a distributed public keys architecture ables to distribute the certification authority role (CA), and to prevent the single point failure [36]. To this end, we introduce the anonymity concept to hide the real identities of nodes who are acting as CA.

These contributions are results of two PhD thesis:

— Nadia Haddadou, University Paris-Est Marne-la-Vallée (UPEM), co-supervised with Y. Ghamri, and G. Roussel ([28, 27, 31, 32, 33, 29, 30])
— Tahani Gazdar, University of Manouba (Tunisia), co-supervised with A. Benslimane, and A. Belghith ([35, 34, 36])

Chapter 4

WSNs

In this chapter, we focus on some contributions related to QoS, including energy efficiency and security for data transportation and routing protocols through the following questions: "*How to find a trade-off between security and QoS in data transportation protocols?*", "*How to improve the transportation protocols through nodes localization?*", and "*How to track communicating and non-communicating target using nodes localization?*. We have provided answers to these questions through some contributions classified into two main topics: i) QoS, energy and security coexistence, and ii) localization and target tracking algorithms.

In the first topic, two main contributions are proposed: our first contribution is an *efficient* model based on PID (Proportional Integral Derivative) controller able to integrate security and QoS metrics in order to dynamically select the adapted security level for the routing protocol [38, 37]. In the second contribution, we propose the Efficient Dynamic Selective Encryption Framework (EDES) to reduce the energy consumption and increase the QoS while ensuring a secure multimedia traffic [39].

In localization and target tracking, we propose a comparative study of RSSI-based localization algorithms (Trilateration, and Multilateration) using spatial diversity in WSNs [40, 41]. We consider different kinds of single / multiple antenna systems: Single Input Single Output (SISO) system, Single Input Multiple Output (SIMO) system, Multiple Input Single Output (MISO) system and Multiple Input Multiple Output (MIMO) system. Secondly, we focus on the localization time (delay of localization), particularly the time bounded localization using Multidimensional Scaling (MDS) technique [42].

Regarding target tracking in WSN, we focus on both communicating and non-communicating mobile targets. In order to optimize the communication between concerned sensors and then to reduce the energy consumption, we use a deployment strategy based on virtual forces (VFA: Virtual Forces Algorithm) associated to a distributed tracking algorithm [79]. In the case of non-communicating targets which is more frequent and complex, we propose an analytical model to decide whether to activate or not the nodes' cameras with different scenarios: heterogeneous and homogenous environments [43, 5, 44]. We focus on target mobility models and we propose a predictive model based on Extended Kalman filter, and a change detection mechanism called CuSum (Cumulative Summuray) to efficiently compute the future target coordinates, and to select which sensors to activate [45, 46].

4.1 Coexistence between security and QoS guarantee

4.1.1 Research context

The advanced technology on the sensing board device enables the use of new applications in WSNs like video surveillance, people and object tracking, etc [80][81]. However, these applications require significant network resources like throughput, delay, and energy. Moreover, these applications require security services like end-to-end data confidentiality between the sensors and the sink, mutual authentication, and data integrity. However, the characteristics of WSNs such as: limited resources (bandwidth, energy, memory and processing), wireless link and mobility make the proposition of an efficient security solution a real challenge.

Many solutions proposed to secure WSNs are based on static security services without taking into account the quality of services (QoS) and the impact on the network performance. We know that the security cost can directly impact the network performance and QoS. For instance, when the size of packets increases because of the addition of security information like numerical packet signature, the data throughput decreases.

Unlike existing works, which focus on security, QoS and energy efficiency separately, we propose two frameworks to optimize security services and QoS parameters: one based on a PID (Proportional Integral Derivative) controller from the feedback control theory [38, 37], the second one is based on a dynamic selective encryption strategy named EDES [39].

4.1.2 PID controller approach

We propose a new framework based on PID controller from the feedback control theory able to integrate security and QoS metrics in order to dynamically select the adapted security level [38, 37]. Moreover, the cross-layer approach is selected to correctly evaluate the different QoS parameters at different layers. The proposed model is introduced in an AODV routing protocol called QwS-AODV in order to evaluate it. The goal of the proposed solution is to improve security in terms of robustness without negatively impacting the QoS and lifetime of sensors.

System model

The PID controller is based on the combination of three control actions: Proportional to the error (P part); proportional to the integral of the error (I part); and proportional to the derivative of the error (D part). These can be used separately or in combination. The proportional term reacts immediately (works on information at the present time) to the error, the integral term remembers and integrates the error history and corrects slowly, and the derivative term predicts the future and makes fast corrections compared to P or I controller. We use the combination of three parts P, I, and D in order to better optimize the system.

We present the QoS parameters at different layers: MAC, routing and application layers. Each layer plays an important role to ensure the end-to-end QoS. That is why the communication between different layers called cross-layer approach is significant to optimally manage the QoS in WSNs.

At the application layer, we can distinguish different types of services like DiffServ architecture [82]: guaranteed service (for application sensitive to delay and jitter like VoIP), load-control service (for applications that need an important throughput like video streaming) and Best effort service (for the applications without any QoS constraints).

The routing layer must take into account the QoS constraints of the application in the routing process particularly in the routing metrics. The selection of the route depends on these parameters: 1) minimum end-to-end delay; 2) minimum end-to-end jitter; 3) maximum end-to-end throughput; 4) optimal energy consumption; 5) load balancing.
At this layer, we can compute a set of metrics such as: number of hops, network traffic state (Queuing/Buffer occupancy), throughput and delay. We introduce the trust level metric as a new parameter for the routing process.

At the MAC layer, a set of important parameters can be obtained such as:
— the average delay to access communication channel,
— the average collision ratio,
— the quality of link based on SINR,
— the energy consumption related to the packets transmission/retransmission, the packets reception and the overhearing.

Description of QoS and Security parameters adaptation

We use the PID controller to select the adapted security services according to the network resources availability and the required QoS parameters for each kind of traffic. The main aim of this controller is to maximize the security level without impacting the QoS parameters. This controller formalizes the variation of QoS parameters and the stability of security levels.

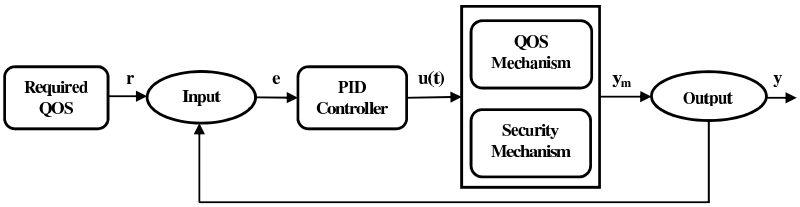


Figure 4.1 – PID controller for QoS and security parameters

Figure 4.1 shows the proposed PID controller which is based on two mechanisms: QoS and security. The QoS mechanism enables to manage QoS parameters and to make a decision about the network traffic. The security mechanism manages the security services and then the security level according to the available resources. Both mechanisms enable to select the appropriate path for each kind of network traffic. That is why we propose a routing protocol called QwS-AODV (QoS with Security AODV). QwS-AODV is based on classical AODV protocol with a difference: the route selection process. This process takes into account the QoS parameters not only to select the route but also to add or remove the security services.

Figure 4.2 illustrates the global flowchart, and it describes the interaction between the different operations and the proposed PID controller. The first step is the network traffic classification into three classes of services: guaranteed services (GS), controlled load (CL), and best effort (BE). It is important to indicate the requirement of each data flow in terms of QoS. This classification can be customized according to different required classes. In the second step, the route discovery process is started, and it is based on two packets: a Route Request packet (REQ) and a Route Reply packet (REP). This process enables to assess the network metrics like Throughput, Delay, Trust level, Energy and SINR. According to this assessment and the selected class of services, the PID controller makes a decision about the appropriate strategy to introduce the security services. For instance, in the case of a low availability of the network resources and high QoS requirements, the PID

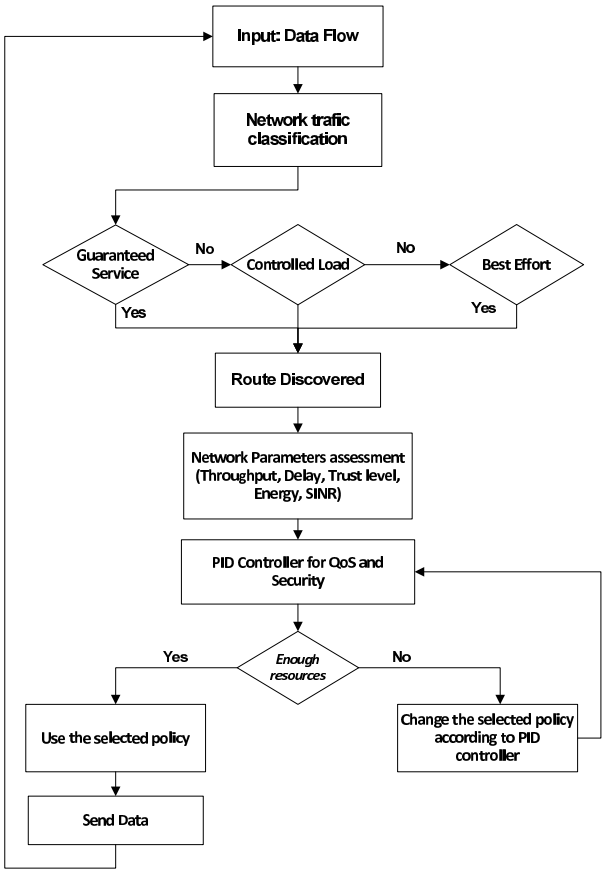


Figure 4.2 – Flowchart of QwS-AODV protocol

controller can request the security mechanism to select the adapted security level by using $u(t)$ parameter. The gap between the required QoS and the QoS assessment parameters is represented by error e. If e is significant, the correction is done by the PID controller, it requests both mechanisms: QoS and security to adapt the services according to $u(t)$.

The path selection

The aim of the path selection process is to select the route with the adapted QoS for each kind of network traffic and application. That is why, a set of path metrics are required in order to describe the state of the path. The required QoS and trust level in the path are picked on by the application and converted into routing metrics. The applications are sensitive to one or more parameters: the throughput, the latency and the jitter.

In the case of audio applications, the latency is very important and the path with the lowest latency is selected. The latency of path k between nodes: source (s) and destination (d) is computed as follows:

$$Lag.P_k^{s,d} = \frac{S(P_k) \times BO.P_k}{TH.P_k} \tag{4.1}$$

where $TH.P$ is the average throughput, $BO.P$ is the Buffer Occupancy and $S(P)$ the Number of Hops.

In the case of video applications, the throughput and traffic load are important parameters and the path with the highest throughput and the lowest overload is selected.

The throughput of path k between nodes: source (s) and destination (d) is computed as follows:

$$TH.P_k^{s,d} = \frac{min(TH(i,j))}{S(P_k) \times BO.P_k} \tag{4.2}$$

where $TH(i,j)$ is the average throughput between two neighbor nodes i and j belonging to path k.

If the application has no particular QoS requirements, then the short path is selected ($min(S(P_j))$).

4.1.3 Selective Encryption approach

We propose the Efficient Dynamic Selective Encryption Framework (EDES) in order to reduce the energy consumption and increase the QoS while ensuring a secure multimedia traffic in WSN. EDES proposes three security levels (high, medium and low) and the selection of each level depends on the energy and QoS parameters. We introduce a new function called capacity to assess the available resources in terms of throughput, delay, link quality and energy. This function is proposed to evaluate the possibility to increase or decrease the security level.

System model

The different types of video frames do not have the same importance. The compression exploits temporal and spatial correlations in an image sequence, so there is a dependency between frames created by the inter-frame coding. Inter-frame coding uses motion estimation and compensation between successive video frames. For instance, in the case of MPEG4 codec frame types P and B need the adjacent frame I and frame P respectively in order to be correctly decoded. In other words, it is not possible to rebuild frames P and B without the data in frames I and P respectively. Therefore, the frame types significance is not the same. That is why, we use in this work the selective encryption process to differentiate between different frames. In this work, we consider two types of video codecs: MPEG4 and H263.

The capacity function enables to evaluate the resources availability at the transmitter camera sensor node and it is based on four parameters: the throughput, the delay, the link quality index (LQI) and the residual energy. The throughput and the delay are the most important parameters for multimedia traffic. We know that this kind of traffic needs an important throughput and minimum delay. The strategy of CAP function is summarized as follows:

— Maximize the residual energy of the camera sensor (RE)
— Maximize the throughput
— Maximize the Link Quality Index (LQI)
— Minimize the delay

The CAP function between two nodes i and j can be expressed according to the chosen QoS metrics:

$$CAP_{i,j} = \sum_k c_k \times f_k(x_{ij}^k) \tag{4.3}$$

where x_{ij}^k is the value of metric k according to the link between two nodes i and j, c_k is the preference weight of metric k with $\sum_k c_k = 1$, and $f_k(:)$ is a normalized function. x_{ij}^k presents the following QoS parameters: Throughput, Delay, Link quality and Residual energy. The choice of weights c_i depends on the application and the type of traffic (the delay is more important than the loss rate for streaming). CAP function introduces four

formalized functions $f_k(:)$. The normalized function is introduced to express different characteristics of different units with a comparable numerical representation. The most commonly used normalized functions are the sigmoidal (S-shaped) functions. Indeed, sigmoidal functions are well-known functions often used to describe QoS perception [83]. We consider the following analytic expression for the sigmoid form:

$$f(x) = \frac{(x - x_m)^\zeta}{1 + (x - x_m)^\zeta} \tag{4.4}$$

where $x_m > 0$ and $\zeta \geq 2$ are tunable parameters, according to which different users' utilities are differentiated.

In WSNs the sensors equipped with camera send data to the sink node (Many-to-one communication). We assume that the multimedia sensor nodes shared secret keys with the sink node and all known nodes shared the secret group key. In this work, we do not focus on the key distribution algorithms.

EDES description

The Efficient Dynamic Selective Encryption framework (EDES) is based on two main steps. The first step consists in assessing the network performance parameters. We introduce the new capacity function called CAP. This function combines between QoS parameters and residual energy. The second step consists in selecting a security level and using or not the selective encryption algorithm. The security level is selected according to the CAP function. EDES defines three security levels: low, medium and high. The low security level enables the receiver nodes to control data integrity and sender authentication by using the Hashed-based Message Authentication Code (HMAC) [84]. However, this level does not ensure data confidentiality. The medium level has the same security services as the low level and ensures data confidentiality by using Standard (AES) algorithm. If the network traffic requires confidentiality, EDES chooses either the medium or the high security level according to the network status. The difference between the high and medium security levels is the percentage of encryption which is higher than $\%Th_{high}$ in the case of a high security level. In addition, EDES differentiates between frame types in order to select the important frame called key-frame (ie. frame I in the case of MPEG-4 codec). The percentage of encryption in the case of I frame (Enc_I) is not the same for other frames.

In order to switch between three security levels, we define three CAP threshold values. The high security level needs a sufficient network performance and residual energy. The medium security level is an intermediate level which enables to ensure the confidentiality with an acceptable resource consumption. Without enough resource availability a minimum security is ensured by the low level. The following equation defines the switching between different security levels:

$$\begin{cases} if(CAP \geq \%Th_{high}) & Enc_I = \%Th_{high} \\ if(\%Th_{min} \leq CAP \leq \%Th_{high}) & Enc_I = 50\% \\ if(CAP \leq \%Th_{min}) & Enc_I = 0\% \end{cases}$$

where Th_{high} and Th_{min} can be tuned according to wireless nodes technologies and the desirable security.

4.1.4 Summary of results

In our first contribution, the Quality-of-Services and the energy consumption parameters are combined with the security levels to find the optimal solution for the

routing process using PID controller. This solution is introduced in a classical AODV protocol called QwS-AODV protocol. QwS-AODV protocol proposes three security levels (high, medium and low) with the ability to ensure authentication, data integrity and confidentiality. The selection of each level depends on the decision of the PID controller. The simulation results illustrate that QwS-AODV protocol ensures security without negatively impacting the network performance. In addition, QwS-AODV protocol increases the lifetime duration of nodes by around 50% compared to the static security services implemented in routing protocol AODV.

In the second contribution, we proposed a solution called Efficient Dynamic Selective Encryption Framework (EDES) in order to ensure dynamic security levels while taking into account network performance and energy consumption. The capacity function is proposed to evaluate the possibility to increase or decrease the security level. The assessment of this function is based on the cross-layer approach to take into account the different parameters at physical, MAC and upper layers. The obtained simulation results show that security is ensured even with a low security level. In addition, EDES increases the lifetime duration of nodes by around 40% compared to the classical encryption algorithm.

4.2 Localization algorithms

4.2.1 Research context

The position information of sensor nodes plays a key role in many applications of Wireless Sensor Networks (WSN). Sensor nodes need to their respective positions in order to track the objects [5] and to route the packets by using the geometrical routing [18]. This position can be defined as absolute location, which combines altitude, longitude and latitude, or relative location, which depends on the positions of the other nodes. We focus on nodes and network localization. First, we propose a comparative study of RSSI-based localization algorithms (Trilateration, and Multilateration) using spatial diversity in WSNs [40, 41]. We study the accuracy of this kind of algorithms in the case of an in-door localization. We consider different kinds of single / multiple antenna systems: Single Input Single Output (SISO) system, Single Input Multiple Output (SIMO) system, Multiple Input Single Output (MISO) system and Multiple Input Multiple Output (MIMO) system. Secondly, we focus on the localization time, particularly the time bounded localization, and the localizability of WSN. We proposed a distributed time-bound localization algorithm based on Multidimensional Scaling (MDS) called D-MDS to ensure relative and physical localization time [42]. The main objective of D-MDS is to maximize the number of localized nodes in a given time bound and to minimize the number of anchors required to physically localize the network.

4.2.2 Spatial diversity approach

We consider RSSI since it is advantageous in terms of cost and energy consumption despite the large variations of its measurements caused by multipath fading as well as shadowing in indoor environments. Various enhancement schemes have been proposed in order to improve the accuracy of nodes with unknown position. We exploit the concept of spatial diversity and investigate its impact on localization accuracy in an indoor environment. The diversity techniques are a common approach that helps mitigating the degrading effects of fading. Different types of diversity are usually used in wireless communication such as time diversity, frequency diversity and spatial diversity. Spatial diversity is the most attractive since additional resources in the wireless link are not

required. The concept behind spatial diversity is relatively simple: the receiver is provided multiple copies of the transmitted signal via different paths so that they will undergo independent fading.

In RSSI-based localization approach, the distance between the target and each reference node (anchor) is estimated by using the received signal power (RSS). In [85], the authors have proved that the accuracy of the RSS ranging is improved and an accurate localization is achieved when reducing the Bit Error Rate (BER). We use spatial diversity that has a direct impact on the BER.
Due to fading, the reliability of the information extracted from the received signal, manifested through the error probability, is poor. The Bit Error Rate (BER) can be defined in terms of probability of error (P_e). In the localization process, we used this information to determine the quality of signal at the receiver nodes. Moreover, different diversity combining techniques are used at the receiver. The common linear combining methods are: Selection Combining (SC), Equal Gain Combining (EGC) and Maximal Ratio Combining (MRC) [86]. The receiver in SC technique selects the best signal from the different antennas. In EGC, all the received signals are co-phased at the receiver and added together, whereas in MRC, the signals from each channel are weighed and added together.

System model

A comparative study of the performance in terms of localization error metric of well-known localization algorithms namely trilateration and multilateration under different system models is conducted. We also show the impact of different diversity combining techniques used at the receiver on position accuracy namely SC, EGC and MRC. The localization process is divided into two phases: 1) range measurements between the unknown node and the reference nodes (anchors) are assessed. 2) Location estimation phase using trilateration and/or multirateration algorithms. Figure **??** shows an example of trilateration based algorithm with MIMO system, where multiple antennas can be used on both anchor and target nodes.

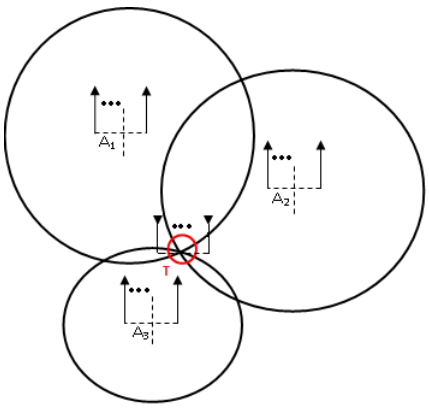


Figure 4.3 – Trilateration algorithm using MIMO model

4.2.3 Time-bounded approach

In order to study the localizability of a network at a given time bound, we propose a new distributed and time bounded localization algorithm based on Multidimensional

Scaling (MDS) called D-MDS [42]. The distributed MDS method is more appropriate to support the scalability of localization systems. In this method, nodes compute their own positions and the positions of their neighbors by using their local information in a Local Coordinate System (LCS). LCS is a relative coordinate system to the node. Each node calculates its position and the positions of its one hop neighbors. Thereafter the local coordinate systems are merged to form a Global Coordinate System (GCS) by using the linear transformation [87]. The linear transformation is to translate the coordinates of nodes from one coordinate system to another. This rotation between two coordinate systems is ensured by using at least *three common and non collinear* nodes in $2-D$ space.

System model

Some important definitions are given below:

— *Round of communications*: it represents the granularity of time to assess the network localization time. One round of communications refers to the time required by the localized sensors to transmit their positions and to receive the positions of localized neighbors.

— *LCS Island (LCSI)*: is a set of mutually convertible local coordinate systems. Any two LCSs from different islands are not convertible to each other when the WSN has a disconnected graph topology [88].

— *Time Localization*: is the number of communication rounds required to merge all the LCS of each island in a single LCS.

— *Time Essential Localization*: is the number of communication rounds expected to translate each LCS to any LCS island [88].

— *The relative localizability of a network at a given time bound*: a WSN is relatively localizable in k rounds of communications if and only if all sensor nodes are localized in their local coordinate systems and all local coordinate systems converge to only one LCSI in k communication rounds.

— *The physical localizability of a network at a given time bound*: the necessary and sufficient condition for the physical localizability of a network with n anchors in k rounds of communications consists in completing the localization process within k rounds of communications and finding a location configuration of n anchors to convert the relative positions of nodes to absolute ones. In fact, for any isolated island, it requires at least three anchors for 2D localization (four anchors for 3D localization) in order to convert the relative coordinates of sensors to the absolute ones.

Algorithm Process

Figure 4.4 illustrates the flowchart of the proposed distributed time-bound localization algorithm called D-MDS. The first step of D-MDS consists in defining the local position of each node and its neighbors. After computing the distance matrix, each node calculates its local position and the positions of one-hop neighbors using the MDS method. The nodes initialize the following data structures:

— *A position table*, it contains the positions of the node and its neighbors in their local coordinate system.

— *An identification table*, it stores the identification of sensors that belong to the LCS.

— *A transformation table*, it specifies the transformation between each LCS in the identification table and a Base LCS (BLCS). The BLCS is an LCS that contains the maximum number of localized nodes.

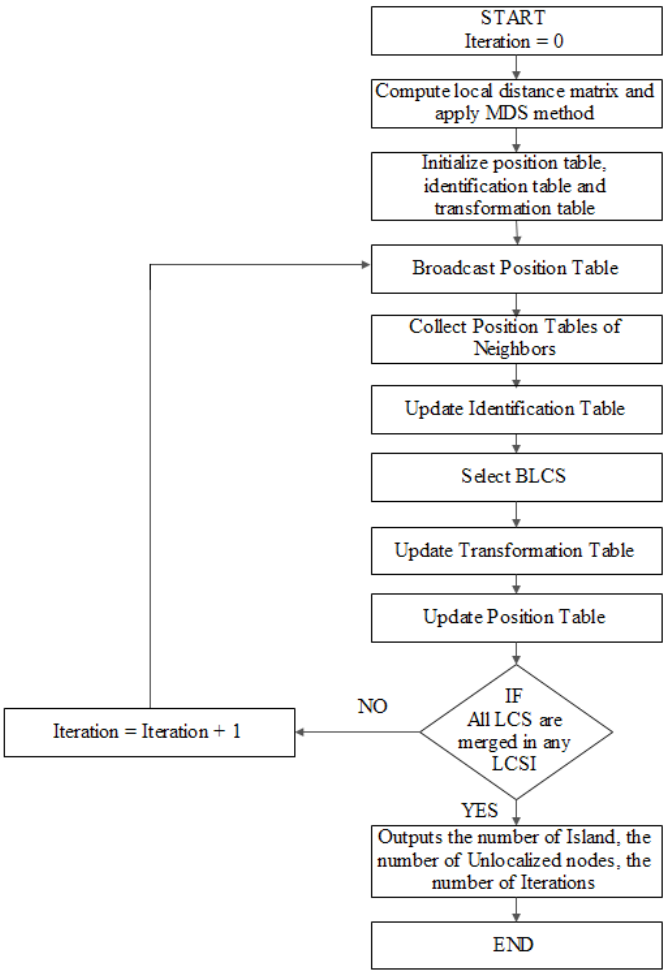


Figure 4.4 – Mode of operation of D-MDS Localization Time Algorithm.

The Base LCS (BLCS) is selected as follows: After collecting the position tables of all neighbors at each communication round and based on the number of localized nodes in each LCS, each sensor chooses its BLCS that is the LCS which localizes the maximum number of nodes.
The second step consists in merging each LCS to any isolated LCS island. After collecting the position tables, each node updates its identification table and selects its BLCS. Once the BLCS is selected, two steps are performed to update the transformation table: 1) a sensor checks its position table to find all the LCSs that can be transformed to the BLCS; 2) the sensor converts all LCSs identified in the first step into the selected BLCS. Finally, the sensor node updates its position table. Based on the results of D-MDS algorithm, we can study the localizability of a network at a given time limit. On the one side, if $iteration \leq k$ where k is the limit of localization time defined by user and $the\ number\ of\ LCS\ Island = 1$ and $the\ number\ of\ unlocalized\ nodes = 0$, the sensor network is k-round relatively localizable. On the other side, the physical localizability of the network can be studied in terms of number of anchors required to physically localize the network. In fact, a sensor is $k - round$ physically localizable if $iteration \leq k$ and the number of anchors required is defined as follows:

$$number\ of\ anchors = 3 \times number\ of\ Islands + \ number\ of\ unlocalized\ nodes \quad (4.5)$$

4.2.4 Summary of results

The obtained results from our study related to the accuracy of the localization algorithm (mainly trilateration, and multilateration) with spatial diversity (SISO, MISO, SIMO, and MIMO) show that MIMO system with multilateration gets better results compared to other combinations. The average localization error of the multilateration and trilateration algorithms respectively is evaluated against the shadowing standard deviation when using different system models with different target positions. In addition, to simulate different indoor environments, the standard deviation of the shadow fading was changed from 1dB to 6dB. The higher the shadowing standard deviation, the worse the performance of both localization algorithms in terms of average localization errors. The good performance of MIMO over SIMO, and MISO systems is attributed to the higher number of signal copies at the receiver having undergone different fading. The SISO system presents the worst performance. We evaluate the impact of the number of antennas at the receiver nodes, the obtained results show an improvement in the performance of about 30% is achieved when using four antennas compared to the case where two antennas are used. Thus, the performance accuracy is considerably improved while the number of antennas is increased. However, this benefit comes at the expense of system complexity. We compared the average localization errors using multilateration algorithm considering three different methods for combining RSSI values at the receiver: Selection Combining (SC), Equal Gain Combining (EGC) and Maximal Ratio Combining (MRC). The results show that the accuracy is the highest for MRC technique and the lowest for SC technique, with EGC performance closer to MRC one. Although it is known that the maximal ratio combining is the optimal linear combining technique, the receiver is more complex since it is dependent on the number of paths available at the receiver.

ute to the localizability of the WSN at a given time bound by proposing D-MDS localization time algorithm. First, we studied the complexity of the proposed solution, and we note that the time complexity of computing all the local coordinate systems is polynomial to the number of nodes in the network. The local coordinate systems (LCS) are merged together to form the LCS islands (LCSI). The transformation of all LCSs into the LCSIs takes at most $O(nL^2)$ time, where n is the number of nodes and L is the number of possible LCS in the network. The network that is k-hop and $d+1$-edge-connected graph is relatively localizable in the k rounds of communications for the d-dimensional space. The total time complexity of physical localizing the network is $T = O(n\beta^3) \times O(nL^2) \times O(a^3+n)$ where a is the number of anchors and n is the number of nodes in the network. In addition, the obtained simulation results show that the number of unlocalized nodes in D-MDS algorithm is less than five nodes for the average node degree 3, while the number of unlocalized nodes of the Trilateration based algorithm is more than 25 nodes for the same average node degree. The reason of this large gap of the unlocalized nodes number between the two algorithms is that the nodes which have a degree equal to one or two are localized by the proposed algorithm; however these nodes are not localized by the Trilateration based algorithm because the localized node requires the co We contribnnection to at least three localized nodes. We analyzed the variation of the number of anchors required for physically localize the network. The obtained simulation results show that the number of anchors is proportional to the number of islands, and the proposed algorithm reduces the number of anchors to physically localize the network by comparing to Trilateration one.

4.3 Target tracking algorithms

The work presented in this section is related to PhD. thesis of Ibtissam Boulanouar, University Paris-Est Marne-la-Vallée (UPEM), 2010-2014. Co-supervised with Stéphane Lohier and Gilles Roussel. Publications [43, 45, 5, 46, 79, 44]

4.3.1 Research context

The Target tracking process is divided into two stages: detection and localization of the target through its evolution inside an area of interest. This application can be used in different fields varied from security to ambient assistant living domains. Unlike classical monitoring systems, WSN offers more flexibility and easier set up. Moreover, due to their versatility and autonomy they can be used in hostile areas, and unreachable for human. However, WSNs have some limitations: wireless links are not reliable, data processing and transmission are greedy processes in term of energy. In order to overcome the energy constraint, only the sensors located in target pathway should be activated.

The existing target tracking solutions in WSNs can be classified in three classes: cluster-based, structure-less and predictive-based. The two first classes are related to network architecture while the last one is related to tracking relaying strategy.
In structure-less approach, no network organization is set up. All the nodes have the same level with no hierarchy between them. The tracking is performed in reactively manner at each stage of target evolution inside the region of interest.
In cluster-based class, the network is organized in clusters of nodes. A cluster is composed of a cluster head and cluster members. In this kind of solution, when a node detects the target, it reports its location to the cluster head (CH) which is responsible to manage the tracking process.
In predictive-based class, models or mechanisms are used to proactively estimate and predict the target movement. This approach can be established on cluster-based or structure-less classes.

We present our contributions related to mobile object tracking in WSN. The idea is to answer this question: how to select sensor nodes to obtain the trade-off between the tracking precision and the energy consumption? We distinguish two kinds of mobile targets: communicating and non-communicating one. In the case of communicating targets, we use a deployment strategy based on virtual forces (VFA: Virtual Forces Algorithm) associated to a distributed tracking algorithm implemented in cluster-based network architecture [43]. In the case of non-communicating target, we need to introduce some multimedia sensor nodes (nodes equipped with camera) in order to detect the target movement. However, camera sensor nodes are energy greedy, and their running must be optimized. The heterogeneous wireless sensor networks are considered where movement detection sensor (MS), and camera sensors (CS) coexist and cooperate to detect and to track the target [5]. When the CS nodes receive notification from MS, they make decision whether to activate or not their cameras based on probabilistic model [44]. In order to enhance the tracking algorithm in terms of accuracy and CS activation process, a prediction approach based on target mobility models is proposed [46, 45]. We use the Extended Kalamn filter as prediction model combined with a change detection mechanism named CuSum (Cumulative Summuray). This mechanism allows to efficiently compute the future target coordinates, and to select which sensors to activate.

4.3.2 Case of communicating target

In this part, we assume that the target node is equipped with communication module, and it's able to communicate with others nodes. We propose a distributed and collaborative target tracking algorithm running with cluster based architecture called CTC (Cluster-based Tracking algorithm for Communicating target). This architecture is suitable in WSN in terms of efficiency in collaboration, data processing and transmission. The deployed network consists in powerful nodes playing the role of cluster heads and Camera Sensors as cluster members. Insofar as the mobility of the sensors is not required for the targeted applications, a static association algorithm is proposed to built the clusters. In the proposed tracking algorithm both intra and inter-cluster collaboration are possible. The tracking algorithm starts when a Camera Sensor receives a periodic beacon from the mobile target. The information collected on this target is then sent to the Cluster Head (CH), which selects a set of three close sensors in order to run the localization process with a Trilateration method. The selection of these sensors is achieved using a probabilistic method. In addition to the clustering and the tracking algorithms, a deployment strategy for both cluster heads and members is proposed. It improves the tracking performances and ensure network connectivity.

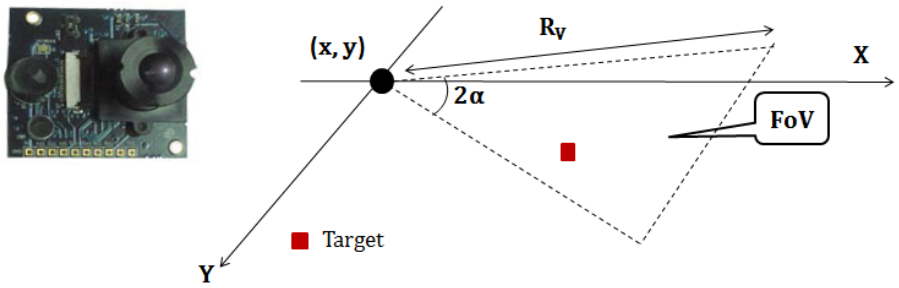


Figure 4.5 – Camera Sensor's Field of View

The wireless sensor node equipped with camera called Camera Sensors (CS). Each CS has a sector and directional Field of View (FoV) with opening angle 2α, video sensing radius R_V and transmission range R_T . Figure 4.5 illustrates CS and and its FoV. In order to minimize the CSs activity, the CHs are in charge of data collection, aggregation and routing. All CSs transmit their collected informations to the CH which processes and forwards them to the sink through multi-hop communication. To optimize the performances of the cluster-based architecture, a deployment strategy is necessary for both multimedia sensors and CHs.

Deployment strategy

The deployment strategy aims to maximize network video coverage as well as network connectivity. To achieve these tasks, we propose an enhanced version of the Virtual Force Algorithm (VFA) [89]. VFA uses repulsive and attractive forces to determine the new location of sensors.

We introduce the critical sub-areas concept where some areas are more important to monitor than others. The critical sub-areas are weighted according to their importance. The weight attributed to each critical sub-area is considered in the deployment process.

Considering this environment, $\vec{F_i}$ is calculated as below:

$$\vec{F_i} = \sum_{\substack{j=1 \\ j \neq i}}^{N} \vec{F_{ij}} + \vec{F_{obs}} + W_{gt}\vec{F_{csa}} \tag{4.6}$$

where $\vec{F_{ij}}$ represents the force applied between CS_i and CS_j. $\vec{F_{obs}}$ is the total repulsive forces applied on CS_i by the surrounding obstacles. Finally, $\vec{F_{csa}}$ is the total attractive or repulsive forces assigned on CS_i by the critical sub-areas. W_{gt} is the weight assign to each one.

We specify then how to calculate $\vec{F_{ij}}$:

$$\vec{F_{ij}} = \begin{cases} (W_A(d_{ij} - d_{th}, \alpha_{ij})), & \text{if} \quad d_{ij} > d_{th} \\ 0, & \text{if} \quad d_{ij} = d_{th} \\ (W_R \frac{1}{d_{ij}}, \alpha_{ij} + \pi) & \text{if} \quad Otherwise \end{cases} \tag{4.7}$$

W_A and W_R are respectively the measure of attractive and repulsive forces. α_{ij} represents the direction of $\vec{F_i}$. d_{ij} is the Euclidean distance between the gravity centers of CS_i and CS_j while d_{th} is the threshold distance which controls how close CSs get to each other. Its value is determined based on the sensing range R_V.

We used W-VFA (Weighted VFA) to deploy the CHs. While the main target behind deploying CSs is to optimize the tracking, the main objective in CHs deployment is to ensure network connectivity. The CHs have omni-directional transmission range. Thus, $\vec{F_i}$ is applied on the gravity center of the circular transmission range. Using the resulting deployment informations, each CH is aware of its final position and each CS is aware of its final position and camera orientation.

Tracking algorithm

The tracking process is divided in four steps: detection, sensor selection, localization and target view

Detection: The CS are in hibernation mode (or deep sleep) when its sensing channel is inactive, and it switches to activate mode and starts the tracking algorithm when it receives a *Beacon* from the target node. The distance d_i between CS and the target is assessed based on the Received-Signal-Strength (RSS) techniques [90]. Then, it informs its CH by sending a *Target-detected* message.

Sensor selection: In order to localize the target, the CH uses the information received from the CS (via *Target-detected* message), and a probabilistic model to select two nodes in its cluster. The Trilateration algorithm is used. The CH computes for each CS the capability C_i of the tracking operation using the following equation.

$$C_i = \beta P_i + (1 - \beta) T_i \tag{4.8}$$

where P_i and T_i represent respectively the remaining power and the tracking accuracy of the i^{th} CS. β is the balancing parameter. The value of $T_i \in [0, 1]$, and it is obtained as detailed below:

$$T_i = 1 - (D_i / R_T) \tag{4.9}$$

D_i is the distance between the i^{th} CS and the target. R_T is the transmission range and thus, the maximal distance beyond which the CS cannot detect or localize the target. If D_i is higher or equal to R_T, the i^{th} CS cannot localize the target.

Finally, the probability Pr that a node would be selected to perform target localization is obtained as shown in equation 4.10:

$$Pr_i = 1 - (N_i/N_c) \tag{4.10}$$

where N_c denotes the number of cluster members within the cluster. N_i is the number of cluster members within the same cluster having a higher capability C_i than the i^{th} CS.

The cluster members with the highest probability are selected by the CH to participate to the localization process. Once the CH selects the best CSs to support it in target localization process, it informs them by sending a *Localization* request. Each of the selected one measures the distance d_i (if it is not already available) between itself and the target by requesting a *beacon* from it. Then, it replies to the CH with *Target-located* message which contains this distance.

Localization: The CH uses a trilateration algorithm for target localization [91].

Target view: When the target is localized, CH selects the best oriented Camera to activate using Target in Sector test [92]. This test aims to check if the target is really in CS's field of view. This Camera belongs to one of the three selected CSs involved in the localization process. Each CH is aware of the orientation of its cluster members via the *Joint-confirmation* message exchanged with the CSs during the clustering phase. The CH informs this selected CS by sending a *Camera-activation* request.

4.3.3 Case of non-communicating target

In literature, many works focus on the communicating mobile target tracking, but few of them are dealing with non-communicating mobile target. In order to track non-communicating target in WSN, we propose two main contributions: one based on probabilistic approach where network is formed by two kinds of sensors nodes: Motion Sensors (MS), and Camera Sensors (CSs); Second, based on predictive approach where we focus on the target mobility to anticipate its detection.

Probabilistic approach

In this contribution called DTA (Deployment and Tracking Algorithm), we introduce two kinds of sensors nodes: Motion Sensors (MS), and Camera Sensors (CSs) where nodes are equipped with infrared detectors, and CMOS cameras respectively. Accordingly, MS has a circular Field of Detection (FoD) with radius R_D (Figure 4.6.A). CS has a directional Field of View (FoV) defined by a cone with radius R_V and angle (Figure 4.6.B).

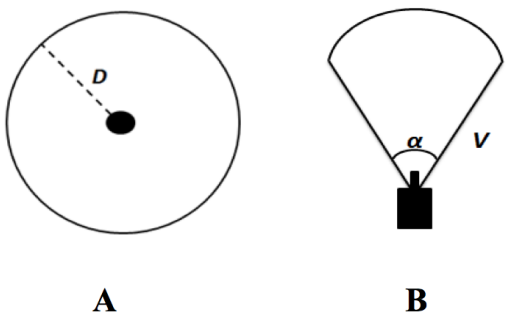


Figure 4.6 – Field of Detection (FoD) vs. Field of View (FoV).

We introduce the concept of the approximate coordinates of the target (X_t, Y_t). They represent the target coordinates calculated by the MSs when no CS is available. We calculate them as follow:

$$\begin{cases} X_t = P_{MS}\left(\frac{\sum_{i=1}^{N} X_m)}{N}\right) \\ Y_t = P_{MS}\left(\frac{\sum_{i=1}^{N} Y_m)}{N}\right) \end{cases} \tag{4.11}$$

Where P_{MS} is the probability that the mobile target is detected by MS, and (X_m, Y_m) are the coordinates of MS. N is the total number of MSs that detect the target at the same time in a given area. The value of P_{MS} is closely related to the distance $d((X,Y),(X_mY_m))$ between the target and the sensor. Where (X, Y) represent the real target coordinates. We can express P_{MS} as follow:

$$P_{MS} = \begin{cases} 1, & if \quad d((x,y),(i,j)) \leq R_D \\ e^{\beta d((x,y),(i,j))}, & if \quad d((x,y),(i,j)) > R_D \end{cases} \tag{4.12}$$

where β defines the physical characteristics of the MS. P_{MS} decreases exponentially while $d((x,y),(i,j))$ increases.

The probability at the mobile target is detected by CS is given by P_{CS}. This probability depends on three parameters: 1) the number of MSs in CS's transmission range that detects the target; 2) the distance between CS and these MSs and 3) the orientation of CS. It is obtained as follows:

$$P_{CS} = 1 - \prod_{j=1}^{N}(1 - P_{CS_i}) \tag{4.13}$$

Hence, we can express the probability P_{CSi} that the mobile target is detected by CS depending only on one MS by the following equation:

$$P_{CSi} = \frac{A_{int}}{FoD} \tag{4.14}$$

A_{int} is the intersection area between FoD and FoV. It is calculated on the basis of the distance between CS and MS: the value of A_{int} decreases with the distance. Figure 4.7 illustres an example of target tracking with different nodes of the network.

We distinguish two main phases: deployment, and target tracking. In deployment strategy, we use the same concepts as the case of communicating target which means the critical sub-area, and the Virtual Force Algorithm (VFA). We divide the Area of Interest (AoI) in cells grid and place the MSs at the center of each cell. Finally, each CS calculates its most beneficial orientation using local information such as neighbors and critical sub-areas.

In target tracking phase, we propose an energy-aware and collaborative tracking algorithm. The MSs that handle the detection consume less energy than CSs, which allows keeping them actives in order to monitor the AoI. CSs are in charge of visual localization. When a MS detects a mobile object, it activates only the CS that can localize it. The performance of the tracking algorithm is closely related to the deployment strategy. Indeed, an efficient deployment strategy ensures a maximal coverage of the area of interest that increases the tracking algorithm performances.

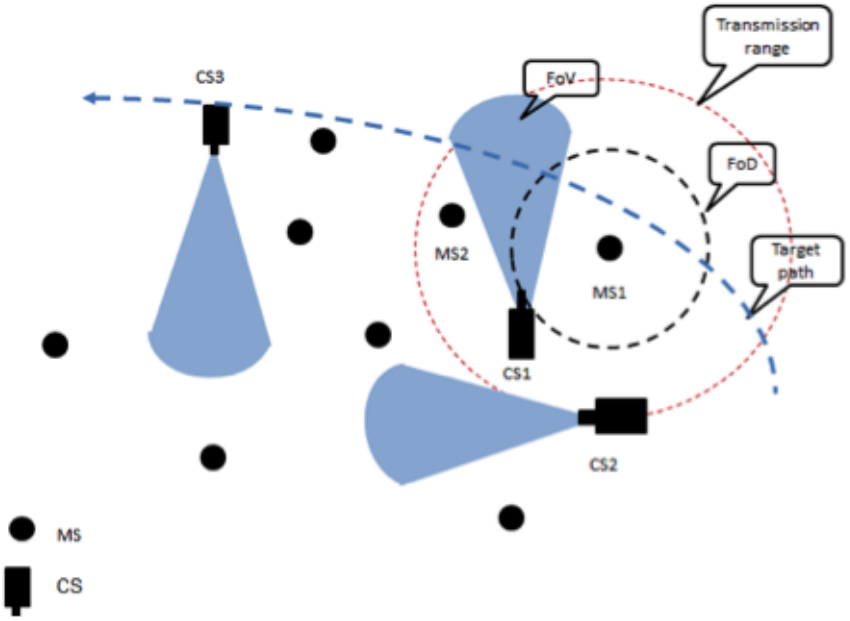


Figure 4.7 – An illustrative example

Prediction approach

In order to improve the tracking process by ensuring the trade-off between the accuracy of the tracking and the energy conservation, we propose a new Predictive-based Target Tracking called PMT^2 [45]. Prediction approach seems to be the best candidate to reach this objective. For this purpose, we introduce an enhanced Extended Kalman Filter combined with a change detection mechanism named CuSum for Cumulative Summary [93]. We show the efficiency of the proposed coupled mechanism in the trajectory prediction and in the reactivity to abrupt direction changes. Figures 4.8 summarizes the proposed algorithm PMT^2 and its five main steps.

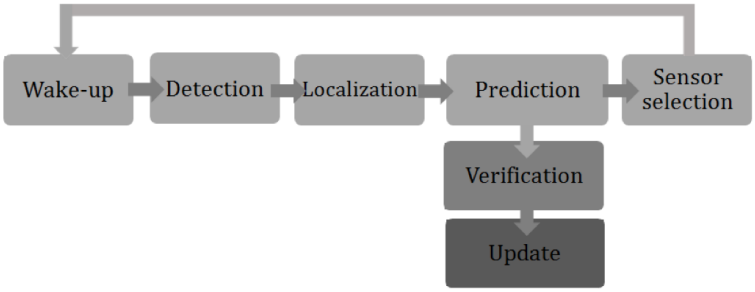


Figure 4.8 – PMT^2 process

Wake up: Initially all CS nodes are in sleeping mode (sensing channel in hibernation), and periodically, a sub-set of CSs is chosen to be activated. We consider CS's location and orientation in selection process. When a selected sub-set returns in sleeping mode; another relevant one wakes up.

Detection: When a CS is in active mode, it captures images of the region of interest. Afterward, using the background subtraction method [94], it checks if the target is in its

FoV. If the target is detected, the next phase starts. Otherwise, the CS returns to the sleeping mode.

Localization: We use an image processing solution [95]. When a CS detects the target, it captures images, and uses them to perform localization. For that purpose, it computes the size of the target on the captured frame by using CS features such as dimensions and focal length. Then, based on its own location it calculates the distance between the target and itself and thus, target location.

Prediction: This is the most important step. Target movement is anticipated, and tracking process is relayed from node to node. The current activated CS uses the proposed enhanced Extended Kalman Filter (EKF) for non-linear models coupled with a change detection mechanism named CuSum. We focus on the mobility model of the target node, and we propose the following model:

$$X_{t+1} = f_t(X_t) + w_t \tag{4.15}$$

$$Z_t = h_t(X_t) + v_t \tag{4.16}$$

Where X_{t+1} is the mobility state vector at time $t+1$:

$$X_{t+1} = [x_{t+1}, v_{x_{t+1}}, a_{x_{t+1}}, y_{t+1}, v_{y_{t+1}}, a_{y_{t+1}}]'$$

x_{t+1} and y_{t+1} are target's 2D coordinates at time $t+1$. $v_{x_{t+1}}$ and $v_{y_{t+1}}$ specify its velocity while $a_{x_{t+1}}$ and $a_{y_{t+1}}$ denote its acceleration. Z_t is the measurement update vector:

$$Z_t = [x_{z_t}, y_{z_t}]'$$

Where x_{z_t} and y_{z_t} specify the measured target coordinates.

$f_t(.)$ is a nonlinear representation and $h_t(.)$ is a nonlinear observation function. w_t and v_t are white Gaussian noise with zero mean and respectively Q_{w_t} and Q_{v_t} variance. We assume that they are independent of each other. EKF [96] is divided in two main steps: prediction and update steps.

— **Prediction step:** The estimated mobility state vector at time $t+1$ ($\widehat{X}_{t+1|t}$) is computed using equation 4.17. The covariance matrix $P_{t+1|t}$ associated to $\widehat{X}_{t+1|t}$ is evaluated from the previous estimated $P_{t|t}$ and process noise covariance matrix Q_{wt} using equation 4.18.

$$\widehat{X}_{t+1|t} = f_t \widehat{X}_{t|t} \tag{4.17}$$

$$P_{t+1|t} = F_t P_{t|t} F_t' + Q_{wt} \tag{4.18}$$

Where F_t is the Jacobian matrix of the state transition function f_t. We obtain it as described below:

$$F_t = \frac{\partial f}{\partial X}|_{\widehat{X}_{t|t}}$$

— **Verification step:** The main objective of this step is to check if the predicted coordinates, belong to the topological graph constructed using Voronoi Diagram. The Voronoi Diagram is used to determine the pathways between the obstacles.

— **Update step:** This step aims to correct the predicted coordinates. While in the verification step, the coordinates are corrected following the mobility graph. In this step, the coordinates are corrected based on the measurement of real target location.

In order to detect the target direction change, we use Cumulative Summary (CuSum) test as follow:

$$g_{t+1} = g_t + S_{t+1} - v \tag{4.19}$$

As initial condition $g_{t+1} = 0$. S_{t+1} is the normalized innovation process of the EKF. In our work, we define it as described below:

$$S_{t+1} = \frac{Z_{t+1} - H_{t+1}\widehat{X}_{t+1|t}}{\sqrt{(P_{t+1|t} + Q_{wt})H_t^2 + Q_{vt}}} \tag{4.20}$$

Where H_t is the Jacobian matrix of observation function h_t.

There are two important parameters in CuSum test, the drift parameter v and the alarm threshold h. The value of v is subtracted at each iteration to prevent positive drifts, that may yield a false alarm. h is called alarm threshold because a direction change is detected when $g_{t+1} > h$. This condition is considered as the stopping rule of the CuSum test. After an alarm, the value of g_{t+1} is reset to zero. The smaller the values of v and h, the more sensitive the test is. Their values is chosen according to the application context.

Next sensor selection: Once the future target location is predicted; the next sensor selection phase starts based on two criteria: location and orientation angle. In this phase, the objective is to relay the tracking from node to node until the target leaves the area. The CS node must satisfy Target in Sector (TIS) test [92]:

$$\begin{cases} d_{iT} \leq R_v \\ \beta \in [-\alpha, \alpha] \end{cases} \tag{4.21}$$

Where d_{iT} denotes the distance between the node i and the target T. β is the angle between $i\vec{T}$ and $\vec{v}$. $\vec{v}$ is a sensing vector which divide the FoV into half. 2α represents the opening angle of the CS. The sensor with the smallest value of d_{iT}, which means is closest to the target, is selected to be the succeeding one.

4.3.4 Summary of results

In the performance evaluation of our proposed target tracking algorithms, we focus on three metrics: the tracking accuracy, the energy consumption, and the overhead (the number of added exchanged messages).

In the case of contribution for communicating target tracking called CTC, the obtained simulation results show that CTC increases the tracking accuracy by up to 40% compared to the solutions where the Camera Sensors are scattered randomly in the area of interest. We conclude that the used deployment strategy based on W-VFA has a positive impact on tracking performances. This impact is more important than the number of active CSs. In terms of energy consumption, we focus on the energy cost of camera activation, active period duration, localization and communication cost during the tracking process. The simulation results illustrate that CTC has better results compared to classical solutions without any deployment strategy. Regarding the generated overhead, the results show that CTC is less efficient than a classical solution where the cooperation between nodes is limited. However, even if the amount of exchanged messages for CTC algorithm is higher than the compared solutions, it always consumes less energy.

In the case of our contributions for non-communicating target tracking algorithms, the probabilistic approach with DTA solution approves the added value of the deployment strategy in terms of tracking accuracy. In addition, the impact of the number of CS and MS nodes on the tracking accuracy are clearly illustrated where DTA improves this

metric even the number of CS is less important. This allows to significantly reduce the energy consumption. For the same purpose particularly the introduced overhead by DTA is evaluated as reasonable thanks to the probabilistic model which enhance the detection probability and it reduces the false positive rate. We can conclude that DTA with the deployment strategy is the solution which presents the best trade-off between tracking accuracy and energy consumption. It performs tracking with better precision, less energy and a smaller number of exchanged messages than others solutions.
In the case of predictive approach, the obtained simulation results of our proposed solution called PTM^2 show that this solution outperforms others existing solutions with different parameters: the size of the area of interest, target speed, the maximal number of deployed nodes and their sensing range. The Enhanced Extended Kalman Filter coupled with CuSum mechanism allows to predict realistic target behavior, with possible sudden direction changes, and the target accuracy reaches 90% for certain simulation parameters. PTM^2 performs target tracking accuracy with the best results, up to 35% more than existing works. Moreover, it saves up to 55% more energy compared to other works. In terms of overhead, PTM^2 reduces the number of nodes participating in the tracking process, and thus saving resources, thanks to the prediction information.

4.4 Conclusion of chapter

In this chapter, we addressed the coexistence between Quality-of-Services (QoS) and security, localization algorithms, and target tracking issues in WSNs. In our first contribution, we answer the following question: how to ensure the coexistence between opposite parameters related to QoS and security requirements? We propose two frameworks based on different approaches: PID (Proportional Integral Derivative) controller, and dynamic selective encryption mechanism. In the first approach the QoS and the energy consumption parameters are combined with the security levels to find the optimal solution for the routing process. This solution is introduced in a classical AODV protocol called QwS-AODV protocol where three security levels (high, medium and low) are proposed with the ability to ensure authentication, data integrity and confidentiality. The selection of each level depends on the decision of the PID controller. In the second approach, we used a Dynamic Selective Encryption Framework (EDES) in order to ensure dynamic security levels while taking into account the network performance and the energy consumption. EDES uses the capacity function to evaluate the possibility to increase or decrease the security level according to the network performance.

In the second part, we present our contributions to improve the performance of RSSI-based localization algorithms in indoor environments in terms of accuracy, localizability, and time bound. First, we study the accuracy of the localization by using different kinds of spatial diversity. We focus on the multilateration as well as the trilateration algorithms to estimate the target position with three system models: SISO, MISO, SIMO, and MIMO. We show that the localization accuracy is improved compared to the single antenna system (SISO). We compared the average localization error using different diversity combining methods at the receiver, namely, SC, MRC and EGC. We found that MRC performs the best and that SC is the worst although this latter is the simplest in terms of implementation. Secondly, we studied the time of localization for the WSN. We proposed a distributed localization time algorithm based on MDS method called D-MDS localization time algorithm. In this algorithm, each node calculates its position and the positions of its neighbors in the local coordinate system by using the metric MDS method. Then, all the local coordinate systems are merged together into a global coordinate system.

We analyzed the performances of the proposed algorithm in terms of time complexity, and we showed that it is faster to check the relative localizability of the network compared to other algorithms.

In the last part, we present our contributions related to target tracking algorithms. We distinguished between communicating and non-communicating targets. In the case of communicating target we proposed a cluster-based tracking algorithm (CTC) which handles the trade-off between the energy conservation and the tracking performances. The tracking is achieved based on the collaboration between the different nodes of the network. High cost tasks are handled by powerful cluster heads while low-cost tasks are handled by constraint cluster members. In the case of non-communicating target, we proposed two main solutions: first, Deployment and Tracking algorithm called DTA which uses deployment strategy for both kinds of sensors: Camera Sensors (CSs), and Motion Sensors (MSs). The MSs handle the detection phase and the CSs handle the localization phase. Secondly, we proposed a Predictive Mobile Target Tracking Algorithm called PMT^2. Prediction is performed using an Enhanced Extended Kalman Filter associated with a change detection mechanism called Cumulative Summary. This combined mechanism allows to track and capture very realistic target behavior.

These contributions are results of one PhD. thesis and collaborative project:

— Ibtissam Boulanouar, PhD. thesis at University Paris-Est Marne-la-Vallée (UPEM), co-supervised with S. Lohier, and G. Roussel (see papers: [43, 45, 5, 46, 79, 44]), defended on June 2014.

— RECASURG Project: French-Tunisia Collaborative Research Project (PHC-UTIC/CMCU (Comité Mixte de Coopèration Universitaire)) regrouping 3 academic laboratories : Univ. Manouba (HANALab), Univ. Avignon (LIA), Univ. Paris-Est (LIGM). Duration : 36 months (September 2010 – August 2013). Scientific Participation : Localization and Data collecting in Wireless Sensor Networks.

Chapter 5

Conclusions and Perspectives

This chapter presents the general conclusions of this manuscript and it lists a number of perspectives for future work.

5.1 Conclusions

The research described in this manuscript is a summary of my research activities conducted during the last six years. The manuscript is divided into three main chapters related to wireless multi hop networks: Mobile Ad hoc Networks (MANETs), Vehicular Ad hoc Networks (VANETs), and Wireless Sensor Networks (WSNs).

In MANETs chapter, we present our contributions regarding QoS provisioning and security issues. Our first contribution, REFOT (Relative Fairness and Optimized Throughput) is a new dynamic rate adaptation scheme for IEEE 802.11. The added value of REFOT consists in relative fairness guarantee, and throughput optimization in MANETs. The second contribution deals with the resource allocation in the context of wireless coverage extension using MANETs. We proposed an incentive scheduler algorithm called CEI to allocate the resources taking into account not only the QoS parameters but also the cooperation rate of nodes. The key idea is to reward the relayed nodes for their cooperation instead of penalizing them by increasing the cost of cooperation. Our third contribution called MIMODog focuses on the monitoring mechanism based on an overhearing process to detect the misbehaving nodes particularly non-cooperative and selfish nodes. The originality of this solution consists in nullifying the interference at the monitor (detector) nodes and then increase the accuracy of its observation by using the spatial reuse concept with MIMO technology. The fourth contribution focuses on the distribution of the certification authority (CA) role particularly inciting nodes to actively cooperate in the security process. We consider the tradeoff between security and resource consumption by formulating the problem as a nonzero-sum noncooperative game between the CA and attacker.

The second part of this manuscript is dedicated to our contribution regarding QoS and security in data dissemination protocol in VANETs. We handled the network congestion, the overhead (related to data redundancy), and the end-to-end delay in the data dissemination protocol. We proposed ADCD solution based on the characterization of collected data (i.e. its importance, its location, and its time of collection), and the election of the broadcasters nodes. Another contribution called DMS is proposed to balance the Control Channel (CCH) load in IEEE802.11p/1609.4 using the Optimal Stoping Theory. DMS is an efficient scheduler able to tolerate derring delays before sending a packet with a higher packet delivery ratio, and a lower probability of collision. The third contribution is

related to reliability and security aspects, particularly the presence of misbehaving vehicles and their impact on the network performance. We proposed a Distributed Trust Model called DTM^2 based on signaling games, and adapted from job market-signaling model to motivate vehicles to well-behave and to detect the misbehaving ones. The concept is to allocate credits to nodes and to establish the cost of reception to access data. In order to enhance the decision making about the honesty of vehicles and to reduce the false alarms ratio, we proposed a fuzzy-based approach. Another contribution focuses on the trust metric variation and its impact on the trust model is proposed. A Markovian model is used to formalize the trust metric with different vehicles behavior and constraints related to the monitoring mechanism. Finally, we proposed a cluster-based architecture to distribute the CA role and to manage the certificates.

The third and last part of this document focuses on our contributions for WSN. We address the coexistence between security and QoS issue. We proposed a new model and framework based on PID (Proportional Integral Derivative) controller, and selective encryption approaches. In the case of PID controller, we integrate the model in the routing protocol called QwS-AODV to dynamically select the security level adapted to QoS requirements while considering the energy consumption. In the same aim, we proposed an Efficient Dynamic Selective Encryption framework called EDES to ensure adaptive security levels, QoS, and energy efficiency in the case of multimedia traffic in WSNs. The capacity function is used by EDES to assess the available resources in different paths and then it evaluates the possibility to increase or decrease the security level. This solution enables the coexistence between opposite parameters: security, QoS and energy in WSNs. For the sake of ensuring nodes localization in WSN, we focus on two main metrics: the accuracy and time bounded localization. We proposed a comparative study between different communication systems: SISO, SIMO, MISO, and MIMO to evaluate the accuracy of well-known trilateration and multilateration localization algorithms. On the other hand, we proposed a distributed and time bounded localization algorithm based on Multidimensional Scaling (MDS) approach. Finally, we address the tracking issue in WSN based on two approaches: communicating and non-communicating targets. Our contributions are based on heterogeneous WSN and different deployment strategies based on virtual forces technique. In addition, we focus on the target mobility models to predict its movement and to increase the accuracy of tracking algorithm by using the extended Kalman filter.

5.2 Perspectives

In this section, I present short to medium term research directions I intend to pursue in the future.

M2M communications over LTE-A systems: resources management and security

Machine-to-Machine (M2M) communications are a new paradigm that enables the ubiquitous connectivity and the rapid deployment of smart devices with self-organizing capabilities, able to interact with each other without any human intervention. The third generation partnership project (3GPP) has standardized M2M as machine type communication (MTC) in long term evolution and its advancements (LTE-A). 3GPP has been investigating in release 10 and beyond potential problems posed by MTC on their cellular networks optimally designed for human-to-human (H2H) communication [97], [98]. Unlike traditional H2H applications, M2M services have their own specific features: time-tolerant, small data transmission, extra low power consumption and centralized data

collection that makes M2M uplink scheduling a tricky issue to solve. In addition, 3GPP has introduced a new technology called device to device (D2D) for LTE-A in release 12. D2D is defined as the direct communication between two devices without using the base station and a core network [99]. D2D communication enables a lower power consumption (by reducing transmission power), less transmission delay, and less load of a core network. Both D2D and cellular user equipments (CUEs) links share the same radio resources. Allocate radio resources efficiently while ensuring QoS requirement for reliable communications is a challenging issue [100, 101]. Thus, new resource allocation algorithms should be developed to mitigate the co-channel interference. Another challenge is how to extend D2D communications towards multi-hop capability widely adopted in ad-hoc networks. Finally, the security is an important issue for M2M and D2D communications. The limited capabilities of devices nodes in terms of energy and computing resources make it a real challenge to directly introduce the existing solutions. The adapted solutions, and coexistence between security and QoS require an in-depth study.

This will be investigated during the ongoing Ph.D. thesis of Safa Hamdoun, co-supervised with Y. Ghamri.

Vehicular Cloud Computing (VCC): Mobility management, QoS and security awareness

As extension of my research activities related to VANETs, I will deal with an emerging topic which is Vehicular Cloud Computing (VCC). The emergence of new vehicles applications in different areas such as: navigation safety, urban surveillance, and intelligent transport enables to equip vehicles with different sensors, memory, and processing capabilities. These on board resources and the potential services can be provided and lead the conventional Vehicular Ad Hoc Network (VANET) to be viewed as Mobile Computing Cloud (MCC) where vehicles collaborate to collect information from their environment, process the data, disseminate the results and share resources to provide mobile services. This new paradigm is named Vehicular Cloud Computing (VCC) where many researchers still focus on the architectural design in order to provide reliable services. In addition, the existing solution in terms of mobility management, QoS and security in VANETs cannot be directly applied to VCC. This will be conducted by the ongoing Ph.D. thesis of Tesnim Mekki (in collaboration with Issam Jabri).

Internet of Things (IoT): Interoperability, QoS and security coexistence

In the continuity of my WSNs research, I will focus on a new emerging paradigm called Internet of Things (IoT). IoT will not be seen as individual systems, but as an integrated infrastructure upon which many technologies, applications and services can run. The IoT applications extend from sensing and actuation utility in public spaces (smart cities, smart buildings,etc) and industrial fields (smart manufacturing, smart grid, etc) to private spaces, home and apartment. People will be able to run health, energy, security and entertainment applications on the infrastructure.However, IoT concept introduces new constraints that should be considered in order to rethink and/or to adapt security mechanisms to heterogeneity of the objects' nodes. So far, the security issue has been studied in homogeneous context and without worrying about the heterogeneity in terms of technologies and constraints. The interaction between security and constraints heterogeneity should be deeply studied. Indeed, it may have different aspects:

— Considering the security level as new parameter: the security level should be negotiated according to the technologies and resources availability.

— Securing the network resources: The service level should be protected as well as the protocols that enable to negotiate and to contract this service level
— Defining a new threat model adapted to heterogeneous context.
— Choosing a security mechanism according to the needed QoS: for example, the encryption algorithms will bring an extra-delay that should be evaluated.

I plan to investigate these issues within future research projects.

Wireless Software Defined Networks (WSDN): case of multi-hop wireless scenario

Traditionally, packet switched networks consist of nodes running distributed protocols to route packets. The control of the packet's path is attributed to routers which make decisions according to the distributed algorithm. Software Defined Networks (SDN) are a new paradigm where a separation of routing strategy from the device is introduced. This separation of the control and data plans gives more flexibility and enables to control the components of the networking environment through software. In SDN, the control plan is centralized at the network controller which has a global view of the network and is capable of controlling the network infrastructure using OpenFlow protocol.

Introduce SDN paradigm in wireless networks offers many advantages like the dynamic re-programming of wireless interfaces to select the appropriate MAC protocol (e.g., switching from CSMA/CA to TDMA-based access according to the traffic load). In wireless multi-hop networks like WSNs, SDN can simplify the network management, and enables to run different applications on a single WSN. However, some expected issues must be tackled:

— In terms of QoS, the increase of the average latency of the control channel, mainly due to the control overhead. The reliability of the control channel can be negatively impacted because of the potential interference.
— In terms of security, centralizing the network controller creates a single vulnerability point where an attacker needs to compromise to get access to the entire network. In addition, decoupling the control plan from the data plan requires the network controller protocol which must be secured.

I plan to investigate these issues within future research projects.

Bibliography

[1] Mohsen Nader Tehrani, Murat Uysal, and Halim Yanikomeroglu. Device-to-device communication in 5g cellular networks: challenges, solutions, and future directions. *IEEE Communications Magazine*, 52(5):86–92, 2014.

[2] Saif Al-Sultan, Moath M. Al-Doori, Ali H. Al-Bayatti, and Hussien Zedan. A comprehensive survey on vehicular ad hoc network. *J. Netw. Comput. Appl.*, 37:380–392, January 2014.

[3] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci. Wireless sensor networks: a survey. *Computer Networks*, 38:393–422, 2002.

[4] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci. Wireless sensor networks: A survey. *Computer Networks*, 38(4):393–422, March 2002.

[5] Ibtissem Boulanouar, Abderrezak Rachedi, Stéphane Lohier, and Gilles Roussel. Energy-aware object tracking algorithm using heterogeneous wireless sensor networks. In *Proceedings of the IFIP Wireless Days Conference 2011, Niagara Falls, ON, Canada, October 10-12, 2011*, pages 1–6, 2011.

[6] Chun-Wei Tsai, Chin-Feng Lai, and Athanasios V. Vasilakos. Future internet of things: open issues and challenges. *Wireless Networks*, 20(8):2201–2217, 2014.

[7] P. Chevillat, J. Jelitto, Noll A. Barreto, and H. L. Truong. A dynamic link adaptation algorithm for IEEE 802.11a wireless LANs. pages 1141–1145, Anchorage, May 2003.

[8] Y. Xi, B.-S. Kim, J.-B. Wei, and Q.-Y. Huang. Adaptive multirate auto rate fallback protocol for ieee 802.11 wlans. In *Proceedings of IEEE Military Communications Conference (MILCOM'2006), Washington, DC, US*, 2006.

[9] G. Holland, N. Vaidya, and P. Bahl. A rate-adaptive mac protocol for multi-hop wireless networks. In *Proceedings of ACM Mo-biCom'01, Rome, Italy*, 2001.

[10] A. Kamerman and L. Monteban. Wavelan-ii: a high-performance wireless lan for the unlicensed band. *In Bell Labs Technical Journal*, 2(3):118–133, 1997.

[11] Lei Xiao, Thomas E. Fuja, and Daniel J. Costello. Mobile relaying: Coverage extension and throughput enhancement. *Transactions on Communications.*, 58(9):2709–2717, September 2010.

[12] Sheng Zhong, Jiang Chen, and Richard Yang. Sprite: A simple, cheat-proof, credit-based system for mobile ad-hoc networks. In *in Proceedings of IEEE INFOCOM*, pages 1987–1997, 2002.

[13] Yasser Toor, Paul Muhlethaler, Anis Laouiti, and Arnaud De La Fortelle. Vehicle ad hoc networks: Applications and related technical issues. *IEEE communications surveys and tutorials*, 10(3):74 – 88, 2008.

[14] IEEE 802.11-2012, IEEE Standard for Iinformation technology–Telecommunications and information exchange between systems local and

metropolitan area networks–Specific requirements part 11: Wireless lan medium access control (MAC) and physical layer (PHY) specifications, 2012.

[15] IEEE 802.11p, Amendment 6: Wireless Access in Vehicular Environments, July 2010.

[16] P. Papadimitratos, V. Gligor, and J-P. Hubaux. Securing vehicular communications - assumptions, requirements, and principles. In *WORKSHOP ON EMBEDDED SECURITY IN CARS (ESCAR)*, pages 5–14, 2006.

[17] Bryan Parno and Adrian Perrig. Challenges in securing vehicular networks. In *Workshop on Hot Topics in Networks (HotNets-IV)*, 2005.

[18] Brad Karp and H. T. Kung. Gpsr: Greedy perimeter stateless routing for wireless networks. In *Proceedings of the 6th Annual International Conference on Mobile Computing and Networking*, MobiCom '00, pages 243–254, New York, NY, USA, 2000. ACM.

[19] Long Cheng, Chengdong Wu, Yunzhou Zhang, Hao Wu, Mengxin Li, and Carsten Maple. A survey of localization in wireless sensor network. *International Journal of Distributed Sensor Networks*, 2012:1– 12, 2012.

[20] A. Benslimane, A. Rachedi, and D. Diwakar. Relative fairness and optimized throughput for mobile ad hoc networks. In *IEEE International Conference on Communications (ICC)*, Beijing, China, 2008.

[21] A. Benslimane and A. Rachedi. Rate adaptation scheme for ieee 802.11-based manets. *Journal of Network and Computer Applications (JNCA)*, 39(1):126–139, Feb 2014.

[22] C. Gueguen and A. Rachedi. Coverage extension based on incentive scheduler for mobile relaying nodes in wireless networks. In *IEEE Conference onLocal Computer Networks (LCN)*, Bonn, Germany, 2011.

[23] C. Gueguen, A. Rachedi, and M. Guizani. Incentive scheduler algorithm for cooperation and coverage extension in wireless networks. *IEEE Transactions on Vehicular Technology*, 62(2):797 – 808, Feb 2013.

[24] Abderrezak Rachedi, Hakim Badis, and Abderrahim Benslimane. How MIMO cross-layer design enables QoS while detecting non-cooperative nodes in wireless multi-hop networks. *Journal of Network and Computer Applications*, 46:395–406, November 2014.

[25] Abderrezak Rachedi, Abderrahim Benslimane, Hadi Otrok, Noman Mohammad, and Mourad Debbabi. A secure mechanism design-based and game theoretical model for MANETs. *Mobile Networking and Applications (MONET)*, 15(2):191–204, 2010.

[26] Abderrezak Rachedi, Otrok Hadi, Noaman Mohammed, Abderrahim Benslimane, and Mourad Debbabi. A mechanism design-based secure architecture for mobile ad hoc networks. In *IEEE International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob'2008)*, Avignon, France, 2008.

[27] Nadia Haddadou, Abderrezak Rachedi, and Yacine Ghamri-Doudane. Modeling and Performance Evaluation of Advanced Diffusion with Classified Data in Vehicular Sensor Networks. *Wireless Communications and Mobile Computing*, 11(12):1689–1701, 2011.

[28] Nadia Haddadou, Abderrezak Rachedi, and Yacine Ghamri-Doudane. Advanced diffusion of classified data in vehicular sensor networks. In *IWCMC'2011*, IEEE Press, pages 777–782, Istanbul, Turkey, 2011.

[29] Nadia Haddadou, Abderrezak Rachedi, and Yacine Ghamri-Doudane. To Send or To Defer? Improving the IEEE 802.11p/1609.4 Transmission Scheme. *Ad Hoc Networks* , 99(99):X.1–X.11, 2015.

[30] Nadia Haddadou, Abderrezak Rachedi, and Yacine Ghamri-Doudane. L'instant propice à l'envoi d'un message sur la couche IEEE 802.11p/1609.4. In *UbiMob2014 : 10èmes journées francophones Mobilité et Ubiquité* , Sophia Antipolis, France, 2014.

[31] Nadia Haddadou, Abderrezak Rachedi, and Yacine Ghamri-Doudane. A Job Market Signaling Scheme for Incentive and Trust Management in Vehicular Ad Hoc Networks. *IEEE Transactions on Vehicular Technology*, 64(8):3657– 3674, 2015.

[32] Nadia Haddadou and Abderrezak Rachedi. DTM^2: Adapting job market signaling for distributed trust management in vehicular ad hoc networks. In IEEE Press, editor, *IEEE ICC'2013*, pages 1827 – 1832, Budapest, Hungary, 2013.

[33] Nadia Haddadou, Abderrezak Rachedi, and Yacine Ghamri-Doudane. Trust and exclusion in vehicular ad hoc networks: an economic incentive model based approach. In *ComComAP'2013*, pages 13 – 18, Hong Kong, China, 2013.

[34] Tahani Gazdar, Abderrahim Benslimane, Abderrezak Rachedi, and Abdelfettah Belghith. A trust-based architecture for managing certificates in vehicular ad hoc networks. In *ICCIT'2012*, pages 180 – 185, Tunisia, 2012.

[35] Gazdar Tahani, Abderrezak Rachedi, Abderrahim Benslimane, and Belghith Abdelfettah. A distributed advanced analytical trust model for VANETs. In *IEEE GLOBECOM'2012*, pages 219–224, Anaheim, California, United States, 2012.

[36] Gazdar Tahani, Abderrahim Benslimane, Belghith Abdelfettah, and Abderrezak Rachedi. A secure cluster-based architecture for certificates management in vehicular networks. *Security and communication networks*, 7(3):665–683, 2014.

[37] Abderrezak Rachedi and Amina Hasnaoui. Advanced quality of services with security integration in wireless sensor networks. *Wireless Communications and Mobile Computing*, 15(6):1106–1116, 2015.

[38] Abderrezak Rachedi and Amina Hasnaoui. Security with quality-of-services optimization in wireless sensor networks. In *2013 9th International Wireless Communications and Mobile Computing Conference, IWCMC 2013, Sardinia, Italy, July 1-5, 2013*, pages 1319–1324, 2013.

[39] Abderrezak Rachedi, Lamia Kaddar, and Ahmed Mehaoua. EDES - efficient dynamic selective encryption framework to secure multimedia traffic in wireless sensor networks. In *Proceedings of IEEE International Conference on Communications, ICC 2012, Ottawa, ON, Canada, June 10-15, 2012*, pages 1026–1030, 2012.

[40] Safa Hamdoun, Abderrezak Rachedi, and Abderrahim Benslimane. Comparative analysis of RSSI-based indoor localization when using multiple antennas in wireless sensor networks. In *(MoWNeT'2013)*, pages 146 – 151, Montreal, Canada, 2013.

[41] Safa Hamdoun, Abderrezak Rachedi, and Abderrahim Benslimane. RSSI-based Localization Algorithms using Spatial Diversity in Wireless Sensor Networks. *International Journal of Ad Hoc and Ubiquitous Computing (IJAHUC)*, 19(3-4):157–167, 2015.

[42] Ferdews Tlili, Abderrezak Rachedi, and Abderrahim Benslimane. Time-bounded localization algorithm based on distributed multidimensional scaling for wireless sensor networks. In *IEEE International Conference on Communications, ICC 2014, Sydney, Australia, June 10-14, 2014*, pages 233–238, 2014.

[43] Ibtissem Boulanouar, Stéphane Lohier, Abderrezak Rachedi, and Gilles Roussel. DTA: Deployment and Tracking Algorithm in Wireless Multimedia Sensor Networks. *Ad hoc & sensor wireless networks*, 28(1-2):115–135, 2015.

[44] Ibtissem Boulanouar, Stéphane Lohier, Abderrezak Rachedi, and Gilles Roussel. CTA: a collaborative tracking algorithm in wireless sensor networks. In *ICNC' 2013*, pages 529 – 534, San Diego, United States, January 2013.

[45] Ibtissem Boulanouar, Stéphane Lohier, Abderrezak Rachedi, and Gilles Roussel. Pmt^2: A predictive mobile target tracking algorithm in wireless multimedia sensor networks. In *IEEE Symposium on Computers and Communications, ISCC 2014, Funchal, Madeira, Portugal, June 23-26, 2014*, pages 1–7, 2014.

[46] Ibtissem Boulanouar, Stéphane Lohier, Abderrezak Rachedi, and Gilles Roussel. PTA : A Predictive Tracking Algorithm in Wireless Multimedia Sensor Networks. In *Global Information Infrastructure Symposium (GIIS)*, pages 1 – 6, Trento, Italy, October 2013.

[47] A. Rachedi and H. Badis. MIMODog: How to solve the problem of selfish misbehavior detection mechanism in MANETs using MIMO Technology. In *The 8th International Wireless Communications & Mobile Computing Conference (IWCMC) Limassol, Cyprus*, 2012.

[48] P. Chevillat, J. Jelitto, B.-A. Noll, and H.-L. Truong. A dynamic link adaptation algorithm for ieee 802.11a wireless lans. In *Proceedings of IEEE International Conference on Communications (ICC'2003),Anchorage, AK*, 2003.

[49] G. Bianchi. Performance analysis of the ieee 802.11 distributed coordianation function. *IEEE Journal on Selected Areas in Communications*, 18(3):535–547, 2000.

[50] Dah-Ming Chiu and Raj Jain. Analysis of the increase and decrease algorithms for congestion avoidance in computer networks. *Comput. Netw. ISDN Syst.*, 17(1):1–14, June 1989.

[51] Matthew Andrews, Krishnan Kumaran, and Kavita Ramanan. Providing quality of service over a shared wireless link. *IEEE Communications Magazine*, 39:150–154, Feb. 2001.

[52] Xudong Wang and Weidong Xiang. An OFDM-TDMA/SA MAC protocol with QoS constraints for broadband wireless LANs. *ACM/Springer Wireless Networks*, 12(2):159 – 170, 2006.

[53] J. S. Park, N. Alok, M. Gerla, and H. Lee. Space-mac: Enabling spatial reuse using mimo channel-aware mac. In *Proceedings of International Conference Communications (ICC)*, 2005.

[54] V. Simoncini. Variable accuracy of matrix-vector products in projection methods for eigencomputation. *SIAM Journal on Numerical Analysis*, (3):1155 – 1174, 2006.

[55] J. P. Hubaux I. Aad and E. W Knightly. Impact of denial of service attacks on ad hoc networks. *IEEE/ACM Transactions on Networking (TON)*, (4):791 – 802, 2008.

[56] A. Rachedi and A. Benslimane. A secure architecture for mobile ad hoc networks. In *proceedings of International Conference MSN'06, LNCS*, volume 4325, pages 424–435, China, 2006.

[57] A. Mas-Colell, M. Whinston, and J. Green. *Microeconomic Theory.* Oxford University Press, New York, 1995.

[58] M. Willem. *Minimax Theorem.* Birkhauser, USA, 1996.

[59] J. Whitbeck, V. Conan, and M. Dias de Amorim. Performance of opportunistic epidemic routing on edge-markovian dynamic graphs. *IEEE Transactions on Communications*, 59(5):1259–1263, May 2011.

[60] Uichin Lee, Biao Zhou, M. Gerla, E. Magistretti, P. Bellavista, and A. Corradi. Mobeyes: Smart mobs for urban monitoring with a vehicular sensor network. *Wireless Communications*, 13(5):52–57, October 2006.

[61] IEEE 1609.4-2010. Wireless Access in Vehicular Environments (WAVE)-Multi-channel Operation. In IEEE S*tandard*, Feb 2011.

[62] ASTM International. Telecommunications and Information Exchange Between Roadside and Vehicle Systems - 5 GHz Band Dedicated Short Range Communications (DSRC) Medium Access Control (MAC) and Physical Layer (PHY) Specifications. In S*tandard* S*pecification*, April 2009.

[63] S. Eichler. Performance evaluation of the ieee 802.11p wave communication standard. In *IEEE 66th Vehicular Technology Conference (VTC Fall'07)*, Baltimore, MD, USA, November 2012.

[64] C. Campolo, A. Molinaro, and A. Vinel. Understanding the performance of short-lived control broadcast packets in 802.11p/wave vehicular networks. In *IEEE Vehicular Networking Conference (VNC'11)*, Amsterdam, Netherlands, November 2011.

[65] Y.S. Chow, H. Robbins, and D. Siegmund. *Great expectations : the theory of optimal stopping*. Boston [etc.] : Houghton Mifflin, 1971.

[66] J. Taylor. Markov decision processes: Lecture notes for stp 425. In *Stochastic Processes*, Nov 2012.

[67] Standards Committee. Wireless Lan Medium Access Control (MAC) and Physical layer (PHY) specifications:. In A*mendment 8:* M*edium* A*ccess* C*ontrol* (MAC) Q*uality of* S*ervice* E*nhancements*, Jan 2005.

[68] M. L. Puterman. Chapter 8 markov decision processes. *Handbooks in Operations Research and Management Science*, 2:331 – 434, 1990.

[69] Marco Di Felice, Ali J. Ghandour, Hassan Artail, and Luciano Bononi. On the impact of multi-channel technology on safety-message delivery in IEEE 802.11p/1609.4 vehicular networks. In *21st International Conference on Computer Communications and Networks, ICCCN 2012, Munich, Germany, July 30 - August 2, 2012*, pages 1–8, 2012.

[70] K. Govindan and P. Mohapatra. Trust Computations and Trust Dynamics in Mobile Adhoc Networks: A Survey. *IEEE Communications Surveys Tutorials* , 14(2):279 – 298, 2012.

[71] Félix Gómez Mármol, Javier G. Marín-Blázquez, and Gregorio Martínez Pérez. Lftm, linguistic fuzzy trust mechanism for distributed networks. *Concurr. Comput. : Pract. Exper.*, 24(17):2007–2027, December 2012.

[72] Dijiang Huang, Xiaoyan Hong, and Mario Gerla. Situation-aware trust architecture for vehicular networks. *IEEE Communication Magazine*, 48(11):128–135, November 2010.

[73] Félix Gómez Mármol and Gregorio Martínez Pérez. Trip, a trust and reputation infrastructure-based proposal for vehicular ad hoc networks. *Journal of Network Computing Applications*, 35(3):934–941, May 2012.

[74] Ayman Tajeddine, Ayman Kayssi, and Ali Chehab. A privacy-preserving trust model for vanets. In *Proceedings of the 2010 10th IEEE International Conference on Computer and Information Technology*, CIT '10, pages 832–837, 2010.

[75] J. Sobel. Signaling games. *Computational Complexity Theory, Techniques, and Applications*, pages 2830–2844, 2012.

[76] Le site du trusted platform module (tpm). `https://www.trustedcomputinggroup.org/groups/tpm/`.

[77] Z. Charikleia, L.M. Brian, H. Marek, and K.T. Roshan. Robust cooperative trust establishment for manets. In *ACM SASN*, New York, USA, 2006.

[78] Felix Gomez Marmol, Javier G. Marine Blazquez, and Gregorio Martinez Perez. Lftm, linguistic fuzzy trust mechanism for distributed networks. *Journal Concurrency and Computation: Practice Experience*, 24(17):2007–2027, December 2012.

[79] Ibtissem Boulanouar, Stéphane Lohier, Abderrezak Rachedi, and Gilles Roussel. A Collaborative Tracking Algorithm for Communicating Target in Wireless Multimedia Sensor Networks. In *7th IFIP Wireless and Mobile Networking Conference (WMNC)*, pages 1 – 7, Vilamoura, Algarve, Portugal, May 2014.

[80] Ian F Akyildiz, Tommaso Melodia, and Kaushik R Chowdhury. A survey on wireless multimedia sensor networks. *Computer networks*, 51(4):921–960, 2007.

[81] Zhi Sun, Pu Wang, Mehmet C. Vuran, Mznah A. Al-Rodhaan, Abdullah M. Al-Dhelaan, and Ian F. Akyildiz. Bordersense: Border patrol through advanced wireless sensor networks. *Ad Hoc Netw.*, 9(3):468–477, May 2011.

[82] S. Blake, D. Black, M. Carlson, E. Davies, Z. Wang, and W. Weiss. An architecture for differentiated service. United States, 1998. RFC 2475.

[83] Leonardo Badia, Magnus Lindström, Jens Zander, Jens Z, and Michele Zorzi. An economic model for the radio resource management in multimedia wireless systems. *Computer Communications*, 2004:27–1056, 2003.

[84] H. Krawczyk, M. Bellare, and R. Canetti. Hmac: Keyed-hashing for message authentication. United States, 1997. RFC 2104.

[85] Youngmin Kwon, Kirill Mechitov, Sameer Sundresh, Wooyoung Kim, and Gul Agha. Resilient localization for sensor networks in outdoor environments. *ACM Trans. Sen. Netw.*, 7(1):1–30, August 2010.

[86] Niculescu Dragos and Nath Badri. Dv based positioning in ad hoc networks. *Telecommunication Systems*, 22(1-4):267–280, 2003.

[87] Armin Runge, Marcel Baunach, and Reiner Kolla. Precise self-calibration of ultrasound based indoor localization systems. In *2011 International Conference on Indoor Positioning and Indoor Navigation, IPIN 2011, Guimaraes, Portugal, September 21-23, 2011*, pages 1–8, 2011.

[88] Wei Cheng, Nan Zhang, Xiuzhen Cheng, Min Song, and Dechang Chen. Time-bounded essential localization for wireless sensor networks. *IEEE/ACM Trans. Netw.*, 21(2):400–412, 2013.

[89] Yi Zou and Krishnendu Chakrabarty. Sensor deployment and target localization based on virtual forces. In *INFOCOM*, San Francisco, California, USA, 2003.

[90] Samuel Fernández, David Gualda, Juan Carlos García, Juan Jesús García, Jesús Ureña, and Raquel Gutiérrez. Indoor location system based on zigbee devices and

metric description graphs. In *IEEE International Symposium on Intelligent Signal Processing (WISP)*, Floriana, Malta, 2011.

[91] Yun Wang, Xiaodong Wang, Demin Wang, and Dharma P Agrawal. Range-free localization using expected hop progress in wireless sensor networks. *Parallel and Distributed Systems, IEEE Transactions on*, 20(10):1540–1552, 2009.

[92] Yahya Esmail Osais, Marc St-Hilaire, and R Yu Fei. Directional sensor placement with optimal sensing range, field of view and orientation. *Mobile Networks and Applications*, 15(2):216–225, 2010.

[93] F. Gustafsson. *Adaptive filtering and change detection*, volume 1. Wiley New York, 2000.

[94] Yannick Benezeth, Pierre-Marc Jodoin, Bruno Emile, Hélène Laurent, and Christophe Rosenberger. Review and evaluation of commonly-implemented background subtraction algorithms. In *International Conference on Pattern Recognition (ICPR)*, Tampa, FL, USA, 2008.

[95] H. Oztarak, K. Akkaya, and A. Yazici. Efficient localization and tracking of multiple objects in wireless multimedia sensor networks. *Ad Hoc and Wireless Sensor Networks*, 19, 2013.

[96] Paul Zarchan and Howard Musoff. *Fundamentals of Kalman filtering: a practical approach*, volume 208. Aiaa, 2005.

[97] 3gpp ts 22.368 v10.1.0, "service requirements for machine-type communications, 2012.

[98] 3gpp ts 22.888 v11.0.0, "system improvement for machine-type communication, 2012.

[99] Arash Asadi, Qing Wang, and Vincenzo Mancuso. A survey on device-to-device communication in cellular networks. *IEEE Communications Surveys and Tutorials*, 16(2), 2014.

[100] Zubair Md. Fadlullah, Mostafa Fouda, Nei Kato, Akira Takeuchi, Noboru Iwasaki, and Yousuke Nozaki. Toward intelligent machine-to-machine communications in smart grid. *IEEE Communications Magazine*, 49(4):60–65, 2011.

[101] Yan Zhang, Rong Yu, Shengli Xie, Wenqing Yao, Yang Xiao, and Mohsen Guizani. Home m2m networks: Architectures, standards, and qos improvement. *IEEE Communications Magazine*, 49(4):44–52, 2011.

List of publications

Books and book chapters (04)

[1] H. Badis, **A. Rachedi**, "Modeling tools to evaluate the performance of wireless multi-hop networks", in book entitled: *"Modeling and simulation of computer networks and systems: methodologies and applications"*, Eds. M. S. Obaidat, F. Zarai and P. Nicopolitidis, Elsevier, 2015, ISBN: 978-0128008874.

[2] **Abderrezak Rachedi**, "Monitoring Mechanisms for Wireless Sensor Networks: Challenges and Solutions", in book titled: *Wireless Sensor Networks: From Theory To Applications*, Eds. Ibrahiem M. M. El Emary & S.Ramakrishnan, CRC Press, Taylor and Francis Group, 2014. ISBN: 9781466518100.

[3] T. Lemlouma, S. Laborie, P. Roose, **A. Rachedi**, K. Abdelaziz, "mHealth Contents and Services Delivery and Adaptation Challenges for Smart Environments", chapter 17, in book titled: *"Mobile Health (mHealth): Multidisciplinary Verticals"* , Eds. S. Adibi, pages 295-314, ISBN 9781482214802, CRC Press, Taylor and Francis Group.

[4] **Abderrezak Rachedi**, "Contribution à la sécurité dans les réseaux mobiles ad hoc", *Mécanismes de Prévention, de Détection et de Réaction*, by Presses Acamdémiques Francophones, ISBN 978-3-8381-8877-5.

Articles in refereed international journals (18)

[5] N. Haddadou, **A. Rachedi**, Y. Ghamri, "To Send or To Defer ? Improving the IEEE 802.11p/1609.4 Transmission Scheme", in *Ad hoc Networks, Elsevier journal.* 2015. (Accepted with revision)

[6] A. Bradai, K. Singh ,**A. Rachedi**, A. Toufik, "EMCOS: Energy-efficient Mechanism for Multimedia Streaming over Cognitive Radio Sensor Networks", in *Pervasive and Mobile Computing, Elsevier journal.* Volume 22, Pages: 16–32, 2015.

[7] N. Haddadou, **A. Rachedi**, Y. Ghamri, " A Job Market Signaling Scheme for Incentive and Trust Management in Vehicular Ad Hoc Networks", in *IEEE Transactions on Vehicular Technology (TVT).* Volume: 64, Issue: 8, pages: 3657- 3674, 2015.

[8] I. Boulanouar, S. Lohier, **A. Rachedi**, G. Roussel, "DTA: Deployment and Tracking Algorithm in Wireless Multimedia Sensor Networks", in *Ad Hoc and Sensor Wireless Networks*, Volume: 28, Issue: 1-2, pages: 115-135, 2015.

[9] **A. Rachedi**, A. Hasnaoui, "Advanced Quality-of-Services with Security Integration in Wireless Sensor Networks", in *Wireless Communications and Mobile Computing*

journal (WCMC), John Wiley InterScience. Vol. 15, Issue 6, pp. 1106-1116, 2015. DOI: 10.1002/wcm.2562.

[10] S. Hamdoun, **A. Rachedi**, A. Benslimane , "RSSI-based Localization Algorithms using Spatial Diversity in Wireless Sensor Networks", in *International Journal of Ad Hoc and Ubiquitous Computing (IJAHUC)*. Volume: 19, Issue: 3-4, pp.157-167, 2015.

[11] M. Bouaziz, **A. Rachedi**, "A Survey on Mobility Management Protocols in Wireless Sensor Networks based on 6LoWPAN Technology", in *Computer Communications (ComCom), Elsevier Journal*. 2015. (In Press) DOI: 10.1016/j.comcom.2014.10.004.

[12] **A. Rachedi**, H. Badis, A. Benslimane, "How MIMO cross-layer design enables QoS while detecting non-cooperative nodes in wireless multi-hop networks", in *Journal of Network and Computer Applications (JNCA), Elsevier Journal*. Vol. 46, pp.395-406. 2014.

[13] M. H. Rehmani, **A. Rachedi**, S. Lohier, T. Alves, B. Poussot, "Intelligent Antenna Selection Decision in IEEE 802.15.4 Wireless Sensor Networks: An Experimental Analysis", in *Computers and Electrical Engineering, Elsevier Journal*. Volume 40, Issue 2, pages: 443-455, 2014.

[14] A. Benslimane, **A. Rachedi**, " Rate Adaptation scheme for IEEE 802.11-based MANETs", in *Journal of Network and Computer Applications (JNCA), Elsevier Journal*. Volume: 39, Pages: 126-139, 2014.

[15] T. Gazdar, A. Benslimane, A. Belghith, **A. Rachedi**, "A Secure Cluster-based Architecture for Certificates Management in Vehicular Networks", in *Security and Communication Networks (SCN), John Wiley InterScience*, Volume 7, Issue 3, pages 665–683, 2014.

[16] C. Gueguen, **A. Rachedi**, M. Guizani, "Incentive Scheduler Algorithm for Cooperation and Coverage Extension in Wireless Networks", in *IEEE Transactions on Vehicular Technology (TVT)*, Vol. 62, Issue 2, Pages: 797- 808, 2013.

[17] **A. Rachedi**, S. Lohier, S. Cherrier and I. Salhi, "Wireless Network Simulators Relevance Compared to a Real Testbed in Outdoor and Indoor Environments", in *International Journal of Autonomous and Adaptive Communications Systems (IJAACS)*, Volume 5, Number 1, 2012.

[18] N. Haddadou, **A. Rachedi**, Y. Ghamri, "Modeling and Performance Evaluation of Advanced Diffusion with Classified Data in Vehicular Sensor Networks", in *Wireless Communications and Mobile Computing journal (WCMC), John Wiley InterScience*, Volume 11, Issue 12, pages 1689-1701, 2011.

[19] **A. Rachedi**, A. Benslimane, H. Otrok, N. Muhamed and M. Debbabi, "A Secure Mechanism Design-Based and Game Theoretical Model for MANETs", in *Mobile Networking and Applications journal (MONET), ACM/Springer*, Volume 15, Number 2, 2010.

[20] **A. Rachedi**, and A. Benslimane, "A Secure and Resistant Architecture against Attacks for Mobile Ad Hoc Networks", in *Security and Communication Network journal (SCN), John Wiley InterScience*, Volume 3 Issue 2-3, Pages 150 - 166, 2010.

[21] **A. Rachedi** and A. Benslimane, "Impacts and Solutions of Control Packets Vulnerabilities with IEEE 802.11 MAC", in *Wireless Communications and Mobile*

Computing journal (WCMC), John Wiley InterScience, Volume 9, Issue 4, Pages: 469-488, 2009.

[22] **A. Rachedi** and A. Benslimane, "Toward a Cross-layer Monitoring Process for Mobile Ad Hoc Networks", in *Security and Communication Network journal (SCN), John Wiley InterScience*, Volume 2 Issue 4, Pages 351-368, 2009 DOI: 10.1002/sec.72

Articles in refereed international conferences (45)

[23] S. Hamdoun, **A. Rachedi**, Y. Ghamri, "Radio Resource Sharing for MTC in LTE-A: An Interference-Aware Bipartite Graph Approach", *in the IEEE Global Communications Conference: Wireless Networks (GC'2015)*, San Diego, CA, USA, 6-10 December 2015.

[24] A. Bradai, K. D. Singh, **A. Rachedi**, T. Ahmed, "Clustering in Cognitive Radio for Multimedia Streaming over Wireless Sensor Networks", *in the 11th International Wireless Communications & Mobile Computing Conference (IWCMC'2015)*, Dubrovnik, Croatia. August 24-28, 2015.

[25] H. Badis, and **A. Rachedi**, "Performance Evaluation of MIMO-based MAC/PHY cross-layer design in multi-hop ad hoc networks", *In 11th IEEE International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, Abu-Dhabi, UAE, October 2015.

[26] A. Boulemtafes, **A. Rachedi**, and N. Badache, "A Study of Mobility Support in Wearable Health Monitoring Systems: Design Framework", *In ACS/IEEE International Conference on Computer Systems and Applications (AICCSA)*, Marrakech, Morocco, November 2015.

[27] H. Nguyen-Minh, A. Benslimane, and **A. Rachedi**, "Jamming Detection on 802.11p under Multi-channel Operation in Vehicular Networks", *In 11th IEEE International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, Abu-Dhabi, UAE, October 2015.

[28] S. Hamdoun, **A. Rachedi**, Y. Ghamri, "Partage des ressources radio pour MTC dans LTE-A: Une approche basée sur le graphe biparti", *12ème Conférence Internationale sur les NOuvelles TEchnologies de la REpartition (NOTERE)*, Paris, France. 24-27 July, 2015.

[29] F. Tlili, **A. Rachedi**, A. Benslimane, "Time-bounded Localization Algorithm based on Distributed Multidimensional Scaling for Wireless Sensor Networks", *in the IEEE International Conference on Communications (IEEE ICC'2014)*, Sydney, Australia, June 23-26 2014.

[30] I. Boulanouar, S. Lohier, **A. Rachedi**, G. Roussel, "PMT^2: A Predictive Mobile Target Tracking Algorithm in Wireless Multimedia Sensor Networks", *19th IEEE Symposium on Computers and Communications (IEEE ISCC'2014)*, Madeira, Portugal, June 23-26 2014.

[31] I. Boulanouar, S. Lohier, **A. Rachedi**, G. Roussel, "A Collaborative Tracking Algorithm for Communicating Target in Wireless Multimedia Sensor Networks", *7th IFIP Wireless and Mobile Networking Conference (WMNC 2014)*, Vilamoura, Algarve, Portugal, May 20-22, 2014.

[32] A. Bradai, T. Ahmed, **A. Rachedi**, "Enhancing content dissemination for ad hoc cognitive radio", *in the 10th International Wireless Communications & Mobile Computing Conference (IWCMC'2014)*, Nicosia, Cyprus, Aug. 4-8, 2014.

[33] N. Haddadou, **A. Rachedi**, "L'instant propice à l'envoi d'un message sur la couche IEEE 802.11p/1609.4", *10èmes journées francophones Mobilité et Ubiquité (UbiMob2014)*, Sophia Antipolis, France. 2014.

[34] I. Boulanouar, S. Lohier, **A. Rachedi**, G. Roussel, "PTA: A Predictive Tracking Algorithm in Wireless Multimedia Sensor Networks", *in the Global Information Infrastructure and Networking Symposium (GIIS'2013)*, Trento, Italy, Oct. 28-31, 2013.

[35] T. Lemlouma, **A. Rachedi**, M. A. Chalouf, S. Ait Chellouche, "A New Model for NGN Pervasive eHealth Services ", *International Symposium on Future Information and Communication Technologies for Ubiquitous HealthCare*, Jinhua, China, 2013.

[36] N. Haddadou, **A. Rachedi**, "DTM^2: Adapting Job Market Signaling for Distributed Trust Management in Vehicular Ad Hoc Networks", *in the IEEE International Conference on Communications (ICC'2013)*, June 9-13, Budapest, Hungary, 2013. (IEEE Press)

[37] S. Hamdoun, **A. Rachedi**, A. Benslimane, "Comparative Analysis of RSSI-based Indoor Localization when using Multiple Antennas in the in Wireless Sensor Networks", *International Conference on Selected Topics in Mobile and Wireless Networking (MoWNeT)*, Montreal, Canada, June 9-13, Aug 2013. (IEEE Press)

[38] **A. Rachedi**, A. Hasnaoui, "Security with Quality-of-Services Optimization in Wireless Sensor Networks", *in the 9th International Wireless Communications & Mobile Computing Conference (IWCMC'2013)*, Cagliari, Italy, July 1st-5th, 2013. (IEEE Press)

[39] M. H. Rehmani, **A. Rachedi**, S. Lohier, T. Alves, B. Poussot, "On the Feasibility of making Intelligent Antenna Selection Decision in IEEE 802.15.4 Wireless Sensor Networks", *in Computers, Communications and IT Applications Conference (ComComAP 2013)*, Hong Kong, China. (IEEE Press)

[40] N. Haddadou, **A. Rachedi**, Y. Ghamri, "Trust and Exclusion in Vehicular Ad Hoc Networks: An Economic Incentive Model based Approach", *in Computers, Communications and IT Applications Conference (ComComAP 2013)*, Hong Kong, China. (IEEE Press)

[41] I. Boulanouar, S. Lohier, **A. Rachedi**, G. Roussel, "CTA: a Collaborative Tracking Algorithm in Wireless Sensor Networks", *in the IEEE International Conference on Computing, Networking and Communications (ICNC 2013)*, Jan 2013, San Diego, United States. (IEEE Press)

[42] T. Gazdar, **A. Rachedi**, A. Benslimane, A. Belghith, "A Distributed Advanced Analytical Trust Model for VANETs", *the 55th annual IEEE Global Telecommunications Conference (GLOBECOM'2012)*, Anaheim, California , Dec. 3-7, 2012. (IEEE Press)

[43] **A. Rachedi**, H. Badis, "MIMODog: How to solve the problem of Selfish Misbehavior Detection Mechanism in MANETs Using MIMO Technology", *in the IEEE*

The 8th International Wireless Communications & Mobile Computing Conference (IWCMC'2012), Limassol, CYPRUS, August 27-31, 2012. (IEEE Press)

[44] **A. Rachedi**, Lamia Kaddar, Ahmed Mehaoua, "DES - Efficient Dynamic Selective Encryption Framework to Secure Multimedia Traffic in Wireless Sensor Networks", *in the IEEE International Conference on Communications (ICC'2012)*, pp. 1041-1045, Ottawa, Canada, June 10-15, 2012. (IEEE Press)

[45] H. R. Mubashir, T. Alves, S. Lohier, **A. Rachedi**, B. Poussot, "Towards Intelligent Antenna Selection in IEEE 802.15.4 Wireless Sensor Networks". *The International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc2012)*, pp. 245-246, South Carolina, United States, 2012. (ACM Press)

[46] T. Gazdar, A. Benslimane, **A. Rachedi**, A. Belghith, "A Trust-based Architecture for Managing Certificates in Vehicular Ad hoc Networks". *in the 2nd International Conference on Communications and Information Technology (ICCIT)*, Hammamat, Tunisia, June 26-28, 2012. (IEEE Press)

[47] M. H. Rehmani, S. Lohier, **A. Rachedi**, "Channel Bonding in Cognitive Radio Wireless Sensor Networks". *International Conference on Selected Topics in Mobile and Wireless Networking (iCOST)*, Avignon, France, July 2-4, 2012. (IEEE Press)

[48] C. Gueguen, **A. Rachedi**, "Coverage Extension Based on Incentive Scheduler for Mobile Relaying Nodes in Wireless Networks", in *36th Annual IEEE Conference on Local Computer Networks (LCN'2011)*, Bonn, Germany, October 4 - 7, 2011. (IEEE Press)

[49] I. Boulanouar, **A. Rachedi**, S. Lohier, G. Roussel, "Energy-Aware Object Tracking Algorithm using Heterogeneous Wireless Sensor Networks", in *4th. IFIP/IEEE Wireless Days 2011 (WD'2011)*, Niagara Falls, Ontario, Canada, October 10-12. (IEEE Press)

[50] S. Lohier, **A. Rachedi**, I. Salhi, E. Livolant, "Multichannel Access for Bandwidth Improvement in IEEE 802.15.4 Wireless Sensor Networks", in *4th. IFIP/IEEE Wireless Days 2011 (WD'2011)*, Niagara Falls, Ontario, Canada, October 10-12. (IEEE Press)

[51] S. Lohier, **A. Rachedi**, E. Livolant, I. Salhi, "Wireless Sensor Network Simulators Relevance compared to a real IEEE 802.15.4 Testbed", in *the International Wireless Communications and Mobile Computing Conference (IWCMC'2011)*, Istanbul, Turky, July 5-8, 2011. (IEEE Press)

[52] N. Haddadou, **A. Rachedi**, Y. Ghamri, "Advanced Diffusion of Classified Data in Vehicular Sensor Networks", in *the International Wireless Communications and Mobile Computing Conference (IWCMC'2011)*, Istanbul, Turky, July 5-8, 2011. (IEEE Press)

[53] **A. Rachedi**, and H. Baklouti, "muDog: Smart Monitoring Mechanism for Wireless Sensor Networks based on IEEE 802.15.4 MAC", in *the IEEE International Conference on Communications (ICC'2011)*, Kyoto, Japan, 5-9 June 2011. (IEEE Press)

[54] **A. Rachedi**, S. Lohier, S. Cherrier and I. Salhi, "Wireless Network Simulators Relevance Compared to a Real Testbed in Outdoor and Indoor Environments", in *the International Wireless Communications and Mobile Computing Conference (IWCMC'2010)*, Cean, France, June 28 - July 2, 2010. (ACM Press)

[55] S. Lohier, **A. Rachedi** and Y. Ghamri, "Cost Function for QoS-Aware Routing in Multi-tier Wireless Multimedia Sensor Networks", in *the 12th IFIP/IEEE International Conference on Management of Multimedia and Mobile Networks and Services (MMNS'2009)*, Lecture Notes in Computer Science 5842, pp. 81-93, Venice, Italy, October 26 - 30, 2009.

[56] **A. Rachedi** and A. Benslimane, "Security and Pseudo-Anonymity with a Cluster-based approach for MANET", in *the 51th annual IEEE Global Telecommunications Conference (GLOBECOM'2008)*, pp. 1-6, New Orleans, LA, USA, 30 Nov.-3 Dec. 2008. (IEEE Press).

[57] **A. Rachedi**, A. Benslimane, H. Otrok, N. Mohammed and M.Debbabi, "A Mechanism Design-Based Secure Architecture for Mobile Ad Hoc Networks", in *the 4th IEEE International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob'2008)*, pp. 417-422, Avignon, France, 12-14 Oct. 2008. (IEEE Press)

[58] **A. Rachedi** and A. Benslimane, "Smart Attacks based on Control Packets Vulnerabilities with IEEE 802.11 MAC", in *the International Wireless Communications and Mobile Computing Conference (IWCMC'2008)*, pp. 588-593, August 6-8, 2008. Crete Island, Greece. (IEEE Press)

[59] A. Benslimane, **A. Rachedi** and D. Diwakar, "Relative Fairness and Optimized Throughput for Mobile Ad hoc Networks", in *the IEEE International Conference on Communications (ICC'2008)*, pp. : 2233-2237, Beijing, China, 19-23 May, 2008. (IEEE Press)

[60] **A. Rachedi** and A. Benslimane, "Cross-Layer approach to improve the monitoring process for Mobile Ad Hoc Networks based on IEEE 802.11", in *the 50th annual IEEE Global Telecommunications Conference (GLOBECOM'2007)*, pp. 1086-1091, Washington, DC, USA, 26-30 November 2007. (IEEE Press)

[61] **A. Rachedi**, A. Benslimane, L. Guang and C. Assi, "A Confident Community to Secure Mobile Ad-Hoc Networks", in {*the IEEE International Conference on Communications (ICC'2007)*, pp. 1254 - 1259, Glasgow, Scotland, UK, 24-28 June 2007. (IEEE Press)

[62] **A. Rachedi** and A. Benslimane, "A Secure Architecture for Mobile Ad Hoc Networks", in *the 2nd International Conference on Mobile Ad-Hoc and Sensor Networks (MSN2006)*, Lecture Notes in Computer Science 4325, pp.424-435, Hong Kong, China, December 2006. (LNCS Press)

[63] **A. Rachedi** and A. Benslimane, "Trust and Mobility-based Clustering Algorithm for Secure Mobile Ad Hoc Networks". in *the International Conference on Systems and Networks Communications (ICSNC06)*, pp. 72-78, Tahiti, Frunch Polynesia, October 2006 (IEEE Press)

Articles in refereed national conferences (04)

[64] **A. Rachedi**, A. Benslimane, S. Lohier, H. Badis, E. Duris, and G. Roussel, "Surveillance dans les rseaux de capteurs et les rseaux mobiles ad hoc", *dans la 4eme Confrence sur la Scurit des Architectures Rseaux et des Systmes d'Information (SARSSI 2009)*,

[65] **A. Rachedi** and A. Benslimane, "Gestion de confiance et résistance aux attaques dans les réseaux Ad hoc mobiles", *8ème Colloque Francophone de Gestion de Réseaux et de Services, "L'adaptation dynamique des réseaux et des services" (GRES2007).* Hammamet, Tunisie. (Hermes Press)

[66] **A. Rachedi**, and A. Benslimane, "Architecture Hiérarchique Distribuée pour sécuriser les réseaux Ad hoc Mobiles", *8ème Journées Doctorales en Informatique et Réseaux JDIR'2007*, Marne la Vallée.

[67] A. Belkhir, M. D. Naci et **A. Rachedi**, "Contribution à la sécurité du PDA : IDS Embarqué EIDS", *SAR'04 (rencontre francophone sur Sécurité et Architecture Réseaux), 3ème Conférence sur la Sécurité et Architectures Réseaux.* La Londe, France, 2004